Model vrjednovanja informacijske transparentnosti politika privatnosti

Alić, Marta

Sveučilište u Zagrebu

Filozofski fakultet

University of Zagreb

Faculty of Humanities and Social sciences

Marta Alić

MODEL VRJEDNOVANJA INFORMACIJSKE TRANSPARENTNOSTI POLITIKA PRIVATNOSTI

DOKTORSKI RAD

Zagreb, 2022.

Sveučilište u Zagrebu

Filozofski fakultet

Marta Alić

MODEL VRJEDNOVANJA INFORMACIJSKE TRANSPARENTNOSTI POLITIKA PRIVATNOSTI

DOKTORSKI RAD

Mentor:

prof. dr. sc. Ljerka Luić

Zagreb, 2022.

University of Zagreb

Faculty of Humanities and Social sciences

Marta Alić

EVALUATION MODEL OF PRIVACY POLICY INFORMATION TRANSPARENCY

DOCTORAL THESIS

Supervisor:

Prof. Ljerka Luić, PhD

Zagreb, 2022.

Informacije o mentorici

Ljerka Luić, izvanredni profesor, ima multidisciplinarno visoko obrazovanje (tehničko: strojarstvo; pedagoško: profesor politehnike; društveno: magisterij i doktorat znanosti iz polja informacijskih i komunikacijskih znanosti), kao i multidisciplinarno profesionalno iskustvo (programer, inženjer informacijskog sustava, direktor edukacije i ljudskih resursa, direktor razvoja poslovanja) koje je stekla radom u istraživačkoj instituciji (Institut za istraživanje i razvoj), međunarodnoj korporaciji (ABB, SAP) i konzultantskoj tvrtki (B4B), te znanstveno-nastavno iskustvo (Sveučilište Sjever, Filozofski fakultet i Medicinski fakultet Sveučilišta u Zagrebu, Veleučilište u Karlovcu). Certificirani je predavač International Education Society (IES), London. Stručno se usavršavala u inozemstvu (Walldorf i Heidelberg, Njemačka; Chicago, SAD) u području istraživanja i primjene IT/IS rješenja u poslovanju u visokom obrazovanju, zdravstvu i javnom sektoru.

Na Sveučilištu Sjever zaposlena je od 2015. godine. Prvotno kroz dopunski rad, potom zaposlenje u nepunom radnom vremenu, a od 2019. godine na neodređeno puno radno vrijeme na radnom mjestu izvanrednog profesora iz znanstvenog područja društvenih znanosti, polja informacijskih i komunikacijskih znanosti. Objavila je ukupno 75 koautorskih znanstvenih radova, 1 udžbenik, 2 priručnika. Sudjelovala je na više od 50 međunarodnih znanstvenih skupova. Bila je mentoricom 120 završnih/diplomskih radova. Trenutno je mentorica doktorandima pri izradi 2 doktorska rada.

U fokusu njenog znanstveno-istraživačkog interesa su informacije i informacijsko-komunikacijske znanosti, koje se koncentrično šire kroz teme digitalne inteligencije, digitalne pismenosti, digitalnih komunikacija i kompetencija, informatologije, informacijskih sustava, poslovne inteligencije.

Dobitnica je HIZ nagrade SREBRNA ZNAČKA za doprinos razvoju informatičke struke u Hrvatskoj i E-BIZ priznanja za doprinos razvoju elektroničkog poslovanja u Hrvatskoj.

CROSBI profil radova:
https://www.bib.irb.hr/profile/22964

Google Znalac profil citata:
https://scholar.google.com/citations?user=uZGG5uoAAAAJ

POIROT profil znanstvenih projekata:
https://pdb.irb.hr/search?q=&qId=&q=ljerka+lui%C4%87&type=leader&limit=10

Sažetak

Cilj ove disertacije je izraditi model vrjednovanja informacijske transparentnosti politika privatnosti temeljen na polazišnoj pretpostavci da učinkoviti mehanizmi transparentnosti trebaju težiti smanjivanju informacijske asimetrije između organizacija koje prikupljaju i obrađuju podatke ispitanika te samih ispitanika. U tu svrhu postavljena je analitička matrica kojom se analizom sadržaja tekstova politika privatnosti ispitivala ispunjenost definiranih zahtjeva na teorijski definiranim dimenzijama informacijske transparentnosti, teorijski uvjetno nazvanima *vidljivost* i *inferabilnost*, kao operacionaliziranim jedinicama mjerenja određenih stupnjeva informacijske simetrije kao pokazatelja informacijske transparentnosti u međusobnoj korelaciji. Svaka od dimenzija je, nadalje, operacionalizirana je preko određenog broja indikatora i pod-indikatora kao pretpostavljenih zahtjeva koje bi politika privatnosti trebala ispuniti, odnosno zadovoljiti pri postizanju informacijske simetrije prema ispitanicima. Stoga su i zahtjevima dodijeljeni odgovarajući ponderi prema teorijski pretpostavljenoj važnosti pojedinog pod-indikatora u definiranju indikatora, a čija suma iznosi najviše 1 kao „mjera“ ispunjenosti zahtjeva u potpunosti. Primjenom faktorske analize nad prikupljenim podacima, na uzorku od 152 zdravstvene ustanove u javnom i privatnom sektoru na području Republike Hrvatske, izrađen je i validan konceptualni model kojim se prikazuju utjecaji pojedinih faktora na informacijsku transparentnost, odnosno smanjenje informacijske asimetrije između navedenih dionika, prilikom čega su izdvojeni i rezultati drugih statističkih analiza nad uzorkom. Modelom vrjednovanja informacijske transparentnosti na učinkovitost mehanizama transparentnosti u većoj mjeri utječu faktori vidljivosti, definirani odrednicama slojevitosti, ažuriranosti i informativnosti, u odnosu na faktore inferabilnosti, definirane kroz odrednice pristupačnosti, smislenosti i razumljivosti politika privatnosti. I iako međusobno ne koreliraju, definirane faktore moguće je iskoristiti za određivanje stupnja informacijske asimetrije politika privatnosti s ciljem njenog smanjenja korištenjem rezultata analize valjanosti podudaranja provedene tijekom validacije modela. Prilagodbom pojedinih odrednica na temelju dobivenih vrijednosti odstupanja od referentnih vrijednosti na temelju prosjeka ispitanih ustanova, ostvarivo je upravljanje učinkovitošću mehanizmima informacijske transparentnosti.

Ključne riječi: inferabilnost, informacijska asimetrija, informacijska transparentnost, konceptualni model, politika privatnosti, vidljivost, vrjednovanje, zdravstvene ustanove, inženjerstvo zahtjeva, mehanizmi transparentnosti

Abstract

In today's information abundance, information transparency is becoming an integral part of human rights and freedom in digital environments. The rights of the individuals to make their own choice are becoming stronger in the field of privacy protection, and with overall digital transformation, they are increasingly focused on the protection of personal data collected and processed about data subjects. In the environment of modern liberal-based social systems, individuals are placed in a role of mature and free data subjects, with extensive rights to know what data is collected and processed so that they can determine what information they want to share with whom. Also, they have a right to withdraw from undesirable and optional data processing or request the deletion or anonymization of their personal data. These rights to transparency and intervention are described by the term "user-oriented privacy", a concept whose basic idea is that respondents make informed decisions about disclosing personal data, as disclosing their personal data can change the distribution of power in relationships and create damages and risks to them. But for individuals to be able to make informed decisions and have control over their privacy, mechanisms need to be provided to ensure these rights.

Therefore, the aim of transparency is to reduce the existing high information asymmetry between data controllers and data subjects, as subsequent cannot always determine what data is collected about them, to what extent and for what purpose. And in order to meet the requirements of the principles of data protection and privacy, transparency should be meaningful and meet the requirements in relation to the possibility of intervenability as a goal of privacy. In doing so, mechanisms for achieving intervenability should provide respondents with clear, prominent, easily understandable, accessible tools for consuming the right to choose in relation to the processing of their personal data, as well the rights to interrupt the processing of certain data, delete data, correct them and other related rights.

In the disciplines of information management, business and information ethics, the term transparency is usually used for forms of information visibility and access to information, intentions or behaviours that are thus intentionally revealed, representing a form of communication that transmits signals between processors data and individuals, and in order to achieve the effectiveness of the tool, i.e. increase transparency, it is necessary to eliminate or minimize any "noise" as a disruptive factor in the communication process. In the context of

Shannon-Weaver's mathematical model of the communication system, two essentially diverse ways of transmitting messages are distinguished: via discrete signals and via continuous signals. Discrete signals can represent only a finite number of different, recognizable states, while for continuous signals the amounts of signals can vary in an infinite set of values. In this reference framework and the broader thematic framework of privacy assurance, the former can correspond to *ex-ante*, tools which provide the necessary information to the data subjects before collecting and processing data, and the latter as *ex-post* transparency tools that provide the necessary information to the data subjects after data collection and processing.

In the described context of transparency tools and technologies, privacy policy is set as an *ex-ante* tool for raising awareness of respondents, but also as a tool of data controller declarations, serving as the basis for user conscious decisions regarding the protection of personal data. It is a document, a set of data within limited letters, perceived as a discrete communication system, with the aim of informing data subjects with the procedures of the system or organization regarding the collection, sharing, use and storage of their personal data, showing the entire life cycle of personal data within some organization. Today, reporting on data collection and processing practices is an important aspect of data protection frameworks and regulations, such as the General Regulation on Personal Data Protection in European Union, and the effectiveness of this mechanism is an important aspect in examining information transparency.

So, in order to achieve a state of information symmetry, effective transparency tools need to meet certain requirements on both dimensions of transparency. The dimension of *visibility*, focused on the content determinant of transparency, which reflects the degree of completeness of information and the possibility of finding it, and the dimension of *inferability*, characterized by qualitative characteristics of the mechanism of transparency, reflecting the degree to which information can be used to make the right decisions.

The purpose of the research is to develop a model for calculating the levels of information transparency of privacy policies in deviations towards achieving optimal transparency results, i.e. information symmetry, as a basis for improving the effectiveness of transparency mechanisms. The specific goal of the research is to identify factors of dimensions of information transparency, their mutual relationship and intensity of connections as constructs within designed model of privacy policy evaluation. Based on the theoretical study, the relevant

factors are determined on the dimension of visibility: 1) informativeness, 2) currentness and 3) accessibility of the text. The dimension of inferability is determined by: 1) layering, 2) conciseness and 3) understandability of the content.

With proposed research the following hypotheses were tested: H1) The degree of information asymmetry can be determined using the degrees of visibility and infectivity factors; H2) The degree of information asymmetry is significantly influenced by visibility factors compared to infectivity factors and H3) By applying the designed model, it is possible to assess the information transparency of privacy policies.

The study is dominated by a primarily quantitative approach to content analysis of privacy policies. The research was conducted on the documents of 152 health care institutions, of which 56 institutions are in the public health care system, while the remaining institutions are health care institutions in private sector. The reason for this is that many public health care institutions during the research in April and May 2021. did not have available privacy policies on their respected websites. That is, out of 148 health care institutions in the public health care system declared on the website of the Ministry of Health, only 37% had published their privacy policies with a unified content identifier (URI) as a set condition for sample selection.

After the design of an analytical matrix and coding sheet, during the data collection, first the number of interactions required to access privacy policies as a basis for calculating the accessibility requirement coefficient and determining whether the content layering requirement was recorded (through subheadings of certain document sections or other hypertext formatting options).

In the next step, the text of the document was copied and pasted into a blank Word application document in which a unit of further analysis was set up: titles were removed, e-mail addresses and hyperlinks were replaced with X not to affect results of syllable count. Furthermore, through the Wordcount option, the number of words and the number of characters (without spaces) were recorded, while the number of sentences was counted "manually" by the author, professor of Croatian language and literature. The text was then copied into the computer tool syllablecounter.org, which was selected as the most reliable for calculating the number of records after comparing the results of manual counting and by comparing different computer programs for counting records in the text. Furthermore, to help analyse the number

of lexical words, the text is then copied to the text analysis tool on online-utility.org website to single out occurrences in relation to their frequency of occurrences in the text.

In the next steps, the content analysis method was used to examine the fulfilment of informativeness requirements through the presence of criteria defined in the analytical matrix, then currentness, in relation to the date of publication or update of the document and information on how to inform respondents about changes in privacy policies in this document.

Furthermore, based on the obtained results of the number of syllables, words and sentences, using the Flesch Reading Ease (FRE) formula for readability, the indices of text understandability were calculated, and by using The Flesch-Kincaid grade level formula the level of education of the respondents for understanding the privacy notice were determined in reference to the of 2011 census results in Croatia. Furthermore, the number of lexemes was put in proportion to the total number of words as the lexical density is set as a reference for conciseness requirement testing. The analysis was performed in the computer program Excel using custom formulas of for the Croatian language.

In the absence of similar analytical matrices for measuring transparency policies, the design and content validation of the analytical matrix was carried out during the research.

Firstly, as all determinants of transparency dimensions were directly operationalized, i.e. each of them was measured through only one indicator, with a different number of sub-indicators, while the determinant of informativeness was measured through a total of 14 indicators, in order to determine the consistency of the selected 14 indicators as a reliable instrument for measuring the determinant of informativeness, a reliability analysis (Cronbach's alpha reliability coefficient) was performed on data collected from a sample of public institutions and institutions in private sector as well. Both results indicate a very good reliability. Then the results of visibility and inferability dimensions obtained at 56 public health institutions were compared with those obtained at 96 private public institutions throughout t-test methods, showing that data collected is consistent.

Based on the obtained research results, a conceptual model of evaluating information transparency was developed in relation to the defined dimensions of information transparency at the first level, and then in relation to the obtained factor saturations of individual determinants

at each of the dimensions at the second level. In reference to results, determinants were set to reflect different distribution, as determinants of accessibility and layering substituted.

Although the analysis of the collected results showed that the two dimensions, visibility and inferability are not correlated, that is the correlation between these two latent variables is close to zero, contrary to the theoretical assumption, both dimensions can be treated as separate variables or constructs.

As results of performed two-factor analysis, the values of each dimension contribution in explaining the variance were calculated that can be used as a basis for model development. In absolute terms, the "share" of the visibility dimension is 32.04%, and inferability is 19.34%, which together makes 51.38% of the variance explained by the set two-factor model. That is, in relative terms, if the explained variance is set as 100%, then its visibility contributes 62.36%, and inferability 37.64% to the information transparency results.

From the obtained results of calculated factor scores each determinant can be put in relation to determined transparency dimension, assessing its impact to information transparency. Results have shown that informativeness requirements have the greatest impact on the results in the visibility dimension, which is expected, since this indicator only consists of the most sub-indicators (14 of them) compared to other indicators. Furthermore, to a lesser extent, the results in the dimension are affected by the requirements for layering of the text, while the least affected they are by the currentness requirements, i.e. the publication of dates and ways of informing respondents when changing privacy policies.

On the dimension of inferability, the results of information transparency are mostly influenced by the requirement of conciseness as the results of lexical density, and then the requirement of accessibility, reflected in the number of interactions to the text of the privacy policy and finally understandability an indicator of the quality and appropriateness of the language in which the information is provided in relation to the target group.

However, since the results presented by the conceptual model in their interrelation represent the impact of individual determinants and dimensions of transparency on the overall result of information transparency of individual institutions, they can be directed towards examining privacy policies transparency depending on their impact on the overall result of

information (a)symmetry. Therefore, the result of information (a)symmetry as a dependent variable in relation to the analysis of variances of set factor scores on both dimensions of transparency can be examined in order to test auxiliary hypotheses obtained by the set model.

By conducting a Goodness-of-Fit analysis in relation to the reference results of the average results on both dimensions it was possible to determine deviations from the results in relation to changes in individual variations of factor scores over the collected data to validate model.

In relation to the obtained average of all institutions in the visibility dimension, which is 0.39, the greatest influence on the results of information transparency has the determinant of layering, followed by currentness and, finally, informativeness.

Furthermore, on the dimension of inferability in relation to the obtained average of all institutions, which is 0.29, from the obtained results it is possible to conclude that the determinant of understandability does indeed have the least influence on the results of information transparency. It is also possible to conclude that the determinant of accessibility has the greatest impact on the information transparency of the dimension in question.

In relation to the calculated reference average of all institutions on the inferability dimension, 46 institutions have achieved above-average results were singled out, while 76 of them on the visibility dimension, which corresponds to the statement that determinants on the visibility dimension to a greater extent contribute to reducing information asymmetry.

Regarding the tested hypothesis, it is concluded that H1 is confirmed as the degree of information asymmetry can be determined using the degrees of visibility and inferability factors; by interpreting the results when conducting factor analysis over the dimensions of visibility and inferability explained variance over the investigated sample H2 is also confirmed, as the degree of information asymmetry is significantly influenced by visibility factors compared to inferability factors; while H3 is rejected, giving the diverse results within set model and its validation and by applying the designed model, it is not possible to assess the information transparency of privacy policies.

The obtained results, although, in their mutual relationship represent a kind of ordinal scale which shows the impact of individual determinants and dimensions of transparency on

the overall result of information transparency of an individual institution. Since this result is taken as a measure of the effectiveness of the transparency mechanism, the results can be directed towards examining privacy policies in relation to the requirements met on individual determinants of transparency dimensions, depending on their impact on the overall information symmetry score. Therefore, the research results can serve as a basis for the development of guidelines for ensuring effective transparency tools, but also for the development of algorithms for a multi-criteria simulation model based on modern technologies.

Furthermore, this research should significantly contribute to the current literature in the field of requirements engineering, integrating the concept of information (a)symmetry as an element of evaluating the performance of information transparency mechanisms.

Keywords: inferability, information asymmetry, information transparency, conceptual model, privacy policy, visibility, evaluation, healthcare, requirements engineering, transparency mechanisms

SADRŽAJ

1. UVOD

U današnje vrijeme digitalne ekonomije pitanje privatnosti sve je izraženije, kao i mogućnosti kontrole pojedinaca nad svojim podacima. Napredak u informacijskoj tehnologiji omogućio je prikupljanje i upotrebu osobnih podataka nevidljivim. Kao rezultat toga, pojedinci rijetko imaju jasno znanje o tome koje informacije drugi imaju o njima te kako se te informacije koriste i s kakvim posljedicama.

Odlučivanje o privatnosti za pojedince je zapravo dijelom rezultat racionalne „računice“ troškova i koristi [1] na koju utječe percepcija tih troškova i koristi, ali i društvene norme, osjećaji i heuristike. Bilo koji od ovih čimbenika može utjecati na ponašanje drugačije od ustaljenih stavova. U kontekstu digitalne ekonomije, pojedinci se stalno uključuju u transakcije povezane s privatnošću, čak i kad kompromisi u vezi s privatnošću mogu biti neopipljivi ili kada razmjena osobnih podataka možda nije vidljiva ili primarna komponenta transakcije. Primjerice, postavljanje upita na internetskoj tražilici ima jednaku vrijednost prodaji osobnih podataka (preferencija, interesa) u zamjenu za uslugu (rezultate pretraživanja).

Iako se pojedinci ponekad odriču osobnih podataka zbog raznih pogodnosti ili mogućih popusta na usluge, u nekim slučajevima dobrovoljno poduzimaju značajne aktivnosti kako bi zaštitili svoju privatnost. Nadalje, želje za interakcijom, socijalizacijom, otkrivanjem i prepoznavanjem (odnosno slavom) snažni su ljudski motivi, ništa manje temeljni od potrebe za privatnošću, a elektronički mediji današnjeg doba pružaju neviđene mogućnosti djelovanja u zadovoljavanju istih. Kroz društvene medije pojedinci imaju mogućnost izgraditi socijalni kapital [2], povećati samopoštovanje [3] i ispuniti potrebe ega [4]. No, rana istraživanja privatnosti na području sfere društvenih mreža [5][6] pokazuju da u takvim okruženjima pojedinci dijele informacije koje nisu primjerene za određene javnosti, poput budućih poslodavaca, ili mogu dovesti do krađa identiteta, što je svakako potencirano strukturnim tehničkim značajkama [7] samih društvenih mreža i njihovog utjecaja na suvremeno društvo [8]. Granice između javnog i privatnog pomiču se i u stalnoj su transformaciji. Upravo je tu kompleksnost najbolje izrazio talijanski teoretičar demokracije Noberto Bobbio [9] još 1989. godine, imenovanjem razlike između privatnog i javnog „velikom dihotomijom“. Dok privatno uključuje sve ono što je značajno za pojedince ili pojedine skupine, u javno se područje „postavlja“ sve što je značajno za društvo u cjelini, što u modernim, suverenim državama

pretpostavlja i političku dimenziju, pa se koncept javnosti u suvremenim (zapadnim) demokracijama odnosi ponajprije na javnu sferu, u kojoj javno korištenje razuma ili javna rasprava između slobodnih i jednakih građana rezultira formiranjem i izražavanjem javnog mnijenja [10].

Popularizacija društvenih mreža svakako je približila polove dihotomije pa dok se, s jedne strane, poznate i istaknute osobe sve više „prodaju“ s odabranim dijelovima privatnog života putem društvenih medija, s druge strane određene dijelove života štite posredstvom sudova [11] [12] [13], čime zaštita privatnosti postaje i pitanjem komoditeta.

Paradoks privatnosti, odnosno, nesklad između stavova i ponašanja pojedinaca vezano uz zaštitu vlastite privatnosti, potencirale su i današnje platforme tzv. ekonomije dijeljenja [14] koje osmišljavaju vlastite kreditne sustave za segmentaciju korisnika prema određenim atributima, čiji algoritmi, odnosno parametri nisu transparentni. Dapače, dvije kompanije, pioniri takvih poslovnih modela, AirBnB i Uber, zadržavaju pravo otkazivanja svoje usluge bez pružanja obrazloženja [15] korisniku, čime ga zapravo liše prava na svoju uslugu. Širi kontekst predstavlja i primjer iz prve epizode Netflixove dokumentarne serije *Connected: The Hidden Science of Everything* (hrv. Povezano: Skrivena znanost svega, op. a.) [16] koji problematizira netransparentnost algoritama aplikacija za spajanje ljudi.

Izvješće istraživačkog projekta *Horizon 2020* Europske Unije [17] vezano uz privatnost na platformama tzv. ekonomije dijeljenja pokazuje da korisnici s obje strane (pružatelja usluga i korisnika usluga), unatoč relativno visokoj zabrinutosti za privatnost, procjenjuju da su koristi koje imaju od sudjelovanja na platformama veće od rizika privatnosti. Nadalje, pružatelji usluga u većini iskazuju određenu zabrinutost zbog zlouporabe svojih podataka, kao i gubitka kontrole nad svojim internetskim predstavljanjem zbog negativnih recenzija ili komentara drugih korisnika. Zapravo, cijeli koncept tzv. upravljanja impresijama, strateškog dijeljenja osobnih podataka radi stvaranja povoljnijeg internetskog izgleda, izvor je anksioznosti kod korisnika.

Calo [18] konceptualizira štetu, odnosno negativne posljedice kršenja privatnosti, kroz kategorije subjektivnosti i objektivnosti. Dok je subjektivna kategorija štete po privatnost percepcija neželjenog promatranja, koja može prouzročiti nepoželjna mentalna stanja „unutar pojedinca“, poput spomenute anksioznosti i nelagode, objektivna šteta po privatnost može se dogoditi kada se osobni podaci koriste kako bi se opravdalo nepovoljno djelovanje na osobu,

odnosno zloporaba podataka bez znanja ili privole pojedinca. U obje kategorije dolazi do određene nesigurnosti pojedinca po pitanju privatnosti koje mogu utjecati na ponašanje pojedinaca, kao i brigu za očuvanje iste.

Budući da se područje privatnosti često definira kontekstualno senzibilnom kategorijom, ovisno o društvenom kontekstu i postojećim normama u određenom vremenu, ljudi smatraju da je njihova privatnost narušena kada tijek informacija teče suprotno utvrđenim normama te doživljavaju njezino kršenje posebno zabrinjavajućim kada je kontekstualni integritet samih normi pod izazovom [19]. U današnjem digitalnom društvu, pravo na privatnost transformirano je u perspektivu kontrole širenja podataka. Neovlašteno prikupljanje i korištenje osobnih podataka smatra se rizikom za slobodu pojedinca, a koji se postavlja kao aktivni dionik u donošenju odluka vezano uz vlastite podatke.

1.1. Pozadina istraživanja

Kako bi pojedinci mogli donositi informirane odluke i imati kontrolu nad svojom privatnošću potrebno je, prije svega, osigurati informacijsku transparentnost kao etičku kategoriju između svih dionika digitalnog društva, a prvenstveno u okvirima korporativnog upravljanja [20]. U slučaju zaštite podataka, ona postavlja granice između privatnog i javnog, ali postavlja i veću odgovornost organizacija kao dionika na suvremenom tržištu.

Opća uredba o zaštiti podataka (eng. General Data Protection Regulation, GDPR), donesena 2016. godine, a koja se s 25. svibnjem 2018. godine počela primjenjivati u svim državama članicama Europske unije direktno, bez potrebe za dodatnim prenošenjem u nacionalno zakonodavstvo, postavila je zakonodavni okvir s visokim etičkim načelima zaštite prava pojedinaca. Osim informiranja ispitanika o obradama podataka i svrhama istih, kao podlozi za donošenje informiranih odluka, načelo transparentnosti se „proteže“ i na obvezu informiranja o nezakonitom dijeljenju podataka s drugim stranama te svim probojima informacija koji mogu proizvesti štetu po privatnost ispitanika, odnosno subjekta podataka, čiji su podaci na taj način kompromitirani.

No, potencijal transparentnosti informacija predstavlja opći problem u vezi s najboljim načinom odlučivanja koje informacije treba objaviti kako bi se omogućila učinkovitost mehanizama. Radikalni pristupi transparentnosti informacija, poput potpunog otkrivanja ili

potpunog zadržavanja informacija u odnosu na aktivnost organizacije, ne uspijevaju jamčiti pozitivne etičke implikacije [21] te mogu dovesti do kontraproduktivnosti u odnosu na kognitivne spoznaje pojedinaca [22] te posljedično, njihovu autonomiju odlučivanja [23]. Stoga, i sama kvaliteta mehanizama, odnosno načina na koji su informacije učinjene dostupnima i prezentirane, jednako su važan element transparentnosti kao i sâm odabir informacija.

I Radna skupina za zaštitu podataka iz članka 29[1] u svojim Smjernicama o transparentnosti [24] postavlja zahtjeve sažetosti i razumljivosti informacija za ciljanog korisnika, kao i potrebe učinkovitog prikaza informacija u odnosu na (digitalno) okruženje kao važnih kriterija u osiguravanju transparentnosti informacija.

Stoga, problem odabira vrste informacija koju treba otkriti zahtijeva i dubinsko razumijevanje karakteristika entiteta koji će se otkriti. Informacije su pojam koji implicira zavisnost o kontekstu u kojem se podaci interpretiraju pa bi se otkrivene informacije trebale sastojati od značajnih, istinitih, razumljivih, dostupnih i korisnih podataka. Takve informacije nazivaju se semantičkima [25] i mogu se pragmatično povezati s procesima donošenja odluka.

Semantičke informacije nose one ključne atribute koji donose obavijest u elementarnom poimanju informacije kao skupu podataka koji primatelju, u procesu komunikacije, služe za otklanjanje nedoumica ili smanjenje neizvjesnosti te za poduzimanje određenih akcija. Stoga, one u kontekstu kontrole privatnosti ne bi smjele biti rezultat „snimke stanja“ ili pasivnog promatranja, već ovise o proaktivnim, smislenim razradama podataka primatelja [21] te su obavijesne samo ako su istinite. Stoga, iako informacije mogu biti smislene i pružene u razumljivom obliku, ne moraju nužno prenositi činjeničnu situaciju.

Stoga se i predmetno istraživanje u jednome dijelu temelji na taksonomskim zahtjevima transparentnosti [26] postavljenim u odnosu na određene atribute ispunjavanja zadanih regulatornih obaveza navedenih u spomenutoj Općoj uredbi o zaštiti podataka te standarde ISO/IEC 29100:2011 kao mehanizme osiguravanja kvalitete pri obradi osobnih podataka u

[1] Punog naziva "Radna skupina za zaštitu pojedinaca u pogledu obrade osobnih podataka" savjetodavno je tijelo pokrenuto 1996. i sastavljeno od predstavnika tijela za zaštitu podataka svake države članice EU-a, Europskog nadzornika za zaštitu podataka i Europske komisije na temelju Članka 29. Direktive o zaštiti podataka (Direktiva 95/46/EC). Stupanjem na snagu Opće uredbe o zaštiti podataka 25. svibnja 2018., tijelo je zamijenjeno Europskim odborom za zaštitu podataka.

organizacijskim okruženjima. Jer transparentnost se može promatrati kao regulatorni zahtjev, u odnosu na postavljene zakonske obveze, ili dobrovoljni zahtjev, motiviran poboljšanjem kvalitete i izgradnjom povjerenja korisnika.

No, budući da se transparentnost bavi informacijama, ona postaje jedan od glavnih atributa informacijskog sustava, a procesi komuniciranja informacija postaju relevantni kada se uzmu u obzir kvalitativne implikacije transparentnosti. Cilj transparentnosti kao proetičkog alata je poticanje organizacija da postave prioritete u praksama upravljanja podacima od strane korisnika, ne samo da deklarativno izjavljuju o svojim namjerama. Ukoliko informacije ne nude dovoljno obavijesnosti pojedincu vezano uz obradu njegovih podataka, ne može se govoriti o informacijskoj transparentnosti u punom značenju pojma. Stoga se istraživanjem namjerava osmisliti model i odrediti najbolji prediktori za povećanje informacijske transparentnosti kao jednog od alata u osiguravanju informacijske privatnosti pojedinaca.

1.2. Obrazloženje istraživanja

Budući da je briga za privatnost od strane pojedinca ovisna o kontekstu, ona može poprimiti oblike od krajnje zabrinutosti do apatije [27]. Kao jedan od razloga tome može se pretpostaviti informacijska asimetrija, odnosno stanje u kojem jedna strana ima pristup (boljim) informacijama koje druga strana nema. Kanonski primjer iste odnosi se na tržište rabljenih automobila na kojem prodavači znaju jesu li njihovi automobili u dobrom stanju ili su tzv. „limuni“, odnosno u lošem stanju, no kupci nemaju mogućnosti to znati u potpunosti [28]. Posljedično, kupci trebaju uzeti u obzir rizik kupovine automobila u lošem stanju ili odustaju od kupovine.

Pojam informacijske asimetrije često je područje istraživanja na područjima ekonomske znanosti [29][30][31], ali i drugih područja [32][33]. U kontekstu digitalne ekonomije, u kojem su podaci „valuta“ pri određenoj transakciji, moguće je sagledati privatnost i njeno okruženje kao tržište, mjesto gdje se susreću ponuda i potražnja. Na tom tržištu pojedinci, odnosno ispitanici, su aktivni dionici, a da bi mogli donositi informirane odluke i imati kontrolu nad svojim podacima, potrebno je osiguravanje mehanizama za ostvarivanje njihovih prava.

Stoga, da bi pojedinci mogli donositi informirane odluke i imati kontrolu nad svojom privatnošću potrebno je osigurati kvalitetne alate transparentnosti. Budući da transparentnost

zahtijeva zadovoljavanje dva uvjeta – *vidljivost* i *inferabilnost* [34], u odnosu na ispunjavanje njihovih zahtjeva, moguće je odrediti stupanj informacijske asimetrije kao apsolutne vrijednosti.

Predloženim modelom vrjednovanja informacijske transparentnosti politika privatnosti kao referentna vrijednost postavlja se stupanj informacijske asimetrije, kojim je, u odnosu na stanje apsolutne simetrije, moguće izmjeriti vrijednosti u kojima su zadovoljeni uvjeti vidljivosti i inferabilnosti kao dvije dimenzije transparentnosti.

1.3. Privatnost i zdravstveni podaci

Zdravstvene informacije imaju nekoliko karakteristika koje čine privatnost posebno važnom, budući da pojedinci ne kontroliraju što je upisano u njihovu medicinsku dokumentaciju, već evidenciju kreiraju pružatelji zdravstvenih usluga, a informacije mogu biti iskorištene za mnoge svrhe i trajati cijeli život.

Zdravstvena njega je vrlo važna u životima ljudi, a pojedinci nemaju previše izbora kada se radi o izborima vezanima uz nju – ili je mogu koristiti ili je se kloniti na vlastitu štetu i odgovornost. Jednako tako, nemaju previše utjecaja na ono što se unosi u njihove medicinske zapise budući da to čine medicinski profesionalci, a ti uneseni podaci mogu imati značajan utjecaj na njihove živote: prilikom zapošljavanja na određena radna mjesta, stjecanja profesionalnih licenci, prilikom ugovaranja polica osiguranja te konzumiranja nekih drugih prava.

U tom kontekstu, zdravstvene informacije se mogu sagledavati kao bilo koje informacije koje se odnose na stanje pojedinca, bilo fizičko ili psihičko. No, informacije u medicinskoj dokumentaciji mogu uključivati i adresu te brojeve telefona, osobni identifikacijski broj i broj zdravstvenog osiguranja, zaposlenje i njegov status te druge relevantne podatke.

Budući da ljudi jednostavno ne žele da drugi znaju za njihovo zdravlje ili se boje posljedica ako su drugi svjesni da imaju bolesti ili invaliditet, zdravstvene informacije smatraju se osjetljivima [35][36]. Nadalje, zdravstveno stanje može biti važan element identiteta pojedinaca i/ili osnova za ostvarivanje intimnosti između osoba pa je zaštita takvih podataka važna i iz instrumentalnih razloga. Unatoč regulatornim i etičkim zabranama diskriminacije invaliditeta, manje je vjerojatno da će poslodavci zapošljavati ili promovirati osobe za koje

znaju da imaju „narušeno“ zdravstveno stanje. Također, isti se mogu brinuti i radi troškova zdravstvenog osiguranja, ali i zbog troškova odsutnosti, invalidskog osiguranja, i raznih naknada za radnike. S pozitivne strane, poslodavci bi mogli koristiti dostupne zdravstvene informacije za poboljšanje zdravstvenog stanja radnika kroz razne *wellness* programe, a s ciljem poboljšanja njihove produktivnosti. No, takvi programi, uz prednosti, mogu predstavljati i rizike za radnike. Čak i na temelju zbirnih, anonimiziranih podataka poslodavci mogu raditi analize i predviđanja odgovora na pitanja poput koliko će zaposlenica vjerojatno zatrudnjeti u naredno vrijeme [37] ili trebati operacije leđa tijekom nadolazeće godine [38].

Nadalje, dostupnost zdravstvenih informacija također može utjecati na pojedinčevu mogućnost dobivanja zajma ili premije osiguranja. Tvrtke za rudarenje podataka sve više koriste prediktivne modele podataka pri izgradnji algoritama za davanje prijedloga o razinama (zdravstvenih) rizika pojedinaca svojim klijentima. Algoritamska analitika je uglavnom tajna, ali može uključivati informacije koje su izravno ili neizravno povezane sa zdravljem. Primjerice, nagla promjena u određenim navikama koje su vidljive u obrascima kupnje kreditnom karticom ili prestanak redovitog korištenja aplikacije za vježbanje može sugerirati velike promjene u zdravstvenom stanju, a koje, posljedično, analitička tvrtka može komunicirati kao rizik za pružanje zajma. Iako se obrade vrše nad podacima s uklonjenim identifikatorima, ne eliminiraju se u potpunosti rizici ponovne identifikacije osoba. Uz trenutne tehnike upravljanja podacima, rizik na privatnost pojedinaca procjenjuje se na manje od 1%, budući da rizici ponovne identifikacije ovise o metodama anonimizacije [39].

Ipak, podaci o zdravlju stanovništva mogu biti od iznimne važnosti za nacionalnu sigurnost, javno zdravlje, poboljšanje kvalitete zdravstvene zaštite, identifikaciju štetnih nuspojava lijekova ili uređaja, kao i razvoj precizne medicine te, općenito, medicinska istraživanja. Bioterorizam je glavni problem nacionalne sigurnosti. Povremene prijetnje oslobađanjem otrovnih sredstava kao što su ricin ili antraks dovele su do potrebnog prijavljivanja sumnjivih incidenata bioterorizma u Sjedinjenim Američkim Državama, dok Europska unija ima koordiniran sustav izvješćivanja hitne zdravstvene situacije ovakve vrste [40]. U takvim slučajevima medicinske informacije mogu biti ključne za otkrivanje bioterorista u hitnim slučajevima, a identifikacijski podaci pacijenata opravdani su radi provjera točnosti, sprječavanja dvostrukog brojanja pacijenata i omogućavanja intervencija potrebnih za onemogućavanje ili smanjenje širenja bolesti.

Podaci o tzv. „javnom zdravlju“ vrlo su vrijedni unutar pojedinih zajednica, što je naročito bilo važno prilikom primjene epidemioloških mjera za sprečavanje zaraze od Covid-19 virusa. Također, isti su važan dio primjene preventivnih programa sprječavanja malignih bolesti (poput Nacionalnog programa ranog otkrivanja raka debelog crijeva).

Uzevši u obzir i benefite medicinskih podataka na razvoj lijekova i tretmana liječenja te znanstvena istraživanja, vrijednost podataka o zdravstvenom stanju pojedinaca unutar populacije je neupitna. Ali i rizici na prava privatnosti.

E-pošta i elektronička medicinska dokumentacija također predstavljaju nove izazove povjerljivosti za liječnike. Komunikacija s pacijentima putem kanala e-pošte i drugih aplikacija olakšava pristup zdravstvenoj skrbi, ali predstavlja i rizik ukoliko komunikacija nije sigurna, dok pojedini sustavi elektroničke medicinske dokumentacije u upotrebi ne sadrže mehanizme za odvajanje vrsta informacija koje bi mogle zahtijevati posebnu etičku ili pravnu zaštitu [41], kao što su informacije o mentalnom zdravlju, informacije o pobačaju ili drugim reproduktivnim pitanjima te informacije o spolno prenosivim bolestima i genetske informacije. Kada se ovi zapisi dijele, omogućuje se pristup cijelom zapisu, a ne dijelovima koji bi mogli biti relevantni za dotičnu skrb.

Budući da je povjerljivost podataka važna značajka privatnosti specifična za zdravstveni sektor[2] te uzevši u obzir rizike suvremenog digitalnog okruženja [42], istraživanje je provedeno na primjerima politika privatnosti iz zdravstvenog sektora kao specifičnog područja u zaštiti privatnosti koje u navedenom kontekstu nudi prigodnu podlogu za kritičku procjenu rizika, odnosno učinaka na prava privatnosti pojedinaca u digitalnom okruženju.

1.4. Istraživački problem

Budući da suvremeni društveni sustavi zasnovani na liberalizmu postavljaju zrele i slobodne pojedince u ulogu „subjekata“ podataka, isti imaju opsežna prava da znaju koji podaci o njima se prikupljaju i obrađuju kako bi mogli odrediti koje informacije s kime žele dijeliti. Također, ispitanici se mogu povući iz nepoželjnih i neobvezatnih obrada podataka ili zahtijevati

[2] Zaštita privatnosti u liječničkoj profesiji značajna još od 4. stoljeća prije Krista, kada je i postavljena Hipokratova zakletva. Tijekom povijesti ista se često mijenjala da bi na kongresu Međunarodnog saveza liječničkih društava u Ženevi 1948. godine ustanovljena konačna zakleta koja se danas koristi - Ženevska zakletva: “Poštovat ću tajne onog tko mi se povjeri.”

brisanje ili anonimiziranje svojih osobnih podataka. Ova prava na transparentnost i intervenciju opisuju se izrazom „privatnost usmjerena na korisnika“ [43], konceptom čija je osnovna ideja da ispitanici donose svjesne odluke o objavljivanju osobnih podataka, budući da objavljivanje njihovih osobnih podataka može promijeniti raspodjelu moći u odnosima, kao i stvoriti štete i rizike za njih.

No, da bi pojedinci mogli donositi informirane odluke i imati kontrolu nad svojom privatnošću potrebno je osigurati mehanizme za osiguravanje tih prava. Stoga je i cilj transparentnosti smanjenje postojeće visoke informacijske asimetrije između ispitanika i vršitelja te voditelja obrade podataka, budući da ispitanici ne mogu uvijek odrediti koji se podaci o njima prikupljaju, u kojoj mjeri te s kojom svrhom. A da bi zadovoljila zahtjeve načela zaštite podataka i privatnosti, transparentnost treba biti smislena, odnosno zadovoljavati zahtjeve u odnosu na mogućnost intervenabilnosti kao cilja privatnosti. Pri tome, mehanizmi za postizanje intervenabilnosti trebaju pružati ispitanicima jasne, istaknute, jednostavno razumljive, pristupačne alate za konzumiranje prava na izbor u odnosu na obradu njihovih osobnih podataka najranije u vrijeme prikupljanja podataka, odnosno prilikom prve obrade ili u razumno vrijeme, ali i naknadno, kako bi ispitanici mogli konzumirati prava na prekid obrade određenih podataka, brisanje podataka, njihov ispravak i druga pripadajuća prava.

U kontekstu alata i tehnologija transparentnosti politike privatnosti postavljaju se kao *ex-ante* alat za podizanje svijesti ispitanika, ali i deklaracije, budući da pretpostavljaju osnovu za interakciju korisnika pri donošenju svjesnih odluka pojedinca vezano uz zaštitu svojih osobnih podataka. To je dokument, skup podataka s ciljem upoznavanja korisnika, ispitanika, s postupcima sustava ili organizacije u vezi s prikupljanjem, dijeljenjem, korištenjem i pohranom njihovih osobnih podataka, prikazujući cijeli životni ciklus osobnih podataka unutar organizacije.

Danas je obavještavanje o praksama vezanim uz prikupljanje i obradu podataka važan aspekt okvira i propisa o zaštiti podataka [44], poput Opće uredbe o zaštiti osobnih podataka [45] te je učinkovitost tog mehanizma važan aspekt pri ispitivanja informacijske transparentnosti koja se može definirati kroz dvije dimenzije: *vidljivost* i *inferabilnost* [34].

Kako bi se postiglo stanje informacijske simetrije alati transparentnosti trebaju zadovoljiti određene zahtjeve na obje dimenzije transparentnosti. Dimenzija vidljivosti,

usmjerena na sadržajnu determinantu transparentnosti, odražava stupanj cijelosti informacija i mogućnosti njihovog pronalaženja, dok dimenzija inferabilnosti, karakterizirana kvalitativnim karakteristikama mehanizma same transparentnosti, odražava stupanj u kojem informacija može biti iskorištena za donošenje ispravnih odluka [34].

1.5. Cilj istraživanja

Svrha istraživačkog rada je izraditi model za izračun stupnjeva informacijske transparentnosti politika privatnosti na temelju kojih će biti moguće odrediti odstupanja prema postizanju optimalnih rezultata transparentnosti, odnosno informacijske simetrije, kao osnove za poboljšanje učinkovitosti mehanizama transparentnosti. Specifičan cilj istraživanja je identifikacija faktora dimenzija informacijske transparentnosti na osnovu kojih je moguće ispitati i utvrditi postojanje, odnos i intenzitet veza kreiranih konstrukata dizajniranog modela vrjednovanja politika privatnosti u zdravstvu. Na osnovi teorijske studije na dimenziji vidljivosti ispituju se relevantni faktori, odnosno odrednice: 1) informativnosti, 2) ažuriranosti te 3) pristupačnosti teksta. Na dimenziji inferabilnosti to su: 1) slojevitost, 2) smislenost i 3) razumljivost sadržaja.

1.6. Istraživačka pitanja

U cilju postizanja općeg cilja istraživanja te identifikacije faktora na dimenzijama transparentnosti postavljena su sljedeća istraživačka pitanja:

- postoje li i koje korelacije između dimenzija transparentnosti?
- koji su utjecaji pojedinih faktora na definirane dimenzije transparentnosti?
- kako identificirani faktori utječu na rezultate informacijske transparentnosti politika privatnosti?

Budući da je informacijsku transparentnost u odnosu na apsolutnu informacijsku simetriju politika privatnosti moguće mjeriti i kroz stupnjeve odstupanja od optimalnih rezultata transparentnosti, ispitivanjem korelacija između dimenzija transparentnosti, kao i utjecaja pojedinih faktora na dobivene rezultate, moguće je definirati relativnu vrijednost informacijske transparentnost mehanizama, odnosno informacijsku asimetriju, kao osnove za oblikovanje hipoteza istraživanja u nastavku.

1.7. Hipoteze istraživanja

Na temelju postavljenog cilja istraživanja identifikacije faktora dimenzija informacijske transparentnosti te ispitivanja njihova odnosa i intenziteta veza pri kreiranju konstrukata modela vrjednovanja politika privatnosti u zdravstvu, istraživanjem su ispitivane sljedeće hipoteze:

H1: Pomoću stupnjeva faktora *vidljivosti* i *inferabilnosti* moguće je odrediti stupanj informacijske asimetrije.

H2: Na stupanj informacijske asimetrije značajnije utječu faktori *vidljivosti* u odnosu na faktore *inferabilnosti*.

H3: Primjenom dizajniranog modela moguće je procijeniti informacijsku transparentnost politika privatnosti.

Na temelju usporedbe stupnjeva faktora na obje dimenzije transparentnosti H1 se usmjerava ispitivanju postojanja faktora i ispitivanju njihova odnosa. Nadalje, ispitivanjem intenziteta veza faktora s H2 se određuje njihova povezanost u odnosu na rezultate informacijske transparentnosti, na temelju čega se, posljedično, kao ciljem istraživačkog rada, kroz dizajnirani model vrjednovanja informacijske transparentnosti politika privatnosti, nastoji omogućiti predviđanje i mogućnost utjecaja pojedinih faktora na informacijsku transparentnost, kao ciljem H3.

1.8. Metodologija istraživanja

Radom dominira primarno kvantitativni pristup analizi sadržaja politika privatnosti. Za prikupljanje podataka pristupilo se oblikovanju analitičke matrice temeljem definiranja kvalitativnih zahtjeva na obje dimenzije transparentnosti, *vidljivosti* i *inferabilnosti*. Istraživanje je provedeno na uzorku javnih i privatnih zdravstvenih ustanova na temelju čega je, u nedostatku sličnih analitičkih matrica za mjerenje politika transparentnosti, provedena konstrukcijska i sadržajna validacija analitičke matrice. Tijekom istraživanja primjenjivan je namjeran način izbora uzorka budući da je analiza sadržaja pojedinih dokumenta politika privatnosti ovisila o njihovoj dostupnosti, odnosno prisutnosti na mrežnim stranicama zdravstvenih ustanova. Nadalje, prilikom određivanja jedinica uzorka postavljen je kriterij da postoji unificirani identifikator sadržaja (eng. Uniform Resource Identifier, URI) politika

privatnosti, neovisno jesu li iste prikazane kao hipertekst ili u nekom drugom obliku (pdf, doc i sl.). Politike privatnosti za koje je potrebno preuzimanje dokumenta na računalo ili mobilni uređaj korisnika, stoga, nisu bile razmatrane, odnosno nisu smatrane dijelom uzorka.

Dobiveni podaci su analizirani statističkom analizom, prvenstveno metodama faktorske analize, kojom su ekstrahirane odrednice dimenzija, a korištene su i metode analize statističke pouzdanosti te statistički testovi normalnosti distribucije.

Statističke metode i analiza istraživanja opisani su u Poglavlju 4.

1.9. Rezultati istraživanja

Na temelju dobivenih rezultata istraživanja pristupilo se izradi konceptualnog modela vrjednovanja informacijske transparentnosti u odnosu na definirane dimenzije informacijske transparentnosti na prvoj razini, a zatim u odnosu na dobivena faktorska zasićenja pojedinih odrednica na svakoj od dimenzija na drugoj razini, čiji su rezultati opisani u Poglavlju 4.

Dobiveni rezultati u svome međusobnom odnosu predstavljaju svojevrsnu ordinalnu skalu kojom je prikazan utjecaj pojedine odrednice i dimenzije transparentnosti na cjelokupni rezultat informacijske transparentnosti pojedine ustanove. Budući da se taj rezultat uzima kao mjera učinkovitosti mehanizma transparentnosti rezultati mogu biti usmjereni prema ispitivanju politika privatnosti u odnosu na ispunjene zahtjeve na pojedinim odrednicama dimenzija transparentnosti u ovisnosti prema njihovom utjecaju na ukupni rezultat informacijske (a)simetrije.

Nadalje, pri ispitivanju pouzdanosti dizajniranog modela korišten je rezultat informacijske (a)simetrije kao zavisne varijable u odnosu na analizu varijanci postavljenih faktorskih opterećenja na obje dimenzije transparentnosti s ciljem testiranja hipoteza dobivenih postavljenim modelom. Ishodi postupka također su prikazani u Poglavlju 4.

1.10. Važnost istraživanja i znanstveni doprinos

Iako je mnogo istraživanja usmjereno na ispitivanje sadržaja politika privatnosti u odnosu na regulatorne ili zahtjeve pojedinih standarda u zaštiti podataka, malobrojna su istraživanja koja se fokusiraju i na kvalitetu samog mehanizma kojim se ti sadržaji komuniciraju

prema ciljnoj javnosti. Određujući faktore koji se odnose na obilježja jezika pri oblikovanju sadržaja politika privatnosti, postavljajući ih u odnos prema ostalim kvalitativnim svojstvima mehanizama transparentnosti, predmetno istraživanje daje uvid u važnost istih pri oblikovanju strategije informacijske transparentnosti, ne samo na području zaštite podataka, već se rezultati iste mogu primijeniti u odnosu i na druga područja s ciljem smanjenja informacijske asimetrije.

Stoga rezultati istraživanja mogu poslužiti kao podloga za izradu smjernica za osiguravanje učinkovitih alata transparentnosti, ali i za razvoj algoritama višekriterijskog simulacijskog modela zasnovanog na suvremenim tehnologijama.

Nadalje, ovo bi istraživanje trebalo značajno doprinijeti aktualnoj literaturi na području inženjerstva zahtjeva, integrirajući koncept informacijske (a)simetrije kao element vrednovanja uspješnosti mehanizama informacijske transparentnosti.

1.11. Ograničenja istraživanja

Rezultati istraživanja uključuju uzorak koji uključuje ograničeni set zdravstvenih ustanova s dostupnim politikama privatnosti na mrežnim stranicama. Iako se transparentnost, kao što je spomenuto, može promatrati kao regulatorni zahtjev, u odnosu na postavljene zakonske obveze, ili dobrovoljni zahtjev, motiviran poboljšanjem kvalitete i izgradnjom povjerenja korisnika, objava politika privatnosti na mrežnim stranicama nije obavezna.

Naime, sukladno Članku 13. Opće uredbi o zaštiti podataka [45] kao primjenjivog regulatornog okvira na području zaštite podataka u Republici Hrvatskoj, pojedinci moraju biti obaviješteni prije prikupljanja podataka u bilo kojem obliku, što ne postavlja objavu politika na mrežnom mjestu nužnom, iako Radna skupina iz članka 29. kao „odgovarajuću mjeru" za pružanje informacija o transparentnosti u slučaju voditelja obrade podataka koji je prisutan na internetu smatra pružanje informacija politika privatnosti „s pomoću elektroničke izjave/obavijesti o privatnosti" [24].

Stoga se i uzorak zdravstvenih ustanova javnog sektora zdravstvene zaštite, uslijed nedostatka dostupnih objavljenih politika privatnosti na mrežnom mjestu tijekom istraživanja u travnju i svibnju 2021. godine, može smatrati ograničenim setom, budući da su prikupljeni podaci tek za 56 od 148 zdravstvenih ustanova u sustavu javne zdravstvene zaštite, objavljenih na stranicama Ministarstva zdravstva [46].

1.12. Struktura rada

Rad je organiziran u šest poglavlja, a to su uvod, pregled literature, konceptualni i teorijski okvir, metodologija istraživanja (s rezultatima) te rasprava o rezultatima istraživanja i zaključak.

Poglavlje 1: Uvod

Ovo poglavlje postavlja istraživački kontekst i postavlja istraživanje u perspektivu, pružajući opće uvodne informacije, kao i informacije vezane uz istraživački problem.

Poglavlje 2: Pregled literature

Poglavljem se kroz pregled literature na području inženjerstva zahtjeva disertacija usklađuje sa širokim skupom ideja i principa na području upravljanja informacijskom privatnosti kao osnovom za razumijevanje užeg konceptualnog i teorijskog okvira izgradnje mehanizama transparentnosti. Opisani su i objašnjeni istaknuti metodološki pristupi izgradnji sustava arhitekture privatnosti te koncept privatnosti prema dizajnu, a kojih je osiguravanje transparentnosti sastavni i ključni element.

Poglavlje 3: Konceptualni okvir i teorija

Razvoj pravnog okvira za zaštitu privatnosti, kao neodvojivi dio osiguravanja sukladnosti s definiranim zahtjevima na području zaštite podataka, opisan u prvom djelu poglavlja, omogućava razumijevanje pretpostavki za ugradnju istog u tehnološke sustave organizacija, na koje je usmjeren drugi segment poglavlja, a kojim se postavljaju bitne odrednice istraživačkog dijela rada. Kroz pregled značajnih teorija na području privatnosti, preko pregleda značajki privatnosti u kontekstu suvremenih društvenih sustava, pružen je pregled važnih regulatornih dokumenata na europskom kontinentu, a koji se nameću u pojedinim zahtjevima istraživačke metodologije. Posljedično, a i nastavno na prethodno poglavlje vezano uz izgradnju arhitekture privatnosti, opisane su tehnologije i alati za osiguranje takvih sustava, s fokusom na alate i tehnologije za osiguranje informacijske transparentnosti.

Poglavlje 4: Metodologija istraživanja

Ovo poglavlje opisuje dizajn istraživanja kroz faze provedbe, navodeći potrebne informacije o metodama istraživanja, od odabira materijala i uzorka, postupaka prikupljanja podataka, do definiranja analitičke matrice i validacije iste. Kao ishod posljednje faze istraživanja predstavljen je konceptualni model vrjednovanja informacijske transparentnosti politika privatnosti kao primarni cilj istraživanja. Također, prikazani su podaci i postupci njegove validacije.

Poglavlje 5: Rasprava o rezultatima istraživanja

Poglavlje na temelju dobivenih rezultata testira postavljene hipoteze te uključuje raspravu nad rezultatima provedenih analiza, prilikom čega ističu se i raspravljaju nove teme koje su proizašle iz istraživačkog dijela rada, a prikazani su rezultati provedenih daljnjih istraživanja na uzorku zdravstvenih ustanova koje su postigle iznimne rezultate na obje dimenzije transparentnosti.

Poglavlje 6: Zaključak

Ovo poglavlje sažima nalaze i zaključuje rad, postavljajući ga u referenti okvir znanstvenih doprinosa.

2. PREGLED LITERATURE

Transparentnost, koncept definiran razmjerom u kojem jedna strana otkriva potrebne informacije o procesima donošenja odluka, procedurama, uspješnosti i funkcioniranju [47] drugoj, često je proučavan na područjima politologije, ekonomije i novinarstva, kao pravo građana [48] i preduvjet, odnosno zahtjev demokratskih društava [49].

2.1. Transparentnost – definicije i vrijednosti

Transparentnost, dakle, može značiti različite stvari različitim skupinama, ovisno o važnosti razloga koji se njome postižu. Prema Florini [50] transparentnost je „objavljivanje informacija institucija koje su relevantne za ocjenjivanje tih institucija“, bilo da se radi o javnim ili privatnim institucijama. Nadalje, Vishwanath and Kaufmann [51] definiraju transparentnost kao „povećan protok pravovremenih i pouzdanih ekonomskih, društvenih i političkih informacija, dostupnih svim relevantnim dionicima“, dok Organizacija za ekonomsku suradnju i razvoj (eng. The Organization for Economic Cooperation and Development; OECD) opisuje transparentno poslovno okruženje kao ono „u kojem gospodarski subjekti posjeduju bitne informacije o okruženju u kojem djeluju, dok im troškovi pretraživanja i asimetrija informacija ne predstavljaju nepotreban teret“ [52]. Upravo su za skretanje pozornosti na važnost informacija u funkcioniranju tržišta George Akerlof, Michael Spence i Joseph Stiglitz primili su Nobelovu nagradu 2001. za svoju analizu kako nesavršene informacije mogu voditi do tržišnih neuspjeha, postavljajući upravo informacijsku asimetriju ključnim preduvjetom transparentnosti [53].

Nadalje, brojne definicije čvrsto stavljaju važnost transparentnosti u sferu javne odgovornosti, postavljajući je kao sredstvo koje bi građanima omogućilo da javne dužnosnike smatraju odgovornima za svoje postupke [54], te smanjilo korupciju [55], odnosno postavilo im određena ograničenja [56]. U tom kontekstu, informacija sama po sebi nije važna, već da je ista potencijalno dostupna i uočljiva.

Razlike u pristupu transparentnosti uočili su Hallett i Viegi [57] uvodeći model koji razdvaja transparentnost na dvije vrste: ekonomsku transparentnost, usmjerenu prvenstveno na pitanje koje se informacije koriste i političku transparentnost, fokusiranu na način njihove upotrebe, odnosno kako se informacije koriste.

U kontekstu ekonomske transparentnosti, informacijska asimetrija postavljena je kao važan aspekt konkurentskih tržišnih modela pa je tom kontekstu rano u literaturi napravljena razlika između javnih informacija, dostupnih za sve, a koje se smatraju javnim dobrom, i privatnih informacija, dostupnih samo onima koji su ih stvorili (ili kupili) [58] te njihovim utjecajem na makroekonomske pokazatelje kroz ulogu središnje banke u gospodarstvu i učinka njenih informacija i prognoza na volatilnost tržišta [59][60][61]. Nadalje, empirijska istraživanja informacija i njihovog učinka na tržišta često su se fokusirala na financijska tržišta, fokusirajući se ispitujući prvenstveno utjecaj informacija [62][63][64] na tržišne cijene, a zatim na njihovu kvalitetu i količinu [65][66][67], pretpostavljajući da javne informacije dolaze nužno od vlade, a zanemarujući mogućnost da vlada neke zemlje može posjedovati ekonomske, financijske ili političke informacije koje namjerno odluči zatajiti od javnosti, čime se transparentnost automatski postavlja u ulogu mehanizama „odgovornosti“ kao važnog aspekta političke transparentnosti.

No, u kontekstu spomenute javnosti, transparentnost se može koristiti i kao mehanizam kontrole ponašanja javnih službenika, budući da informacija sama po sebi nije bitna, već kako njeno potencijalno objavljivanje može uzrokovati „ispravno“ ponašanje tih službenika. I stoga se transparentnost često koristi kao alat za smanjenje korupcije [68][69] te se teorijska literatura na tom području veže uz važnost slobodnih medija [70][71][72][73][74] kao alata za smanjenje informacijske asimetrije između vlade i građana, kako bi građani mogli donositi bolje odluke prilikom izbora vlasti, odnosno mogli se uvjeriti u vjerodostojnost političara i ostalih javnih dužnosnika kojima trebaju ukazati svoje povjerenje [75][76].

