Pravni aspekti regulacije interneta stvari na tržištu elektroničkih komunikacija Republike Hrvatske

Grgec, Željka

SVEUČILIŠTE U ZAGREBU
CENTAR ZA POSLIJEDIPLOMSKE STUDIJE

SVEUČILIŠNI INTERDISCIPLINARNI SPECIJALISTIČKI STUDIJ
REGULIRANJE TRŽIŠTA ELEKTRONIČKIH KOMUNIKACIJA

Željka Grgec, dipl.iur.

PRAVNI ASPEKTI REGULACIJE INTERNETA STVARI NA TRŽIŠTU ELEKTRONIČKIH KOMUNIKACIJA REPUBLIKE HRVATSKE

SPECIJALISTIČKI RAD

Zagreb, 2023.

UNIVERSITY OF ZAGREB
CENTER FOR POSTGRADUATE STUDIES

UNIVERSITY INTERDISCIPLINARY SPECIALIST STUDY
REGULATION OF THE ELECTRONIC COMMUNICATIONS MARKET

Željka Grgec, dipl.iur.

LEGAL ASPECTS OF THE REGULATION OF INTERNET OF THINGS IN THE ELECTRONIC COMMUNICATIONS MARKET OF REPUBLIC OF CROATIA

SPECIALIST THESIS

Zagreb, 2023

Specijalistički rad izrađen je na Sveučilištu u Zagrebu Fakultetu elektrotehnike i računarstva u sklopu sveučilišnog interdisciplinarnog specijalističkog studija Reguliranje tržišta elektroničkih komunikacija.

Mentor: prof. dr. sc. Siniša Petrović, Sveučilište u Zagrebu Pravni fakultet

Specijalistički rad ima: 145 stranica

Specijalistički rad br.:

Povjerenstvo za ocjenu u sastavu:

1. prof. dr. sc. Gordan Ježić, Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva – predsjednik
2. prof. dr. sc. Siniša Petrović, Sveučilište u Zagrebu Pravni fakultet – mentor
3. izv. prof. dr. sc. Marko Jurić, Sveučilište u Zagrebu Pravni fakultet - član

Povjerenstvo za obranu u sastavu:

1. prof. dr. sc. Gordan Ježić, Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva – predsjednik
2. prof. dr. sc. Siniša Petrović, Sveučilište u Zagrebu Pravni fakultet – mentor
3. izv. prof. dr. sc. Marko Jurić, Sveučilište u Zagrebu Pravni fakultet - član

Datum obrane: 27. studenog 2023.

POPIS KRATICA

AI = Artificial intelligence/umjetna inteligencija

AR = Augmented reality/proširena stvarnost

ARPU = Average revenue per user/ Prosječni prihod po korisniku

BEREC = Body of European Regulators for Electronic Communications / Tijelo europskih regulatora za eletroničke komunikacije

CLOUD COMPUTING=-Računarstvo u oblaku

C-ITS = Cooperative Intelligent Transport Systems / Kooperativni inteligentni prometni sustav

CV = Računalni vid

DHcP = Dynamic Host Configuration Protocol / Dimički protokol glavnog računala

DNS = Domain Name System/ Sustav naziva domene

DMA = Digital Markets Act /Zakon o digitalnom tržištu

DPIA=Data Protection Impact Assesement /Procjena učinka na zaštitu podataka

DSA = Digital Services Act / Zakon o digitalnim uslugama

Embb = Enhanced Mobile Broadband /Poboljšana brzina prijenosa podataka

EMF = Electric and magnetic fields/ Električna i magnetska polja

ENISA = Europska agencija za mrežnu i informacijsku sigurnost

EU = Europska unija

HAKOM = Hrvatska regulatorna agencija za mrežne djelatnosti

IIoT = Industrijski IoT

IoT = Internet of things/ Internet stvari

MIMO = Multiple Input Multiple Output –/višestruki ulaz, višestruki izlaz

ML = Machine learning/strojno učenje

IP Protocol = Internetski protokol

OTT = Over the top / „ dodana vrijednost“- sinonim za uslugu izravne isporuke multimedijskog sadržaja krajnjim korisnicima putem interneta, preko mrežnih usluga njihovog davatelja usluga

RAN = Radio access network/ Radijska pristupna mreža

RFID = Radio-frequency identification /Identifikacija radio frekvencijom

RSPG = Radio spectrum policy group/ Skupina za politiku radiofrekvencijskog spektra

URLLC = Ultra-Reliable Low Latency Communications/ Ultra pouzdana i niskolatentna komunikacija

VR = Virtual reality /Virtualna stvarnost

ZEK = Zakon o elektroničkim komunikacijama

SAŽETAK

Ovaj rad sadrži sveobuhvatan pregled i analizu interneta stvari (IoT), uključujući njegove osnovne koncepte, tehnološke osnove, i povezanost s paradigmom 5G mreže. Dokument detaljno istražuje različite aspekte 5G mreže, uključujući njenu tehnologiju, strategiju implementacije na razini Europske Unije (EU) i Republike Hrvatske, kao i njen utjecaj na globalnu i europsku ekonomiju. Također se razmatra uloga 5G mreže u kontekstu interneta stvari kao i primjena umjetne inteligencije u ovom području.

Drugi dio rada bavi se pravnim aspektima regulacije interneta stvari pružajući detaljan pregled međunarodnog pravnog okvira i pristupa EU-a prema internetu stvari i umjetnoj inteligenciji. To uključuje odnos EU-a prema umjetnoj inteligenciji i pravno-regulatorni okvir interneta stvari unutar EU-a. Također se razmatraju mogući smjerovi regulacije i preporučeni omjer regulacije interneta stvari.

Treći dio rada posvećen je analizi tržišta elektroničkih komunikacija u kontekstu novog zakonodavstva i kibernetičke sigurnosti u Republici Hrvatskoj. To uključuje prikaz tržišta elektroničkih komunikacija, ulogu interneta stvari na tom tržištu, i novi pravno-regulatorni okvir elektroničkih komunikacija. Također se razmatra nacionalni pravno-regulatorni okvir u Republici Hrvatskoj, uključujući analizu ključnih usluga davatelja digitalnih usluga, sukladno Zakonu o elektroničkim komunikacijama i Zakonu o kibernetičkoj sigurnosti.

Konačno, rad pruža sveobuhvatan pregled kibernetičke sigurnosti u elektroničkim komunikacijama, najčešćih vrsta kibernetičkih napada, osviještenosti o rizicima kibernetičkih napada, i mjera zaštite od kibernetičkih napada. Također se istražuje zaštita privatnosti i podataka u kontekstu interneta stvari, kao i regulatorna obilježja usluga pametnih gradova.

Ključne riječi: Internet stvari (IoT); 5G mreža; Umjetna inteligencija (AI); Pravni aspekti; Tržište elektroničkih komunikacija; Najčešće vrste kibernetičkih napada; Zaštita privatnosti i podataka; Uredba (EU 2016/679); NIS 1 i NIS 2 Direktiva; HAKOM

SUMMARY

Keywords: Internet of Things (IoT); 5G network; Artificial Intelligence; Legal aspects; Electronic communications market; The most common types of cyberattacks; Protection of privacy and data; Regulation (EU 2016/679); NIS 1 and NIS 2 Directive; HAKOM

This paper contains a comprehensive overview and analysis of the Internet of Things (IoT), including its basic concepts, technological foundations, and connection to the 5G network paradigm. The document explores in detail various aspects of the 5G network, including its technology, implementation strategy at the level of the European Union (EU) and the Republic of Croatia, as well as its impact on the global and European economy. The role of the 5G network in the context of the Internet of Things is also considered, as well as the application of artificial intelligence in this area.

The second part of the paper deals with the legal aspects of IoT regulation, providing a detailed overview of the international legal framework and the EU's approach to the Internet of Things and artificial intelligence. This includes the EU's attitude towards artificial intelligence and the legal-regulatory framework of the Internet of Things within the EU. Possible directions of regulation and the recommended regulation ratio of the Internet of Things are also considered.

The third part of the paper is devoted to the analysis of the electronic communications market in the context of new legislation and cyber security in the Republic of Croatia. This includes an overview of the electronic communications market, the role of IoT in that market, and the new legal-regulatory framework of electronic communications. The national legal-regulatory framework in the Republic of Croatia is also considered, including an analysis of the Act on Cybersecurity and the Act on Electronic Communications.

Finally, the paper provides a comprehensive overview of cyber security in electronic communications, the most common types of cyber attacks, awareness of the risks of cyber attacks, and measures to protect against cyber attacks. It also explores privacy and data protection in the context of IoT, as well as the regulatory features of smart city services.

SADRŽAJ

1. UVOD

U radu se istražuje pravni aspekt regulacije Interneta stvari (Internet of Things) na tržištu elektroničkih komunikacija Republike Hrvatske, s posebnim fokusom na zakonodavstvo koje regulira kibernetičku sigurnost i zaštitu podataka. Problem koji se prepoznaje je konstantno razvijanje tehnologije koja često nadmašuje postojeće zakonodavne okvire, čineći ih zastarjelima i neučinkovitima.

Predmet ovog rada odnosi se na istraživanje zakonodavstva i regulativa koje se odnose na internet stvari i umjetnu inteligenciju u Republici Hrvatskoj, te usporedba s praksom u Europskoj uniji.

Ciljevi ovog rada uključuju:

- Razumjeti trenutni pravno-regulatorni okvir interneta stvari i umjetne inteligencije u Republici Hrvatskoj i Europskoj uniji.
- Istražiti i analizirati moguće pravne izazove i prepreke u implementaciji tih regulativa.
- Predložiti potencijalne načine usklađivanja nacionalnog zakonodavstva s Aktom Europske unije o kibernetičkoj sigurnosti.

Istraživačka pitanja koja rukovode ovaj rad uključuju:

- Kako je trenutno reguliran internet stvari i umjetna inteligencija u Republici Hrvatskoj?
- Koje su glavne razlike između pristupa Republike Hrvatske i Europske unije u regulaciji interneta stvari i umjetne inteligencije?
- Kako se Hrvatska može bolje uskladiti s Aktom Europske unije o kibernetičkoj sigurnosti?

Metodologija ovog rada uključuje pregled i analizu relevantnih zakona, regulativa i politika, kao i pregled sekundarnih izvora kao što su istraživački radovi, članci i izvješća stručnjaka na temu interneta stvari, umjetne inteligencije i kibernetičke sigurnosti.

Poseban naglasak je bio na istraživanju kako tehnološki napredak utječe na trenutne zakonodavne okvire i njihovu primjenjivost. Nalazi analize sugeriraju da je unatoč naporima, uvijek postojao jaz između brzine tehnološkog razvoja i prilagodbe zakonodavstva. Ova dinamika stvara brojne izazove, uključujući i pitanja o kibernetičkoj sigurnosti i zaštiti privatnosti.

U svom radu, autorica proučava značajne literaturne izvore, koji su oblikovali razumijevanje tehnološkog pejzaža u posljednjem desetljeću. Bruce Schneier, u svojoj knjizi *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, objavljenoj 2016. godine, istražuje pitanja privatnosti i sigurnosnih izazova u eri interneta stvari. Schneier posebno naglašava kako bi regulatori trebali biti oprezniji i posvetiti više pažnje ovim sigurnosnim aspektima.

S druge strane, Adam Greenfield u *Radical Technologies: The Design of Everyday Life*, objavljenoj 2017. godine, preispituje kako tehnologije, uključujući umjetnu inteligenciju, mijenjaju svakodnevni život ljudi. Greenfield posebno ukazuje na etičke dileme koje se pojavljuju s napretkom tehnologije, naglašavajući pitanja privatnosti i načina na koji tehnologija može utjecati na društvene norme i vrijednosti.

U kontekstu pristupa internetu i njegove neutralnosti, autorica se oslanjala na uvide Barbare van Schewick iz knjige *Internet Architecture and Innovation* iz 2010. godine. Van Schewick argumentira o važnosti očuvanja neutralnosti mreže kako bi se osigurao slobodan i otvoren pristup internetu. Autorica se složila s ovim stajalištem i istaknula potrebu za sličnom filozofijom kad je u pitanju internet stvari. Nalazi analize ukazuju na nužnost konstantnog praćenja tehnoloških trendova i ažuriranja zakonodavstva u skladu s tim, pri čemu se ističe potreba za multidisciplinarnim pristupom, gdje će regulatori, tehnološki stručnjaci, etičari i drugi stručnjaci morati surađivati kako bi se izgradilo pravično i sigurno digitalno društvo.

Razumijevanje ovih izazova i njihovo adekvatno adresiranje od velike je važnosti za stvaranje sigurnog i pouzdanog okruženja za daljnji razvoj interneta stvari i umjetne inteligencije u Republici Hrvatskoj.

2. OSNOVNI KONCEPTI I TEHNOLOŠKE OSNOVE INTERNETA STVARI

Internet stvari (IoT) je termin koji se koristi za opisivanje mreže objekata koji su povezani internetom, omogućujući im da komuniciraju jedni s drugima i s korisnicima. Ovi pametni objekti mogu biti različiti: od kućanskih aparata do automobila, od medicinskih uređaja do cijelih gradova.

Arhitektura IoT-a može se konceptualno podijeliti na nekoliko slojeva: sloj uređaja, sloj mreže i sloj aplikacija. Sloj uređaja se sastoji od fizičkih uređaja i kontrolera, dok sloj mreže obuhvaća protokole i komunikacijske tehnologije koje omogućuju povezivanje uređaja. Naposljetku, sloj aplikacija obuhvaća softver i aplikacije koje korisnicima omogućuju interakciju s IoT uređajima.

U poglavlju su navedene i analizirane različite definicije IoT-a, pozivom na brojne stručnjake i istraživače u ovom području, naglašavajući kako se definicije mogu razlikovati ovisno o kontekstu i primjeni.

Kroz ovu analizu, ističe se složenost i raznolikost IoT-a, naglašavajući njegov potencijal, ali i izazove koji proizlaze iz njegovog daljnjeg razvoja i implementacije.

2.1. Definiranje Interneta stvari (IoT)

IoT predstavlja revolucionarnu prekretnicu u tehnološkom napretku, koja je omogućila komunikaciju između uređaja bez potrebe za ljudskim uplitanjem. Ova povezanost omogućuje uređajima da prikupljaju, analiziraju i razmjenjuju podatke, transformirajući način na koji ljudi doživljavaju i koriste tehnologiju u svakodnevnom životu. Gubbi i suradnici (2013) definiraju IoT kao mrežu fizičkih objekata koji su povezani sa senzorima i mogućnošću komunikacije s drugim uređajima preko interneta. Ova definicija naglašava kako se kod IoT-a ne radi samo o mrežnoj povezanosti, već i o inteligenciji uređaja koji koriste podatke kako bi donijeli informirane odluke.

Whitmore, Agarwal i Da Xu (2015) objašnjavaju da IoT omogućuje pametne uređaje, koji su sposobni prepoznati i reagirati na svoje okruženje. Ovaj aspekt je presudan za razumijevanje kako IoT mijenja način interakcije ljudi s tehnologijom ne samo kao pasivnih korisnika, već i kao aktivnih sudionika u mreži uređaja koji komuniciraju i reagiraju na njihove potrebe. Ko, Lu, Thing, Westphal i Scanzio (2012) dodatno naglašavaju kako IoT predstavlja tehnološku paradigmu koja omogućava novi način interakcije i razmjene informacija. Napretkom IoT-a, uređaji nisu samo povezani, već su i inteligentni, omogućavajući novi nivo personalizacije i prilagodljivosti. No, kako Evans (2011) upozorava, s razvojem IoT-a dolaze i brojni izazovi, posebno u područjima privatnosti i sigurnosti. Kako bi se iskoristile prednosti IoT-a, potrebno je pažljivo razmotriti ova pitanja i razviti odgovarajuće strategije za njihovo rješavanje.

Uzimajući u obzir sve prethodno navedeno, jasno je da IoT predstavlja novi pravac u razvoju tehnologije, koji je već počeo transformirati svakodnevni život i rad. Kako se ova tehnologija nastavlja razvijati, potrebno je osigurati odgovarajući regulatorni okvir i zaštitu podataka kako bi se omogućilo njeno daljnje širenje i razvoj.

IoT, kako ga definiraju Miorandi i suradnici (2012), jest dinamička globalna mrežna infrastruktura s inteligentnim sposobnostima samokonfiguracije temeljena na standardnim i interoperabilnim komunikacijskim protokolima. Ključne značajke ove definicije su inteligencija i samokonfiguracija uređaja, koji mogu komunicirati međusobno bez ljudske intervencije.

Perera i suradnici (2017) ističu da je koncept samokonfiguracije od temeljne važnosti za IoT. Uređaji moraju biti sposobni automatski se konfigurirati kako bi radili u mreži s drugim uređajima. Ova samostalnost uređaja omogućava nesmetano funkcioniranje kompleksnih sustava, bez potrebe za stalnim ljudskim nadzorom.

Interoperabilnost, kao drugi bitan aspekt definicije Miorandi i suradnika, također je fundamentalna karakteristika IoT-a. U skladu s Atzori, Iera i Morabito (2010), interoperabilnost se odnosi na sposobnost različitih sustava i uređaja da surađuju i razmjenjuju informacije. U kontekstu IoT-a, to znači da uređaji različitih proizvođača i standarda mogu međusobno komunicirati, što je ključno za uspostavljanje globalne mreže uređaja.

No, kako Sundmaeker i suradnici (2010) upozoravaju, unatoč potencijalnim prednostima, IoT također donosi brojne izazove. Primjerice, pitanje sigurnosti i privatnosti podataka postaje sve

važnije kako se povećava broj uređaja koji komuniciraju i razmjenjuju informacije. Kako bi se iskoristile sve prednosti IoT-a, ovi izazovi moraju biti adekvatno riješeni.

Jasno je da koncept IoT donosi potpuno novu razinu povezanosti i interakcije između uređaja, omogućavajući razvoj kompleksnih sustava koji mogu autonomno funkcionirati i pružiti korisnicima jedinstveno iskustvo. Međutim, kako se ovaj koncept nastavlja razvijati, važno je uzeti u obzir i potencijalne izazove i razmotriti kako ih najbolje riješiti. IoT, prema Atzori, Iera i Morabito (2010), ne samo da omogućava razmjenu podataka između uređaja, već omogućuje i stvaranje novih usluga temeljenih na tim podacima. Ova mogućnost donosi revolucionarne promjene u mnogim sektorima, od industrije do kućanstva, omogućavajući automatizaciju procesa i otvarajući vrata za neviđene mogućnosti razvoja novih tehnologija.

Na primjer, Gubbi i suradnici (2013) navode da IoT može olakšati automatizaciju domaćinstva. Uređaji kao što su pametni termostati, hladnjaci i rasvjeta mogu komunicirati jedni s drugima i s korisnicima, pružajući inteligentniju, energetski učinkovitiju i udobniju kućnu okolinu. Prema Cisco Systems (2011), IoT također ima potencijal za duboko transformiranje industrijskog sektora. Na primjer, u industriji 4.0, kao što su predvidjeli Lee i Lee (2015), strojevi, senzori i proizvodni sustavi mogu komunicirati i surađivati jedni s drugima kako bi poboljšali proizvodnju i održavanje. Međutim, kako Whitmore, Agarwal i Da Xu (2015) upozoravaju, s velikim mogućnostima dolaze i veliki izazovi. Na primjer, problemi s sigurnošću, privatnošću i interoperabilnošću mogu ometati uspješnu implementaciju IoT-a. Dakle, da bi se potpuno iskoristile prednosti koje IoT pruža, važno je pravilno riješiti ove probleme.

Povijesno gledano, koncept IoT doista potječe iz ranih godina 21. stoljeća, specifično iz razvoja tehnologija kao što su RFID (Identifikacija radio frekvencijom) i bežična komunikacija. Autori Kevin Ashton (2009) često se pripisuje prvi put kovanje izraza Internet stvari 1999. godine tijekom svog rada u Procter & Gamble, ističući potencijal RFID-a u kontekstu povezivanja fizičkog svijeta s internetom. Međutim, kako navodi Sundmaeker i suradnici (2010), pravi procvat IoT-a započinje tek s pojavom naprednih bežičnih tehnologija, senzora i jeftinog računalnog hardvera. Razvoj ovih tehnologija omogućio je izgradnju mreže uređaja sposobnih za prikupljanje, obradu i razmjenu podataka na načine koji ranije nisu bili mogući.

IoT je od tada postao ključnim elementom digitalne transformacije, s dubokim utjecajem na različite industrije. Prema spoznajama Manyika i suradnika (2015) iz McKinsey Global

Institute, IoT ima potencijal stvoriti do 11,1 trilijuna dolara vrijednosti do 2025. godine kroz poboljšanja u operativnoj učinkovitosti, poboljšanu korisničku uslugu i nove poslovne modele.

No, s ovim brzim rastom dolaze i izazovi. Prema autorima Roman, Najera i Lopez (2011), problemi sigurnosti i privatnosti postaju sve ozbiljniji s porastom povezanih uređaja. To stvara potrebu za uspostavom odgovarajućih pravno-regulatornih okvira za rukovanje podacima i osiguranje sigurne i pouzdane komunikacije u IoT ekosustavu.

Koncept IoT temelji se na nekoliko osnovnih postavki. Prema Whitmore, Agarwal i Da Xu (2015), ovi temelji uključuju povezivanje uređaja s internetom, prikupljanje i razmjenu podataka, te analizu i obradu tih podataka radi optimizacije procesa. U ovom kontekstu, uređaji obuhvaćaju širok spektar fizičkih objekata i to od jednostavnih senzora i uređaja do složenijih strojeva i vozila. Ovi uređaji, često opremljeni sa senzorima, prikupljaju podatke iz svoje okoline i komuniciraju te podatke preko interneta, često koristeći bežične tehnologije za povezivanje.

Mrežne veze služe za prijenos podataka između uređaja i podatkovnih centara ili drugih uređaja. Ove veze mogu koristiti razne protokole i tehnologije, uključujući Wi-Fi, mobilne mreže, Bluetooth i druge. Podatkovni centri, često bazirani na cloud tehnologijama, koriste se za pohranu i obradu prikupljenih podataka. Ovi centri koriste sofisticirane algoritme i tehnike analize podataka kako bi izvukli vrijedne uvide iz prikupljenih podataka, omogućujući optimizaciju procesa i donošenje informiranih odluka. Korisnička sučelja, naposljetku, omogućuju korisnicima da interagiraju s IoT sustavima, pregledavaju prikupljene podatke, i koriste rezultate analiza za potrebe donošenja odluka ili upravljanja IoT uređajima.

Međutim, unatoč brojnim prednostima, IoT donosi i neke izazove. Prema spoznajama Webera (2010), jedan od bitnih izazova leži u pitanjima sigurnosti i zaštite privatnosti, posebno s obzirom na velike količine podataka koje IoT uređaji mogu prikupljati i razmjenjivati. Razvoj IoT-a donosi niz izazova koje treba prepoznati i adresirati. Prema studiji koju su sproveli Weber (2010) i Roman, Najera i Lopez (2011), izazovi uključuju pitanja vezana uz sigurnost, privatnost i interoperabilnost.

Sigurnost je jedan od glavnih izazova u IoT okruženju. Kako su uređaji sve više povezani, postaju i više izloženi mogućim sigurnosnim prijetnjama. Uređaji povezani s internetom mogu biti meta za hakerske napade, što može rezultirati krađom osjetljivih podataka ili oštećenjem

samih uređaja. Prema autorima Whitmore, Agarwal i Da Xu (2015), potrebno je uložiti dodatne napore u poboljšanje sigurnosnih mehanizama u IoT ekosustavu kako bi se smanjila ova rizika.

Pitanje privatnosti je također važno. IoT uređaji često prikupljaju velike količine podataka, uključujući i osobne podatke korisnika. Kako se ti podaci koriste i dijele između različitih strana može biti osjetljivo pitanje. Roman, Najera i Lopez (2011) naglašavaju potrebu za razvojem odgovarajućih mehanizama zaštite privatnosti koji mogu osigurati da su podaci korisnika zaštićeni.

Interoperabilnost se odnosi na sposobnost različitih uređaja da međusobno surađuju i komuniciraju. Kako IoT ekosustav raste, interoperabilnost postaje sve izazovnija. Atzori, Iera i Morabito (2010) ukazuju na potrebu za razvojem standarda koji bi omogućili uređajima različitih proizvođača da međusobno komuniciraju i surađuju.

Kako se tehnologija nastavlja razvijati, postaje sve važnije ažurirati pravno-regulatorni okvir kako bi se riješili ovi izazovi. Stalno prilagođavanje zakonodavstva i regulative potrebno je kako bi se omogućile daljnje inovacije u području IoT-a, ističu Marquezan et al. (2019). U ovom kontekstu, suradnja između tehnoloških stručnjaka, pravnika i regulatora je ključna za uspostavljanje okvira koji omogućava siguran, zaštićen i efikasan razvoj IoT tehnologija.

2.2. Arhitektura Interneta stvari

Arhitektura interneta stvari počiva na različitim komponentama koje omogućuju povezivanje uređaja i pristup podacima. Prema spoznajama Al-Fuqaha et al., (2015), arhitektura interneta stvari može se podijeliti na pet slojeva: uređaj, pristupno mrežno, mrežno, middleware i aplikacijski sloj.

Svijet je već prepun pametnih uređaja, od kućanskih aparata, nosivih tehnologija, do autonomnih vozila. Prema Gubbi et al., (2013), svi ti uređaji - stvari - mogu biti dijelom IoT-a0.

Senzori su osnovni elementi ovih uređaja koji omogućuju prikupljanje podataka iz okoline. To može uključivati podatke o temperaturi, vlažnosti, svjetlosti, zvuku, kretanju, pa čak i biometrijske podatke poput otkucaja srca ili razine glukoze u krvi. Kao što Atzori et al., (2010) navode, senzori su oči i uši interneta stvari.

Aktuatori, ili uređaji za aktivaciju, često djeluju u tandemu sa senzorima. Oni preuzimaju podatke i provode fizičke akcije u stvarnom svijetu. Na primjer, termostat može biti programiran da koristi podatke s temperaturnih senzora i automatski prilagodi grijanje ili hlađenje u sobi. Svaki takav uređaj mora biti opremljen nekim oblikom mrežne tehnologije kako bi komunicirao s ostalim dijelovima mreže.

Uređaji u IoT okruženju mogu biti povezani na različite načine. To uključuje kabelsku vezu, Wi-Fi, Bluetooth, LoRaWAN, ZigBee, Cellular IoT i druge metode bežične komunikacije. Prema Miorandi et al., (2012), izbor tehnologije komunikacije ovisi o specifičnim zahtjevima uređaja i primjeni, uključujući raspon, brzinu prijenosa podataka, potrošnju energije i sigurnost.

Na kraju, važno je razumjeti da su ovi uređaji, odnosno stvari vitalna komponenta IoT-a. Bez njih, ne bi bilo podataka za prikupljanje, analizu i djelovanje. Njihova sposobnost prikupljanja podataka i komuniciranja preko mreže čini temelj IoT-a, omogućujući stvaranje pametnijeg povezanijeg svijeta.

Pristupna mreža, ili kako je često zovu sloj povezivanja ili pristupna točka, omogućava prijenos podataka između uređaja i mreže. Ovaj sloj predstavlja bitnu komponentu arhitekture IoT-a, jer omogućava uređajima da se povežu i komuniciraju s mrežom.

Wi-Fi je jedan od najčešće korištenih načina povezivanja uređaja s mrežom. Prema nalazima spoznaja Bandyopadhyay i Sen (2011), Wi-Fi omogućava brz i pouzdan prijenos podataka na relativno velike udaljenosti, što ga čini idealnim za primjene koje zahtijevaju veliku količinu podataka, kao što su streaming videozapisa ili prijenos velikih datoteka.

Bluetooth je druga uobičajena tehnologija povezivanja uređaja s mrežom. U svom radu, Collotta et al., (2014) ističu da Bluetooth Low Energy (BLE) omogućava energetski učinkovit prijenos podataka na male udaljenosti, što ga čini prikladnim za primjene koje ne zahtijevaju visoku brzinu prijenosa podataka, poput povezivanja senzora ili kontrolnih uređaja.

NFC ili Near Field Communication, omogućuje prijenos podataka na vrlo malim udaljenostima, obično manje od 10 centimetara. Coskun et al., (2013) ističu da NFC omogućava brzo i jednostavno povezivanje uređaja, što ga čini idealnim za primjene poput beskontaktnih plaćanja ili brzog prijenosa podataka između uređaja. Osim ove tri tehnologije, postoje i mnoge druge koje se mogu koristiti za povezivanje uređaja s mrežom. Prema studiji Zanella et al., (2014), to može uključivati tehnologije poput Zigbee, Z-Wave, LoRaWAN, Sigfox, i druge koje su dizajnirane za specifične IoT primjene.

Svaka od ovih tehnologija ima svoje prednosti i nedostatke i odabir prave tehnologije za određenu primjenu može biti složen proces. Bez obzira na to, pristupna mreža igra ključnu ulogu u omogućavanju povezivanja uređaja s mrežom, što je temeljni aspekt IoT-a.

Mrežni sloj, u kontekstu arhitekture interneta stvari, igra ključnu ulogu u usmjeravanju podataka između uređaja i mreža. Prema definiciji Kortuem et al., (2010), ovaj sloj omogućava rutiranje informacija s uređaja na odredište, bilo da se to odredište nalazi unutar lokalne mreže ili na drugoj strani svijeta.

Da bi uspješno isporučio podatke, mrežni sloj koristi različite protokole. Na primjer, IP protokol (Internet Protocol) služi za usmjeravanje podataka na mreži. Patel et al., (2016) napominju da se IP koristi u velikom broju IoT uređaja zbog svoje opsežne podrške i univerzalne prirode.

Osim toga, mrežni sloj omogućava pristup nizu usluga koje olakšavaju komunikaciju na mreži. To uključuje DNS (Domain Name System), koji je, prema Al-Fuqaha et al., (2015), esencijalan za prevođenje imena domena u IP adrese. Ova usluga omogućava uređajima da se povežu s odredištem koristeći lako pamtljiva imena umjesto kompleksnih numeričkih IP adresa.

Još jedna važna usluga koju pruža mrežni sloj je DHCP (Dynamic Host Configuration Protocol). Prema Zhou et al., (2014), DHCP omogućuje dinamičko dodjeljivanje IP adresa uređajima, što olakšava upravljanje mrežom i smanjuje potrebu za ručnim konfiguriranjem uređaja.

Sve u svemu, mrežni sloj je središnji dio IoT arhitekture, koji omogućava pouzdanu i učinkovitu komunikaciju između uređaja i mreža. Bez ovog sloja, IoT uređaji ne bi mogli dijeliti podatke i komunicirati međusobno na globalnoj razini.

Middleware sloj, u kontekstu arhitekture IoT-a, koristi se za obradu i upravljanje podacima prije nego što se podaci dostave aplikaciji. Prema studiji Guinard et al., (2010), ovaj sloj može obuhvatiti različite usluge koje omogućuju, olakšavaju i poboljšavaju komunikaciju između uređaja i aplikacija. Posrednički poslužitelji, ili proxy servers, su najvažniji elementi middleware sloja. Prema Liu et al., (2014), proxy poslužitelji djeluju kao posrednici između klijenta (npr. IoT uređaja) i poslužitelja (npr. cloud servisa ili aplikacije), upravljajući zahtjevima, odgovorima i sigurnosnim aspektima komunikacije.

Baze podataka, koje često djeluju kao osnovne komponente middleware sloja, skupljaju, pohranjuju i upravljaju podacima koje generiraju IoT uređaji. Kako je istaknuo Bonomi et al.,

(2012), ove baze podataka omogućavaju efikasnu analizu i obradu podataka, olakšavajući izvlačenje vrijednih informacija iz velikih količina podataka koje IoT uređaji proizvode.

Servisi za obradu podataka predstavljaju još jednu vitalnu komponentu middleware sloja. Prema Chen et al., (2014), ti servisi mogu obuhvaćati širok raspon funkcionalnosti, uključujući, ali ne ograničavajući se na, prepoznavanje obrazaca, filtriranje podataka, kompresiju i enkripciju. Ovi servisi omogućavaju obradu podataka na način koji najbolje odgovara potrebama određene IoT aplikacije.

U konačnici, middleware sloj je najvažniji dio arhitekture IoT-a, povezujući donje slojeve (fizičke uređaje i mreže) s gornjim slojevima (aplikacijama i korisnicima). Bez ovog sloja, efikasna komunikacija i upravljanje podacima u IoT sustavima bili bi znatno otežani.

Aplikacijski sloj predstavlja krajnji sloj arhitekture IoT-a i služi kao sučelje za korisnike. Ovaj sloj obuhvaća razne aplikacije i usluge koje korisnici koriste za interakciju s uređajima i podacima generiranim u IoT ekosustavu. Prema Al-Fuqaha et al., (2015), aplikacijski sloj može uključivati različite aplikacije prilagođene specifičnim industrijskim sektorima, kao što su zdravstvena skrb, poljoprivreda, transport, pametne kuće i mnoge druge. Ove aplikacije omogućuju korisnicima pristup podacima prikupljenima od IoT uređaja i pružaju mogućnost kontroliranja tih uređaja.

Osim specifičnih aplikacija, aplikacijski sloj također može uključivati različite usluge koje omogućuju korisnicima da upravljaju i analiziraju podatke prikupljene od IoT uređaja. Prema studiji Zhou et al., (2014), to može uključivati usluge kao što su sustavi za upravljanje podacima, alati za vizualizaciju podataka i analitički alati. Dalje, aplikacijski sloj igra ključnu ulogu u sigurnosti IoT sustava. Kao što Makhdoom et al., (2018) navode, ovaj sloj mora implementirati različite mehanizme sigurnosti, uključujući autentifikaciju, autorizaciju i šifriranje, kako bi zaštitio podatke i uređaje od mogućih napada. Ukratko, aplikacijski sloj je onaj dio IoT arhitekture s kojim korisnici najčešće dolaze u kontakt. Bez ovog sloja, korisnici ne bi mogli interaktivno koristiti IoT uređaje ili pristupiti vrijednim podacima koji se generiraju u IoT ekosustavu.

Na osnovi navedenog evidentno proizlazi da je arhitektura Iot-a, složen sustav koji se sastoji od brojnih komponenti. Njegov cilj je omogućiti povezivanje uređaja i pristup podacima na način koji je praktičan za korisnike, dok istovremeno osigurava pouzdanost, sigurnost i učinkovitost.

2.3. Uvid u paradigmu 5G mreže

5G mreža predstavlja sljedeću (aktualnu) generaciju bežične tehnologije koja donosi značajna poboljšanja u odnosu na prethodne generacije. Pritom, glavne karakteristike koje 5G mreža donosi uključuju povećane brzine prijenosa podataka, smanjenu latenciju i povećan kapacitet mreže. Povećana brzina prijenosa podataka, koju 5G mreža donosi, od iznimne je važnosti za podršku rastućim zahtjevima za propusnošću u suvremenom digitalnom društvu. Prema studiji koju su proveli Andrews et al. (2016), ispunjena su očekivanja da će 5G mreže omogućiti brzine prijenosa do 20 Gbit/s, što je značajno brže od 4G mreža.

Smanjeno vremensko kašnjenje (latencija) još je jedan važan aspekt 5G mreža. Prema istraživanju koje su proveli Aijaz et al. (2018), ispunjena su očekivanja da će 5G mreže omogućiti latenciju manju od 1 milisekunde, što je važno za primjene koje zahtijevaju trenutni odziv, poput autonomnih vozila ili virtualne stvarnosti.

Povećani kapacitet mreže, što je istaknuto u studiji Boccardi et al. (2014), omogućava 5G mrežama da podrže veliki broj povezanih uređaja. To je od ključne važnosti u kontekstu Interneta stvari (IoT), gdje se očekuje da će milijuni, pa čak i milijarde uređaja biti povezane. Prema Ghosh et al. (2016), 5G mreže koriste napredne tehnike, kao što su masivno MIMO (Multiple Input Multiple Output) i zrakoplovne komunikacije, kako bi se ostvarile ove prednosti. Ove tehnologije omogućavaju 5G mrežama da podrže veći broj korisnika, omogućavaju brži prijenos podataka i smanjuju latenciju.

Na kraju, Chih-Lin et al. (2014) ističu kako 5G mreže pružaju poboljšane mehanizme zaštite, uključujući napredne tehnike enkripcije i autentifikacije, što je ključno za zaštitu podataka i privatnosti korisnika u svijetu gdje je sve više povezano.

2.3.1. Tehnologija 5G mreže

Tehnologija 5G mreža donosi brojne inovacije koje su značajno poboljšale način na koji se koristi bežične komunikacije. U osnovi ovih inovacija su napredne tehnološke komponente koje

5G mreža koristi. MasivnI MIMO, ili Multiple Input Multiple Output, je tehnologija koju 5G mreža koristi da bi poboljšala kapacitet mreže i omogućila veće brzine prijenosa podataka.

Prema spoznajama Boccardi et al. (2014), ova tehnologija uključuje korištenje velikog broja antena za prijenos i primanje signala. To se značajno razlikuje od tehnologija korištenih u prethodnim generacijama mreža, koje su obično koristile manji broj antena.

U studiji koju su proveli Björnson et al. (2016), analiziran je utjecaj tehnologije masivnog MIMO-a na performanse mreže. Istraživanje je pokazalo da ova tehnologija omogućuje značajno povećanje kapaciteta mreže. To je omogućeno sposobnošću tehnologije masivnog MIMO-a da istovremeno poslužuje više korisnika koristeći istu frekvenciju, što se naziva prostorno multiplexiranje.

Osim toga, Luo et al. (2017) su u svojoj studiji istaknuli kako masivni MIMO omogućava veće brzine prijenosa podataka. Masivni MIMO to postiže kroz korištenje preciznog usmjerenja signala, što rezultira smanjenjem smetnji između različitih korisnika i povećanjem ukupne efikasnosti mreže.

Konačno, prema spoznajama Larsson et al. (2014), tehnologija masivnog MIMO-a također donosi poboljšanja u energetskoj efikasnosti mreže. Budući da masivni MIMO omogućava preciznije usmjeravanje signala, manje energije se gubi u procesu prijenosa, što rezultira većom energetskom efikasnošću mreže.

Mrežni slicing, ili mrežno kriškiranje, je tehnologija koju koristi 5G mreža da bi pružila prilagodljiva i efikasna rješenja za različite potrebe korisnika. Ghosh et al. (2016) navode da ovu tehnologiju karakterizira sposobnost stvaranja virtualnih 'kriški' mreže koje su prilagođene specifičnim zahtjevima korisnika ili aplikacija. Na primjer, može se stvoriti kriška mreže koja je optimizirana za IoT uređaje, kojima su možda potrebne niske brzine prijenosa, ali visoka pouzdanost i niska latencija. S druge strane, može se stvoriti druga kriška koja je optimizirana za aplikacije koje zahtijevaju velike brzine prijenosa, poput striminga video sadržaja visoke rezolucije ili virtualne stvarnosti.

Kostopoulos et al. (2017) navode da mrežni slicing donosi brojne prednosti. Prvo, omogućuje bolje iskorištavanje resursa mreže, budući da se resursi mogu dinamički dodjeljivati i optimizirati za svaku kršku mreže. Drugo, omogućuje operaterima da pruže personalizirane usluge koje bolje zadovoljavaju potrebe korisnika. Treće, omogućava brže uvođenje novih

usluga, budući da se nove kriške mreže mogu lako dodati bez potrebe za prepravkom cijele mreže.

Ordonez-Lucena et al. (2017) ističu da mrežni slicing ima potencijal da promijeni način na koji se mreže dizajniraju i upravljaju, nudeći više fleksibilnosti i omogućujući bolje ispunjavanje zahtjeva različitih korisnika i aplikacija.

Milimetarski valovi, koji se često koriste u 5G mrežama, predstavljaju radiofrekvencijski spektar koji obuhvaća frekvencije od 30 do 300 GHz. Njihova upotreba u kontekstu 5G mreža, kako je istaknuto u radu Andrews et al. (2016), omogućava velike brzine prijenosa podataka, ali ima i neke očite izazove. S obzirom na to da milimetarski valovi imaju kraći domet i veću osjetljivost na fizičke prepreke u odnosu na niže frekvencije, zahtijevaju line-of-sight (LoS) ili direktnu vidljivost između antene i uređaja. To znači da zgrade, drveće ili čak atmosferske uvjeti poput kiše mogu blokirati ili značajno oslabiti signal.

Uprkos ovim izazovima, istraživanja, poput onog kojeg su proveli Rappaport et al. (2013), sugeriraju da se ti problemi mogu prevladati kroz korištenje tehnologija kao što su *beamforming* (usmjeravanje snopa) i masivni MIMO. Beamforming omogućava preciznije usmjeravanje radio signala prema korisnicima, dok masivni MIMO, koristeći veliki broj antena, može povećati kapacitet mreže i kompenzirati slabljenje signala koje uzrokuju prepreke.

Usprkos ovim tehničkim izazovima, milimetarski valovi imaju veliki potencijal u kontekstu 5G mreža. Kako je istaknuto u radu Han et al. (2015), upotreba milimetarskih valova može značajno povećati kapacitet mreže i omogućiti brže brzine prijenosa, što se zaista ukazuje bitnim u smislu podrške novim i zahtjevnim aplikacijama poput virtualne stvarnosti, ultra HD video sadržaja i autonomnih vozila.

Sigurnost je ključna komponenta u svijetu brzo rastućih digitalnih komunikacija, posebno s obzirom na brojne prijetnje koje su prisutne u suvremenom digitalnom okruženju. Kao što je istaknuto u radu Chih-Lin et al. (2014), 5G mreža pruža napredne mehanizme sigurnosti, koji uključuju poboljšane tehnike enkripcije i autentifikacije.

2.3.2. EU strategija za 5G mrežu

EU strategija za 5G mrežu ima za cilj stvoriti okruženje koje omogućava brzo, efikasno i široko korištenje 5G tehnologija. To uključuje poboljšanje kapaciteta mreže, odnosno broja uređaja koji mogu biti povezani na mrežu bez gubitka kvalitete usluge.