Općenito, empirijska literatura o odgovornosti u makroekonomskim okvirima slijedila je niz puteva koji sežu od transparentnosti samog proračuna [77][56] sve do posljedica transparentnosti na druge ekonomske rezultate [78][79], no dva su zajednička kriterija o tome što čini „transparentnost“: povećanje količine i kvalitete informacija dostupnih zainteresiranim stranama te povećanje ograničenja za javne dužnosnike kako bi se građanima omogućilo da te dužnosnike smatraju odgovornima za svoje postupke.

Prvim kriterijem pretpostavlja se postojanje mehanizama transparentnosti uopće, kao i njegova kvaliteta, dok se drugim kriterijem ti mehanizmi postavljaju kao elementi odgovornosti koja može biti u manjoj ili većoj mjeri obavezna.

U kontekstu poslovanja organizacija, kao mikroekonomskog okvira, transparentnost poslovnih subjekata ovisi o poslovnim informacijama, financijskim i nefinancijskim, koje omogućavaju pouzdanost, zakonsku sukladnost, kao izgradnju povjerenja između organizacije i njezinih dionika. Dok transparentnost financijskih informacija podrazumijeva objavljivanje financijskih izvješća, nefinancijska transparentnost informacija povezana je s društvenom odgovornošću poduzeća. Prva je često regulatorni zahtjev, dočim druga može biti motivirana izgradnjom brenda i povjerenja kod pojedinaca [80][81], ali i zakonskim obavezama u određenim aspektima poslovanja [82]. Tako s napretkom na području tehnologije i prava potrošača obaveznim postaju objave Općih uvjeta poslovanja [83] na mrežnim stranicama, a transparentnost postaje preduvjetom pri sklapanju ugovora o kupovini putem interneta, ugrađenim još u Strategiju jedinstvenog digitalnog tržišta na području Europske unije iz 2015. godine.

Još jedno područje u kojem se transparentnost postavlja kao prvoklasni koncept zahtjeva u odnosu na osiguravanje prava ispitanika je područje zaštite podataka i privatnosti koje je u društveno-tehničkim sustavima današnje, digitalne ekonomije [84] je neodvojivo od primjene informatičko-komunikacijskih tehnologija te arhitekture informacijskih sustava sukladno tim zahtjevima.

2.2. Izgradnja informacijskih sustava privatnosti

Usklađivanje softvera sa zahtjevima privatnosti je izazovan zadatak, budući da još uvijek nema jedinstvene metodologije izgradnje arhitekture takvog sustava, već postoji više okvira kojima se isti zahtjevi referenciraju [85][86], budući da zaštita privatnosti ne podrazumijeva puku zaštitu podataka, već zahtijeva holistički pristup sigurnosti kompletnih informacijskih sustava kroz poslovne prakse i osiguravanje kvalitete u svakom dijelu životnog ciklusa podataka.

Jedno razumijevanje tehničke privatnosti usredotočuje se na osiguranje osobnih podataka koji se obrađuju pomoću tehnika informacijske sigurnosti. Implementacijom svojstava tzv. trijade povjerljivosti, integriteta i dostupnosti [87] uz pomoć kriptografije, tehnologija kontrole pristupa i drugih načina, podržava se privatnost. Međutim, spomenute tehnike ne podržavaju mnoge zahtjeve za zaštitu podataka, kao što je prikupljanje podataka iz privolu pojedinaca ili usklađivanje obrade s pravilima privatnosti.

Iako je kriptografija je bitan alat za pružanje dobre privatnosti informacija, kriptografski protokoli koji omogućuju i održavaju privatnost informacija, međutim, mnogo su raznolikiji i složeniji od algoritama za šifriranje.

Privatnost unutar informacijskih sustava, stoga, treba promatrati kao upravljanje sporazumnim procesima i protokom informacija s osobnim podacima te kao interakcije temeljene na intervencijama ispitanika kao subjekata podataka. Mnoge aplikacije informacijsko-komunikacijskih tehnologija implementiraju poslovne procese koji zahtijevaju osobne podatke koji se posredstvom raznih transakcija razmjenjuju između ljudi ili digitalnih agenata uključenih u informacijski sustav.

U literaturi vezano uz upravljanje sustavima informacijsko-komunikacijskih tehnologija u odnosu na zahtjeve privatnosti ističu se koncepti PDCA i PMRM modela, zatim LINDDUN pristupa te arhitekture privatnosti prema dizajnu pri razvoju novih te evoluciji postojećih sustava.

2.2.1. Model planiranja, izvršenja, provjere i prilagodbe

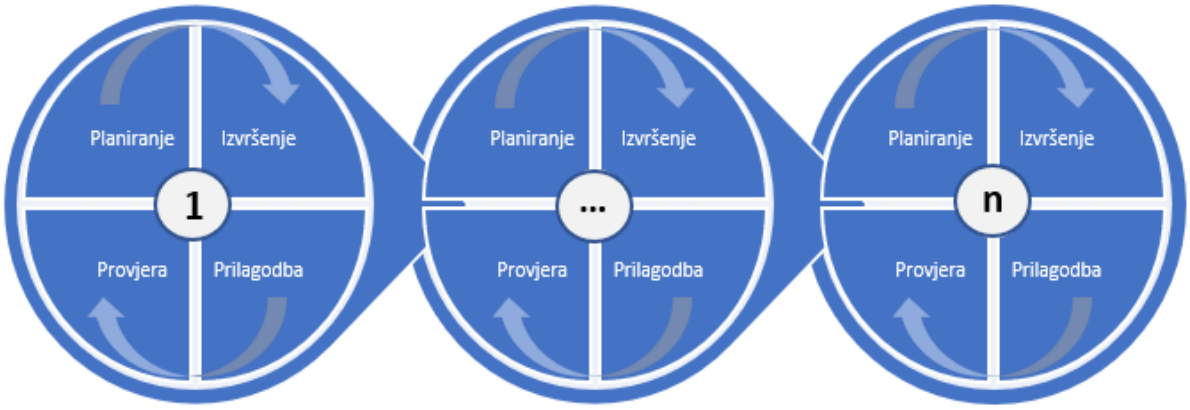
Model planiranja, izvršenja, provjere i prilagodbe (eng. Plan-Do-Check-Act model), odnosno PDCA model, je procesno orijentiran pristup za kontinuirano poboljšanje poslovnih procesa. U načelu predstavlja ciklički dijagram toka primjenjiv u poslovanju za učenje, kontrolu i poboljšanje proizvoda ili procesa, zasnovan na iterativnoj metodi upravljanja u četiri koraka: planiranju (eng. Plan), izvršenju (eng. Do), provjeri (eng. Check), prilagodbi (eng. Act) u odnosu na rezultate dobivene u prethodnoj fazi.

Poznat u literaturi i kao Demingov krug[3], model kao cilj ima poboljšanje procesa ili uklanjanje problema kao dio interaktivnog procesa zasnovanog na procjeni rizika. Stoga je isti sastavni dio mnogih standarda upravljanja informacijskim tehnologijama. Primjerice, skup ISO 2700x standarda za upravljanje sigurnošću informacija je zapravo implementacija PDCA modela, opisujući načine na koje organizacija može odgovoriti na rizike kroz izgradnju plana tretmana rizika, odnosno odabira odgovarajućih kontrola.

[3] Originalno Shewhartov krug kojeg je popularizirao još 1950. godine W. Edward Deming

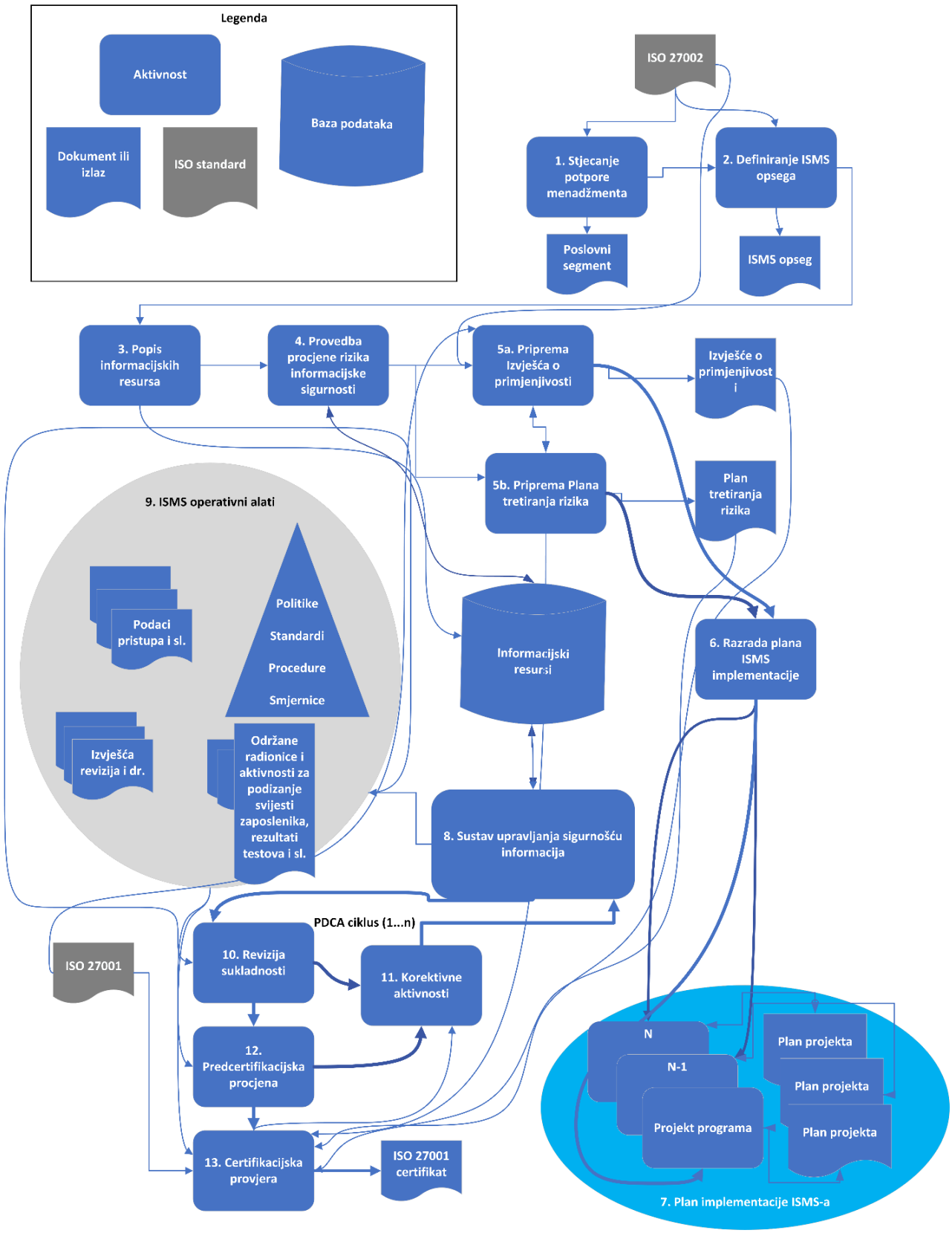
I dok ISO 27001 pruža zahtjeve za sustav upravljanja sigurnošću informacija (eng. Information Security Management System, ISMS), ISO 27701 pruža okvir za upravljanje privatnošću podataka. ISMS je bitan dio zaštite podataka, a njegovo stalno usavršavanje je ključno. Kako bi se osiguralo, implementira se PDCA model gdje se u prvoj fazi planiranja identificiraju poslovni ciljevi, stječe se podrška uprave te se definira opseg sustava za upravljanje informacijskom sigurnošću, kao i metode analize rizika s prihvatljivim rezultatima. Nadalje, u narednoj fazi generira se plan tretmana rizika te se kreiraju politike upravljanja istima, dodjeljuje se proračun, obučava se osoblje. U fazi provjere prati se provedba aktivnosti upravljanja sigurnošću i eventualno se priprema za certifikaciju njezinih rezultata, da bi se u posljednjoj, fazi prilagodbe provodile revizije ponovne procjene koje ocjenjuju ukupni ishod korektivnih radnji i pokreće novi krug ciklusa s korektivnim unosom, ako je potrebno [88].

Ako prva iteracija PDCA ciklusa ne ukloni rizike na zadovoljavajući način - ili ako bi nove procjene identificiraju nove rizike - tada će se ciklus ponavljati iznova, sve dok se glavni sigurnosni problemi ne riješe na zadovoljavajući način. Slika 1 prikazuje kontinuirane iteracije PDCA ciklusa.



Slika 1 Višestruke iteracije PDCA ciklusa se ponavljaju dok se problem ne riješi
Izvor: autorica

Sustav upravljanja sigurnošću informacija u skladu s ISO 27001 standardom zahtijeva vrlo detaljnu pripremu te posebne resurse i posvećenost osoblja u organizaciji. Potpuni ISMS je stoga često izvediv u velikim organizacijama s korporativnim politikama, obukom i profesionalnim upraviteljima informacijske sigurnosti. Na Slici 2 detaljno je prikazan organizacijski sustav okruženja takvog sustava.

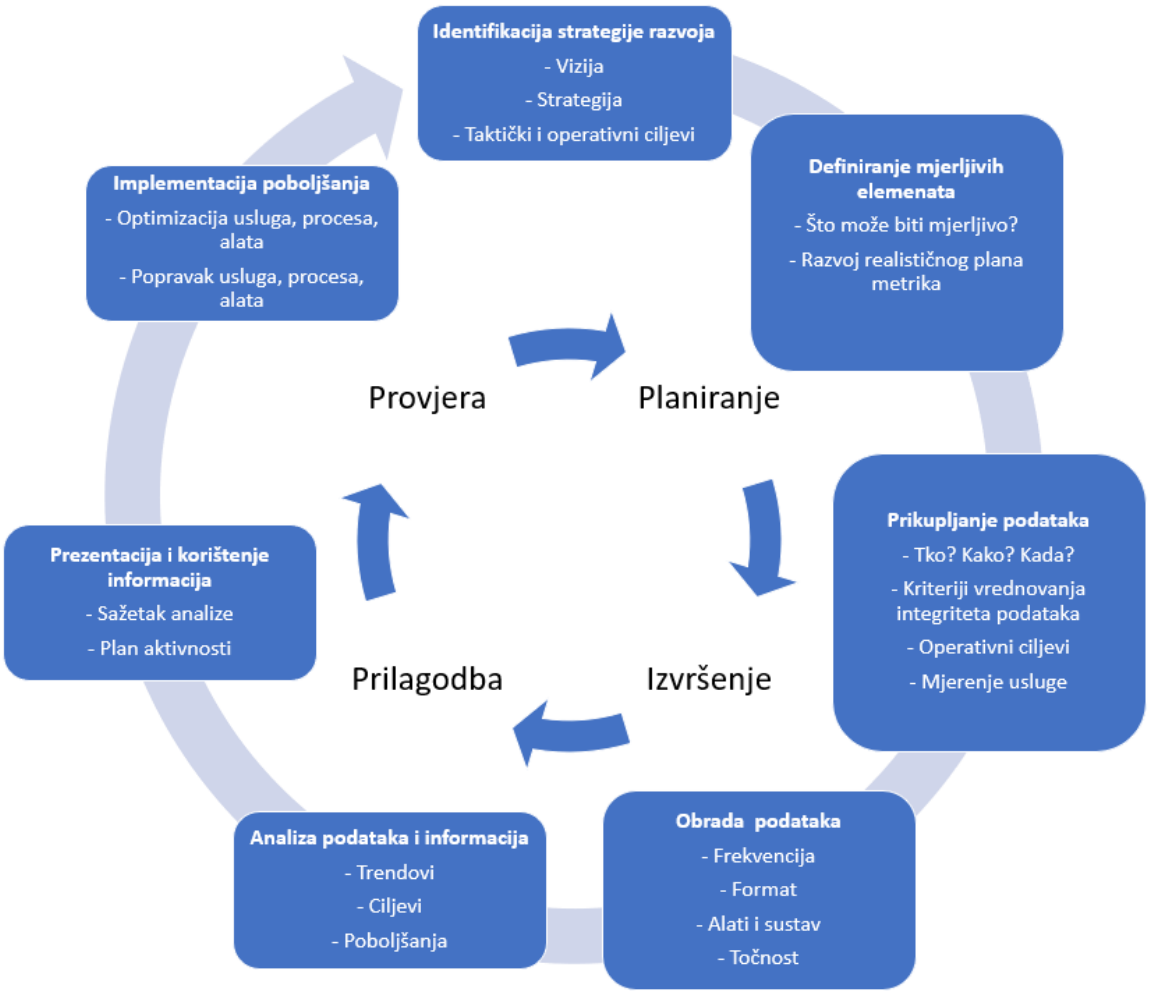


Slika 2 Detaljna skica ISO27001 sustava za upravljanja sigurnošću informacija
Izvor: [89], prijevod i prilagodba: autorica

Nadalje, PDCA model u središtu je ITIL (eng. Information Technology Infrastructure Library) radnog okvira kojeg je, reagirajući na rastuću ovisnost o uslugama informacijskih tehnologija, razvila Središnja agencija za računala i telekomunikacije Velike Britanije 1980. godine. U načelu radi se o biblioteci koja je svojoj inicijalnoj verziji opisivala niz preporuka, procesa, procedura i zadaća osmišljenih za standardizaciju najboljih praksi upravljanja informacijskim tehnologijama u vladinim uredima. Preporuke su izgrađene oko upravljanja operacijama koje se temelje na procesnom modelu Demingovog PDCA ciklusa te su do danas doživjele 4 izdanja, trajno se oslanjajući na isti. U međuvremenu ITIL okvir je postao svojevrsna norma za upravljanje uslugama vezanim uz informatičku potporu [90] te može biti primjenjiv i kao okvir usklađivanja sa zahtjevima privatnosti kao jednom od usluga, odnosno vrijednosti koje se pruža ispitanicima. Okvir je proširio PDCA model kroz model kontinuiranog poboljšanja usluge (eng. Continual Service Improvement; CSI) koji u središte modela stavlja procjenu sadašnjeg stanja koje mora biti prepoznato, dokumentirano i prihvaćeno od strane svih sudionika. U četvrtoj verziji radnog okvira kontinuirano poboljšanje jedna je od šest ključnih aktivnosti, ali i jedna od 14 općih praksi upravljanja.

Kao osnovnu funkciju na svim razinama u procjeni sadašnjeg stanja model kontinuiranog poboljšanja stavlja upravo inicijativu za promjenom i jasne ciljeve koji se mogu mjeriti kako bi se dobile informacije o stanju sustava u odnosu na ono željeno. U kontekstu inženjerstva zahtjeva radi se o metodi analize zahtjeva temeljene na ciljevima (eng. Goal-Based Requirements Analysis Method; GBRAM) [91][92], jednostavnom metodičkom pristupu identificiranju i preciziranju ciljeva koje softverski sustavi moraju postići, pretvarajući ih u operativne zahtjeve. Metoda predlaže strategije i tehnike identifikacije cilja i usavršavanja kroz uključivanje skupa heuristika kao oblika znanja i zaključivanja za konstrukciju odgovarajućih slučajeva uporabe i scenarija u softverskom inženjerstvu. CSI model slijedi pristup od 7 koraka za pregled, evaluaciju, planiranje i provedbu procesa poboljšanja, prikazanih kroz dijagram na Slici 3.

Kroz ovaj proces ITIL osigurava da se podaci dobiveni iz sustava interpretiraju i obrade u kontekstu do razine u kojoj postaju „naučene lekcije“, budući da su oba - i model i proces – iterativni, a trebaju se ponavljati na svim razinama (operativnoj, taktičkoj i strateškoj) kontinuirano.



Slika 3 Sedam koraka ITIL procesa
Izvor: [93]; prijevod i prilagodba: autorica

2.2.2. Model i metodologija za upravljanje privatnošću

Organizacija za razvoj otvorenih standarda OASIS (eng. Organization for the Advancement of Structured Information Standards) [94], usmjerena na poticanje razvoja, konvergenciju i usvajanje otvorenih standarda za globalno informacijsko društvo kroz svoj PMRM (eng. Privacy Management Reference Model and Methodology) model i metodologiju za upravljanje privatnošću predlaže standard za primjenu načela dizajna privatnosti kroz jasan set pravila i koraka za detaljnu analizu sustava i mapiranje potreba i postavki privatnosti kroz zaokruženi, pregled od 360° za sve dionike organizacijskog sustava.

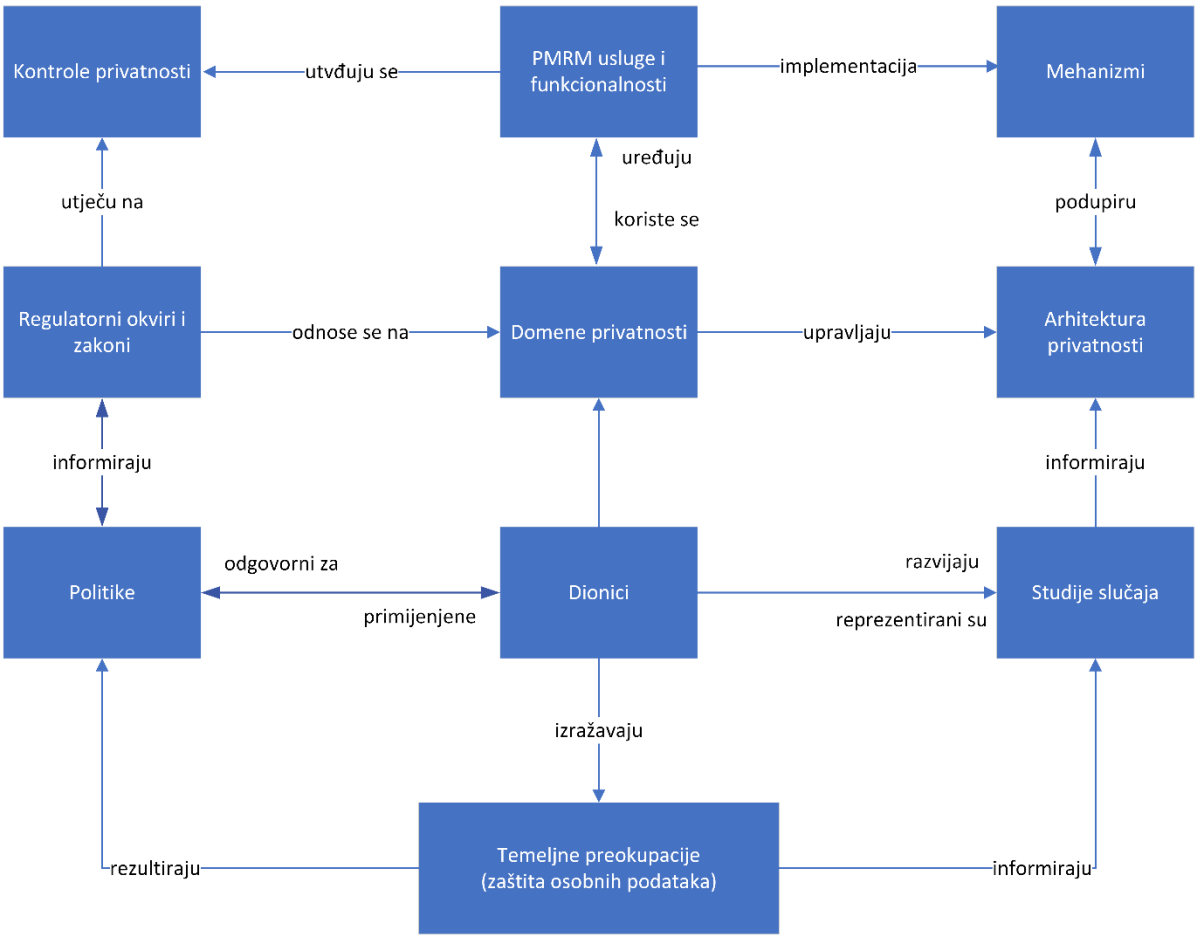
PMRM je također ciklički model, zasnovan na iteraciji, fokusiran isključivo na izgradnju sustava za upravljanje postavkama privatnosti. Radi se o setu pravila za izradu scenarija studija slučajeva, koji je potka za daljnju detaljnu analizu upravljanja privatnošću, a

implementatori imaju slobodu izabrati razinu granulacije do koje žele ići u određenom scenariju. Detaljna analiza privatnosti i popratna dokumentacija pogodna je za primjenu višestrukim akterima na području izgradnje i osiguranja zahtjeva privatnosti: činovnicima i rukovoditeljima te inženjerima na području procjene rizika, arhitektima poslovnih sustava, djelatnicima na izgradnji softverskih rješenja, kao i upravnim tijelima koji određuju i postavljaju politike privatnosti na razini cijelog sustava. Predstavljenu metodologiju za upravljanje privatnošću moguće je koristiti kao standard, unificirani alat za komunikaciju između svih spomenutih dionika te je ista korisna u poticanju interoperabilnih politika i standarda, kao i rješenja za upravljanje organizacijskih politikama vezanim za privatnost [94].

Model, prikazan dijagramom na Slici 4 podrazumijeva elemente kontrola privatnosti, implementirane od strane usluga i njihovih temeljnih funkcionalnosti kroz mehanizme, a koji rezultiraju visokim razinama analize sustava za uređivanje privatnosti (eng. Privacy Management Analysis; PMA) te podupiru arhitekturu privatnosti.

Metodologijom se podupiru zadaci:

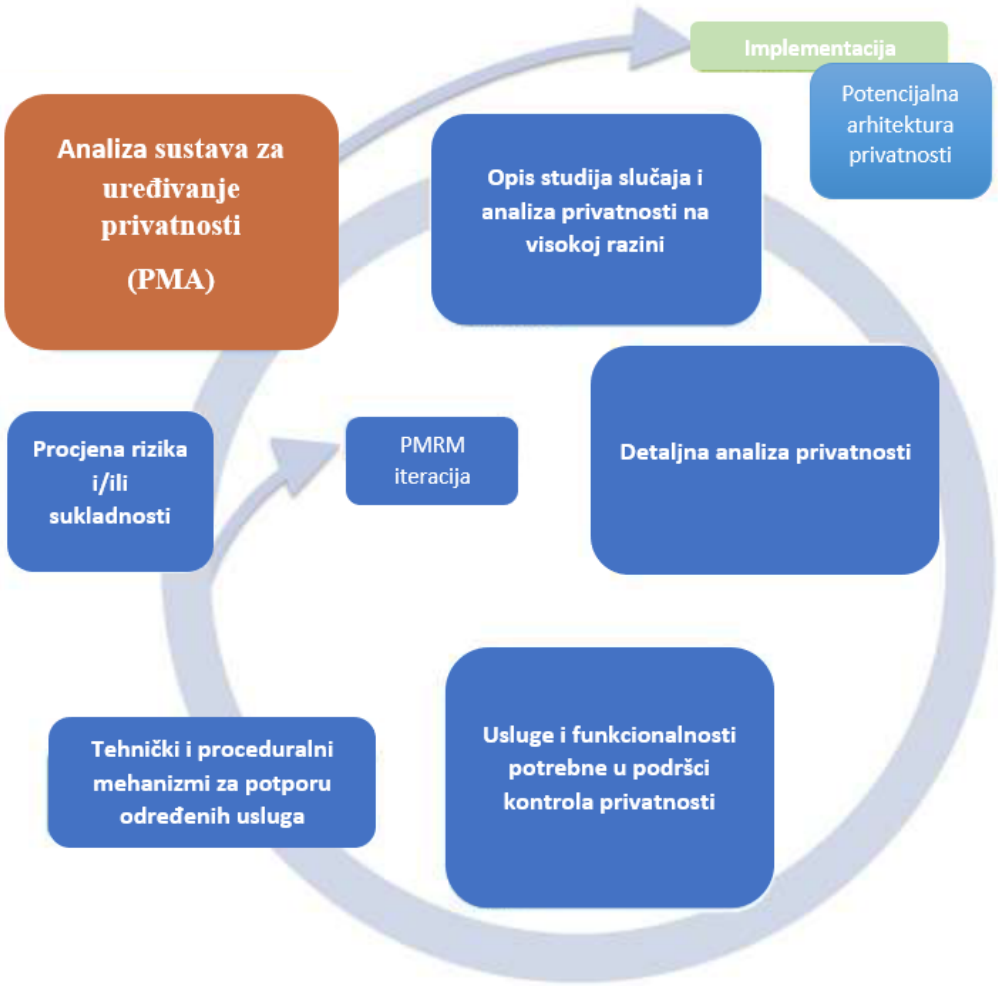
- definiranja i opisivanja studija slučajeva,
- identifikacije pojedinih poslovnih domena te razumijevanja uloga svih dionika u odnosu na politike privatnosti,
- identificiranja tijekova podataka te čvorova svih osobnih podataka unutar domena,
- određivanja različitih kontrola privatnosti,
- identificiranja domena kroz koje prolaze tijekovi osobnih podataka, a koje zahtijevaju kontrole privatnosti,
- mapiranja domena i usluga te funkcionalnosti, a zatim tehničkih i proceduralnih mehanizama,
- provođenja procjene rizika i sukladnosti te
- dokumentiranja PMA analize za buduće iteracije te za informiranje arhitekture privatnosti.



Slika 4 Dijagram PMRM modela za postizanje sveobuhvatne operativne privatnosti
IZVOR: [94], prijevod i prilagodba: autorica

Rezultati PMA analize, kao i postignuta arhitektura privatnosti, nadalje, mogu biti predmetom poboljšanja usluga, funkcionalnosti i mehanizama kroz nove inicijative smanjenja rizika, povećanja sukladnosti regulatornim zahtjevima te odgovornosti organizacije na području osiguranja privatnosti kroz metodologiju okvira prikazanu na Slici 5.

Dok opisi studija slučaja i analiza privatnosti na visokoj razini podrazumijevaju opise poslovnih procesa i aplikacija, definiranje regulatornih okvira za prilagodbu te identifikaciju implementacije potrebnih politika privatnosti temeljem inicijalne analize sustava, detaljna analiza je fokusirana na specifikaciju svih elemenata modela: domena i dionika, njihovih uloga i odgovornosti, tijekova podataka i čvorova ulaznih i izlaznih te interno kreiranih osobnih podataka kroz sustav kontrola privatnosti.



Slika 5 PMRM metodologija
Izvor: [94]; prijevod i prilagodba: autorica

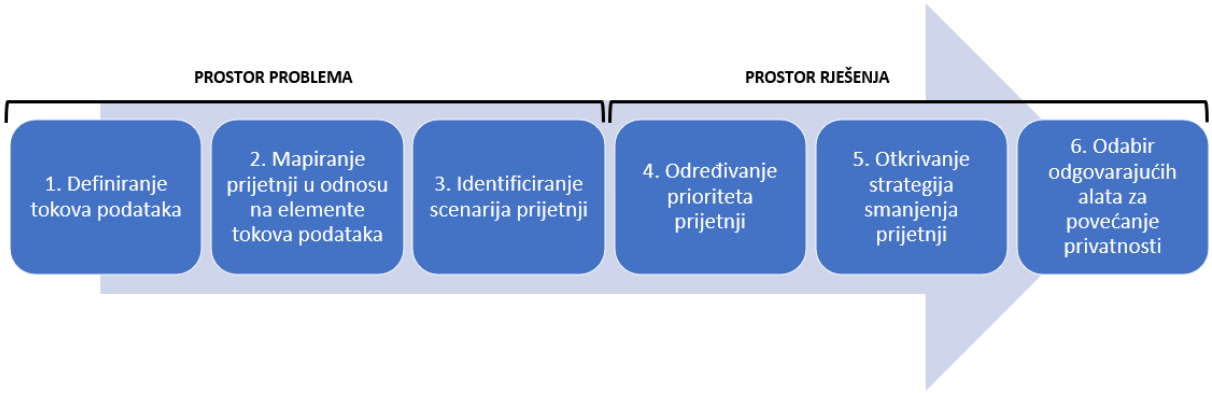
Nadalje, iako su faze poredane sukcesivno radi jasnoće, nijedan korak nije apsolutni preduvjet za početak rada na narednom koraku, budući da je cjelokupni proces iterativan. Jednako tako, proces provođenja odgovarajuće razine analize te određivanje kako i kada će se implementacija provesti, može započeti u bilo kojoj fazi tijekom cjelokupnog procesa.

2.2.3. LINDDUN metoda za dizajn privatnosti temeljen na prijetnjama

Još jedan pristup izgradnji sustava privatnosti je tzv. LINDDUN [akronim od Linkability (hrv. povezivost), Identifiability (hrv. mogućnost identificiranja), Non-repudiation (hrv. nemogućnost odbijanja), Detectability (hrv. mogućnost otkrivanja), Disclosure of information (hrv. otkrivanje informacija), Unawareness (hrv. nesvjesnost), Non-compliance (neusklađenost)] [95], metoda analize koja procjenjuje situaciju prijetnje privatnosti,

podržavajući analitičara privatnosti sa stablima prijetnji koja pomažu u odabiru odgovarajućih kontrola privatnosti. LINDDUN je razvila grupa istraživača DistriNet i COSIC zajednice KU Leuven u Belgiji [96].

LINDDUN je dvofazni proces od 6 koraka, predstavljenih na Slici 6, koji prvo definira prostor problema, a zatim prikazuje prostor rješenja za prijetnje privatnosti. Kao i prethodni model i LINDDUN se temelji na dijagramima toka kojima se mapira tijek osobnih podataka između raznih aktera i komponenti informacijskog sustava.



Slika 6 LINDUNN proces
Izvor: [97], prijevod i prilagodba: autorica

S ciljem definiranja problemskog prostora, LINDDUN u prvom koraku zahtijeva definiranje tokova podataka kako bi se omogućilo mapiranje prijetnji privatnosti u narednom koraku te se identificirali scenariji prijetnji kao korak kojim se „zatvara“ tzv. prostor problema te se pristupa prostoru iznalaženja rješenja za identificirane prijetnje. Četvrtim korakom se, nastavno, prijetnjama određuje prioritet, a zatim se u idućem koraku nastoje iznaći strategije smanjenja prijetnji. Konačno, šestim korakom odabiru se učinkovite protumjere, preslikavanjem identificiranih strategija ublažavanja u tehnologije privatnosti.

Kako bi se olakšala analiza, LINDDUN pruža i popise prijetnji, ali i tehnologije za poboljšanje privatnosti kategorizirane kroz sedam glavnih prijetnji privatnosti koje se nalaze i u nazivnom akronimu.

Povezivost (eng. linkability) ili mogućnost povezivanja sama po sebi nije nužno problem privatnosti, ali može rezultirati ozbiljnim prijetnjama kada međusobno „povezivi“

podaci dovode do identifikacije osobe ili zaključivanja o istoj. Povezivost se stoga odnosi na stanje u kojem je moguće dovoljno razlikovati jesu li dvije „stavke od interesa“ povezane ili ne, čak i bez poznavanja stvarnog identiteta subjekta povezive „stavke od interesa“ [98]. Drugi riječima, radi se o prijetnji privatnosti u kontekstu nemogućnosti sakrivanja veze između dvije ili više radnji/identiteta/dijelova informacija.

Nastavno, mogućnost identificiranja (eng. identifiability) odnosi se na nemogućnost sakrivanja veza između identiteta i radnji/dijelova informacija [98] te je u relaciji s postavkama anonimnosti i pseudonimnosti. Dok se anonimnost odnosi na skrivanje veze između identiteta i radnje ili informacije, pseudonimnost je korištenje pseudonima kao identifikatora subjekta, a kojih može biti više u odnosu na isti subjekt.

Nemogućnost odbijanja (eng. non-repudiation), nadalje, odnosi se na „posjedovanje nepobitnih dokaza o pojavljivanju ili nepojavljivanju događaja ili radnji“ [99], a povezano je „uvjerljivim poricanjem“ instanci privatnosti. Uvjerljivo poricanje osigurava da “instanca komunikacije između računalnih sustava ne ostavlja za sobom nedvojbene dokaze da se ista dogodila“ [99]. Drugim riječima, potrebno je osigurati komunikacijske protokole koji ne ostavljaju mogućnost poricanja određenih događaja ili aktivnosti kao sigurnosni aspekt informacijskih sustava kojima se osigurava odgovornost; odnosno, za svaku podatkovnu transakciju potrebno je osigurati vjerodostojnost.

Mogućnost otkrivanja (eng. detectability) definirana kao svojstvo u kojem „napadač može dovoljno razlučiti postoji li stavka od interesa ili ne“ [98]. U kontekstu informacijske sigurnosti određena poruka se može smatrati stavkom od interesa te je potrebno osigurati svojstva nemogućnosti njenog otkrivanja, ali i neopažljivosti prema svim subjektima koji nisu uključeni u komunikaciju, uključujući i anonimnost subjekata uključenih u korespondenciju.

Otkrivanje informacija (eng. disclosure of information) je pandan povjerljivosti, a koja se odnosi na skrivanje sadržaja podataka ili kontrolirano objavljivanje podatkovnog sadržaja. Izlaganje informacija nekome tko nije ovlašten da ih vidi smatra se prijetnjom privatnosti te je važan aspekt sigurnosti upravo očuvanje ovlaštenih ograničenja pristupa informacijama unutar organizacijskih politika.

Nesvjesnost (eng. unawareness) u kontekstu zaštite privatnosti se odnosi na razumijevanje posljedica dijeljenja osobnih podataka u prošlosti, sadašnjosti i budućnosti [100].

Pojedinac mora biti svjestan posljedica dijeljenja informacija, a organizacije trebaju osigurati transparentnost vezano uz njihove prakse nad podacima.

Naposljetku, neusklađenost (eng. non-compliance) odnosi se na nepoštivanje zakona (o zaštiti podataka), regulatornih odredbi ili postojećih suglasnosti korisnika vezano uz postavke privatnosti.

2.2.4. Arhitektura privatnosti prema dizajnu

Razvoj spomenutih okvira za upravljanje privatnošću unutar informacijskih sustava uslijedio je razvojem tzv. pristupa „privatnosti prema dizajnu“ (eng. Privacy by Design), konceptu vezanom uz inženjerstvo sustava koji privatnost stavlja u fokus tijekom cijelog procesa oblikovanja sustava. Riječ je o terminu koji je evoluirao 1990-ih, a sazrijevao 2000-ih, a koji se često koristio u političkom i aktivističkom kontekstu za promicanje ideja privatnosti informacija usmjerene na korisnika, kao preteče današnjih regulatornih i voluntarnih okvira za osiguravanje privatnosti.

Koncept privatnosti prema dizajnu popularizirala je Ann Cavoukian, povjerenica za informiranje i privatnost kanadske pokrajine Ontario od 1997. do 2014. godine, a temelji se na 7 principa koji se proširuju na „trilogiju obuhvatnih aplikacija: 1) sustavi informacijskih tehnologija; 2) odgovorno poslovanje; i 3) umrežena infrastruktura.“ [101]

Za razumijevanje koncepta „privatnosti prema dizajnu“ potrebno je shvaćanje konteksta tog vremena. Informacijski sustavi su dizajnirani s načinom razmišljanja mrežnog klijenta spojenog na veliki poslužitelj, dok je jedina svrha sustava bila provedba poslovne svrhe, a relevantni kriteriji za odabir sustava bili su minimalni troškovi implementacije i održavanja. Takvo okruženje dovelo je do brojnih strategija i taktika za usklađenost zaštite podataka, poput kreiranja složenih i nečitljivih politika privatnosti koje su napravljene kako bi se sakrila stvarna velika količina podataka koja se obrađuje neovisno o privoli pojedinaca [102], odbijanje usluga korisnicima koji nisu pristali na postavljene uvjete privatnosti te zanemarivanje i/ili odbijanje zahtjeva za uvid u obradu podataka na temelju tvrdnji o poslovnoj tajni. Nadalje, zaštita privatnosti korisnika ovisila je isključivo o vlastitoj inicijativi i odgovornosti, korištenjem u to vrijeme rijetkih alata, dok su softverske aplikacije s opcijama za konfiguraciju prilagođene privatnosti često imale zadane konfiguracijske postavke koje su omogućavale prikupljanje i obradu osobnih podataka.

U opisanom kontekstu, istraživači privatnosti prepoznali su situaciju u kojoj pojedinci, krajnji korisnici usluga, nikada neće imati dovoljno moći, resursa ili vremena da stvarno ostvare svoja prava zajamčena tadašnjim zakonima o zaštiti podataka. Isti su također zaključili da teret isporuke usklađenih sustava informacijskih tehnologija treba staviti na dobavljače sustava, a ne na njihove korisnike, te iste smatrati odgovornima za dizajniranje sustava s omogućavanjem prilagođenih postavki privatnosti.

Koncept privatnosti prema dizajnu tako je 2010. godine, na 32. Međunarodnoj konferenciji povjerenika za zaštitu podataka i privatnost (eng. International Conference of Data Protection and Privacy Commissioners) u Jeruzalemu, priznat kao „ključna komponenta temeljne zaštite privatnosti“ [103]. Netom nakon jeruzalemske konferencije, Savezna trgovinska komisija (eng. Federal Trade Commission; FTC) Sjedinjenih Američkih Država prepoznala je koncept kao jedan od tri preporučene prakse za zaštitu *online* privatnosti u svome dokumentu *Zaštita korisničke privatnosti u eri brzih promjena* [104], a isti je odmah utkan u prijedlog Opće uredbe o zaštiti podataka koji je objavljen 25. siječnja 2012. godine.

Danas kada je prijedlog napokon usavršen i Uredba prihvaćena, privatnost korisnika bi trebala biti „zadanom“ (eng. Privacy by default) tj. potrebno je osigurati automatsku primjenu najstrožih postupaka za osiguravanje privatnosti kroz bilo koji informacijski sustav ili poslovnu praksu, kao jedan od ključnih načela dizajna privatnosti. Da bi se to postiglo, potrebno je osigurati detaljnu procjenu rizika i to na način da se optimiziraju svi zahtjevi te se ne zadire u punu funkcionalnost sustava, pa je privatnost stoga postavljena u četvrtom principu kao pozitivna suma (eng. positive-sum) funkcionalnosti samih sustava i privatnosti. Naravno, ti zahtjevi trebaju biti poštivani kroz cijeli životni ciklus podataka (eng. end-to-end), prema petom principu, od prikupljanja do uništavanja podataka, što se može postići postavljanjem sigurnosnih mjera kroz cijeli proces.

Preduvjeti vidljivosti i transparentnosti iz šestog principa trebaju biti osigurani kroz dokumentirane i jasno komunicirane procedure kroz sve razine poslovanja, dok iste trebaju biti osigurane kroz najviše standarde sigurnosti postavljene preventivno, a ne reaktivno kroz cijeli organizacijski sustav i kulturu poslovanja, kao prvi od principa dizajna privatnosti.

Budući da se korisnika stavlja u središte poslovanja pa time i zaštite privatnosti, u posljednjem, sedmom principu koncepta dizajna privatnosti istome je potrebno osigurati opcije

privole za obradu podataka, za osiguravanje točnosti i ažurnosti podataka, kao i pristup podacima te mogućnost prigovora obradi.

Drugim riječima, privatnost se treba ugraditi u dizajn arhitekture cijelog tzv. ekosustava osobnih podataka (eng. personal data ecosystem) [105] u kojem pojedinci imaju mogućnost upravljanja svojim osobnim podacima, a koji mora uzeti u obzir sljedeće uvjete:

- prvenstvo korisnika, odnosno uvjet da korisnici trebaju steći kontrolu nad vlastitim podacima i imati mogućnost odlučivanja o dijeljenu njihovih podskupova;
- čitkost podataka, uvjet da sustav mora osigurati visokorazvijene alate i objašnjenja o implikacijama korisnikovih odluka vezanih uz podatke kako bi razumjeli rizike prikupljanja, dijeljenja i pohrane podataka i
- dugoročnu povezanost, odnosno zahtjev kojim bi sustav trebao poticati na stalnu aktivnost korisnika za održavanjem relevantnosti i ažurnosti podataka.

Regulatori, aktivisti i političari percipirali su koncept privatnosti prema dizajnu kao metodologiju za ugrađivanje privatnosti u novodizajnirane sustave. Međutim, iako načela izražavaju glavne zahtjeve za ugrađenu privatnost, ona su ipak bliža pravnoj filozofiji privatnosti nego procesu softverskog inženjeringa. Stoga su se razvile različite vrste kritika pristupa, osobito nakon rezolucije povjerenika za zaštitu podataka i privatnost u Jeruzalemu [103].

Koncept je u literaturi kritiziran kao „nejasan" [106], ostavljajući mnoga otvorena pitanja o njihovoj primjeni u inženjerskim sustavima [107], posebice u raznim kontekstima digitalne ekonomije [106] u kojima su rizici na privatnost pojedinca povećani [108][109].

2.3. Procjena utjecaja na privatnost

Procjena utjecaja na privatnost (eng. Privacy Impact Assessment; PIA) je naziv za proces koji analizira i dokumentira budući učinak koji će obrada osobnih podataka imati na pojedince, ispitanike. „Utjecaj na privatnost" su sve moguće, neželjene i nevidljive, posljedice koje obrada podataka može nametnuti pojedincima ili organizaciji kao rezultat obrade osobnih podataka, povrede podataka ili prikupljanja podataka.

Ideja o procjeni utjecaja na privatnost prisutna je od 1970-ih godina [110], no do danas ne postoji sustavna metoda za provođenje iste, već se koriste razne metode, poput spomenute PMRM, te smjernice određenih nacionalnih tijela i stručnih organizacija koje su objavile popise za provjeru zahtjeva. Također, izvješće o provedeno analizi potrebno je kao dokaz sukladnosti prema nadzornom tijelu. Detaljnu analizu za različita regulatorna okruženja i njihove zahtjeve za PIA objavili su Tanrock, Pearson i Charlesworth [111].

U svojoj taksonomiji privatnosti Solove [112] identificira četiri radnje koje krše privatnost, a utječu na ispitanike: prikupljanje podataka, obrada istih, njihovo dijeljenje i invazije.

Prikupljanjem informacija povećava se skup informacija, čime se mijenja ravnoteža moći između ispitanika i obrađivača podataka, a prikupljanje netočnih ili naših zastarjelih podataka može kasnije uzrokovati štetu. Nadalje, obrada osobnih podataka, elektroničko odlučivanje i gomilanje podataka može rezultirati diskriminacijom, isključenjem, uskraćivanjem ili pružanjem nepotpune usluge, pogrešnim zaključcima, neopravdanom kombinacijom podataka, greškama u klasifikaciji.

Dijeljenjem informacija iste se šire drugim procesorima, privatnim ili profesionalnim krugovima, javnosti, kriminalcima, a uzroci mogu biti dio legitimne aplikacije ili povrede podataka (hakiranje, krađa podataka ili kvarovi sustava). Dijeljenje podataka uključuje i kompleksna pitanja o slobodi pristupa informacijama od strane policije, vlade te pitanje domovinske sigurnosti.

Invazije su sve vrste izravnih ili neizravnih interakcija s ispitanikom, a koje se temelje na osobnim podacima, od neželjenog oglašavanja preko profiliranja do mogućih ucjena.

Pojedinci, ispitanici izloženi su riziku kršenja privatnosti već od koraka prikupljanja podataka, a taj rizik raste sa svakim korakom prema invaziji. Stoga, analizom utjecaja na privatnost treba uzeti u obzir sve rizike.

Prema PIAF (eng. A Privacy Impact Assessment Framework for data protection and privacy rights) okviru proizašlom iz istoimenog projekta [113], PIA je cjelokupni proces ili projekt sastavljen od sljedećih koraka:

1. rani početak razvojnog projekta,
2. opis projekta,
3. savjetovanje dionika,
4. upravljanje rizicima,
5. provjera zakonske usklađenosti,
6. preporuke i izvješća,
7. odluka i provedba preporuka i
8. revizija i pregled.

Isključujući prvi ili početni, koraci su zapravo slični PDCA ciklusu te koracima upravljanja privatnošću modela i metodologije za upravljanje privatnošću OASIS organizacije.

Nadalje, budući da su prava na privatnost i zaštitu osobnih podataka temeljna prava u europskom pravnom poretku, kako bi se osigurala najviša razina njihove zaštite, PIA bi se trebala baviti svim vrstama pitanja privatnosti, a ne samo zaštitom osobnih podataka, a organizacija bi trebala moći dokazati da je PIA provedena na odgovarajući način [114]. Također, PIA proces treba uživati barem minimalnu razinu transparentnosti; i procjenitelj i dionici moraju imati sve relevantne informacije za procjenu implikacija predloženog projekta na privatnost i zaštitu podataka. Stoga je potrebno u procjenu uključiti sve dionike, što je moguće reprezentativnije, te uključujući i javnost, ako je primjenjivo, kroz redovne obavijesti o planiranom projektu i procesima procjene. Njihove stavove treba tražiti i uzeti u obzir, a politika provedbe projekta trebala bi osigurati eksplicitne mehanizme za savjetovanje s dionicima. Posljedično, i finalno izvješće treba biti javno i lako dostupno.

Također, proces procjene utjecaja na privatnost trebao bi biti podvrgnut vanjskoj reviziji i/ili reviziji. Neovisni pregledi i/ili revizije treće strane su jedini način da se osigura da su procjene utemeljene na razumijevanju rizika te da će njihove preporuke biti provedene [115]. Budući da nadzorna tijela za zaštitu podataka, a koja ujedno imaju i savjetodavnu ulogu, nemaju resurse za reviziju svih izvješća, alternativno, neovisni revizori mogu preuzeti ovaj zadatak. Također, razne organizacije stručnjaka, poput Međunarodne udruge stručnjaka za privatnost (eng. The International Association of Privacy Professionals; IAPP) pružaju mogućnosti za certificiranje, kako pojedinaca, tako i ustanova.

Na kraju, rezultati procjene trebaju ublažiti sve moguće rizike i druge negativne utjecaje na privatnost svih dionika, dok preostali rizici trebaju biti opravdani. Proces procjene rizika zahtijeva relativnu kvantifikaciju rizika, pri čemu procjenjivač treba uzeti u obzir vjerojatnost pojave rizika na privatnost u odnosu na posljedice istog. Razmatrajući značaj rizika i vjerojatnost njegove pojave te veličinu utjecaja, ako se rizik dogodi, razina rizika može biti klasificirana kao niska, srednja ili visoka.

Agencija Europske unije za mrežnu i informacijsku sigurnost (eng. The European Union Agency For Network and Information Security; ENISA) objavila je smjernice za procjenu rizika privatnosti za mala i srednja poduzeća [116] koje sadrže smjernice o procjena utjecaja na privatnost usmjerene na ispitanike, a u kojima su definirane četiri razine utjecaja na privatnost prikazane u Tablici 1.

Tablica 1 Razine utjecaja na privatnost

Razina utjecaja	**Opis**
Niska	Pojedinci se mogu susresti s nekoliko manjih neugodnosti koje će prevladati bez ikakvih problema (npr. vrijeme potrošeno na ponovni unos informacija, smetnje, iritacije itd.).
Srednja	Pojedinci se mogu susresti sa značajnim neugodnostima koje će unatoč nekoliko poteškoća moći prevladati (npr. dodatni troškovi, uskraćivanje pristupa poslovnim uslugama, strah, nerazumijevanje, stres, manja tjelesna oboljenja i dr.).
Visoka	Pojedinci se mogu susresti sa značajnim posljedicama koje bi trebali moći prevladati, iako uz ozbiljne poteškoće (npr. pronevjera sredstava, stavljanje na crnu listu od strane financijskih institucija, oštećenje imovine, gubitak posla, sudski poziv, pogoršanje zdravstvenog stanja itd.).
Vrlo visoka	Pojedinci kod kojih mogu nastupiti značajne, pa čak i nepovratne posljedice, koje možda neće prevladati (npr. nesposobnost za rad, dugotrajna psihička ili tjelesna oboljenja, smrt i sl.).

Izvor: [116], str. 20; prijevod: autorica

2.4. Kontrole privatnosti

Za razliku od paradigme "sigurnosti perimetra" koja je godinama bila ključna za informacijsku sigurnost, rizici po privatnost javljaju se i unutar i izvan informacijskog sustava.

Pojavom poslovnih modela digitalne ekonomije mnogi sustavi na internetu trguju osobnim podacima i obrađuju ih kao samu svrhu sustava, a učinci povrede sigurnosti privatnih informacija mogu utjecati na vlasnika informacijskog sustava kao i na osobu o kojoj se podaci odnose, što izaziva dualnost rizika po privatnost [117] koji se dijele na poslovne rizike za organizacije te rizike za pojedince.

Među poslovne tako se mogu svrstati i reputacijski rizici, odnosno gubitak povjerenja i imidža kod korisnika (koji posljedično mogu utjecati na povećanje izdataka za marketing), rizici vezano uz sukladnost i izgubljene prilike. Osim mogućih novčanih kazni, rizici koji se tiču nesukladnosti s zakonskim zahtjevima mogu dovesti do sudskih tužbi i procesa, gubitaka licenci, isključivanja iz potencijalnih poslovnih prilika s javnim i državnim organizacijama te, općenito, povećanih pravnih troškova. Izgubljene prilike, osim spomenutih reputacijskih gubitaka kod pojedinaca, mogu uključivati i isključivanje iz poslovnih prilika na međunarodnom tržištu, izgubljene korisnike i/ili više troškove njihove akvizicije [118].

Rizici za pojedince, odnosno ispitanike dijele se na rizike tzv. samodeterminacije, intransparentnosti te rizika na zdravlje i slobode [117]. Pod rizike samodeterminacije ubrajaju se gubici reputacije, cjenovne diskriminacije, primanje neželjene pošte i/ili poruka telemarketinga te veći napori pri održavanju kontrole nad podacima. Nadalje, rizici tzv. intransparentnosti, odnosno smanjene transparentnosti, mogu prouzročiti konfuziju pojedinca vezano uz znanje drugih o istome, neizvjesnost, gubitak povjerenja te u konačnici, tzv. „društva dosjea“, tj. društva u kojem se održavaju računalne evidencije o pojedinim građanima, a vlada ih koristi za praćenje aktivnosti građana kako bi se obeshrabrilo političko neslaganje i druge vrste ponašanja koje se ne odobrava [119]. Posljedično i rizici na zdravlje i slobode mogu uključivati totalitarizam, intruzije te neželjeno praćenje.

Međutim, u područjima upravljanja rizikom i odluka o ulaganju, dualnost rizika po privatnost do jačanja suvremenih regulatornih okvira kojima se jačaju prava ispitanika nije bila predmetom veće zabrinutosti. Incidenti vezani uz povredu informacijske sigurnosti rijetko su razmatrali štete vezano uz povredu privatnosti ispitanika.

Dvije okolnosti otežavaju implementaciju sustava upravljanja rizikom privatnosti. Prvo, za razliku od proračuna sigurnosnog rizika, u domeni privatnosti pitanje rizika nije usredotočeno isključivo na vlasnika informacijskog sustava tj. organizacije i odgovarajuće štete

nanesene njegovim radom. Upravljanje privatnošću uključuje i privatne podatke, ne samo ispitanika, već i zaposlenika i drugih dionika u poslovanju i potencijalnu štetu nanesenu njima, čime se komplicira stvaranje jednostavne baze podataka s troškovima i vjerojatnošću kršenja privatnosti, jer svaka vrsta korisnika - ovisno o aplikaciji - ima različitu osobnu vrijednost na riziku, a temeljna pitanja u procjeni rizika privatnosti su: koliko će štete prouzročiti određena povreda privatnosti; koliko dugo će osobni podaci koji su izašli u javnost predstavljati rizik; je li rizik konstantan tijekom vremena, smanjuje li se ili će se povećavati; kako se rizik mijenja kada se osobni podaci kombiniraju s drugim informacijama; kako pojedina obrada koji koristi osobne podatke utječe na rizik [117].

Koncept kontrole privatnosti odnosi se na popise mjera koje će smanjiti rizik privatnosti u informacijskom sustavu, a koje odgovaraju na rizike identificirane u procesu analize rizika s obzirom na postavljene razine utjecaja utvrđene u analizi utjecaja na privatnost. Upravitelj rizikom odabire odgovarajuće kontrole koje ispunjavaju niz zahtjeva iz kategorija tehničkih kontrola i administrativnih kontrola.

Prva kategorija su kontrole koje su dio informacijske tehnologije koja se koristi za obradu osobnih podataka te su često zapravo funkcije informacijske sigurnosti, poput kontrole pristupa, enkripcije, zaštite integriteta, osiguranja dostupnosti. Nadalje, sigurnosne funkcije kao što su zaštita od požara, osiguravanje redundantnih izvora napajanja te rezervnog hardvera također su dio tehničkih kontrola. Tehničke kontrole implementiraju se u tehničku infrastrukturu kroz za to predviđene projekte i pri većim promjenama tehnološke baze.

Nadalje, sve administrativne kontrole su ne-tehničke kontrole. Administrativne kontrole su, na primjer, upravljanje kvalifikacijama osoblja, sigurnosna provjera osoblja, odgovarajuća administracija privole ispitanika i politike privatnosti u skladu s praksama obrade podataka. Administracija fizičkog pristupa računalnom hardveru i uređajima za pohranu podataka, upravljanje ulogama i privilegijama koje dovode do autorizacije u sustavima kontrole pristupa te autorizacija i nadzor podizvođača kao izvršitelja obrade podataka drugi su primjeri administrativnih kontrola. Administrativne kontrole implementiraju se u procese, procedure, politike i operacije.

Kontrole su podijeljene u četiri vrste: preventivne, detekcijske, korektivne i kompenzacijske [120]. Za svaku vrstu mogu postojati tehničke i administrativne, odnosno netehničke kontrole.

Preventivne kontrole koriste se kako bi se spriječilo da se prijetnja ostvari i nastane šteta. Detekcijske kontrole pomažu prepoznati da je, i kako je, prijetnja utjecala na sustav. Korektivne kontrole smanjuju učinak prijetnje smanjenjem ostvarene štete. Kompenzacijske kontrole koriste se za ublažavanje ili smanjenje štete osiguravanjem alternativnih izvora.

Iako se u procesu dizajna arhitekture privatnosti razmatraju uglavnom preventivne kontrole, detektivske kontrole važan su okidač za važne reakcije na povredu podataka ili kompromitaciju podataka koja se stvarno dogodila, što je važan aspekt zaštite podataka, ali i regulatorne sukladnosti u odnosu na odredbe Opće uredbe za zaštitu podataka. Budući da pokreću tretman kompromisa s korektivnim kontrolama, pokreću korištenje kompenzacijskih kontrola u slučaju nedovoljnog rezultata korekcije ili usporedno s korekcijom te „proizvode" nova znanja u spoznaje o rizicima i učinkovitosti postojećih preventivnih kontrola, važan su aspekt upravljanja privatnosti te u kontekstu PDCA ciklusa predstavljaju korak provjere, svojevrsni katalizator usavršavanja sustava zaštite privatnosti.

Tretiranje identificiranih rizika dio je većeg procesa upravljanja rizikom privatnosti. Mnogi utvrđeni standardi usredotočuju se isključivo na tehničke aspekte, aspekte informacijske sigurnosti ili aspekte menadžerskih odgovornosti i procesa. Dok se standardi upravljanja informacijskim tehnologijama često fokusiraju na aspekte tehnologije i pouzdanosti, upravljanje privatnošću zadire u domene kao što su pravo, poslovanje, optimizacija ulaganja i usklađenost. Strukturirani proces za odluke o ulaganju u privatnost sastoji se od pet koraka [117]:

1. analiza okruženja sustava;
2. analize utjecaja na privatnost;
3. izbor protumjera;
4. analize ukupnog troška vlasništva;
5. dizajna i implementacije.