Prema radu Boccardi et al. (2014), 5G mreža je sposobna podržati povezivanje velikog broja uređaja, što je od važnosti za IoT, gdje je tisuće uređaja često povezano na mrežu istovremeno. To ne samo da omogućava veću razinu povezanosti, već omogućava i razvoj novih aplikacija koje zahtijevaju visoku propusnost mreže. Brzine prijenosa podataka u 5G mrežama značajno su veće u usporedbi s prethodnim generacijama mreža, što omogućava brzo i učinkovito prenošenje velikih količina podataka. To je ključno za mnoge suvremene aplikacije, uključujući video streaming visoke kvalitete, virtualnu i proširenu stvarnost, te automatizirana vozila.

Niža latencija, odnosno vrijeme potrebno za prenošenje podataka od izvora do odredišta druga je važna karakteristika 5G mreže koja se ističe u strategiji EU. Prema istraživanjima Ghosh et al. (2016), smanjenje latencije do razine od samo nekoliko milisekundi otvara vrata za nove primjene poput telemedicine, automatizirane industrije i autonomnih vozila, gdje je brza komunikacija od presudne važnosti.

EU strategija za 5G mrežu donosi brojne koristi, od kojih su neke povećanje kapaciteta mreže, bolja povezanost, veće brzine prijenosa podataka i niža latencija. Prema radu Boccardi et al. (2014), ove poboljšane performanse omogućit će novim aplikacijama, poput IoT-a, da dosegnu svoj puni potencijal.

Prema spoznajama autora Frattasi et al. (2016), EU strategija za 5G mrežu također ima važan ekonomski aspekt. Uvođenje 5G tehnologije donijelo je značajan ekonomski rast u EU, stvarajući nova radna mjesta i potičući inovacije u širokom spektru industrija.

Osim toga, EU strategija prepoznaje i važnost sigurnosti u 5G mrežama. Prema studiji koju su proveli Chih-Lin et al. (2014), ispunjen je plan da 5G mreže budu opremljene najnovijim tehnikama enkripcije i autentifikacije kako bi se zaštitili korisnički podaci i održalo povjerenje u digitalno društvo.

EU strategija za 5G mrežu materijalizirana je kroz Akcijski plan koji je Europska komisija objavila 14. rujna 2016. godine. Pod naslovom *5G za Europu*, plan je predstavio europski

raspored za komercijalno tržišno lansiranje 5G tehnologije do kraja 2020. godine. Cilj je bio da do 2025. godine 5G bude sveobuhvatno dostupan u svim mjestima i gradovima, kao i na svim ključnim prometnim pravcima.

EU strategija prepoznaje važnost koordiniranog pristupa kako bi se izbjegla neučinkovitost i stvorilo okruženje pogodno za ulaganja. U skladu s tim, Akcijski plan naglašava važnost međunarodno usklađenog postupka u pogledu istraživanja, planiranja i koordinacije. EU Akcijski plan za 5G obuhvaća različite aktivnosti, uključujući pružanje i usklađivanje frekvencija za 5G. To uključuje pronalaženje optimalne kombinacije fiksne mreže i bežične tehnologije kako bi se osigurala široka dostupnost 5G. Plan također promiče ulaganja u inovacije povezane s 5G, što bi trebalo potaknuti rast. Cilj je stvoriti povoljne političke okvirne uvjete koji će omogućiti društvu i gospodarstvu da imaju koristi od konkurentne EU.

Akcijski plan *5G za Europu* povezan je sa strategijom Europske komisije o jedinstvenom digitalnom tržištu i Europskim kodeksom elektroničkih komunikacija. Cilj ovih programa je učiniti jedinstveno digitalno tržište privlačnim i konkurentnim, a s njim i Europu kao središte tehnologije.

Kao dio svog javno-privatnog partnerstva za 5G (5G PPP), EU podupire 5G istraživačke projekte s više od 400 milijuna eura. 5G PPP pokrenut je 2013. godine za istraživanje i promicanje 5G tehnologija u Europi i od tada je poduzeo niz ključnih koraka za planiranje budućeg smjera.

Kada je riječ o kibersigurnosti, EU je prepoznala važnost zaštite 5G mreže. Države članice su, na preporuku Europske komisije, provele procjenu rizika sigurnosti 5G mreže i složile se podići zahtjeve kibernetičke sigurnosti. To je rezultiralo sveobuhvatnim izvješćem o procjeni rizika za EU, objavljenim krajem 2019. godine. Izvješće definira strateške i tehničke mjere za smanjenje rizika i očuvanje sigurnosti mreže. Države članice surađuju s Komisijom na procjeni učinaka i utvrđivanju jesu li potrebne dodatne mjere.

U svrhu jačanja jedinstvenog digitalnog tržišta, EU je u okviru svog javno-privatnog partnerstva za 5G (5G PPP) podržala 5G istraživačke projekte s više od 400 milijuna eura. 5G PPP, koji je pokrenut 2013. godine, služi istraživanju i promicanju 5G tehnologija u Europi. Kroz ovaj program, dodatna privatna ulaganja u ukupnom iznosu od preko milijardu eura postala su dostupna, dodatno jačajući vodeću ulogu EU-a u promicanju 5G usluga.

EU strategija za 5G prepoznaje kolosalnu vrijednost koju 5G tehnologija može donijeti gospodarstvu. Stručnjaci predviđaju godišnji promet od oko 200 milijardi eura diljem svijeta zahvaljujući 5G do 2025. godine. Također, očekuje se stvaranje oko 2 milijuna novih radnih mjesta unutar EU, što svjedoči o ekonomskoj snazi te strategije. Sve ove ambicije ovisne su o uspješnoj provedbi 5G Akcijskog plana EU-a. U skladu s tim, u centru EU strategije za 5G je Akcijski plan *5G za Europu*, koji čini bitan dio nastojanja EU da zadrži konkurentske prednosti Europe u digitalnom prostoru, potiče inovacije i potiče ekonomski rast.

U konačnici, dok se EU brzo kreće prema sveobuhvatnoj implementaciji 5G tehnologije, ona također ostaje fokusirana na sigurnost i zaštitu svojih digitalnih mreža i građana, stvarajući robustan i zaštićen digitalni prostor u kojem se očekuje da će 5G tehnologija igrati ključnu ulogu u budućnosti. Europski 5G Opservatorij prati napredak u postizanju ciljeva politike EU-a vezane uz 5G tehnologiju. Financira ga Europska komisija, a od kolovoza 2021. godine proizvode ga konzorcij tri tvrtke: VVA, PolicyTracker i LS Telcom.

5G Opservatorij se bavi problemima kao što su pokrivenost 5G mreže, dodjela spektra, usvajanje od strane novih vertikalnih industrija poput proizvodnje i poljoprivrede te javne politike za poticanje rasta 5G. Glavni fokus Opservatorija je na 5G tehnologiji u Europi, ali se također bave i velikim međunarodnim tržištima poput SAD-a, Japana, Kine i Južne Koreje. Svakog kvartala izrađuju detaljno izvješće koje analizira najnovija događanja.

5G Opservatorij započeo je svoje djelovanje 2018. godine i trenutno je u trećoj fazi. U svojoj prvoj fazi procijenio je napredak prema ciljevima politike postavljenim u 5G Akcijskom planu, od kojih je većina već postignuta. Bitan cilj je bio poticanje koordiniranog pristupa EU-a prema 5G tehnologiji, s puštanjem pionirskih opsega 5G spektra (700 MHz, 3,5 GHz i 26 GHz) i komercijalnim lansiranjem do 2020. godine. To se dogodilo u većini država članica, ali ne u svim. Opservatorij nastavlja procjenjivati napredak u ovom području.

Međutim, u trećoj fazi, glavni fokus 5G Opservatorija su ciljevi politike EU-a sadržani u inicijativi Digitalno desetljeće i Alatu za sigurnost 5G. To uključuje:

- 5G pokrivenost svih naseljenih područja do 2030. godine
- Paneuropsku implementaciju 5G koridora
- 5G inicijative za više zemalja
- Korištenje EU fondova za oporavak za projekte 5G
- Poboljšanje sigurnosti 5G mreža

- Ograničavanje bilo kakve ovisnosti o jednom dobavljaču 5G tehnologije
- Poticanje EU-a kao proizvođača 5G opreme

Da bi se pratili ti ciljevi, Opservatorij ispituje pitanja kao što su pokrivenost 5G, dodjela spektra te javne politike za poticanje rasta 5G. Posebno je važno usvajanje 5G tehnologije od strane novih vertikalnih industrija poput proizvodnje.

Studija o „Europskom 5G opservatoriju faza III" (CNECT/2021/OP/0008) pruža pregled napretka u razvoju 5G mreže unutar Europske Unije u periodu od tri mjeseca, sve do listopada 2022.

Aukcije za frekvencijski spektar koje su potrebne za postavljanje 5G mreže su održane u nekoliko država EU, uključujući Estoniju i Litvu. Ove aukcije omogućuju mobilnim operaterima da kupe pravo na korištenje određenih frekvencijskih opsega za postavljanje i operiranje 5G mreža.

Na razini EU i država članica, javno financiranje 5G i 6G projekata nastavlja se. Kao primjer, Španjolska je pokrenula drugu fazu svog 5G i 6G R&D fonda.

Mobilni operateri u Europi nastavljaju poboljšavati pokrivenost uslugama i uvode nove 5G funkcionalnosti. Njemački operater zračne luke Fraport objavio je ugovor s japanskom telekomunikacijskom tvrtkom NTT za izgradnju najveće europske 5G privatne mreže.

Operateri i telekomunikacijske tvrtke aktivno isprobavaju napredne tehnologije kao što su rezanje mreže (network slicing), koje omogućuje bolju kontrolu nad mrežnim resursima, i nezemaljski 5G.

Postoji rasprava o tome trebaju li usluge strujanja i druge velike tehnološke platforme dati pravedan doprinos troškovima 5G mreže u Europi. Ova debata je u tijeku.

Izvješće prati napredak u postizanju ciljeva 5G pokrivenosti do 2025. godine.

Sigurnost je ključna u 5G mrežama, a izvješće pokriva napredak u implementaciji alata za kibernetičku sigurnost.

Izvješće se bavi i pitanjima održivosti, uključujući doprinos mreža sljedeće generacije postizanju ciljeva i rješavanju Green Deala.

Ukupno gledano, ovo izvješće daje pregled širokog spektra aktivnosti koje se odvijaju u kontekstu razvoja 5G mreže (CNECT/2021/OP/0008).

Ispitivanje utjecaja ovog naprednog tehnološkog razvoja uključuje analizu:

- Tehnoloških unapređenja

5G donosi značajne inovacije kao što su ultra-visoke brzine prijenosa podataka, izuzetno niska latencija, povećani kapacitet, poboljšana povezanost i sposobnost povezivanja masovnog broja uređaja odjednom. Ove inovacije mogu omogućiti stvaranje novih industrijskih primjena i poslovnih modela.

- Utjecaja na ekonomiju

Uvođenje 5G mreže može imati značajan utjecaj na gospodarski rast. To uključuje direktno stvaranje radnih mjesta kroz izgradnju i održavanje mreže, kao i indirektno kroz poticanje inovacija u drugim sektorima.

- Sigurnosnih implikacija

Sa širenjem 5G mreže, povećavaju se i izazovi vezani za cyber sigurnost. Kako bi se osiguralo povjerenje u 5G mreže, važno je provesti temeljitu analizu potencijalnih sigurnosnih rizika i razviti strategije za njihovo ublažavanje.

- Utjecaja na okoliš

5G tehnologija ima potencijal za poboljšanje održivosti kroz promociju energetske učinkovitosti i podršku održivim inicijativama. S druge strane, izgradnja i održavanje 5G infrastrukture može imati određeni utjecaj na okoliš.

- Regulativnih aspekata

Za potpuno korištenje potencijala 5G tehnologije, potrebna je adekvatna regulativa koja će omogućiti inovacije, osigurati poštenu konkurenciju i zaštititi interese korisnika.

Studija o „Europskom 5G opservatoriju faza III" (CNECT/2021/OP/0008) opisuje stanje razvoja 5G mreže u EU i međunarodno, a potom ističe ključne strateške ciljeve EU za ovaj razvoj, tehnologiju i metode praćenja napretka.

5G Semafor je odjeljak koji pruža pregled dosadašnjeg napretka unutar EU. Sada su sve zemlje članice EU uspjele pokrenuti komercijalne 5G usluge barem na nekim dijelovima zemlje. Postoji oko 256,074 aktivnih 5G baznih stanica u EU, većinom koristeći Dynamic Spectrum Sharing (DSS) tehnologiju. Približno 72% stanovništva EU pokriveno je barem jednom 5G

mrežom. Kada se pogleda na globalnoj razini, Kina dominira sa skoro 1.8 milijuna instaliranih 5G baznih stanica. Južna Koreja ima najviše 5G baznih stanica po milijunu stanovnika. SAD je dodijelila najviše spektra za 5G mreže. Najčešće dodijeljeni 5G spektar u Europi je srednji pojas.

Napredak prema nadziranim ciljevima i strateškim implikacijama je odjeljak koji opisuje strateške ciljeve EU-a u vezi s 5G mrežom, uključujući 5G Akcijski plan, politiku Digitalnog desetljeća i 5G Cybersecurity Toolbox. Napredak prema ovim ciljevima praćen je kroz razne publikacije.

5G perspektive: Komentar i zapažanja o potrebi za daljnjim javnim inicijativama je odjeljak, koji se bavi ciljem EU-a da osigura neprekidni 5G za sva urbanizirana područja i glavne prometne pravce do 2025. godine, a do 2030.godine, pokriti sva naseljena područja. Razmatra se broj potrebnih 5G baznih stanica da se postigne ovaj cilj, posebno fokusirajući na bazne stanice od 3.6 GHz. Srednji spektri, poput 3.6 GHz, su ključni za postizanje većih brzina i niže latencije koje razlikuju 5G od 4G. Međutim, niži spektri ne pružaju visokokvalitetnu 5G uslugu.

Sve u svemu, izvješće predstavlja aktualno stanje razvoja 5G mreže u EU i svijetu, te ukazuje na strategije EU za postizanje njihovih ciljeva. Tekst naglašava važnost praćenja napretka, ulaganja u infrastrukturu, i ispravno korištenje spektra kako bi se postigle optimalne brzine i performanse koje 5G tehnologija omogućuje (CNECT/2021/OP/0008).

Jedan od bitnih ciljeva EU-a je osigurati neprekinuti 5G pristup za sve urbane i prometne regije do 2025. godine, te pokriti sva naseljena područja do 2030. godine. To zahtijeva značajna ulaganja u infrastrukturu, posebno u postavljanje i održavanje velikog broja baznih stanica koje omogućuju 5G signal.

Također, ispravno korištenje spektra je od presudne važnosti. Iz teksta je jasno da se srednji spektar (kao što je 3,6 GHz) smatra bitnim za pružanje visokokvalitetne 5G usluge, s obzirom na to da omogućuje veće brzine i niže latencije u odnosu na 4G. Niži spektri, s druge strane, ne mogu pružiti istu kvalitetu 5G usluge.

EU je postavila ambiciozne ciljeve za 5G pokrivenost, ali ostvarenje tih ciljeva zahtijeva strateško planiranje, investicije i pažljivo upravljanje raspoloživim resursima. Analizirana studija sugerira da će praćenje napretka biti presudno za ostvarenje tih ciljeva, te će podaci prikupljeni tijekom tog procesa pomoći u identificiranju područja koja zahtijevaju dodatnu pažnju ili resurse.

Niže se navodi nekoliko ključnih aspekata strategije EU-a za 5G mrežu:

- Performanse 5G Mreže

Studija navodi da 5G mreža pruža značajna poboljšanja performansi u srednjem pojasu, s primjerom T-Mobileove 5G mreže koja je postigla značajan porast brzina preuzimanja u usporedbi s 4G mrežom.

- Važnost optimalnog 5G

Studija ističe da se raspravlja o tome koliko su velike brzine i niska latencija, koje pruža 5G u srednjem pojasu, zaista potrebne. Za određene slučajeve upotrebe, poput automatiziranih tvornica ili poljoprivrednih primjena, ove će značajke biti vrlo važne. Međutim, za potrošače, brzine iznad određene točke možda neće donijeti mnogo veću korist.

- Rasprava o potrebi za brzinom

Dok neki smatraju da brzine iznad određene točke nisu potrebne za većinu potrošača, drugi smatraju da bi se za veće brzine moglo naplatiti više, što bi moglo povećati prosječan prihod po korisniku (ARPU).

- Važnost privatnih mreža

Za najnovije i najinovativnije 5G aplikacije, privatne mreže mogu biti ključne. Ove mreže mogu se instalirati od strane samih tvrtki ili sistemskih integratora. Izazov leži u tome što bi tisuće lokalnih vlasnika licenci moglo pružiti privatne 5G mreže, što bi moglo otežati praćenje napretka i procjenu stvarne vrijednosti 5G.

- Urbana vs Ruralna Pokrivenost

Studija postavlja pitanje o važnosti osiguravanja optimalne 5G pokrivenosti u svim područjima. Iako bi za neke vertikalne primjene, kao što su industrijske ili poljoprivredne, moglo biti korisno imati visoke brzine 5G, većina potrošača možda neće biti značajno pogođena nedostatkom velike brzine 5G.

Ova analiza studije naglašava kompleksnost pristupa uvođenju 5G mreže. EU mora balansirati između ulaganja u infrastrukturu, razumijevanja stvarnih potreba korisnika i istraživanja novih poslovnih modela koji bi mogli optimizirati iskorištavanje ove nove tehnologije. U svemu tome, najvažnija je strateška odluka o tome kako najbolje raspodijeliti spektar kako bi se postigao optimalan balans između performansi, pokrivenosti i troška (CNECT/2021/OP/0008).

Pri donošenju ove odluke, regulatori bi trebali razmotriti različite potrebe korisnika. Neki korisnici, poput industrijskih tvrtki koje koriste automatizirane strojeve, mogu imati visoke zahtjeve u pogledu brzine i latencije. Međutim, većina potrošača možda neće imati tako visoke zahtjeve. Iz toga proizlazi potreba za fleksibilnim pristupom koji može zadovoljiti različite potrebe korisnika.

Pored toga, EU bi trebala razmotriti ulogu privatnih 5G mreža. Ove mreže mogu pružiti snažne performanse za specifične upotrebe, ali njihovo korištenje može biti složeno zbog velikog broja potencijalnih vlasnika licenci. Iz tog razloga, regulatori bi trebali osmisliti učinkovite načine za nadzor i regulaciju ovih mreža.

Konačno, EU mora razmotriti ravnotežu između urbane i ruralne pokrivenosti. Postoji rizik da bi ruralna područja mogla ostati bez pristupa optimalnom 5G, što bi moglo imati negativne posljedice za ruralnu ekonomiju i društvo. Da bi se ovo izbjeglo, potrebno je osigurati adekvatna ulaganja u ruralnu infrastrukturu i odgovarajuće strategije za raspodjelu spektra.

Ukupno gledano, EU strategija za 5G mrežu zahtijeva sveobuhvatan i fleksibilan pristup koji uzima u obzir različite potrebe korisnika, kompleksnost tehnologije i geografske razlike unutar EU. Važno je da se prilikom planiranja i implementacije ovih strategija provodi pažljiva analiza i rasprava. Da bismo razumjeli rumunjski pristup i ciljeve politike Digitalnog desetljeća, najprije ćemo istražiti neke od ključnih koncepta koji su spomenuti.

Rumunjski pristup ogleda radi koristi sve prednosti 5G tehnologije, ali postavlja se pitanje privatnosti 5G mreže, posebno u ruralnim područjima gdje bi mogle biti potrebne za specifične primjene. Politika Digitalnog desetljeća ima cilj neprekinutog 5G pokrivenosti za sva urbana područja do 2025. godine, te pokrivenosti u svim naseljenim područjima do 2030. godine. Pritom, 5G mreže u nižim frekvencijskim pojasevima pružaju umjereno povećanje brzine i povećan kapacitet, što je posebno korisno u urbanim područjima. S druge strane, nije uvijek opravdano osigurati pokrivenost srednjim frekvencijama u ruralnim područjima, što zahtijeva značajne izdatke. Uz to, navodi se da će 5G pokrivenost svih naseljenih područja do 2030. godine biti postignuta kroz prirodni ciklus obnove opreme. No, postoji rizik da korisnici u ruralnim područjima neće osjetiti značajne koristi od 5G, osim ako postoji dobra pokrivenost i dovoljan kapacitet u nižim frekvencijskim pojasevima.

S gledišta 5G perspektive za 2025. godinu, izvještaj Ericssona predviđa značajan porast 5G pretplata u zapadnoj Europi, ali sporije prihvaćanje u srednjoj i istočnoj Europi. S druge strane,

izvještaj GSMA predviđa da će udio 5G tehnologije na tržištu Europe iznositi 44% do 2025. godine.

Ovi podaci ukazuju na to da EU strategija za 5G mrežu mora uzeti u obzir različite geografske, ekonomske i tehnološke aspekte. Potrebno je napraviti balans između pokrivenosti urbanog i ruralnog područja, kao i između nižih i srednjih frekvencija. Također, potrebno je stvoriti regulatorno okruženje koje omogućava pristup optimalnom 5G, uzimajući u obzir potrebe različitih korisnika, uključujući vertikale (specifične industrije). Strategija EU za 5G mrežu obuhvaća širok spektar aktivnosti koje ciljaju na unaprjeđenje uvjeta za uspostavu i razvoj 5G mreža u državama članicama EU.