U prvom koraku uspostavlja se kontekst sustava prikupljanjem pravnog i tehničkog okvira, korisničkih zahtjeva i ograničenja poslovnog modela. Drugi korak procjenjuje prijetnje

privatnosti, modelira imovinu osobnih podataka i provodi analizu rizika i procjenu utjecaja na privatnost. Tijekom trećeg koraka odabiru se potencijalne protumjere protiv prijetnji, što uključuje kontrolu privatnosti i druge protumjere. U četvrtom koraku perspektiva povrata ulaganja u privatnost pomaže u razumijevanju ograničenja odabranih kontrola. Konačno, u petom koraku odabrane kontrole i protumjere se postavljaju, dokumentiraju i procjenjuju kao dio životnog ciklusa aplikacija informacijskog sustava.

Nadalje, zahtjevi privatnosti mogu se kategorizirati i u odnosu na životni ciklus podataka unutar informacijskog sustava. U odnosu na aktivnosti koje se vrše nad podacima tj. obrade[4] moguće je definirati određenu strategiju zaštite privatnosti kao svojevrsni cilj u osiguravanju holističkog sustava, pa Colesky, Hoepman i Hillen [121] definiraju model kako se te strategije mogu primijeniti protiv radnji koje smanjuju privatnost. Za svaku radnju nad podacima ili obradu duž životnog ciklusa, od rukovanja i pohrane, preko zadržavanja, prikupljanja i dijeljenja do izmjene i povrede, moguće je izdvojiti primjenjivu strategiju. Autori identificiraju osam različitih strategija koje se koriste za poboljšanje privatnosti: provedbu, demonstraciju, informiranje, kontrolu, minimiziranje, apstrakciju, odvajanje, sakrivanje.

Slika 7 prikazuje tablični model kojim se za svaku aktivnost, može prikazati odgovarajuća strategija, označena sivom bojom pozadine. Nadalje, aktivnosti su podijeljene i s obzirom na taksonomiju privatnosti Daniela Solovea [112], odnosno radnje koje krše privatnost, a utječu na ispitanike.

Aktivnosti	Taksonomska grupa	Odnosi se na	PROVEDBA	DEMONSTRACIJA	INFORMIRANJE	KONTROLA	MINIMIZIRANJE	APSTRAKCIJA	ODVAJANJE	SAKRIVANJE
Rukovanje	Obrada									
Pohrana										
Zadržavanje										
Prikupljanje	Prikupljanje									
Dijeljenje	Diseminacija									
Izmjena	Invazija									
Povreda										

Slika 7 Strategije kontrola privatnosti preslikane u odnosu na radnje nad podacima
Izvor: [121]; prijevod: autorica

[4] Opća uredba o zaštiti podataka definira Člankom 4. sveobuhvatni pojam obrade kao „svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje“.

Predložene strategije su već definirane u literaturi [122] te su sastavni dio određenih standardizacijskih ili zakonskih okvira na području zaštite podatka i/ili privatnosti.

Tako strategija minimiziranja, a koja zagovara minimalno prikupljanje i obrađivanje osobnih podataka, može uključivati pristupe [122]: „sve ili ništa“, odnosno ekskluzivno odbijanje obrade podataka od strane pojedinaca ili pružanje detaljnih, selektivnih postavki privatnosti.

Iako je minimiziranje strategija prepoznata u ISO 29100 i u konceptu privatnosti prema dizajnu, ta dva pristupa razdvajaju minimiziranje podataka od ograničavanja prikupljanja podataka. Tako za Cavoukian [101] minimiziranje zapravo započinje sa zbirkom osobnih podataka koja treba biti ograničena i svedena na strogi minimum, tj. potiče se nesakupljanje nesvrsishodnih podataka, dok se ista strategija u ISO 29100 odnosi na smanjenje operacija nad podacima, a koje trebaju biti usmjerene na princip dijeljenja podataka samo s nužnim stranama.

Nadalje, strategija vezana uz sakrivanje podataka odnosi se na taktike ograničenja zadržavanja podataka, ali i na zahtjeve povjerljivosti podataka, nemogućnost njihova otkrivanja i/ili identificiranja [98], pri čemu se zaštitne mjere i principi mogu povezati sa opisanim LINDDUN metodama te su također sastavni dio ISO 29100 standardizacijskog okvira.

Odvajanje podataka ili obrada podataka, odnosi se na distribuciju ili izolaciju osobnih podataka, u pohrani ili radu, ovisno o taksonomskoj grupi D. Solovea, kako bi se otežala korelacija istih za zlouporabu. Strategija se odnosi na sprječavanje povezivanja dovoljnog seta podataka pri stvaranju informacija koje bi mogle ugroziti ispitanikovu privatnost te je, u načelu, vrlo „bliska“ prethodnoj strategiji sakrivanja podataka. Također, ista se može povezati sa strategijom minimiziranja podataka u odnosu na svrhe obrade podataka te ograničenje istih i odvajanje u skladu sa specifikacijama njihove namjene, a njene taktike mogu se odnositi kako na sistemske operacije i tablice u bazi podataka, tako i na fizičke distribuirane sustave unutar mogućnosti.

Strategija apstrakcije oslanja se na metode agregacije, odnosno sažimanja ili grupiranja podataka do najviše razine agregiranosti, a koja omogućava daljnji rad nad istima. Strategija se oslanja na koncept k-anonimnosti koji su na područje informacijske sigurnosti i privatnosti uvele Latanya Sweeney i Pierangela Samarati 1998. godine [123].

Strategije kontrole i informiranja međusobno su povezane i odnose na ciljeve transparentnosti te intervenabilnosti, mogućnosti utjecaja ispitanika na ishode vezano uz obrade njihovih osobnih podataka. Dok su taktike vezano uz prvu strategiju detaljno opisane temom rada, taktike vezano uz kontrolu djelomično se odnose na također u nastavku opisan koncept privole te prava ispitanika na ažuriranje ili brisanje određenih podataka u sustavu, kao i na povlačenje iz obrada kao i njihovu obustavu. Obje ove strategije usmjerene su na odnos ispitanika i voditelja obrade, dok su preostale dvije strategije usmjerene su na voditelja obrade i nadzorno tijelo.

Tako se strategija provedbe odnosi na stvaranje i održavanje sustava za upravljanje postavkama privatnosti kroz tehničke i administrativne kontrole te se „ogleda“ kroz usklađenost sa zakonskim odredbama, za što je potrebno osigurati što više dokaza, a koji se definiraju i realiziraju kroz strategiju demonstracije. Dok se prva strategija može taktizirati kroz osiguravanje pravnih osnova za obradu podataka, minimiziranje podataka i strategije sigurnosti istih u odnosu na kontrole pristupa, druga strategija uključuje praćenje aktivnosti nad podacima, osiguravanje komunikacijskih protokola koji ne ostavljaju mogućnost „uvjerljivog poricanja“ aktivnosti vezano uz zaštitu privatnosti, provedbu redovitih unutarnjih i vanjskih revizija te izvješćivanja.

2.5. Inženjerstvo zahtjeva transparentnosti

2.5.1. „Okviri“ zahtjeva transparentnosti

Slijedom opisanih metoda i pristupa, razvidno je kako arhitektura privatnosti unutar organizacijskog sustava podržava transparentnosti kao bitni i nezaobilazni aspekt.

I sâm koncept privatnosti prema dizajnu ističe načelo transparentnosti kojim [101] „nastoji uvjeriti sve dionike da bez obzira na poslovnu praksu ili tehnologiju, organizacija zapravo djeluje u skladu s navedenim obećanjima i ciljevima, ovisno i o neovisnoj provjeri. Ispitanik je u potpunosti upoznat s prikupljenim osobnim podacima i za koju svrhu, dok su svi sastavni dijelovi i operacije vidljivi i transparentni, kako za korisnike tako i za pružatelje usluga.“

Načelo nadalje završava upozorenjem: „Zapamtite, vjerujte, ali provjerite!“ (eng. „Remember, trust but verify!“) kojim se zapravo „ocrtava“ ključno svojstvo transparentnosti – osiguravanje integriteta, odnosno točnosti i cjelovitosti informacija vezano uz prakse obrade podataka, kao i cilj transparentnosti za krajnje korisnike, a koji se materijalizira u mogućnosti verifikacije, odnosno provjere funkcionira li sustav kako je deklarirano, a kako bi se mogle odrediti odgovornosti za diskrepancije. Inače, radi se o staroj ruskoj poslovici koja je popularizirana od strane američkog predsjednika Ronalda Reagana u vrijeme tzv. hladnoratovskog sukoba, obilježenog nepovjerenjem između dvije sile, između zapadnih sila, predvođenih Sjedinjenim Američkim Državama, i istočnih sila, predvođenih Savezom Sovjetskih Socijalističkih Republika, a u svome diskursu nastavili su je koristiti mnogi istaknuti političari u Sjedinjenim Američkim Državama [124]. U opisanom kontekstu zaštite privatnosti, jasno se očitava utjecaj transparentnosti na povjerenje od strane korisnika.

Kao osnova za implementaciju načela transparentnosti i vidljivosti u organizacijske strukture [125] konceptom privatnosti prema dizajnu se nadalje definiraju prakse odgovornosti, otvorenosti i usklađenosti u odnosu na osnovna načela obrade osobnih podataka. Tako odgovornost (voditelja obrade) prilikom prikupljanja osobnih podataka podrazumijeva i dužnost brige za njihovu zaštitu. Odgovornost za sve politike i postupke vezane uz privatnost mora se dokumentirati i priopćiti na odgovarajući način i dodijeliti određenoj osobi, a prilikom prijenosa osobnih podataka trećim osobama potrebno je osigurati jednaku zaštitu privatnosti putem ugovornih ili drugih sredstava. Navedena odgovornost postiže se transparentnošću koja se instrumentalizira u pružanju informacija o politikama i praksama koje se odnose na upravljanje osobnim informacijama dostupnim pojedincima. Jednako tako, potrebno je uspostaviti mehanizme za podnošenje pritužbi i obeštećenja, a informacije o njima potrebno je komunicirati pojedincima, uključujući i način pristupa sljedećoj razini žalbe. Nadalje, potrebno je poduzeti potrebne korake za praćenje, procjenu i provjeru usklađenosti s politikama privatnosti i procedurama.

Spomenute prakse „proizašle“ su iz *Praksi poštenog informiranja* (eng. Fair Information Practices; FIP), koje je razvio Odjel za zdravstvo, obrazovanje i socijalnu skrb Sjedinjenih Američkih Država još 1960-ih godina kao reakcija na zabrinutost zbog implementacije velikih vladinih baza podataka koje sadrže informacije o građanima [126]. Taj skup načela za zaštitu privatnosti osobnih podataka u sustavima evidencije nadalje je proširen od strane Organizacije

za ekonomsku suradnju i razvoj 1980. godine u dokumentu pod naslovom *Smjernice OECD-a o zaštiti privatnosti i prekograničnim tokovima osobnih podataka* [127] koji je postao temelj za većinu postojećih zakona i propisa o zaštiti podataka u naredna tri desetljeća. Godine 2013. OECD je izdao revidirane smjernice u dokumentu pod nazivom *Okvir za privatnost OECD-a* [128]. U predgovoru dokumenta navedeno je da je, „u usporedbi sa situacijom prije 30 godina, došlo do duboke promjene opsega u pogledu uloge osobnih podataka u našim gospodarstvima, društvima i svakodnevnom životu", te da je "okruženje u kojem se tradicionalna načela privatnosti sada provode doživjelo značajne promjene" [126].

Svaka verzija spomenutih načela od strane OECD-a kao rezultat predstavlja konsenzus o osnovnim načelima koja bi se trebala „ugraditi" u postojeće nacionalno zakonodavstvo ili poslužiti kao temelj za zakonodavstvo u zemljama koje ga još nemaju, odražavajući tehnološki napredak tog vremena, a nastojeći omogućiti kontinuiranu trgovinu i gospodarski rast između država, izbjegavajući prepreke slobodnom protoku informacija. Tako je u azijsko-pacifičkoj regiji razvijen *Okvir privatnosti* od strane organizacije Azijsko-pacifička ekonomska suradnja (eng. The Asia-Pacific Economic Cooperation; APEC) [129], a koji modelira temeljne vrijednosti OECD-ovih *Smjernica o zaštiti privatnosti i prekograničnih tokova osobnih podataka* te potvrđuje važnost privatnosti za pojedince i informacijsko društvo.

Nadalje, *Okvir za privatnost* Nacionalnog instituta za standarde i tehnologiju (eng. The National Institute of Standards and Technology; NIST) Ministarstva trgovine Sjedinjenih Američkih Država iz [130], usmjerava se na upravljanje rizicima za privatnost pojedinaca, usredotočujući se više na razvoj praktičnih zahtjeva inženjeringa privatnosti, umjesto na opća načela koja su priznata u dokumentima OECD-a i APEC-a, postavljajući detaljan pregled aktivnosti i ishoda kao osnove za donošenje daljnjih odluka vezanih uz upravljanje rizicima privatnosti. I *Općeprihvaćena načela privatnosti* (eng. Generally Accepted Privacy Principles; GAPP) koje su razvili Udruženje međunarodnih certificiranih profesionalnih računovođa (eng. The Association of International Certified Professional Accountants; AICPA) i Radna skupina za zaštitu privatnosti Kanadskog instituta ovlaštenih računovođa (eng. Canadian Institute of Chartered Accountants; CICA) usmjerena su na potrebe usklađivanja s nacionalnim i međunarodnim regulatornim okvirima vezanim uz zaštitu podataka iz privatnosti, ali iz poslovne perspektive. Tako GAPP operacionalizira složene zahtjeve privatnosti u jedan cilj privatnosti koji je podržan s 10 načela privatnosti opisanih s objektivnim, mjerljivim kriterijima

koji čine osnovu za učinkovito upravljanje rizikom privatnosti i usklađenošću u organizaciji [131].

Svaki od navedenih okvira privatnosti upućuje na važnost komunikacijskih praksi vezanih uz obradu podataka prema pojedincima te tematici posvećuje zaseban dio dokumenta, ali s različitom terminologijom. Tako *Općeprihvaćena načela privatnosti* te *Okvir privatnosti* od strane organizacije Azijsko-pacifička ekonomska suradnja taj zahtjev jednostavno nazivaju obaviješću (eng. Notice), dok se *Smjernice OECD-a o zaštiti privatnosti i prekograničnim tokovima osobnih podataka* na isti referiraju kao „specifikacija svrhe“ (eng. Specification of Purpose), a *Okvir za privatnost* Nacionalnog instituta za standarde i tehnologiju kao „svjesnost o obradi podataka“ (eng. Data Processing Awareness).

2.5.2. Zahtjevi transparentnosti kao softverska „disciplina“

U kontekstu informacijskih sustava, transparentnosti se pristupa iz perspektive softverskog inženjerstva u kojem se ona odnosi na specifikaciju unutarnjih procesa funkcioniranja sustava te se stoga obično kategorizira kao nefunkcionalni zahtjev u odnosu na funkcionalnost softvera, smatrajući se prvenstveno pitanjem kvalitete [132], čime je uglavnom proučavana kao koncept „drugog razreda“.

Prva su istraživanja na području inženjerstva zahtjeva predlagala primjenu okvira nefunkcionalnih zahtjeva (eng. NFR Framework) [133] te metodu i* modeliranja [134], ostavljajući zaključno mogućnost da to nisu konačna rješenja te da su potrebna daljnja istraživanja.

Daljnja istraživanja dovela su do definiranja aspekata transparentnosti [135], koncepta koji sadrži sljedećih pet nefunkcionalnih zahtjeva: dostupnosti, upotrebljivosti, informativnosti, razumljivosti i mogućnosti revizije, kao uvjeta za postizanje transparentnosti. Nadalje, usmjereni na korisničke zahtjeve u dva rada Dabbish i dr. [136][137], kao primjer transparentnog softverskog okruženja navode platformu Github, dovodeći ju u odnos s paradigmom otvorenosti društvenih mreža, dok [138] predlaže primjenu tzv. okvira argumentacije (eng. Argumentation Framework), odnosno pristupa usmjerenom zadovoljavanju korisničkih zahtjeva transparentnosti pri softverskom inženjerstvu.

Nadalje, kao funkcionalni zahtjev informacijskih sustava transparentnost se veže uz atribute pouzdanosti [139], povjerenja [140] [141] [142] [143], odgovornosti [144] [145], ali i informiranog donošenja odluka dionika u određenom sustavu [146] [21].

Uočivši nedostatak vezane literature na području zahtjeva transparentnosti sa stanovišta ispitanika, a nastavno na prethodna istraživanja [84][147], Hosseini i dr. se fokusiraju na identificiranje upravo zahtjeva potrebnih za donošenje informiranih odluka od strane ispitanika u svrhu izrade jezika za modeliranje zahtjeva transparentnosti [148] te, posljedično, postavljanja konceptualnih modela [149] istih u odnosu na poslovno-informacijske sustave. Modelom tzv. korisne transparentnosti [149], u formi spektra postignute transparentnosti, postavljeni su zahtjevi transparentnosti za donošenje odluka od strane ispitanika: od dostupnosti informacija kao prvog, preko interpretacije, pristupačnosti, percepcije, razumljivosti, prihvaćanja te mogućnosti poduzimanja radnji kao zadnjeg stupnja spektra, odnosno koraka u postizanju tzv. korisne transparentnosti. Nadalje, kao prepoznati [150][151] ključan aspekt transparentnosti, kvaliteta informacija predmetom je drugog referentnog modela istih autora [149] koji zahtjeve iste postavljaju kroz dimenzije kvalitete informacija preuzete od Kahn [152], dovodeći posljedično elemente oba modela u međuovisnost.

Istraživanja vezana uz politike privatnosti pokazala su da su pojedinci zainteresirani za nekoliko različitih informacija koje se nalaze u politikama privatnosti [153][154], no pokazalo se da su često one neučinkovite [155][156], zbog svoje kompleksnosti i nerazumljivosti [157] [158][159], a zbog njihove dužine često se one niti ne čitaju [23].

Nadalje, opsežna istraživanja, stoga su usmjerena na pitanja upotrebljivosti obavijesti o privatnosti [155][160][161][162] kako bi predložila njihova poboljšana sučelja [163], posebice u suvremenim digitalnim okruženjima. Tako se dio istraživača posvetio automatiziranoj obradi pravila o privatnosti [164][165], nastojeći iskoristiti metode obrade prirodnog jezika i strojnog učenja za rješavanje problema automatske kategorizacije politika privatnosti [166] i grupiranje segmenata od politike temeljene na pitanjima privatnosti kojima se bave [167].

U tome smjeru moguće je izdvojiti istraživačke projekte prema razvoju strojno čitljivih jezika, obično temeljenih na XML jeziku za označavanje podataka, a koji bi omogućio napredne postavke privatnosti u odnosu na korisničke preference. Uspoređujući stvarne postavke s onima koje je korisnik odredio, također u strojnom obliku, omogućuje se jednostavnije i zatim

vidljivije prezentiranje informacija u kojoj mjeri politika servisne strane ispunjava očekivanja korisnika i koliko daleko može odstupiti od njegovih ili njezinih preferencija privatnosti u trenutku kada se od korisnika traži da pristane na otkrivanje podataka. Primjeri takvih jezika politika privatnosti uključuju *Platformu za postavke privatnosti* (eng. Platform for Privacy Preferences), ili ukratko P3P [168], koju je razvio i preporučio W3C konzorcij 2002. godine. Međutim, razvoj tog jezika ubrzo je prestao, a osim P3P verzije dodatka za rukovanje kolačićima u Internet Explorer pregledniku, vrlo malo je poznatih implementacija jezika. Također, napredni jezici politika privatnosti razvijani su kroz istraživačke projekte financirane sredstvima Europske unije. Primjerice, *Projektom odgovornosti u oblaku* (eng. The Cloud Accountability Project), ili skraćeno A4Cloud projektom, razvijen je PrimeLife Policy Language (PPL) koji također omogućava provedbu tzv. „ljepljivih politika“ [169] usporedbom politika privatnosti organizacije i preferencija korisnika. Međutim, strojni jezici politika privatnosti rijetko se koriste izvan opsega istraživačkih projekata.

3. KONCEPTUALNI I TEORIJSKI OKVIR

3.1. Koncept i dimenzije privatnosti

Privatnost, koncept vrlo bogat u značenju, i često vrlo cijenjen, posebice pri njegovom izostanku, težak je za definiranje. Prvu definiciju kao "prava na ostavljanje na miru" (eng. “The right to be left alone”) ponudili su Samuel D. Warren i (budući sudac Vrhovnog suda SAD-a) Louis D. Brandeis 1890. godine za članak u Harvard Law Review časopisu [170]. Na to ih je potaknuo tehnološki napredak novih medija koji se očitovao u sve većoj primjeni fotografija u tadašnjem „tisku“, otvorivši pravnu diskusiju o postavljanju granica između javnog i privatnog.

Nadalje, Bok [171] definira privatnost kao „stanje zaštićenosti od neželjenog pristupa od strane drugih – ili fizičkog pristupa, osobnih informacija, ili pažnje“, dok Westin [172], jedan od najranijih teoretičara područja, identificira privatnost kao „pravo pojedinaca, grupa, ili institucija da za sebe odluče kada, kako, i u kojoj mjeri su informacije o njima komunicirane drugima“.

Dakle, u svom načelu, privatnost se odnosi na postavljanje granica, odnosno kontrole pri zaštiti jastva ili sebstva u odnosu na druge, odnosno javnost, te se često veže uz svojstvo tajnosti, sprečavanja drugih da znaju o nečijim postupcima, mislima i komunikaciji. Drugim riječima, privatnost se može definirati kao stanje ili okolnost ograničenog pristupa osobi. Tako se u raznim područjima života pojedinaca isprepliću različite dimenzije privatnosti: prostorna i fizička privatnost, privatnost komunikacija te informacijska privatnost [173].

Dok se fizička privatnost odnosi na sigurnost vlastitog tijela od nepoželjnih kontakata, poput neželjenih seksualnih kontakata ili medicinskih zahvata pa i torture, prostorna privatnost temelji se na zaštiti određenih prostora od neželjenih intruzija. Najčešće su to prostori spavaonice, kupaonice i ureda, ali i zaključanih kovčega te automobilskih prtljažnika. U tome kontekstu, i prenapučeni stambeni prostori te životni uvjeti također se mogu smatrati stanjem smanjene privatnosti.

Privatnost komunikacije odnosi se na povjerljivost poštanskih pošiljaka, telefonskih razgovora i drugih oblika komunikacije, što je ujedno i ustavna kategorija mnogih zemalja,

uključujući i Republiku Hrvatsku[5] [174]. Naposljetku, zaštita podataka, zapravo njihova povjerljivost, svojstvo je privatnosti koje se definira mogućnošću pojedinaca da odabiru s kim (i na koji način) će dijeliti informacije o sebi pa se informacijska privatnost često povezuje i sa značajkom identiteta. Anonimizacija i deidedentifikacija procesi su kojima se disociraju informacije od identifikatora osobe [175], uklanjajući sponu kojom bi se mogli izvesti odnosi između pojedinih podataka o određenoj osobi.

Privatnost odražava postojeće norme o granicama osobe, ali nije ograničena tim normama, koje često mogu biti odraz vremena i općeg društvenog konsenzusa [19]. Stoga je i sâm koncept privatnosti promjenjiv, a promjene mogu biti postupne ili mogu dolaziti u nizu radikalnih pomaka, poput novih tehnologija (primjerice, razvoja infrastrukture interneta stvari i umjetne inteligencije) ili socijalnih poremećaja (poput pandemija, ratova i revolucija). Stoga, norme privatnosti treba sagledavati u odnosu na kontekst sustava društvenih normi koji utječu na protok informacija, a koje distribuiraju moć, štite odnose i interese te omogućiti ljudima interakciju bez nanošenja štete jedni drugima. Ljudi smatraju da je njihova privatnost narušena kada informacija teče suprotno utvrđenim normama, i doživljavaju njeno kršenje posebno zabrinjavajućim kada je kontekstualni integritet samih normi pod izazovom.

Bez privatnosti, pojedinci mogu biti izloženi upadima koji, budući da su neželjeni, mogu biti ponižavajući. Nadalje, kontrola nad osobnim podacima nužna je za razvoj individualnosti te samopoštovanja kao pojedinca, budući da može zaštiti osobu od neugodnosti, stigmatizacije ili diskriminacije, pri čemu je povjerljivost senzitivnih informacija, poput medicinskog stanja, seksualne orijentacije, vjerske ispovijesti ključna.

U središtu koncepta privatnosti je, sukladno tome, zaštita osobe na više načina, a temeljne vrijednosti koje se na taj način „štite“ su autonomija, osjećaj sposobnosti donošenja autentičnih izbora o važnim životnim pitanjima, i dostojanstvo osobe.

3.2. Teorije privatnosti

Među teorijama privatnosti kao dvije najbolje artikulirane i najbolje potkrijepljene teorije privatnosti ističu se dijela Irwina Altmana i već spomenutog Alana Westina. Iste su

[5]Prema Članku 36. Ustava Republike Hrvatske „sloboda i tajnost dopisivanja i svih drugih oblika općenja zajamčena je i nepovrediva“.

tijekom vremena istaknute u glavnim pregledima privatnosti posljednja tri desetljeća 20. stoljeća [176][177][178] te su utjecale na suvremene teorije 21. stoljeća, usmjerenim proučavanju novih medija i razumijevanju interpersonalne komunikacije posredovane računalima, poput teorije upravljanja komunikacijskom privatnošću Sandre Petronio [179].

Westinova teorija privatnosti [172] govori o tome kako se ljudi štite privremenim ograničavanjem pristupa drugih prema sebi. Postavljajući privatnost kao „zahtjev pojedinaca, grupa ili institucija da sami određuju kada, kako i u kojoj mjeri se informacije o njima prenose drugima“ Westin tvrdi da je ljudima potrebna privatnost koja, u odnosu i na druge potrebe, pomaže osobama da se emocionalno prilagode svakodnevnim međuljudskim interakcijama.

Stoga, za Westina, privatnost je ujedno i dinamički proces koji se mijenja s tijekom vremena u odnosu na emotivni razvoj pojedinca. Budući da osobe reguliraju privatnost kako bi bila dovoljna za ispunjavanje trenutačnih potreba i zahtjeva uloge koju osoba preuzima u određenom trenutku, ljudi mogu imati premalo, dovoljno ili previše privatnosti čime njena funkcija nije monotona, već se „ogleda“ u tim izmjenama.

Nadalje, Westin posebno ograničava svoju teoriju na zapadne demokracije jer je privatnost u skladu sa sociopolitičkim vrijednostima tih demokracija gdje privatnost nije samodostatan cilj sam po sebi, već je sredstvo za postizanje sveukupnog kraja samospoznaje pa postulira četiri stanja privatnosti: samoću, intimnost, anonimnost i rezerviranost.

Dok je samoća sloboda od promatranja od strane drugih, intimnost se odnosi na izolaciju male grupe ljudi s ciljem postizanja bliskosti, opuštenosti i iskrenog odnosa. Anonimnost se, nadalje odnosi na slobodu od identifikacije i od nadzora na javnim mjestima i za javne radnje, a rezerviranost se temelji na želji ograničavanja „otkrivanja drugima“, odnosno zahtjevu da druge osobe prepoznaju i poštuju tu želju.

Navedena stanja su ujedno i sredstva pomoću kojih se ostvaruju funkcije (svrhe ili ciljevi) postignute privatnosti, a koje opet definira kroz četiri stavke. Osobna autonomija odnosi se na želju da se izbjegne postojanje manipuliranosti, dominacije ili izloženosti od strane drugih. Emocionalno oslobađanje odnosi se na oslobađanje od napetosti društvenog života i zahtjeva koji isti nameće, pružajući sigurni odmak od raznih društvenih uloga, emocionalnih stanja i/ili devijacija istih te upravljanje istima.

Samoevaluacija se odnosi na integriranje iskustva osobe u smislene obrasce i nametanje individualnosti kroz događanja što uključuje obradu informacija i proces planiranja vezano uz „otkrivanje“ drugima, kao i integraciju iskustava kroz prizmu moralnih i vjerskih stavova. Konačna funkcija, ograničena i zaštićena komunikacija, ima dva aspekta. Dok ograničena komunikacija postavlja međuljudske granice, zaštićena komunikacija omogućava dijeljenje osobnih podataka s osobama od povjerenja.

I Altman je [180], poput Westina, proučavao privatnost u odnosu na pojedince i grupe s ciljem analize regulacijskih mehanizama koji djeluju na koherenciju sustava. Zauzimajući dijalektičku perspektivu regulacije privatnosti, on istu opisuje kroz dinamički proces interakcije s drugima; pojedinci mijenjaju razinu „otvorenosti“ prema drugima kao odgovor na promjene u njihovim unutarnjim stanjima i vanjskim uvjetima.

Budući da je socijalni i ekološki psiholog, Altman postavlja društvenu interakciju u temelj svoje teorije te koristi okolinu za pružanje mehanizama regulacije privatnosti. Pri tome je privatnost za njega "selektivna kontrola pristupa sebi" koja ima pet svojstava.

Prvo, privatnost uključuje dinamički proces interpersonalne kontrole osobnih granica. Drugo, razlikuju se željene i stvarne razine privatnosti. Treće, privatnost je nemonotona funkcija s optimalnom razinom privatnost koja se očituje u jednakosti željene i aktualne razine privatnosti, dok se ostale mogućnosti uključuju razinu prevelike privatnosti (kada je aktualna razina viša od željene) te suprotno, niske privatnosti (kada je želja za privatnošću viša od aktualne razine). Četvrto, privatnost je dvosmjerna, odnosno uključuje „ulaze“ drugih ljudi (npr. šumovi) i „izlaze“ prema drugima (npr. usmena komunikacija). Peto, privatnost djeluje na individualnoj i grupnoj razini.

Za Altmana postoji više bihevioralnih mehanizama za reguliranje privatnosti (npr. teritorijalno ponašanje, kulturne norme) koji djeluju kao koherentan sustav. Posljedično, jedan mehanizam može se zamijeniti drugim (primjerice, kimanje glavom u znak odobravanja zamjenjuje riječ "da"), može ga intenzivirati (npr. viknuti "ne" i zalupiti vrata) ili može modulirati drugog (npr. ponuditi ispriku za određeno ponašanje). Štoviše, Altman postavlja hijerarhiju funkcija privatnosti, od kojih je središnja stvaranje samoidentiteta.

U Altmanovom pristupu tri su obilježja privatnosti posebno važna. Prvo, privatnost je inherentno društveni proces. Drugo, pravilno razumijevanje psiholoških aspekata privatnosti

mora uključivati međuigru ljudi, njihovog društvenog i fizičkog okruženja, kao i prirode društvenih fenomena tog vremena. Treće, privatnost ima kulturni kontekst; konkretno, ista je kulturološki univerzalna, ali su njene psihološke manifestacije kulturološki specifične [180][181].

Ove dvije neovisne, dobro podržane teorije dijele toliko toga zajedničko, sugerirajući da pružaju razumnu osnovu za razumijevanje osnove privatnosti kao psihološkog koncepta. U načelu obje teorije opisuju privatnost kao dinamički proces regulacije unutarnjih i vanjskih uvjeta s ciljem postizanja željene razine samoće ili odnosa spram drugih. A zauzvrat, postignuta privatnost može utjecati na unutarnja stanja pojedinca. Također, pokušaji reguliranja privatnosti mogu biti neuspješni: moguće je postići više ili manje privatnosti nego što osoba želi, a privatnost može imati mnoge oblike. Iako ima univerzalne karakteristike, priroda oblika koje privatnost može poprimiti je vjerojatno kulturno specifična. Nadalje, oba teoretičara razlikuju oblike (ili kako) od funkcija (ili zašto) privatnosti te se slažu da funkcije privatnosti uključuju prilike za samoevaluaciju pri čemu privatnost doprinosi samoidentitetu i individualnosti. Osnovna razlika je u tome što Altmanova teorija relativno uključuje fenomene privatnosti, naglašavaju prije svega društvenu interakciju, dok se Westinova teorija često fokusira na privatnost informacija kao podskup društvene interakcije.

3.2.1. Paradoks i ekonomija privatnosti

U svom daljnjem radu, Westin [182] opisuje različite empirijski izvedene stavove privatnosti javnosti te je postavlja okvir za analizu privatnosti informacija, gdje promatra tri okoline ispitanika – političku, društveno-kulturalnu i osobnu. Dok politička okolina opisuje političko uređenje lokacije na kojoj se pojedinci nalaze, društveno-kulturalna uzima u obzir društvo i kulturu tog mjesta, budući da ovisno o tim varijablama osobe imaju ili nemaju utjecaj na vlastitu privatnost u odnosu na druge. Osobna privatnost odnosi se pak na svakodnevni život određenog pojedinca koji se neprestano mijenja u odnosu na obiteljske okolnosti, društvenu klasu, ali i psihološko stanje.

Nadalje, kroz mnoga istraživanja od 1978 do 2004. Westin je osmislio preko 30 indeksa za mjerenje razine privatnosti koji tematski variraju, od općenitih do onih orijentiranih na specifične teme, kao što su medicina ili trgovina. Nadalje, pomoću indeksa sumirao je rezultate, prikazujući trenutne trendove oko privatnosti koje je moguće uspoređivati s vremenom.

Prilikom kreiranja indeksa, ispitanike kategorizira u tri skupine: fundamentaliste, pragmatičare i nezabrinute.

U odnosu na prikupljanje osobnih podataka od strane organizacija, fundamentalisti izražavaju najveću zabrinutost oko privatnosti, smatrajući da institucije ne bi smjele prikupljati podatke svojih korisnika, dok nezabrinutima nije važno ukoliko im se narušava privatnost jer gledaju prvenstveno na benefite koje mogu ostvariti tom „transakcijom“. Naposljetku, kao pragmatičare ističe skupinu pojedinaca koja je svjesna rizika, ali kalkulira rizike i benefite od dobivenih usluga.

No, proučavanje ponašanja pojedinaca u odnosu na privatnost intenziviralo se u posljednja dva desetljeća pojavom medija posredovanih *Web 2.0* tehnologijama[6], a kojima se granice između javne i privatne sfere preuređuju i redefiniraju, dok korisnici postaju ujedno stvaratelji sadržaja i publika, otvarajući mogućnosti razvoja novih poslovnih modela zasnovanih na ekonomiji dijeljenja [183].

Empirijski dokazi pokazuju da su pojedinci spremni trgovati svojim osobnim podacima za relativno male nagrade. Primjerice, korisnici interneta cijene svoju povijest pregledavanja za oko 7 eura, što je ekvivalent Big Mac obroka, dok, s druge strane, istraživanja stavova korisnika interneta pokazuju jaku zabrinutost korisnika za svoju privatnost te prikupljanje i korištenje njihovih osobnih podataka [184][185]. Ova dihotomija stava o privatnosti informacija i stvarnog ponašanja poznata je kao "paradoks privatnosti", izraz koji je prvi definirala Barnes [6], proučavajući razlike u korištenju društvenih mreža između odraslih osoba i tinejdžera. Nastavno, znatan broj istraživanja potvrdilo je prisutnost paradoksa privatnosti kod pojedinaca na društvenim mrežama [5][186][187][188][189].

Međutim, neke studije nisu poduprle paradoks privatnosti [190][191][192][188]. Istraživanje Krasnove i dr. [193] pokazuje kako je percipirani rizik privatnosti, konstrukt koji

[6] Za razliku od tzv. tradicionalnih medija koji podrazumijevaju prvenstveno jednosmjernu komunikaciju, novi, digitalni mediji u komunikacijski prostor uvode obilježja: (1) digitalnosti – obrađivanja podataka u digitalnom obliku; (2) multimedijalnosti – koju karakterizira snažna integracija različitih kodova i sredstava izražavanja prilikom kreiranja medijskog teksta; (3) interaktivnosti – koja obuhvaća odnos između dva subjekta ili između više subjekata komunikacije te (4) hipertekstualnosti – nelinearnog povezivanja skupova informacija [258].

usko nalikuje zabrinutosti za privatnost, značajno povezan s količinom samootkrivanja ispitanika na društvenim mrežama. Nadalje, negativna iskustvima na internetu otkrila su da čak kada su korisnici vrijeđani na internetu, isti mijenjanu samo svoje informacijsko, ali ne i društveno ili psihološko ponašanje spram privatnosti [194].

U suvremenom okruženju digitalne ekonomije paradoks privatnosti ima značajne implikacije na e-trgovinu, e-vladu, internetsko društveno umrežavanje, kao i na vladinu regulaciju privatnosti. Mjesta za e-trgovinu i internetske društvene mreže sakupljaju ogromne količine osobnih podataka. Dokaz paradoksa privatnosti potaknuo bi ih da povećaju prikupljanje i korištenje osobnih podataka te razvijaju poslovne modele iskorištavajući njihovu vrijednost. Kreatori vladine politike, s druge strane, pravdaju propise o privatnosti zabrinutošću ljudi za privatnost kao jedno od temeljnih ljudskih prava.

Pojedinci kao osobe i kao potrošači, dakle, u stalnom su stanju balansiranja između javne i privatne sfere. A odluke koje donose određuju opipljive i nematerijalne koristi i troškove, za njih i za društvo.

U kontekstu ekonomije privatnost je kompromis koji proizlaze iz zaštite ili dijeljenja osobnih podataka u odnosu na percipirane rizike. Osobine i atributi osobe (kao što su dob osobe, adresa, spol, prihod, preferencije i cijene rezervacija, ali i njezini klikovi, komentari objavljeni na internetu, fotografije postavljene na društvene medije i tako dalje) sve se više smatraju sredstvima koja se mogu koristiti za usmjeravanje usluga ili ponuda, pružanje relevantnog oglašavanja ili trgovanje s drugim stranama. U nastojanju da se iskoristi vrijednost koja je svojstvena osobnim podacima, pojavile su se nove usluge i nova tržišta koja podupiru složeni ekosustav internetskog oglašavanja [195].

Alati i proizvodi koje je omogućila povećana dostupnost osobnih podataka donijeli su koristi podjednako ispitanicima i nositeljima podataka. Unatoč tim prednostima, povećana je zabrinutost privatnosti. Ako je istina da je informacija moć, tada kontrola nad osobnim podacima može utjecati na ravnotežu ekonomske moći među stranama. Stoga je privatnost zapravo pitanje kontrole nad dijeljenjem podataka.

Za pojedince potencijalne prednosti strateškog dijeljenja određenih podataka uz zaštitu drugih podataka mogu biti i psihološke [196] i ekonomske: na primjer, personalizirane usluge i popusti koje netko dobiva nakon pridruživanja programu vjernosti trgovca ili smanjeni

troškovi pretraživanja i povećana točnost pronalaženja informacija koje netko doživljava kada ih tražilica pomnije prati. Te se koristi pretvaraju u oportunitetne troškove kada pojedinac odluči ne otkriti određene osobne podatke.

Analizirani kao ekonomska dobra, privatnost i osobne informacije otkrivaju druga, osebujna svojstva. Prvo, kada se dijele, osobni podaci mogu imati karakteristike javnog dobra, kao u slučajevima sprječavanja zaraza ili drugih potencijalnih ugroza. Pa ipak, vrijednost zaštite nekih osobnih podataka i vrijednost njihovog poznavanja gotovo u potpunosti ovise o kontekstu i ovise o suštinski neizvjesnim kombinacijama stanja u svijetu. Nadalje, osjetljivost i stavovi u vezi s privatnošću su subjektivni, jer se ono što čini osjetljive informacije razlikuje od pojedinca do pojedinca. Konkretno, pojedinci se razlikuju po tome što bi mogli doživjeti ako bi se neke privatne informacije podijelile s drugima ili učinile javnim, kao i po svojim uvjerenjima u slučaju da bi informacije mogle biti objavljene. Različite informacije bit će različite za različite ljude, a vrijednost informacija mijenja se tijekom vremena. Stoga i kompromisi vezani uz privatnost često miješaju opipljivo (popust koji ću dobiti od trgovca; povećanje premije koju ću platiti osiguravatelju), s nematerijalnim (psihološka nelagoda koju pojedinac doživljava kada se nešto vrlo osobno izloži bez njegova pristanka), te gotovo nemjerljive (učinak nadzora od strane različitih aktera i gubitak autonomije) [197].

Nadalje, otkrivanje podataka često uzrokuje poništavanje informacijske asimetrije, rezultati čega su intertemporalni vidovi trgovine [7], budući da isto često nosi neposrednu korist, bilo da je ona nematerijalna (intrinzično zadovoljstvo) ili opipljiva (npr, određeni popust na cijenu proizvoda ili usluge) [198]. No, troškovi su često neizvjesni i općenito nastaju u dalekoj vremenskoj točki, budući da voditelj obrade može prikupljati podatke o pojedincima u jednom trenutku te ih koristiti za postizanje koristi s vremenskim odmakom.

Ipak, nije uvijek očito kako pravilno vrednovati privatnost i osobne podatke u odnosu na koristi koje pojedinac ostvaruje dijeljenjem podataka te rizika koje time preuzima. Za većinu proizvoda i usluga koje ekonomisti tradicionalno proučavaju, način rješavanja ovih pitanja općenito je očigledan: tržište bilježi točnu cijenu privatnosti i osobnih podataka, odražavajući

[7] Intertemporalna funkcija trgovine ogleda se u njezinu osiguranju dostave robe na tržište u trenutku kada za njom postoji stvarna potražnja [259].

pretpostavke autonomnosti pojedinaca da donose odluke vezano uz zaštitu svoje privatnosti u određenim situacijama. Međutim, još uvijek ne postoji otvoreno, priznato tržište osobnih podataka na kojem bi isti mogli sudjelovati. Osobni podaci se kontinuirano trguju među tvrtkama (od agencija za kreditno izvješćivanje preko reklamnih tvrtki do takozvanih "infomedijara", koji kupuju, prodaju i trguju osobnim podacima), ali sami potrošači nemaju pristup tim tržištima: još uvijek ne mogu učinkovito otkupiti svoje podatke ili ponuditi svoje podatke na prodaju [199].

3.3. Pravo na privatnost u modernom društvu

No, pravo na privatnost nije moderna ideja. Povijesni korijeni privatnosti nalaze se u filozofskim raspravama iz antičkih vremena. Dok je Aristotel postavio razliku između javne sfere politike i privatne sfere obitelji, Hipokrat je kroz zakletvu liječnika na pridržavanje određenih etičkih standarda, postavio u praksu jedan element informacijske privatnosti – povjerljivost podataka. U novoj eri povjerljivost podataka prisutna je kroz sakrament ispovijedi u Katoličkoj crkvi, dok je još jedan element privatnosti – tajnost podataka – prisutan u europskim zakonskim regulativama već više od 300 godina, od pruskog Općeg zakona o pošti iz 1712. godine, a odnosi se na tajnost pisane korespondencije, odnosno pisama.

Ipak, kao jedno od determinirajućih prava modernog društva, čije se vrijednosti „ogledaju“ kroz civilizacijski ideal u vidu slobode, posebice nakon Drugog svjetskog rata, privatnost se osigurava normativnim okvirima. U suvremenom pravnom sustavu pravo na privatnost može se razmatrati s nekoliko aspekata: kao čovjekovo pravo međunarodnopravne prirode, kao temeljno ustavom zagarantirano pravo te kao osobno pravo zaštićeno instrumentima građanskoga prava [173].

Tako 1948. godine *Opća deklaracija o ljudskim pravima* Ujedinjenih naroda, u Članku 12. navodi kako „nitko ne smije biti podvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili dopisivanje, niti napadima na njegovu čast i ugled“. Nadalje, „svatko ima pravo na zakonsku zaštitu protiv takvog miješanja ili napada“ [200]. Dvije godine poslije, nacrt *Europske konvencije o ljudskim pravima* iz 1950. godine ista prava navodi u Članku 8.[8], da bi

[8] Članak 8., naslova "Pravo na poštovanje privatnog i obiteljskog života", u prvom paragrafu ističe kako "svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja" te u drugom paragrafu to pravo

i privatnost, kroz Članak 7., ali i zaštita podataka, kroz Članak 8., bili posljedično zaštićeni *Poveljom o temeljnim pravima Europske unije* [201] iz 2000. godine, kao jedinstvenim dokumentom koji okuplja temeljna prava zaštićena na teritoriju Unije. Povelja je pravno obvezujuća za sve članice postala 2009. godine.

3.3.1. Informacijska privatnost kao osnova demokracije

Privatnost je, dakle, usko povezana s pravom na informacijsko samoodređenje, odnosno pravo pojedinaca da samostalno donose odluke u vezi s otkrivanjem i korištenjem njihovih osobnih podataka koje je postavljeno i kao ustavno pravo modernih država. To je izraz ljudskog dostojanstva koji bi bio narušen ukoliko se osobe nadziru i profiliraju bez ograničenja. U tom kontekstu informacijsko samoodređenje, ili informacijska privatnost, nije samo temeljno pojedinačno pravo, već i osnovni preduvjet za funkcioniranje slobodnog demokratskog društva. Primjerice, ako nije transparentno nadgleda li se pojedinac tijekom sudjelovanja u političkim i građanskim aktivnostima, isti može odlučiti apstinirati od aktivnosti, što bi, međutim, utjecalo i na slobodni demokratski poredak koji se temelji na slobodnom djelovanju i političkoj suradnji građana koji slobodno izražavaju svoje mišljenje.

Utoliko, je političko sudjelovanje temeljno očekivanje ljudi koji žive u demokratskim političkim porecima. No, isto nije ujednačeno prakticirano u većini demokracija pa se ni političko sudjelovanje ne razumije na isti način. Očekivanja za sudjelovanje ponekad su prigrljena, ponekad tretirana skeptično, a ponekad i odbačena u cijelosti, a privatnost može imati značajnu ulogu pri stvaranju oblika demokratskog sudjelovanja [202] budući da je potrebna je velika količina privatnosti da bi se sudjelovanje odvijalo bez straha ili bilo istinski smisleno.

No, demokracija nije sadržana samo u tajnosti glasovanja. Dapače, privatnošću se štiti i intelektualna slobodu za promišljeno sudjelovanje u društvenom poretku kroz slobodu istraživanja, misli i izraza.

S druge strane, ako demokracija zahtijeva informirano građanstvo, znači da zahtijeva i transparentnost koja je u suprotnosti s privatnošću. Ako ljudi nemaju odgovarajuće informacije

obrazlaže: "javna vlast se neće miješati u ostvarivanje tog prava, osim u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprječavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih".

o političkim kandidatima ili drugim vođama, možda neće moći odabrati inteligentno. Javnost bi možda željela znati ne samo kandidate političke pozicije, ali i podatke o njihovim privatnim životima, a koji mogu biti relevantni za njihovo poštenje, iskrenost njihovih pogleda, odnosno njihovu sposobnost za određenu funkciju. U protivnome korupcija i utjecaj mogu napredovati. Stoga se transparentnost često predlaže kao korektiv za sukobe interesa u politici.

Nastavno, još jedan način na koji demokracija i privatnost mogu biti povezani odnosi se na mjeru u kojoj sama država treba biti transparentna o tome što radi. Transparentnost o vladinim poslovima može otkriti podatke o pojedincima koje vlada posjeduje, a koje oni smatraju privatnima. Stoga, zakoni o slobodi informiranja jasno definiraju iznimke za pružanje informacija, nastojeći pri tome zaštititi svoje građane, a što je vlast transparentnija, to više građana u mogućnosti je ispitati jesu li sigurnosne mjere prikladno razinama prijetnje uspostavljenog poretka.

Sam termin informacijska privatnost objedinjuje pravne vrijednosti zaštite onog aspekta privatnosti koji se odnosi na prikupljanje podataka o osobi, upravljanje tim podacima i njihovo korištenje [203]. Kako informacija predstavlja jedan od najznačajnijih resursa u gotovo svim područjima ljudske djelatnosti kao nositelj poruke u komunikacijskim procesima koji predstavljaju temelj za donošenje odluka [204], njeno prenošenje, kao i očuvanje integriteta predstavlja sve veći izazov suvremenog društva. Utoliko je bitno Razlikovanje pojma informacije i pojma (osobnog) podatka u kontekstu prava na privatnost.

3.3.1.1. Zaštita podataka i pravo na privatnost

Budući da se podatak i informacija često koriste kao sinonimi, važno je, prije svega, napraviti razliku između tih pojmova. Informacija kao nositelj određene poruke u komunikacijskom procesu i rezultat je obrade, analize i organiziranja podataka na način koji dodaje znanje primatelju. Drugim riječima, informacija pruža kontekst u kojem su podaci uzeti te nudi isti za njihovo tumačenje.

Prema Zakonu o tajnosti podataka [205] „podatak je dokument, odnosno svaki napisani, umnoženi, nacrtani, slikovni, tiskani, snimljeni, fotografirani, magnetni, optički, elektronički ili bilo koji drugi zapis podatka, saznanje, mjera, postupak, predmet, usmeno priopćenje ili informacija, koja s obzirom na svoj sadržaj ima važnost povjerljivosti i cjelovitosti za svoga vlasnika.“ Drugim riječima, podatak je beskoristan sve dok ne prenosi neku informaciju.

Nadalje, podaci o osobi, odnosno „osobni podaci“ definirani su kao svi podaci koji se odnose na pojedinca čiji se identitet može utvrditi 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“ [45].

Činjenice sadržane u osobnim podacima smatraju se nematerijalnim vrijednostima osoba, odnosno ispitanika te se povredom tih podataka ne radi o povredi podataka u doslovnom smislu, već se radi o povredi osobe, odnosno njene osobnosti. Stoga je i zaštita osobnih podataka kao temeljnih sastavnica osobe u pravnom okviru prihvaćena kao zaštita prava na privatnost. A normativni okviri s jedne strane usmjereni su smanjenju zloporabe takvih podataka postavljajući granice tzv. protupravnosti, granice koje jedna strana ne smije prijeći u ostvarivanju suprotnog interesa za očuvanjem nedodirljivosti prava na privatnost, odnosno prava na osobnost druge strane tj. pojedinca, nastojeći osigurati i poštovati pri tome spomenute slobode pojedinaca na informacijsko samoodređenje.

3.3.2. Zaštita podataka na europskom kontinentu

Informatizacijom su vlade i velike korporacije počele prikupljati i obrađivati sve više podataka o građanima pa se i potreba za regulacijom obrade osobnih podataka počela javljati u javnom prostoru 1960-ih godina na području Europe i Sjedinjenih Američkih Država. Prvi američki Zakon o privatnosti formalizirao je propise o obradi državnih podataka 1974. godine, a 1977. za sve njemačke savezne države uvedeno je zakonodavstvo o zaštiti podataka. Francuski parlament je 1978. godine odredio da se svaka organizacija ili državna agencija koja neovlašteno prima ili obrađuje osobne podatke može kazniti do šest mjeseci zatvora i maksimalnom kaznom od 20.000 franaka (3.000 eura, 4.115 američkih dolara) [206].

3.3.2.1. Konvencija Vijeća Europe 108

Prekretnica u europskoj zaštiti podataka je bila Konvencija Vijeća Europe 108 ili *Konvencija o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka* iz 1981. godine koja je postavila temelje za približavanje propisa o zaštiti podataka na teritoriju koji je tek trebao postati Europskom unijom. S pojavom informacijske tehnologije u 1960-ima, razvila se rastuća potreba za detaljnijim pravilima za zaštitu pojedinaca zaštitom njihovih (osobnih) podataka. Do sredine 1970-ih, Odbor ministara Vijeća Europe usvojio je razne rezolucije o

zaštiti osobnih podataka, pozivajući se na članak 8. *Europske konvencije o ljudskim pravima,* da bi godine 1981. Konvencija 108 bila otvorena je za potpisivanje [207].

Konvencija 108 je bila, i još uvijek ostaje, jedini pravno obvezujući međunarodni instrument u području zaštite podataka. Sve države članice Europske unije ratificirale su dokument, a 1999. godine isti je izmijenjen i dopunjen kako bi EU postala stranka u međunarodnom pravu. Nadalje, godine 2001. usvojen je i dodatni protokol uz Konvenciju, a kojim su uvedene odredbe o prekograničnom protoku podataka prema državama koje nisu stranke, nazvanim „trećim zemljama", te o obveznoj uspostavi nacionalnih nadzornih tijela za zaštitu podataka.

Konvencija 108 odnosi se na sve obrade podataka koje provode i privatni i javni sektor, kao što su obrade podataka od strane pravosuđa i tijela za provođenje zakona. Dokumentom se štiti pojedinac od zlouporaba koje mogu pratiti prikupljanje i obradu osobnih podataka, a načela utvrđena u konvenciji se posebno tiču poštenog i zakonitog prikupljanja i automatske obrade podataka, pohranjenih u određene legitimne svrhe, a ne za korištenje u svrhe koje nisu u skladu s tim svrhama, niti za čuvanje duže nego što je potrebno. Također, odredbe se tiču i kvalitete podataka, a isti moraju biti primjereni, relevantni, točni te u prikupljeni u proporcionalnosti sa svrhama obrade. Nadalje, u nedostatku odgovarajuće pravne zaštite, zabranjuje se obrada 'osjetljivih' podataka, poput rase, političkih stavova, zdravstvenog stanja, vjere, seksualnog opredjeljenja ili kriminalnog dosjea. Konvencija također jamči pravo pojedinaca da znaju koje su informacije o njima pohranjene i, ako je potrebno, da mogu tražiti njihov ispravak. Ograničenja prava utvrđenih konvencijom moguća su samo kada su u pitanju važniji interesi, poput državne sigurnosti ili obrane.

3.3.2.2. Direktiva o zaštiti podataka

Nadalje, kao glavni pravni instrument Europske unije o zaštiti podataka donesena je *Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka* (Direktiva o zaštiti podataka). Usvojena u vrijeme kada je nekoliko država članica već usvojilo nacionalne zakone o zaštiti podataka, dok je slobodno kretanje robe, kapitala, usluga i ljudi unutar unutarnjeg tržišta zahtijevalo je slobodan protok podataka, a koji se nije mogao ostvariti ukoliko se države članice nisu mogle osloniti na jedinstvenu visoku razinu zaštite podataka, cilj joj je bio

usklađivanje zakona o zaštiti podataka na nacionalnoj razini [208], pri čemu usuglašavanje ne bi trebalo rezultirati bilo kakvim smanjenjem zaštite koju postojeći zakoni pružaju, već, naprotiv, treba nastojati osigurati visoku razinu zaštite u EU. Posljedično, državama članicama dopuštena je ograničena sloboda manevriranja pri provedbi direktive.

Direktiva o zaštiti podataka osmišljena je kako bi dala sadržaj načelima prava na privatnost već sadržanim u Konvenciji 108 i proširila ih, a činjenica da su svih 15 država članica EU-a 1995. također bile ugovorne stranke Konvencije 108 isključuje usvajanje proturječnih pravila u ova dva pravna instrumenta. Direktiva o zaštiti podataka stoga se oslanja na mogućnost dodavanja instrumenata zaštite podataka, predviđenu u članku 11. Konvencije 108. Konkretno, uvođenje neovisnog nadzora kao instrumenta za poboljšanje usklađenosti s pravilima o zaštiti podataka pokazalo se važnim doprinosom učinkovitom funkcioniranju europskog prava o zaštiti podataka.

Teritorijalna primjena Direktive proteže se izvan 28 država članica EU te uključuje i države koje su dio Europskog gospodarskog prostora prema Sporazumu o Europskom gospodarskom prostoru koji je stupio na snagu s 1. siječnjem 1994. godine, a napose Island, Lihtenštajn i Norvešku. Sud Europske unije u Luksemburgu ima nadležnost utvrditi je li država članica ispunila svoje obveze prema Direktivi o zaštiti podataka te donositi preliminarne odluke u vezi s valjanošću i tumačenjem Direktive, kako bi se osigurala njezina učinkovita i jedinstvena primjena u državama članicama. Važna iznimka od primjenjivosti Direktive o zaštiti podataka je takozvana iznimka za kućanstva, odnosno obrada osobnih podataka od strane privatnih osoba samo u osobne svrhe ili u svrhe kućanstva. Takva se obrada, prema drugom stavku 3 članka, smatra dijelom sloboda privatne osobe. Nadalje, izvan područja primjene Direktive su pitanja suradnje vezana uz zaštitu privatnosti u kontekstu policijske zaštite i kaznenog pravosuđa, koje je uređeno drugim pravnim instrumentima [207].

Na temelju postojećih odredaba, a s ciljem još boljeg usuglašavanja regulatornih zahtjeva na području zaštite podataka u EU, konačno, 2016. godine dogovorena je standardizirana europska uredba o zaštiti podataka: Opća uredba o zaštiti podataka koja se počela primjenjivati od 25. svibnja 2018. u svim članicama Unije. Njome se definiraju prava građana, odnosno ispitanika, kao i dužnosti voditelja i vršitelja obrade podataka, kao entiteta odgovornih za obradu podataka. Također, definira se i uloga nacionalnih nadzornih tijela i službenika za zaštitu podataka unutar organizacija.

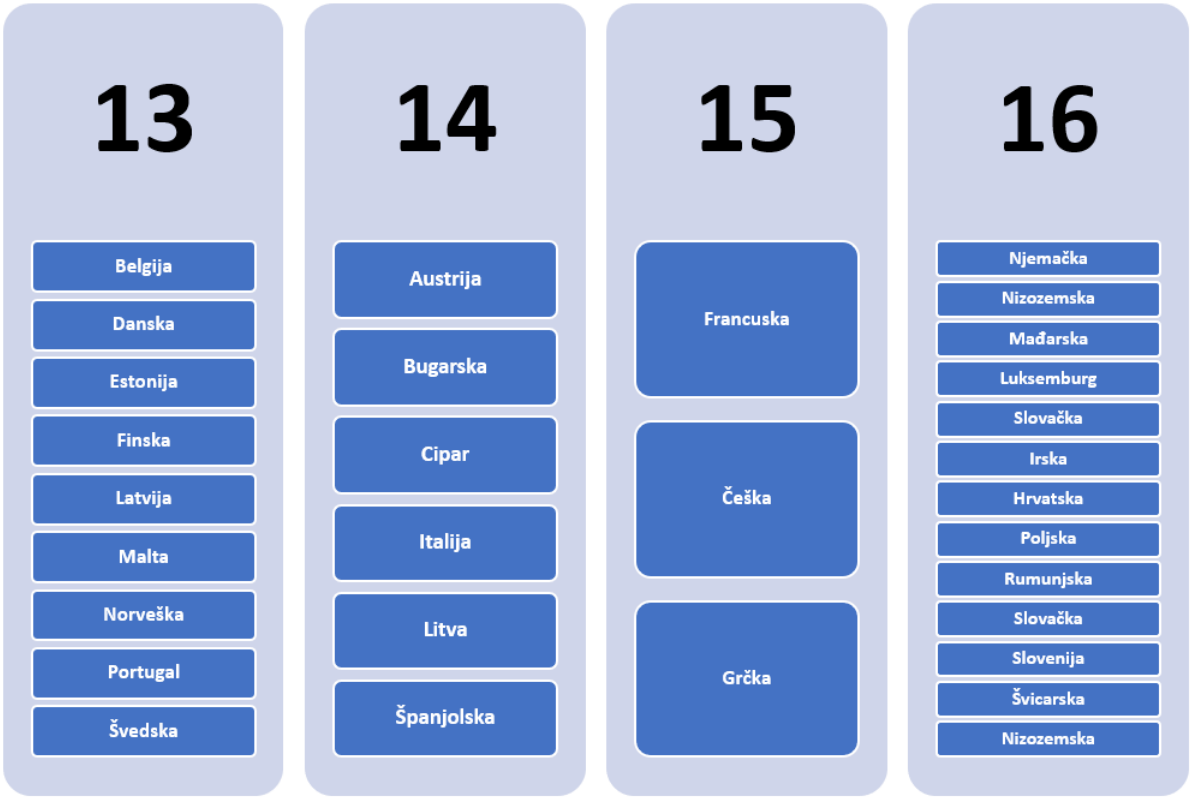
3.3.2.3. Opća uredba o zaštiti podataka

Osim usklađivanja zakona o zaštiti podataka diljem Europe, Uredba također ima za cilj modernizirati pravila o zaštiti podataka, posebno u zaštiti korisnika u globalnom gospodarstvu, budući da su odredbe primjenjive na svaku organizaciju, bez obzira na to gdje se nalazi, a koja obrađuje osobne podatke građana EU-a čime je njena primjena donijela izmjene u praksama poslovanja diljem svijeta. A kako bi se poboljšale razine usklađenosti, Uredba uvodi značajne kazne (u odnosu na prethodne okvire, a koje su bile prilično niske tako da povrede podataka namjerno ili iz nemara nisu bile neuobičajene) za organizacije koje ne ispunjavaju svoje regulatorne obveze, a koje se suočavaju se s kaznama do 4% godišnjeg globalnog prometa ili 20 milijuna eura, ovisno o tome što je veće. Time je stavljen naglasak i na važnost odgovornosti za sukladnost.

Veliki pomak u zaštiti pojedinaca su i odredbe vezane uz djecu, koja su prepoznata kao osobito ranjiva skupina jer ne mogu adekvatno raspolagati sa svojim osobnim podacima, odnosno često nisu svjesna opasnosti kojima se izlažu prilikom neopreznog disponiranja sa svojim osobnim podacima. Stoga djeca (do dobne granice od 13 do 16 godina, ovisno o državi članici, prikazano na Slici 8) mogu koristiti određene internetske usluge i servise za koje je potrebno dati osobne podatke isključivo uz roditeljski pristanak.

Još jedna bitna odredba koju Uredba uvodi u Odjeljku 4., od članka 37. do 39., je imenovanje službenika za zaštitu podataka kao osobe unutar organizacija[9] zaduženih za praćenje regulatornih zahtjeva te za osiguravanje sukladnosti s istima.

[9] Člankom 37. definirana je obaveza imenovanja službenika za zaštitu podataka od strane voditelja obrade i izvršitelj obrade ukoliko:
(a) obradu provodi tijelo javne vlasti ili javno tijelo, osim za sudove koji djeluju u okviru svoje sudske nadležnosti,
(b) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri, ili
(c) osnovne djelatnosti voditelja obrade ili izvršitelja obrade sastoje se od opsežne obrade posebnih kategorija podataka na temelju članka 9. (obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu te obrada genetskih podataka, biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca, podataka koji se odnose na zdravlje ili podataka o spolnom životu ili seksualnoj orijentaciji pojedinca) i osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima iz članka 10.



Slika 8 Dobna granica potrebne roditeljske privole za obradu podataka
Izvor: [209]; prijevod i prilagodba: autorica

Zadaće službenika za zaštitu podataka, definirane Člankom 39. Uredbe [45] uključuju:

(a) informiranje i savjetovanje voditelja obrade ili izvršitelja obrade te zaposlenika koji obavljaju obradu o njihovim obvezama iz ove Uredbe te drugim odredbama Unije ili države članice o zaštiti podataka;

(b) praćenje poštovanja ove Uredbe te drugih odredaba Unije ili države članice o zaštiti podataka i politika voditelja obrade ili izvršitelja obrade u odnosu na zaštitu osobnih podataka, uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;

(c) pružanje savjeta, kada je to zatraženo, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja u skladu s člankom 35.;

(d) suradnja s nadzornim tijelom;

(e) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje iz članka 36. te savjetovanje, prema potrebi, o svim drugim pitanjima.

Nadalje, istim je člankom definirana zadaća službenika vezana uz vođenje „računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade“ [45], a odredbe vezane uz obvezu provođenja procjene učinka na zaštitu podataka definirane su Odjeljkom 3. te konkretno Člankom 35.

Budući da je koncept službenika za zaštitu podataka nov na području izgradnje sustava zaštite privatnosti te nema formalnog obrazovanja za predloženu funkciju, Uredba nudi određene smjernice za odabir odgovarajuće osobe, kao i opis radnog mjesta iste [10]. Tako se „službenik za zaštitu podataka imenuje se na temelju stručnih kvalifikacija, a osobito stručnog znanja o pravu i praksama u području zaštite podataka te sposobnosti izvršavanja zadaća iz članka 39“ te „može biti član osoblja voditelja obrade ili izvršitelja obrade ili obavljati zadaće na temelju ugovora o djelu“. Nadalje, bitna odrednica pri osiguravanju funkcije je osiguranje neovisnosti u radu službenika. Stavkom 3. Članka 38. Uredbe „voditelj obrade i izvršitelj obrade osiguravaju da službenik za zaštitu podataka ne prima nikakve upute u pogledu izvršenja tih zadaća“, stoga ne smije biti razriješen dužnosti ili kažnjen zbog izvršavanja istih.

Također, službenik za zaštitu podataka obvezan je tajnošću ili povjerljivošću u vezi s obavljanjem svojih zadaća, u skladu sa Stavkom 5. istog članka.

I u kontekstu suvremenih tehnologija Uredba je napravila odmak u odnosu na Direktivu pa ograničava "profiliranje" i daje ispitanicima značajna prava da izbjegnu odluke temeljene na profiliranju te, također, omogućava ispitanicima pravo ne podlijeganja odlukama koje se temelje isključivo na automatiziranoj obradi, koja proizvodi pravne učinke koji se tiču njih ili odlukama koje značajno utječu na njih.

Naposljetku, važan aspekt osiguravanja privatnosti za ispitanike je i obveza informiranja o povredama osobnih podataka od strane voditelja obrade podataka. Ako se povreda osobnih podataka ne rješava na odgovarajući način i pravodobno, ona može prouzročiti fizičku,

[10] Detaljne smjernice objavila je Radna skupina za zaštitu podataka iz članka 29. [260]

materijalnu ili nematerijalnu štetu pojedincima, kao što su gubitak nadzora nad osobnim podacima ili ograničavanje njihovih prava, diskriminacija, krađa identiteta ili prijevara, financijski gubici, neovlašteni obrnuti postupak pseudonimizacije, šteta za ugled, gubitak povjerljivosti osobnih podataka zaštićenih poslovnom tajnom ili bilo koju drugu ekonomsku ili društvenu štetu za dotičnog pojedinca. Tako čim voditelj obrade primijeti da je došlo do povrede osobnih podataka, trebao bi o tome izvijestiti nadležno nadzorno tijelo bez nepotrebnog odgađanja i to, ako je izvedivo, najkasnije 72sata nakon saznanja o toj povredi osobnih podataka, osim ako voditelj obrade može dokazati, u skladu s načelom odgovornosti, da povreda osobnih podataka vjerojatno neće prouzročiti rizik za prava i slobode pojedinaca.

3.3.2.4. Direktiva o privatnosti i elektroničkim komunikacijama

Kako bi odgovorila na zahtjeve novih digitalnih tehnologija i olakšala napredak elektroničkih komunikacijskih usluga Europska unija 12. srpnja 2002. godine donosi *Direktivu 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija* ili skraćeno *Direktivu o privatnosti i elektroničkim komunikacijama*. Direktiva nadopunjuje Direktivu *95/46/EZ* o zaštiti podataka i primjenjuje se na sva pitanja koja nisu izričito obuhvaćena tom Direktivom [210]. Konkretno, predmet Direktive poznate i pod nazivom e-Privacy je pravo na privatnost u sektoru elektroničkih komunikacija[11] te slobodno kretanje podataka, komunikacijske opreme i usluga. Prva opća obveza u Direktivi je zajamčiti sigurnost elektroničkih komunikacijskih usluga od strane njihovih pružatelja prema ispitanicima.

Odredbe Direktive tako uključuju dužnost obavještavanja pretplatnika usluga kada god postoji određeni rizik vezano uz informatičku sigurnost, kao što je virus ili drugi zlonamjerni napad te održavanje povjerljivosti informacija. Nadalje, Direktiva obvezuje pružatelje usluga da izbrišu ili anonimiziraju obrađene podatke o prometu kada više nisu potrebni, osim ako su ispunjeni uvjeti iz Članka 15 kojim se omogućavaju iznimke na prava i obveze unutar Direktive unutar zakonskih okvira pojedinih država ukoliko ograničenja predstavljaju „nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s ciljem zaštite nacionalne sigurnosti (odnosno

[11] Pojam "e-privatnost" sve se češće javlja uslijed sve češćeg udruživanja problematike informacijske sigurnosti i zaštite osobnih podataka u okruženju suvremenih ekonomskih okvira. Pojam se odnosi na koncept zaštite podataka vezan uz komunikaciju putem elektroničkih mreža u bilo kojem obliku, a problematika e-privatnosti najčešće se veže uz elektroničku poštu i zaštitu osobnih podataka koji se prikupljaju putem mrežnih stranica [173].

državne sigurnosti), obrane, javne sigurnosti te s ciljem sprečavanja, istrage, otkrivanja i progona kaznenih djela odnosno neovlaštene uporabe elektroničkog komunikacijskog sustava“. Tako je zadržavanje podataka dopušteno za potrebe naplate, ali samo dok ne nastupi zakonska zastara. Podaci se još mogu zadržati samo uz korisnikov pristanak za marketinške usluge i usluge s dodanom vrijednošću, a ispitanici moraju biti obaviješteni zašto i koliko dugo se podaci obrađuju. Isto tako, korisnici moraju moći isključiti identifikaciju pozivne linije, a kada se podaci koji se odnose na lokaciju korisnika ili drugi promet mogu obrađivati, Člankom 9 propisuje da će to biti dopušteno samo ako su ti podaci anonimizirani, ako su korisnici dali privolu ili za pružanje usluga s dodanom vrijednošću. Kao i u prethodnom slučaju, korisnici moraju biti unaprijed obaviješteni o karakteru prikupljenih informacija i imati mogućnost isključivanja iz obrade podataka.

Člankom 13, nadalje, zabranjuje se korištenje adresa elektroničke pošte u marketinške svrhe te Direktiva uspostavlja režim privole, gdje se neželjena elektronička pošta može slati samo uz prethodni pristanak primatelja. Također, slanje neželjenih tekstualnih poruka, bilo u obliku SMS (eng. Short Message Service) poruka, odnosno kratkih tekstualnih poruka unutar standarda mobilne telefonije te tzv. *push,* trenutnih poruka iz aplikacija ili bilo kojeg sličnog formata dizajniranog za potrošačke prijenosne uređaje (mobilni telefoni, dlanovnici) također potpada pod zabranu.

Ipak, dvije kategorije elektroničke pošte (ili komunikacije općenito) su isključene iz opsega zabrane. Prva je iznimka za postojeće odnose s kupcima, a druga za marketing sličnih proizvoda i usluga.

Odredba Direktive primjenjiva na kolačiće je Članak 5, stavak 3. Iako se kroz uvodnu izjavu 25 Preambule prepoznaje važnost i korisnost kolačića za funkcioniranje modernog interneta, ali prethodna izjava također upozorava na opasnost koju takvi instrumenti mogu predstavljati za privatnost. Tako zakonske odredbe ne trebaju utjecati na sve vrste kolačića, već treba izuzeti one koji se smatraju "strogo nužnima kako bi se pružila neka usluga informacijskog društva koju je pretplatnik ili korisnik izričito zatražio“ [211], kao što su na primjer kolačići koji prate sadržaj korisničke košarice za kupnju na internetskoj usluzi kupnje.

Iako je Članak 5 tehnološki „neutralan“, odnosno ne spominje nikakva specifična tehnološka sredstva koja se mogu koristiti za pohranjivanje podataka, odnosi se na sve

informacije za koje mrežno mjesto uzrokuje pohranjivanje u pregledniku korisnika, što odražava želju zakonodavca Europske unije da režim direktive ostavi otvorenim za budući tehnološki razvoj.

Adresati obveze su države članice koje moraju osigurati da je korištenje elektroničkih komunikacijskih mreža za pohranu informacija u pregledniku posjetitelja dopušteno samo ako se korisniku pruže „jasne i sveobuhvatne informacije“ o svrhama pohrane ili opcijama pristupa tim informacijama te dao je svoj pristanak, u skladu s Direktivom 95/46/EZ o zaštiti podataka. Tako postavljeni, opcijski režim znači da pojedinac mora dati svoj pristanak prije nego što se kolačići ili bilo koji drugi oblik podataka pohrani u njegov preglednik, što zahtjeva osiguravanje raznih mehanizama transparentnosti.

Dana 10. siječnja 2017. Europska komisija objavila je Prijedlog Uredbe o e-privatnosti koja se odnosi na pravila o privatnosti za sektor elektroničkih komunikacija. Uredba bi nakon donošenja trebala zamijeniti predmetnu o elektroničkoj privatnosti. Zamišljena u provedbi kao *lex specialis* Opće uredbe o zaštiti podataka s ciljem nadjačavanja i nadopunjavanja iste s specifičnijim pravilima za elektroničke komunikacije, Uredba još nije stupila na snagu radi nesuglasica između Vijeća Europske unije i Parlamenta Europske unije oko niza značajnih pitanja.

Prema nacrtu koji je „procurio“ 4. studenog 2021. godine[212] Vijeće i Parlament dogovorili su brojne izmjene i dopune sljedeća tri poglavlja nacrta:

1) Poglavlje III (Prava krajnjih korisnika na kontrolu elektroničkih komunikacija) – očekuje se da će ovo poglavlje regulirati:
   (i) prikaz poziva i identifikacije povezane linije (npr. identificira li zaslon uređaja broj dolaznog poziva);
   (ii) blokiranje neželjenih zlonamjernih ili neugodnih poziva;
   (iii) uključivanje informacija, uključujući osobne podatke, u javno dostupne imenike; i
   (iv) neželjene izravne marketinške komunikacije (npr. neželjena e-pošta i SMS tekstovi).
2) Poglavlje V. (Pravni lijekovi, odgovornost i kazne) – očekuje se da ovo poglavlje regulira:

(i) pravne lijekove;
(ii) pravo na naknadu i odgovornost;
(iii) opće uvjete za izricanje upravnih novčanih kazni; i
(iv) kazne.

3) Poglavlje VI. (Završne odredbe) – očekuje se da ovo poglavlje regulira stupanje na snagu nacrta Uredbe i naknadno praćenje njezine provedbe od strane Europske komisije.

Međutim, Vijeće i Parlament još uvijek se ne slažu oko niza značajnih pitanja. Na primjer, Vijeće i Parlament još se nisu složili oko definicije "neželjenih poziva". Također se ne slažu oko opsega zabrane slanja izravnih marketinških komunikacija bez pristanka primatelja; Vijeće ovu zabranu namjerava primijeniti samo na komunikacije poslane “fizičkim osobama”, dok parlamentarci žele da se zabrana odnosi na slanje komunikacija i pravnim osobama. Parlament, nadalje, nastoji proširiti tradicionalnu definiciju izravnog marketinga (koja uključuje automatizirane telefonske aparate, telefaks aparate i elektroničku poštu, uključujući SMS poruke) na razne druge vrste reklama, kao što su "skočni prozori ili reklame slične elektroničkoj pošti" (npr. *push* obavijesti), nešto što Vijeće trenutno ne odobrava.

Iako predložena Uredba o e-privatnosti uvodi jedinstvena pravila za poboljšanje zaštite privatnosti u sektoru elektroničkih komunikacija diljem Europe, ona također uključuje odredbe koje se mogu kritički promatrati iz perspektive privatnosti. Radna skupina za zaštitu podataka iz članka 29. posebno je kritizirala određene predložene odredbe kao područja koja izazivaju veliku zabrinutost. Prije svega, Prijedlog Uredbe dopušta prikupljanje podataka koje emitiraju uređaji korisnika, kao što su MAC (eng. Media Access Control) adrese kao jedinstvenog identifikatora koji se dodjeljuje kao mrežna adresa u komunikacijama unutar mrežnog segmenta, bez prethodnog pristanka korisnika, pod uvjetom da je korisnik dobio jasnu i istaknutu obavijest koja objašnjava mjere koje pojedinci mogu poduzeti kako bi smanjili ili zaustavili prikupljanje podataka. Radna skupina zahtijeva da ove odredbe, a koje omogućuju praćenje putem Wi-Fi mreža ili "Bluetooth-praćenje" budu u skladu s Općom uredbom o zaštiti podataka i stoga trebaju zahtijevati pristanak. U Mišljenju se također preporučuje donošenje tehničkog standarda za mobilne uređaje koji će automatski signalizirati prigovor protiv praćenja i omogućiti pojedincima da povuku prethodno dani pristanak.

Nadalje, članak 6. predložene Uredbe predviđa različite razine zaštite metapodataka i sadržaja poruka. Radna skupina kaže da se Prijedlogom ne podržava ova razlika jer su obje kategorije podataka vrlo osjetljive i treba im se dodijeliti jednako visoka razina zaštite. Polazište bi stoga trebalo biti da je općenito zabranjeno obrađivati metapodatke, kao i sadržaj poruka, za analitiku, profiliranje i profiliranje ponašanja bez pristanka svih krajnjih korisnika (što znači i pošiljatelja i primatelja).

Treće, Radna skupina također poziva na zaštitu od takozvanih "zidova za praćenje", što je praksa pri kojoj se uskraćuje pristup mrežnoj stranici ili usluzi osim ako pojedinci ne pristanu da budu praćeni na drugim mrežnim stranicama ili uslugama. Budući da praćenje može ozbiljno zadirati u privatnost pojedinca, Radna skupina zahtijeva izričitu zabranu takve prakse kao "uzmi ili ostavi izbora" koji prisiljava korisnike da pristanu na praćenje u zamjenu za pristup usluzi.

Na kraju, ali ne manje važno, skupina preporučuje da terminal i softver prema zadanim postavkama moraju nuditi proaktivne postavke privatnosti i moraju ponuditi jasne opcije za potvrdu ili promjenu tih postavki tijekom instalacije i upotrebe. Postavke privatnosti ne bi trebale biti ograničene na kolačiće, već bi korisnicima posebno trebalo omogućiti da signaliziraju određeni pristanak putem postavki preglednika.

3.3.2.5. Prekogranični prijenos podataka

Izvan granica Europske unije primjenjuju se različiti zakoni o privatnosti ili režimi zaštite podataka. Neke zemlje mogu imati vrlo malo ili nimalo propisa što dovodi do zabrinutosti zakonodavstva Unije za prekogranični prijenos osobnih podataka, koji je dopušten samo organizacijama i zemljama koje se smatraju ekvivalentnima postavljenim standardima Uredbe.

Ipak, većina propisa o zaštiti podataka slijedi osnovne principe privatnosti koje je definirala Organizacija za gospodarsku suradnju i razvoj prvotno u originalnim, a zatim i revidiranim *Smjernicama o zaštiti privatnosti i prekograničnom tijeku osobnih podataka* [127] [128].

EU Direktiva o zaštiti podataka ograničila je u svom Članku 25 prijenos osobnih podataka u treće zemlje bez odgovarajuće razine zaštite podataka.

Budući da nema odgovarajuću razinu zaštite podataka jer nedostaju opći zakoni o zaštiti podataka koji pokrivaju cijeli privatni sektor, kao i institucija povjerenika za zaštitu podataka te nadzorna tijela koja bi pratila usklađenost i postupala po pritužbama pojedinaca, Sjedinjene Američke Države nemaju odgovarajuću razinu zaštite podataka.

Kako bi se spriječilo da prijenos podataka od strane američkih tvrtki bude prekinut od strane EU, Europska komisija je 2000. godine prihvaća Međunarodna načela privatnosti „sigurne luke“ [213], koja su bila vezana uz samoregulirajuću privatnost organizacija, a razvilo ih je Ministarstvo trgovine Sjedinjenih Američkih Država. Međutim, nakon što je Max Schrems, austrijski aktivist za privatnost, poduzeo pravni postupak protiv sporazuma i požalio se da su njegovi podaci na Facebook društvenoj mreži nedovoljno zaštićeni, posebno u kontekstu otkrića Edwarda Snowdena[12], a kao rezultat toga, Europski sud pravde objavio je u listopadu 2015. da je Odluka o „sigurnoj luci“ nevažeća.

Nadalje, Europska komisija i Sjedinjene Američke Države složile su 2. veljače 2016. se uspostaviti novi okvir za transatlantske protoke podataka, poznat kao "EU-US Štit privatnosti“, koji su kritizirali europski povjerenici za zaštitu podataka, a koji je u srpnju 2020. godine Europski sud pravde ukinuo takozvanom *Schrems II* presudom. Dana 4. lipnja 2021. Europska komisija donijela je dva skupa standardnih ugovornih klauzula za zamjenu stare sheme prijenosa, čime se omogućuje lakši prijenos osobnih podataka između zemalja Europske unije i zemalja bez odluke o primjerenosti.

Napuštanjem Europske unije 1. siječnja 2021. Ujedinjeno Kraljevstvo postalo je "treća zemlja“ tj. zemlja izvan EU-a bez odluke o adekvatnosti za prijenos podataka. Dana 28. lipnja 2021. Europska unija je donijela odluku o primjerenosti za Ujedinjeno Kraljevstvo, kojom se osigurava slobodan protok osobnih podataka između dva teritorijalna bloka u razdoblju od četiri godine (do lipnja 2025.). Za britanske mrežne stranice, tvrtke i organizacije koje obrađuju osobne podatke pojedinaca unutar Unije ta odluka o primjerenosti znači neograničeno poslovanje, kao i prije tzv. Brexita, sljedeće četiri godine, a nakon lipnja 2025. EU će se morati

[12] Edward Snowden je bivši američki konzultant za računalnu inteligenciju koji je 2013. odao visoko povjerljive podatke iz Agencije za nacionalnu sigurnost Sjedinjenih Američkih Država, dok je bio njezin zaposlenik i podizvođač. Njegova otkrića otkrila su brojne globalne programe nadzora od strane državnih agencija uz suradnju telekomunikacijskih kompanija i europskih vlada, te potaknula kulturnu raspravu o nacionalnoj sigurnosti i privatnosti pojedinca.

uključiti u novi postupak o primjerenosti kako bi se utvrdilo osigurava li Ujedinjeno Kraljevstvo još uvijek jednaku razinu zaštite podataka kako bi se odluka o primjerenosti obnovila.

3.3.3. Legitimnost privole

Zaštita informacijskog aspekta privatnosti vezana je uz koncept privole kao legitimne osnove za obradu osobnih podataka pojedinca od strane drugih osoba. To je oblik autonomne autorizacije kojim pojedinac (ispitanik) ovlašćuje voditelja obrade podataka da obrađuje njegove osobne podatke. S druge strane, radi se o transformativnom aktu kojim pristanak uspostavlja u zaštiti podataka stanje u kojem ono što bi se inače smatralo kršenjem prava na (informativnu) privatnost pojedinca više ne doživljava kao takvo [214].

Sam koncept privole na kojem počiva razmjena podataka i zaštita prava ispitanika, definiran je kroz pet načela *Praksi poštenog informiranja* [126] – obavijest/svijest, izbor/pristanak, pristup/sudjelovanje, integritet/sigurnost i provedba/pravna zaštita.

Solove [215], iako hvali koncept i nužnost privole kao regulatornog režima, ističe da takav pristup zaštiti informacijske privatnosti ne pruža pojedincima značajnu kontrolu nad njihovim podacima, pri čemu ukazuje na brojne strukturne probleme prilikom njegove realizacije. Prije svega, ukazuje na kognitivne probleme koji potkopavaju sposobnost pojedinaca za donošenje informiranih, racionalnih odluka o troškovima i koristima pri „samoupravljanju“ privatnošću. Ističe kako čak i dobro informirani i racionalni pojedinci ne mogu na odgovarajući način upravljati svojom privatnošću jer je previše dionika koji prikupljaju i koriste osobne podatke te se privole odnose na niz izoliranih transakcija. A bez razumijevanja potencijalnih daljnjih upotreba podataka, odnosno kumulativne i cjelovite procjene potencijalne štete na privatnost, nije moguće donijeti smislene odluke. U svome članku *Taksonomija privatnosti* [112] autor grupira aktivnosti kršenja privatnosti u četiri skupine: prikupljanje podataka, obrada informacija, širenje informacija te invazije. Nadalje, aktivnosti prikupljanja podataka dijeli u dvije skupine: nadzor i ispitivanje. Nadzor se odnosi na promatranje i prikupljanje bez privole ispitanika, dok se ispitivanje odnosi na prikupljanje podataka kao rezultata traženja podataka od ispitanika pod nekom vrstom prisile.

Obrada informacija je aktivnost koja koristi ili prikuplja osobne podatke te ih veže za identificiranu osobu ili druge identificirane podatke. Sekundarna uporaba podataka, izvan prvotne svrhe prikupljanja, a za koju ispitanik nije dao privolu, dovodi do kršenja privatnosti,

baš kao i širenje podataka, odnosno otkrivanje osobnih podataka drugim stranama, a za koje nije dobivena privola od ispitanika. Invazije, nepozvani upadi u zbirke podataka, posljednja su skupina ugroza privatnosti, a odnose se na proboje podataka od strane hakera i/ili neovlaštenih osoba kao posljedica smanjene razine sigurnosti podataka.

Opća uredba o zaštitu podataka definira jasne odredbe privole. Privola bi se trebala davati jasnom potvrdnom radnjom, kojom se izražava dobrovoljan, poseban, informiran i nedvosmislen pristanak ispitanika na obradu osobnih podataka koji se odnose na njega, poput pisane izjave, uključujući elektroničku, ili usmene izjave. To znači da je za valjanu suglasnost potrebno ispuniti nekoliko uvjeta. Da je privola dana dobrovoljno znači da nema neravnoteže u moći između stana, odnosno, nema negativnih posljedica ako pristanak nije dan. Poseban pristanak, nadalje, podrazumijeva izdvojeni pristanak za jednu ili više specifičnih svrha, odnosno da nositelj podataka mora imati zaseban izbor u odnosu na svaku od navedenih svrha. Uvjet informiranosti podrazumijeva transparentnost u odnosu na određene elemente informacija koje su ključne za donošenje izbora o davanju pristanka, uključujući identitet voditelja obrade, svrhe obrade podataka, vrsta podataka, pravo na povlačenje privole te bilo kakvo korištenje za odluke koje se temelje isključivo na automatiziranoj obradi, kao i rizike prijenosa podataka u treće zemlje. Potvrdna radnja, koja je također potrebna za privolu, zahtijeva da je pojedinac poduzeo namjernu radnju za pristanak. Nemogućnost izbora kao i unaprijed označeni okviri, stoga ne bi trebali predstavljati pristanak.

Nadalje, voditelj obrade mora čuvati dokaze da je ispitanik dao privolu, što znači Uredba stavlja teret dokazivanja na voditelja obrade što je još jedan element organizacije tokova podataka pri dizajniranju arhitekture privatnosti. Upravljanje privolama zahtjeva mogućnosti praćenja izbora pojedinaca s obzirom na opcije, ali vrijeme trajanja pristanka (budući da se isti ima pravo odbiti obradu podataka na određeno vrijeme). Stoga povlačenje privole bi trebalo biti jednostavno kao i davanje pristanka.

3.3.4. Načela obrade (osobnih) podataka

Prije svega, obrada podataka mora biti zakonita te pravna osnova treba biti definirana za svaku obradu podataka. Nadalje, minimizacija podataka, odnosno načelo prikupljanja samo nužnih podataka je ključno pri zaštiti privatnosti i smanjenju rizika ugroze iste, a prema načelu proporcionalnosti, podaci koji se prikupljaju i obrađuju trebaju biti primjereni i relevantni.

Štoviše, ako više nisu potrebni za svrhe zbog kojih su prikupljeni, podatke treba brisati ili izvršiti anonimizaciju ili pseudonimizaciju, što znači da bi i vrijeme zadržavanja podataka trebalo svesti na minimum.

Sljedeće važno načelo privatnosti je načelo specifikacije svrhe i obvezivanja na istu, što znači da se osobni podaci trebaju prikupljati i kasnije koristiti u samo određene svrhe. Ovo je načelo važno jer na osjetljivost osobnih podataka uglavnom utječe njihova svrha i kontekst upotrebe. Iako postoje osobni podaci koji sami po sebi već sadrže osjetljive podatke (npr. medicinski podaci), ovisno o svrsi i kontekstu upotrebe, takvi osjetljivi podaci mogu postati još osjetljiviji, a podaci koji se čine neosjetljivima (npr. adrese) mogu postati i vrlo osjetljivi s obzirom na namjenu. Stoga, ako se osobni podaci žele prikupljati ili obrađivati, svrha obrade podataka mora biti jasno navedena, a naknadna uporaba treba biti ograničena na ispunjavanje tih svrha.

Stoga je i načelo transparentnosti obrade podataka preduvjet za informacijsko samoodređenje i za poštenu obradu podataka. Društvo u kojem pojedinci više ne bi mogli znati tko, koje i kada te u kojim situacijama prikuplja i obrađuje njihove podatke, bilo bi u suprotnosti s pravom informacijskog samoodređenja. Stoga, subjekti podataka, odnosno ispitanici, trebaju imati opsežne informacije i pravo pristupa podacima te mogućnost „intervencije“ u obradu svojih osobnih podataka, kada je to neopravdano, kao i pravo prigovoriti obradi ili tražiti brisanje ili ispravljanje svojih podataka. Nadalje, načelo odgovarajuće sigurnosti podataka postavlja zahtjeve da se osobni podaci trebaju obrađivati na način koji osigurava odgovarajuću sigurnost osobnih podataka, a koja je usmjerena na očuvanje povjerljivosti, cjelovitosti i dostupnosti podataka. Konačno, princip odgovornosti zahtijeva da voditelj obrade podataka treba biti odgovoran za poštivanje mjera za provedbu ovih osnovnih, navedenih principa privatnosti. Neovisni povjerenici ili službenici za zaštitu podataka stoga postoje radi praćenja poštivanja načela i postupanja po pritužbama ispitanika u organizacijama.

3.4. Privatnost i tehnologija

Da bi se, dakle, osigurala privatnost korisnika kao mogućnosti samoodređivanja pojedinaca, temeljnog preduvjeta demokratskog poretka, potrebno je implementirati načela privatnosti u sustav organizacija, odnosno osigurati mehanizme za konzumiranje stečenih prava na transparentnost i intervenabilnost od strane pojedinaca. Oba zahtjeva u suvremenom

kontekstu informacijskih i organizacijskih sustava podupirana su tzv. tehnologijama za povećanje privatnosti (eng. privacy-enhancing technology, PET).

Kao istraživačku temu tehnologijama za povećanje privatnosti pokrenuo je David Chaum 1981. godine radom koji opisuje metodu anonimne i nevidljive dostave elektroničkih poruka pod nazivom "Mix" [216]. Autor koristi sigurnosne protokole i naknadne slojeve enkripcije kako bi osigurao zaštitu privatnosti „miješanjem" prometa e-pošte nekoliko ljudi u šifriranom obliku. Koncept je kasnije implementiran u MixMaster sustav anonimizacije e-pošte koji je prvi praktično dostupan PET sustav.

Sama pojava tehnoloških mjera za zaštitu privatnosti poklapa se s jačanjem zakonske regulative vezane uz korištenje osobnih podataka u informacijskim sustavima da bi se uslijed sve većeg usvajanja interneta i mobilne telefonije u društvu tijekom 1990-ih povećali istraživački napori na području, a Chaumov koncept se prilagođava novonastalim okruženjima, odnosno medijima [217][218][219]. Početkom novog tisućljeća, javljaju se i javno financirani istraživački projekti na području [220][221][222], istraživači su istraživali kriptografiju i tehnologiju skrivanja informacija kako bi proizveli protokole koji podržavaju privatnost kao što su anonimne vjerodajnice [223], a tvrtke počinju razvijati poslovne modele vezano uz zaštitu privatnosti. Prekretnica u razvoju i shvaćanju PET tehnologija je pojava *Priručnika o tehnologijama za poboljšanje privatnosti* [224] koji su napisali predstavnici regulatornih tijela, kao „uvertira" za donošenje regulatornih okvira koji su danas na snazi, a koji učvršćuju potrebu za primjenom istih.

3.4.1. Tehnologije i alati za povećanje privatnosti

Tehnologijama za povećanje privatnosti Fritsch [225] dijeli na alate transparentnosti i alate (ne)prozirnosti kao što je prikazano Tablicom 2.

Alati za transparentnost namijenjeni su stvaranju uvida u obrade podataka, a njihov je učinak bolje razumijevanje postupaka, praksi i posljedica obrade osobnih podataka, dok alati za neprozirnost namijenjeni su skrivanju identiteta korisnika ili njegove veze s osobnim podacima, najčešće kroz tehnike šifriranja, razdvajanja podataka, anonimizacije i pseudonimizacije te ograničavanja pristupa i/ili korištenja.

Tablica 2 Primjeri alata za transparentnost i neprozirnost

	Alati transparentnosti	Alati (ne)prozirnosti
Definicija	Alati koji osobi jasno pokazuju koji se osobni podaci obrađuju, kako se obrađuju i tko ih obrađuje.	Alati koji skrivaju identitet osobe ili njezin odnos s podacima dok ih netko drugi obrađuje.
Ne-tehnički primjeri	• zakonska prava na informiranje o obradi podataka; • revizije privatnosti.	• pseudonimni pristup internetskim uslugama; • tajnost glasovanja.
Tehnički primjeri	• sučelja za reviziju baza podataka; • agenti za provedbu revizije; • datoteke zapisnika (eng. log files).	• anonimna e-pošta u sustavu MixMaster; • preglednici s tehnologijama slojevite enkripcije za anonimizirano mrežno pregledavanje poput The Onion Router ili TOR platforme**;** • pseudonimizacija.

Izvor: [225] str. 10-11; prijevod: autorica

Tehnologije i alati za povećanje privatnosti raspoređeni su u širi kontekst informacijskih sustava, koji zauzvrat upravljaju zahtjevima korisnika, s jedne, i poslovnog sustava, s druge strane, odnosno njima se implementira koherentan sustav mjera informacijsko-komunikacijskih tehnologija koji štiti privatnost uklanjanjem ili smanjenjem osobnih podataka ili sprječavanjem nepotrebne i/ili neželjene obrade osobnih podataka, a bez gubitka funkcionalnosti informacijskog sustava [226].

3.4.1.1. Zahtjevi i alati transparentnosti

Alati transparentnosti, odnosno tehnologije za povećanje transparentnosti (eng. transparency-enhancing technology, TET) u tom kontekstu, predstavljaju kombinaciju tehnoloških rješenja i pravnih ili proceduralnih okvira [227], koji imaju za cilj smanjenje postojeće visoke informacijske asimetrije između ispitanika i vršitelja te voditelja obrade podataka, a koja može posljedično imati štetne utjecaje na privatnost ispitanika [18]. Hansen [228] ih, stoga, definira kao „alate koji mogu pojedincu pružiti jasnu vidljivost aspekata bitnih za njegove (osobne) podatke i privatnost“, dok ih Hedbom [229] postavlja kao tehnološke alate koji imaju jednu ili više sljedećih karakteristika:

• daju informacije o namjeravanom prikupljanju, pohrani i/ili obradi podataka ispitaniku ili opunomoćeniku koji djeluje u njegovo ime s ciljem poboljšanja privatnosti;

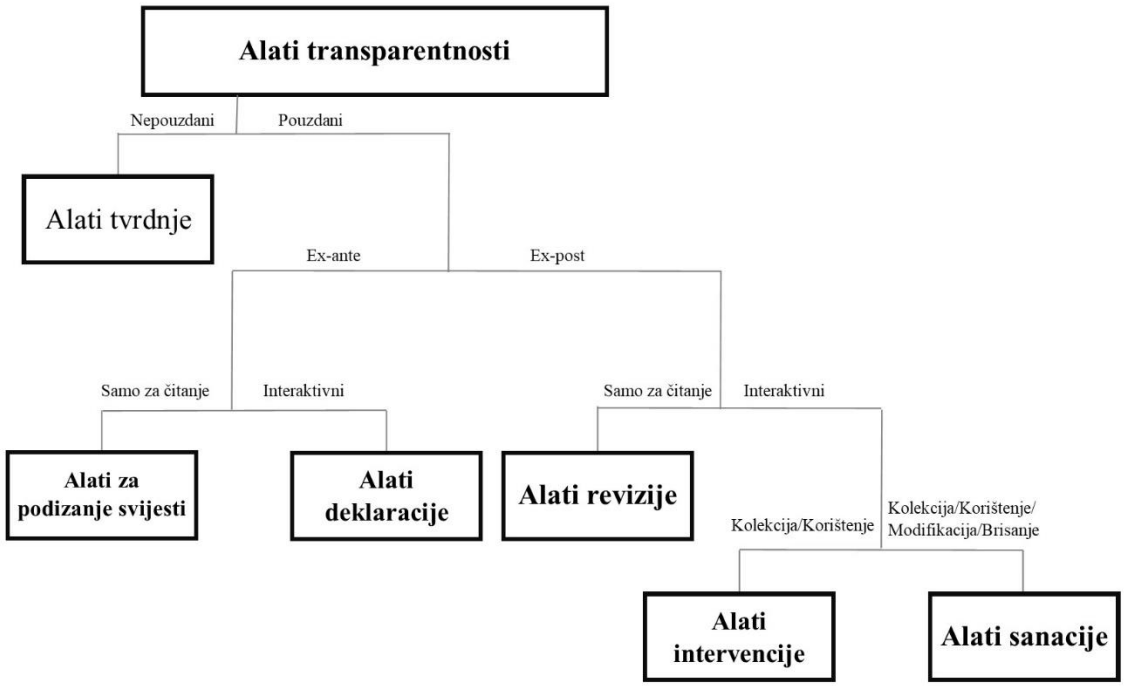
• pružaju ispitaniku ili opunomoćeniku koji djeluje u njegovo ime pristup pohranjenim podacima i/ili logici obrade podataka s ciljem poboljšanja privatnosti;

• pružaju ispitaniku ili opunomoćeniku koji djeluje u njegovo ime mogućnost kontra-profiliranja kako bi "pogodio" kako se njegovi podaci podudaraju s relevantnim grupnim profilima koji mogu utjecati na rizike i mogućnosti, implicirajući da vidljivo i strojno čitljivo ponašanje okoline pojedinca pruža dovoljno podataka za predviđanje implikacija njegova ponašanja.

Alati ili tehnologije transparentnosti dijele se u odnosu na njihovu pouzdanost u prenošenju informacija, odnosno smanjenja informacijske asimetrije [230]. Pouzdani, odnosno alati koji zapravo informiraju o obradi podataka, dijele se na *ex-ante* alate, koji pružaju potrebne informacije ispitaniku prije prikupljanja i obrade podataka, *ex-post* alate, koji pružaju potrebne informacije ispitaniku nakon prikupljanja i obrade podataka. Nadalje, *ex-ante* alati se dalje dijele na alate za podizanje svijesti i alate tzv. deklaracije, gdje je prva kategorija informativna, dok druga kategorija uključuje interakciju pojedinaca, ispitanika u inspekciji i prihvaćanju obrade podataka. *Ex-post* alati podijeljeni su na alate revizije za inspekciju od strane subjekata podataka, te interventne alate, koji omogućuju ograničenje prikupljanja i korištenja podataka, i alate za sanaciju, a koji omogućavaju manipulaciju i uklanjanje osobnih podataka.

Alati za poboljšanje transparentnosti mogu se definirati kao alati koji pružaju uvid u to kako se podaci pojedinaca prikupljaju i obrađuju, nastojeći prenijeti povezane rizike na točan i razumljiv način. Dok *ex-ante* alati informiraju o namjeravanom prikupljanju, obradi i otkrivanju podataka te na taj način nastoje pomoći korisnicima u predviđanju posljedica prilikom donošenja odluka hoće li i pod kojim uvjetima otkriti osobne podatke, *ex-post* alati pomažu korisnicima da steknu uvid u to koje je podatke tko prikupio, obradio ili otkrio te je li obrada podataka bila u skladu s dogovorenim ili navedenim politikama privatnosti.

Najčešći i najvažniji alat za povećanje transparentnosti je pružanje potrebnih informacija u obliku izjava o tim politikama privatnosti, koje se, ukoliko se koristi jezik za strojno čitanje, mogu automatski usporediti s korisničkim postavkama privatnosti, dok informacije o transparentnosti mrežnog mjesta može, primjerice, pružiti i vanjska povjerljiva strana u obliku rezultata reputacije ili drugih podataka o pružatelju usluge.



Slika 9 Podjela alata transparentnosti
Izvor: [230] str. 11. prijevod i prilagodba: autorica

Najčešći i najvažniji alat za povećanje transparentnosti je pružanje potrebnih informacija u obliku izjava o tim politikama privatnosti, koje se, ukoliko se koristi jezik za strojno čitanje, mogu automatski usporediti s korisničkim postavkama privatnosti, dok informacije o transparentnosti mrežnog mjesta može, primjerice, pružiti i vanjska povjerljiva strana u obliku rezultata reputacije ili drugih podataka o pružatelju usluge.

Nadalje, *ex-post* alati za povećanje transparentnosti mogu se podijeliti i prema strani na kojoj se informacije o transparentnosti prikupljaju, obrađuju i stavljaju na raspolaganje ispitanicima. Oni na strani korisnika prikupljaju sve informacije o transparentnosti tako da ostaju pod korisnikovom kontrolom. Primjer takvog alata je funkcionalnost „poboljšane zaštite od praćenja“ Firefox pregledniku za stolna računala koji omogućuje korisniku pregled mrežnih mjesta prve i treće strane s kojima komunicira na Internetu [231].

Alati za povećanje transparentnosti na strani pružatelja usluga pružaju korisniku sučelje nadzorne ploče koje mu omogućuje elektronički pristup, kontrolu ili izvoz osobnih podataka. Primjer je nadzorna ploča „Moja aktivnost“ [232] tvrtke Google koju mogu koristiti registrirani korisnici usluga te tvrtke za pregled i djelomičnu kontrolu nad podacima koje je tvrtka prikupila o njima.

Također, kao primjer alata na „trećoj“ strani može se razmotriti DataBait alat, koji je razvijen i testiran u okviru istraživačkog projekta USEMP [233], financiranog iz sredstava programa EU FP7. Alat omogućuje korisnicima društvenih mreža da dijele svoje podatke sa sigurnom pouzdanom istraživačkom platformom, koja koristi algoritme strojnog učenja za pružanje transparentnosti profila, objašnjavajući kako korisnici mogu biti „ciljani“ na temelju njihovih objava i podataka o ponašanju.

No, iako je osnovno načelo privatnosti, transparentnost može dovesti do pitanja povjerljivosti informacija. Primjerice, datoteke dnevnika koji bilježe pristupe elektroničkim zdravstvenim kartonima mogu stvoriti probleme s privatnošću budući da i sam podatak tko je pristupio kartonima, primjerice psihijatar, može biti kategoriziran kao osjetljiv. Štoviše, datoteke dnevnika pristupa bi se mogle koristiti i za praćenje uspješnosti i kvalitete rada (medicinskog) osoblja koje se može osjećati pod stresom na svom poslu kada se pomno promatra.

No, problem za povjerljivost poslovanja može predstavljati i transparentno evidentiranje, ako se radi na finoj razini granularnosti podataka. Primjerice, spomenute datoteke bi se mogle koristiti za reverzni inženjering algoritama za obradu podataka, kao što su algoritmi profiliranja kontrolora podataka, koji su često kategorizirani kao poslovne tajne, što je objašnjeno i u recitalu 63 preambule Opće uredbe o zaštiti podataka [45]. Iako Uredba spominje da pravo na transparentnost ne smije negativno utjecati na takve poslovne tajne, ono ne smije dovesti do toga da se ispitaniku odbije pravo na sve informacije. Time se implicira da bi se informacije o transparentnosti trebale pružiti barem na višoj razini granularnosti te trebaju biti osmišljene tako da uzimaju u obzir kompromise s pravima drugih, ne zanemarujući istodobno zahtjeve „da svaka informacija i komunikacija u vezi s obradom tih osobnih podataka bude lako dostupna i razumljiva te da se upotrebljava jasan i jednostavan jezik“, kao preduvjet transparentnosti opisan recitalom 39 spomenute Uredbe.

3.4.1.2. Učinkovitost alata transparentnosti

U disciplinama upravljanja informacijama, poslovne i informacijske etike pojam transparentnosti obično se koristi za oblike vidljivosti informacija te mogućnosti pristupa informacijama, namjerama ili ponašanjima koja su, na taj način, namjerno otkrivena [21], predstavljajući komunikacijski oblik kojim se prenosi signal između voditelja obrada podataka

i pojedinaca, pri čemu je za postizanje učinkovitosti alata, odnosno povećanja transparentnosti, potrebno ukloniti ili pak minimizirati svaki „šum“ ili „buku“ kao ometajućeg čimbenika komunikacijskog procesa. U kontekstu Shannon-Weaverova matematičkog modela sustava komunikacije [234] razlikuju se dva bitno različita načina za prijenos poruka: putem diskretnih signala i putem kontinuiranih signala. Diskretni signali mogu predstavljati samo konačan broj različitih, prepoznatljivih stanja, dok kod kontinuiranih signala količine signala mogu varirati u beskonačnom skupu vrijednosti. U tom referencijalnom okviru te širem tematskom sklopu osiguranja privatnosti, prvi mogu korespondirati s *ex-ante*, a drugi kao *ex-post* alatima transparentnosti, a budući da politike privatnosti, koje se izražavaju ograničenim slovima abecede, pretpostavljaju diskretan komunikacijski sustav, dok ostala rješenja mogu poprimiti razne oblike poput opisanih *ex-post* alata.

Nadalje, u odnosu na razinu buke, komunikacija se može odvijati u prisutnosti ili odsutnosti iste, pri čemu u kontekstu transparentnosti cilj je osigurati komunikaciju koja će težiti njenom uklanjanju kako bi primatelji imali mogućnost reproduciranje poruka u njenom izvornom obliku, a čime bi došlo do smanjenja informacijske asimetrije kao temeljnog cilja.

Tako se učinkovitost mehanizama transparentnosti kao diskretnih sustava, odnosno politika privatnosti kao predmeta istraživanja, može sagledavati u odnosu na entropiju, ključnu mjeru u teoriji informacija, kojom se kvantificira količina neizvjesnosti u prijenosu informacija, a koja je jednaka logaritmu broja različitih poruka koje se mogu poslati odabirom iz istog skupa simbola, kao mjere maksimalne moguće učinkovitosti bilo koje sheme kodiranja. Drugim riječima, prosječna distribucija znakova u abecedi poruke određuje granicu, na najboljoj prosječnoj (to jest, najkraćoj) mogućoj shemi kodiranja.

Stoga primjena opisanih koncepata može pružiti sredstvo za mjerenje suvišnosti ili učinkovitosti simboličkog predstavljanja unutar određenog jezika te se elementi određenih lingvističkih kategorija svakako trebaju sagledavati kao mjerilo učinkovitosti mehanizama transparentnosti.

Budući da komunikacijski signali trebaju biti sagledani izolirano od poruka koje prenose, a kako bi se posredno mogla ocijeniti kvaliteta komunikacijskog kanala, koja se u kontekstu osiguravanja privatnosti ogleda u mogućnosti intervenabilnosti primatelja signala, odnosno ispitanika da samostalno donose zaključke vezano uz zaštitu svojih podataka, ta se

komponenta može sagledati kao jedna dimenzija pri mjerenju učinkovitosti mehanizama transparentnosti.

Ipak, u kontekstu transparentnosti sa ciljem smanjenja informacijske asimetrije sadržaj poruke ne može biti zanemaren čime se pretpostavlja njegovo postojanje i dostupnost kao preduvjet komunikacije, kao druga vrijednosna komponenta i dimenzija učinkovitosti alata transparentnosti.

Stoga je za mjerenje učinkovitost alata transparentnosti potrebno razmatrati zahtjeve na sadržajnoj, ali komponenti kvalitete samog mehanizma transparentnosti, koje su u istraživanju postavljene kao dimenzije transparentnosti *vidljivost* i *inferabilnost* s pripadajućim odrednicama.

Dimenzija *vidljivosti* definirana je sljedećim odrednicama: zahtjevima informativnosti, ažuriranosti i pristupačnosti, dok je dimenzija *inferabilnosti* definirana odrednicama razumljivosti, smislenosti i slojevitosti.

Odrednica informativnosti odnosi se na sposobnost prenošenja dobre kvalitete informacija [235] i predstavlja sadržaj koji treba biti prenesen, odnosno komuniciran prema ispitanicima. Budući da se transparentnost u području zaštite podataka može smatrati više regulatornim nego dobrovoljnim zahtjevom, organizacije nastoje prilagoditi alate transparentnosti u skladu s postavljenim zakonskim okvirima ili standardima. U odnosu na ISO/IEC 29100:2011 [236] standard te spomenutu Opću uredbu o zaštiti osobnih podataka [45] predložena je i validirana taksonomija zahtjeva koji se odnose na sadržaj politika privatnosti te njihovu prezentaciju [26]:

- pružanje informacija kako i koji podaci se prikupljaju;
- informiranje o drugim izvorima podataka;
- pružanje dovoljnog objašnjenja kada se koriste osjetljivi podaci;
- pružanje informacije o osobnim podacima potrebnim za specificiranu svrhu obrade;
- pružanje objašnjenja zašto je svrha prikupljanja podataka legitimna;
- određivanje strana s kojima podaci mogu biti podijeljeni;
- pružanje informacija o transferu podataka prema trećoj zemlji ili međunarodnoj organizaciji i razinu zaštite koja je pružena od te strane;
- pružanje informacija kako i koji se podaci pohranjuju;

- pružanje informacija o roku pohrane podataka i njihovom brisanju;
- pružanje informacija o (sigurnosnim) mehanizmima za zaštitu podataka;
- pružanje informacija o mogućnostima ograničavanja obrade osobnih podataka;
- pružanje informacija o pravu pristupa podacima, ispravljanju, brisanju podataka te prigovoru na obradu podataka;
- pružanje informacija o sredstvima za pristup, ispravak i uklanjanje osobnih podataka;
- pružanje informacija o identitetu i kontaktu voditelja obrade.

Nadalje, faktor ili odrednica ažuriranosti na istoj dimenziji transparentnosti metrika je koja ukazuje na stupanj pouzdanosti informacija u odnosu na stvarne procese u sustavu organizacije, a ovisi o vremenu koje prolazi između nečega što se događa u sustavu i sustava koji o tome pruža informacije. Stoga se zahtjev za pružanjem informacija o ažuriranosti stranica može smatrati važnim aspektom pri povećanju učinkovitosti mehanizama transparentnosti u odnosu na osiguravanje elemenata odgovornosti kao jednog od ciljeva alata transparentnosti.

Odrednicom pristupačnosti nastoji se mjeriti jednostavnost pristupa mehanizmu, čime se zapravo ispituje taksonomski zahtjev da „informacije o upravljanju osobnim podacima trebaju biti lako dostupne“ [26], a koji je i zahtjev transparentnosti Opće uredbe o zaštiti osobnih podataka, elaboriran u Smjernicama o transparentnosti na temelju Uredbe 2016/679 [24] Radne skupine za zaštitu podataka iz članka 29. I dok se odrednica slojevitosti na dimenziji inferabilnosti, usmjerena na postizanje jednakog cilja u smanjenju „napora“ za pojedinca, odnosi na pojedinačne cjeline teksta u relaciji na cijeli dokument politika privatnosti, kod faktora pristupačnosti „informacijska“ jedinica podrazumijeva cjelokupni dokument politika privatnosti. Stoga primjena zahtjeva da su „informacije prikazane slojevitim prikazom“, slojevitog pristupa pri prezentaciji sadržaja može olakšati razumijevanje i pružiti jasan pregled dostupnih informacija čime se postiže veća učinkovitost mehanizama transparentnosti. Zahtjev da su „informacije prikazane slojevitim prikazom“ [24], stoga se odnosi na smanjenje „napora“ koji ispitanici trebaju uložiti prilikom traženja informacija, odnosno pridonosi smanjenju informacijske entropije, odnosno neizvjesnosti u prijenosu informacija.

I faktor smislenosti, mjeren kroz leksičku gustoću, donekle ovisi o tematskim cjelinama teksta, a određuje kvalitativna svojstva teksta u prenošenju smisla poruke, odnosno obavijesti, s ciljem što manjeg „informacijskog opterećenja“. Mjerenje leksičke gustoće jedna je od metoda koja se koristi pri opisu diskursa, te stoga ovisi o jezičnom registru i žanru teksta. Što

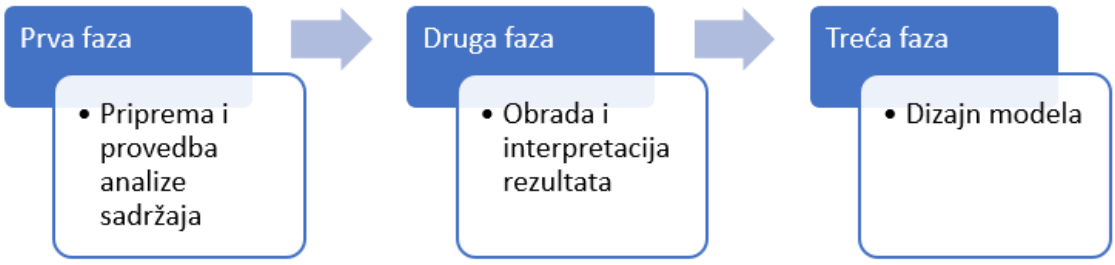
je veći broj leksičkih riječi, tekst je i leksički gušći pa je kod složenijih tekstova ta vrijednost bliža vrijednosti 1 [237]. Stoga je i zahtjev da „dokument nije prezasićen informacijama“ usmjeren prema smanjenju preopterećenosti informacijama koje, dovodeći do kognitivnog zasićenja pojedinaca, imaju porazni učinak na intervenabilnost odnosno donošenje (ispravnih) odluka ispitanika te je dobar vrijednosni pokazatelj u odnosu na smanjenje redundantnosti u prijenosu informacija spram mogućnosti kodiranja diskretnih sustava.

I posljednja, odrednica razumljivosti povezana je s jezičnom kvalitetom teksta, odnosno mehanizmom kodiranja. Predstavljena kao „sposobnost postizanja razumljivog značenja“ [235] njome se odražava zahtjev transparentnosti kojim „jezik za pružanje informacija treba biti jasan i prilagođen“ [26] određenoj ciljnoj skupini, a moguće ju je mjeriti analizama čitkosti teksta kao još jednom lingvističkom kategorijom pri mjerenju učinkovitosti kanala komunikacije.

4. METODOLOGIJA ISTRAŽIVANJA

4.1. Dizajn istraživanja

Istraživanje temeljeno na kvalitativnoj analizi sadržaja politika privatnosti objavljenih na mrežnim stranicama zdravstvenih ustanova, podrazumijeva primjenu *desk*-metoda istraživanja [238] te je osmišljeno i provedeno kroz tri faze prikazane na Slici 10.



Slika 10 Dijagram tijeka dizajna istraživanja

U prvoj, fazi pripreme i provedbe analize sadržaja prikupljene su adrese mrežnih stranica zdravstvenih ustanova (Prilog 1 i 2) kao materijala istraživanja te je izrađena analitička matrica (Prilog 3), kao i obrazac kodiranja (Prilog 3) te su standardizirane procedure prikupljanja podataka (Prilog 4). Pošto su dobiveni podaci obrađeni i interpretirani u drugoj fazi, u trećoj fazi pristupilo se dizajniranju modela vrjednovanja informacijske transparentnosti politika privatnosti i njegovoj validaciji kao krajnjem rezultatu istraživanja.

4.1.1. Prva faza: priprema i provedba analize sadržaja

4.1.1.1. Odabir materijala i uzorka

Istraživanje je provedeno na politikama privatnosti 152 zdravstvene ustanove, pri čemu je 56 ustanova u sustavu javne zdravstvene zaštite (Prilog 1), dok su preostale ustanove privatne zdravstvene zaštite. Razlog tome je da u slučaju zdravstvenih ustanova javnog sektora zdravstvene zaštite tijekom istraživanja u travnju i svibnju 2021. godine pojedine ustanove nisu imale objavljene dokumente politika privatnosti. Odnosno, od 148 zdravstvenih ustanova u sustavu javne zdravstvene zaštite, objavljenih na stranicama Ministarstva zdravstva [46] samo njih 37% imalo je objavljene politike privatnosti s unificiranim identifikatorom sadržaja kao postavljenim uvjetom za odabir uzorka. Uzorkom, također, nisu obuhvaćeni dokumenti tzv. politika kolačića kao zasebnih dokumenta, budući da se posredstvom tehnologija kolačića ne prikupljaju zdravstvene informacije u kontekstu opisanom kroz segment 1.3. prvog poglavlja – Privatnost i zdravstveni podaci.

Ustanove u sustavu zdravstva Republike Hrvatske sukladno članku 29. Zakona o zdravstvenoj zaštiti [239] podijeljene su na 4 razine: primarnu, sekundarnu i tercijarnu razinu te razinu zavoda.

Razinom primarne zdravstvene zaštite obuhvaćeni su domovi zdravlja, obavljanjem djelatnosti obiteljske (opće) medicine, dentalne zdravstvene zaštite, dentalne tehnike, zdravstvene zaštite žena, zdravstvene zaštite predškolske djece, medicine rada i/ili medicine rada i sporta, logopedije, laboratorijske, radiološke i druge dijagnostike, sanitetskog prijevoza, ljekarničke djelatnosti, fizikalne terapije, patronažne zdravstvene zaštite, zdravstvene njege te palijativne skrbi, kao i obavljanjem specijalističko-konzilijarne djelatnosti.

Sekundarnom razinom zdravstvene zaštite obuhvaćene su opće i specijalne bolnice, lječilišta i poliklinike. Opća bolnica i specijalna bolnica su zdravstvene ustanove koje obavljaju djelatnost dijagnostike, liječenja, medicinske rehabilitacije i zdravstvene njege bolesnika te osiguravaju boravak i prehranu bolesnika, pri čemu je opća bolnica zdravstvena ustanova koja obavlja najmanje djelatnosti kirurgije, interne medicine, pedijatrije, ginekologije i porodiljstva te hitne medicine i ima posteljne, dijagnostičke i druge mogućnosti prilagođene svojoj namjeni, dok je specijalna bolnica usmjerena na djelatnost specijalističko-konzilijarnog i bolničkog

liječenja određenih bolesti ili određenih dobnih skupina stanovništva. Nadalje, lječilišta su ustanove u kojoj se prirodnim ljekovitim izvorima provodi preventivna zdravstvena zaštita, specijalistička i bolnička rehabilitacija, dok su poliklinike zdravstvene ustanove u kojoj se obavlja specijalističko-konzilijarna zdravstvena zaštita, dijagnostika i medicinska rehabilitacija, a osim bolničkog liječenja moraju obavljati djelatnost najmanje u dvije ambulante različitih ili istih specijalističkih ili užih specijalističkih djelatnosti ,odnosno u jednoj ambulanti specijalističke odnosno uže specijalističke djelatnosti i laboratoriju.