Ovaj studija isto tako detaljno razrađuje komercijalni razvoj i pokrivenost stanovništva 5G mrežama u nekoliko država članica (CNECT/2021/OP/0008)

- Komercijalni razvoj

Siječanj 2022. godine, označen je kao trenutak kada je komercijalni 5G postao dostupan u svih 27 država članica EU-a. Detalji o pokretanjima po operaterima, upotrebi frekvencija, primjeni DSS tehnologije (Dinamičko dijeljenje spektra), konfiguraciji mreže (npr. 5G Non Standalone (NSA) u odnosu na samostalne (SA) implementacije) i ciljevima pokrivenosti dostupni su na web stranici Europskog 5G opservatorija. Tekst donosi nekoliko specifičnih primjera razvoja 5G u državama poput Njemačke, Grčke, Italije, Portugala i Španjolske.

- Pokrivenost stanovništva

Izvješće navodi da je osnovna vrijednost za 5G pokrivenost u EU bila 14% naseljenih područja u ožujku 2020. Metodologija za praćenje pokrivenosti stanovništva promijenjena je i sada koristi podatke prikupljene od strane Komisije za Digital Economy and Society Index (DESI). Trenutna procijenjena pokrivenost za EU27 je 72%, što je izračunato na temelju ukupnog broja obuhvaćenih ljudi u svakoj zemlji podijeljeno s ukupnom populacijom EU27.

U studiji se naglašava napredak u implementaciji 5G mreža u državama članicama EU, ali i ukazuje na kontinuirane napore i planove za proširenje i poboljšanje pokrivenosti 5G u budućnosti. Ova analiza daje pregled o usporedbi implementacije 5G mreže u različitim svjetskim regijama, s posebnim fokusom na EU. Ključne teme koje analiza pokriva uključuju postavljanje 5G baznih stanica, dodjelu 5G spektra i razlike u trendovima dodjele spektra među različitim regijama.

Prvi odjeljak (A1.3) pruža pregled broja 5G baznih stanica po različitim regijama. Po ovom pokazatelju, Južna Koreja je najnaprednija u implementaciji 5G tehnologije, s jednom baznom stanicom na svakih 319 stanovnika. Slijedi Kina, a zatim EU, koja je ispred SAD-a.

Kada je u pitanju dodjela 5G spektra, 3,6 GHz pojas je najčešće korišteni globalno, a svaka od četiri navedene zemlje (Južna Koreja, Kina, EU, SAD) ga je dodijelila. Opseg od 28 GHz je također široko usvojen, ali situacija u EU je složenija jer svaka zemlja dodjeljuje vlastiti spektar. U nastavku studije naglašavaju se razlike u dodjeli 5G spektra između EU-a i ostatka svijeta. Predstavljaju se pionirski pojasevi identificirani u EU za početno pokretanje 5G usluga, koji uključuju opsege ispod 1 GHz, između 1 GHz i 6 GHz, i iznad 6 GHz.

Ističe se da su sve države članice EU trebale dodijeliti frekvencijske pojaseve od 700 MHz i 3,6 GHz do kraja 2020., no neke države to nisu učinile. Također, pokazuje se da je 3,6 GHz najčešće dodijeljeni pojas, dok je 26 GHz najmanje dodijeljen.

Konačno, analiza studije pruža međunarodni pregled dodjele spektra, pokazujeći različite pojaseve spektra koji su dodijeljeni za 5G na raznim međunarodnim tržištima. Ovo je važno za shvaćanje kako se implementacija 5G tehnologije odvija na globalnoj razini:

- Dodjela 5G spektra

Pojmovi srednjepojasni, niskopojasni i visokopojasni spektar se odnose na različite frekvencijske pojaseve koje 5G tehnologija koristi. Na globalnoj razini, srednjepojasni spektar je bio najpopularniji za 5G mreže, dok su niskopojasni i visokopojasni spektar bili nešto manje popularni, ovisno o tržištu.

- 5G vertikale

Vertikalne industrije se odnose na specifične industrije koje bi mogle profitirati od implementacije 5G tehnologija, poput automobilske industrije, zdravstva, industrijske automatizacije, i druge. EU je financirala istraživanje i razvoj ovih vertikala putem projekta 5G javno-privatnog partnerstva (5G JPP).

- Spektar za 5G vertikale

Model licenciranja potreban za 5G vertikale predmet je tekuće rasprave. 5G vertikale mogu koristiti spektar dodijeljen mobilnim operaterima, ili se mogu osloniti na namjenske licence za spektar koje izdaju vlade. Postoji rizik od fragmentacije 5G spektra ako se previše frekvencija

dodijeli vertikalama, što bi moglo rezultirati smanjenom brzinom i kvalitetom usluge. No, mnoge zemlje, uključujući mnoge članice EU, su počele dodjeljivati određene frekvencije namijenjene specifično za 5G vertikale.

- Međunarodni kontekst

5G tehnologija nije samo relevantna za EU, već i za globalno tržište. Analiza pruža nekoliko primjera razvoja 5G tehnologija u drugim zemljama, poput Kine, SAD-a, Japana i Južne Koreje.

- Različiti frekvencijski opsezi 5G spektra

Analiza navodi da su različite zemlje dodijelile različite količine spektra za 5G mrežu u različitim opsezima. Niskopojasni spektar (700 MHz) nije bio vrlo popularan, ali se to može promijeniti s novim inicijativama u Kini. Srednjepojasni spektar je osnovni pojas za 5G u većini država, s Japanom i Kinom kao vodećim državama u dodjeli spektra. Visokopojasni spektar je inicijalno bio vrlo popularan, posebno u SAD-u, no njegova popularnost možda je dosegnula vrhunac.

- 5G vertikale

5G mreža ne koristi se samo za ljudsku komunikaciju, već ima potencijal pružanja usluga za razne industrije, uključujući automobilsku industriju, industrijsku i poljoprivrednu automatizaciju, zdravstvo i druge. 5G standardi se neprestano ažuriraju kako bi optimizirali 5G za ove vertikalne domene.

- Licenciranje spektra za 5G vertikale

Postoje rasprave o tome trebaju li 5G vertikale koristiti spektar koji je već dodijeljen mobilnim operaterima, ili se trebaju osloniti na posebne licence za spektar koje izdaju vlade. Dok neki podržavaju ideju posebnih licenci za spektar, postoje argumenti protiv toga. Bez obzira na ove rasprave, brojne zemlje, uključujući nekoliko zemalja EU-a, usvajaju model licenciranja koji koristi posebni spektar za 5G vertikale. Ovaj pristup može varirati između različitih zemalja, što može uzrokovati probleme pri standardizaciji opreme.

U kontekstu EU-a, 5G se smatra najvažnijim za digitalnu transformaciju poslovanja. EU financira projekte povezane s 5G mrežom kroz Javno privatno partnerstvo (5G-PPP), a postoji i Task Force za koordinaciju i praćenje aktivnosti.

Frekvencijski opsezi 5G spektra odnose se na različite dijelove radiofrekvencijskog spektra koji se koriste za bežičnu komunikaciju. Ova tri opsega redom: niskopojasni, srednjepojasni i visokopojasni imaju različite karakteristike koje ih čine pogodnima za različite upotrebe.

Niskopojasni spektar (do 1 GHz, obično oko 700 MHz) ima izvrsnu sposobnost prodiranja kroz zgrade i druge prepreke, a signal može putovati velikim udaljenostima. Međutim, ovaj spektar može prenijeti samo ograničenu količinu podataka, što znači da ne može podržati veliki broj korisnika ili visokokvalitetne usluge kao što je 4K video.

Srednjepojasni spektar (1-6 GHz) predstavlja dobru ravnotežu između sposobnosti prodiranja i kapaciteta. To ga čini izborom broj jedan za većinu 5G mreža.

Visokopojasni spektar (24 GHz i više, poznat kao milimetarski valovi) može prenijeti veliku količinu podataka, što omogućuje vrlo brze brzine i velike količine korisnika. Međutim, ima loše prodiranje kroz zgrade i ne putuje velikim udaljenostima.

S obzirom na ove razlike, različite zemlje dodjeljuju različite količine spektra u ovim opsezima za 5G. Niskopojasni spektar možda nije bio popularan zbog svoje ograničene propusnosti, ali inicijative u Kini mogu to promijeniti. Srednjepojasni spektar je izbor za većinu zemalja zbog svoje ravnoteže između prodiranja i kapaciteta. Visokopojasni spektar je bio popularan zbog svoje velike propusnosti, ali njegova popularnost dosegnula je vrhunac zbog njegovih ograničenja u prodiranju i dometu. Termin 5G vertikale odnosi se na različite industrijske sektore koji mogu imati koristi od primjene 5G tehnologija. One nisu samo korisne za poboljšanje bežične komunikacije među ljudima (putem pametnih telefona, na primjer), već pružaju velike mogućnosti za transformaciju različitih industrijskih sektora. Evo nekoliko primjera: (CNECT/2021/OP/0008)

- Automobilska industrija

5G može podržati razvoj autonomnih vozila putem naprednih komunikacijskih mreža koje omogućuju vozilima komunikaciju s drugim vozilima, infrastrukturom i pješacima.

- Industrijska i poljoprivredna automatizacija

5G tehnologija može omogućiti bolju koordinaciju i upravljanje robotima i automatiziranim sustavima u industrijskim postrojenjima i na poljoprivrednim površinama.

- Zdravstvo

5G može omogućiti daljinsko praćenje pacijenata, telemedicinu, brže prenošenje medicinskih podataka, kao i napredne kirurške postupke poput daljinskih operacija.

Ostale industrije mogu uključivati energetiku, medije i zabavu, obrazovanje, trgovinu i mnoge druge.

Standardi 5G se neprestano ažuriraju kako bi se osigurala njegova optimalna primjena u ovim vertikalnim domenama. To znači da inženjeri i istraživači stalno rade na poboljšanju načina na koji 5G tehnologija može zadovoljiti specifične potrebe svake od ovih industrija. Spektralne licence su dozvole koje vlade izdaju da bi se koristile određene frekvencije radio spektra. Za 5G vertikale, postoji rasprava o tome kako bi se spektar trebao licencirati. S jedne strane, neki ljudi smatraju da bi 5G vertikale trebale koristiti spektar koji je već dodijeljen postojećim mobilnim operaterima. To bi moglo olakšati upotrebu i implementaciju 5G u tim industrijskim sektorima, jer bi mogli koristiti postojeću infrastrukturu i tehnologiju. S druge strane, neki smatraju da bi 5G vertikale trebale dobiti posebne spektralne licence. Argument je da bi to omogućilo specifične upotrebe spektra koje su optimizirane za određene industrijske sektore, potencijalno pružajući bolju uslugu za te sektore (CNECT/2021/OP/0008).

Postoje argumenti protiv posebnih licenci za spektar. Na primjer, može biti teško upravljati i koordinirati korištenje spektra ako se dodjeljuju različite licence za različite sektore. Također, postoji rizik od fragmentacije tržišta, s obzirom da oprema proizvedena za jednu specifičnu licencu možda neće biti kompatibilna s opremom za drugu licencu.

Nekoliko zemalja, uključujući nekoliko članica EU-a, usvojilo je model licenciranja koji koristi posebni spektar za 5G vertikale. Ovo stvara raznolikost u načinu na koji se 5G implementira u različitim zemljama, što može dovesti do problema u standardizaciji opreme, budući da oprema koja je kompatibilna sa spektrom u jednoj zemlji možda neće biti kompatibilna s onom u drugoj. Ovaj tekst pokriva mnogo aspekata 5G strategije u EU. Evo sažetka i tumačenja ključnih segmenata:

Privatne 5G mreže su specijalizirane mreže koje koriste tvrtke za specifične svrhe, kao što su automatizacija proizvodnje, vođenje velikih kampusa, luka i zračnih luka. Nisu namijenjene javnoj upotrebi kao što su uobičajene mobilne usluge. Opservatorij je sastavio popis ovih mreža za daljnje istraživanje i analizu.

Trendovi tržišta opskrbe (dobavljači) navodi se da su veliki telekom operateri u zemljama EU-a nedavno obavili velike nabave za izgradnju 5G mreže. Također se spominje otvoreni RAN

(Radio Access Network), koji se odnosi na ideju decentralizacije mreže koristeći standarde i tehnologije koje mogu podržavati više dobavljača.

Elektromagnetska polja (EMF) predstavljaju moguću brigu u vezi s 5G tehnologijom. Ovaj dio navodi da je postojala nekonzistentnost u primjeni ograničenja EMF-a u državama članicama EU-a. Znanstveni odbor za zdravlje, okoliš i Emerging Risks (SCHEER) zadužen je za davanje mišljenja o tehničkoj reviziji postojećih preporuka i smjernica.

Kibernetička sigurnost je važan aspekt razvoja 5G, te EU ima sveobuhvatne mjere za sigurnost 5G mreže. Doprinos mreža postizanju ekoloških standarda naglašava važnost održivosti u kontekstu 5G razvoja, uključujući smanjenje emisija i potrošnje energije. Naglašava se da 5G mreže mogu biti do 90% energetski učinkovitije po jedinici prijenosa podataka od 4G mreža. Svaki od ovih segmenata pokriva specifičan aspekt strategije EU-a za 5G tehnologiju, uključujući implementaciju, kibernetičku sigurnost, održivost, zdravstvene i sigurnosne smjernice, i kako ova tehnologija može pridonijeti ekonomskim i društvenim ciljevima. EU strategija za 5G mrežu uključuje brojne inicijative kako bi se osiguralo pravovremeno i učinkovito uvođenje ove tehnologije. Jedan od najvažnijih alata u ovoj strategiji je Preporuka Komisije o zajedničkom skupu alata Unije, poznat kao *Connectivity Toolbox*. Ova preporuka poziva države članice da potaknu ulaganja u infrastrukturu za širokopojasnu vezu velikog kapaciteta, uključujući 5G, što je ključno za digitalnu transformaciju i oporavak (CNECT/2021/OP/0008).

Connectivity Toolbox je skup najboljih praksi namijenjen pomoći u pravovremenoj implementaciji 5G i brzih širokopojasnih mreža. Ovaj alat pruža smjernice za implementaciju optičkih i 5G mreža, te pomaže mrežnim operaterima smanjiti troškove postavljanja mreža. Države članice mogu koristiti ove mjere kako bi operaterima omogućile pristup potrebnom spektru za uvođenje 5G, kao i poticanje daljnjih ulaganja u 5G pokrivenost. Posebna skupina za povezivanje, sastavljena od predstavnika država članica i Komisije, osnovana je kako bi pomogla državama članicama u identificiranju i dogovoru o najboljim praksama. Ova skupina surađuje, gdje je to prikladno, s različitim relevantnim grupama i regulatorima, uključujući Grupu za politiku radijskog spektra (RSPG), Tijelo europskih regulatora za elektroničke komunikacije (BEREC), nacionalna regulatorna tijela (NRA), mrežu Ureda za kompetenciju širokopojasnog pristupa (BCO mreža) i relevantna tijela zadužena za poslove jedinstvene informacijske točke (CNECT/2021/OP/0008).

Slijedom analiziranog, jasno proizlazi da se EU strategija za 5G mrežu koristi različitim alatima i resursima kako bi potaknula ulaganja, smanjila troškove i osigurala pravovremeno uvođenje 5G mreža. Ovaj koordinirani pristup osigurava da se 5G tehnologija može učinkovito i efikasno implementirati u cijeloj EU, što će donijeti značajne gospodarske prilike i potaknuti digitalnu transformaciju

2.3.3. Strategija 5G mreže u Republici Hrvatskoj

Strategija za implementaciju 5G mreže u Republici Hrvatskoj ima jasan cilj pokriti sva naseljena područja 5G mrežom do 2030. godine. Ova ambiciozna vizija osigurat će da sva naseljena područja u zemlji budu povezana s ovom naprednom tehnologijom, pružajući pristup bržim i učinkovitijim mobilnim uslugama. Do danas, napredak je već ostvaren u pogledu implementacije 5G mreže. Broj baznih stanica koje su postavljene već premašuje 2,711, što pokazuje značajan napredak u infrastrukturi mreže. Osim toga, performanse mreže već pokazuju brzine prijenosa podataka od 111,83 Mbit/s, što je znatno brže od prethodnih generacija mobilnih mreža.

Dodatno, cijeli spektar 5G pionirskih bendova sada se koristi u potpunosti, što ukazuje na to da je Hrvatska potpuno iskoristila dostupni 5G spektar za implementaciju mreže. Trenutačno je pokriveno 60% stanovništva, ali cilj je da do 2030. godine ta brojka naraste do 100%. Međutim, postoji nekoliko područja gdje su informacije još uvijek nedostupne. Na primjer, podaci o broju prijeđenih kilometara glavnih prometnih ruta koje su pokrivene 5G mrežom još uvijek nisu dostupni. Također, nisu identificirani nikakvi sporazumi ili projekti povezani s 5G koridorima.

Kada je u pitanju vertikalna primjena 5G mreže, Republika Hrvatska ima cilj uključiti 5G tehnologiju kao središnji dio novih proizvoda, proizvodnih procesa i poslovnih modela. Međutim, trenutačno nema identificiranih projekata ili inicijativa koji se bave ovom oblasti.

U kontekstu neizravno relevantnih ciljeva, Republika Hrvatska planira da 20% svojih sredstava za oporavak i otpornost bude usmjereno na digitalne prioritete, uključujući 5G.

Ova strategija za 5G pokazuje jasnu predanost Republike Hrvatske da bude na čelu implementacije ove tehnologije. Kako se bližimo 2030. godini, očekuje se da će se ovi napori samo povećati kako bi se osiguralo da sva naseljena područja u Hrvatskoj imaju pristup brzim, pouzdanim i sigurnim 5G uslugama.

Na kraju, EU strategija za 5G mrežu naglašava potrebu za suradnjom između država članica, industrije, akademske zajednice i ostalih dionika u procesu implementacije ove tehnologije. Kako je istaknuto u radu Frattasi et al. (2016), ovaj multidisciplinarni pristup ključan je za ostvarivanje punog potencijala 5G tehnologije.

2.3.4. Utjecaj 5G mreže na globalnu ekonomiju

5G tehnologija predstavlja važan tehnološki preokret s potencijalno velikim ekonomskim utjecajem. Prema studiji koju je objavio Qualcomm, globalni proizvođač čipova i tehnoloških rješenja, očekuje se da će do 2035. godine 5G tehnologija generirati do 13,2 bilijuna dolara globalne ekonomske vrijednosti i podržavati 22,3 milijuna radnih mjesta širom svijeta.

Prednosti 5G mreže, uključujući superbrzi internet, ultra nisku latenciju i sposobnost povezivanja velikog broja uređaja, mogu dovesti do velikog napretka u brojnim sektorima. Na primjer, u automobilskoj industriji, 5G će omogućiti bolju implementaciju autonomnih vozila i poboljšati sigurnost na cestama. U zdravstvenom sektoru, 5G može omogućiti daljinski monitoring pacijenata i telemedicine, poboljšavajući pristup i kvalitetu zdravstvene skrbi.

Prema Qualcommovom izvještaju, proizvođači 5G tehnologije mogli bi investirati do 3,5 bilijuna dolara do 2035., čime bi se dodatno potaknulo zapošljavanje i ekonomski rast. Također, očekuje se da će sektor informacijskih i komunikacijskih tehnologija imati najveći udio u ekonomskom utjecaju 5G-a, s očekivanim rastom od 35% u sljedećih 15 godina.

U kontekstu globalne ekonomije, očekuje se da će 5G tehnologija imati značajan utjecaj na proizvodnju, produktivnost i zaposlenost. Kao što Qualcomm navodi u svojoj studiji, potencijal 5G-a za transformaciju industrijskih sektora, unapređenje proizvoda i usluga, te poticanje inovacija i produktivnosti, čini ga ključnim čimbenikom globalnog ekonomskog rasta u nadolazećim desetljećima.

Iz ovoga se može zaključiti da je 5G tehnologija ne samo ključna za budućnost telekomunikacija, već i za globalnu ekonomiju. Kroz svoje sposobnosti, 5G pruža nove mogućnosti za industrije, poduzeća i potrošače, dok istovremeno potiče ekonomski rast i stvaranje radnih mjesta. Stoga je razumijevanje i iskorištavanje potencijala 5G-a od ključne važnosti za budućnost globalne ekonomije (Qualcomm, 2023).

2.3.5. Utjecaj 5G tehnologije na europsku ekonomiju

Ovo poglavlje istražuje utjecaj 5G tehnologije, sljedećeg velikog koraka u svijetu tehnologije, na ekonomiju Europe, uključujući članice EU-a i Ujedinjeno Kraljevstvo. Analiza uključuje detaljno ispitivanje ekonomske koristi koju 5G donosi, prikaz kako će ključne industrije biti pod utjecajem velikih industrijskih primjena 5G, kao i identifikaciju mogućnosti za ubrzanje ekonomskih koristi od 5G. 5G se očekuje da će biti pokretačka sila za rast i otpornost u post-COVID europskom gospodarstvu.