Treću razinu zdravstvene zaštite čine kliničke ustanove: klinika, klinička bolnica i klinički bolnički centar. Klinika jest zdravstvena ustanova ili dio zdravstvene ustanove u kojoj se uz obavljanje specijalističko-konzilijarne i bolničke djelatnosti izvodi nastava visokih učilišta i provodi znanstveni rad za djelatnost za koju je osnovana. Klinička bolnica jest opća bolnica u kojoj najmanje dvije od navedenih djelatnosti (interna medicina, kirurgija, pedijatrija, ginekologija i porodiljstvo) nose naziv klinika, kao i najmanje još dvije druge djelatnosti drugih specijalnosti odnosno dijagnostike. Klinički bolnički centar je opća bolnica u kojoj osim naziva klinike za djelatnost interne medicine, kirurgije, pedijatrije, ginekologije i porodiljstva, naziv klinike ima i više od polovice ostalih specijalnosti i u kojima se izvodi više od polovice nastavnog programa studija medicine, dentalne medicine, farmacije i medicinske biokemije odnosno sestrinstva.

Naposljetku, razina zavoda odnosi se na razne potporne institucije u sustavu zdravstva: državne zdravstvene zavode, zavode za javno zdravstvo jedinica područne (regionalne) samouprave i zavode za hitnu medicinu jedinica područne (regionalne) samouprave.

Državni zdravstveni zavodi su zdravstvene ustanove za obavljanje stručnih i znanstvenih djelatnosti iz okvira prava i dužnosti Republike Hrvatske na području javnozdravstvene djelatnosti, medicine rada, telemedicine, toksikologije i antidopinga, transfuzijske medicine te hitne medicine. To su Hrvatski zavod za javno zdravstvo, Hrvatski zavod za transfuzijsku medicinu te Hrvatski zavod za hitnu medicinu.

Zavodi za hitnu medicinu jedinica područne (regionalne) samouprave su zdravstvene ustanove za obavljanje poslova iz okvira prava i dužnosti jedinica područne (regionalne) samouprave na području hitne medicine.

S obzirom na organizacijski oblik, relativno najveći udio uzorkom obuhvaćenih zdravstvenih ustanova potpada pod kategoriju specijalnih bolnica (21%, n=12) te općih bolnica (18%, n=10). Tipologija uzorkom obuhvaćenih zdravstvenih ustanova prikazana je u Tablici 3.

Tablica 3 Tipologija uzorkom obuhvaćenih javnih zdravstvenih ustanova

Vrsta javne zdravstvene ustanove	Frekvencije	Postotci
Specijalne bolnice	12	21.4%
Opća bolnica	10	17.9%
Dom zdravlja	9	16.1%
ŽZHM	9	16.1%
Poliklinika	5	8.9%
KBC	4	7.1%
Klinika	2	3.6%
Lječilište	2	3.6%
Zavod	2	3.6%
Klinička bolnica	1	1.8%
Ukupno	**56**	**100.0%**

Nadalje, s obzirom na razinu zdravstvene zaštite koju pružaju, najveći udio uzorkom obuhvaćenih ustanova, više od polovice (52%, n=29), pruža sekundarnu zdravstvenu zaštitu. Nešto manje zastupljene su ustanove na razini zavoda (20%, n=11), dok 16% ustanova (n=9) pruža primarni oblik zdravstvene zaštite. Najmanji udio uzrokom obuhvaćenih zdravstvenih ustanova pripada tercijarnoj (13%, n=7) razini zdravstvene zaštite. Podaci o razinama zdravstvene zaštite koju pružaju uzorkom obuhvaćene zdravstvene ustanove, prikazani su u Tablici 4.

Tablica 4 Razina zdravstvene zaštite uzorkom obuhvaćenih zdravstvenih ustanova

Razina zdravstvene zaštite	Frekvencije	Postotci
Primarna	18	32.1%
Sekundarna	29	51.8%
Tercijarna	7	12.5%
Zavodi	2	3.6%
Ukupno	**56**	**100.0%**

Prilikom odabira zdravstvenih ustanova u privatnom sektoru (Prilog 2) u obzir je uzet uvjet da usluge ustanove u većini zadovoljavaju potrebe cjelokupnog stanovništva, odnosno da usluge nisu usmjerene pretežno prema pojedinom spolu pojedinca, poput primjerice ginekoloških zdravstvenih ustanova, kako bi se dobiveni rezultati mogli postaviti u referentni okvir potrebne razine školovanja za ispitivanje pod-indikatora odrednice razumljivosti teksta,

a koji je postavljen na temelju rezultata razine školovanja na temelju uzorka cijele populacije prema Popisu stanovništva iz 2011. godine [240] pa su prilikom odabira uzorka selektirane ustanove koje pružaju usluge u jednakom omjeru pripadnicima oba spola, poput ordinacija stomatološke i oftalmološke medicine te bolnica i ustanova usmjerenih na pružanje usluga dijagnostike, zdravstvene njege i fizikalne terapije, čija je tipologija prikazana u Tablici 5.

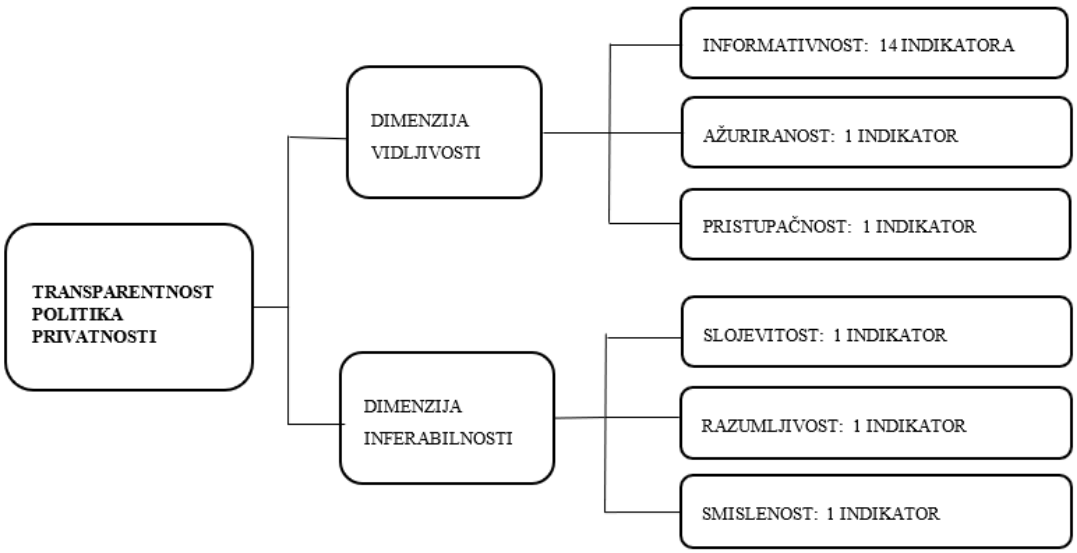
Tablica 5 Tipologija uzorkom obuhvaćenih privatnih zdravstvenih ustanova

Vrsta privatne zdravstvene ustanove	Frekvencije	Postotci
Poliklinika	63	65.63%
Ordinacija	25	26.04%
Bolnica	6	6.25%
Ustanova za zdravstvenu njegu	1	1.04%
Centar za fizikalnu terapiju, rehabilitaciju i edukaciju	1	1.04%
Ukupno	**96**	**100.00%**

4.1.1.2. Izrada analitičke matrice i kodnog obrasca

Kao osnova za provedbu analize sadržaja, analitička matrica konstruirana je uz pretpostavku da se informacijska transparentnost politika privatnosti može mjeriti preko dimenzija transparentnosti – dimenzije vidljivosti i dimenzije inferabilnosti. Kako bi mjerenje dimenzija bilo moguće, svaka od njih operacionalizirana je preko određenog broja indikatora i pod-indikatora, kojima su dodijeljeni odgovarajući ponderi prema teorijski pretpostavljenoj važnosti pojedinog pod-indikatora u definiranju indikatora. Suma pondera pod-indikatora na svakom indikatoru iznosi 1. kao „mjera“ ispunjenosti zahtjeva u potpunosti. Primjerice, ako se indikator sastoji od dva pod-indikatora jednake važnosti, onda je svakom pod-indikatoru dodijeljen ponder 0.5. Ako je jedan pod-indikator važniji od drugoga, onda su pod-indikatorima dodijeljeni ponderi 0.75 i 0.25. Ako je bilo tri pod-indikatora jednake važnosti, dodijeljeni ponderi su iznosili 0.33 itd. Svaki od definiranih indikatora mogao je postići vrijednost između 0 i 1.

U nastavku, prikazana Slikom 11, nalazi se shema dimenzija informacijske transparentnosti, njihovih odrednica i broja indikatora.



Slika 11 Shema dimenzija informacijske transparentnosti po odrednicama i broju indikatora

4.1.1.2.1. Dimenzija vidljivosti

Dimenzija vidljivosti definirana je sljedećim odrednicama: zahtjevima informativnosti, ažuriranosti i pristupačnosti.

Odrednica informativnosti odnosi se na informacije pružene dokumentom te je mjerena putem 14 indikatora definiranih u najvećoj mjeri korištenjem taksonomskih zahtjeva transparentnosti [26] prikazanih u Tablici 6.

Tablica 6 Indikatori i pod-indikatori odrednice informativnosti

Indikator	**Pod-indikatori**	**Ponderske vrijednosti pod-indikatora**	**Suma pondera na indikatoru**
Pružanje informacija kako i koji podaci se prikupljaju	Mehanizmi prikupljanja podataka jasno su objašnjeni	0.5	1.0
	Definirani su podaci ili kategorije podataka koje se prikupljaju	0.5	
Informiranje o drugim izvorima podataka	Navedeno je postoje li drugi izvori podataka	0.75	1.0
	Mehanizmi prikupljanja podataka iz drugih izvora podataka jasno su objašnjeni	0.25	

Indikator	Pod-indikatori	Ponderske vrijednosti pod-indikatora	Suma pondera na indikatoru
Pružanje dovoljnog objašnjenja kada se koriste osjetljivi podaci	Objašnjeno je korištenje posebne kategorije podataka	1.0	1.0
Pružanje informacije o osobnim podacima potrebnim za specificiranu svrhu obrade	Svrhe obrade (kategorija) podataka jasno su navedene	0.75	1.0
	Navedeni su podaci ili kategorije podataka koji se obrađuju u pojedinoj svrsi obrade	0.25	
Objasniti zašto je svrha prikupljanja podataka legitimna	Navedene su pravne osnove za obradu podataka organizacije	0.75	1.0
	Pravne osnove su definirane za svaku obradu podataka	0.25	
Određivanje strana s kojima podaci mogu biti podijeljeni	Postoji sekcija u dokumentu u kojoj je navedeno (ne)postojanje trećih strana	0.25	1.0
	Navedene su treće strane s kojima se dijele podaci	0.50	
	Navedene su podaci ili kategorije podataka koje se dijele	0.25	
Pružanje informacija o transferu podataka prema trećoj zemlji ili međunarodnoj organizaciji i razina zaštite koja je pružena od te strane	Postoji sekcija u dokumentu u kojoj je navedeno (ne)postojanje transfera podataka unutar ili izvan gospodarskog pojasa EU)	0.50	1.0
	Navedeno je i objašnjeno dijeljenje podataka prema trećim zemljama	0.25	
	Definirane su mjere zaštite pri transferu podataka	0.25	

Indikator	Pod-indikatori	Ponderske vrijednosti pod-indikatora	Suma pondera na indikatoru
Pružanje informacija kako i koji se podaci pohranjuju	Navedeni su mehanizmi pohrane podataka	0.5	1.0
	Navedeni su podaci ili kategorije podataka u sustavu pohrane	0.5	
Pružanje informacija o roku pohrane podataka i njihovom brisanju.	Navedeni su rokovi pohrane ili kriteriji za njihovo određivanje	0.75	1.0
	Objašnjeni su postupci po navedenom roku (brisanje, anonimizirana pohrana)	0.25	
Informiranje o (sigurnosnim) mehanizmima za zaštitu podataka	Mehanizmi sigurnosti podataka su navedeni	0.75	1.0
	Mehanizmi zaštite eksplicitno su objašnjeni	0.25	
Pružanje informacija o mogućnostima ograničavanja obrade osobnih podataka	Mogućnost ograničavanja obrade od strane ispitanika jasno je objašnjena	0.75	1.0
	Postupak ograničavanja obrade osobnih podataka jasno je definiran	0.25	
Pružanje informacija o pravu pristupa podacima, ispravljanju, brisanju podataka te prigovoru na obradu podataka	Pravo ispitanika na pristup podacima jasno je izrečeno	0.25	1.0
	Pravo ispitanika na ispravak podataka jasno je izrečeno	0.25	
	Pravo ispitanika na brisanje podataka jasno je izrečeno	0.25	
	Pravo ispitanika na prigovor obradi podataka jasno je izrečeno	0.25	

Indikator	Pod-indikatori	Ponderske vrijednosti pod-indikatora	Suma pondera na indikatoru
Pružanje informacija o sredstvima za pristup, ispravak i uklanjanje osobnih podataka.	Postupak pristupa podacima je jasno definiran	0.33	1.0
	Postupak ispravka podataka jasno je objašnjen	0.33	
	Postupak uklanjanja podataka jasno je objašnjen	0.33	
Pružanje informacija o identitetu i kontaktu voditelja obrade.	Identitet voditelja obrade jasno je naveden	0.5	1.0
	Kontakt podaci i mehanizmi voditelja obrade jasno su navedeni	0.5	

Budući da je odrednica informativnosti postavljena na dimenziji transparentnosti kojom se prvenstveno nastoji mjeriti faktor vidljivosti informacija prilikom definiranja ponderskih vrijednosti pod-indikatora veći težinski je omjer vrijednosti postavljen u smjeru ispitivanja prisutnosti informacija u dokumentu, odnosno jedinici ispitivanja, dok je manji usmjeren na kvalitativne aspekte zadovoljavanja samog zahtjeva.

Zahtjevi za ***Pružanje informacija kako i koji podaci se prikupljaju*** te ***Informiranje o drugim izvorima podataka*** odnose se na pružanje informacija o početku životnog ciklusa podataka unutar organizacije, odnosno propisuju da ispitanici moraju biti informirani o tome kako i koji se podaci od njih prikupljaju. Prvi zahtjev pružanja informacija kako i koji podaci se prikupljaju odnosi se na opis mehanizama izravnog prikupljanja podataka od ispitanika (primjerice, putem internetske forme, telefonski, u osobnom kontaktu), koji je izražen kroz prvi kriterij, te navođenje podataka koji se prikupljaju tim mehanizmima, izražen kroz drugi kriterij za ispitivanje.

Budući da su zahtjevom definirana oba kriterija (kako se podaci prikupljaju i koji se podaci prikupljaju) jednako, tako su raspoređene i njihove ponderske vrijednosti.

Nadalje, zahtjev za informiranjem o drugim izvorima podataka zapravo je istančani oblik prethodnog zahtjeva, a odnosi se na mogućnost neizravnog prikupljanja podataka te ponovnog korištenja već postojećih podataka, pa se i kao kriterij ispitivanja prvo postavlja jesu li navedeni drugi izvori podataka, što može biti i pristup zdravstvenim podacima iz informacijskih sustava izvan organizacije, ali i automatizirana obrada podataka putem kolačića ili drugih mehanizama, radi čega je težinski omjer postavljen u „korist“ prvog kriterija. Prisustvo kolačića na internetskim stranicama, prema regulatornim zahtjevima, također treba biti transparentno navedeno već pri dolasku na stanice te se u odnosu na taj zahtjev može odrediti postoji li takva obrada podataka te je li ona navedena u politikama privatnosti. U nekim slučajevima organizacije opisuju takvu obradu podataka kroz zasebni dokument (politike o korištenju kolačića) te se ispitivanje (ne)ispunjenosti kriterija zahtjeva treba sagledati i s tog stanovišta. Budući da politike o korištenju kolačića nisu u primarnom fokusu istraživanja jer se radi o podacima koje ne sadrže zdravstvene podatke niti tzv. jedinstvene identifikatore, no u kombinaciji s drugim podacima mogu biti iskorišteni u svrhu profiliranja ili segmentiranja korisnika, kriterij ima manju pondersku vrijednosti u odnosu na prvi kriterij zahtjeva.

Nadalje, sljedeći zahtjev ***Pružanje dovoljnog objašnjenja kada se koriste osjetljivi podaci*** je važan i nezaobilazan u području zaštite podataka u zdravstvu, a odnosi se na specificiranje podataka koji su pod posebnom kategorijom radi svoje „osjetljivosti“ po pitanju privatnosti ispitanika. Razlučivanje takvih podataka može biti važan aspekt pri donošenju odluka ispitanika.

Pružanje informacije o osobnim podacima potrebnim za specificiranu svrhu obrade smatra se ključnim zahtjevom u postizanju transparentnosti, usmjerenim na pružanje odgovora na pitanje zašto se podaci prikupljaju i koriste, pri čemu se osobni podaci mogu grupirati u kategorije te se u odnosu na iste mogu navesti svrhe, zbog čega i taj kriterij ima težinski veći omjer u odnosu na drugi kriterij kojim se detaljnije ispituje zahtjev, a budući da bi se u cilju postizanja najvećeg stupnja transparentnosti trebale identificirati svrhe korištenja za svaku pojedinu kategoriju podataka.

Jednako tako, za svaku obradu podataka i njenu svrhu potrebno je pružiti informacije o njenoj legitimnosti, odnosno navesti pravnu osnovu prema kojoj se podaci obrađuju, što se ispituje zahtjevom ***Objasniti zašto je svrha prikupljanja podataka legitimna***. Jednako kao i kod prethodnog zahtjeva, prvi kriterij navođenja legitimne osnove ispituje postojanje pojedinih

informacija u dokumentu, te, stoga, ima veću pondersku vrijednost od drugog kriterija koji zapravo ispituje „kvalitetu“ ispunjenosti postavljenog zahtjeva.

Zahtjev ***Određivanje strana s kojima podaci mogu biti podijeljeni*** propisuje navođenje (ovlaštenih) osoba kojima bi se osobni podaci mogli otkriti, odnosno trećih strana. Navođenje trećih strana ujedno je i jedna od „standardiziranih“ sekcija politika privatnosti kojom se detaljnije opisuje tijek podataka u organizaciji, pa je njeno postojanje kao kriterij ispitivanja ispunjenosti zahtjeva težinski označeno s ponderskom vrijednošću 0.25 budući da i proklamacija da se podaci ne dijele s trećim stranama smatra ispunjenim zahtjevom. U tom slučaju daljnja dva kriterija, koja ispituju kvalitativna svojstva ispunjenosti zahtjeva, smatraju se također ispunjenima, dok se u protivnome, ako se podaci dijele s trećim stranama, navođenje tih strana vrednuje s 0.5 ponderske vrijednosti, a navođenje i samih podataka koje se dijele s 0.25, budući da se radi o zadovoljavanju najvećeg stupnja učinkovitosti u postizanju transparentnosti za taj zahtjev.

Još jedan zahtjev koji se odnosi na specificiranje tijeka podataka je i zahtjev ***Pružanje informacija o transferu podataka prema trećoj zemlji ili međunarodnoj organizaciji i razina zaštite koja je pružena od te strane***, koji je posebno važan u kontekstu usklađivanja s regulatornim pravilima Opće uredbe o zaštiti podataka te je posebno aktualan nakon odluke Suda Europske unije od 16. srpnja 2020. godine [241] u slučaju poznatom pod nazivom *Schrems II,* kojom je stavljen van snage EU-US Privacy Shield sporazum Europske komisije i američkog Ministarstva trgovine o zaštiti osobnih podataka koji se iz Europske unije prenose u Sjedinjene Američke Države. Učinkoviti mehanizmi transparentnosti stoga bi trebali navesti postoji li transfer podataka izvan gospodarskog pojasa EU ili se podaci pohranjuju i obrađuju samo unutar pojasa Europske unije, što je težinski najviše vrednovani kriterij u ispunjavanju zahtjeva prema kojem se onda sagledavaju i ostala dva kriterija. Ukoliko se podaci ne dijele izvan gospodarskog pojasa EU zahtjev se smatra u potpunosti ispunjen, odnosno oba sljedeća kriterija su ispunjena, dok u protivnome, potrebno je navesti i objasniti dijeljenje podataka prema trećim zemljama (o kojim se zemljama i podacima radi) kao i definirati mjere zaštite pri transferu podataka. Poglavlje V. Opće uredbe, s pripadajućih 7 članaka, posvećeno je upravo načelima prijenosa i zaštite podataka prema trećim zemljama ili međunarodnim organizacijama.

Zahtjevi ***Pružanje informacija kako i koji se podaci pohranjuju*** i ***Pružanje informacija o roku pohrane podataka i njihovom brisanju*** u taksonomiji zahtjeva [26] su postavljeni kao

zahtjevi vezani uz atribut retencije podataka. Dok se kroz prvi zahtjev nastoje pružiti informacije vezano uz životni ciklus podataka u svrhu povećanja informacijske transparentnosti, on nije regulatorno „zadan“ poput drugog zahtjeva. Člankom 13.[13] Opće uredbe o zaštiti podataka „kako bi se osigurala poštena i transparentna obrada“ potrebno je navođenje „razdoblja u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, kriterija kojima se utvrdilo to razdoblje“. Nadalje, prvi zahtjev, u kontekstu životnog ciklusa podataka, pruža informacije koje ispitanicima mogu bolje razjasniti mehanizme sigurnosti podataka, što je ujedno i kasnije objašnjen zahtjev.

Dakle, zahtjevom za pružanjem informacija kako i koji se podaci pohranjuju definirani su jednako vrijednosni kriteriji: navedeni su mehanizmi pohrane podataka, ali i podaci ili kategorije podataka u sustavu pohrane. Nadalje, kriteriji zahtjeva za navođenjem rokova pohrane i njihovom brisanju postavljeni su, stoga, vezano, na način da se prvim kriterijem, koji je ujedno i vrednovan više u odnosu na drugi kriterij, ispituje postojanje regulatorno obveznih informacija o određivanju roka pohrane, dok se drugim kriterijem ispituju navođenje postupaka nad podacima po isteku navedenih rokova.

Informiranje o (sigurnosnim) mehanizmima za zaštitu podataka, iako nije regulatorni zahtjev, važan je aspekt osiguravanja načela pravednog informiranja te su i kriteriji za ispitivanje zahtjevi postavljeni u skladu s istima. Samo postojanje informacija o mehanizmima sigurnosti, vrednovano je kao pozitivan aspekt u kontekstu smanjenja informacijske asimetrije, pa je i veći težinski omjer postavljen u odnosu na taj aspekt osiguravanja transparentnosti. No, sama izjava da organizacija poduzima i koristi „suvremene tehničke i organizacijske mjere“ u zaštiti podataka ne nudi dovoljno informacija ispitaniku pa je postavljen i „kvalitativni“ kriterij mehanizama s manjom težinskom vrijednošću u zadovoljavanju zahtjeva.

Zahtjev ***Pružanje informacija o mogućnostima ograničavanja obrade osobnih podataka*** ključan je zahtjev tzv. kontrole ispitanika nad podacima koji proizlazi isto iz načela pravednog informiranja, a odnosi se na koncept privole kao oblika autonomne autorizacije kojim pojedinac (ispitanik) ovlašćuje voditelja obrade podataka da obrađuje njegove osobne podatke. Stoga je i kriterij isticanja autonomnosti ispitanika pri pružanju podataka unutar dokumenta politika privatnosti postavljen s višim ponderskim vrijednostima od kriterija koji se

[13] I članak 14. Opće uredbe o zaštiti podataka pod informacije koje se trebaju pružiti ako osobni podaci nisu dobiveni od ispitanika također postavlja navođenje svrhe obrade podataka kao mandatorno.

odnosi na samu mogućnost kontrole od strane ispitanika, odnosno jasno definiranog postupka ograničavanja obrade osobnih podataka, budući da se informacije o ustezanju privole moraju postaviti i unutar mehanizama za davanje privola te nisu utoliko važan aspekt u ispunjavanju zahtjeva.

Ipak, taj zahtjev u taksonomiji [26] je detaljnije razložen zahtjevima ***Pružanje informacija o pravu pristupa podacima, ispravljanju, brisanju podataka te prigovoru na obradu podataka*** i ***Pružanje informacija o sredstvima za pristup, ispravak i uklanjanje osobnih podataka***.

Pravo na pristup podacima regulatorno je definirano člankom 15. Opće uredbe o zaštiti podataka, pravo na ispravak podataka člankom 16., dok je pravo na brisanje podataka, odnosno „pravo na zaborav“, definirano člankom 17. iste uredbe [45]. Pravo na prigovor vezano uz obrade podataka, definirano člankom 18. Uredbe, odnosi se na ograničavanje već započete obrade podataka od strane ispitanika te za razliku od zahtjeva za pružanjem informacija o mogućnostima ograničavanja obrade osobnih podataka postavlja se kao zahtjev *ex-post* transparentnosti te se osigurava kroz pripadajuće alate i mehanizme.

Zahtjev za pružanjem informacija o sredstvima za pristup, ispravak i uklanjanje osobnih podataka nadopunjuje prethodni zahtjev s obzirom na prava pristupa, ispravka te brisanja podataka, uzimajući u obzir suvremene informacijske sustave te mogućnosti pristupa podacima od strane korisnika. Objašnjeni postupci u odnosu na potrebne operacije za ostvarivanje navedenih prava ili navođenje ispitanika na slanje poruke elektroničke pošte sa zahtjevom za ostvarivanje navedenih prava smatra se djelomično ili u potpunosti ispunjenim zahtjevom.

Posljednji zahtjev na odrednici informativnosti odnosi se na ***Pružanje informacija o identitetu i kontaktu voditelja obrade***[14] koji je postavljen i stavkom 1. članaka 13. i 14. Opće uredbe o zaštiti podataka. Voditeljem obrade podataka označava se „fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka“ [45] te se time smatra i pravno odgovornom za te obrade podataka. Uostalom, odgovornost voditelja obrade za obradu i dokazivanje usklađenosti s regulatornim i/ili standardima dobre prakse jedno je od principa privatnosti prema Smjernicama

[14] Ako je primjenjivo potrebno je navesti i predstavnike voditelja obrade.

Organizacije za ekonomsku suradnju i razvoj [127] pa je važan element u osiguravanju transparentnosti u prikupljanju i obradi (osobnih) podataka.

Nadalje, da bi određena politika privatnosti bila što transparentnija u prikazu realnih procesa vezanih uz obradu podataka unutar organizacije potrebno je dokument ažurirati u skladu s izmjenama. Odrednica ažuriranosti, stoga je zapravo dodatni kvalitativni faktor informativnosti, a mjeri se kroz dva predložena kriterija iskazana u Tablici 7.

Tablica 7 Indikatori i pod-indikatori odrednice ažuriranosti

Indikator	**Pod-indikatori**	**Ponderske vrijednosti pod-indikatora**	**Suma pondera na indikatoru**
Pružanje informacija o ažuriranosti stranica	Datum posljednjeg ažuriranja eksplicitno je naveden	0.75	1.0
	Pružene su informacije o načinu obavještavanja ispitanika o izmjenama politika privatnosti	0.25	

Iako pružanje informacija o načinu obavještavanja ispitanika o izmjenama politika privatnosti pozitivno utječe na poboljšanje informacijske transparentnosti te je svakako dobra praksa pri osiguravanju veće privatnosti za pojedinca, pri zadovoljavanju zahtjeva navođenje datuma ažuriranosti nudi ispitaniku više obavijesnosti prema čemu je i ponderski omjer postavljen sukladno.

Odrednicom pristupačnosti na dimenziji vidljivosti mjeri se koliko je korisniku jednostavan pristup mehanizmu transparentnosti, odnosno politici privatnosti, ako mu je uopće dostupan. Mjera je određena u odnosu na broj interakcija (klikova) na mrežnom mjestu potrebnih za pristup dokumentu, prilikom čega je potrebno odrediti maksimalni broj interakcija (k) koji se smatra prihvatljivim za pristup politikama privatnosti. Prema Smjernicama o transparentnosti na temelju Uredbe 2016/679 [24] Radne skupine za zaštitu podataka iz članka 29 „izravna poveznica na izjavu/obavijest o privatnosti trebala bi biti jasno vidljiva na svakoj stranici tog portala pod pojmom koji se uobičajeno koristi (primjerice, „Privatnost", „Politika privatnosti" ili „Obavijest o zaštiti podataka").

Suvremeni pristupi dizajnu mrežnih stranica omogućavaju objavu poveznice u podnožje internetskih stranica, što omogućava pristup navedenoj obavijesti iz jedne interakcije, ili

posredstvom tzv. padajućih izbornika, čime su korisniku potrebne dvije interakcije za pristup dokumentu. Stoga, postavljen je referentni kriterij od 2 interakcije, odnosno k=2. Dakle, za vrijednosti od jedne ili dvije interakcije potrebne za pristup dokumentu zahtjev se smatra ispunjenim te je vrijednost indikatora 1.

Nadalje, broj potrebnih interakcija do dokumenta označen je kao n(int) pa je formula za izračun faktora pristupačnosti k/(n)int, gdje se za vrijednosti broja interakcija veće od k vrijednosti indikatora linearno smanjuje od vrijednosti 1 za svaki naredni broj interakcije.

Prilikom proračunavanja odrednice pristupačnosti postavljen je jedan pod-indikator s vrijednostima prikazan u Tablici 8.

Tablica 8 Indikatori i pod-indikatori odrednice pristupačnosti

Indikator	**Pod-indikator(i)**	**Vrijednost indikatora**
Informacije o upravljanju osobnim podacima trebaju biti lako dostupne	Dokumenti politika lako su dostupni	0-1.0

4.1.1.2.2. Dimenzija inferabilnosti

Dimenzija inferabilnosti definirana je sljedećim odrednicama: slojevitosti, razumljivosti i smislenosti.

Smjernice Radne skupine za zaštitu podataka iz članka 29 [24] ističu zahtjev „slojevitog pristupa u digitalnom okruženju i slojevite izjave/obavijesti o privatnosti“, preporučujući korištenje kombiniranih metoda za osiguravanje transparentnosti.

Radi izbjegavanja umaranja zbog prekomjernih informacija, obavijesti bi stoga trebale primjenjivati postupke kategorizacije informacija, što pridonosi i razumijevanju teksta, pa je jedan od kriterija za ispitivanje indikatora slojevitosti usmjeren na ispitivanje odijeljenosti tematskih jedinica unutar teksta politika privatnosti.

Tematske cjeline dokumenta politika privatnosti moguće je „standardizirati“ u odnosu na sekcije prikazane i prilikom analize stupnjeva leksičke gustoće, a definirane su s obzirom na spomenuta načela *Praksi poštenog informiranja* (obavijest/svijest, izbor/pristanak, pristup/sudjelovanje, integritet/sigurnost i provedba/pravna zaštita), prihvaćena od strane

Savezne trgovinske komisije te Organizacije za ekonomsku suradnju i razvoj te su potvrđene u radovima [242] [158]:

- prikupljanje/kolekcija: odjeljak objašnjava koje se informacije prikupljaju od korisnika i kako se prikupljaju informacije od strane ispitanika;
- svrha: odjeljak objašnjava svrhu prikupljanja i korištenja podataka od strane davatelja usluga;
- izbor/kontrola: odjeljkom se objašnjavaju opcije ispitanika u odnosu na postavke privatnosti, poput davanja privole ili opcija odjavljivanja korištenja određenih usluga;
- dijeljenje: odjeljak navodi s kime (tzv. treća strana) i pod kojim se okolnostima dijele informacije ispitanika;
- sigurnost: odjeljak raspravlja o standardnoj praksi zaštite podataka korisnika od strane davatelja usluga;
- zadržavanje podataka (retencija): odjeljak objašnjava postupak i rok zadržavanja osobnih podataka ispitanika;
- specifično: navode se prakse koje se odnose samo na određenu skupinu korisnika (npr. djecu ili građane pojedinih teritorijalnih oblasti u odnosu na tamošnje važeće regulatorne okvire);
- promjena politika: objašnjava se kako će korisnici biti informirani o promjeni praksi privatnosti.

Stoga se prilikom istraživanja pozitivno označila vrijednost pod-indikatora ako se u dokumentu uočila tendencija prema grupiranju informacija s obzirom na predložene tematske cjeline, odnosno sekcije, kao jedan od kriterija u zadovoljavanju zahtjeva slojevitosti.

Nadalje, „dizajn i grafičko uređenje prvog sloja izjave/obavijesti o privatnosti trebali bi biti takvi da ispitanik ima jasan pregled informacija koje su mu dostupne o obradi njegovih osobnih podataka i o tome gdje/kako može pronaći detaljne informacije unutar slojeva izjave/obavijesti o privatnosti“ [24]. Digitalno okruženje omogućava mnoga aplikacijska rješenja kojima se na internetskim stranicama jednostavno može manipulirati sadržajem, poput kartičnog prikaza i postavljanja tzv. knjižnih oznaka i sl., dok se hijerarhija teksta može naznačiti i naslovima (što je čest slučaj kod dokumenata politika privatnosti u .pdf formatu) pa je i jedan od kriterija za ispitivanje indikatora usmjeren na ispitivanje upravo tog elementa.

Iz tih razloga postavljen je indikator odrednice slojevitosti s pod-indikatorima prikazanima u Tablici 9.

Tablica 9 Indikatori i pod-indikatori odrednice slojevitosti

Indikator	**Pod-indikatori**	**Ponderske vrijednosti pod-indikatora**	**Suma pondera na indikatoru**
Informacije su prikazane slojevitim prikazom	Izražena je tendencija grupiranju informacija s obzirom na tematske cjeline, odnosno sekcije.	0.5	1.0
	Hijerarhija teksta označena je naslovima ili drugim (grafičkim) metodama	0.50	

Odrednica razumljivosti teksta pretpostavlja zahtjev da je jezik kojim se pružaju informacije jasan i prilagođen određenoj ciljnoj skupini pa je prilikom ispitivanja odrednice razumljivosti potrebno provesti analizu čitkosti teksta s obzirom na kriterije upotrebe jasnog i jednostavnog jezika te prilagođenosti jezika ciljnoj skupini.

Prvi pod-indikator moguće je ispitati primjenom formule za izračun čitkosti Flesch Reading Ease (FRE) koja je svedena na dvije varijable, prosječnu dužinu riječi i prosječnu dužinu rečenice, te glasi FRE = 206.835 – 0.846 AWL – 1.015 ASL, gdje je AWL prosječna dužina riječi izražena brojem slogova (engl. Average word length), a ASL dužina prosječna rečenice izražena brojem riječi (engl. Average sentence length).

Prema Brangan [243] modifikacija originalne formule za hrvatski jezik, dobiveni rezultat uvećava se za 50 te se s time u skladu usklađuje i ljestvica razumijevanja, odnosno prihvatljiv indeks razumljivosti teksta za ciljnu skupinu: 80 – 100 = lako; 60 – 80 = standardno; 50 – 60 = donekle teško; te 0 – 50 = vrlo teško.

Stoga je prilikom određivanja ispunjenosti kriterija postavljena referentna vrijednost FRE >= 60 pa su i dokumentima s vrijednošću većom od referentne vrijednosti dodijeljene ponderske vrijednosti pod-indikatora (0.5).

Nadalje, iz modifikacije tzv. Kincaid formule (broj razreda = (0.4 ASL) + (12 ASW) – 15) za engleski jezik na hrvatski jezik (broj razreda = (0.4 ASL) + (12 ASW) –22) iste autorice

[244] moguće je odrediti i potreban broj razreda, odnosno razine školovanja ispitanika za razumijevanje obavijesti privatnosti čime se omogućava mjerenje kriterija prilagođenosti teksta ciljanoj skupini.

Prema podacima Državnog zavoda za statistiku iz Popisa stanovništva 2011. godine [240] većina populacije u Republici Hrvatskoj ima završeno srednjoškolsko obrazovanje tako da je referentni stupanj obrazovanja postavljen na 12 razreda pa su, stoga, i vrijednostima do 12 razreda dodijeljene ponderske vrijednosti pod-indikatora (0.5).

Na osnovu te dvije formule čitkosti postavljeni su pod-indikatori odrednice prikazani u Tablici 10.

Tablica 10 Indikatori i pod-indikatori odrednice razumljivosti

Indikator	**Pod-indikatori**	**Ponderske vrijednosti pod-indikatora**	**Suma pondera na indikatoru**
Jezik za pružanje informacija treba biti jasan i prilagođen	Informacije su pružene jasnim jezikom	0.50	1.0
	Jezik je prilagođen ciljnoj skupini	0.50	

Odrednica smislenosti, kao i odrednica razumljivosti, mjeri kvalitativna svojstva (kodiranja) teksta te je u ovom istraživanju izražena postotkom leksičke gustoće. Leksičkom gustoćom zapravo određuje se koliko je tekst smislen, odnosno koliko informacija, obavijesti nastoji prenijeti. Tekstovi veće gustoće deskriptivniji su i stoga sadrže više obavijesnosti.

Izlagački (ekspozitorni) tekstovi, poput vijesti, informativnih i tehničkih članaka imaju veću leksičku gustoću od fikcije, dok je za tekstove ne-fikcije postavljena gornja granica od 40% [245]. Nadalje, Berber-Sardinha [246] otkriva kako leksička gustoća može drastično varirati unutar jednog teksta, što je slučaj i kod politika privatnosti koje su tematski podijeljene u različite sekcije koje mogu biti različite u odnosu na diskurs. S jedne strane, kao donekle pravni dokumenti, imaju specifičnosti izlagačkih tekstova koji teže većoj leksičkoj gustoći, iznad 40%, dok s, druge strane, radi dijelova koji se u svojoj formi oslanjaju na nabrajanje, zadržavaju specifičnosti razgovornog jezika, a čiji rezultati pokazuju leksičku gustoću ispod 40%, a obilježeni su manjom zastupljenošću leksičkih riječi.

To potvrđuju i rezultati preliminarnog istraživanja provedenog u sklopu istraživanja nad politikama privatnosti tvrtki Microsoft [247] i Google [248] na 5 jezika u odnosu na različite sekcije dokumenta. Analiza provedena kroz proporciju broja različitih riječi u odnosu na ukupni broj riječi, odnosno pojavnica, pokazuje da dokumenti politika privatnosti sadrže više tematskih sekcija s nižim postotcima, odnosno s više nabrajanja, a rezultati su pokazali i da najveću leksičku gustoću u odnosu na druge jezike ima verzija na hrvatskom jeziku i to u slučaju dokumenata obje tvrtke.

Nadalje, spomenutim istraživanjem na hrvatskom jeziku provedena je i detaljnija analiza dokumenta kroz proporciju leksičkih riječi (leksema) u odnosu na ukupni broj riječi. Leksemi u hrvatskom jeziku definirani su kao punoznačne riječi ili punoznačnice, riječi koje imaju i gramatičko i leksičko značenje same po sebi te ne ovise o sintaktičkim vezama u kojima sudjeluju. To su sljedeće vrste riječi: imenice, glagoli, zamjenice, pridjevi, brojevi, prilozi.

Tijekom spomenute analize izdvojene su punoznačnice i u odnosu na ukupan broj riječi u dokumentima proračunate su prosječne vrijednosti politika privatnosti koje su ispod 40%. Usporedni prikaz rezultata gustoće Googleovih i Microsoftovih obavijesti o privatnosti na hrvatskom jeziku prikazan je u Tablici 11.

Tablica 11 Rezultati leksičke gustoće Googleovih i Microsoftovih obavijesti

	Analiza prema jezicima		**Detaljna analiza na hrvatskom jeziku**	
Sekcija	**Google**	**Microsoft**	**Google**	**Microsoft**
Kolekcija	36.82%	33.12%	25.57%	19.81%
Svrha	39.66%	33.46%	28.84%	22.37%
Izbor/kontrola	40.34%	30.64%	28.13%	21.14%
Dijeljenje	49.15%	47.64%	38.38%	35.92%
Sigurnost	63.13%	72.51%	56.47%	71.60%
Retencija	56.83%	52.33%	41.34%	42.24%
Specifično	45.82%	26.14%	36.73%	14.96%
Promjena politika	57.11%	67.70%	46.19%	54.54%
Prosjek	**48.61%**	**45.44%**	**37.71%**	**35.32%**

Nadalje, ista metodologija odnosa punoznačnica u odnosu na ukupan broj pojavnica je provedena prilikom ispitivanja dokumenata politika privatnosti javnih zdravstvenih ustanova gdje je na uzorku od 56 njih proračunata medijalna vrijednost od 46% sa percentilnim vrijednostima prikazanim u Tablici 12.

Tablica 12 Rezultati izračuna medijalne vrijednosti leksičke gustoće

Medijan		46.285
Percentilne vrijednosti	25	40.5525
	50	46.285
	75	51.9675

Izvor: IBM SPSS 25

Stoga je prilikom proračunavanja odrednice smislenosti postavljen indikator s vrijednostima pod-indikatora prikazan u Tablici 13.

Tablica 13 Indikatori i pod-indikatori odrednice smislenosti

Indikator	**Pod-indikatori**	**Ponderske vrijednosti pod-indikatora**	**Vrijednost indikatora**
Dokument nije prezasićen informacijama	Postotak leksičke gustoće je do 41%	1	0-1
	Postotak leksičke gustoće je između 41% i 52%	0.50	
	Postotak leksičke gustoće viši je od 52%	0	

Budući da preopterećenost informacijama može dovesti do kognitivnog zasićenja koje onda smanjuje mogućnost inferabilnosti, odnosno donošenje odluka i poduzimanje aktivnosti od strane pojedinca, tendencija prema nižim vrijednostima leksičke gustoće postavljena je kao parametar prema raspodjeli ponderskih vrijednosti.

4.1.1.3. Procedura prikupljanja podataka

Prilikom prikupljanja podataka pristupalo se dokumentima politika privatnosti koje su zadovoljile kriterije da postoji unificirani identifikator sadržaja dokumenta, neovisno jesu li iste prikazane kao hipertekst ili u nekom drugom obliku (pdf, doc i sl.), tijekom čega se bilježio broj interakcija potrebnih za pristup politikama privatnosti kao osnove za izračun koeficijenta zahtjeva pristupačnosti te se utvrđivalo je li zahtjev za slojevitošću prikaza sadržaja ispunjen (kroz podnaslove određenih sekcija dokumenata ili druge mogućnosti oblikovanja hiperteksta).

U narednom koraku istraživanja, tekst dokumenta preuzet je u cijelosti i kopiran u prazan dokument Word aplikacije u kojem se postavila jedinica daljnje analize: uklonjeni su

naslovi, a adrese elektroničke pošte te hiperpoveznice zamijenjene su s X kako ne bi utjecale na rezultate broja slogova te leksičku gustoću.

Nadalje, posredstvom opcije Wordcount, očitan je broj riječi te broj znakova (bez praznina), a broj rečenica brojan je „ručno“ od strane autorice, profesorice hrvatskog jezika i književnosti. Potom je tekst kopiran u računalni alat syllablecounter.org [249] dostupan na internetu, koji je odabran kao najpouzdaniji za proračun broja slogova nakon usporedbe rezultata ručnog brojenja te kroz usporedbu različitih računalnih programa za brojanje slogova u tekstu. Metodologija i rezultati odabira računalnog programa opisana je u Prilogu 4. disertacije. Nadalje, za pomoć pri analizi broja punoznačnica tekst je zatim kopiran i u alat za analizu teksta [250] kako bi se izdvojile pojavnice u odnosu na njihovu frekvenciju pojava u tekstu. Iz dobivenih rezultata izdvojene su punoznačnice te je njihov konačan broj zabilježen za daljnju analizu rezultata leksičke gustoće teksta.

Na tekstu u daljnjim koracima, metodom analize sadržaja, ispitivana je ispunjenost zahtjeva informativnosti kroz prisustvo kriterija definiranih u analitičkoj matrici, zatim ažuriranosti, u odnosu na postojanje datuma objave ili ažuriranja dokumenta te informacija o načinu obavještavanja ispitanika o izmjenama politika privatnosti u predmetnom dokumentu.

Nastavno, na temelju dobivenih rezultata broja slogova, riječi i rečenica, uporabom Flesch Reading Ease (FRE) formule za čitkost, izračunati su indeksi razumljivosti teksta, a modifikacijom tzv. Kincaid formule određen je i potreban broj razreda, odnosno razina školovanja ispitanika za razumijevanje obavijesti privatnosti, kao dva kriterija za ispitivanje zahtjeva razumljivosti dokumenta od strane pojedinaca. Nadalje, broj punoznačnica (leksema) stavljen je u omjer s ukupnim brojem riječi u tekstu kako bi se odredili rezultati vezani uz ispunjenost zahtjeva na odrednici smislenosti. Analiza je provođena u računalnom programu Excel korištenjem prilagođenih formule za hrvatski jezik [29].

Prikupljanje podataka na mrežnim stranicama javnih zdravstvenih ustanova provedeno je tijekom travnja i svibnja 2021. godine. Ista metodologija primijenjena je pri prikupljanju podataka na mrežnim stranicama privatnih zdravstvenih ustanova tijekom srpnja i kolovoza iste godine.

4.1.1.4. Validacija analitičke matrice

U nedostatku sličnih analitičkih matrica za mjerenje politika transparentnosti tijekom istraživanja provedena je konstrukcijska i sadržajna validacija analitičke matrice.

Iz sheme prikazane na Slici 3. sa stranice 49. vidljivo je da su sve odrednice dimenzija transparentnosti direktno operacionalizirane, odnosno svaka od njih je mjerena preko samo jednog indikatora, s različitim brojem pod-indikatora, dok je odrednica informativnosti mjerena kroz ukupno 14 indikatora. Kako bi se utvrdila konzistentnost odabranih 14 indikatora, odnosno pouzdanost instrumenta za mjerenje odrednice informativnosti, provedena je analiza pouzdanosti (Cronbachov alfa koeficijent pouzdanosti) i to na podacima prikupljenim na uzorku javnih institucija (n=56). Rezultati analize pouzdanosti nalaze se u Tablici 14.

Tablica 14 Analiza pouzdanosti informativnosti kod javnih zdravstvenih ustanova

Cronbachov alfa	Broj čestica (indikatora)
0.817	14

Izvor: IBM SPSS 25

Vrijednost Cronbachovog alfa koeficijenta 0.817 upućuje na vrlo dobru pouzdanost dijela analitičke matrice za mjerenje odrednice informativnosti. Nakon utvrđivanja visoke razine konzistencije ovog dijela analitičke matrice, a u svrhu povećanja uzorka, pristupilo se prikupljanju podataka o transparentnosti politika privatnosti privatnih zdravstvenih ustanova (n=96). Analiza pouzdanosti dijela analitičke matrice za mjerenje odrednice informativnosti ponovo je provedena samo na uzorku privatnih ustanova. Rezultati analize nalaze se u Tablici 15.

Tablica 15 Analiza pouzdanosti informativnosti kod privatnih zdravstvenih ustanova

Cronbachov alfa	Broj čestica (indikatora)
0.752	14

Izvor: IBM SPSS 25

Na ovom uzorku, procijenjena je nešto manja pouzdanost, no ona se još uvijek smatra vrlo dobrom.

Konačno, analiza pouzdanosti dijela analitičke matrice za mjerenje odrednice informativnosti provedena je na ukupnom uzorku javnih i privatnih ustanova, s rezultatima prikazanim u Tablici 16.

Tablica 16 Analiza pouzdanosti informativnosti kod svih zdravstvenih ustanova

Cronbachov alfa	Broj čestica (indikatora)
0.772	14

Izvor: IBM SPSS 25

Nadalje, budući da za validaciju analitičke matrice nije bilo moguće usporediti rezultate dobivene primjenom ove analitičke matrice za mjerenje informacijske transparentnosti politika privatnosti, jer rezultati dobiveni nekom drugom, sličnom analitičkom matricom koja bi mjerila informacijsku transparentnost politika privatnosti nisu dostupni, primijenjena je druga vrsta validacije, odnosno, uspoređeni su rezultati dimenzija vidljivosti i inferabilnosti dobiveni na 56 javnih zdravstvenih ustanova s onima dobivenima na 96 privatnih javnih ustanova, rezultati koje su opisani u odlomku 4.1.2.3. Pouzdanost dobivenih rezultata.

4.1.2. Druga faza: obrada i interpretacija podataka

Na temelju prikupljenih podataka u prethodnoj fazi, u nastavku istraživanja usmjerilo se prema interpretaciji podataka u odnosu na elemente informacijske transparentnosti kao zavisne i nezavisne varijable istraživanja.

4.1.2.1. Ekstrakcija dimenzija transparentnosti kao latentnih varijabli

Kako bi se pristupilo uspoređivanju rezultata obje dimenzije potrebno je bilo prije svega kroz faktorsku analizu definirati faktorske skorove, odnosno „izmjeriti“ vrijednost svake pojedine dimenzije transparentnosti u odnosu na postavljene odrednice.

U faktorsku analizu uključeno je stoga 6 manifestnih varijabli, odnosno 6 odrednica, za koje je teorijski prvotno bilo pretpostavljeno da čine dimenzije vidljivosti i inferabilnosti:

1. Odrednica informativnosti
2. Odrednica ažuriranosti — *Vidljivost*
3. Odrednica pristupačnosti
4. Odrednica razumljivosti
5. Odrednica smislenosti — *Inferabilnost*
6. Odrednica slojevitosti

Faktorska analiza provedena je metodom glavnih komponenti, prilikom koje je u prvom koraku ekstrahirana bazična solucija bez rotacije, zatim je primijenjena ortogonalna rotacija (*Varimax*) te u trećem koraku i kosa rotacija (*Direct Oblimin*).

U bazičnoj soluciji ekstrahirane su dvije dimenzije transparentnosti, odnosno latentne varijable, sa svojstvenom vrijednošću većom od 1. Prvim faktorom objašnjeno je 32,04% varijance, a drugim 19,34%, što čini ukupno 51.38% varijance objašnjene ovim modelom.

U Tablici 17 prikazane su saturacije manifestnih varijabli, koje predstavljaju faktorska opterećenja, i to: bez rotacije vektora, uz ortogonalnu rotaciju vektora, pod pretpostavkom da je korelacija između dimenzija jednaka nuli te uz kosu rotaciju vektora, pod pretpostavkom da je korelacija između dimenzija različita od nule.

Tablica 17 Faktorska opterećenja po provedenoj faktorskoj analizi

Rezultati faktorske analize – metoda glavnih komponenti						
Manifestna varijabla	**Bazična solucija**		***Varimax***		***Direct Oblimin***	
Komponenta (faktor)	1	2	1	2	1	2
Informativnost	0.811	-0.042	0.804	-0.114	0.806	-0.134
Ažuriranost	0.739	0.122	0.747	0.056	0.745	0.037
Pristupačnost	-0.112	0.493	-0.068	0.501	-0.081	0.503
Razumljivost	-0.238	0.631	-0.180	0.650	-0.198	0.654
Smislenost	0.181	0.708	0.243	0.689	0.225	0.683
Slojevitost	0.786	0.026	0.785	-0.044	0.786	-0.064

Izvor: IBM SPSS 25

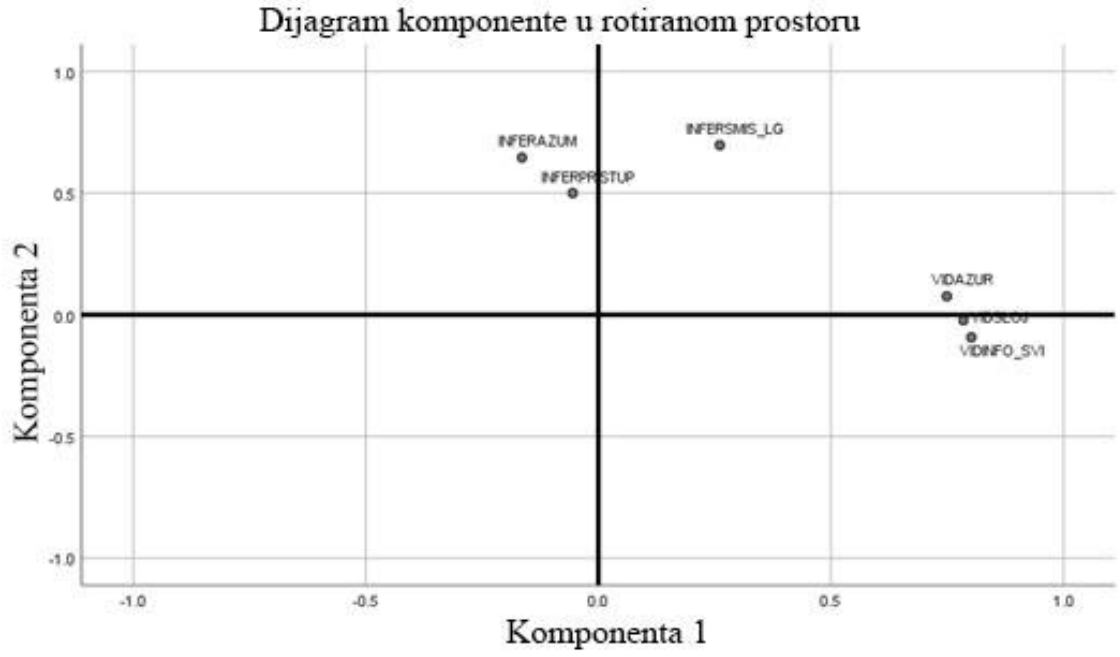
Iz Tablice 17 je vidljivo da su sve tri solucije dale vrlo slične rezultate, odnosno faktorska opterećenja su se neznatno promijenila u trenutku rotacije vektora. Na prvom faktoru sve tri varijable imaju visoke saturacije, dok na drugom faktoru samo jedna varijabla (odrednica smislenosti) ima vrlo visoku saturaciju, a preostale dvije nižu. Minimalna razlika u saturacijama između *Varimax* i *Direct Oblimin* solucije dovodi do zaključka da je korelacija između ovih

dviju latentnih varijabli, odnosno dimenzija transparentnosti, bliska nuli. Točnije, korelacija između dimenzija dobivena u *Direct Oblimin* soluciji je negativna i iznosi r=-0.052, što znači da korelacije između dimenzija *Vidljivost* i *Inferabilnost* nema (p=0.527).

Nadalje, iz Tablice 16 je također vidljivo da su odrednice dimenzija grupirane drugačije nego što je to bilo teorijski pretpostavljeno pa pripadnost odrednica na temelju rezultata analize dimenzijama vidljivosti i inferabilnosti izgleda ovako:

1. Odrednica informativnosti
2. Odrednica slojevitosti — *Vidljivost*
3. Odrednica ažuriranosti
4. Odrednica smislenosti
5. Odrednica razumljivosti — *Inferabilnost*
6. Odrednica pristupačnosti

Nadalje, faktorski skorovi na komponentama, dimenzijama vidljivosti i inferabilnosti, dobiveni faktorskom analizom, te njihove „grupacije“ prikazani su kao varijable u koordinatnom sustavu na Slici 12.



Slika 12 Grafički prikaz faktorskih opterećenja na ekstrahiranim komponentama
Izvor: IBM SPSS 25

Vrijednosti faktorskih skorova su standardizirane varijable s aritmetičkom sredinom nula i varijancom 1 te je njihova vrijednost pokazatelj pozicije koju pojedina ustanova na pojedinoj komponenti zauzima u odnosu na sve ostale rezultate – zdravstvene ustanove.

4.1.2.2. Definiranje dimenzija vidljivosti i inferabilnosti

Rezultat koji je određena ustanova dobila na dimenziji vidljivosti, dobivena je zbrajanjem rezultata odrednica informativnosti, ažuriranosti i pristupačnosti, koje su prethodno ponderirane faktorskim opterećenjima dobivenim faktorskom analizom, a primjenom ortogonalne Varimax rotacije na bazičnu soluciju. S obzirom na to da je odrednica informativnosti mjerena kroz 14 indikatora i da je potencijalan rezultat odrednice informativnosti mogao biti 14, dok je za odrednice slojevitosti i ažuriranosti maksimalan mogući rezultat 1. rezultat odrednice informativnosti prvo je podijeljen sa 14, nakon čega je ponderiran i pribrojen ponderiranim vrijednostima odrednica slojevitosti i ažuriranosti. Rezultat ustanove na dimenziji inferabilnosti dobiven je na isti način – zbrajanjem vrijednosti odrednica razumljivosti, smislenosti i pristupačnosti prethodno ponderiranih dobivenim faktorskim opterećenjima.

Na taj su način dimenzije vidljivosti i inferabilnosti definirane kao varijable s deskriptivnim karakteristikama na ukupnom uzorku javnih i privatnih zdravstvenih ustanova prikazanim u Tablici 18.

Tablica 18 Deskriptivne karakteristike uzorka javnih i privatnih zdravstvenih ustanova

	n	**Minimum**	**Maksimum**	**Aritmetička sredina**	**Standardna devijacija**	**Asimetrija**	**Zaobljenost**
Dimenzija vidljivosti	152	0.01	0.73	0.39	0.20	0.002	-0.893
Dimenzija inferabilnosti	152	0.06	0.61	0.29	0.10	0.305	0.657

Izvor: IBM SPSS 25

Kako bi se ispitale dodatne karakteristike ovako definiranih varijabli, odnosno dimenzija, nastavno je proveden Shapiro-Wilk test normalnosti distribucije. Nulta hipoteza

testa je odbačena (p=0.000), čime je izveden zaključak da se rezultati ovih dviju varijabli ne distribuiraju u skladu s normalnom distribucijom.

No, budući da su statistički testovi normalnosti distribucije izrazito rigorozni te nisu uvijek primjenjivi na podatke dobivene primjenom instrumenata mjerenja namijenjenih društvenim znanostima, u ocjeni normalnosti ovih distribucija primijenjen je „blaži“ kriterij koji kao bitne pokazatelje uzima u obzir koeficijente asimetrije (engl. *skewness*) i zaobljenosti (engl. *kurtosis*) distribucije [251][252][253][254], pa distribucija čiji je koeficijent asimetrije unutar raspona -3/+3, a koeficijent zaobljenosti manji od 10. može se smatrati bliskom normalnoj distribuciji. Stoga će i distribucije ovih dviju varijabli u daljnjim statističkim postupcima biti tretirane kao normalne distribucije.