Od 2009. godine kada je prva 4G LTE mreža pokrenuta u Švedskoj, mobilne tehnologije su duboko utjecale na gospodarstva i društva. Sada, 14 godina kasnije, očekuje se da će 5G mreže i tehnologija dodatno revolucionirati bežične komunikacije transformirajući postojeće tržišne sektore i industrije. Osim poboljšanja mogućnosti omogućenih 4G, poput bržeg streaminga videozapisa, 5G će otključati novi potencijal za tehnologije poput umjetne inteligencije (AI), rubnog računanja i IoT-a. 5G će biti od ključne važnosti za uspjeh ovih tehnologija nudeći bogatu dvosmjernu komunikaciju i potencijal za podršku do milijun uređaja po kvadratnom kilometru, te ultra-pouzdan odziv u manje od milisekunde.

Prema Accentureovoj najnovijoj analizi, utjecaj 5G na europsko gospodarstvo potaknut će do 2,0 bilijuna eura inkrementalnog rasta bruto proizvodnje između 2021. i 2025. godine. U istom razdoblju, 5G bi mogao dodati do 1,0 trilijuna eura europskom BDP-u, ima potencijal stvoriti ili transformirati do 20 milijuna radnih mjesta u svim sektorima gospodarstva, a učinci multiplikacije osjetit će se u svakoj industriji.

5G će imati utjecaj na svaku regiju, od stvaranja dodatnih 10 milijardi eura BDP-a i transformacije do 190 tisuća radnih mjesta u Grčkoj, do stvaranja 182 milijarde eura BDP-a i 4,6 milijuna radnih mjesta u Njemačkoj. Ključno je napomenuti da će 5G tehnologija pozicionirati europsko gospodarstvo za ubrzani oporavak od posljedica pandemije COVID-19. Dok se poduzeća suočavaju s nezapamćenom potražnjom i poremećajima u lancima opskrbe, 5G će potaknuti prijeko potrebni rast i unaprijediti dugoročnu fleksibilnost lanaca vrijednosti. Također, 5G ekosustav će potaknuti buduću ekonomsku otpornost oslobađanjem većeg broja radnika od fizičkih radnih stanica, potičući rast u novim industrijama koje su digitalne u svojoj srži i unapređujući učinkovitost i produktivnost u brojnim drugim industrijama. Ubrzana

implementacija 5G može osigurati da europsko gospodarstvo izađe iz ove krize jače nego ikad prije.

5G se smatra temeljnom tehnologijom koja omogućuje komunikaciju i podržava razvoj uređaja kroz lanac vrijednosti, od proizvođača čipseta do razvijača infrastrukture. Razvoj bežične tehnologije zahtijeva od tvrtki velika i dosljedna ulaganja u istraživanje i razvoj kako bi se potaknule inovacije s dugoročnim horizontom prije nego što se koristi materijaliziraju, čime se potiče ravnoteža između suradnje u cijelom ekosustavu i snažne strategije zaštite intelektualnog vlasništva.

U osnovi, poboljšana mobilna širokopojasna veza (eMBB) je najvažnija komponenta 5G-a koja omogućuje visoko brzi prijenos podataka, znatno premašujući kapacitete 4G mreže. Prema mišljenju stručnjaka, to može dramatično transformirati način na koji koristimo digitalne tehnologije, otvarajući potpuno nove prilike za inovacije. Kada se radi o ekonomskom utjecaju, poboljšana širokopojasna veza omogućuje stvaranje novih industrija, usluga i poslovnih modela. Na primjer, istraživači poput Thomasa L. Friedmana sugeriraju da će povećane brzine prijenosa omogućiti intenzivnije korištenje tehnologija poput proširene stvarnosti (AR) i virtualne stvarnosti (VR). AR i VR trenutačno su ograničene zbog tehničkih izazova vezanih uz brzinu prijenosa i latenciju, ali s dolaskom 5G-a, ove tehnologije bi se mogle ubrzano razvijati i šire koristiti, otvarajući potpuno novu industriju s potencijalom za stvaranje novih radnih mjesta i gospodarskog rasta.

Pored toga, eMBB će bitno promijeniti i način na koji komuniciramo i dijelimo informacije. Kako ističe Erik Brynjolfsson, direktor MIT Initiative on the Digital Economy, 5G tehnologija pruža mogućnost za bogat dvosmjerni prijenos podataka. To znači da ne samo da ćemo moći preuzimati podatke brže, već ćemo ih i brže slati. To će potaknuti daljnji razvoj tehnologija kao što su računalni vid (CV) i strojno učenje (ML), što će omogućiti stvaranje naprednih AI sustava koji se mogu koristiti u nizu industrija, od zdravstva do automobilske industrije.

Za tvrtke, eMBB pruža priliku za poboljšanje svoje produktivnosti i efikasnosti. Kako ističe Harald Haas, profesor Mobile Communications na Sveučilištu u Edinburghu, 5G će omogućiti tvrtkama da prenesu velike količine podataka brže nego ikad prije, što će im omogućiti da brže donose odluke i bolje upravljaju svojim operacijama.

5G omogućuje simultanu povezanost do potencijalno milijun veza po kvadratnom kilometru. Ova masivna gustoća povezivanja ključna je za učinkovitu implementaciju naprednih aplikacija

industrije 4.0 i pametnih gradova. MIoT će omogućiti iznimnu količinu IoT uređaja da komuniciraju međusobno na istom području, što je ključno za automatizaciju i optimizaciju procesa u industrijskom kontekstu, kao i za potporu rastućim zahtjevima urbanizacije u okviru koncepta pametnih gradova.

Na primjer, IoT uređaji mogu se koristiti za nadzor rada strojeva u industriji, omogućujući tvrtkama da otkriju i poprave probleme prije nego što uzrokuju značajnije poteškoće. Ovo može značajno smanjiti vremenske i financijske troškove povezane s održavanjem opreme. Dodatno, IoT uređaji mogu prikupljati podatke o radu strojeva kako bi se optimizirala njihova učinkovitost i smanjila potrošnja energije.

U kontekstu pametnih gradova, masivna povezanost IoT uređaja omogućuje kreiranje mreže senzora i uređaja koji mogu nadzirati i kontrolirati različite aspekte urbanog života, od prometa do upravljanja otpadom. Ovo može značajno poboljšati učinkovitost gradskih usluga i kvalitetu života stanovnika.

Prema mišljenju stručnjaka poput Brenna Bermana, izvršnog direktora City Tech Collaborative-a, mIoT će biti najvaćniji za rješavanje izazova s kojima se suočavaju moderni gradovi. Ističe da će mIoT omogućiti gradovima da postanu pametniji kroz poboljšanje učinkovitosti, smanjenje troškova, poboljšanje kvalitete života građana i smanjenje utjecaja na okoliš.

U ekonomskom smislu, masivna implementacija IoT uređaja mogla bi potaknuti stvaranje novih industrija i poslovnih modela, povećavajući potražnju za uređajima, softverom, uslugama i infrastrukturom vezanom uz IoT. Također, mogla bi potaknuti inovacije i produktivnost u postojećim industrijama kroz automatizaciju i optimizaciju procesa. Treći ključni napredak koji 5G donosi je ultra pouzdana i niskolatentna komunikacija (URLLC):

Ultra pouzdana i niskolatentna komunikacija (URLLC) odnosi se na latenciju ili vrijeme potrebno da informacija putuje od točke A do točke B, te se drastično smanjuje s 5G tehnologijom. 5G se očekuje smanjiti latenciju na manje od milisekunde, što je značajno poboljšanje u odnosu na 4G mreže koje trenutno imaju latenciju između 10 i 50 milisekundi. Ova izuzetno niska latencija ključna je za podršku aplikacijama koje zahtijevaju gotovo trenutačnu reakciju, kao što su autonomna vozila, telemedicina, industrijska automatizacija i druge kritične infrastrukture.

Autonomna vozila, na primjer, zahtijevaju gotovo trenutačnu komunikaciju između vozila i infrastrukture kako bi mogla sigurno i učinkovito funkcionirati. Isto tako, u telemedicini, niska latencija može omogućiti daljinske operacije, gdje kirurg, koji se nalazi na drugom mjestu, upravlja robotskim instrumentima u realnom vremenu.

Ekonomski, ULRLC će omogućiti stvaranje novih industrija i poslovnih modela koji se oslanjaju na visoku pouzdanost i nisku latenciju. Na primjer, moglo bi se potaknuti široko prihvaćanje autonomnih vozila, što bi moglo dovesti do značajnih ušteda u pogledu vremena i sigurnosti. Također, mogao bi se potaknuti razvoj telemedicine, što bi moglo poboljšati pristup zdravstvenoj skrbi, smanjiti troškove i poboljšati ishode za pacijente.

Prema nekim procjenama, kao što je ona koju je objavio World Economic Forum, sektor telemedicine mogao bi dostići tržišnu vrijednost od 266,8 milijardi dolara do 2026. godine, djelomično zahvaljujući mogućnostima koje donosi 5G.

Dakle, ULRLC je još jedan aspekt 5G tehnologije koji ima potencijal značajno potaknuti ekonomski rast i inovacije, omogućavajući razvoj novih industrija i poboljšavajući produktivnost u postojećima.

2.4. 5G mreža u kontekstu Interneta stvari

5G mreža, kako je to istaknuo Wang et al., (2020), unosi revolucionarne promjene u domenu IoT-a. Njezine ključne karakteristike, poput brzih brzina prijenosa, velikog kapaciteta mreže i smanjenog kašnjenja, omogućavaju bolje performanse i novu razinu funkcionalnosti IoT uređaja. Brzina prijenosa podataka od vitalne je važnosti za IoT. Prema Gao et al., (2016), 5G mreža omogućava prijenos podataka velikom brzinom koja doseže do 20 gigabita u sekundi. Ovo je znatno brže u usporedbi s prethodnim generacijama mobilnih mreža, što omogućava IoT uređajima brzo slanje i primanje velike količine podataka. Ovo je posebno važno za IoT aplikacije koje zahtijevaju velike protokove podataka, poput autonomnih vozila ili pametnih gradova.

Pored brzine prijenosa, kapacitet mreže također igra ključnu ulogu u IoT ekosustavu. Prema izvještaju Boccardi et al., (2014), 5G mreže imaju sposobnost podržavanja do milijun uređaja po kvadratnom kilometru. Ovo omogućava povezivanje velikog broja IoT uređaja, što je

neophodno u scenarijima kao što su pametni gradovi ili industrijski IoT, gdje se velik broj uređaja treba simultano povezati na mrežu.

Konačno, 5G mreža pruža smanjenje kašnjenja, što je važan element za mnoge IoT aplikacije. Kao što je prikazano u studiji Aijaz et al., (2018), 5G mreža omogućava latenciju manju od 1 milisekunde. Ova ultra niska latencija omogućava gotovo trenutačan prijenos podataka, što je od kritične važnosti za aplikacije koje zahtijevaju brzi odziv, poput industrijske automatizacije, autonomnih vozila ili zdravstvenih usluga. 5G mreža donosi značajne prednosti koje će oblikovati budućnost Interneta stvari. Njene bitne značajke, kao što su brza brzina prijenosa, veliki kapacitet mreže i ultra niska latencija, pružaju novi set mogućnosti za IoT aplikacije.

Brže brzine prijenosa, koje 5G mreža omogućava, predstavljaju temeljni element u realizaciji naprednih IoT aplikacija. Prema studiji Andrews et al., (2016), velika brzina prijenosa podataka ključna je za aplikacije koje zahtijevaju intenzivno korištenje podataka.

Na primjer, autonomna vozila koriste veliki broj senzora za prikupljanje podataka iz okruženja. Da bi se osigurala njihova sigurna i učinkovita operacija, ti podaci moraju biti preneseni i obrađeni gotovo u realnom vremenu. Bez brzih brzina prijenosa koje 5G omogućava, to jednostavno ne bi bilo moguće. Ova tvrdnja je dodatno potkrijepljena istraživanjima Xiong et al., (2021), koji su naglasili ključnu ulogu 5G mreže u autonomnom vožnji.

Slično tome, telemetrijski podržana medicina, poznata i kao telemedicina, koristi se za pružanje medicinskih usluga na daljinu. Pojačanje ovog sektora, kako to pokazuje Guo et al., (2019), omogućuje zdravstvenim stručnjacima pristup vitalnim podacima pacijenata gotovo u realnom vremenu. Ovo ne samo da poboljšava pružanje medicinske skrbi, već i omogućava pravovremeno liječenje pacijenata, što može biti ključno u hitnim situacijama. Ove aplikacije također zahtijevaju brzu brzinu prijenosa podataka, što je još jedan aspekt gdje 5G mreža donosi znatno poboljšanje.

Povećani kapacitet mreže koji 5G tehnologija nudi od iznimne je važnostije za podršku velikom broju IoT uređaja. Kako je Boccardi et al., (2014) objasnio, 5G mreže imaju sposobnost podržavanja do milijun uređaja po kvadratnom kilometru. Ovaj povećani kapacitet mreže omogućava simultano povezivanje i komunikaciju velikog broja uređaja bez ikakvog smanjenja performansi mreže. Primjer ovog može se vidjeti u konceptu pametnih gradova, gdje se tisuće uređaja koristi za nadzor i kontrolu različitih aspekata urbanog okruženja, od prometa do

energetske učinkovitosti. Prema izvještaju Nikitakos et al., (2020), bez visokog kapaciteta mreže koji 5G nudi, integracija i efikasno upravljanje ovim uređajima bilo bi teško postići.

Slično tome, industrijski IoT, koji se često koristi u industrijskim postrojenjima i proizvodnim pogonima, zahtijeva mrežu koja može podržati veliki broj povezanih uređaja. Istraživanje Al-Fuqaha et al., (2015) naglasilo je da je održavanje stabilne i učinkovite mreže ključno za postizanje optimalne proizvodnje i smanjenje pogrešaka u industrijskom IoT okruženju. Stoga, 5G mreža s povećanim kapacitetom omogućuje bezbrižno povezivanje i komunikaciju velikog broja IoT uređaja. Bilo da se radi o pametnim gradovima ili industrijskom IoT-u, ovaj povećani kapacitet mreže donosi novu razinu učinkovitosti i performansi.

Smanjenje kašnjenja, ili latencije, predstavlja jedan od ključnih aspekata koji 5G tehnologija donosi u kontekstu IoT-a. Kao što je Aijaz et al., (2018) pojasnio, niska latencija koju 5G omogućava, ključna je za IoT aplikacije koje zahtijevaju brzi odziv i gotovo trenutni prijenos podataka. Industrijska automatizacija, na primjer, obuhvaća procese koji zahtijevaju brze reakcije i visoku preciznost. Bilo da se radi o preciznom pozicioniranju robota na proizvodnoj liniji ili o nadzoru sigurnosnih parametara, kašnjenje u prijenosu podataka može rezultirati neefikasnostima ili čak nesrećama. Zhang et al., (2019) su u svojoj studiji naglasili da niska latencija koju 5G pruža omogućava efikasnu industrijsku automatizaciju uz visok stupanj pouzdanosti.

Slično tome, bežični kontrolni sustavi također zahtijevaju brzi prijenos podataka. U primjeni poput bežičnog upravljanja dronovima, kašnjenje u prijenosu podataka može rezultirati lošim kontrolnim odlukama, s potencijalno ozbiljnim posljedicama. Istraživanje Guo et al., (2019) pokazalo je da 5G mreža, s niskom latencijom, omogućava precizno i pouzdano upravljanje bežičnim kontrolnim sustavima.

Niska latencija koju 5G mreža donosi od elementarne je važnosti za IoT aplikacije koje zahtijevaju brzi odziv. Bilo da se radi o industrijskoj automatizaciji ili bežičnim kontrolnim sustavima, brzi prijenos podataka koji 5G omogućava igra ključnu ulogu u uspješnom funkcioniranju tih sustava. Da bi omogućio poboljšanja kao što su povećani kapacitet, brzina i smanjena latencija, 5G koristi niz naprednih tehnika. Jedna od tih tehnika je masivno MIMO (Multiple Input Multiple Output). Kako ističe Ghosh et al., (2016), masivno MIMO omogućava mreži da istovremeno komunicira s velikim brojem uređaja, povećavajući tako kapacitet mreže.

Masivno MIMO koristi veliki broj antena za prijenos i prijam signala, omogućujući mreži da podrži više uređaja odjednom. Ova tehnika može poboljšati učinkovitost mreže i smanjiti interferencije, što rezultira pouzdanih i stabilnih konekcijama, kako to opisuje studija Larsson et al., (2014).

Zrakoplovne komunikacije, s druge strane, koriste usmjerene zrake za prijenos podataka umjesto širenja signala u svim smjerovima. Ova tehnika, kako to ističe Nitsche et al., (2014), omogućava precizniji i efikasniji prijenos podataka, povećavajući brzinu prijenosa i smanjujući latenciju. Ovo je posebno korisno u gusto naseljenim područjima ili u situacijama gdje su potrebne visoke brzine prijenosa podataka.

U svijetu sve veće povezanosti, sigurnost podataka postaje sve važnija. 5G, kao nova generacija mobilnih mreža, uključuje napredne mehanizme sigurnosti kako bi se odgovorilo na ovu rastuću potrebu. Prema Chih-Lin et al., (2014), ovi mehanizmi uključuju poboljšane tehnike enkripcije i autentifikacije, što je od ključne važnosti za zaštitu uređaja u ekosustavu IoT-a.

Enkripcija je proces pretvaranja čitljivih podataka (poznatih kao čisti tekst) u nečitljivi niz znakova (poznatih kao šifrirani tekst) kako bi se osigurala povjerljivost podataka. Prema istraživanju Alrawais et al., (2017), 5G mreže koriste napredne algoritme enkripcije kako bi osigurale da samo ovlašteni korisnici mogu pristupiti podacima koji se prenose preko mreže.

Autentifikacija je još jedan bitan aspekt sigurnosti u IoT-u. Autentifikacija osigurava da je uređaj koji pristupa mreži ili šalje podatke zaista onaj za koga se tvrdi da jest. Kao što to ističe Roman et al., (2011), 5G mreže koriste robustne mehanizme autentifikacije kako bi se smanjila mogućnost lažnog predstavljanja i napada. Sve u svemu, 5G mreže pružaju napredne mehanizme sigurnosti, uključujući poboljšane tehnike enkripcije i autentifikacije. Ove sigurnosne mjere su ključne za zaštitu IoT uređaja i podataka, što pomaže u izgradnji povjerenja u IoT ekosustav.

Evidentno je sukladno iznijetim spoznajama da 5G mreža ima esencijalan značaj u omogućavanju punog potencijala Interneta stvari, nudeći brže brzine, veći kapacitet, smanjenu latenciju, i poboljšanu sigurnost. Bez ovih napredaka, mnoge od obećavajućih IoT aplikacija ne bi bile moguće.

2.5. Umjetna inteligencija u kontekstu Interneta stvari

Umjetna inteligencija (AI) u kontekstu Iot-a smatra se kulminacijskom točkom razvoja tehnologije. Koristići napredne algoritme i računalne modele, AI-a, može prepoznati obrasce, naučiti iz iskustva, predvidjeti trendove i donijeti složene odluke koje daleko nadmašuju kapacitete ljudske analize. Kombinacija ove sofisticirane tehnologije s IoT-om, mrežom uređaja povezanih putem interneta koji komuniciraju i razmjenjuju podatke, otvara brojne mogućnosti za poboljšanje efikasnosti, produktivnosti i kvalitete života. Prema spoznajama autora poput Kai-Fu Leeja, poznatog stručnjaka za umjetnu inteligenciju, AI u IoT kontekstu ima potencijal revolucionirati gotovo svaku industriju. Lee navodi da je jedan od najvažnijih aspekata ove revolucije automatizacija poslova, gdje AI može preuzeti rutinske zadatke, ostavljajući ljude slobodnima za fokusiranje na složenije i kreativnije zadatke (2022).

Na primjer, u poljoprivredi, IoT uređaji opremljeni AI-om mogu sakupljati informacije o temperaturi, vlažnosti i kvaliteti tla, dok AI može analizirati ove podatke i optimizirati uzgoj usjeva, smanjujući troškove i povećavajući produktivnost. U medicini, AI i IoT mogu omogućiti daljinsko praćenje pacijenta i personalizirane tretmane, poboljšavajući ishode liječenja i smanjujući troškove zdravstvene skrbi. Andreas Kaplan, profesor na ESCP Europe, naglašava da kombinacija AI i IoT tehnologija otvara put prema konceptu pametnih gradova. U ovakvom urbanom okruženju, infrastruktura nije samo pasivna, već komunicira sa drugim sustavima kako bi se optimizirala učinkovitost i kvaliteta života (2023).

Prema Kaplanovim istraživanjima, primjena AI-a i IoT-a u gradovima ne odnosi se samo na smanjenje potrošnje energije, već i na optimizaciju prometa. Kroz korištenje senzora, kamere i ostalih IoT uređaja, moguće je prikupiti velike količine podataka o uvjetima na cestama i uzorcima prometa. AI algoritmi mogu zatim analizirati ove podatke, predvidjeti prometne uvjete i sugerirati najučinkovitije rute za smanjenje zagušenja. Osim toga, Kaplan vidi AI i IoT kao ključne tehnologije za poboljšanje kvalitete života u gradovima. Na primjer, pametne zgrade mogu koristiti AI i IoT za optimizaciju potrošnje energije i poboljšanje komfora stanara. IoT uređaji mogu nadzirati različite aspekte zgrade, poput temperature, vlažnosti i osvjetljenja, dok AI može analizirati te podatke, učiti iz njih i automatski prilagoditi postavke kako bi se postigla optimalna učinkovitost i udobnost (2023).

Također, Kaplan ukazuje na mogućnost upotrebe AI-a i IoT-a za bolje upravljanje resursima grada, poput vode i otpada. Primjena ovih tehnologija može dovesti do preciznijeg praćenja

potrošnje resursa, predviđanja potreba i optimizacije procesa, što rezultira smanjenjem rasipanja i povećanjem učinkovitosti.

Iako ova tehnološka kombinacija donosi ogromne mogućnosti, autori poput Nick Bostroma, sa Sveučilišta u Oxfordu, upozoravaju na potencijalne etičke i sigurnosne izazove. Primjerice, privatnost podataka i sigurnost mreže moraju biti glavni prioriteti kako bi se zaštitila osjetljiva informacija i spriječili potencijalni zloupotrebe (2016). Ipak, unatoč ovim izazovima, sve više se priznaje da su AI i IoT ključne tehnologije za budućnost, koje će oblikovati način na koji radimo, živimo i komuniciramo u narednim desetljećima.

Stuart Russell, profesor sa Sveučilišta u Berkeleyu, ističe da je ključno integrirati AI i IoT u različite sektore, poput energetike, transporta, zdravstva i obrazovanja, kako bi se maksimalno iskoristile prednosti koje ove tehnologije pružaju. Prema Russellovim spoznajama, jedno od područja s velikim potencijalom za primjenu AI-a i IoT-a je energetska industrija. Upravljanje energetskim mrežama može se dramatično poboljšati kroz upotrebu AI-a i IoT-a. Na primjer, pametna mjerenja i senzori omogućeni IoT-om mogu pružiti stvarno vrijeme informacija o potrošnji energije, dok AI može analizirati ove podatke i predvidjeti trendove potražnje. Ovo bi omogućilo energetskim tvrtkama da učinkovitije distribuiraju energiju, minimizirajući rasipanje i optimizirajući resurse (2022).

Russell također navodi primjere u transportu, gdje AI i IoT mogu omogućiti inteligentna vozila i infrastrukturu koja bi poboljšala sigurnost, učinkovitost i održivost. U zdravstvu, AI i IoT mogu omogućiti personaliziranu medicinu i praćenje stanja pacijenata u stvarnom vremenu, dok bi u obrazovanju mogli pružiti personalizirano učenje i pomoć u učenju. Russellovo razmišljanje ukazuje na to da je ova kombinacija tehnologija ključna za izgradnju pametnih gradova i održivih društava u budućnosti. Kako se AI i IoT nastavljaju razvijati, mogućnosti za njihovu primjenu samo će rasti, otvarajući nove prilike za inovacije i poboljšanje kvalitete života (2021).

Također, AI i IoT su važni za razvoj autonomnih vozila. Profesor Sebastian Thrun, pionir u ovom području, smatra da će se, uz napredak AI tehnologija i IoT-a, autonomna vozila postati sveprisutna. Ova tehnologija može značajno smanjiti broj prometnih nesreća, povećati učinkovitost transporta i smanjiti emisije stakleničkih plinova. Nadalje, AI i IoT već sada pružaju velike koristi u sektoru zdravstva. Prema Dr. Ericu Topolu, vodećem stručnjaku za

digitalno zdravlje, korištenje AI u kombinaciji s IoT uređajima za praćenje zdravstvenog stanja pacijenata, omogućuje rano otkrivanje zdravstvenih problema i pružanje personalizirane skrbi.

Očekuje se da će ove tehnologije imati snažan utjecaj i na obrazovni sektor. Sugata Mitra, poznati edukacijski inovator, smatra da bi AI i IoT mogli omogućiti personalizirano učenje prilagođeno individualnim potrebama učenika, čime bi se potaknulo dublje razumijevanje i bolje akademske performanse (2022).

Podaci su postali ključni resurs u digitalnom dobu, a IoT uređaji generiraju ogromne količine tih podataka svaki dan. Bez mogućnosti za obradu i analizu tih podataka, njihova vrijednost ostaje neiskorištena. Ovdje ulogu igra umjetna inteligencija, a njen doprinos je dvojak: s jedne strane, AI omogućava obradu podataka u velikim količinama (tzv. big data), a s druge strane, omogućuje njihovu sofisticiranu analizu kroz algoritme strojnog učenja. Tao Jiang, profesor na Sveučilištu u Waterloo, ističe ključnu ulogu AI-a u analizi podataka generiranih kroz IoT. Kroz svoje istraživanje, pokazuje kako AI može prepoznati uzorke u velikim količinama podataka, što je od ključne važnosti za razumijevanje korisničkog ponašanja. Ova sposobnost AI-a može pomoći tvrtkama da bolje razumiju potrebe svojih korisnika i da prilagode svoje proizvode i usluge na temelju tih uvida (2021).

Osim toga, AI može koristiti podatke generirane kroz IoT za optimizaciju procesa. U industriji, na primjer, AI može koristiti podatke s senzora na strojevima da bi predvidio potrebu za održavanjem, optimizirao proizvodne procese ili smanjio potrošnju energije. Još jedan značajan doprinos AI-a u kontekstu IoT-a je mogućnost predviđanja. Korištenjem algoritama strojnog učenja, AI može analizirati prošle podatke i na temelju njih predvidjeti buduće trendove ili događaje. To može biti od velike pomoći u raznim sektorima, od financijskog sektora, gdje AI može predvidjeti tržišne trendove, do zdravstvenog sektora, gdje AI može predvidjeti potencijalne zdravstvene probleme na temelju podataka prikupljenih putem IoT uređaja. Stoga, kako Jiang ističe, kombinacija AI-a i IoT-a predstavlja moćan alat za obradu i analizu podataka, omogućavajući bolje razumijevanje korisničkog ponašanja, optimizaciju procesa i predviđanja koja mogu pridonijeti boljoj odlučivanju. Ovaj napredak ne samo da mijenja način na koji tvrtke i organizacije posluju, već ima potencijal duboko utjecati na cijelo društvo (2021).

Marie-Christine Sawley, stručnjak za superračunala u Intel Labs, naglašava važnost kombinacije AI-a i IoT-a u kontekstu održivosti. Prema njenim riječima, ova tehnologija može pomoći u smanjenju emisija ugljičnog dioksida i optimizaciji korištenja resursa. S IoT

uređajima koji prate i pružaju informacije o potrošnji energije, a AI koja analizira i prepoznaje obrasce, postoji mogućnost za značajno smanjenje ekološkog otiska (2019).

Sherry Turkle, sociologinja sa Massachusetts Institute of Technology (MIT), predviđa značajnu transformaciju u industriji zabave zahvaljujući interakciji AI-a i IoT-a. Prema njenim spoznajama, virtualna stvarnost (VR) i proširena stvarnost (AR) će biti ključne u ovom procesu. Te tehnologije, koje su evoluirale kroz rapidni napredak AI-a i IoT-a, mogu omogućiti potpuno nove načine interakcije, zabave i učenja. Turkle smatra da ove inovacije nude priliku za preispitivanje našeg odnosa prema tehnologiji, kako bi se osigurala humanizirana upotreba i da bi se smanjile potencijalne negativne posljedice. Konkretno, virtualna i proširena stvarnost, koje koriste sofisticirane algoritme AI-a za interakciju s korisnicima na intuitivan način, mogu promijeniti način na koji se ljudi zabavljaju, komuniciraju i uče. Ove tehnologije imaju potencijal promijeniti tradicionalne paradigme zabave, kreirajući potpuno nove iskustvene okruženja i načine interakcije (2020).

Evidentno je da AI i IoT pružaju priliku za dublje, bogatije i personalizirane iskustvo korisnika, otvarajući vrata novim načinima interakcije koje su nekad bile domena znanstvene fantastike. Međutim, kako Turkle upozorava, potrebno je promišljati o etičkim pitanjima i potencijalnim implikacijama koje proizlaze iz šire primjene ovih tehnologija.

2.5.1. Prednosti i nedostaci umjetne inteligencije

Prednosti i nedostaci AI-a potrebno je sagledati kao dva lica iste kovanice. Razumijevanje ove dinamične teme proizlazi iz spoznaja brojnih stručnjaka i autoriteta u području AI-a. Kada je riječ o AI, spoznaje Daniela Kahnemana, istaknutog psihologa i Nobelovca, sugeriraju da AI donosi brojne prednosti u pogledu efikasnosti i produktivnosti. Kahnemanova razmišljanja naglašavaju da umjetna inteligencija može obaviti rutinske i monotone zadatke brže i točnije nego ljudi, što omogućava ljudskim radnicima da se posvete zadacima koji zahtijevaju viši stupanj kreativnosti i intelektualne angažiranosti (2022).

Dodatno, Andrew Ng, suosnivač Coursera-e i istaknuti stručnjak za duboko učenje, naglašava da je AI sposobna obraditi i analizirati ogromne količine podataka koje su danas dostupne. AI, uključujući metode poput strojnog učenja, može otkrivati složene obrasce i trendove u tim podacima, pružajući vrijedne uvide koji mogu potaknuti bolje odlučivanje i strateško planiranje.

Na primjer, AI se može koristiti za analizu potrošačkih podataka i predviđanje tržišnih trendova, čime se tvrtkama omogućuje prilagodba svojih strategija kako bi ostale konkurentne (2019).

Prema Erik Brynjolfssonu, direktoru Inicijative za digitalnu ekonomiju na MIT-u, jedna od najvažnijih prednosti umjetne inteligencije leži u njenoj dosljednosti i preciznosti. Za razliku od ljudi, AI sustavi ne trpe od umora, nepažnje ili promjenjivih raspoloženja. Ova dosljednost omogućava AI sustavima da obavljaju zadatke s konzistentnom preciznošću tijekom dužeg vremenskog perioda (2020).

Nadalje, francuski matematičar i osnivač tvrtke Cerebras Systems, Pierre Baldi, ističe još jednu prednost AI-a u sposobnosti kontinuiranog učenja. Algoritmi strojnog učenja, poput dubokog učenja, sposobni su učiti iz iskustva i poboljšavati svoju performansu tijekom vremena. Ovo ne samo da omogućava AI-u da se prilagodi novim situacijama, već također omogućuje evoluciju AI-a tijekom vremena kako bi se bolje nosio s budućim zadacima i izazovima (2021). No, unatoč ovim prednostima, AI također ima svoje nedostatke. Kao što Wendy Hall, profesorica računalnih znanosti na Sveučilištu u Southamptonu, ukazuje, AI može predstavljati rizik za privatnost i sigurnost podataka. Tehnologija AI-a često se oslanja na masovnu obradu podataka, što otvara mogućnosti zloupotrebe ili neovlaštenog pristupa (2023).

Osim toga, Eliezer Yudkowsky, istraživač na Institutu za budućnost čovječanstva na Sveučilištu u Oxfordu, upozorava na problem etičkih dilema vezanih za AI. Na primjer, AI sustavi mogu donositi odluke koje direktno utječu na ljude, ali ne posjeduju moralnu svijest ili empatiju (2022).

U konačnici, važno je priznati i prednosti i nedostatke AI-a. Tek tada se može donijeti informirana odluka o tome kako najbolje koristiti ovu moćnu tehnologiju.

2.5.2. Etičke smjernice

Prema spoznajama autora kao što je Shannon Vallor, profesorica na Sveučilištu Santa Clara, etičke smjernice u umjetnoj inteligenciji iznimno su važne s obzirom na utjecaj koji AI može imati na individualnu autonomiju i privatnost. Vallor ističe da AI može ograničiti individualnu autonomiju ako su njeni algoritmi dizajnirani da nadmašuju ili manipuliraju ljudskim odlukama. Kako bi se poštovale etičke smjernice, važno je osigurati da AI poštuje prava pojedinaca na samostalno odlučivanje (2022).

Drugi etički izazov kojeg Vallor ističe odnosi se na zaštitu privatnosti. S obzirom na sposobnost AI-a da obrađuje ogromne količine osobnih podataka, postoji rizik od zloupotrebe tih podataka ili njihove upotrebe na načine koji krše privatnost pojedinaca. Etičke smjernice u ovom kontekstu zahtijevaju stroge mjere zaštite podataka i poštovanje prava pojedinaca na zaštitu svoje privatnosti (2022). U svojim radovima, Ryan Calo, profesor prava na Sveučilištu u Washingtonu, posebno naglašava etička pitanja povezana s pristranošću i pravičnošću u umjetnoj inteligenciji. AI algoritmi često se treniraju na temelju povijesnih podataka, a ako ti podaci sadrže pristranosti, AI može nehotice reproducirati te pristranosti u svojim odlukama i preporukama. Calo ističe važnost etičkih smjernica koje se bave ovim pitanjem, uključujući transparentnost u treniranju AI-a i provođenje redovitih revizija kako bi se osiguralo da AI ne perpetuira diskriminaciju (2022).

Prema spoznajama autora poput Kate Crawford, istraživačice na Microsoft Research, etičke smjernice u kontekstu umjetne inteligencije moraju također uključivati element odgovornosti. Crawford navodi da se pridavanje odgovornosti u kontekstu umjetne inteligencije odnosi na pitanje tko je odgovoran kada dođe do pogreške ili štete koju je uzrokovala umjetna inteligencija. Budući da AI može donositi odluke koje izravno utječu na ljudske živote, poput odluka o kreditima, zapošljavanju ili čak vođenju vozila, važno je definirati tko je odgovoran kada dođe do štete. Odgovornost se može odnositi na programere, korisnike, proizvođače ili vlasnike AI sistema, ovisno o kontekstu (2022).

Druga spoznaja koju navodi Roba Kitchin, profesor na Nacionalnom sveučilištu u Irskoj, odnosi se na pravednost u AI-u. AI može pojačati ili reproducirati socijalne pristranosti ako se ne postupa s oprezom. To se može dogoditi ako su podaci na kojima AI uči pristrani, što može dovesti do pristranih izlaznih rezultata. Kitchin naglašava važnost etičkih smjernica koje promiču pravednost i ravnopravnost u razvoju i primjeni AI-a. Te smjernice mogu obuhvatiti upotrebu alata i metoda za prepoznavanje i ispravljanje pristranosti u AI-u te promociju raznolikosti i inkluzivnosti u razvoju AI sistema (2021).

Fei-Fei Li ističe da bi pravednost u kontekstu umjetne inteligencije trebala biti neodvojivi dio dizajna i implementacije AI sistema. Naglašava kako bi razvojni timovi trebali biti svjesni mogućnosti pristranosti u algoritmima i raditi na uklanjanju takvih nepravilnosti. U tom kontekstu, potrebno je obratiti pažnju na setove podataka koji se koriste za treniranje AI sistema, kako bi se osiguralo da ne perpetuiraju diskriminaciju ili nepravdu (2022).

Uz to, pristup koristima AI tehnologije također je važan element pravednosti. Prema spoznajama autora kao što je Ruha Benjamin, profesorica na Sveučilištu Princeton, nužno je da prednosti umjetne inteligencije budu dostupne svim članovima društva, neovisno o njihovom socioekonomskom statusu, rasi, spolu ili dobi. AI bi trebala biti alat koji služi svima, a ne samo privilegiranim skupinama (2021). Na koncu, etičke smjernice u kontekstu AI-a, uključuju niz važnih načela, od transparentnosti i odgovornosti do pravednosti. Kako AI sve više oblikuje naš svijet, nužno je nastaviti razvijati i usvajati ove smjernice kako bi se osiguralo da se AI koristi na način koji je u skladu s našim najvišim etičkim idealima.

Arkina, profesor na Georgia Institute of Technology, smatra se jednim od vodećih stručnjaka u području etike i AI-a. Prema njegovim spoznajama, odgovornost u kontekstu AI-a je iznimno važna. Arkin ističe da bi dizajneri, programeri i operatori AI sistema trebali snositi određeni stupanj odgovornosti za odluke i postupke koje AI poduzima. To se posebno odnosi na situacije kada AI tehnologija ima potencijal da uzrokuje štetu ili ugrozi sigurnost ljudi (2022). Odgovornost se također odnosi na uspostavljanje jasnih mehanizama odgovornosti i nadzora. S obzirom na to da AI tehnologija može donositi odluke koje utječu na ljude i društvo, od ključne je važnosti da postoji regulacija koja nadgleda i provjerava rad AI sistema (2022).

Elon Musk, CEO Tesla Inc., također je izrazio slične stavove o važnosti odgovornosti u kontekstu AI-a. Musk je istaknuo potrebu za pravovremenom regulacijom AI-a, naglašavajući da je ključno utvrditi tko je odgovoran ako AI počini grešku koja rezultira štetom. Osim toga, Musk je naglasio da se pravila i smjernice trebaju postaviti prije nego što AI postane široko rasprostranjena i utječe na veći broj ljudi (2023).

Kombinacija ovih spoznaja naglašava važnost odgovornosti kao ključnog etičkog principa u kontekstu umjetne inteligencije. To uključuje jasno definiranje tko je odgovoran za odluke i radnje koje AI poduzima, kao i uspostavljanje mehanizama za nadzor i regulaciju kako bi se osigurala sigurnost i dobrobit ljudi.

Sve u svemu, etičke smjernice u kontekstu AI-a temelj su za održavanje povjerenja u AI tehnologije i osiguravanje njihove koristi za sve segmente društva.

3. PRAVNI ASPEKTI REGULACIJE INTERNETA STVARI (IoT)

IoT predstavlja ne samo prilike za inovacije i napredak, već i izazove u pogledu zaštite privatnosti, sigurnosti i interoperabilnosti.

U poglavlju 3.1. razmatra se međunarodni pravni okvir regulacije IoT-a, analizirajući kako se različite zemlje i međunarodne organizacije bave ovim izazovima.

U poglavlju 3.2. fokus se prebacuje na pristup EU IoT-u i AI-u . Ovo podpoglavlje dublje se bavi politikama i regulativama koje EU primjenjuje u kontekstu IoT-a i AI-a te kako EU ravnoteži poticanje inovacija s potrebom za zaštitom građana i njihovih prava.

Poglavlje 3.3. pruža detaljan pregled pravno-regulatornog okvira IoT-a u EU. Ovaj dio obuhvaća povijesni pregled regulacije u svijetu, sa posebnim naglaskom na EU regulative kao što su Uredba (EU 2016/679) o zaštiti pojedinaca i Uredba o E-privatnosti. Razmatraju se mogući smjerovi regulacije, preporučeni omjeri i ključna pitanja privatnosti podataka. Također, posebna pažnja posvećuje se vezi između AI-a i zaštite podataka, te kako ovi aspekti utječu na regulativu IoT-a u EU.

Pravni aspekti regulacije IoT-a smatraju se složenim i sveobuhvatnim. Regulacija IoT-a obuhvaća mnoga pravna pitanja, uključujući, ali ne ograničavajući se na, pitanja privatnosti, sigurnosti, autorskih prava i upravljanja podacima. Ryan Calo, poznati stručnjak za pravna pitanja vezana uz tehnologiju, posebno naglašava neophodnost zaštite privatnosti i sigurnosti korisnika u kontekstu IoT-a. Kada su u pitanju privatnost korisnika, Calo predlaže da regulacija mora osigurati zaštitu osobnih podataka koji se prikupljaju putem IoT uređaja. To znači da moraju postojati zakonske smjernice koje sprečavaju neovlašteni pristup, korištenje ili zloupotrebu tih podataka. U vezi s sigurnošću, Calo ističe kako IoT uređaji mogu biti meta cyber napada. Ovi napadi mogu ne samo kompromitirati privatnost korisnika, nego i uzrokovati štetu ukoliko su IoT uređaji povezani s kritičnom infrastrukturom, kao što su energetske mreže ili transportni sustavi. Stoga, zaštita IoT uređaja od takvih napada postaje ključni dio regulative. To bi moglo uključivati obavezne sigurnosne standarde za proizvođače IoT uređaja, kao i smjernice za korisnike o sigurnom korištenju tih uređaja (2023).

Drugi pravni aspekt regulacije IoT-a odnosi se na autorska prava i intelektualno vlasništvo. U kontekstu IoT-a, pitanja autorskih prava i intelektualnog vlasništva dobivaju novu dimenziju. Kao što Peter K. Yu, stručnjak za intelektualno vlasništvo, ističe, IoT uređaji generiraju

ogromne količine podataka, koje mogu uključivati razne vrste intelektualnog vlasništva, poput autorskih prava, patenata, tajnih podataka, ili čak osobnih podataka (2022).

Yu naglašava da je pravni okvir za IoT mora osigurati poštivanje prava intelektualnog vlasništva. To uključuje jasno definiranje tko posjeduje prava na podatke generirane putem IoT uređaja, kao i pravila o tome kako i kada se ti podaci mogu koristiti. Istodobno, Yu ukazuje na potrebu da se zakonodavstvo ne smije pretjerano ograničiti inovacije i kreativnost. Na primjer, trebalo bi omogućiti razmjenu i korištenje podataka kada to ne krši prava intelektualnog vlasništva i kada može poticati razvoj novih tehnologija ili usluga (2022).