4.1.2.3. Pouzdanost dobivenih rezultata

Usporedba deskriptivnih pokazatelja navedenih varijabli između javnih zdravstvenih ustanova i privatnih zdravstvenih ustanova napravljena je i u svrhu daljnje validacije analitičke matrice. Iako bi prava validacija zahtijevala postojanje druge, slične analitičke matrice i njenih rezultata na jednako definiranom uzorku, u spomenutom nedostatku takve matrice, razlika u obvezama prilikom objave politikama privatnosti između ovih dvaju tipova ustanova[15] te razlika u periodu prikupljanja podataka uzeta je kao određeni indikator nezavisnosti jednog i drugog mjerenja.

Deskriptivni pokazatelji dobiveni na varijablama koje predstavljaju dimenzije vidljivosti i inferabilnosti, zasebno na uzorku javnih zdravstvenih ustanova i privatnih zdravstvenih ustanova prikazani su u Tablici 19.

[15] Člankom 44. stavkom 2 Zakona o provedbi Opće uredbe o zaštiti podataka (NN 42/2018) Republike Hrvatske ograničava se izricanje upravne novčane kazne protiv pravne osobe s javnim ovlastima ili protiv pravne osobe koja obavlja javnu službu u smjeru da ista "ne smije ugroziti obavljanje takve javne ovlasti ili javne službe" čime se pri ispunjavanju regulatornih obaveza vezanih uz transparentnost praksi vezanih uz prikupljanje i obradu podataka može postaviti razlika između navedenih tipova institucija.

Tablica 19 Deskriptivne karakteristike uzorka zdravstvenih ustanova prema tipu institucije

	Ustanova	n	Minimum	Maksimum	Aritmetička sredina	Standardna devijacija	Asimetrija	Zaobljenost
Vidljivost	Javna	56	0.01	0.69	0.38	0.20	-0.361	-0.943
Vidljivost	Privatna	96	0.02	0.73	0.39	0.19	0.236	-0.862
Inferabilnost	Javna	56	0.06	0.61	0.28	0.11	0.376	0.300
Inferabilnost	Privatna	96	0.11	0.61	0.30	0.09	0.406	0.916

Izvor: IBM SPSS 25

Iz Tablice 19 je vidljivo da se deskriptivne karakteristike varijabli *Dimenzija vidljivosti* i *Dimenzija inferabilnosti* između poduzoraka vrlo malo razlikuju.

U svrhu testiranja razlike u prosjecima između ova dva poduzorka, prvo je testirana pretpostavka normalnosti distribucija provedbom Shapiro-Wilk testa, ovoga puta za svaki poduzorak zasebno. Nulta hipoteza testa je odbačena ($p=0.000$) za dimenzije inferabilnosti na oba poduzorka te na dimenziji vidljivosti na poduzorku privatnih zdravstvenih ustanova, a potvrđena je samo za dimenziju vidljivosti na poduzorku javnih zdravstvenih ustanova ($p=0.117$). Time je izveden zaključak da se rezultati ovih dviju varijabli ne distribuiraju u skladu s normalnom distribucijom u poduzorku privatnih ustanova, a u poduzorku javnih ustanova samo se vidljivost distribuira u skladu s normalnom distribucijom. S obzirom na ove rezultate analize, kao i u prethodnom slučaju primijenjen je „blaži kriterij“ raspona koeficijenata asimetrije i zaobljenosti manji od 10. te će se i distribucije ovih dviju varijabli/dimenzija u poduzorcima u daljnjim statističkim postupcima tretirati kao normalne distribucije.

Razlika u prosjecima poduzoraka na objema varijablama testirana je t-testom za nezavisne uzorke na razini signifikantnosti od 5% ($p<0.05$). Rezultati testa prikazani su u Tablici 20.

Tablica 20 Rezultati testa razlika u prosjecima poduzoraka

		Leveneov test jednakosti varijanci		t-test za nezavisne uzorke, razina signifikantnosti 5%				
		F	**p**	**t**	**df**	**p**	**Razlika u prosjecima**	**Standardna pogreška razlike**
Dimenzija vidljivosti	**Pretpostavka jednakih varijanci**	0.17	0.68	-0.09	150	0.926	-0.00307	0.033
	Pretpostavka nejednakih varijanci			-0.09	111.510	0.927	-0.003	0.033
Dimenzija inferabilnosti	**Pretpostavka jednakih varijanci**	3.73	0.06	-1.25	150	0.213	-0.020	0.016
	Pretpostavka nejednakih varijanci			-1.17	92.265	0.247	-0.020	0.018

Izvor: IBM SPSS 25

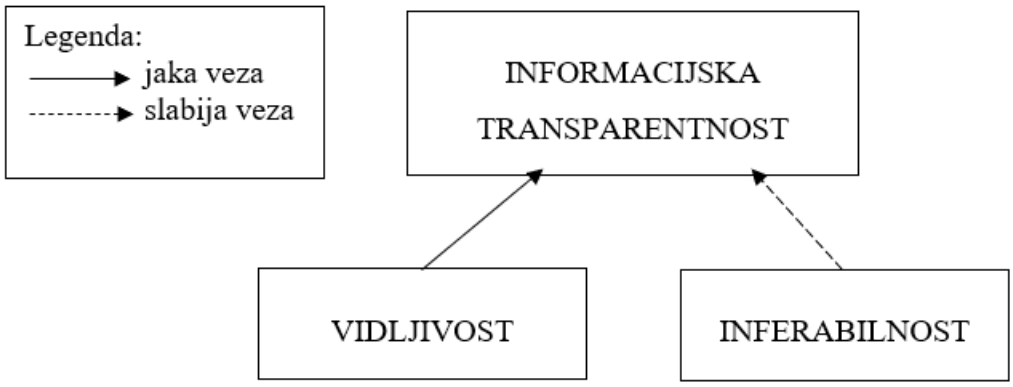
Iz tablice je vidljivo da su varijance poduzoraka homogene u objema dimenzijama (p=0.68; p=0.06) na razini rizika od 5%. Niti u jednoj dimenziji nije utvrđena statistički značajna razlika u prosjecima između poduzoraka, što znači da su rezultati prikupljeni analitičkom matricom na mrežnim stranicama javnih, a kasnije i privatnih zdravstvenih ustanova konzistentni.

4.1.3. Treća faza: dizajniranje modela

Iako je analizom rezultata u prethodnoj fazi istraživanja pokazano kako vrijednosti dimenzija *vidljivosti* i *inferabilnosti* ne koreliraju, svaka od njih se može postaviti i promatrati kao zasebna varijabla, odnosno konstrukt pri dizajniranju modela kojim se prikazuje utjecaj istih na rezultate informacijske transparentnosti, kao operacionalizirane jedinice mjerenja određenih stupnjeva informacijske simetrije.

Budući da je prilikom ekstrakcije dimenzija vidljivosti i inferabilnosti kao latentnih varijabla provedena dvofaktorska analiza kojom se utvrđuje koliko vrijednosti svake od dimenzija doprinose objašnjenju varijance tog dvofaktorskog modela, rezultati iste se mogu upotrijebiti kao vrijednosti konstrukata pojedinih dimenzija u odnosu na rezultate informacijske

transparentnosti. U apsolutnom smislu „udio“ dimenzije vidljivosti iznosi 32.04%, a inferabilnosti 19.34%, što zajedno čini 51.38% varijance objašnjene postavljenim dvofaktorskim modelom. Odnosno, u relativnom smislu, ako se postavi objašnjena varijanca kao 100%, onda joj vidljivost doprinosi 62.36%, a inferabilnost 37.64%.



Slika 13 Model udjela pojedinih dimenzija na informacijsku transparentnost

Slikom 13 prikazan je konceptualni model utjecaja pojedinih dimenzija transparentnosti, *vidljivosti* i *inferabilnosti*, na rezultate informacijske transparentnosti. Budući da rezultati odrednica na dimenziji vidljivosti u većoj mjeri utječu na povećanje ili smanjenje informacijske transparentnosti relacija je označena punom oznakom relacije u odnosu na dimenziju inferabilnosti čija je relacija označena isprekidanom oznakom.

Nadalje, rezultati provedene metode glavnih komponenti tijekom faktorske analize pokazuju faktorska opterećenja svake pojedine odrednice, odnosno njihov „utjecaj“ pri definiranju rezultata pojedine dimenzije transparentnosti te se mogu promatrati kao konstrukti pri daljnjoj izgradnji modela.

Prema rezultatima Varimax rotacije, a koja je odabrana kao najkorektnija za ponderiranje[16], saturacije faktora na dimenziji vidljivosti prikazane su u Tablici 21.

[16] Budući da su saturacije odrednica na svakom pojedinom faktoru bile vrlo slične u sve tri faktorske analize (bazična solucija, uz ortogonalnu rotaciju (Varimax) i uz kosu rotaciju (Direct Oblimin)), u svrhu ponderiranja uzete su saturacije dobivene u faktorskoj analizi u kojoj je primijenjena ortogonalna rotacija. Razlog tome je da se bazična solucija rijetko kada uzima kao finalna, zbog toga što bilo koja vrsta rotacije obično bolje rasporedi varijable po vektorima. Varimax rezultati, a ne Direct Oblimin, uzeti su zbog toga što Direct Oblimin daje najbolje rezultate kad postoji korelacija između dimenzija, što je testirano u prethodnim analizama i vidjelo se da to nije slučaj.

Tablica 21 Faktorska opterećenja odrednica na dimenziji vidljivosti

Odrednica	Faktorsko opterećenje
Informativnost	0.80
Slojevitost	0.79
Ažuriranost	0.75

Iz dobivenih rezultata moguće je zaključiti da zahtjevi informativnosti najviše utječu na rezultate u dimenziji vidljivosti, što je očekivano, budući da se taj indikator jedini sastoji od najviše pod-indikatora (njih 14) u odnosu na ostale indikatore. Nadalje, u nešto manjoj mjeri na rezultate u dimenziji utječu zahtjevi za slojevitošću prikaza teksta, dok najmanje utječe ažuriranost, odnosno objava datuma te načina informiranja ispitanika prilikom izmjena politika privatnosti.

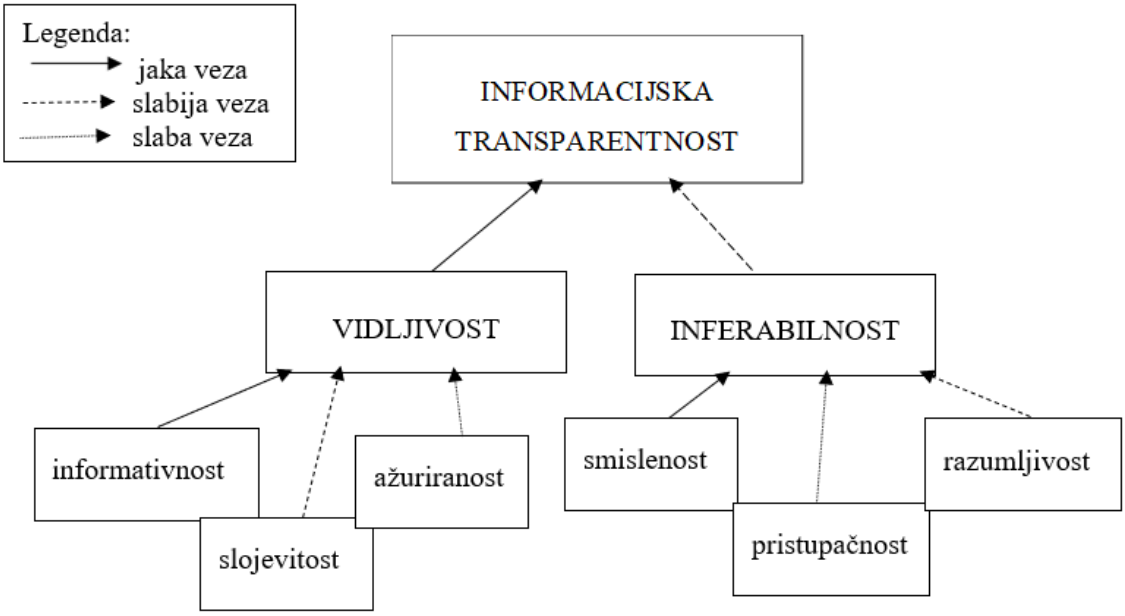
Na dimenziji inferabilnosti utjecaj pojedinih zahtjeva je raspoređen tako da na rezultate najviše utječe zahtjev smislenosti, odnosno rezultata leksičke gustoće kao pokazatelja obavijesnosti teksta u odnosu na informacijsko zasićenje, a zatim zahtjev pristupačnosti, ogledan u broju interakcija do teksta politika privatnosti te, naposljetku, zahtjeva razumljivosti kao pokazatelja kvalitete i prilagođenosti jezika kojim se pružaju informacije u odnosu na ciljnu skupinu. Prikaz saturacija pojedinih odrednica na dimenziji inferabilnosti prikazan je kroz Tablicu 22.

Tablica 22 Faktorska opterećenja odrednica na dimenziji inferabilnosti

Odrednica	Faktorsko opterećenje
Smislenost	0.69
Razumljivost	0.65
Pristupačnost	0.50

Primjenom metode modeliranja [255] nastavno na postavljeni model udjela pojedinih dimenzija na informacijsku transparentnost moguće je izgraditi konceptualni model prikaza utjecaja pojedinih odrednica na dimenzije transparentnosti kao konstrukata modela, prikazan na Slici 14.

Slika 14 Model udjela odrednica transparentnosti na informacijsku transparentnost



Na dimenziji vidljivosti najveći utjecaj na rezultate informacijske transparentnosti ima odrednica informativnosti, a zatim slojevitosti pa ažuriranosti, dok na dimenziji inferabilnosti najviši je faktorski skor „postigla“ odrednica smislenosti, nešto niži odrednica razumljivosti, a najniži odrednica pristupačnosti.

4.2. Validacija modela

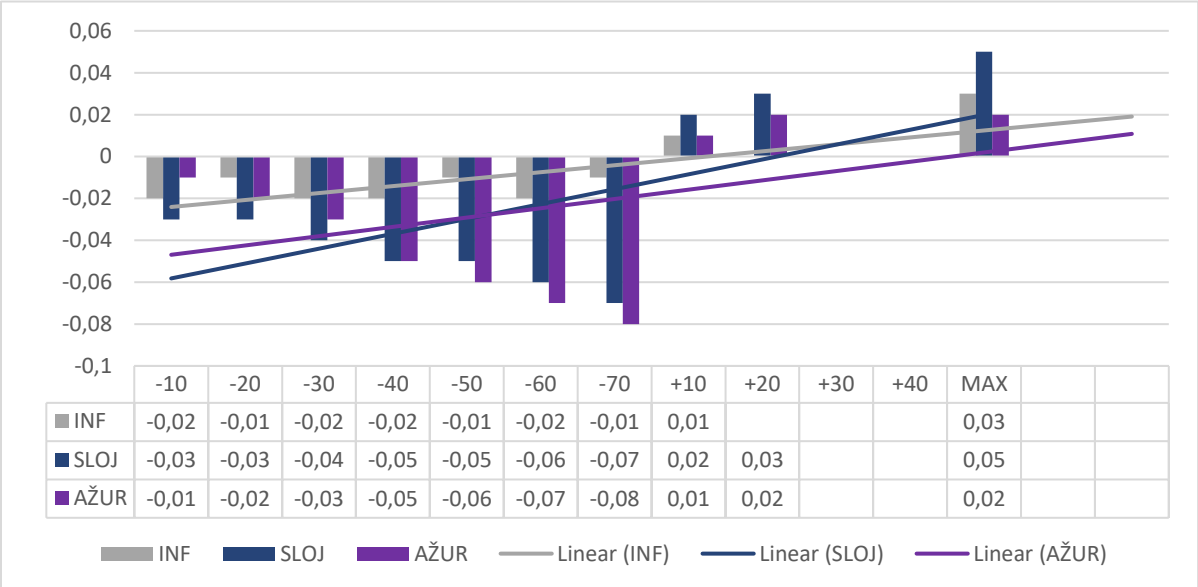
Budući da rezultati predstavljeni konceptualnim modelom u svome međusobnom odnosu predstavljaju utjecaj pojedine odrednice i dimenzije transparentnosti na cjelokupni rezultat informacijske transparentnosti pojedine ustanove, kao mjere učinkovitosti mehanizma transparentnosti, isti mogu biti usmjereni prema ispitivanju politika privatnosti u odnosu na ispunjene zahtjeve na pojedinim odrednicama dimenzija transparentnosti u ovisnosti prema njihovom utjecaju na ukupni rezultat informacijske (a)simetrije. Stoga i rezultat informacijske (a)simetrije kao zavisne varijable u odnosu na analizu varijanci postavljenih faktorskih opterećenja na obje dimenzije transparentnosti može biti ispitivan s ciljem testiranja pomoćnih hipoteza dobivenih postavljenim modelom.

U odnosu na dobiveni prosjek svih ustanova na dimenziji vidljivosti, koji iznosi 0.39, moguće je izdvojiti sljedeće pomoćne hipoteze:

- na informacijsku transparentnost dimenzije vidljivosti u najvećoj mjeri utječu zahtjevi informativnosti,
- na informacijsku transparentnost dimenzije vidljivosti u većoj mjeri utječu zahtjevi slojevitosti nego ažuriranosti,
- na informacijsku transparentnost dimenzije vidljivosti u najmanjoj mjeri utječu zahtjevi ažuriranosti.

Provedbom analize valjanosti podudaranja (eng. Goodness-of-Fit) u odnosu na referentne rezultate postavljenog prosjeka moguće je odrediti odstupanja od rezultata u odnosu na izmjene pojedinih varijanci faktorskih opterećenja nad prikupljenim podacima ispunjenosti zahtjeva politika privatnosti zdravstvenih ustanova.

Na Slici 15 prikazani su rezultati odstupanja vrijednosti na svakoj od odrednica u odnosu na referentnu prosječnu vrijednost svih ustanova na dimenziji vidljivosti. Faktorska opterećenja na svakoj od odrednica dimenzija vidljivosti postupno su umanjivana pa uvećavana od referentne vrijednosti za 10 u svakom koraku (do maksimalne vrijednosti od 1) kako bi se očitala prosječna vrijednost svih ustanova u odnosu na promijenjene vrijednosti, a koje su potom stavljene u odnos prema referentnoj vrijednosti od 0.39.



	-10	-20	-30	-40	-50	-60	-70	+10	+20	+30	+40	MAX		
INF	-0,02	-0,01	-0,02	-0,02	-0,01	-0,02	-0,01	0,01				0,03		
SLOJ	-0,03	-0,03	-0,04	-0,05	-0,05	-0,06	-0,07	0,02	0,03			0,05		
AŽUR	-0,01	-0,02	-0,03	-0,05	-0,06	-0,07	-0,08	0,01	0,02			0,02		

Slika 15 Graf odstupanja vrijednosti na dimenziji vidljivosti
Izvor: autorica

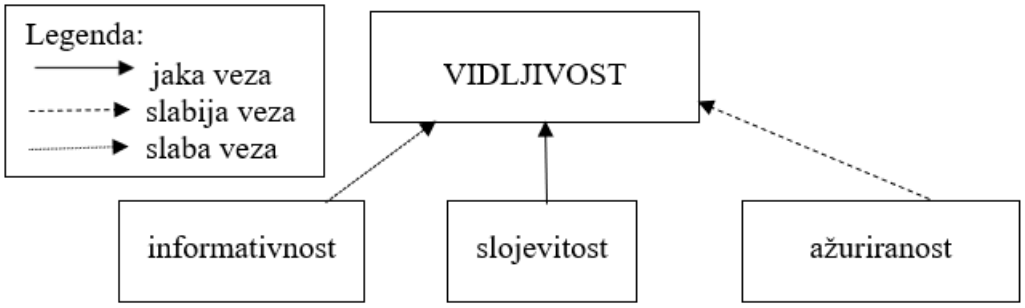
Prema prikazanim rezultatima uočljivo je kako rezultati na odrednici informativnosti ne pokazuju najveća odstupanja od referentne vrijednosti, što upućuje na odbijanje pomoćne

hipoteze kako zahtjevi odrednice informativnosti u najvećoj mjeri utječu na informacijsku transparentnost dimenzije vidljivosti budući da bi svaka, i najmanja, promjena faktorskih opterećenja trebala imati najveći utjecaj na rezultate informacijske transparentnosti u odnosu na faktorska opterećenja drugih odrednica.

Zatim, tvrdnju da na informacijsku transparentnost dimenzije vidljivosti u većoj mjeri utječu zahtjevi slojevitosti nego ažuriranosti moguće je potvrditi, budući da je uočljiv trend prevalencije razlika od referentne vrijednosti upravo na odrednici slojevitosti, dok je tvrdnju da na informacijsku transparentnost dimenzije vidljivosti u najmanjoj mjeri utječu zahtjevi ažuriranosti moguće opovrgnuti, budući da najmanji utjecaj na promjenu rezultata imaju zapravo zahtjevi odrednice informativnosti.

Stoga nakon provedene analize valjanosti podudaranja predloženi model na dimenziji vidljivosti bi trebao odražavati udjele pojedinih odrednica dimenzije vidljivosti na informacijsku transparentnost prikazane na Slici 16.

Odnosno, na dimenziji vidljivosti najveći utjecaj na rezultate informacijske transparentnosti ima odrednica slojevitosti, zatim ažuriranosti te, naposlijetku, informativnosti.



Slika 16 Model udjela odrednica vidljivosti po analizi valjanosti podudaranja

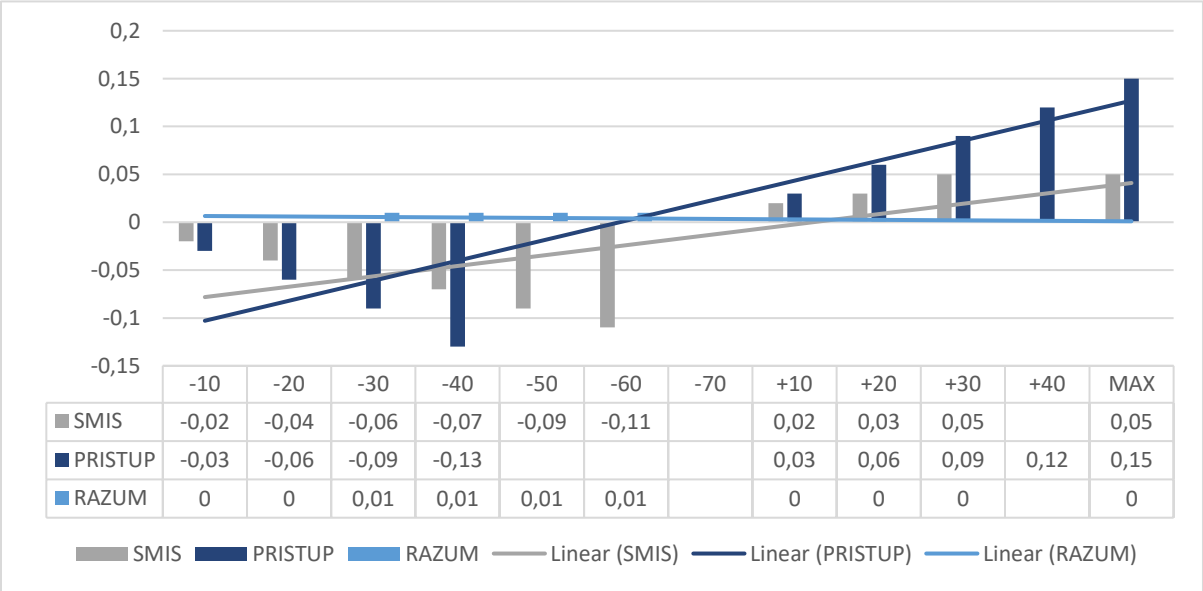
Nadalje, na temelju predloženog modela na dimenziji inferabilnosti u odnosu na dobiveni prosjek svih ustanova na dimenziji inferabilnosti, koji iznosi 0.29, moguće je izdvojiti sljedeće pomoćne hipoteze:

- na informacijsku transparentnost dimenzije inferabilnosti u najvećoj mjeri utječu zahtjevi smislenosti,
- na informacijsku transparentnost dimenzije inferabilnosti u većoj mjeri utječu zahtjevi razumljivosti nego pristupačnosti,

- na informacijsku transparentnost dimenzije inferabilnosti u najmanjoj mjeri utječu zahtjevi pristupačnosti.

Koristeći istu metodu postupnog smanjivanja i uvećavanja faktorskih opterećenja na svakoj od odrednica dimenzija inferabilnosti te računanja odstupanja vrijednosti u odnosu na zadanu referentnu prosječnu vrijednost svih ustanova na dimenziji inferabilnosti moguće je odrediti utjecaj pojedinih faktorskih odrednica na informacijsku transparentnost. Rezultati su prikazani na Slici 17.

Iz dobivenih rezultata moguće je zaključiti kako odrednica razumljivosti u najmanjoj mjeri utječe na rezultate informacijske transparentnosti, dok u najvećoj mjeri na njih utječe odrednica pristupačnosti, a ne smislenosti, kako je pretpostavljeno predloženim prvotnim modelom.



	-10	-20	-30	-40	-50	-60	-70	+10	+20	+30	+40	MAX
SMIS	-0,02	-0,04	-0,06	-0,07	-0,09	-0,11		0,02	0,03	0,05		0,05
PRISTUP	-0,03	-0,06	-0,09	-0,13				0,03	0,06	0,09	0,12	0,15
RAZUM	0	0	0,01	0,01	0,01	0,01		0	0	0		0

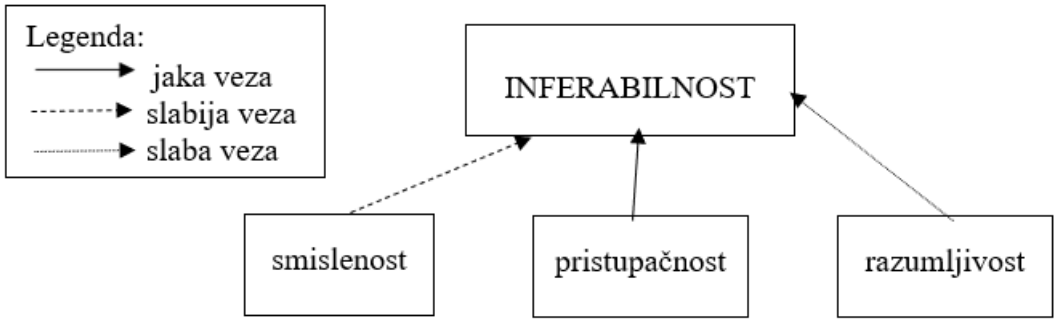
Slika 17 Graf odstupanja vrijednosti na dimenziji inferabilnosti
Izvor: autorica

Iz dobivenih rezultata također je moguće zaključiti i kako odrednica pristupačnosti u najvećoj mjeri utječe na informacijsku transparentnost dimenzije inferabilnosti, što dovodi do odbijanja pomoćne hipoteze prvotno postavljenim modelom da na informacijsku transparentnost dimenzije inferabilnosti u najvećoj mjeri utječu zahtjevi smislenosti.

Ipak, što se tiče odnosa između odrednica pristupačnosti i razumljivosti, moguće je opovrgnuti pomoćnu hipotezu da na informacijsku transparentnost dimenzije inferabilnosti u

većoj mjeri utječu zahtjevi razumljivosti nego pristupačnosti, kao i tvrdnju da na informacijsku transparentnost dimenzije inferabilnosti u najmanjoj mjeri utječu zahtjevi pristupačnosti.

Posljedično, nakon provedene analize valjanosti podudaranja predloženi model na dimenziji inferabilnosti bi trebao odražavati udjele pojedinih odrednica dimenzije inferabilnosti na informacijsku transparentnost prikazane na Slici 18. odnosno, na dimenziji inferabilnosti najveći utjecaj na rezultate informacijske transparentnosti ima odrednica pristupačnosti, zatim smislenosti te, naposlijetku, razumljivosti.



Slika 18 Model udjela odrednica inferabilnosti po analizi valjanosti podudaranja

No, s obzirom na to da se analiza provodila na uzorku koji se sastojao od dijelom javnih i dijelom privatnih zdravstvenih ustanova, usporedbom kojih je i validirana analitička matrica, nad dobivenim rezultatima moguća je daljnja deskriptivna analiza u svrhu stjecanja uvida u specifičnosti pojedinog seta ustanova.

4.3. Rezultati sporednih analiza nad uzorkom

U odnosu na proračunati referentni prosjek svih ustanova na dimenziji inferabilnosti izdvojeno je 46 ustanova koje su ostvarile rezultate iznad prosjeka, dok je na dimenziji vidljivosti njih 76, što ujedno korespondira s tvrdnjom da odrednice na dimenziji vidljivosti u većoj mjeri doprinose smanjenju informacijske asimetrije od onih na dimenziji inferabilnosti.

Na dimenziji vidljivosti najviši prosječni rezultat izdvojenih ustanova se očituje u indikatoru slojevitosti (0.96) pa na indikatoru informativnosti (0.58), a zatim na indikatoru ažuriranosti (0.56). Odrednica slojevitosti, može poprimiti tri vrijednosti u zadovoljavanju ispunjenosti kriterija: 0, 0.5 i 1. Modus ili dominantna vrijednost na uzorku ustanova koje su

postigle rezultate iznad prosjeka, kao i na cjelokupnom uzorku (n=152) je 1. što ukazuje na učestalost ispunjavanja tog zahtjeva kod zdravstvenih ustanova.

Nadalje, odrednica informativnosti, koja se „mjerila“ u odnosu na ispunjavanje 14 zahtjeva različitih u broju postavljenih kriterija, odnosno indikatora, u cjelokupnom uzorku zauzima vrijednosti od 0.04 (minimum) do 0.88 (maksimum) s dominantnom vrijednošću od 0.50, a koja je tek neznatno viša (0.51) u skupu ustanova koje imaju iznadprosječne rezultate (n=76).

Na odrednici ažuriranosti ustanova može postići rezultate ispunjenosti zahtjeva u odnosu na dva kriterija koji nisu bili jednako ponderirani, pa su moguće vrijednosti: 0, 0.25, 0.50 i 1. Dominantna vrijednost na uzorku svih ustanova (n=152) je 0, odnosno veliki broj ustanova nije zadovoljio niti jedan od postavljenih kriterija. Štoviše, 16 (21%) ili više od 1/5 ustanova koje su postigle rezultate iznad prosjeka nije postiglo nikakav rezultat na ovome zahtjevu što sugerira da ustanove u velikoj mjeri ne datiraju svoje dokumente politika privatnosti, niti pružaju informacije o načinu obavještavanja ispitanika o izmjenama politika privatnosti. Ipak kao dominantna vrijednost kod spomenutih ustanova je 1. budući da je taj zahtjev ispunilo 28 (36%) ustanova. Inače, samo 13 ustanova u cijelom uzorku (n=152) datiralo je svoje politike privatnosti, dok je praksa informiranja o načinu obavještavanja ispitanika o izmjenama politika privatnosti češća, no samo kod 35 ustanova u odnosu na cijeli uzorak.

Nadalje, od 76 ustanova koje su postigle rezultate iznad prosjeka većina njih (45) je u privatnom vlasništvu, dok je 31 ustanova iz sustava javnog zdravstva. Struktura ustanova javnih ustanova prema razini zdravstvene zaštite prikazana je u Tablici 23.

Tablica 23 Razine javnih ustanova iznad prosjeka na dimenziji vidljivosti

Razina ustanove	**Učestalost**
Sekundarna	15
Specijalna bolnica	6
Lječilište	1
Opća bolnica	3
Poliklinika	5
Primarna	10
Dom zdravlja	5
Županijski zavod za hitnu medicinu	5
Tercijarna	5
Klinika	2
Klinički bolnički centar	3
Zavod	1

Nadalje, na dimenziji inferabilnosti najviši prosječni rezultat se očituje u indikatoru pristupačnosti (0.93) pa na indikatoru smislenosti (0.53), a zatim na indikatoru razumljivosti (0.04), što korespondira s rezultatima validacije modela.

Što se tiče odrednice pristupačnosti, odnosno broja interakcija potrebnih za pristup politikama privatnosti, najviše ustanova, njih 127 (83%) ispunilo je zahtjev koji je postavljen u odnosu na referentnu vrijednost od 2. Kod 21 ustanove (14%) potrebno je tri interakcije, dok je najveći broj interakcija, njih 6, potrebno za pristup do politika privatnosti kod jedne (javne) ustanove.

Odrednica smislenosti, koja je izražena izračunom leksičke gustoće teksta, može poprimiti tri vrijednosti u zadovoljavanju ispunjenosti kriterija: 0, 0.5 i 1. Modus ili dominantna vrijednost na ukupnom uzorku ustanova je 0.5, čime se ukazuje da je najčešći postotak leksičke gustoće između 41% i 52%, dok je dominantna vrijednost leksičke gustoće kod ustanova koje su postigle rezultate iznad prosjeka (n=46) 1, odnosno ispod 41%, čime se ukazuje pozitivan trend prema smanjenju zasićenja informacijama pri izradi dokumenta politika privatnosti.

Rezultati na području razumljivosti teksta, ogledani kroz formule čitkosti, ukazuju na poražavajuće razine prilagođenosti teksta ciljanoj skupini. Na ukupnom uzorku ustanova (n=152) taj zahtjev, na oba kriterija, u odnosu na vrijednosti FRE indeksa razumljivosti teksta te potrebnog broj razreda, odnosno razine školovanja ispitanika za razumijevanje obavijesti privatnosti, ispunilo je samo 4 (0.02%) ustanove. Jednaki broj ustanova ostvario je rezultate od 0.5, i to u kriteriju potrebne razine školovanja. Budući da se radi o modifikaciji formula čitkosti, ustanove koje su postigle dovoljnu razinu FRE indeksa, ujedno su i zadovoljile kriterij potrebne razine školovanja ispitanika za razumijevanje teksta pa se ukupni broj ustanova koji je djelomično ili u potpunosti zadovoljio postavljeni zahtjev da jezik za pružanje informacija treba biti jasan i prilagođen svodi na 8.

Nadalje, i kod 46 ustanova koje su postigle rezultate iznad prosjeka većina njih (28) je u privatnom vlasništvu, dok je 18 ustanova iz sustava javnog zdravstva. Struktura ustanova javnih ustanova prema razini zdravstvene zaštite prikazana je u Tablici 24.

Tablica 24 Razine javnih ustanova iznad prosjeka na dimenziji inferabilnosti

Razina ustanove	**Učestalost**
Sekundarna	12
Specijalna bolnica	8
Lječilište	1
Opća bolnica	2
Poliklinika	1
Primarna	4
Dom zdravlja	2
Županijski zavod za hitnu medicinu	2
Tercijarna	2
Klinička bolnica	1
Klinički bolnički centar	1

Dobiveni rezultati, diskutirani u narednom poglavlju, mogu pružiti vrijedne spoznaje u istraživačkom kontekstu vrjednovanja zahtjeva transparentnosti te pružiti osnovu za daljnja istraživanja.

5. RASPRAVA O REZULTATIMA ISTRAŽIVANJA

Iako se provedbom faktorske analize nad prikupljenim rezultatima pokazalo kako dvije dimenzije, *vidljivost* i *inferabilnost* nisu u korelaciji, odnosno da je korelacija između ovih dviju latentnih varijabli (dimenzija) bliska nuli, suprotno teorijskoj pretpostavci, obje dimenzije moguće je obrađivati kao zasebne varijable, odnosno konstrukte transparentnosti u odnosu na informacijsku transparentnost, kako je i sugerirano predloženim konceptualnim modelom.

5.1. Diskusija hipoteza istraživanja

Primjenom metoda deskriptivne statistike na dobivene rezultate moguća je i daljnja analiza nad indikatorima dimenzija transparentnosti usmjerena na tumačenje rezultata ispitivanja s obzirom na stupnjeve informacijske (a)simetrije, ujedno pretpostavljene u H1.

Iz prikupljenih rezultata o ispunjenosti zahtjeva na pojedinim odrednicama izračunati su prosječni rezultati svake pojedine ustanove na dimenziji vidljivosti i dimenziji inferabilnosti, prilikom čega su rezultati ustanova na svakoj odrednici ponderirani su faktorskim opterećenjem (saturacijom) koju je odrednica imala u faktorskoj analizi. Na taj način dobiveni faktori pojedinih dimenzija odražavaju „važnost“, odnosno utjecaj svake od odrednica na dimenziji. Drugim riječima, svaka odrednica dimenzije vidljivosti sudjeluje u prosječnom rezultatu upravo onoliko kolika je njezina važnost u cijeloj dimenziji vidljivosti, a svaka odrednica dimenzije inferabilnosti sudjeluje u prosječnom rezultatu također onoliko kolika je njena važnost u cijeloj dimenziji inferabilnosti.

Nadalje, kroz izračunati prosjek svih zdravstvenih ustanova (n=152) moguće je odrediti nadalje i prosječni rezultat za svaku pojedinu dimenziju transparentnosti kao stupnjeva faktora vidljivosti inferabilnosti na obrađenom uzorku.

Tako prosjek svih ustanova na dimenziji vidljivosti iznosi 0.39, dok na inferabilnosti 0.29, čime je zapravo izračunat prosjek zadovoljavanja postavljenih zahtjeva ustanova pri postizanju informacijske simetrije. Odnosno, iz dobivenih rezultata moguće je izračunati stupanj informacijske asimetrije kao razliku, odnosno otklon dobivenih rezultata od apsolutne simetrije koja se postavlja kao 1.

Prema tome, stupanj asimetrije je moguće izračunati primjenom sljedeće formule:

stupanj asimetrije = 1 – stupanj simetrije

gdje se kao umanjenik postavlja apsolutna simetrija, a kao umanitelj postignuti rezultat simetrije pojedinih ustanova.

Time se zadovoljava i potvrđuje tvrdnja iz H1: „pomoću stupnjeva faktora vidljivosti i inferabilnosti moguće je odrediti stupanj informacijske asimetrije“. **Hipoteza H1 je potvrđena.**

Nadalje, pretpostavku „na stupanj informacijske asimetrije značajnije utječu faktori vidljivosti u odnosu na faktore inferabilnosti“ oblikovanu u H2, moguće je zaključiti i potvrditi interpretacijom rezultata pri provođenju faktorske analize nad dimenzijama vidljivosti i inferabilnosti kojima je objašnjeno 51.38% varijance nad istraživanim uzorkom, pri čemu udjelu od 32.04% doprinose faktori vidljivosti, a 19.34% inferabilnosti, odnosno, uzevši ukupnu objašnjenu varijancu kao apsolutnu vrijednosti (100%), onda joj *vidljivost* doprinosi 62.36%, a *inferabilnost* 37.64%. **Hipoteza H2 je potvrđena.**

Postavljeni omjeri uzeti su kao osnova za izgradnju predloženog modela vrjednovanja informacijske transparentnosti politika privatnosti. No, je li „primjenom dizajniranog modela moguće procijeniti informacijsku transparentnost politika privatnosti“, kako je pretpostavljeno u H3?

U odnosu na rezultate faktorskih opterećenja odrednica na obje dimenzije, a na temelju kojih je postavljen ishodišni modela vrjednovanja informacijske transparentnosti, te rezultata validacije kroz analizu valjanosti podudaranja nije moguće zaključiti da je primjenom ishodišnog modela moguće procjenjivati informacijsku transparentnost politika privatnosti te je pretpostavku oblikovanu kao H3 potrebno opovrgnuti**. Hipoteza H3 je pobijena.**

5.2. Elaboracija doprinosa istraživanja

Ipak, dodatne analize provedene nad prikupljenim podacima nude vrijedne uvide utjecaja pojedinih faktora na informacijsku transparentnost. Uzimajući u obzir rezultate koje su „postigle“ zdravstvene ustanove iznad definiranog prosjeka kao studiju slučaja u odnosu na

parametre dobivene modelom moguće je izdvojiti određene smjernice u izradi politika privatnosti ka povećanju transparentnosti.

Na dimenziji vidljivosti, prema teorijskoj pretpostavci usmjerenoj prvenstveno na sadržajnu determinantu transparentnosti, a kojom se odražava stupanj cijelosti informacija, uočljiva je dominantna vrijednost od 0.5 pri ispunjavanju 14 definiranih zahtjeva informativnosti, što sugerira da je većina zdravstvenih ustanova pružila djelomične informacije vezano uz prakse obrade podataka definirane u Republici Hrvatskoj važećim regulatornim okvirom Opće uredbe o zaštiti podataka. Nadalje, pružanje informacija o načinu obavještavanja ispitanika o izmjenama politika privatnosti kao jedan, ne nužni, zahtjev kojim se povećava mogućnost kontrole ispitanika nad svojim podacima, prevladava u odnosu na datiranje politika privatnosti kao dokumenata s pravnim karakteristikama. S obzirom na te dvije odrednice moguće je ocijeniti stupanj cijelosti informacija u navedenom uzorku.

Vezano uz odrednice kojima se ispituju lingvističke karakteristike teksta kao mjere učinkovitosti samog mehanizma transparentnosti i u odnosu na signal komunikacije, smislenost i razumljivost, rezultati pokazuju kako oblikovanje tekstova s ciljem smanjenja zasićenja informacijama ima veći utjecaj na inferabilnost pojedinaca od prilagođavanja teksta prema mogućnostima razumijevanja ciljne skupine. Iako je prvim stavkom Članka 12. Opće uredbe o zaštiti podataka postavljeni zahtjev da informacije u vezi s obradom podataka „trebaju biti pisane uz uporabu jasnog i jednostavnog jezika“ [45], rezultati pokazuju nisku tendenciju zadovoljavanja istog od strane uzorkovanih zdravstvenih ustanova.

Ipak, rezultati odrednica slojevitosti i pristupačnosti izdvojeni kao faktori s najviše utjecaja na smanjenje informacijske (a)simetrije prilikom validacije modela izdvajaju se i kao primjeri „dobre prakse“ kod ispitivanog uzorka što se može sagledati i u odnosu na sastav uzorka. Budući da među zdravstvenim ustanovama koje su postigle rezultate iznad prosjeka prevladavaju one u privatnom vlasništvu, tendenciju za zadovoljavanjem zahtjeva vezanih uz zaštitu privatnosti korisnika moguće je tumačiti u odnosu na težnje izgradnje odnosa povjerenja s pojedincima, postavljajući zaštitu podataka i privatnost kao dodatnu vrijednost, uz već postojeće usluge s kojima se ustanova natječe na tržištu. Nadalje, na osnovu drugog stavka Članka 44. Zakona o provedbi Opće uredbe o zaštiti podataka [256] na teritoriju Republike Hrvatske određeno je da „ako se upravna novčana kazna izriče protiv pravne osobe s javnim ovlastima ili protiv pravne osobe koja obavlja javnu službu, izrečena upravna novčana kazna

ne smije ugroziti obavljanje takve javne ovlasti ili javne službe“, čime se u nešto „nepovoljniji“ položaj stavljaju pravne službe u privatnom sektoru koje su stoga „motiviranije“ za ispunjavanje regulatornih odredbi. Također, pokazatelji o kršenju odredaba na temelju Opće uredbe o zaštiti podataka pokazuju da je, kako u iznosu, tako i u samom broju izrečenih kazni, najviše organizacija iz privatnog sektora gospodarstva [257].

U tom kontekstu se može sagledati i tendencija prema što manjem broju interakcija potrebnih za pristup politikama privatnosti na mrežnim stranicama privatnih zdravstvenih ustanova u odnosu na one javnih ustanova, a koje objavu dokumenata politika privatnosti sagledavaju kao još jedan od zahtjeva za sukladnost, u relativnom položaju sa regulatornim obavezama iz drugih područja. Pa tako je i najveći broj interakcija, čak 6, zabilježen upravo kod ustanove iz javnog sektora zdravstvene zaštite.

Odrednice slojevitosti i pristupačnosti ujedno predstavljaju faktore s najviše utjecaja na informacijsku transparentnost s obzirom na rezultate provedene validacije modela. Time se mogu sagledavati i kao primarni zahtjevi, odnosno preduvjeti za daljnje kvalitativne karakteristike mehanizama transparentnosti koji se izražavaju kroz pružanje potrebnih informacija (ažuriranost, informativnost) i to u obliku koji je usmjeren na ispitanika (smislenost, razumljivost) kao sekundarnih zahtjeva u životnom ciklusu mehanizama transparentnosti.

6. ZAKLJUČAK

Informacijska transparentnost kompleksan je koncept prisutan u mnogim područjima istraživanja koji se veže uz preduvjet smanjenja informacijske asimetrije kao kvantificirajućeg faktora. Na području zaštite privatnosti, transparentnost je postavljena i kao regulatorni mehanizam zaštite podataka kojim se nastoji pojedincima osigurati pravo na intervenabilnost kroz pristupačne alate za konzumiranje prava na izbor u odnosu na obradu njihovih osobnih podataka, prekid obrade određenih podataka, brisanje podataka, ispravak podataka i druga pripadajuća prava. No, transparentnost, da bi bila učinkovita treba osiguravati element odgovornosti, odnosno omogućavati kontrolu ispitanicima je li obrada podataka bila u skladu s dogovorenim ili navedenim politikama privatnosti.

U odnosu na oba uvjeta, politike privatnosti stoga postavljaju se kao mehanizam transparentnosti koji zahtjeva minucioznu pripremu, kao i izgradnju holističkog sustava usmjerenog na zaštitu privatnosti kroz, ne samo informacijske sustave poduprte suvremenim tehnologijama, već i cijeli poslovni sustav, a kako bi se osigurao odgovor na postavljene zahtjeve kroz cijeli životni ciklus mehanizama transparentnosti.

U tom kontekstu predloženim modelom vrednovanja informacijske transparentnosti politika privatnosti kao referentna vrijednost postavljen je upravo stupanj informacijske asimetrije, kojim je, u odnosu na stanje apsolutne simetrije, moguće izmjeriti vrijednosti elemenata na dvije dimenzije transparentnosti – *vidljivost*i i *inferabilnosti,* kao preduvjeta za utvrđivanje razina učinkovitosti mehanizama transparentnosti kao podloge za procjenu rizika, odnosno učinaka na prava i slobode osoba u digitalnom okruženju. Kroz provedeno istraživanje identificirani su faktori na svakoj pojedinoj dimenziji kao stupnjevi informacijske transparentnosti politika privatnosti na temelju kojih je omogućeno određivanje odstupanja prema postizanju optimalnih rezultata transparentnosti, odnosno informacijske simetrije, kao osnove za poboljšanje učinkovitosti mehanizama transparentnosti, ujedno potvrđujući hipotezu H1 da je pomoću stupnjeva faktora *vidljivosti* i *inferabilnosti* moguće je odrediti stupanj informacijske asimetrije.

.

Nadalje, iako se istraživanjem pokazalo da, suprotno teorijskoj pretpostavci, definirane dimenzije ne koreliraju, u odnosu na rezultate analize objašnjene varijance nad istraživanim uzorkom, pokazalo se kako na stupanj informacijske asimetrije značajnije utječu faktori *vidljivosti* u odnosu na faktore *inferabilnosti*, čime je potvrđena i istraživačka hipoteza H2.

Postavljanjem faktorskih opterećenja u međusobni odnos spram pripadajućih dimenzija transparentnosti, kao zasebnih varijabli, u nastavku je dizajniran naslovni model vrjednovanja te su validacijom modela preispitani su njihovi utjecaji na informacijsku transparentnost kroz analizu varijanci postavljenih faktorskih opterećenja na obje dimenzije transparentnosti, na temelju koje je opovrgnuta istraživačka hipoteza H3, odnosno da je primjenom dizajniranog modela moguće procijeniti informacijsku transparentnost politika privatnosti.

No, provedbom sporednih analiza nad uzorkom dobiveni rezultati mogu pružiti uvide za daljnja istraživanja. Definiranjem dimenzija informacijske transparentnosti, kako sa konceptualnog stanovišta pravne regulative, tako i sa teorijskog stanovišta osiguranja komponente kvalitete samih mehanizama kao komunikacijskog kanala, postavljen je okvir istraživanja informacijske transparentnosti na razini znanstvenog doprinosa. Nadalje, detaljnom identifikacijom pojedinih zahtjeva postavljen je metodološki okvir kojim se, uz sadržajni aspekt informacijske transparentnosti, ispituju i lingvističke kategorije samog mehanizma transparentnosti, kao važan aspekt transparentnosti u odnosu na ciljnu skupinu ispitanika. Isti se na razini aplikativnih doprinosa može primijeniti kao podloga za procjenu rizika, budući da navedeni podaci vezani uz (ne)ispunjenost zahtjeva mogu pružiti osnovu za identifikaciju pojedinih „opasnosti“ na prava i slobode osoba vezano uz zaštitu njihovih prava, ali i preventivnih mjera s obzirom na njihovu vrijednosnu, odnosno pondersku komponentu unutar pojedinih zahtjeva. Budući da je isti razvijan na uzorku politika privatnosti iz zdravstvenog sektora, područja koje se radi mnogih rizika vezano uz obrade zdravstvenih podataka može smatrati „senzitivnim“, parametri vrednovanja pojedinih indikatora usmjereni su na osiguranje najviših standarda pri zaštiti podataka, model vrjednovanja može biti korišten kao alat za razvoj učinkovitih mehanizama transparentnosti neovisno o području primjene, čime se ostvaruje doprinos i aktualnoj literaturi na području inženjerstva zahtjeva.

I rezultati analiza provedenih nad uzorkom zdravstvenih ustanova koje su ostvarile „iznadprosječne“ rezultate, odnosno koje su ostvarile rezultate najniže informacijske asimetrije na pojedinim dimenzijama transparentnosti mogu pružiti osnovu za brojna istraživanja na

navedenom području, poput utjecaja pojedinih uvjetno nazvanih „segmenata“ odrednica u životnom ciklusu mehanizama transparentnosti (pristupačnosti i slojevitosti; ažuriranosti i informativnosti; smislenosti i razumljivosti) kao primarnih, sekundarnih i tercijarnih zahtjeva na informacijsku (a)simetriju. A s obzirom na ograničenja pri istraživanju, kojima je set zdravstvenih ustanova ograničen s dostupnim politikama privatnosti na mrežnim stranicama, istraživanje bi se moglo proširiti na druge medije prikaza politika privatnosti, kao i na uzorke organizacija iz drugih sektora kao još jedan od mogućih smjerova za daljnja istraživanja na području .

POPIS LITERATURE

[1] M. Laufer, Robert and Wolfe, "Privacy as a Social Issue and Behavioural Concept," *J. Soc. Issues*, vol. 33, no. 3, pp. 22–41, 1977.

[2] P. S. Adler and S. W. Kwon, "Social capital: Prospects for a new concept," *Acad. Manag. Rev.*, vol. 27, no. 1, pp. 17–40, 2002, doi: 10.5465/AMR.2002.5922314.

[3] C. Steinfield, N. B. Ellison, and C. Lampe, "Social capital, self-esteem, and use of online social network sites: A longitudinal analysis," *J. Appl. Dev. Psychol.*, vol. 29, no. 6, pp. 434–445, 2008, doi: 10.1016/j.appdev.2008.07.002.

[4] C. L. Toma and J. T. Hancock, "Self-Affirmation Underlies Facebook Use," *Personal. Soc. Psychol. Bull.*, vol. 39, no. 3, pp. 321–331, 2013, doi: 10.1177/0146167212474694.

[5] A. Acquisti and R. Gross, "Imagined communities: awareness, information sharing and privacy on Facebook," *Enhancing Technol. Work.*, pp. 1–16, 2006.

[6] S. B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday*, vol. 11(9), 2006.

[7] B. T.K., C. S. R. Annavarapu, and A. Bablani, "Machine learning algorithms for social media analysis: A survey," *Comput. Sci. Rev.*, vol. 40, p. 100395, 2021, doi: https://doi.org/10.1016/j.cosrev.2021.100395.

[8] M. Petrescu and A. S. Krishen, "The dilemma of social media algorithms and analytics," *J. Mark. Anal.*, vol. 8, no. 4, pp. 187–188, 2020, doi: 10.1057/s41270-020-00094-4.

[9] N. Bobbio, *Democracy and Dictatorship: The Nature and Limits of State Power*. Polity, 1989.

[10] S. Splichal, "Masovni mediji između javnosti i javne sfere," pp. 5–24, 2014.

[11] "Princess Caroline of Monaco wins privacy ruling," *Out-Law News*, 2004.

[12] C. Tryhorn, “Rowling wins the right to privacy trial,” *Media law*, 2008.

[13] O. Gibson, “Campbell wins privacy case against Mirror,” *Daily Mirror*, 2004.

[14] A. Sundararajan, *The Sharing Economy; The End of Employment and the Rise of Crowd-Based Capitalism*. 2016.

[15] K. Hill, “Uber Doesn’t Want You to See This Document About Its Vast Data Surveillance System,” *Gizmodo*, 2017. https://gizmodo.com/uber-doesn-t-want-you-to-see-this-document-about-its-va-1795151637.

[16] A. LaPenne, “Connected: The Hidden Science of Everything,” Netflix, 2020.

[17] G. Ranzini, M. Etter, and I. E. Vermeulen, “Privacy in the Sharing Economy: European Perspectives,” *SSRN Electron. J.*, 2017, doi: 10.2139/ssrn.3048152.

[18] R. Calo, “The Boundaries of Privacy Harm,” *Indiana Law J.*, vol. 86, pp. 1132–1161, 2011.

[19] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010.

[20] C. Mallin and UNCTAD, “The relationship between corporate governance, transparency and financial disclosure,” *UNCTAD Work. Corp. Gov.*, vol. 10, no. 4, pp. 1–10, 2003.

[21] M. Turilli and L. Floridi, “The ethics of information transparency,” *Ethics Inf. Technol.*, vol. 11, no. 2, pp. 105–112, 2009, doi: 10.1007/s10676-009-9187-9.

[22] J. R. Reidenberg *et al.*, “Disagreeable Privacy Policies: Mismatches between Meaning and Userss Understanding,” *SSRN Electron. J.*, no. January, 2018, doi: 10.2139/ssrn.2418297.

[23] A. M. Mcdonald and L. F. Cranor, “The Cost of Reading Privacy Policies,” *A J. Law Policy Inf. Soc.*, pp. 1–22, 2008.

[24] Radna skupina za zaštitu podataka iz članka 29., “Smjernice o transparentnosti na

temelju Uredbe 2016/679," pp. 1–25, 2017.

[25] S. Sequoiah-Grayson, "The metaphilosophy of information," *Minds Mach.*, vol. 17, no. 3, pp. 331–344, 2007, doi: 10.1007/s11023-007-9072-4.

[26] R. Meis, R. Wirtz, and M. Heisel, "A Taxonomy of Requirements for the Privacy Goal Transparency," in *Trust, Privacy and Security in Digital Business (Lecture Notes in Computer Science)*, no. October, S. Fischer-Hübner, L. C., and L. J., Eds. Springer, Cham, 2015.

[27] C. J. Hoofnagle and J. M. Urban, *Alan Westin's Privacy Homo Economicus*, vol. 49. 2014.

[28] G. Akerlof, "THE MARKET FOR 'LEMONS': QUALITY UNCERTAINTY AND THE MARKET MECHANISM," *Q. J. Econ.*, vol. 4, no. 3, pp. 488–500, 1970.

[29] Y. Boujelbene and L. Besbes, "The Determinants of Information Asymmetry between Managers and Investors: A Study on Panel Data," *IBIMA Bus. Rev.*, vol. 2012, pp. 1–11, 2012, doi: 10.5171/2012.818936.

[30] S. C. Myers and N. S. Majluf, "Corporate financing and investment decisions when firms have information that investors do not have," *J. financ. econ.*, vol. 13, no. 2, pp. 187–221, 1984, doi: 10.1016/0304-405X(84)90023-0.

[31] N. Dierkens, "Measuring firm/market information asymmetry," no. July 1990, 1991.

[32] J. Laugesen, K. Hassanein, and Y. Yuan, "The impact of internet health information on patient compliance: A research model and an empirical study," *J. Med. Internet Res.*, vol. 17, no. 6, p. e143, 2015, doi: 10.2196/jmir.4333.

[33] M. Sceral, J. A. Erkoyuncu, and E. Shehab, "Identifying information asymmetry challenges in the defence sector," *Procedia Manuf.*, vol. 19, pp. 127–134, 2018, doi: 10.1016/j.promfg.2018.01.018.

[34] G. Michener and K. Bersch, "Identifying transparency," *Inf. Polity*, vol. 18, no. 3, pp. 233–242, 2013, doi: 10.3233/IP-130299.

[35] L. Rainie and M. Duggin, “Privacy and Information Sharing,” 2016. Dostupno: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

[36] Bradley University, “The Body Project,” 2016. Dostupno: https://www.bradley.edu/sites/bodyproject/.

[37] V. Zarya, “Employers Are Quietly Using Big Data to Track Employee Pregnancies,” *Fortune*, 2016.

[38] R. E. Silverman, “Bosses Tap Outside Firms to Predict Which Workers Might Get Sick,” *The Wall Street Journal*, 2016.

[39] K. Benitez and B. Malin, “Evaluating re-identification risks with respect to the HIPAA privacy rule,” *J. Am. Med. Informatics Assoc.*, vol. 17, no. 2, pp. 169–177, 2010, doi: 10.1136/jamia.2009.000026.

[40] European_Commission, “The Commission Health Emergency Operations Facility: for a coordinated management of public health emergency at EU level,” p. 20, 2007.

[41] M. Končar and L. Luić, “Privacy and Ethics Requirements with Electronic Healthcare Record Systems Implementations,” in *Proceedings of the European Federation for Medical Informatics “Medical Informatics in Enlarged Europe,”* 2007, pp. 108–113.

[42] L. Luić and D. Striber-Devaja, “The significance of information standards for development of integrated health information system,” *Arch. Oncol.*, vol. 14, no. 1–2, pp. 64–66, 2006, doi: 10.2298/AOO0602064L.

[43] S. Awanthika and and J. S. , Awanthika, Nalin AG Arachchilage, and Jill Slay. Senarath, , Nalin AG Arachchilage, “Designing Privacy for You: A User Centric Approach For Privacy Designing Privacy for You,” no. May, 2017. Dostupno: http://arxiv.org/abs/1703.09847.

[44] G. Greenleaf, “Sheherezade and the 101 data privacy laws : Origins , significance and global trajectories,” *J. Law, Inf. Sci.*, no. 23, 2014.

[45] EU, “Opća uredba o zaštiti podataka,” no. 3, 2016.

[46] Ministarstvo zdravstva, “Zdravstvene ustanove u Republici Hrvatskoj.” https://zdravlje.gov.hr/arhiva-80/ministarstvo-zdravlja/zdravstvene-ustanove-u-republici-hrvatskoj/656.

[47] D. Curtin and A. J. Meijer, “Does transparency strengthen legitimacy?,” *Inf. Polity*, vol. 11, no. 2, pp. 109–122, 2018, doi: 10.3233/ip-2006-0091.

[48] R. Araujo, Y. Taher, W.-J. Van Den Heuvel, and C. Cappelli, “Evolving government-citizen ties in public service design and delivery,” *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. P-221, pp. 19–26, 2013. Dostupno: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84918594649&partnerID=40&md5=0b325d9c39e04fc4ab50f18849aa1b09.

[49] O. H. Swank and B. Visser, “Is Transparency To No Avail?,” *Scand. J. Econ.*, vol. 115, no. 4, pp. 967–994, 2013, doi: 10.1111/sjoe.12029.