Pitanja upravljanja podacima u središtu su IoT regulative, kako Julie E. Cohen, profesorica prava, ističe. IoT uređaji su, prirodom svoje tehnologije, konstantni prikupljači, obraditelji i prenositelji podataka. Ti podaci mogu biti vrlo osjetljivi, posebno ako se odnose na osobne informacije korisnika. Prema Cohen, regulacija bi trebala pružiti jasne smjernice o tome kako se podaci mogu koristiti i dijeliti. To bi moglo uključivati ograničenja na vrste podataka koje IoT uređaji mogu prikupljati, pravila o tome kako se podaci mogu pohraniti i zaštititi, i zahtjeve za dobivanje pristanka korisnika prije obrade ili prijenosa njihovih podataka (2019).

Transparentnost je iznimno bitna u ovom kontekstu. Korisnici bi trebali imati pravo znati koje se informacije o njima prikupljaju, kako se te informacije koriste, i s kime se mogu dijeliti. Regulativa bi, prema Cohen, trebala osigurati mehanizme koji omogućuju korisnicima da ispune ova prava. Ova pravila ne samo da bi osigurala zaštitu korisnika, već bi i povećala povjerenje u IoT tehnologiju, što bi moglo potaknuti njen daljnji razvoj i prihvaćanje.

3.1.Povijesni pregled regulacije u svijetu

Evolucija regulacije IoT-a, kako sugerira Ibarra-Esquer et al. (2017), pokazuje da je put do stvaranja pouzdane i sigurne mreže bio ispunjen brojnim preprekama. Razvoj od prvih pokušaja regulacije do danas ilustrira kako je sazrijevanje IoT-a rezultiralo sve sofisticiranijim pristupima regulaciji, ali i izazovima koji se neprestano mijenjaju i rastu.

Prema Weberu (2016), početak regulacije IoT-a bio je fokusiran na osiguranje funkcionalnosti i interoperabilnosti među uređajima. Tijekom vremena, fokus se postupno pomaknuo prema pitanjima sigurnosti i privatnosti, s obzirom na to da je broj uređaja povezanih na Internet naglo porastao.

Prvi pokušaji regulacije, prema istraživanju Webera (2009), nisu uspjeli u potpunosti adresirati kompleksne izazove IoT ekosustava, poput privatnosti korisnika, sigurnosti podataka i interoperabilnosti uređaja. Iako su se regulative tada usredotočile na definiranje osnovnih standarda, prema Lombardi et al. (2021), oni nisu bili dovoljno sveobuhvatni da bi učinkovito riješili pitanja koja su se pojavila.

Istraživanje Paula Brousa, Marijna Janssena, i Pauliena Herdera (2020) pokazuje kako je u središtu ovih izazova bio brzi razvoj tehnologije, koji je često pretekao mogućnosti regulatornih okvira. Ovo je istaknuto i u studiji Webera (2010) koji navodi da je brzi tehnološki razvoj stvorio pravnu prazninu koja je ostavila korisnike IoT-a ranjivima na niz sigurnosnih prijetnji.

Uslijed ovih izazova, regulacija IoT-a počela se razvijati u složenijim i sveobuhvatnijim smjerovima, prema studiji koju je proveo Tzafestas (2018). Sada se ne samo usmjeravaju na tehničke aspekte IoT-a, već i na pitanja etike, sigurnosti i privatnosti. Ova promjena fokusa prema etičkim pitanjima i privatnosti korisnika istaknuta je u istraživanju Taherdoosa (2023). On navodi da je s obzirom na osobnu prirodu mnogih podataka koje IoT uređaji prikupljaju, zaštita privatnosti korisnika postala ključni aspekt regulacije.

Ali et al. (2022) dodatno naglašavaju kako regulacija mora obuhvatiti i zaštitu podataka te naglašavaju potrebu za razvojem naprednih sigurnosnih okvira. Ovi okviri trebali bi biti u stanju obraditi se s rastućim sigurnosnim prijetnjama koje dolaze s proširenjem i razvojem IoT ekosustava. S obzirom na to da IoT uređaji često prikupljaju i prenose osjetljive podatke, pitanja poput krađe podataka, neovlaštenog pristupa i zloupotrebe podataka postali su presudni problemi koje treba riješiti, što ističu Ali et al. (2022).

Najvažniji dio ove evolucije uključuje razvoj standarda za zaštitu podataka, kako bi se osigurala njihova sigurnost i privatnost. Prema Lombardi et al. (2021), regulative su usmjerene na definiranje protokola i standarda za IoT uređaje, a cilj je osigurati njihovu sigurnu i učinkovitu upotrebu. To uključuje standardizirane protokole za šifriranje podataka, autentifikaciju korisnika i sigurnosne značajke kako bi se spriječila neovlaštena manipulacija IoT uređajima i podacima koje prikupljaju.

Unatoč ovim naporima, postoje brojni izazovi u regulaciji IoT-a. Kao što Taherdoos (2023) ističe, potrebna je sveobuhvatna regulacija koja obuhvaća sve aspekte IoT-a, uključujući sigurnost, privatnost, interoperabilnost i etičke aspekte. Ovo je složen zadatak, jer se mora uzeti

u obzir širok spektar uređaja i tehnologija, kao i različite primjene i kontekste u kojima se IoT koristi.

Daljnje komplikacije nastaju zbog brzog razvoja tehnologije. Kao što Yaqoob et al. (2017) objašnjavaju, novi uređaji, aplikacije i tehnologije neprestano se razvijaju, što znači da se i sigurnosne prijetnje stalno mijenjaju i evoluiraju. To predstavlja stalni izazov za regulaciju IoT-a, jer regulatorni okviri moraju biti dovoljno fleksibilni da se prilagode ovim promjenama, a istovremeno dovoljno robusni da osiguraju zaštitu korisnika i njihovih podataka.

U konačnici, regulacija IoT-a je složen i stalno evoluirajući proces. Istraživanja poput onih koje su proveli Weber (2010), Ali et al. (2022), Lombardi et al. (2021) i Taherdoos (2023) pokazuju da, iako se regulacija IoT-a poboljšava i prilagođava brzo mijenjajućem tehnološkom krajobrazu, još uvijek postoje brojni izazovi koje treba riješiti. Ovi izazovi vjerojatno će i dalje rasti kako se IoT tehnologija i njena primjena nastavljaju širiti i diversificirati. Tehnološki napredak često nadmašuje trenutne regulatorne okvire, ostavljajući praznine u sigurnosti i zaštiti privatnosti koje mogu biti iskorištene. S obzirom na ubrzani rast i evoluciju IoT-a, istraživači i donosioci odluka suočeni su s kontinuiranim izazovom prilagođavanja regulative kako bi ostali u korak s ovim promjenama (Ali et al., 2022).

U svjetlu svega ovoga, jasno je da će IoT ostati na vrhu regulatorne agende u godinama koje dolaze. S obzirom na brzinu kojom tehnologija napreduje, od suštinske je važnosti da regulatorni okviri ne samo da se prilagode sadašnjim potrebama, već da budu dovoljno fleksibilni da se mogu prilagoditi i budućim izazovima i mogućnostima.

Povijest IoT-a pokazuje značajan tehnološki razvoj. Kao što FIA (2021) navodi, IoT koncepti počeli su s osnovnim implementacijama poput pametnih aparata u ranim 1980-im. Dolaskom RFID tehnologije, koja je omogućila bežičnu komunikaciju među uređajima, IoT je doživio pravi procvat (TECHAHEAD, 2022). No, s porastom ove tehnologije, rasla je i potreba za sveobuhvatnom regulacijom koja bi zaštitila korisnike i njihove podatke.

Sve ovo pokazuje da regulacija IoT-a nije samo pitanje tehnološkog razvoja. Ona uključuje i niz socijalnih, etičkih i pravnih pitanja. To znači da se donosioci odluka i regulatori moraju baviti širokim spektrom izazova kako bi osigurali sigurnu i odgovornu upotrebu IoT-a.

Razvoj naprednih IoT tehnologija u posljednjem desetljeću, poput autonomnih automobila, pametnih domova i industrijskog IoT-a, doista je dodao složenost u regulatornu sliku. Khan et

al. (2021) pružaju uvid u ove izazove, naglašavajući kako se IoT tehnologija suočava s brojnim problemima, uključujući sigurnosna pitanja, interoperabilnost i zaštitu privatnosti.

Sigurnosna pitanja vrh su popisa prioriteta, kako navodi Khan et al. (2021). Kako IoT uređaji postaju sve prožimajući, potencijal za sigurnosne propuste raste. Bez odgovarajuće regulative i protokola, ti uređaji mogu postati ranjive točke za cyber napade. Stoga, kako bi se osigurala sigurnost IoT-a, regulatorni okviri moraju uključivati zaštitu podataka i mrežne sigurnosti, što ističu Ali et al. (2022).

Interoperabilnost je drugi veliki izazov u regulaciji IoT-a. Kako IoT uređaji postaju sve složeniji i raznolikiji, postoji potreba za standardima koji omogućuju komunikaciju između različitih uređaja i sustava. Lombardi et al. (2021) naglašavaju važnost uspostavljanja standarda i protokola koji osiguravaju interoperabilnost, što je ključno za učinkovito funkcioniranje IoT ekosustava.

Naposljetku, zaštita privatnosti korisnika je središnje pitanje u regulaciji IoT-a. Kako IoT uređaji prikupljaju sve više osobnih podataka, raste i potreba za zaštitom tih podataka.

Složenost IoT-a proizlazi iz njegove inherentne povezanosti i raznolikosti, što donosi brojne izazove. Povezivanje različitih uređaja različitih proizvođača stvara složene mreže koje zahtijevaju jasne protokole interoperabilnosti. Osim toga, privatnost i sigurnost podataka korisnika moraju biti prioritet. Izazov leži u stvaranju regulacija koje omogućuju fleksibilnost i inovaciju, ali istovremeno štite interese i privatnost korisnika.

S druge strane, Malhotra et al. (2021) dodatno naglašavaju rastuće sigurnosne izazove i brige s rastom IoT ekosustava. Kako se IoT ekosustav nastavlja širiti, tako se povećava i broj potencijalnih prijetnji i sigurnosnih rizika. Postojeći sigurnosni standardi i regulative često se čine nedostatnim u pružanju odgovarajuće zaštite, što zahtijeva daljnji razvoj i prilagodbu u ovom brzorastućem području.

Sveobuhvatna regulacija IoT-a zahtijeva kontinuirano praćenje tehnoloških trendova, kao i prilagodbu pravilima i standardima koji se trenutno koriste. Ovo će omogućiti stvaranje okruženja u kojem IoT može nastaviti rasti i evoluirati, dok se istovremeno osigurava zaštita korisnika i njihovih podataka.

Salih et al. (2022) posebno ističu industrijski IoT (IIoT) kao sektor koji je posebno osjetljiv na izazove regulacije. IoT uključuje upotrebu IoT tehnologija u industrijskom sektoru, uključujući

proizvodnju, poljoprivredu, transport, energetiku i mnoge druge industrije. Kako industrijski sektor postaje sve više digitaliziran i povezan, složenost u pogledu sigurnosti i privatnosti podataka raste.

Kao što su Ali et al. (2022) i Lombardi et al. (2021) naglasili, zaštita podataka i sigurnost su najbitniji aspekti regulacije IoT-a. U kontekstu IIoT-a, ovi izazovi postaju još izraženiji. Ne samo da se podaci prikupljaju na velikom broju uređaja, već se ti podaci često koriste za kritične operacije. Uz to, broj uređaja i aplikacija u IIoT okruženju stalno raste, što samo povećava potencijalne sigurnosne rizike i čini sigurnosne okvire još složenijima.

Prema Salih et al. (2022), ova nova paradigma zahtijeva pažljivo promišljanje o regulativi. Potrebno je razviti nove, proaktivne pristupe regulaciji kako bi se osigurala sigurna i održiva budućnost. To podrazumijeva stvaranje regulacija koje su fleksibilne, ali istovremeno dovoljno snažne da osiguraju zaštitu korisnika i njihovih podataka.

Iako Taherdoos (2023) ukazuje na potrebu za sveobuhvatnom regulacijom koja obuhvaća sve aspekte IoT-a, Malhotra et al. (2021) naglašavaju rastuće sigurnosne izazove i brige s rastom IoT ekosustava. Ovi izazovi postaju još izraženiji u kontekstu industrijskog IoT-a, što zahtijeva stalni razvoj i prilagodbu regulativa.

Ande et al. (2020) donose važan uvid u pristup regulaciji IoT sigurnosti, sugerirajući da regulativne mjere moraju biti jednako dinamične kao i sama tehnologija koju nastoje regulirati. U svijetu gdje IoT tehnologija napreduje brzo i kontinuirano, regulativa se mora prilagoditi kako bi ostala u korak s tom dinamikom. Statički pristup regulaciji neće biti dovoljan u takvom okruženju.

Važnost ove dinamike nije samo u brzini promjena, već i u načinu na koji se sigurnosti pristupa unutar IoT arhitekture. Kako Ande et al. (2020) ističu, sigurnost mora biti integrirana u samu arhitekturu IoT-a, a ne da se dodaje kao naknadna zaštita. Ovo je ključno jer je mnogo učinkovitije spriječiti sigurnosne propuste na početku nego pokušati popraviti štetu nakon što se dogodi.

Ovaj integrirani pristup sigurnosti pomaže u osiguranju da se svi aspekti IoT arhitekture, od hardvera do softvera i mrežne infrastrukture, projektiraju s obzirom na sigurnost. To znači da se sigurnosni rizici mogu prepoznati i riješiti u ranim fazama dizajna i implementacije, što je učinkovitije i smanjuje mogućnost budućih problema.

Ovo se poklapa s mišljenjem Taherdoosa (2023), koji također ističe potrebu za sveobuhvatnom regulacijom koja bi obuhvatila sve aspekte IoT-a. Samo kroz sveobuhvatan pristup može se osigurati da regulacija pruža zaštitu koja je potrebna u brzo rastućem i stalno evoluirajućem IoT ekosustavu.

Webber (2010) se slaže s ovim mišljenjem i dodaje da IoT predstavlja nove izazove za sigurnost i privatnost koji zahtijevaju nove pristupe regulaciji. Posebno upozorava na potrebu za prilagodljivim regulatornim okvirima koji mogu pratiti brzi razvoj tehnologije.

S obzirom na ove izazove, neka istraživanja sugeriraju da bi rješenje moglo ležati u razvijanju globalnih standarda i regulativa za IoT. Ova vrsta globalne regulative mogla bi osigurati dosljednost u pristupu sigurnosti i privatnosti na različitim tržištima.

U konačnici, kako navode Nižetić et al. (2020), cilj regulacije IoT-a trebao bi biti stvaranje okruženja u kojem tehnologija može napredovati na održiv način, uzimajući u obzir sve potencijalne prednosti i izazove. Takvo bi okruženje omogućilo korisnicima da s povjerenjem koriste IoT tehnologije, znajući da su njihova prava i privatnost zaštićeni.

U tom kontekstu, Brous et al. (2020) sugeriraju da regulacija treba biti usmjerena na stvaranje povjerenja u IoT tehnologije, što uključuje transparentnost u pogledu načina na koji se podaci koriste i zaštite.

3.2. Međunarodni pravni okvir regulacije Interneta stvari

Prema spoznajama Laure DeNardis, profesorice i međunarodne stručnjakinje za Internet upravljanje, međunarodni pravni okvir je iznimno bitan za regulaciju IoT-a zbog globalne prirode IoT-a. IoT uređaji su povezani preko interneta, mreže koja ne poznaje geografske granice, što rezultira nizom prekograničnih pravnih i sigurnosnih izazova. DeNardis ističe da međunarodni pravni okvir treba uskladiti različite nacionalne zakone i regulative kako bi se adekvatno rukovalo pitanjima poput zaštite podataka, sigurnosti uređaja i odgovornosti proizvođača (2023).

Još jedna ugledna autorica na ovom polju, Mireille Hildebrandt, profesorica prava i tehnologije na Universiteit Brussel, naglašava da međunarodni pravni okvir također treba uzeti u obzir različite kulturne i socijalne kontekste u kojima se IoT uređaji koriste. Hildebrandt smatra da

bi takav okvir trebao omogućiti fleksibilnost za prilagodbu različitim potrebama i uvjetima, dok istovremeno osigurava poštivanje univerzalnih prava i standarda (2022).

Urs Gasser, priznati stručnjak u polju prava digitalnih tehnologija, naglašava važnost uspostave robustnog međunarodnog pravnog okvira koji može učinkovito rješavati ključna pitanja koja se odnose na IoT. Gasser upozorava na potrebu za snažnim pravnim mjerama za zaštitu privatnosti i podataka. S obzirom na ogromne količine osobnih i osjetljivih podataka koje IoT uređaji generiraju i obraduju, nužno je osigurati da se ti podaci koriste na etičan i pravno reguliran način. To uključuje zaštitu podataka od neovlaštenog pristupa, korištenja ili zloupotrebe. Osim zaštite podataka, Gasser ističe važnost sigurnosti IoT uređaja. Kako bi se smanjila mogućnost cyber napada i zloupotrebe, IoT uređaji moraju biti dizajnirani i održavani s najvišim standardima sigurnosti (2019).

Interoperabilnost između uređaja i mreža također je važna tema u međunarodnom pravnom okviru, prema Gasseru. U svijetu u kojem je sve više i više uređaja povezano, važno je da ti uređaji mogu učinkovito komunicirati i surađivati jedni s drugima. Na kraju, Gasser naglašava potrebu za zaštitom prava intelektualnog vlasništva u kontekstu IoT-a. To uključuje zaštitu autorskih prava na softver i tehnologije koje se koriste u IoT uređajima, kao i zaštitu patenata na inovativne IoT tehnologije (2019).

Michael Geist, ugledni pravni stručnjak specijaliziran za tehnologiju, naglašava ključnu ulogu koju bi međunarodni pravni okvir trebao igrati u regulaciji IoT-a. Geist tvrdi da bi pravni okvir trebao obvezivati proizvođače IoT uređaja na uspostavu minimalnih sigurnosnih standarda. S obzirom na rastuću prijetnju od cyber napada, sigurnost IoT uređaja ne bi trebala biti opcionalna, već bi trebala biti integralni dio dizajna i implementacije tih uređaja.

Osim sigurnosnih standarda, Geist smatra da bi pravni okvir trebao uključivati jasne smjernice o prikupljanju, obradi i pohrani podataka. S obzirom na ogromne količine podataka koje IoT uređaji generiraju, potrebno je osigurati da se ti podaci koriste na odgovoran način, štiteći privatnost korisnika i sprječavajući zloupotrebu podataka (2018). Geist također upozorava na potrebu da se razjasni pitanje odgovornosti u vezi s IoT uređajima. S obzirom na složenost IoT ekosustava, koji uključuje proizvođače uređaja, pružatelje usluga, operatore mreža i korisnike, ključno je odrediti tko je odgovoran u slučaju štete ili problema koji proizlaze iz upotrebe IoT uređaja. Ovo je od posebne važnosti u situacijama koje mogu uključivati štetu na imovini, povrede privatnosti, pa čak i tjelesne povrede (2018).

Jack Goldsmith, ugledni stručnjak za pravo i tehnologiju na Sveučilištu Stanford, ističe složenost uspostave međunarodnog pravnog okvira za regulaciju IoT-a. Goldsmith primjećuje da različite zemlje i regije imaju različite pristupe regulaciji IoT-a, što može otežati uspostavu jedinstvenih međunarodnih standarda. Primjerice, razlike mogu postojati u tome kako različite jurisdikcije tumače i primjenjuju principe zaštite privatnosti, sigurnosti i intelektualnog vlasništva. Ove razlike mogu utjecati na sve od dizajna IoT uređaja do načina na koji se podaci prikupljaju, obrađuju i pohranjuju (2019).

Goldsmith naglašava da je za prevladavanje ovih izazova potrebna suradnja na međunarodnoj razini. Suradnja može uključivati razmjenu informacija, usuglašavanje standarda i praksi te suradnju na razvoju međunarodnih pravila i smjernica. Unatoč izazovima, Goldsmith vjeruje da je potreba za međunarodnim pravnim okvirom za regulaciju IoT-a neupitna. Kako IoT uređaji postaju sve prisutniji u svakodnevnom životu, ključno je da postoji jasna i dosljedna regulativa koja će štititi prava i interese korisnika, promicati sigurnost i podržavati inovacije i razvoj (2019).

3.3. Pristup Europske unije Internetu stvari i umjetnoj inteligenciji

Europska unija (EU) je usredotočena na razvoj regulativnih okvira koji promiču etički i odgovorni razvoj umjetne inteligencije (AI) i Interneta stvari (IoT). Prema radu Prof. Floridija u Sage Journals, EU vidi AI i IoT kao dva snažna alata za poboljšanje ekonomskog rasta i društvenog blagostanja, ali istovremeno priznaje potrebu za regulacijom kako bi se osigurala sigurnost i privatnost građana (2021).

Vincent Muller je istaknuo da EU priznaje da AI i IoT imaju potencijal transformirati društvo na različite načine, ali da su također izvor potencijalnih rizika i izazova, uključujući pitanja privatnosti, sigurnosti, etike i pravde (2022).

Kao što je opisano u Izvještaju o umjetnoj inteligenciji EIT Digital, EU također nastoji osigurati da njezin pristup AI-u i IoT-u potiče održivost, u skladu s njenim ambicijama za zelenu tranziciju. To uključuje fokus na razvoj tehnologija koje smanjuju emisije stakleničkih plinova, poboljšavaju energetsku učinkovitost i pomažu u ostvarivanju ciljeva održivog razvoja (2021).