[50] A. M. Florini, “Does the Invisible Hand Need a Transparent Glove? The Politics of Transparency,” *Annu. World Bank Conf. Dev. Econ.*, pp. 1–40, 1999.

[51] T. Vishwanath and D. Kaufmann, “Towards Transparency in Finance and Governance,” *SSRN Electron. J.*, 2005, doi: 10.2139/ssrn.258978.

[52] OECD, *Foreign Direct Investment for Development- Maximising Benefits, Minimising Costs*. 2002.

[53] The Nobel Prize, “The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 2001.” https://www.nobelprize.org/prizes/economic-sciences/2001/summary/.

[54] G. Kopits and J. D. Craig, *Transparency in Government Operations*. International Monetary Fund, 1998.

[55] I. Kolstad and A. Wiig, “Is Transparency the Key to Reducing Corruption in Resource-Rich Countries?,” *World Dev.*, vol. 37, no. 3, pp. 521–532, 2009, doi: 10.1016/j.worlddev.2008.07.002.

[56] N. Andreula, A. Chong, and J. B. Guillen, “Institutional quality and fiscal

transparency,” 2009.

[57] A. H. Hallett and N. Viegi, “Imperfect transparency and the strategic use of information: An ever present temptation for central bankers?,” *Manchester Sch.*, vol. 71, no. 5, pp. 498–520, 2003, doi: 10.1111/1467-9957.00364.

[58] S. Morris and H. S. Shin, “Social value of public information,” *Am. Econ. Rev.*, vol. 92, no. 5, pp. 1521–1534, 2002, doi: 10.1016/0167-2681(85)90035-6.

[59] I. Muto, “Productivity growth, transparency, and monetary policy,” *J. Econ. Dyn. Control*, vol. 37, no. 1, pp. 329–344, 2013, doi: https://doi.org/10.1016/j.jedc.2012.08.005.

[60] P. M. Geraats, “Trends in monetary policy transparency,” *Int. Financ.*, vol. 12, no. 2, pp. 235–268, 2009, doi: 10.1111/j.1468-2362.2009.01239.x.

[61] V. Hahn, “Should central banks remain silent about their private information on cost-push shocks?,” *Oxf. Econ. Pap.*, vol. 64, no. 4, pp. 593–615, Oct. 2012, doi: 10.1093/oep/gpr056.

[62] L. Bauwens, W. Ben Omrane, and P. Giot, “News announcements, market activity and volatility in the euro/dollar foreign exchange market,” *J. Int. Money Financ.*, vol. 24, no. 7, pp. 1108–1125, 2005, doi: https://doi.org/10.1016/j.jimonfin.2005.08.008.

[63] P. Balduzzi, E. J. Elton, and T. C. Green, “Economic News and Bond Prices : Evidence from the U.S. Treasury Market,” vol. 36, no. 4, pp. 523–543, 2013.

[64] T. Gilbert, “Information aggregation around macroeconomic announcements: Revisions matter,” *J. financ. econ.*, vol. 101, no. 1, pp. 114–131, 2011, doi: 10.1016/j.jfineco.2011.02.013.

[65] A. Williams, “On the release of information by governments: Causes and consequences,” *J. Dev. Econ.*, vol. 89, no. 1, pp. 124–138, 2009, doi: https://doi.org/10.1016/j.jdeveco.2008.08.001.

[66] R. Islam, “Does more transparency go along with better governance?,” *Econ. Polit.*, vol. 18, no. 2, pp. 121–167, 2006, doi: 10.1111/j.1468-0343.2006.00166.x.

[67] J. R. Hollyer, B. P. Rosendorff, and J. R. Vreeland, “Democracy and transparency,” *J. Polit.*, vol. 73, no. 4, pp. 1191–1205, 2011, doi: 10.1017/S0022381611000880.

[68] A. Brunetti and B. Weder, “A free press is bad news for corruption,” *J. Public Econ.*, vol. 87, no. 7, pp. 1801–1824, 2003, doi: https://doi.org/10.1016/S0047-2727(01)00186-4.

[69] F. Bastida and B. Benito, “Central government budget practices and transparency: An international comparison,” *Public Adm.*, vol. 85, no. 3, pp. 667–716, 2007, doi: 10.1111/j.1467-9299.2007.00664.x.

[70] T. Besley and A. Prat, “Handcuffs for the Grabbing Hand? Media Capture and Government Accountability,” *Am. Econ. Rev.*, vol. 96, no. 3, pp. 720–736, 2006, doi: 10.1257/aer.96.3.720.

[71] A. Prat, “The wrong kind of transparency,” *Am. Econ. Rev.*, vol. 95, no. 3, pp. 862–877, 2005.

[72] S. K. Chowdhury, “The effect of democracy and press freedom on corruption: an empirical test,” *Econ. Lett.*, vol. 85, no. 1, pp. 93–101, 2004, doi: https://doi.org/10.1016/j.econlet.2004.03.024.

[73] S. Djankov, C. McLiesh, T. Nenova, and A. Shleifer, “Who Owns the Media?,” *J. Law Econ.*, vol. 46, no. 2, pp. 341–381, 2003.

[74] S. Freille, M. E. Haque, and R. Kneller, “A contribution to the empirics of press freedom and corruption,” *Eur. J. Polit. Econ.*, vol. 23, no. 4, pp. 838–862, 2007, doi: https://doi.org/10.1016/j.ejpoleco.2007.03.002.

[75] A. Gavazza and A. Lizzeri, “Transparency and Economic Policy,” *Rev. Econ. Stud.*, vol. 76, no. 3, pp. 1023–1048, 2009, doi: 10.1111/j.1467-937X.2009.00547.x.

[76] J. E. Alt and R. C. Lowry, “Transparency and Accountability: Empirical Results for Us States,” *J. Theor. Polit.*, vol. 22, no. 4, pp. 379–406, 2010, doi: 10.1177/0951629810375641.

[77] S. Gollwitzer, “Budget institutions and fiscal performance in Africa,” *J. Afr. Econ.*, vol.

20, no. 1, pp. 111–152, 2011.

[78] R. Glennerster and Y. Shin, “Does transparency pay?,” *IMF Staff Pap.*, vol. 55, no. 1, pp. 183–209, 2008.

[79] International Monetary Fund, “Fiscal Transparency and Economic Outcomes,” *IMF Work. Pap.*, vol. 05, no. 225, p. 1, 2005, doi: 10.5089/9781451862447.001.

[80] M. Alić and V. Antolović, “Percepcija društveno odgovornog poslovanja kod generacije Z,” in *MIPRO 2019 proceedings*, 2019, pp. 1565–1570.

[81] B. Fernandez-Feijoo, S. Romero, and S. Ruiz, “Effect of Stakeholders’ Pressure on Transparency of Sustainability Reports within the GRI Framework,” *J. Bus. Ethics*, vol. 122, no. 1, pp. 53–63, 2014, doi: 10.1007/s10551-013-1748-5.

[82] F. Caputo, S. Pizzi, L. Ligorio, and R. Leopizzi, “Enhancing environmental information transparency through corporate social responsibility reporting regulation,” *Bus. Strateg. Environ.*, vol. 30, no. 8, pp. 3470–3484, 2021, doi: 10.1002/bse.2814.

[83] Sabor RH, *Zakon o zaštiti potrošača*. 2020.

[84] M. Hosseini, A. Shahri, K. Phalp, and R. Ali, “Towards engineering transparency as a requirement in socio-technical systems,” *2015 IEEE 23rd Int. Requir. Eng. Conf. RE 2015 - Proc.*, pp. 268–273, 2015, doi: 10.1109/RE.2015.7320435.

[85] C. Kalloniatis, E. Kavakli, and S. Gritzalis, “Addressing privacy requirements in system design: The PriS method,” *Requir. Eng.*, vol. 13, no. 3, pp. 241–255, 2008, doi: 10.1007/s00766-008-0067-3.

[86] S. Spiekermann and L. F. Cranor, “Engineering privacy,” *IEEE Trans. Softw. Eng.*, vol. 35, no. 1, pp. 67–82, 2009, doi: 10.1109/TSE.2008.88.

[87] E. Yanakieva, M. Youssef, A. H. Rezae, and A. Bieniusa, “On the Impossibility of Confidentiality, Integrity and Accessibility in Highly-Dostupno File Systems,” in *Networked Systems*, 2021, pp. 3–18.

[88] C. Pelnekar, “Planning for and Implementing ISO 27001,” *ISACA J.*, vol. 4, 2011.

Dostupno: https://www.isaca.org/resources/isaca-journal/past-issues/2011/2011-planning-for-and-implementing-iso-27001.

[89] ISECT, “ISO 27k Toolkit.” https://www.iso27001security.com/html/toolkit.html.

[90] J. Iden and T. R. Eikebrokk, “Implementing IT Service Management: A systematic literature review,” *Int. J. Inf. Manage.*, vol. 33, no. 3, pp. 512–523, 2013, doi: https://doi.org/10.1016/j.ijinfomgt.2013.01.004.

[91] A. I. Anton and C. Potts, “Use of goals to surface requirements for evolving systems,” in *Proceedings - International Conference on Software Engineering*, 1998, pp. 157–166, doi: 10.1109/icse.1998.671112.

[92] A. Van Lamsweerde, “Goal-oriented requirements engineering: A guided tour,” *Proc. IEEE Int. Conf. Requir. Eng.*, pp. 249–261, 2001, doi: 10.1109/isre.2001.948567.

[93] A. Cartlidge *et al.*, “An Introductory Overview of ITIL® 2011.” London, 2012.

[94] OASIS, “Privacy Management Reference Model and Methodology (PMRM) Version 1.0.” 2012. Dostupno: http://docs.oasis-open.org/pmrm/PMRM/v1.0/csd01/PMRM-v1.0-csd01.html.

[95] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, “A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements,” *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, 2011, doi: 10.1007/s00766-010-0115-7.

[96] DistriNet Research Group, “About,” *Linddun.org*, 2020. https://www.linddun.org/about.

[97] K. Wuyts and W. Joosen, “LINDDUN tutorial,” vol. C, no. July, 2015.

[98] A. Pfitzmann and M. Hansen, “A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,” *Tech. Univ. Dresden*, no. January 2010, pp. 1–98, 2010. Dostupno: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml%5Cnhttp://dud.inf.tu-

dresden.de/literatur/Anon_Terminology_v0.34.pdf.

[99] M. Roe, “Cryptography and evidence,” no. 780, 2010.

[100] M. Sohlenkamp, “Supporting group awareness in multi user environments through perceptualization,” 1998.

[101] I. & P. C. Ann Cavoukian and C. Ontario, “Privacy by Design, The 7 Foundational Principles,” pp. 7–8, 2011, doi: 10.1016/S0969-4765(07)70084-X.

[102] A. Anton and J. Earp, “A requirements taxonomy for reducing Web site privacy vulnerabilities,” *Requir. Eng.*, vol. 9, no. 3, pp. 169–185, 2004, doi: 10.1007/s00766-003-0183-z.

[103] Data Protection and Privacy Commissioners, “Resolution on Privacy by Design,” *32nd Int. Conf. Data Prot. Priv. Comm.*, pp. 1–2, 2010.

[104] Federal Trade Commision (FTC), “Protecting Consumer in an Era of Rapid Change: Recommendations for businesses and policymakers,” *Fed. Trade Commision*, no. March, pp. 1–112, 2012. Dostupno: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[105] A. Cavoukian, “Privacy by Design and the Emerging Personal Data Ecosystem,” no. October, pp. 1–39, 2012.

[106] I. Rubstein and N. Good, “Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents,” *Priv. Technol. Policy*, pp. 55–72, 2014.

[107] S. Gurses, C. Troncoso, and C. DIaz, “Engineering: Privacy by design,” doi: 10.1126/science.1143464.

[108] D. Tancock, S. Pearson, and A. Charlesworth, “A Privacy Impact Assessment Tool for Cloud Computing,” in *Privacy and Security for Cloud Computing*, S. Pearson and G. Yee, Eds. London: Springer London, 2013, pp. 73–123.

[109] S. Sannon, B. Sun, and D. Cosley, “Privacy, Surveillance, and Power in the Gig Economy,” 2022, doi: 10.1145/3491102.3502083.

[110] R. Clarke, “Privacy impact assessment: Its origins and development,” *Comput. Law Secur. Rev.*, vol. 25, pp. 123–135, 2009, doi: 10.1016/j.clsr.2009.02.002.

[111] D. Tancock, S. Pearson, and A. Charlesworth, “Analysis of Privacy Impact Assessments within Major jurisdictions,” in *2010 Eighth International Conference on Privacy, Security and Trust*, 2010, pp. 118–125, doi: 10.1109/PST.2010.5593260.

[112] D. J. Solove, “A Taxonomy of Privacy,” *Univ. PA. Law Rev.*, vol. 154, no. 477, pp. 477–560, 2006.

[113] P. De Hert, D. Kloza, and D. Wright, *Recommendations for a privacy impact assessment framework for the European Union*, Deliverabl. PIAF project, 2012.

[114] D. Wright, “The state of the art in privacy impact assessment,” *Comput. Law Secur. Rev.*, vol. 28, no. 1, pp. 54–61, 2012, doi: 10.1016/j.clsr.2011.11.007.

[115] J. Stoddart, “Auditing Privacy Impact Assessments: The Canadian Experience,” in *Privacy Impact Assessment*, D. Wright and P. De Hert, Eds. Dordrecht: Springer Netherlands, 2012, pp. 419–436.

[116] ENISA, *Guidelines for SMEs on the security of personal data processing*, no. December. 2016.

[117] L. Fritsch and H. Abie, “Towards a Research Road Map for the Management of Privacy Risks in Information Systems.,” 2008, pp. 1–15.

[118] R. Gellman, “Privacy , Consumers , and Costs - How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete,” no. March, pp. 1–37, 2002. Dostupno: https://archive.epic.org/reports/dmfprivacy.html.

[119] T. N. C. I. Center, “A Preliminary Assessment of the National Crime Information Center and the Computerized Criminal History System,” 1978.

[120] H. F. Tipton and M. Krause, *Information Security Management Handbook*, 6th ed.

2008.

[121] M. Colesky, J. H. Hoepman, and C. Hillen, “A Critical Analysis of Privacy Design Strategies,” 2016, doi: 10.1109/SPW.2016.23.

[122] J.-H. Hoepman, “Privacy Design Strategies,” in *ICT Systems Security and Privacy Protection*, 2014, pp. 446–459.

[123] P. Samarati and L. Sweeney, “Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression,” 1998.

[124] N. Shevchenko, “Did Reagan really coin the term ‘Trust but verify,’ a proverb revived by HBO’s Chernobyl?,” *Russia Beyond*, 2019.

[125] A. Cavoukian and others, “Privacy by design: The 7 foundational principles; Implementation and Mapping of Fair Information Practices,” *Inf. Priv. Comm. Ontario, Canada*, 2009. Dostupno: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

[126] R. Gellman, “Fair Information Practices: A Basic History,” *SSRN Electron. J.*, 2014, doi: 10.2139/ssrn.2415020.

[127] OECD, “Organisation for Economic Cooperation and Development guidelines Annex to the recommendation of the Council of 23 September 1980: Guidelines governing the protection of privacy and transborder flows of personal data,” no. September, 1980.

[128] OECD, *The OECD Privacy Guidelines*. 2013.

[129] Asia Pacific Economic Cooperation, *APEC Privacy Framework*. 2005.

[130] National Institute of Standards and Technology, *NIST Privacy Framework - a tool for improving privacy through enterprise risk management*. 2020.

[131] M. F. Dennedy, J. Fox, and T. R. Finneran, *The Privacy Engineer’s Manifesto*. 2014.

[132] J. C. S. do P. Leite and C. Cappelli, “Software Transparency,” *Bus. Inf. Syst. Eng.*, vol. 2, no. 3, pp. 127–139, 2010, doi: 10.1007/s12599-010-0102-z.

[133] L. Chung, B. A. Nixon, E. Yu, and J. Mylopoulos, *Non-Functional Requirements in Software Engineering*. New York: Springer International Publishing, 2000.

[134] E. S. Yu, “Modelling Strategic Relationships for Process,” p. 121, 1995.

[135] C. Cappeli and J. Leite, “C.S.P. . Exploring i* Characteristics that Support Software,” no. June 2014, 2008.

[136] L. Dabbish, H. C. Stuart, J. Tsay, and J. D. Herbsleb, “Social Coding in GitHub: Transparency and Collaboration in an Open Software Repository,” *Proc. ACM 2012 Conf. Comput. Support. Coop. Work*, no. 2011, pp. 1277–1286, 2012, doi: 10.1145/2145204.2145396.

[137] L. Dabbish, C. Stuart, J. Tsay, and J. Herbsleb, “Leveraging transparency,” *IEEE Softw.*, vol. 30, no. 1, pp. 37–43, 2013, doi: 10.1109/MS.2012.172.

[138] M. Serrano and J. C. S. Do Prado Leite, “Capturing transparency-related requirements patterns through argumentation,” *2011 1st Int. Work. Requir. Patterns, RePa’11*, vol. 00, no. c, pp. 32–41, 2011, doi: 10.1109/RePa.2011.6046723.

[139] R. T. Stein, *Software for Dependable Systems: Sufficient Evidence?*, vol. 42, no. 4. 2008.

[140] A. D. Miyazaki, “Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage,” *J. Public Policy Mark.*, vol. 27, no. 1, pp. 19–33, 2008, doi: 10.1509/jppm.27.1.19.

[141] T. Ermakova, H. Krasnova, and B. Fabian, “Exploring the impact of readability of privacy policies on users’ trust,” *24th Eur. Conf. Inf. Syst. ECIS 2016*, no. April, 2016.

[142] B. R. Rawlins, “Measuring the Relationship Between Organizational Transparency and Trust,” *Public Relat. J.*, vol. 2, no. 2, pp. 1–21, 2008. Dostupno: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Measuring+the+relationship+between+organizational+transparency+and+employee+trust+.#0.

[143] B. Zieni, “Software Requirements Engineering for Transparency,” University of Leicester, 2021.

[144] D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. J. Sussman, “Information accountability,” *Commun. ACM*, vol. 51, no. 6, pp. 82–87, 2008, doi: 10.1145/1349026.1349043.

[145] D. Hess, “Social Reporting and New Governance Regulation,” *Bus. Ethics Q.*, vol. 17, no. 3, pp. 453–476, 2007, doi: 10.5840/beq200717348.

[146] C. Ball, “What Is Transparency?,” *Public Integr.*, vol. 11, no. 4, pp. 293–308, 2009, doi: 10.2753/PIN1099-9922110400.

[147] M. Hosseini, A. Shahri, K. Phalp, and R. Ali, “Foundations for transparency requirements engineering,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9619, pp. 225–231, 2016, doi: 10.1007/978-3-319-30282-9_15.

[148] J. Krogstie, H. A. R. Eds, I. Conference, and D. Hutchison, “Advanced Information Systems Engineering p624-625,” 2005, vol. 3520, doi: 10.1007/b136788.

[149] M. Hosseini, A. Shahri, K. Phalp, and R. Ali, “Four reference models for transparency requirements in information systems,” *Requir. Eng.*, 2018, doi: 10.1007/s00766-017-0265-y.

[150] B. Rawlins, *Give the Emperor a Mirror: Toward Developing a Stakeholder Measurement of Organizational Transparency*, vol. 21, no. 1. 2009.

[151] J. C. Griffith, “Beyond Transparency : New Standards for Legislative Information Systems,” *Inf. Syst.*, no. June, 2006.

[152] B. K. Kahn, D. M. Strong, and R. Y. Wang, “Information quality benchmarks: product and service performance,” *Commun. ACM*, vol. 45, no. 4ve, pp. 184–192, 2002, doi: 10.1145/505999.506007.

[153] P. G. Leon *et al.*, “What matters to users? Factors that Affect Users’ Willingness to Share Information with Online Advertisers,” *SOUPS 2013 - Proc. 9th Symp. Usable Priv. Secur.*, p. 1, 2013, doi: 10.1145/2501604.2501611.

[154] J. Lin, B. Liu, N. M. Sadeh, and J. I. Hong, “Modeling Users’ Mobile App Privacy

Preferences: Restoring Usability in a Sea of Permission Settings," 2014.

[155] L. F. Cranor, "Necessary but not sufficient: Standardized mechanisms for privacy notice and choice," *J. Telecommun. High Technol. Law*, vol. 10, pp. 273–308, 2011.

[156] F. Cate, "The Limits of Notice and Choice," *IEEE Secur. Priv.*, no. April, pp. 59–62, 2010, doi: 10.1109/MSP.2010.84.

[157] I. Pollach, "What's wrong with online privacy policies?," *Commun. ACM*, vol. 50, no. 9, pp. 103–108, 2007.

[158] S. Wilson *et al.*, "The Creation and Analysis of a Website Privacy Policy Corpus," in *Proceedings ofthe 54th Annual Meeting of the Association for Computational Linguistics*, 2016, pp. 1330–1340.

[159] J. R. Reidenberg *et al.*, "Disagreeable privacy policies: Mismatches between meaning and users' understanding," *Berkeley Technol. Law J.*, vol. 30, no. 1, pp. 39–88, 2015.

[160] C. Jensen and C. Potts, "Privacy Policies as Decision-Making Tools : An Evaluation of Online Privacy Notices," *Conf. Hum. Factors Comput. Syst. - Proceedings, CHI 2004*, vol. 6, no. 1, pp. 471–478, 2004.

[161] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, "Standardizing Privacy Notices : An Online Study of the Nutrition Label Approach," *CHI 2010 - 28th Annu. CHI Conf. Hum. Factors Comput. Syst. Conf. Proc.*, pp. 1573–1582, 2010.

[162] F. Schaub, R. Balebako, and L. F. Cranor, "Designing Effective Privacy Notices and Controls," *IEEE Internet Comput.*, 2017.

[163] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A 'nutrition label' for privacy," *SOUPS 2009 - Proc. 5th Symp. Usable Priv. Secur.*, vol. 1990, 2009, doi: 10.1145/1572532.1572538.

[164] N. Sadeh *et al.*, "Towards usable privacy policies: Semi-automatically extracting data practices from websites' privacy policies," *Symp. Usable Priv. Secur. (SOUPS 2014)*, no. July, pp. 2–3, 2014. Dostupno: https://www.researchgate.net/profile/Florian_Schaub/publication/263083431_Towards

_Usable_Privacy_Policies_Semi-automatically_Extracting_Data_Practices_From_Websites'_Privacy_Policies_Poster/links/00b7d53a44af41ea53000000/Towards-Usable-Privacy-Policies-Se.

[165] S. Zimmeck *et al.*, "Automated analysis of privacy requirements for mobile apps," *AAAI Fall Symp. - Tech. Rep.*, vol. FS-16-01-, no. 132, pp. 286–296, 2016, doi: 10.14722/ndss.2017.23034.

[166] W. Ammar, S. Wilson, N. Sadeh, and N. A. Smith, "Automatic categorization of privacy policies: A pilot study," *Sch. Comput. Sci. Lang. Technol. Institute, Tech. Rep. C.*, 2012. Dostupno: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.278.5073&rep=rep1&type=pdf.

[167] F. Liu, R. Ramanath, N. Sadeh, and N. A. Smith, "A step towards usable privacy policy: Automatic alignment of privacy statements," *COLING 2014 - 25th Int. Conf. Comput. Linguist. Proc. COLING 2014 Tech. Pap.*, pp. 884–894, 2014.

[168] W3C, "Platform for Privacy Preferences (P3P) Project." https://www.w3.org/P3P/.

[169] D. Miorandi, A. Rizzardi, S. Sicari, and A. Coen-Porisini, "Sticky Policies: A Survey," *IEEE Trans. Knowl. Data Eng.*, vol. 32, no. 12, pp. 2481–2499, 2020, doi: 10.1109/TKDE.2019.2936353.

[170] S. D. W. L. D. Brandeis, "The right to privacy.," *Linacre Q.*, vol. 40, no. 2, pp. 138–43, 1973. Dostupno: http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C%0Ahttp://www.ncbi.nlm.nih.gov/pubmed/11660962.

[171] S. Bok, *Secrets: On the ethics of concealment and revelation*. New York: Pantheon, 1982.

[172] A. F. Westin, *Privacy and Freedom*. New York: Atheneum, 1967.

[173] M. Boban, "Pravo na privatnost i pravo na pristup informacijama u suvremenom informacijskom društvu," *Zb. Rad. Pravnog Fak. u Split.*, vol. 49, no. 3, pp. 575–598,

2012.

[174] Hrvatski Sabor, “Ustav Republike Hrvatske,” 2010, doi: 10.1017/CBO9781107415324.004.

[175] J. Ponesse, “The ties that blind: Conceptualizing anonymity,” *J. Soc. Philos.*, vol. 45, no. 3, pp. 304–322, 2014, doi: 10.1111/josp.12066.

[176] S. T. Margulis, “Conceptions of Privacy: Current Status and Next Steps,” *J. Soc. Issues*, vol. 33, no. 3, pp. 5–21, 1977, doi: 10.1111/j.1540-4560.1977.tb01879.x.

[177] E. Sundstrom, M. G. Sundstrom, and S. Eric, *Work Places: The Psychology of the Physical Environment in Offices and Factories*. Cambridge University Press, 1986.

[178] P. B. Newell, “Perspectives on privacy,” *J. Environ. Psychol.*, vol. 15, no. 2, pp. 87–104, 1995, doi: 10.1016/0272-4944(95)90018-7.

[179] S. Petronio, *Boundaries of Privacy: Dialectics of Disclosure*. Albany: State University of New York Press, 2002.

[180] I. Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Publishing Company, 1975.

[181] I. Altman, “Privacy Regulation: Culturally Universal or Culturally Specific?,” *J. Soc. Issues*, vol. 33, no. 3, pp. 66–84, 1977, doi: https://doi.org/10.1111/j.1540-4560.1977.tb01883.x.

[182] A. F. Westin, “Social and Political Dimensions of Privacy,” *J. ofSocial Issues*, vol. 59, no. 2, pp. 431–453, 2003. Dostupno: www. forstbuch. de.

[183] Ž. Ivanković, *Besplatno; Uvod u političku ekonomiju digitalnog doba*. Zagreb: Jesenski i Turk, 2018.

[184] TRUSTe, “Consumer Opinion and Business Impact,” 2014. Dostupno: http://info.truste.com/lp/truste/Web-Resource-HarrisConsumerResearchUS-ReportQ12014_LP.html.

[185] M. Madden, L. Rainie, K. Zickuhr, M. Duggan, and A. Smith, “Public Perceptions of Privacy and Security in the Post-Snowden Era,” *Pew Res. Cent.*, pp. 3–57, 2011, doi: 202.419.4372.

[186] N. B. Ellison, J. Vitak, C. Steinfield, R. M. Gray, and C. Lampe, “Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment,” 2011.

[187] A. Nosko *et al.*, “Examining priming and gender as a means to reduce risk in a social networking context: Can stories change disclosure and privacy setting use when personal profiles are constructed?,” *Comput. Human Behav.*, vol. 28, no. 6, pp. 2067–2074, 2012, doi: 10.1016/j.chb.2012.06.010.

[188] F. Stutzman and J. Kramer-Duffield, “Friends only: examining a privacy-enhancing behavior in facebook,” *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, 2010.

[189] Z. Tufekci, “Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites,” *Bull. Sci. Technol. Soc.*, vol. 28, no. 1, pp. 20–36, 2008, doi: 10.1177/0270467607311484.

[190] N. Mohamed and I. H. Ahmad, “Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia,” *Comput. Human Behav.*, vol. 28, no. 6, pp. 2366–2375, 2012, doi: https://doi.org/10.1016/j.chb.2012.07.008.

[191] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, “Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences,” *J. Comput. Commun.*, vol. 15, no. 1, pp. 83–108, 2009, doi: 10.1111/j.1083-6101.2009.01494.x.

[192] A. N. Joinson, U. D. Reips, T. Buchanan, and C. B. P. Schofield, “Privacy, trust, and self-disclosure online,” *Human-Computer Interact.*, vol. 25, no. 1, pp. 1–24, 2010, doi: 10.1080/07370020903586662.

[193] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, “Online social networks: Why we disclose,” *J. Inf. Technol.*, vol. 25, no. 2, pp. 109–125, 2010, doi: 10.1057/jit.2010.6.

[194] S. Trepte, T. Dienlin, and L. Reinecke, “Risky behaviors: How online experiences influence privacy behaviors,” *From Gutenb. Galaxy to Google Galaxy*, no. November, pp. 225–244, 2014.

[195] D. S. Evans, “The online advertising industry: Economics, evolution, and privacy,” *J. Econ. Perspect.*, vol. 23, no. 3, pp. 37–60, 2009, doi: 10.1257/jep.23.3.37.

[196] D. I. Tamir and J. P. Mitchell, “Disclosing information about the self is intrinsically rewarding,” *Proc. Natl. Acad. Sci.*, vol. 109, no. 21, pp. 8038–8043, 2012, doi: 10.1073/pnas.1202129109.

[197] R. A. Posner, “The Economics of Privacy,” *Am. Econ. Rev.*, vol. 71, no. 2, pp. 405–409, 1981, doi: 10.1057/978-1-349-95121-5_340-2.

[198] A. Acquisti and J. Grossklags, “Privacy and Rationality in Individual Decision Making,” *IEEE Secur. Priv.*, no. February 2005, 2005, doi: 10.1109/MSP.2005.22.

[199] A. Acquisti, C. Taylor, and L. Wagman, “The economics of privacy,” *J. Econ. Lit.*, vol. 54, no. 2, pp. 442–492, 2016, doi: 10.1257/jel.54.2.442.

[200] UN, *Opća deklaracija o ljudskim pravima*. 1948, pp. 1–7.

[201] EU, *Povelja Europske Unije o temeljnim pravima*. 2000, pp. 389–405.

[202] A. Lever, “Privacy Rights and Democracy: A Contradiction in Terms?,” *Contemp. Polit. Theory*, vol. 5, no. 2, pp. 142–162, 2006, doi: 10.1057/palgrave.cpt.9300187.

[203] J. K. Burgoon, “Privacy and Communication,” *Ann. Int. Commun. Assoc.*, vol. 6, no. 1, pp. 206–249, 1982, doi: 10.1080/23808985.1982.11678499.

[204] Ž. Hutinski, “Pristup izgradnji podsustava čuvanja i zaštite podataka i informacija,” *Zb. Rad. Fak. Organ. i Inform.*, pp. 35–46, 1990.

[205] *Zakon o tajnosti podataka*. 2007.

[206] M. Guinness, “France maintains long tradition of data protection,” *Deutsche Welle*.

[207] European Union Agency for Fundamental Rights & Council of Europe, *Handbook on*

European Data Protection Law. 2014.

[208] M. Burri and R. Schär, “The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy,” *J. Inf. Policy*, vol. 6, no. 1, pp. 479–511, 2016, doi: 10.5325/jinfopoli.6.2016.0479.

[209] C. Quinn, “GDPR Age of ‘Digital’ Consent,” *PRIVO*, 2021. https://www.privo.com/blog/gdpr-age-of-digital-consent.

[210] European Data Protection Board, “Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence , tasks and powers of data protection authorities,” no. Opinion of the Board (Art. 64), pp. 1–25, 2019.

[211] Europski parlament i Vijeće Europske unije, “Direktiva o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija,” *Službeni List Eur. unije*, vol. 13, no. 52, pp. 111–121, 2002.

[212] D. Cooper, K. Van Quathem, and A. Oberschelp de Meneses, “Progress on the Pending EU ePrivacy Regulation,” *Covington*, 2021. https://www.globalpolicywatch.com/2021/11/progress-on-the-pending-eu-eprivacy-regulation/.

[213] *KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU I VIJEĆU o funkcioniranju „sigurne luke” iz perspektive građana EU-a i poduzeća s poslovnim nastanom u Europskoj uniji*. 2013.

[214] B. W. Schermer, B. Custers, and S. van der Hof, “The crisis of consent: how stronger legal protection may lead to weaker consent in data protection,” *Ethics Inf Technol*, vol. 16, pp. 171–182, 2014, doi: 10.1007/s10676-014-9343-8.

[215] D. J. Solove, “Introduction: Privacy self-management and the consent dilemma,” *Harv. Law Rev.*, vol. 126, no. 7, pp. 1880–1903, 2013.

[216] D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” *Commun. ACM*, vol. 24, no. 2, pp. 84–90, 1981, doi:

10.1145/358549.358563.

[217] A. Pfitzmann, B. Pfitzmann, and M. Waidner, “ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead,” pp. 451–463, 1991, doi: 10.1007/978-3-642-76462-2_32.

[218] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, “Hiding routing information,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1174, pp. 137–150, 1996, doi: 10.1007/3-540-61996-8_37.

[219] A. Jerichow, J. Müller, A. Pfitzmann, B. Pfitzmann, and M. Waidner, “Real-time mixes: A bandwidth-efficient anonymity protocol,” *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 495–508, 1998, doi: 10.1109/49.668973.

[220] G. Lacoste, B. Pfitzmann, M. Steiner, and M. Waidener, “Secure Electronic Marketplace for Europe,” 2000, doi: 10.1007/b75215.

[221] M. Bellare and P. Rogaway, “PRIME – Privacy and Identity Management for Europe,” *Adv. Cryptology—Eurocrypt’96*, no. June, pp. 399–416, 2010, doi: 10.1007/3-540-68339-9_34.

[222] Europska unija, “The Future of Identity in the Information Society (FIDIS).” https://cordis.europa.eu/project/id/507512.

[223] J. Camenisch and E. Van Herreweghen, “Design and implementation of the idemix anonymous credential system,” *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 21–30, 2002, doi: 10.1145/586110.586114.

[224] G. Van Blarkom, J. J. Borking, and J. G. E. Olk, “Handbook of privacy and privacy-enhancing technologies,” *Priv. Inc. Softw. …*, pp. 42–50, 2003. Dostupno: http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf%5Cnhttp://www.cbpweb.nl/downloads_technologie/pisa_handboek.pdf.

[225] L. Fritsch, *State of the art of Privacy-enhancing Technology (PET)*, vol. Deliverabl. 2007.

[226] J. Borking, “Der identity protector,” *Datenschutz und Datensicherheit*, vol. 20, no. 11,

pp. 654–658, 1996.

[227] R. Peeters and T. Pulls, “Regaining the end-users’ trust with transparency-enhancing tools”. Dostupno: http://www.project-opacity.com.

[228] M. Hansen, “Marrying transparency tools with user-controlled identity management,” 2008, doi: 10.1007/978-0-387-79026-8_14.

[229] H. Hedbom, “A Survey on Transparency Tools for Enhancing Privacy,” 2009.

[230] C. Zimmermann, “A Categorization of Transparency-Enhancing Technologies,” 2015.

[231] Mozilla, “Enhanced Tracking Protection in Firefox for desktop.” https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop.

[232] Google, “Moja aktivnost.” https://myactivity.google.com/myactivity.

[233] “User empowerment for Enhanced Online Management (USEMP).” https://www.usemp.eu/.

[234] C. E. Shannon and W. Weaver, “The Theory of Mathematical Communication,” *Int. Bus.*, p. 131, 1949. Dostupno: https://pure.mpg.de/rest/items/item_2383164_3/component/file_2383163/content.

[235] D. Spagnuelo, C. Bartolini, and G. L. B, “Metrics for Transparency,” in *Data Privacy Management and Security Assurance:11th International Workshop, DPM 2016 and 5th International Workshop, QASA 2016, Heraklion, Crete, Greece, September 26-27, 2016*, 2016, pp. 3–18, doi: 10.1007/978-3-319-47072-6.

[236] ISO/IEC, “ISO/IEC 29100:2011 Information technlogy - Security techniques - Privacy Framework; Technical report.”

[237] V. Johansson, “Lexical diversity and lexical density in speech and writing: a developmental perspective,” *Work. Pap. Linguist.*, vol. 53, no. 0, pp. 61–79, 2009.

[238] V. Lamza-Posavec, *Metodologija društvenih istraživanja*. Zagreb: Institut društvenih znanosti Ivo Pilar, 2004.

[239] *Zakon o zdravstvenoj zaštiti*. .

[240] Državni zavod za statistiku Republike Hrvatske, "Popis stanovništva RH 2011: Stanovništvo prema obrazovnim obilježljima". Dostupno: https://www.dzs.hr/Hrv_Eng/publication/2016/SI-1582.pdf.

[241] Sud Europske unije, "Presuda Suda (veliko vijeće) od 16. srpnja 2020.," 2020. Dostupno: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:62018CJ0311&from=hr.

[242] N. Guntamukkala, R. Dara, and G. Grewal, "A machine-learning based approach for measuring the completeness of online privacy policies," *Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015*, pp. 289–294, 2016, doi: 10.1109/ICMLA.2015.143.

[243] S. Brangan, "KVANTITATIVNA PROCJENA TEŽINE TEKSTA NA HRVATSKOM JEZIKU," vol. 1, pp. 35–58, 2014.

[244] S. Brangan, "Razvoj formula čitkosti za zdravstvenu komunikaciju na hrvatskom jeziku," 2011.

[245] J. Ure, "Lexical density and register differentiation," *Appl. Linguist.*, vol. 443–452, 1971.

[246] T. Berber-Sardinha, "Comparing corpora with WordSmith Tools: How large must the reference corpus be ?," *WCC '00 Proc. Work. Comp. corpora*, pp. 7–13, 2000.

[247] "Microsoftova Izjava o zaštiti privatnosti," 2020. Dostupno: https://privacy.microsoft.com.

[248] *Googleova pravila o privatnosti*. 2020.

[249] "Syllable Counter." https://syllablecounter.org/.

[250] "Text Analyser," *Online-Utility.org*. https://www.online-utility.org/text/analyzer.jsp.

[251] B. M. Byrne, *Structural Equation Modeling with AMOS: Basic Concepts, Applications,*

and Programming (1st Ed.), vol. 20. 2001.

[252] A. M. R., M. Zainol, I. Fazli, A. M., and S. N. R. M., "Measuring Value - Based Productivity: A Confirmatory Factor Analytic (CFA) Approach," *Int. J. Bus. Soc. Sci.*, vol. 2, no. 6, pp. 85–93, 2011.

[253] H. Chemingui and H. Ben Lallouna, "Resistance, motivations, trust and intention to use mobile financial services," *Int. J. Bank Mark.*, vol. 31, no. 7, pp. 574–592, 2013, doi: 10.1108/IJBM-12-2012-0124.

[254] D. B. Wright and J. A. Herrington, "Problematic standard errors and confidence intervals for skewness and kurtosis," *Behav. Res. Methods*, vol. 43, no. 1, pp. 8–17, 2011, doi: 10.3758/s13428-010-0044-x.

[255] M. Žugaj, K. Dumičić, and V. Dušak, *Temelji znanstvenoistraživačkog rada: metodologija i metodika*. Varaždin: Fakultet organizacije i informatike, 2006.

[256] *Zakon o provedbi Opće uredbe o zaštiti podataka*. Republika Hrvatska, 2018.

[257] CMS.Law, "GDPR Enforcement Tracker." https://www.enforcementtracker.com/?insights#sectorstatistics%0A.

[258] D. Labaš, *Novi mediji - nove tehnologije - novi moral*. Zagreb: Hrvatski studiji, 2009.

[259] Leksikografski zavod Miroslav Krleža, "Trgovina," *Hrvatska enciklopedija, mrežno izdanje*. Leksikografski zavod Miroslav Krleža.

[260] Radna skupina za zaštitu podataka iz članka 29., "Smjernice o službenicima za zaštitu podataka." p. 29, 2016.

POPIS TABLICA

POPIS SLIKA

POPIS KRATICA

OASIS (eng. Organization for the Advancement of Structured Information Standards); organizacija za razvoj otvorenih standarda

PMRM (eng. Privacy Management Reference Model and Methodology); model i metodologija za upravljanje privatnošću

LINDDUN (eng. Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Non-compliance); metoda analize koja procjenjuje situaciju prijetnje privatnosti

PDCA (eng. Plan-Do-Check-Act); model za učenje, kontrolu i poboljšanje proizvoda ili procesa

FIP (eng. Fair Information Practices); Prakse poštenog informiranja

OECD (eng. The Organisation for Economic Cooperation and Development); Organizacija za ekonomsku suradnju i razvoj

APEC (eng. The Asia-Pacific Economic Cooperation): organizacija Azijsko-pacifička ekonomske suradnje

NIST (eng. The National Institute of Standards and Technology); Nacionalni institut za standarde i tehnologiju

GAPP (eng. Generally Accepted Privacy Principles); Općeprihvaćena načela privatnosti

AICPA (eng. The Association of International Certified Professional Accountants); Udruženje međunarodnih certificiranih profesionalnih računovođa

CICA (eng. Canadian Institute of Chartered Accountants); Kanadski institut ovlaštenih računovođa

P3P (eng. Platform for Privacy Preferences); platforma za postavke privatnosti

W3C (eng. World Wide Web Consortium); organizacija koja se bavi standardizacijom tehnologija korištenih na Internetu

PPL (eng. PrimeLife Policy Language); jezik za strojno čitanje politika privatnosti

GDPR (eng. General Data Protection Regulation); Opća uredba o zaštiti podataka

FRE (eng. Flesch Reading Ease); formula za izračun čitkosti teksta

AWL (eng. Average word length); prosječna dužina riječi izražena brojem slogova

ASL (eng. Average sentence length); dužina prosječna rečenice izražena brojem riječi

FTC (eng. Federal Trade Commission); Savezna trgovinska komisija

URI (eng. Uniform Resource Identifier); jedinstveni identifikator elektroničkog izvora

NFR (eng. Non-functional requirement); nefunkcionalni zahtjev

USEMP (eng. User empowerment for Enhanced Online Management); projekt sufinanciran od Europske unije kojim je razvijen DataBait alat

EU FP7 (eng. European Union Framework Programme 7); program financiranja iz fonda Europske unije

ISMS (eng. Information Security Management System); sustav upravljanja sigurnošću informacija

ITIL (eng. Information Technology Infrastructure Library); radni okvir s nizom preporuka, procesa, procedura i zadaća osmišljenih za standardizaciju najboljih praksi upravljanja informacijskim tehnologijama

CSI (eng. Continual Service Improvement); model kontinuiranog poboljšanja usluge

GBRAM (eng. Goal-Based Requirements Analysis Method; metodi analize zahtjeva temeljena na ciljevima

PMA (eng. Privacy Management Analysis); analiza sustava za uređivanje privatnosti unutar metodologije za upravljanje privatnošću

PIA (eng. Privacy Impact Assessment); procjena utjecaja na privatnost

PIAF (eng. A Privacy Impact Assessment Framework for data protection and privacy rights); okvir i istoimeni projekt razvoja

IAPP (eng. The International Association of Privacy Professionals; IAPP); Međunarodna udruga stručnjaka za privatnost

ENISA (eng. The European Union Agency For Network and Information Security); Agencija Europske unije za mrežnu i informacijsku sigurnost

SMS (eng. Short Message Service), usluga kratkih tekstualnih poruka unutar standarda mobilne telefonije

MAC (eng. Media Access Control) adresa; adresa kontrole pristupa medijima, jedinstveni identifikator koji se dodjeljuje kontroleru mrežnog sučelja za korištenje kao mrežna adresa u komunikacijama unutar mrežnog segmenta

PRILOZI

Prilog 1 Popis obrađenih javnih zdravstvenih ustanova

Oznaka	Zdravstvena ustanova	Poveznica	Pristup
J1	Bolnica za ortopedsku kirurgiju i rehabilitaciju "Prim.dr. Martin Horvat" Rovinj	https://www.bolnica-rovinj.hr/images/dokumenti/zastita_osobnih/Izjava_o_zastiti_privatnosti_i_sigurnosti_osobnih_podataka.pdf	25.04. 2021.
J2	Dom zdravlja Koprivničko-Križevačke županije	https://dzkkz.hr/wp-content/uploads/2019/04/IZJAVA-O-ZA%C5%A0TITI-OSOBNIH-PODATAKA.pdf	17.04. 2021.
J3	Dom zdravlja Metković	http://www.dom-zdravlja-metkovic.hr/wp-content/uploads/2020/04/Politika-za%C5%A1tite-osobnih-podataka.pdf	17.04. 2021.
J4	Dom zdravlja Ogulin	https://domzdravlja-ogulin.hr/politika-privatnosti/	17.04. 2021.
J5	Dom zdravlja Sisak	https://www.dz-sisak.hr/index.php/opci-uvijeti-zastite-osobnih-podataka	17.04. 2021.
J6	Dom zdravlja Zadarske županije	https://www.dzzdzup.hr/izjava-o-zastiti-privatnosti-i-sigurnosti-osobnih-podataka	17.04. 2021.
J7	Dom zdravlja Zagrebačke županije	http://www.domzdravlja-zgz.hr/informacije/gdpr/	18.04. 2021.
J8	Dom zdravlja Zagreb Centar	https://dzz-centar.hr/wp-content/uploads/2018/11/Informacija-privola-pacijenti.pdf	18.04. 2021.
J9	Dom zdravlja Zagreb Zapad	https://www.dzz-zapad.hr/opcitekstovi.php?kat=37&title=Op%C4%87i%20akti/Izjava-o-zastiti-osobnih-podaztaka.pdf	18.04. 2021.
J10	Hrvatski zavod za hitnu medicinu	https://www.hzhm.hr/pravila-privatnosti	13.05. 2021.
J11	Hrvatski zavod za zdravstveno osiguranje	https://hzzo.hr/izjava-o-privatnosti	13.05. 2021.
J12	Istarski domovi zdravlja	https://idz.hr/wp/wp-content/uploads/2020/06/Istarski-domovi-zdravlja-Izjava-o-zastiti-osobnih-podataka.pdf	17.04. 2021.

Oznaka	Zdravstvena ustanova	Poveznica	Pristup
J13	Klinička bolnica Merkur	https://www.kb-merkur.hr/gdpr_infos/	25.04. 2021.
J14	Klinički bolnički centar "Sestre milosrdnice"	https://www.kbcsm.hr/zastitapodataka/	23.04. 2021.
J15	Klinički bolnički centar Osijek	https://www.kbco.hr/wp-content/uploads/2018/06/SKM_C224e19051313550.pdf	16.05. 2021.
J16	Klinički bolnički centar Rijeka	http://kbc-rijeka.hr/pravila-privatnosti/	16.05. 2021.
J17	Klinički bolnički centar Zagreb	https://www.kbc-zagreb.hr/EasyEdit/UserFiles/zastita-osobnih-podataka/politika-o-zastiti-osobnih-podataka-i-privatnosti.pdf	16.05. 2021.
J18	Klinika za kardiovaskularne bolesti Magdalena	http://www.magdalena.hr/media/1377/26-11-2018-izjava-o-zastiti-osobnih-podataka-magdalena.pdf	12.05. 2021.
J19	Klinika za psihijatriju Vrapče	https://bolnica-vrapce.hr/privatnost/politika-privatnosti/	12.05. 2021.
J20	Lječilište Bizovačke toplice	https://www.ljeciliste-bizovacke.hr/EasyEdit/UserFiles/politika-privatnosti-ljeciliste-bizovacke-toplice.pdf	28.04. 2021.
J21	Lječilište Veli Lošinj	https://www.ljeciliste-veli-losinj.hr/hrvatski/gdpr_2/	28.04. 2021.
J22	Nastavni zavod za hitnu medicinu Grada Zagreba	https://www.hitnazg.hr/politika-privatnosti/64	13.05. 2021.
J23	Neuropsihijatrijska bolnica "Dr. Ivan Barbot" Popovača	https://www.npbp.hr/ostalo/opci-uvjeti	02.05. 2021.
J24	Opća bolnica "Dr. Ivo Pedišić" Sisak	https://obs.hr/wp/2019/06/28/politika-zastite-osobnih-podataka	21.04. 2021.

Oznaka	Zdravstvena ustanova	Poveznica	Pristup
J25	Opća bolnica "Dr. Josip Benčević" Slavonski Brod	https://www.bolnicasb.hr/o-nama/zastita-osobnih-podataka	18.04. 2021.
J26	Opća bolnica Bjelovar	https://www.obbj.hr/o-bolnici/zastita-osobnih-podataka	21.04. 2021.
J27	Opća bolnica dr. Tomislav Bardek Koprivnica	https://www.obkoprivnica.hr/zastita-osobnih-podataka	21.04. 2021.
J28	Opća bolnica Gospić	https://www.obgospic.hr/images/pdf-2018/Pravila_privatnosti_za_Internet_stranicu-_OP%C4%86A_BOLNICA_GOSPI%C4%86.pdf	21.04. 2021.
J29	Opća bolnica Pula	http://www.obpula.hr/wp-content/uploads/izjava-za-zastitu-osobnih-podataka.pdf	25.04. 2021.
J30	Opća bolnica Virovitica	http://bolnica-virovitica.hr/dokumenti/Zaštita-osobnih-podataka.pdf	25.04. 2021.
J31	Opća bolnica Zadar	https://www.bolnica-zadar.hr/pacijenti-i-posjetitelji/prava/zastita-osobnih-podataka	25.04. 2021.
J32	Opća županijska bolnica Požega	https://www.pozeska-bolnica.hr/uvjeti-koristenja-i-privatnost-podataka	25.04. 2021.
J33	Poliklinika za prevenciju kardiovaskularnih bolesti i rehabilitaciju Srčana	https://www.srcana.hr/hr/multimedija/Obavijest%20o%20obradi%20osobnih%20podataka.pdf	02.05. 2021.
J34	Poliklinika za rehabilitaciju slušanja i govora SUVAG	http://www.suvag.hr/nova/wp-content/uploads/Politika-privatnosti-Poliklinika-SUVAG.pdf	02.05. 2021.
J35	Poliklinika za zaštitu djece grada Zagreba	https://www.poliklinika-djeca.hr/zastita-privatnosti	02.05. 2021.
J36	Psihijatrijska bolnica "Sveti Ivan"	http://www.pbsvi.hr/pravila-privatnosti	30.04. 2021.
J37	Psihijatrijska bolnica Lopača	https://www.pbl.hr/zastita-privatnosti	30.04. 2021.
J38	Psihijatrijska bolnica Rab	https://www.bolnicarab.hr/hr/politika_privatnosti/961/146	30.04. 2021.

Oznaka	Zdravstvena ustanova	Poveznica	Pristup
J39	Psihijatrijska bolnica za djecu i mladež	https://djecja-psihijatrija.hr/politika-privatnosti	30.04. 2021.
J40	Specijalna bolnica za medicinsku rehabilitaciju “Biokovka”	https://www.biokovka.hr/hr/poslovne-informacije/zastita-osobnih-podataka	25.04. 2021.
J41	Specijalna bolnica za medicinsku rehabilitaciju Lipik	https://bolnica-lipik.hr/hr/politika-privatnosti/stranica/18	25.04. 2021.
J42	Specijalna bolnica za medicinsku rehabilitaciju Naftalan	https://www.naftalan.hr/hr/opca-pravila-privatnosti/	26.04. 2021.
J43	Specijalna bolnica za medicinsku rehabilitaciju Stubičke Toplice	http://sbst.hr/opce-informacije/zastita-podataka	26.04. 2021.
J44	Specijalna bolnica za medicinsku rehabilitaciju Varaždinske Toplice	http://www.minerva.hr/zastita-osobnih-podataka	26.04. 2021.
J45	Stomatološka poliklinika Split	http://www.spst.hr/Portals/0/docs/SPST_PRAVILA_PRIVATNOSTI.pdf	02.05. 2021.
J46	Stomatološka poliklinika Zagreb	https://spz.hr/wp-content/uploads/2019/01/POLITIKA-O-ZA%C5%A0TITI-OSOBNIH-PODATAKA-I-PRIVATNOSTI-KORISNIKA-ZDRAVSTVENIH-USLUGA-ISPITANIKA.pdf	02.05. 2021.
J47	Thalasotherapia Crikvenica	https://thalasso-ck.hr/poslovne-informacije/zastita-osobnih-podataka	26.04. 2021.
J48	Zavod za hitnu medicinu Istarske županije	https://zhmiz.hr/pravila-privatnosti	17.05. 2021.

Oznaka	Zdravstvena ustanova	Poveznica	Pristup
J49	Zavod za hitnu medicinu Karlovačke županije	https://zzhm-kz.hr/izjava-o-privatnosti	17.05. 2021.
J50	Zavod za hitnu medicinu Koprivničko-križevačke županije	https://www.hitna-kckz.hr/wp-content/uploads/2018/08/Politika-o-za%C5%A1titi-osobnih-podataka-pacijenata.pdf	17.05. 2021.
J51	Zavod za hitnu medicinu Međimurske županije	https://zhm-mz.hr/pravila-privatnosti	17.05. 2021.
J52	Zavod za hitnu medicinu Požeško-slavonske županije	https://www.hitna-psz.hr/Dokumenti/Stranica/Katalog%20informacija/GDPR/politika%20za%C5%A1tite%20osobnih%20podataka%20pacijenata.pdf	17.05. 2021.
J53	Zavod za hitnu medicinu Splitsko-dalmatinske županije	https://www.zhmsdz.hr/2019/sluzbenidokumenti/pdfPolitikaOZastitiOsobnihPodatakaIPrivatnosti.pdf	17.05. 2021.
J54	Zavod za hitnu medicinu Zadarske županije	https://www.zhmzz.hr/transparentnost/za%C5%A1tita-osobnih-podataka	17.05. 2021.
J55	Županijska bolnica Čakovec	http://www.bolnica-cakovec.hr/o-nama/zastita-osobnih-podataka	17.05. 2021.
J56	Županijski zavod za hitnu medicinu Bjelovarko-bilogorske županije	https://hitnabbz.hr/?page_id=7	17.05. 2021.

Prilog 2 Popis obrađenih privatnih zdravstvenih ustanova

Oznaka	Naziv ustanove	Poveznica	Pristup
P1	Očna poliklinika Medić Jukić	https://poliklinika-medicjukic.hr/uvjeti-koristenja/	16.07. 2021.
P2	Poliklinika za oftalmologiju Knezović	https://knezovic.com.hr/pravila-privatnosti/	16.07. 2021.
P3	Specijalna bolnica za oftalmologiju Svjetlost	https://svjetlost.hr/pravila-o-privatnosti/4930	16.07. 2021.
P4	Poliklinika Bilić Vision	https://bilicvision.hr/hr/izjava-o-zastiti-podataka	16.07. 2021.
P5	Očna poliklinika "Okulistički centar"	https://www.okuc.hr/izjava-o-privatnosti	17.07. 2021.
P6	Poliklinika Optical Express	https://www.opticalexpress.hr/pravila-o-privatnosti	17.07. 2021.
P7	Dental centar Mirakul	https://dental-centar-mirakul.hr/pravila-privatnosti	18.07. 2021.
P8	Dentalni centar DentIN	https://dentin.hr/pravila-privatnosti	18.07. 2021.
P9	Poliklinika Ćosić	http://poliklinika-cosic.hr/privatnost-korisnika-web-stranice	18.07. 2021.
P10	Poliklinika Slavonija/Medicina rada Turjak	http://poliklinika-turjak.hr/izjava-o-povjerljivosti-podataka	20.07. 2021.
P11	Poliklinika Sinteza	https://poliklinika-sinteza.hr/zastita-osobnih-podataka	20.07. 2021.
P12	Specijalna bolnica Medico	https://www.medico.hr/o-nama/pravila-zastite-osobnih-podataka	20.07. 2021.
P13	Poliklinika IMED	https://imed.hr/hr/o-nama/pravila-zastite-privatnosti-osobnih-podataka	20.07. 2021.
P14	Specijalna bolnica dr. Nemec	https://www.bolnica-nemec.hr/hr/izjava_o_privatnosti/230/37	20.07. 2021.
P15	Poliklinika Sveti Rok	https://www.poliklinika-svetirok.hr/zastita-osobnih-podataka-2	23.07. 2021.
P16	Logo centar BLAŽI d.o.o.	https://www.blazi.hr/politika-privatnosti	23.07. 2021.
P17	Ustanova za zdravstvenu njegu Ćorluka	http://sanatorij.com/zastita-osobnih-podataka-ustanova	23.07. 2021.
P18	Poliklinika Croatia Osiguranje	https://www.poliklinikacroatia.hr/static/images/2019_Informacija_o_zastiti_osobnih_podataka_PKL.pdf	23.07. 2021.

Oznaka	Naziv ustanove	Poveznica	Pristup
P19	Poliklinika Atria	https://www.poliklinika-atria.hr/pravila-privatnosti	23.07. 2021.
P20	Poliklinika Fiziodent	https://fiziodent.hr/zastita-privatnosti	27.07. 2021.
P21	Poliklinika ARENA	http://arenapoliklinika.hr/zastita-privatnosti	27.07. 2021.
P22	Poliklinika Šebetić	http://poliklinika-sebetic.hr/uvjeti/poslovanje/izjava-o-privatnosti	27.07. 2021.
P23	Dental centar Picek	http://www.dentalcentarpicek.hr	27.07. 2021.
P24	Poliklinika Došen	http://www.poliklinika-drdosen.hr/pravila-privatnosti	27.07. 2021.
P25	Poliklinika Marija	https://www.poliklinikamarija.hr/wp-content/uploads/2018/05/GDPR-poliklinikamarija.pdf	27.07. 2021.
P26	Poliklinika Roth	https://www.poliklinika-roth.hr/izjava-o-privatnosti	29.07. 2021.
P27	VisoDent	https://visodent.com/uvjeti-privatnosti	29.07. 2021.
P28	Poliklinika Analizalab	https://www.poliklinika-analizalab.hr/sigurnost-podataka	29.07. 2021.
P29	Centar dentalne medicine Štimac	https://drstimac.com/pravila-privatnosti	01.08. 2021.
P30	Poliklinika Drinković	https://drinkovic.hr/pravila-privatnosti	01.08. 2021.
P31	Dentalni centar Dvojković	http://dental-dvojkovic.hr/pravila-privatnosti	01.08. 2021.
P32	Stomatološka ordinacija dr. Banožić	https://www.drbanozic.com/pravila-privatnosti	01.08. 2021.
P33	Poliklinika Krhen	https://poliklinika-krhen.hr/pravila-privatnosti	01.08. 2021.
P34	Polivalentna ordinacija dentalne medicine Bival	https://dental-bival.eu/hr/pravila-privatnosti-i-politika-kolacica	01.08. 2021.
P35	Ustanova za zdravstvenu njegu Domnius	https://domnius.hr/o-nama/pravne-informacije	02.08. 2021.
P36	Dental centar Smile	https://www.dental-centar-smile.hr/pravila-privatnosti	02.08. 2021.
P37	Poliklinika Apnea dijagnostika	http://poliklinika-apnea.hr/pravila-privatnosti	02.08. 2021.
P38	Poliklinika Cortex	https://poliklinikacortex.hr/pravila-privatnosti	02.08. 2021.
P39	Zubni rendgen dr. Lauc	https://www.lauc.net/politika-privatnosti	02.08. 2021.

Oznaka	Naziv ustanove	Poveznica	Pristup
P40	Poliklinika Lumbalis	https://lumbalis.net/politika-privatnosti	02.08. 2021.
P41	Ordinacija dentalne medicine Mdent	https://www.mdent.hr/pravila-privatnosti	03.08. 2021.
P42	Ortodoncija Reljanović Protega	https://www.ortodoncija-reljanovicprotega.hr/politika-privatnosti	03.08. 2021.
P43	Poliklinika Medikol	https://medikol.hr/zastita-osobnih-podataka	03.08. 2021.
P44	Specijalna bolnica Agram	https://www.agram-bolnica.hr/o-nama/zastita-privatnosti	03.08. 2021.
P45	Ortodoncija Šalinović	https://www.ortodoncija-salinovic.com/uvjeti-koristenja	03.08. 2021.
P46	Poliklinika dr. Lacić	http://www.poliklinika-lacic.hr	04.08. 2021.
P47	Poliklinika Šiljeg	https://www.siljeg.hr/pravila-privatnosti	04.08. 2021.
P48	Stomatološka poliklinika Ksaver	http://www.stomatolog-ksaver.hr/o-nama/izjava-o-zastiti-osobnih-podataka	04.08. 2021.
P49	Ordinacija dentalne medicine Josip Siber	https://www.siber.hr/site	04.08. 2021.
P50	Dijagnostika 2000	https://www.dijagnostika2000.hr/pravila-privatnosti	04.08. 2021.
P51	Poliklinika Sremac Bohaček	https://www.poliklinika-sremac-bohacek.com/hr/pravila-privatnosti	07.08. 2021.
P52	Poliklinika Glavić	https://www.polyclinic-glavic.com/zastita-privatnosti	07.08. 2021.
P53	Fiziovita	https://www.fiziovita.hr/pravila-privatnosti	07.08. 2021.
P54	Ordinacija Bilan	https://www.ordinacija-bilan.hr/usluge/zastita-podataka	07.08. 2021.
P55	Poliklinika Intermed	https://www.poliklinika-intermed.hr/opci-uvjeti#zastita-privatnosti	07.08. 2021.
P56	Dentex stomatološka poliklinika	https://www.dentex-croatia.com/hr/politika-privatnosti	07.08. 2021.
P57	Poliklinika za stomatološku protetiku, ortodonciju dr. Zubović	https://zubovic.com/privatnost	08.08. 2021.
P58	Poliklinika Niveus	https://niveus-poliklinika.hr/izjava-o-povjerljivosti	08.08. 2021.
P59	Zagorje zub	https://zagorjezub.com/polica-privatnosti	08.08. 2021.
P60	Poliklinika Žaja	https://poliklinikazaja.hr/zastita-podataka	08.08. 2021.

Oznaka	Naziv ustanove	Poveznica	Pristup
P61	B.dent	https://www.bdent.eu/hr/pravila-o-privatnosti	08.08. 2021.
P62	Poliklinika Arcadia	https://poliklinika-arcadia.hr/pravila-privatnosti	09.08. 2021.
P63	Stomatološka Poliklinika Dr. Pavlić	https://poliklinika-pavlic.hr/ortodoncija-rijeka/zastita-privatnosti	09.08. 2021.
P64	Optički studio i poliklinika Monokl	https://www.monokl.hr/info/privatnost	09.08. 2021.
P65	Poliklinika Perić-Staničić	https://www.poliklinika-ps.hr/zastita-osobnih-podataka	09.08. 2021.
P66	Poliklinika Trupeljak	https://www.trupeljak.hr/izjava-o-privatnosti	09.08. 2021.
P67	Poliklinika Analiza	https://poliklinika-analiza.hr/politika-zastite-osobnih-podataka	10.08. 2021.
P68	Poliklinika Breyer	http://breyer.hr/info/obavijest-o-obradi-podataka-korisnici-usluga	10.08. 2021.
P69	Dentalni implantološko protetski centar Hurčak	https://dipc.hr/politika-privatnosti	10.08. 2021.
P70	Poliklinika MedikaDent	https://medikadent.com/polica-privatnosti	10.08. 2021.
P71	Dentus Perfectus d.o.o.	https://www.dentusperfectus.hr/politika-privatnosti	10.08. 2021.
P72	Poliklinika Konja	https://poliklinikakonja.hr/politika-privatnosti	12.08. 2021.
P73	Poliklinika Dermaplus	https://poliklinika-dermaplus.com/pravila-zastite-privatnosti	12.08. 2021.
P74	Poliklinika Poliderma	https://poliderma.hr/o-poliklinici/pravila-privatnosti	12.08. 2021.
P75	Affidea Hrvatska	https://affidea.hr/obavijest-o-privatnosti-podataka-web-mjesta-drustva-affidea	12.08. 2021.
P76	Poliklinika Magnolija	https://www.poliklinika-magnolija.hr/uporaba-kolacica#politika_privatnosti	12.08. 2021.
P77	Poliklinika Binova	https://poliklinika-binova.hr/pravila-privatnosti	13.08. 2021.
P78	Poliklinika Kaliper	https://kaliper.hr/zastita-osobnih-podataka	13.08. 2021.
P79	Poliklinika Kvarantan	https://poliklinika-kvarantan.hr/izjava-o-zastiti-privatnosti	13.08. 2021.
P80	Poliklinika Vura	http://poliklinika-vura.hr/home/pravne-obavijesti/izjava-o-zastiti-osobnih-podataka	13.08. 2021.
P81	Dental Kraljić	https://www.dental-kraljic.com/pravila-privatnosti	13.08. 2021.

Oznaka	Naziv ustanove	Poveznica	Pristup
P82	Poliklinika Lekić	http://poliklinika-lekic.hr/zastita-osobnih-podataka/zastita-osobnih-podataka	13.08. 2021.
P83	LedikDent	https://ledikdent.hr/hr/izjava-o-privatnosti	14.08. 2021.
P84	Poliklinika Lastrić	https://www.poliklinika-lastric.hr/polica-privatnosti	14.08. 2021.
P85	Ordinacija Ortolook	https://ortolook.hr/pravila-privatnosti	14.08. 2021.
P86	Poliklinika Šlaj-Anić	https://www.slaj-anic.com/gdpr	14.08. 2021.
P87	Poliklinika K-centar	https://www.k-centar.hr/politika-privatnosti	14.08. 2021.
P88	Specijalistička ordinacija dentalne medicine Ivanec	https://ortodoncija-ivanec.hr/privatnost-podataka	14.08. 2021.
P89	Poliklinika PremiumDent	https://www.premiumdent.hr/polica-privatnosti	17.08. 2021.
P90	Ortodoncija Ana Petrović	http://www.ortodoncija-anapetrovic.hr/politika-privatnosti	17.08. 2021.
P91	Stomatologija i estetika dr. Goran Jovićević	https://sie.hr/hr/uvjeti-koristenja-stranice	17.08. 2021.
P92	Ordinacija Knego	https://www.ordinacijaknego.hr/pravila-privatnosti	17.08. 2021.
P93	Poliklinika Nika	https://www.poliklinika-nika.hr/hr/polica-privatnosti	18.08. 2021.
P94	Dental centar Dijan	https://www.dentaldijan.com/hr/pravila-privatnosti	18.08. 2021.
P95	Poliklinika Nado	https://www.nado.hr/pravila-o-privatnosti	18.08. 2021.
P96	Poliklinika Homolak	https://poliklinika-homolak.hr/zastita-privatnosti	18.08. 2021.

Prilog 3 Analitička matrica i kodni list

Oznaka	Zahtjev	Kodiranje
T11	**Pružanje informacija kako i koji podaci se prikupljaju**	
T11a	Mehanizmi prikupljanja podataka jasno su objašnjeni	0.5
T11b	Definirani su podaci ili kategorije podataka koje se prikupljaju	0.5
T28	**Informiranje o drugim izvorima podataka**	
T28a	Navedeno je postoje li drugi izvori podataka (treća strana)	0.75
T28b	Mehanizmi prikupljanja i obrade podataka jasno su objašnjeni	0.25
T19	**Pružiti dovoljno objašnjenja kada se koriste osjetljivi podaci**	
T19a	Korištenje posebne kategorije podataka je spomenuto.	1
T10	**Pružanje informacije o osobnim podacima potrebnim za specificiranu svrhu obrade.**	
T10a	Svrhe obrade (kategorija) podataka jasno su navedene	0.75
T10b	Navedeni su podaci ili kategorije podataka koji se obrađuju u pojedinoj svrsi obrade	0.25
T23	**Objasniti zašto je svrha prikupljanja podataka legitimna.**	
T23a	Navedene su pravne osnove za obradu podataka organizacije	0.75
T23b	Pravne osnove su definirane za svaku obradu podataka	0.25
T4	**Određivanje strana s kojima podaci mogu biti dijeljeni; otkriveni.**	
T4a	Postoji sekcija u dokumentu u kojoj je navedeno (ne)postojanje trećih strana	0.25
T4b	Navedene su treće strane s kojima se dijele podaci	0.5
T4c	Navedene su podaci ili kategorije podataka koji se dijele	0.25
T27	**Pružanje informacija o transferu podataka prema trećoj zemlji ili međunarodnoj organizaciji i razinu zaštite koja je pružena od te strane.**	
T27a	Postoji sekcija u dokumentu u kojoj je navedeno (ne)postojanje transfera podataka unutar ili izvan gospodarskog pojasa EU)	0.5

Oznaka	Zahtjev	Kodiranje
T27b	Navedeno je i objašnjeno dijeljenje podataka prema trećim zemljama	0.25
T27c	Definirane su mjere zaštite pri transferu podataka	0.25
T13	**Pružanje informacija kako i koji podaci se pohranjuju**	
T13a	Navedeni su mehanizmi za pohranu podataka	0.5
T13b	Navedeni su podaci ili kategorije podataka u sustavu pohrane	0.5
T15	**Pružanje informacija o roku pohrane podataka i njihovom brisanju.**	
T15a	Navedeni su rokovi pohrane ili kriteriji za njihovo određivanje	0.75
T15b	Objašnjeni su postupci po navedenom roku (brisanje, anomimizirana pohrana)	0.25
T22	**Informiranje o (sigurnosnim) mehanizmima za zaštitu podataka**	
T22a	Mehanizmi sigurnosti podataka su navedeni	0.75
T22b	Mehanizmi zaštite eksplicitno su objašnjeni	0.25
T6	**Pružanje informacija o mogućnostima ograničavanja obrade osobnih podataka**	
T6a	Mogućnost ograničavanja obrade od strane ispitanika jasno je objašnjena	0.75
T6b	Postupak ograničavanja obrade osobnih podataka jasno je definiran	0.25
T26	**Pružanje informacija o pravu pristupa podacima, ispravljanju, brisanju podataka te prigovoru na obradu podataka**	
T26a	Pravo ispitanika na pristup podacima jasno je izrečeno	0.25
T26b	Pravo ispitanika na ispravak podataka jasno je izrečeno	0.25
T26c	Pravo ispitanika na brisanje podataka jasno je izrečeno	0.25
T26d	Pravo ispitanika na prigovor obradi podataka jasno je izrečeno	0.25
T7	**Pružanje informacija o sredstvima za pristup, ispravak i uklanjanje osobnih podataka.**	
T7a	Postupak pristupa podacima je jasno definiran	0.33
T7b	Postupak ispravka podataka jasno je objašnjen	0.33

Oznaka	Zahtjev	Kodiranje
T7c	Postupak brisanja podataka jasno je objašnjen	0.33
T5	**Pružanje informacija o identitetu i kontaktu voditelja obrade.**	
T5a	Identitet voditelja obrade jasno je naveden	0.5
T5b	Kontakt podaci i mehanizmi voditelja obrade jasno su navedeni	0.5
T2	**Dokumenti politika lako su dostupni**	0-1
T18	**Jezik za pružanje informacija treba biti jasan i prilagođen.**	
T18a	Informacije su pružene jasnim jezikom	0.5
T18b	Jezik je prilagođen ciljnoj skupini	0.5
AŽ	**Pružene su informacije o ažuriranosti stranica**	
AŽ1	Datum posljednjeg ažuriranja eksplicitno je naveden	0.75
AŽ2	Pružene su informacije o načinu obavještavanja ispitanika o izmjenama politika privatnosti	0.25
SL	**Informacije su prikazane slojevitim prikazom**	
SL1	Izražena je tendencija grupiranju informacija s obzirom na tematske cjeline, odnosno sekcije.	0.5
SL2	Hijerarhija teksta označena je naslovima ili drugim (grafičkim) metodama	0.5
LG	Dokument nije prezasićen informacijama	0/0.5/1

Prilog 4 Metodologija odabira računalnog programa za računanje slogova

Prilikom odabira računalnog programa za brojanje slogova kao materijal je uzet dokument politika privatnosti hrvatskog nadzornog tijela za provedbu Opće uredbe o zaštiti podataka – Agencije za zaštitu osobnih podataka (AZOP) [17].

Probni uzorak je uzet u odnosu na različite tematske sekcije politike privatnosti tako da je izdvojen jedan odlomak sekcije koji je nastavno kopiran u aplikaciju Word. Na svakome odlomku pristupilo se prvo „ručnom“ brojanju slogova od strane autorice, profesorice hrvatskog jezika i književnosti, a zatim je nad tekstom provedena analiza kroz tri računalna alata dostupna na Internetu. Računalni program 1 odnosi se na aplikaciju dostupnu na mrežnoj stranici: https://syllablecounter.org. Računalni program 2 odnosi se na kalkulator slogova dostupan na stranici: https://www.wordcalc.com/, dok je računalni program 3 dostupan na mrežnom mjestu https://syllablecounter.net/. Rezultati analize prikazani su u Tablici 25.

Tablica 25 Usporedni prikaz rezultata prilikom brojenja slogova

	Broj slogova			
	Ručno brojanje	**Program 1**	**Program 2**	**Program 3**
Prikupljanje podataka/kolekcija	156	145	158	145
Svrha obrade podataka	100	104	84	89
Kontrola	215	212	197	182
Retencija	105	103	86	90
Sigurnost	144	145	130	133
Promjena politika privatnosti	104	103	85	89
Dijeljenje podataka s trećim stranama	144	144	124	130

[17] Test dokumenta nalazi se na stranici: https://azop.hr/politika-privatnosti/

Prilog 5 Rezultati istraživanja

Prilog 5.1. Rezultati istraživanja javnih zdravstvenih ustanova od zahtjeva T11 do T27

Oznaka	T11	T11a	T11b	T28	T28a	T28b	T19	T19a	T10	T10a	T10b	T23	T23a	T23b	T4	T4a	T4b	T4c	T27	T27a	T27b	T27c
J1	1	.5	.5	0	0	0	0	0	1	.75	.25	1	.75	.25	.8	.25	.5	0	0	0	0	0
J2	1	.5	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	.5	.5	0	0
J3	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	.8	.25	.5	0	0	0	0	0
J4	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
J5	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	.8	.25	.5	0	0	0	0	0
J6	1	.5	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	0	0	0	0
J7	1	.5	.5	.75	.75	0	1	1	1	.75	.25	1	.75	.25	.8	.25	.5	0	1	.5	.25	.25
J8	0	0	0	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	0	0	0	0
J9	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J10	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J11	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J12	0	0	0	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	.8	.5	.25	0
J13	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
J14	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
J15	1	.5	.5	0	0	0	0	0	1	.75	.25	0	0	0	.8	.25	.5	0	0	0	0	0
J16	1	.5	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	1	.25	.5	.25	0	0	0	0
J17	.5	.5	0	0	0	0	0	0	.75	.75	0	0	0	0	.8	.25	.5	0	.5	.5	0	0
J18	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J19	1	.5	.5	1	.75	.25	0	0	1	.75	.25	.75	.75	0	1	.25	.5	.25	0	0	0	0
J20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J21	.5	0	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	0	0	0	0
J22	.5	0	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	0	0	0	0
J23	1	.5	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	0	0	0	0
J24	1	.5	.5	0	0	0	0	0	0	0	0	0	0	0	.3	.25	0	0	0	0	0	0
J25	.5	0	.5	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	1	.5	.25	.25
J26	1	.5	.5	0	0	0	0	0	1	.75	.25	0	0	0	1	.25	.5	.25	1	.5	.25	.25
J27	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J28	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
J29	0	0	0	0	0	0	0	0	.75	.75	.25	.75	.75	0	0	0	0	0	0	0	0	0
J30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J31	1	.5	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	1	.25	.5	.25	0	0	0	0
J32	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J33	0	0	0	0	0	0	0	0	.75	.75	0	.75	.75	0	0	0	0	0	0	0	0	0
J34	1	.5	.5	.75	.75	0	0	0	1	.75	.25	.75	.75	0	0	0	0	0	0	0	0	0
J35	1	.5	.5	1	.75	.25	0	0	.75	.75	0	.75	.75	0	1	.25	.5	.25	0	0	0	0
J36	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
J37	0	0	0	0	0	0	0	0	.75	.75	0	.75	.75	0	.8	.25	.5	0	0	0	0	0
J38	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J39	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
J40	.5	.5	0	0	0	0	0	0	0	0	0	0	0	0	.3	.25	0	0	0	0	0	0
J41	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.8	.25	.5	0	0	0	0	0
J42	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J44	.5	.5	0	0	0	0	0	0	0	0	0	0	0	0	.3	.25	0	0	.5	.5	0	0
J45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	.5	0	0
J46	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
J47	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.8	.25	.5	0	0	0	0	0
J48	.5	.5	0	0	0	0	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
J49	.5	.5	0	0	0	0	0	0	0	0	0	0	0	0	.8	.25	.5	0	0	0	0	0
J50	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	.8	.25	.5	0	0	0	0	0
J51	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	.8	.25	.5	0	0	0	0	0
J52	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
J53	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J54	.5	.5	0	0	0	0	0	0	.75	.75	0	0	0	0	.3	.25	0	0	0	0	0	0
J55	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J56	0	0	0	0	0	0	0	0	.75	.75	0	.75	.75	0	.3	.25	0	0	0	0	0	0

Prilog 5.2. Rezultati istraživanja javnih zdravstvenih ustanova od zahtjeva T13 do T5

Oznaka	T13	T13a	T13b	T15	T15a	T15b	T22	T22a	T22b	T6	T6a	T6b	T26	T26a	T26b	T26c	T26d	T7	T7a	T7b	T7c	T5	T5a	T5b
J1	0	0	0	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J2	0	0	0	.8	.75	0	.8	.75	0	.8	.75	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
J3	0	0	0	1	.75	.25	1	.25	.75	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J4	0	0	0	1	.75	.25	1	.75	.25	.8	.75	0	1	.25	.25	.25	.25	.33	.3	0	0	1	.5	.5
J5	0	0	0	1	.75	.25	1	.75	.25	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J6	0	0	0	1	.75	.25	.8	.75	0	.8	.75	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
J7	0	0	0	1	.75	.25	.8	.75	0	1	.75	.25	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J8	.5	.5	0	.8	.75	0	1	.75	.25	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J9	0	0	0	.8	.75	0	.8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J10	0	0	0	0	0	0	.8	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J11	0	0	0	1	.75	.25	1	.25	.75	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J12	0	0	0	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J13	0	0	0	1	.75	.25	1	.75	.25	.8	.75	0	1	.25	.25	.25	.25	.33	.3	0	0	1	.5	.5
J14	0	0	0	1	.75	.25	1	.75	.25	.8	.75	0	1	.25	.25	.25	.25	.33	.3	0	0	1	.5	.5
J15	1	.5	.5	.3	0	.25	.8	.75	0	1	.75	.25	1	.25	.25	.25	.25	0	0	0	0	.5	0	.5
J16	0	0	0	1	.75	.25	.3	.25	0	1	.75	.25	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J17	0	0	0	.8	.75	0	1	.75	.25	.8	.75	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
J18	0	0	0	0	0	0	.8	.75	0	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J19	1	.5	.5	1	.75	.25	.8	.75	0	1	.75	.25	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J20	0	0	0	0	0	0	0	0	0	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J21	0	0	0	1	.75	.25	.8	.75	0	1	.75	.25	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
J22	0	0	0	1	.75	.25	.3	.25	0	1	.75	.25	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J23	0	0	0	1	.75	.25	.8	.75	0	.8	.75	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
J24	0	0	0	1	.75	.25	.3	.25	0	.8	.75	0	0	0	0	0	0	0	0	0	0	0	0	0
J25	0	0	0	.8	.75	0	1	.25	.75	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J26	1	.5	.5	.8	.75	0	1	.75	.25	0	0	0	.8	0	.25	.25	.25	1	.3	.3	.3	.5	0	.5
J27	0	0	0	.8	.75	0	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	1	.3	.3	.3	.5	0	.5
J28	0	0	0	0	0	0	.8	.75	0	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J29	0	0	0	0	0	0	0	0	0	1	.75	.25	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J30	0	0	0	0	0	0	.8	.75	0	0	0	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
J31	0	0	0	1	.75	.25	.8	.75	0	1	.75	.25	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J32	0	0	0	0	0	0	0	0	0	.3	0	.25	.8	.25	.25	.25	0	.33	0	0	.3	.5	0	.5
J33	0	0	0	0	0	0	.8	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	1	.5	.5
J34	0	0	0	0	0	0	.3	.25	0	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	.5	0	.5
J35	0	0	0	1	.75	.25	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	.33	.3	0	0	1	.5	.5
J36	0	0	0	0	0	0	.8	.75	0	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J37	.5	.5	0	.8	.75	0	1	.25	.75	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J38	.5	.5	0	1	.75	.25	0	0	0	0	0	0	.8	.25	.25	.25	0	1	.3	.3	.3	1	.5	.5
J39	0	0	0	0	0	0	.3	.25	0	.8	.75	0	.8	.25	.25	.25	0	0	0	0	0	0	0	0
J40	0	0	0	0	0	0	.8	.75	.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J41	.5	.5	0	0	0	0	.8	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	0	.5
J42	0	0	0	0	0	0	.3	.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J43	0	0	0	0	0	0	.8	.75	0	0	0	0	1	.25	.25	.25	.25	1	.3	.3	.3	.5	0	.5
J44	0	0	0	.8	.75	0	0	0	0	.8	.75	0	0	0	0	0	0	0	0	0	0	0	0	0
J45	0	0	0	0	0	0	0	0	0	.8	.75	0	.8	.25	.25	.25	0	0	0	0	0	.5	0	.5
J46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	.3	.3	.3	1	.5	.5
J47	.5	.5	0	0	0	0	.8	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	0	.5
J48	.5	.5	0	0	0	0	.8	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J49	.5	.5	0	0	0	0	.8	.75	0	0	0	0	.8	.25	.25	.25	0	1	.3	.3	.3	.5	0	.5
J50	0	0	0	.8	.75	0	0	0	0	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J51	0	0	0	.8	.75	0	0	0	0	.8	.75	0	1	.25	.25	.25	.25	1	.3	.3	.3	1	.5	.5
J52	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
J53	0	0	0	.3	0	.25	0	0	0	.8	.75	0	1	.25	.25	.25	.25	0	0	0	0	.5	0	.5
J54	0	0	0	0	0	0	0	0	0	0	0	0	.3	0	0	.25	0	.33	0	0	.3	0	0	0
J55	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	0	.5
J56	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Prilog 5.3. Rezultati istraživanja javnih zdravstvenih ustanova od zahtjeva T2 do LG

Oznaka	T2	T18	T18a	T18b	AŽ	AŽ1	AŽ2	SL	SL1	SL2	LG
J1	.3	0	0	0	.3	0	.3	1	.5	.5	0
J2	.7	0	0	0	.3	0	.3	1	.5	.5	0
J3	1	0	0	0	0	0	0	1	.5	.5	0
J4	.7	0	0	0	0	0	0	1	.5	.5	0
J5	.7	0	0	0	.8	.8	0	1	.5	.5	0
J6	.7	0	0	0	.8	.8	0	1	.5	.5	0
J7	1	0	0	0	.3	0	.3	1	.5	.5	0
J8	.7	0	0	0	.8	.8	0	1	.5	.5	0
J9	1	0	0	0	0	0	0	.5	.5	0	0
J10	1	0	0	0	0	0	0	.5	.5	0	0
J11	1	0	0	0	.8	.8	0	1	.5	.5	0
J12	1	0	0	0	.3	0	.3	.5	.5	0	0
J13	.7	0	0	0	.8	.8	0	1	.5	.5	0
J14	.7	0	0	0	.8	.8	0	1	.5	.5	0
J15	1	0	0	0	.3	0	.3	1	.5	.5	.5
J16	.7	0	0	0	.3	0	.3	1	.5	.5	.5
J17	.7	0	0	0	1	.8	.3	1	.5	.5	.5
J18	1	0	0	0	1	.8	.3	1	.5	.5	.5
J19	.7	0	0	0	0	0	0	1	.5	.5	.5
J20	1	0	0	0	.8	.8	0	1	.5	.5	.5
J21	.7	0	0	0	.3	0	.3	1	.5	.5	.5
J22	1	0	0	0	1	.8	.3	1	.5	.5	.5
J23	1	0	0	0	.3	0	.3	.5	.5	0	.5
J24	1	0	0	0	0	0	0	0	0	0	.5
J25	1	0	0	0	0	0	0	.5	0	.5	.5
J26	1	.5	0	.5	0	0	0	1	.5	.5	.5
J27	1	0	0	0	0	0	0	1	.5	.5	.5
J28	.5	0	0	0	0	0	0	0	0	0	.5
J29	1	0	0	0	0	0	0	.5	0	.5	.5
J30	1	0	0	0	0	0	0	1	.5	.5	.5
J31	1	0	0	0	1	.8	.3	1	.5	.5	.5
J32	1	1	.5	.5	.3	0	.3	0	0	0	.5
J33	1	0	0	0	0	0	0	.5	.5	0	.5
J34	.7	0	0	0	0	0	0	1	.5	.5	.5
J35	.7	0	0	0	.8	.8	0	1	.5	.5	.5
J36	1	0	0	0	0	0	0	.5	0	.5	.5
J37	1	0	0	0	1	.8	.3	1	.5	.5	.5
J38	1	.5	0	.5	0	0	0	1	.5	.5	.5
J39	1	0	0	0	1	.8	.3	1	.5	.5	.5
J40	1	.5	0	.5	.3	0	.3	.5	0	.5	.5
J41	1	0	0	0	.3	0	.3	1	.5	.5	.5
J42	1	0	0	0	.3	0	.3	1	.5	.5	.5
J43	1	0	0	0	0	0	0	0	0	0	1
J44	1	1	.5	.5	0	0	0	.5	.5	0	1
J45	1	0	0	0	0	0	0	0	0	0	1
J46	.7	0	0	0	0	0	0	1	.5	.5	1
J47	1	0	0	0	.3	0	.3	1	.5	.5	1
J48	1	0	0	0	.3	0	.3	1	.5	.5	1
J49	1	0	0	0	.8	.8	0	.5	.5	0	1
J50	.7	0	0	0	.8	.8	0	1	1	1	1
J51	.7	0	0	0	.8	.8	0	1	.5	.5	1
J52	1	0	0	0	0	0	0	0	0	0	1
J53	.7	0	0	0	1	.8	.3	0	0	0	1
J54	1	.5	0	.5	0	0	0	0	0	0	1
J55	.7	0	0	0	0	0	0	0	0	0	1
J56	1	0	0	0	0	0	0	0	0	0	1

Prilog 5.4. Rezultati istraživanja privatnih zdravstvenih ustanova (P1-P57) od zahtjeva T11 do T27

Oznaka	T11	T11a	T11b	T28	T28a	T28b	T19	T19a	T10	T10a	T10b	T23	T23a	T23b	T4	T4a	T4b	T4c	T27	T27a	T27b	T27c
P1	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	0	0	0	0	.25	0	.25	0
P2	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	0	0	0	0
P3	1	.5	.5	0	0	0	0	0	1	.75	.25	0	0	0	1	.25	.5	.25	0	0	0	0
P4	.5	0	.5	0	0	0	0	0	1	.75	.25	1	.75	.25	.75	.25	.5	0	0	0	0	0
P5	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.25	.25	0	0	0	0	0	0
P6	1	.5	.5	1	.75	.25	0	0	1	.75	.25	.75	.75	0	1	.25	.5	.25	1	.5	.25	.25
P7	1	.5	.5	1	.75	.25	0	0	1	.75	.25	1	.75	.25	1	.25	.5	.25	1	.5	.25	.25
P8	1	.5	.5	.75	.75	0	0	0	.75	.75	.25	0	0	0	0	0	0	0	0	0	0	0
P9	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
P10	.5	.5	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
P11	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	0	0	0	0
P12	1	.5	.5	0	0	0	0	0	1	.75	.25	1	.75	.25	0	0	0	0	0	0	0	0
P13	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
P14	1	.5	.5	1	.75	.25	0	0	1	.75	.25	1	.75	.25	.75	.25	.5	0	.75	.5	.25	0
P15	0	0	0	0	0	0	0	0	0	0	0	.75	.75	0	.25	.25	0	0	0	0	0	0
P16	1	.5	.5	0	0	0	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
P17	1	.5	.5	1	.75	.25	0	0	1	.75	.25	1	.75	.25	.25	.25	0	0	1	.5	.25	.25
P18	1	.5	.5	1	.75	.25	1	1	.75	.75	0	1	.75	.25	1	.25	.5	.25	0	0	0	0
P19	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	0	0	0	0
P20	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
P21	.5	.5	0	.75	.75	0	0	0	0	0	0	0	0	0	.25	.25	0	0	0	0	0	0
P22	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	0	0	0	0	.25	0	.25	0
P23	.5	.5	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P24	1	.5	.5	1	.75	.25	0	0	.75	.75	.25	.75	.75	0	.75	.25	.5	0	0	0	0	0
P25	1	.5	.5	1	.75	.25	0	0	0	0	0	.75	.75	0	.5	0	.5	0	.25	0	.25	0
P26	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	.75	0	.5	.25	0	0	0	0
P27	.5	.5	0	.75	.75	0	0	0	.75	.75	0	0	0	0	.25	.25	.5	.25	1	.5	.25	.25
P28	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	1	.25	.5	.25	0	0	0	0
P29	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	0	0	0	0	.75	.5	.25	0
P30	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
P31	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.25	.25	0	0	0	0	0	0
P32	.5	.5	0	1	.75	.25	0	0	0	0	0	0	0	0	.75	.25	.5	0	.75	.5	.25	0
P33	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.25	.25	0	0	0	0	0	0
P34	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	1	.25	.5	.25	0	0	0	0
P35	.5	.5	0	.75	.75	0	0	0	.75	.75	0	.75	.75	0	.75	.25	.5	0	0	0	0	0
P36	0	0	0	.75	.75	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
P37	1	.5	.5	1	.75	.25	0	0	.75	0	0	.75	.75	0	0	0	0	0	0	0	0	0
P38	.5	.5	0	.75	.75	0	0	0	.75	.75	0	.75	.75	0	.5	0	.5	0	0	0	0	0
P39	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	.5	0	.25	.25
P40	.5	.5	0	1	.75	.25	0	0	.75	.75	0	.75	.75	0	.5	0	.5	0	.25	0	.25	0
P41	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.5	0	.5	0	0	0	0	0
P42	0	0	0	1	.75	.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P43	.5	.5	0	0	0	0	0	0	.75	.75	0	1	.75	.25	1	.25	.5	.25	0	0	0	0
P44	1	.5	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	1	.25	.5	.25	0	0	0	0
P45	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	0	0	0	0	1	.5	.25	.25
P46	.5	.5	0	0	0	0	1	1	.75	.75	0	.75	.75	0	.75	.25	.5	0	1	.5	.25	.25
P47	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	.75	.5	.25	0
P48	.5	0	.5	0	0	0	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	1	.5	.25	.25
P49	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	1	.25	.5	.25	0	0	0	0
P50	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.5	0	.5	0	0	0	0	0
P51	1	.5	.5	1	.75	.25	0	0	1	.75	.25	.75	.75	0	.25	.25	0	0	1	.5	.25	.25
P52	1	.5	.5	1	.75	.25	0	0	1	.75	.25	1	.75	.25	.5	0	.5	0	0	0	0	0
P53	1	.5	.5	1	.75	.25	0	0	1	.75	.25	.75	.75	0	.25	.25	0	0	1	.5	.25	.25
P54	0	0	0	.75	.75	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
P55	0	0	0	1	.75	.25	0	0	.75	.75	0	0	0	0	.25	.25	0	0	0	0	0	0
P56	1	.5	.5	.75	.75	0	0	0	.75	.75	0	1	.75	.25	.75	.25	.5	0	1	.5	.25	.25
P57	1	.5	.5	1	.75	.25	0	0	1	.75	.25	1	.75	.25	.25	.25	.5	.25	0	0	0	0

Prilog 5.5. Rezultati istraživanja privatnih zdravstvenih ustanova (P58-P96) od zahtjeva T11 do T27

Oznaka	T11	T11a	T11b	T28	T28a	T28b	T19	T19a	T10	T10a	T10b	T23	T23a	T23b	T4	T4a	T4b	T4c	T27	T27a	T27b	T27c
P58	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	.5	0	.5	0	0	0	0	0
P59	.5	.5	0	1	.75	.25	0	0	.75	.75	.25	0	0	0	0	0	0	0	1	.5	.25	.25
P60	.5	.5	0	.75	.75	0	0	0	1	.75	.25	0	0	0	.75	.25	.5	0	.75	.5	.25	0
P61	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	.5	0	.5	0	.25	0	.25	0
P62	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
P63	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	0	0	0	0	0	0	0	0
P64	1	.5	.5	.75	.75	0	0	0	1	.75	.25	0	0	0	0	0	0	0	0	0	0	0
P65	1	.5	.5	.75	.75	0	0	0	1	.75	.25	0	0	0	.75	.25	.5	0	0	0	0	0
P66	.5	0	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.5	0	.5	0	0	0	0	0
P67	1	.5	.5	.75	.75	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0
P68	1	.5	.5	1	.75	.25	1	1	1	.75	.25	1	.75	.25	.75	.25	.5	0	0	0	0	0
P69	.5	.5	0	.75	.75	.25	0	0	.75	.75	0	.75	.75	.25	.75	.25	.5	0	0	0	0	0
P70	.5	0	.5	0	0	0	0	0	.75	.75	0	0	0	0	.25	.25	0	0	0	0	0	0
P71	1	.5	.5	0	0	0	0	0	.75	.75	0	.75	.75	0	.25	.25	0	0	0	0	0	0
P72	1	.5	.5	1	.75	.25	0	0	.75	.75	.25	.75	.75	0	0	0	0	0	0	0	0	0
P73	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	.5	0	.5	0	0	0	0	0
P74	.5	0	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	0	0	0	0
P75	.5	.5	0	1	.75	.25	0	0	.75	.75	.25	.75	.75	0	.75	.25	.5	0	1	.5	.25	.25
P76	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P77	.5	.5	0	0	0	0	0	0	0	0	0	0	0	0	.5	.25	0	.25	0	0	0	0
P78	1	.5	.5	0	0	0	1	1	1	.75	.25	.75	.75	0	.5	0	.5	0	0	0	0	0
P79	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	0	0	0	0	0	0	0	0
P80	.5	.5	0	1	.75	.25	0	0	.75	.75	0	0	0	0	.5	0	.5	0	1	.5	.25	.25
P81	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	1	.25	.5	.25	0	0	0	0
P82	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	0	0	0	0	1	.5	.25	.25
P83	.5	0	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	0	0	0	0
P84	1	.5	.5	1	.75	.25	0	0	1	.75	.25	0	0	0	.75	.25	.5	0	0	0	0	0
P85	1	.5	.5	1	.75	.25	0	0	.75	.75	0	0	0	0	.75	.25	.5	0	0	0	0	0
P86	.5	.5	0	1	.75	.25	0	0	0	0	0	0	0	0	.25	.25	0	0	.25	0	0	.25
P87	1	.5	.5	0	0	0	0	0	1	.75	.25	0	0	0	.25	.25	0	0	0	0	0	0
P88	1	.5	.5	0	0	0	0	0	1	.75	.25	.25	0	.25	1	25	.5	.25	0	0	0	0
P89	1	.5	.5	1	.75	.25	0	0	1	.75	0	0	0	0	.75	0	.5	.25	1	.5	.25	.25
P90	.5	.5	0	1	.75	.25	0	0	0	0	0	0	0	0	.25	.25	0	0	0	0	0	0
P91	.5	.5	0	1	.75	.25	0	0	0	0	0	0	0	0	.75	.25	.5	0	0	0	0	0
P92	.5	.5	0	.75	.75	0	0	0	.75	.75	0	.75	.75	0	.25	.25	0	0	0	0	0	0
P93	1	.5	.5	1	.75	.25	0	0	1	.75	.25	.75	.75	0	.25	.25	0	0	1	.5	.25	.25
P94	1	.5	.5	1	.75	.25	0	0	1	.75	.25	.75	.75	0	.25	.25	0	0	1	.5	.25	.25
P95	1	.5	.5	1	.75	.25	0	0	1	.75	.25	.75	.75	0	.25	.25	0	0	1	.5	.25	.25
P96	1	.5	.5	.75	.75	0	1	1	1	.75	.25	.75	.75	0	0	0	0	0	1	.5	.25	.25

Prilog 5.6. Rezultati istraživanja privatnih zdravstvenih ustanova (P1-P55) od zahtjeva T13 do T5

Oznaka	T13	T13a	T13b	T15	T15a	T15b	T22	T22a	T22b	T6	T6a	T6b	T26	T26a	T26b	T26c	T26d	T7	T7a	T7b	T7c	T5	T5a	T5b
P1	0	0	0	1	.75	.25	.75	.75	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	0	0	0
P2	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	0	.5
P3	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	0	.5
P4	0	0	0	.75	.75	0	0	0	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P5	0	0	0	0	0	0	.75	.75	0	0	0	0	.75	.25	.25	.25	0	1	.33	.33	.33	1	.5	.5
P6	0	0	0	1	.75	.25	0	0	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P7	.5	.5	0	1	.75	.25	1	.75	.25	.75	.75	0	1	.25	.25	.25	.25	.33	.33	.33	.33	1	.5	.5
P8	.5	.5	0	1	.75	.25	0	0	0	.75	.75	0	.75	.25	.25	.25	0	1	.33	.33	.33	.5	0	.5
P9	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P11	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	0	.5
P12	0	0	0	1	.75	.25	0	0	0	1	.75	.25	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
P13	0	0	0	0	0	0	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P14	0	0	0	.75	.75	0	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P15	0	0	0	.75	.75	0	0	0	0	0	0	0	.75	.25	.25	.25	0	0	0	0	0	1	.5	.5
P16	.5	.5	0	.25	0	.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P17	0	0	0	1	.75	.25	0	0	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P18	0	0	0	.75	.75	0	0	0	0	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P19	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	.5	0	.5
P20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P21	0	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0
P22	0	0	0	1	.75	.25	.75	.75	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	0	0	0
P23	0	0	0	1	.75	.25	0	0	0	0	0	0	.25	0	0	.25	0	.33	0	0	.33	.5	0	.5
P24	1	.5	.5	1	.75	.25	.75	.75	.25	0	0	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
P25	.5	.5	0	.75	.75	0	0	0	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P26	.5	0	.5	.75	.75	0	0	0	0	.75	.75	0	.25	0	0	.25	0	.33	0	0	.33	.5	0	.5
P27	0	0	0	0	0	0	.75	.75	.25	.75	.75	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
P28	0	0	0	.75	.75	0	1	.75	.25	.75	.75	0	0	0	0	0	0	.33	0	0	.33	.5	0	.5
P29	1	.5	.5	0	0	0	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P30	1	.5	.5	.75	.75	0	0	0	0	0	0	0	.25	0	0	.25	0	.33	0	0	.33	.5	0	.5
P31	0	0	0	0	0	0	1	.75	.25	0	0	0	.75	.25	.25	.25	0	1	.33	.33	.33	.5	0	.5
P32	0	0	0	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P33	0	0	0	1	.75	.25	1	.75	.25	0	0	0	.75	.25	.25	.25	0	1	.33	.33	.33	.5	0	.5
P34	0	0	0	.75	.75	0	.75	.75	0	0	0	0	1	.25	.25	.25	.25	0	0	0	0	.5	0	.5
P35	0	0	0	.75	.75	0	0	0	0	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P36	0	0	0	0	0	0	0	0	0	.75	.75	0	.25	0	0	.25	0	0	0	0	0	0	0	0
P37	0	0	0	.75	.75	0	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P38	0	0	0	0	0	0	.75	.75	0	.75	.75	0	1	.25	.25	.25	.25	.33	.33	0	0	.5	0	.5
P39	.5	.5	0	0	0	0	0	0	0	1	.75	.25	.75	.25	.25	.25	0	1	.33	.33	.33	.5	0	.5
P40	.5	.5	0	.75	.75	0	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P41	0	0	0	.75	.75	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	.5	0	.5
P42	0	0	0	0	0	0	1	.75	.25	0	0	0	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
P43	0	0	0	1	.75	.25	0	0	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P44	1	.5	.5	.75	.75	0	1	.75	.25	.75	.75	.25	1	.25	.25	.25	.25	.33	.33	0	0	1	.5	.5
P45	0	0	0	0	0	0	1	.75	.25	0	0	0	.5	.25	.25	0	0	.66	.33	.33	0	.5	0	.5
P46	0	0	0	1	.75	.25	.75	.75	0	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P47	.5	.5	0	.75	.75	0	1	.75	.25	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P48	0	0	0	0	0	0	0	0	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P49	1	.5	.5	0	0	0	0	0	0	0	0	0	.75	.25	.25	.25	0	1	.33	.33	.33	0	0	0
P50	0	0	0	.25	0	.25	.75	.75	0	0	0	0	.5	0	.25	.25	0	0	0	0	0	0	0	0
P51	.5	.5	0	.75	.75	.25	.75	.75	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P52	0	0	0	0	0	0	0	0	0	1	.75	.25	0	0	0	0	0	0	0	0	0	.5	0	.5
P53	.5	.5	0	.75	.75	0	.75	.75	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P54	0	0	0	0	0	0	0	0	0	.75	.75	0	.25	0	0	.25	0	0	0	0	0	0	0	0
P55	0	0	0	0	0	0	1	.75	.25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Prilog 5.7. Rezultati istraživanja privatnih zdravstvenih ustanova (P56-P96) od zahtjeva T13 do T5

Oznaka	T13	T13a	T13b	T15	T15a	T15b	T22	T22a	T22b	T6	T6a	T6b	T26	T26a	T26b	T26c	T26d	T7	T7a	T7b	T7c	T5	T5a	T5b
P56	0	0	0	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P57	.5	.5	0	1	.75	.25	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	0	0	0	0	1	.5	.5
P58	0	0	0	1	.75	.25	1	.75	.25	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P59	0	0	0	0	0	0	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P60	0	0	0	0	0	0	.75	.75	0	1	.75	.25	0	0	0	0	0	0	0	0	0	1	.5	.5
P61	.5	.5	0	0	0	0	1	.75	.25	.75	.75	.25	1	.25	.25	.25	.25	0	0	0	0	.5	.5	0
P62	0	0	0	1	.75	.25	1	.75	.25	0	0	0	.25	.25	0	0	0	1	.33	.33	.33	.5	0	.5
P63	0	0	0	0	0	0	0	0	0	0	0	0	.25	.25	0	0	0	.33	.33	0	0	0	0	0
P64	0	0	0	1	.75	.25	1	.75	.25	.75	.75	0	1	.25	.25	.25	.25	0	0	0	0	.5	0	.5
P65	0	0	0	0	0	0	0	0	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P66	0	0	0	1	.75	.25	.75	.75	0	0	0	0	.75	.25	.25	.25	0	0	0	0	0	0	0	0
P67	0	0	0	0	0	0	1	.75	.25	1	.75	.25	.25	.25	0	0	0	.33	.33	0	0	0	0	0
P68	0	0	0	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P69	0	0	0	.75	.75	0	.25	0	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P70	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
P71	0	0	0	1	.75	.25	.75	.75	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P72	0	0	0	.75	.75	0	0	0	0	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P73	0	0	0	1	.75	.25	1	.75	.25	0	0	0	.75	.25	.25	0	.25	0	0	0	0	.5	.5	0
P74	0	0	0	0	0	0	0	0	0	.75	.75	0	0	0	0	0	0	0	0	0	0	0	0	0
P75	0	0	0	1	.75	.25	.75	.75	0	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P76	0	0	0	0	0	0	0	0	0	0	0	0	.25	0	0	.25	0	.33	0	0	.33	.5	0	.5
P77	0	0	0	1	.75	.25	1	.75	.25	.75	.75	0	.75	.25	0	.25	.25	.33	0	0	.33	.5	.5	0
P78	.5	.5	0	0	0	0	1	.75	.25	1	.75	.25	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P79	.5	.5	0	0	0	0	1	.75	.25	0	0	0	.75	.25	.25	.25	0	0	0	0	0	.5	0	.5
P80	.5	.5	0	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P81	0	0	0	.25	0	.25	.75	.75	0	1	.75	.25	.25	.25	0	0	0	0	0	0	0	0	0	0
P82	.5	.5	0	0	0	0	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P83	0	0	0	.75	.75	0	1	.75	.25	0	0	0	.75	.25	.25	.25	0	0	0	0	0	1	.5	.5
P84	.5	.5	0	1	.75	.25	0	0	0	0	0	0	.5	.25	0	.25	0	0	0	0	0	0	0	0
P85	0	0	0	0	0	0	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P86	.5	.5	0	1	.75	.25	1	.75	.25	0	0	0	.5	.25	0	.25	0	1	.33	.33	.33	0	0	0
P87	0	0	0	0	0	0	0	0	0	0	0	0	1	.25	.25	.25	.25	0	0	0	0	0	0	0
P88	0	0	0	0	0	0	1	.75	.25	0	0	0	.75	.25	.25	.25	0	1	.33	.33	.33	0	0	0
P89	0	0	0	0	0	0	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	.5	0	.5
P90	.5	.5	0	.75	.75	0	1	.75	.25	0	0	0	.5	.25	0	.25	0	0	0	0	0	0	0	0
P91	.5	.5	0	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	0	0	0
P92	.5	.5	0	1	.75	.25	1	.75	.25	.75	.75	0	.25	.25	0	0	0	1	.33	.33	.33	1	.5	.5
P93	.5	.5	0	.75	.75	0	.75	.75	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P94	.5	.5	0	.75	.75	0	.75	.75	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P95	.5	.5	0	.75	.75	0	.75	.75	0	.75	.75	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5
P96	1	.5	.5	1	.75	.25	1	.75	.25	0	0	0	1	.25	.25	.25	.25	1	.33	.33	.33	1	.5	.5

Prilog 5.8. Rezultati istraživanja privatnih zdravstvenih ustanova (P1-P57) od zahtjeva T2 do LG

Oznaka	T2	T18	T18a	T18b	AŽ	AŽ1	AŽ2	SL	SL1	SL2	LG
P1	1	0	0	0	0	0	0	.5	.5	.5	.5
P2	1	0	0	0	0	0	0	.5	.5	0	.5
P3	1	1	.5	.5	.25	0	.25	.5	.5	0	.5
P4	1	0	0	0	.25	0	.25	1	.5	.5	1
P5	1	0	0	0	0	0	0	1	.5	.5	.5
P6	1	0	0	0	.25	0	.25	1	.5	.5	1
P7	1	0	0	0	.25	0	.25	1	.5	.5	1
P8	1	0	0	0	0	0	0	.5	.5	0	.5
P9	1	0	0	0	0	0	0	0	0	0	1
P10	1	0	0	0	.25	0	.25	.5	.5	0	0
P11	1	0	0	0	0	0	0	1	.5	.5	.5
P12	1	0	0	0	0	0	0	1	.5	.5	.5
P13	1	0	0	0	.25	0	.25	1	.5	.5	1
P14	1	0	0	0	0	0	0	1	.5	.5	.5
P15	1	0	0	0	0	0	0	0	0	0	0
P16	.666	0	0	0	.25	0	.25	0	0	0	0
P17	1	0	0	0	1	.75	.25	1	.5	.5	1
P18	1	0	0	0	0	0	0	.5	.5	0	.5
P19	1	0	0	0	0	0	0	.5	.5	0	.5
P20	1	0	0	0	0	0	0	.5	.5	0	0
P21	1	0	0	0	0	0	0	.5	.5	0	0
P22	1	0	0	0	0	0	0	.5	.5	0	.5
P23	1	0	0	0	0	0	0	0	0	0	0
P24	1	0	0	0	.25	0	.25	1	.5	.5	.5
P25	1	0	0	0	0	0	0	1	.5	.5	1
P26	0	0	0	0	.25	0	.25	.5	.5	0	1
P27	1	0	0	0	1	.75	.25	1	.5	.5	1
P28	1	0	0	0	0	0	0	1	.5	.5	1
P29	1	0	0	0	1	.75	.25	1	.5	.5	1
P30	1	0	0	0	0	0	0	1	.5	.5	.5
P31	1	0	0	0	1	.75	.25	1	.5	.5	.5
P32	1	0	0	0	0	0	0	1	.5	.5	.5
P33	1	0	0	0	0	0	0	1	.5	.5	0
P34	1	0	0	0	0	0	0	0	0	0	.5
P35	1	0	0	0	0	0	0	1	.5	.5	.5
P36	1	0	0	0	0	0	0	.5	.5	0	.5
P37	1	0	0	0	.25	0	.25	.5	.5	0	1
P38	1	0	0	0	.25	0	.25	1	.5	.5	.5
P39	1	0	0	0	1	.75	.25	1	.5	.5	1
P40	1	0	0	0	.25	0	.25	.5	.5	0	1
P41	0	0	0	0	0	0	0	0	0	0	.5
P42	1	0	0	0	1	.75	.25	.5	.5	0	.5
P43	1	0	0	0	.25	0	.25	1	.5	.5	.5
P44	.666	.5	.5	0	0	0	0	1	.5	.5	.5
P45	1	0	0	0	.25	0	.25	.5	.5	0	.5
P46	1	0	0	0	.25	0	.25	1	.5	.5	1
P47	1	0	0	0	1	.75	.25	.5	.5	0	0
P48	1	0	0	0	0	0	0	.5	0	.5	.5
P49	1	0	0	0	0	0	0	1	.5	.5	0
P50	1	0	0	0	.25	0	.25	.5	.5	0	.5
P51	1	0	0	0	1	.75	.25	1	.5	.5	.5
P52	1	0	0	0	0	0	0	.5	.5	0	.5
P53	1	0	0	0	1	.75	.25	1	.5	.5	.5
P54	1	0	0	0	0	0	0	.5	.5	0	.5
P55	1	0	0	0	.25	0	.25	.5	.5	0	.5
P56	1	0	0	0	1	.75	.25	1	.5	.5	1
P57	1	0	0	0	1	.75	.25	1	.5	.5	1

Prilog 5.9. Rezultati istraživanja privatnih zdravstvenih ustanova (P58-P57) od zahtjeva T2 do LG

Oznaka	T2	T18	T18a	T18b	AŽ	AŽ1	AŽ2	SL	SL1	SL2	LG
P58	1	0	0	0	.25	0	.25	.5	.5	0	.5
P59	1	0	0	0	1	.75	.25	1	.5	.5	.5
P60	1	0	0	0	0	0	0	0	0	0	.5
P61	1	0	0	0	0	0	0	0	0	0	.5
P62	1	0	0	0	0	0	0	0	0	0	.5
P63	1	0	0	0	0	0	0	0	0	0	0
P64	1	0	0	0	0	0	0	.5	.5	0	1
P65	1	0	0	0	0	0	0	1	.5	.5	.5
P66	1	0	0	0	0	0	0	.5	.5	0	0
P67	1	0	0	0	0	0	0	1	.5	.5	1
P68	.666	0	0	0	1	.75	.25	1	.5	.5	1
P69	1	0	0	0	1	.75	.25	1	.5	.5	.5
P70	1	0	0	0	0	0	0	1	.5	.5	0
P71	1	0	0	0	0	0	0	1	.5	.5	1
P72	1	0	0	0	1	.75	.25	1	.5	.5	1
P73	1	0	0	0	0	0	0	.5	.5	0	.5
P74	1	0	0	0	0	0	0	1	.5	.5	.5
P75	1	0	0	0	.25	0	.25	.5	.5	0	1
P76	1	0	0	0	0	0	0	0	0	0	0
P77	1	0	0	0	0	0	0	.5	.5	0	.5
P78	1	0	0	0	.25	0	.25	.5	.5	0	1
P79	1	0	0	0	0	0	0	.5	.5	0	.5
P80	1	0	0	0	.75	.75	0	.5	.5	0	.5
P81	1	0	0	0	1	.75	.25	.5	.5	0	.5
P82	1	0	0	0	0	0	0	1	.5	.5	1
P83	1	0	0		.25	0	.25	1	.5	.5	.5
P84	1	1	.5	.5	.75	.75	0	1	.5	.5	1
P85	1	0	0	0	1	.75	.25	1	.5	.5	.5
P86	1	0	0	0	0	0	0	.5	.5	0	.5
P87	1	0	0	0	0	0	0	.5	.5	0	0
P88	1	0	0	0	0	0	0	.5	0	.5	0
P89	1	0	0	0	1	.75	.25	1	.5	.5	.5
P90	1	0	0	0	0	0	0	1	.5	.5	.5
P91	1	0	0	0	0	0	0	.5	.5	0	.5
P92	1	0	0	0	0	0	0	.5	.5	0	.5
P93	1	0	0	0	1	.75	.25	1	.5	.5	.5
P94	1	0	0	0	1	.75	.25	1	.5	.5	.5
P95	1	0	0	0	1	.75	.25	1	.5	.5	50
P96	1	0	0	0	1	.75	.25	1	.5	.5	1

Životopis autorice

Marta Alić rođena je 14. srpnja 1980. godine u Zagrebu, gdje završava osnovnu i srednju školu, nakon koje upisuje Veleučilište VERN' na kojem 2000. godine stječe zvanje referenta na području ekonomije poduzetništva. Iste godine upisuje dvopredmetni studij kroatistike i informatologije na Filozofskom fakultetu Sveučilišta u Zagrebu koji završava 2007. godine izradom diplomskog rada na području digitalizacije grčko-hrvatskog rječnika u okviru projekta *Hrvatska rječnička baština i hrvatski europski identitet*; znanstvenog projekta prihvaćenog od strane Ministarstva znanosti i obrazovanja te pod vodstvom mentora prof.dr.sc. Damira Borasa. Završetkom fakulteta stječe zvanje profesorice hrvatskog jezika i književnosti te informatologije (smjer: opća informatologija). 2003. godine, paralelno s navedenim studijem, upisuje dvogodišnji studij novinarstva na Fakultetu političkih znanosti Sveučilišta u Zagrebu koji završava 2009. godine diplomskim radom „Budućnost i perspektiva informacijskih i komunikacijskih znanosti“, čime stječe zvanje diplomiranog novinara.

Za vrijeme studija radila je u NCL media grupi d.o.o., a po završetku Filozofskog fakulteta zapošljava se u tvrtki InOptimum d.o.o. kao asistent u marketingu te za šest mjeseci prelazi u tvrtku Ćuk d.o.o. gdje radi kao voditeljica marketinga. Godine 2012. zapošljava se na Tehničkom veleučilištu Zagreb, gdje i danas radi, prvo kao stručni savjetnik za marketing i prodaju, a od 2013. kao asistent. Godine 2017. izabrana je u nastavno zvanje predavača.

Tijekom rada na Veleučilištu izvodi nastavu iz predmeta Tablični kalkulatori, Napredna UNIX rješenja, Skriptni jezici, Primjena računala te s izborom u nastavno zvanje predavača postupno preuzima nositeljstvo nad kolegijima Napredno elektroničko poslovanje u ekonomiji i Napredno elektroničko poslovanje u informatici, Sustavi elektroničkog poslovanja, Poslovna inteligencija, ERP i CRM poslovno informacijski sustavi, Taktički i operativni informacijski sustavi, Poslovna inteligencija i Gospodarsko-industrijska transformacija.

Popis objavljenih djela

1. Luić, Ljerka; Alić, Marta

THE IMPORTANCE OF DEVELOPING STUDENTS' DIGITAL SKILLS FOR THE DIGITAL TRANSFORMATION OF THE CURRICULUM *// 16th annual International Technology, Education and Development Conference* (2022)

2. Barić, Mateja; Alić, Marta

Digital Transformation in Croatia: Contextual analysis *// Proceedings of the Central European Conference on Information and Intelligent Systems*, Varaždin, 2021. str. 57-64

3. Barić, Mateja Alić, Marta

Circular Economy in Croatian Society *// MIPRO Proceedings 2021* / Skala, Karolj (ur.), Opatija: Croatian Society for Information, Communication and Electronic Technology – MIPRO, 2021. str. 1542-1547

4. Dolčić, Ozana; Alić, Marta

Generation Z Buyer's Journey *// Proceedings of Sciencefora international conference Dubrovnik, Croatia*, Dubrovnik: Institute for Technology and Research (ITRESEARCH), 2020. str. 60-64

5. Alić, Marta

Privacy Policy Understandability Analysis of Croatian Electronic Publications *// Mipro 2020 proceedings* / Skala, Karolj (ur.), Rijeka: Croatian Society for Information, Communication andElectronic Technology–MIPRO, 2020. str. 1784-1788

6. Alić, Marta; Antolović, Vanda

Percepcija društveno odgovornog poslovanja kod generacije Z *// MIPRO 2019 proceedings*, Opatija, Hrvatska, 2019. str. 1565-1570

7. Alić, Marta; Krakar, Ivan

Modeliranje procesa usklađivanja s GDPR uredbom *// Zbornik 6. međunarodne konferencije "Vallis Aurea"* / Katalinić, Branko (ur.), Požega: Veleučilište Požega, 2018.

8. Uzelac, Nataša Alić, Marta

Empathy – Is It Measurable and Teachable? *// CIET 2018 Conference Proceedings*, Split, Hrvatska, 2018. str. 724-735

9. Alić, Marta

Emotivna košarica kupnje 2026. *// Suvremena trgovina*, 42 (2017), str. 16-19

10. Alić, Marta; Žagar, Marinko

Social CRM as a platform for digital transformation *// CIET 2016 Conference Proceedings* / Plazibat, Bože ; Kosanović, Silvana (ur.), Split: University of Split, University Department of ProfessionalStudies, 2016.

11. Žagar, Marinko; Alić, Marta

Socijalni CRM u središtu inovativnog procesa *// Tiskarstvo & Dizajn 2016* / Vujić Žiljak, Jana (ur.). Zagreb: Akademija Tehničkih Znanosti Hrvatske - Centar za grafičko inženjerstvo, 2016. str. 44-44

12. Alić, Marta

Bitrix24 – integrated business-information system for sales process support *// The Future of Information Sciences (INFuture),* Zagreb, Hrvatska, 2015.

13. Bračun, Sanja; Alić, Marta

Zadovoljstvo studenata Tehničkog veleučilišta u Zagrebu korištenjem Moodle platforme za e-učenje *// Međunarodni znanstveni skuo Tiskarstvo & Dizajn 2015 : Zbornik radova* / Žiljak, Vujić, Jana (ur.), Zagreb: Fotosoft, 2015. str. 224-238

14. Alić, Marta; Bajić, Milan; Mauher, Mladen

Upotreba video sadržaja kao sredstva za učenje – studija slučaja na predmetu Sustavi elektoničkog poslovanja na Tehničkom veleučilištu u Zagrebu *// Tiskarstvo&Dizajn2014 ; Knjiga sažataka* / Žiljak, Vučić, Jana (ur.). Zagreb: FS, Fotosoft, 2014. str. 111-111