Ovi napori su u skladu s izvješćem iz Europske strategije za podatke, koja naglašava potrebu za promicanjem digitalnih inovacija koje doprinose općem dobru, istovremeno štiteći prava i slobode građana (2020).

U kontekstu IoT-a, kao što je navedeno na web stranici Digital Strategy EC, EU je posvećena promicanju inovacija u području IoT-a uz osiguranje zaštite potrošača i privatnosti podataka. Jedan od ključnih aspekata ovog pristupa je razvoj sigurnih identiteta IoT uređaja, kako je istaknuto na portalu Intertrust. Ovo osigurava da se podaci mogu sigurno prenositi između uređaja i da se mogu poduzeti mjere za zaštitu uređaja i podataka od neovlaštenih pristupa (2022).

Kada je riječ o AI-u, sudeći prema izvještaju s Brookings TechTank portala, EU je uspostavila regulativni okvir koji je usmjeren na poticanje inovacija u području AI-a, dok istovremeno postavlja jasne standarde za etički i odgovorni razvoj AI tehnologija (2021).

Ovo je u skladu s radom Floridija i Vincenta Mullera, gdje se naglašava da se u EU pristup AI-u i IoT-u gleda kroz prizmu etičkih, pravnih i socijalnih izazova. U skladu s tim, EU je razvila politike i regulative koje se bave tim pitanjima, a koje uključuju transparentnost, poštovanje privatnosti, pravičnost i zaštitu temeljnih prava građana (2021).

Stav EU prema AI-u i IoT-u može se opisati kao holistički, budući da se nastoji sagledati širok spektar pitanja od tehnoloških i ekonomskih do socijalnih i etičkih. Prema spoznajama Orla Lynskeya, profesora na London School of Economics, EU ističe važnost zaštite temeljnih prava i vrijednosti u kontekstu ovih naprednih tehnologija (2021).

Osim toga, EU postavlja snažne standarde za zaštitu djece u kontekstu AI-a i IoT-a. Prema studiji objavljenoj u *Children and Youth Services Review*, EU razmatra mjere kao što su ograničenja za upotrebu AI-a i IoT-a u kontekstu dječje igre i obrazovanja, te postavljanje strogih standarda za sigurnost dječjih IoT uređaja (2023).

Izazovi povezani s sigurnošću IoT uređaja priznati su kao prioritetna područja za EU, prema spoznajama iz članka *Journal of Reliable Intelligent Environments*. Sigurnost uređaja, uključujući aspekte poput zaštite podataka, autentifikacije i kontrole pristupa, predstavlja ključnu komponentu regulative koju EU razvija za IoT (Augusto i Coronato, 2021).

3.3.1. Odnos Europske unije prema umjetnoj inteligenciji

Kao što ističe istraživanje Irene Albarrán Lozano i suradnika, percepcija AI-a među državama članicama EU je uglavnom pozitivna, ali varira (Albarrán Lozano et al., 2021). Ovaj odnos prema AI-u nije jednoliko pozitivan u svim članicama, ali općenito ukazuje na spremnost za prihvaćanje i integraciju AI tehnologija.

No, kako naglašava Robert Veldhuizen (2022), postoji naglašena potreba za ozbiljnijim pristupom AI-u unutar EU. U skladu s njegovom analizom, EU treba prilagoditi svoje regulative kako bi se nosila s brzo rastućim tehnološkim napretkom. To se odnosi ne samo na proaktivno reguliranje novih AI tehnologija, već i na osiguravanje da regulative prate tempo inovacija kako ne bi gušile razvoj.

U kontekstu zdravstva, profesor Glenn Cohen i suradnici (2020) pružaju važan uvid u izazove i implikacije povezane s umjetnom inteligencijom. Oni ističu kako strategija EU vezana uz AI ima veliki utjecaj na digitalno zdravstvo. Ovaj segment ističe ključnu točku o tome kako će strategija EU o AI-u utjecati na široki spektar industrija, uključujući kritične sektore poput zdravstva.

Fontes, Corrigan i Lütge (2023) ističu da je upravljanje AI-om na razini EU doživjelo niz izazova, posebno u pogledu regulativa i etičkih pitanja. Izazovi su nastali uslijed potrebe za brzim donošenjem odluka tijekom pandemije, koje su uključivale korištenje AI-a u svrhu analize i predviđanja širenja virusa, kao i za razvoj strategija za suzbijanje pandemije.

No, unatoč ovim izazovima, EU je pokazala predanost ovom području kroz različite inicijative. Kao što Laux, Wachter i Mittelstadt (2023) ističu, jedan od važnih koraka EU bio je izdanje AI Act, regulative punog naziva *The EU Artificial Intelligence Act*, koja ima za cilj osigurati da AI i druge nove tehnologije budu sigurno i pravedno korištene unutar granica Unije. Ovaj akt predstavlja značajan korak prema stvaranju sveobuhvatnog pravno-regulatornog okvira koji će omogućiti europskim građanima, poduzećima i državama članicama da maksimalno iskoriste potencijal AI-a, ali i da se zaštite od mogućih rizika.

3.3.2. Pravno-regulatorni okvir Interneta stvari u Europskoj uniji

IoT, kao mreža međusobno povezanih digitalnih uređaja sposobna prikupljati, slati i primati podatke, predstavlja veliki potencijal za poboljšanje učinkovitosti, ali sa sobom donosi i brojne izazove, posebno u pogledu privatnosti podataka i sigurnosti.

Rolf H. Weber (2013) bio je među prvim stručnjacima koji su prepoznali značaj ovih izazova i potrebu za stvaranjem sveobuhvatnog pravnog okvira koji će riješiti pitanja vezana uz IoT. Njegov rad daje osnovu za razumijevanje složenosti ovog područja i naglašava potrebu za daljnjim istraživanjima. U kasnijem radu, Barr-Kumarakulasinghe Cheryl, Boon-Kwee Ng Chan i Yuan Wong (2020) pružaju detaljniju analizu pravnog okvira EU za IoT, istražujući kako su se politike i regulative razvijale kako bi odgovorile na promjenjive potrebe i izazove koje donosi IoT.

Posebno se naglašava pitanje privatnosti podataka i sigurnosti IoT-a. Karageorgiou i Petrakis (2020) predstavljaju problematiku ove teme, dok Chiara (2022) dodatno pojačava ovu raspravu kroz prizmu novog EU cybersecurity regulatornog okvira. Ovi radovi zajedno oslikavaju nastojanja EU da uspostavi robusne i učinkovite regulative koje će zaštititi privatnost građana i sigurnost digitalne infrastrukture, dok će omogućiti iskorištavanje prednosti koje IoT donosi.

Sve veći broj gradova širom svijeta teži prema statusu takozvanih pametnih gradova, gdje se digitalne tehnologije, uključujući IoT, koriste za poboljšanje kvalitete života, efikasnosti usluga i održivosti. No, kako navode Boban i Weber (2018), krajnji cilj ne bi trebao biti samo stvaranje pametnih gradova, već njihova transformacija u inteligentne gradove.

Koncept inteligentnog grada podrazumijeva korak dalje od pametnog grada, gdje se IoT, AI i ostale tehnologije ne koriste samo za optimizaciju gradskih usluga, već i za stvaranje gradova koji su u stanju učiti, prilagođavati se i donositi odluke kako bi unaprijedili kvalitetu života svojih stanovnika. Ovo, međutim, donosi i nove izazove u pogledu privatnosti, sigurnosti i upravljanja podacima, te zahtijeva pažljivo razrađen pravno-regulatorni okvir.

Kao što Boban i Weber (2018) naglašavaju, ovaj okvir bi trebao biti u stanju zaštiti prava građana i osigurati sigurnost, dok istovremeno omogućava inovacije i tehnološki napredak. Ovaj pristup, kako autori ističu, nije samo pitanje tehnologije, već i politike, etike, zakonodavstva i upravljanja, što zahtijeva široki i interdisciplinarni pristup. Ovaj rad, zajedno

s ranije citiranim radovima, čini važan doprinos razumijevanju složenosti pravno-regulatornog okvira IoT-a u EU.

IoT svojom nevjerojatnom povezanošću i mogućnošću prikupljanja velike količine podataka, donosi brojne izazove kada je u pitanju vlasništvo nad osobnim podacima. Janeček (2018) ukazuje na te izazove, naglašavajući kako je pitanje vlasništva nad osobnim podacima u kontekstu IoT-a složeno i zahtijeva pažljivo promišljanje. Ovo je posebno istaknuto u kontekstu EU-a, koja je prihvatila snažan pristup zaštiti privatnosti svojih građana.

EU je na ove izazove odgovorila kroz različite regulatorne instrumente i inicijative, poput Opće uredbe o zaštiti podataka (GDPR) i Zakona o umjetnoj inteligenciji (AI Act). GDPR, koji je stupio na snagu 2018. godine, postavio je nove standarde za zaštitu podataka unutar EU-a. Njegova svrha je osigurati da se osobni podaci građana EU-a štite bez obzira na to gdje se ti podaci obrađuju.

U kontekstu IoT-a, ovo je izuzetno važno, s obzirom da su uređaji često povezani preko granica, a podaci mogu lako prelaziti iz jedne jurisdikcije u drugu. Stoga, regulatorni okvir poput GDPR-a igra ključnu ulogu u zaštiti podataka i prava građana.

Međutim, s obzirom na brzi razvoj tehnologije, postoji stalna potreba za prilagodbom i evolucijom ovog regulatornog okvira. Pored GDPR-a, EU je također uvela AI Act, dodatno nastojeći regulirati korištenje tehnologija poput AI-a u različitim sektorima, uključujući i IoT. Ove mjere pokazuju predanost EU-a zaštiti podataka i prava svojih građana dok se istovremeno nastoji potaknuti inovacije i tehnološki razvoj.

AI Act, ili Zakon o umjetnoj inteligenciji, predstavljen 2021. godine, još je jedan važan regulatorni instrument koji je EU usvojila kako bi se nosila s izazovima koje donose napredne tehnologije kao što su AI i ML- strojno učenje. Ovaj zakon odražava predanost EU u uređenju i reguliranju korištenja AI-a na način koji podržava inovacije i ekonomski razvoj, dok istovremeno štiti građane EU-a od potencijalnih rizika i zloupotreba.

AI Act pruža jasnu definiciju i klasifikaciju AI sustava, što je presudno za uspostavljanje efikasnog regulatornog okvira (Laux, Wachter, Mittelstadt, 2023). Preciznim definiranje što se smatra AI sustavom, EU je uspostavila okvir za pravila koja su primjenjiva na različite oblike AI-a, uključujući one koji se koriste u kontekstu IoT-a.

Pored toga, AI Act postavlja pravila za transparentnost, odgovornost i sigurnost AI sustava. Transparentnost je ključna kako bi se osiguralo da korisnici razumiju kako AI sustavi rade i donose odluke, dok odgovornost omogućuje odgovarajuće reakcije kada stvari pođu po zlu. Sigurnost AI sustava je posebno važna s obzirom na njihov potencijal za zloupotrebu ili nezakonito korištenje.

AI Act se, dakle, bavi nizom izazova koji se pojavljuju s rastom i razvojem tehnologija poput AI-a i IoT-a. Kroz ovaj zakon, EU nastoji osigurati da te tehnologije budu sigurne, transparentne i odgovorne, pružajući korisnicima povjerenje u njihovu upotrebu i pomažući u izgradnji povjerenja u digitalno društvo.

Unatoč proaktivnim mjerama koje je Europska unija poduzela, kao što su GDPR i AI Act, brojni izazovi povezani s vlasništvom nad osobnim podacima u kontekstu IoT-a ostaju nerješeni. Jedan od najvećih izazova je sama definicija vlasništva nad podacima.

Tradicionalni koncepti prava vlasništva obično se odnose na fizičke objekte, dok je vlasništvo nad nematerijalnim entitetima, poput podataka, puno manje jasno. Ova pravna neizvjesnost postaje još složenija u svijetu IoT-a, gdje uređaji kontinuirano generiraju, prikupljaju i dijele podatke (Janeček, 2018).

Neki stručnjaci argumentiraju da pojedinci trebaju imati potpuno vlasništvo nad svojim osobnim podacima, što bi im omogućilo da kontroliraju tko može koristiti te podatke i na koji način. Ovo gledište potiče na veću odgovornost i poštovanje privatnosti pojedinca (Janeček, 2018).

S druge strane, neki vjeruju da bi podaci trebali biti percipirani kao zajedničko dobro. Ova perspektiva potiče ideju dijeljenja podataka za opće dobro, a podupire je ideja da široko dostupni podaci mogu potaknuti inovacije i društveni napredak. Međutim, ovaj pristup stvara napetost s pravom pojedinca na privatnost i potrebom za zaštitom osjetljivih podataka (Barr-Kumarakulasinghe, Ng Chan, i Wong, 2020).

Dakle, EU je suočena s izazovom izbalansiranja ove dvije perspektive kako bi uspostavila pravno-regulatorni okvir koji će osigurati zaštitu privatnosti, poticati inovacije i omogućiti ekonomski razvoj u digitalnom društvu. Ova se pitanja i dalje aktivno istražuju i debatiraju, a kako IoT nastavlja evoluirati, tako će i zakoni i regulative morati nastaviti pratiti taj napredak.

Drugi značajan izazov s kojim se EU suočava u kontekstu IoT-a jest usklađenost sa GDPR-om i AI Act-om. IoT uređaji neprekidno prikupljaju velike količine podataka, uključujući i one koji mogu biti osobne prirode. Ova praksa postavlja brojna pitanja o načinima na koje se ti podaci mogu prikupljati, obrađivati i koristiti, a da se pritom poštuju regulative.

Prema GDPR-u, subjekti koji obrađuju osobne podatke moraju se pridržavati načela minimalnosti podataka i svrhovitosti. To znači da bi se trebale prikupljati samo one vrste podataka koje su neophodne za ostvarivanje određene svrhe i ništa više (Weber, 2013). Međutim, u IoT okruženju, gdje su uređaji programirani da prikupljaju što je moguće više podataka, često nije jasno koje su sve informacije nužne, što otežava pridržavanje ovih načela (Barr-Kumarakulasinghe, Ng Chan i Wong, 2020).

S druge strane, AI Act stavlja dodatni naglasak na transparentnost i odgovornost AI sustava, uključujući one koji se koriste u IoT uređajima. On zahtijeva od proizvođača AI tehnologije da osiguraju jasnoću u pogledu toga kako se podaci koriste i kako se donose odluke na temelju tih podataka. Ova potreba za transparentnošću može biti izazovna u IoT okruženjima, gdje su procesi obrade podataka često složeni i nejasni za korisnike (Laux, Wachter i Mittelstadt, 2023).

Upravo ova složenost u pogledu pristupa i obrade podataka čini pitanje usklađenosti s GDPR-om i AI Act-om u kontekstu IoT-a izuzetno složenim. To zahtijeva kontinuirano prilagođavanje i razvijanje novih tehničkih i pravnih rješenja kako bi se postigla usklađenost, ali i kako bi se zaštitila prava pojedinaca u svijetu sve prisutnijeg IoT-a (Janeček, 2018; Karageorgiou i Petrakis, 2020).

Naposljetku, tu je i pitanje sigurnosti. IoT uređaji su često ranjivi na sigurnosne prijetnje, što može dovesti do kompromitacije osobnih podataka. Regulatori se moraju boriti s ovim izazovom kroz stroge sigurnosne standarde i regulacije.

EU nastavlja raditi na rješavanju ovih izazova kroz daljnje regulative i inicijative, prilagođavajući se dinamičkom i brzo mijenjajućem se pejzažu tehnologije.

3.4. Mogući smjerovi regulacije Interneta stvari

Svijet koji postaje sve povezaniji otvara vrata za brojne inovacije i prilike, a IoT predstavlja ključnu komponentu te transformacije. IoT, prema Wong, Tan i Lee (2022), predstavlja revoluciju u načinu na koji ljudi, uređaji i sustavi komuniciraju i dijele informacije. No, kako se ističe, s tom revolucijom dolaze i značajni izazovi - pitanja sigurnosti, privatnosti i regulative, koje je potrebno učinkovito adresirati kako bi se osigurao siguran i održiv ekosistem IoT-a.

D'Adamo, Di Vaio, Formiconi i Soldano (2022) upozoravaju na potrebu za snažnijim pravnim okvirima koji bi regulirali upotrebu i implementaciju IoT-a. Prema njihovom mišljenju, pravna pitanja kao što su vlasništvo nad podacima, odgovornost za sigurnosne propuste i zaštita privatnosti korisnika su ključni izazovi koje treba riješiti. Bez odgovarajućih regulativa, moguće je da će se stvarati praznine koje mogu biti iskorištene na štetu korisnika ili šireg društva.

Osim toga, Taherdoost (2023) naglašava kako regulatorni okviri trebaju biti fleksibilni i sposobni prilagoditi se brzo promjenjivom tehnološkom pejzažu. S obzirom na brzi razvoj IoT tehnologija, pravila koja su bila primjenjiva danas mogla bi biti zastarjela sutra. Iz tog razloga, zahtijeva se stalno osvježavanje i revidiranje pravila kako bi se osiguralo da ona učinkovito štite interese korisnika i društva.

Na drugoj strani, Song, Tu i Qin (2022) predlažu inovativna tehnička rješenja za poboljšanje sigurnosti i regulacije IoT-a. Oni se zalažu za korištenje tehnologija poput blockchaina, koje mogu pružiti transparentan i decentraliziran način upravljanja IoT uređajima i podacima.

Beyer i Su (2023) izvješćuju o konkretnim regulatornim inicijativama na razini država, poput *IoT Cybersecurity Improvement Act 2020* u SAD-u, dok se u Europskoj uniji provodi Uredba o kibernetičkoj sigurnosti (EU) 2019/881. S obzirom na izazove i potencijale koje donosi IoT, Obaidat, Obeidat, Holst, Al Hayajneh i Brown (2020) ističu važnost postizanja pravog omjera regulacije.

Prema podacima Europske agencije za mrežnu i informacijsku sigurnost (ENISA), kao i iz drugih relevantnih izvora poput studije *European IoT Use in Homes* (2023), regulacija IoT-a može se razviti u nekoliko potencijalnih smjerova. Ovaj razvoj uključuje niz mjera kao što su sigurnosne smjernice, standardi i propisi, koji bi obuhvaćali cijeli lanac opskrbe IoT-a, od

proizvodnje uređaja do krajnjeg korisnika. Zaštita privatnosti jedan je od bitnih aspekata regulacije IoT-a. Prema Marasoviću, Bugarinoviću i Jovanoviću (2023), adekvatna regulacija IoT-a trebala bi osigurati da su osobni podaci korisnika zaštićeni, da korisnici imaju kontrolu nad svojim podacima, te da su upotreba i prikupljanje podataka transparentni. Ova bi regulacija također trebala odrediti tko je odgovoran u slučaju povrede podataka.

Sigurnosni standardi i smjernice također su važna komponenta regulative. Kako navode Xu, He i Li (2023), stvaranje robusnih sigurnosnih standarda za IoT uređaje može pomoći u osiguranju da su ovi uređaji otporni na sigurnosne prijetnje. Ovi bi standardi trebali biti u skladu s postojećim tehnološkim mogućnostima i trebali bi se redovito ažurirati kako bi odražavali najnovija tehnička dostignuća i prijetnje. Osim toga, postoji potreba za regulativom koja obuhvaća cijeli lanac opskrbe IoT-a. Prema Georgakopoulosu i Jayaramanu (2022), ovo bi uključivalo sve, od proizvođača IoT uređaja, preko pružatelja usluga, do krajnjih korisnika. Regulativa bi trebala osigurati da svaki čimbenik u lancu opskrbe poštuje određene sigurnosne i etičke standarde.

Ukupno gledano, izazov je stvoriti sveobuhvatnu regulativu koja će učinkovito adresirati brojne aspekte povezane s IoT-om, od privatnosti i sigurnosti, preko etičkih pitanja, do pitanja vlasništva nad podacima i odgovornosti. Kako ističu Greenfield i Smith (2023), važno je da se regulativa razvija u korak s tehnološkim napretkom, kako bi se osiguralo da je IoT ekosistem siguran i povoljan za sve korisnike.

Sigurnost opskrbnog lanca predstavlja esencijalan aspekt regulative IoT tehnologija. Prema smjernicama ENISE, mjere zaštite potrebne su tijekom cijelog procesa proizvodnje i distribucije IoT uređaja kako bi se osigurala njihova otpornost na potencijalne sigurnosne prijetnje. Kako sugerira ENISA (2022), zaštita opskrbnog lanca mora početi već u fazi dizajniranja uređaja. Proizvođači bi trebali implementirati sigurnosne mehanizme tijekom ove faze kako bi se osiguralo da uređaji nisu ranjivi na potencijalne napade. To može uključivati korištenje sigurnosnih protokola i enkripcije u svim komunikacijskim kanalima uređaja.

Tijekom proizvodnje, kako navode Xu, He i Li (2023), potrebno je provesti strogu kontrolu kvalitete i sigurnosne provjere kako bi se osiguralo da uređaji nisu kompromitirani. To može uključivati testiranje uređaja protiv različitih vrsta napada i provjeru da su svi sigurnosni mehanizmi ispravno implementirani. Distribucija IoT uređaja također predstavlja potencijalne sigurnosne izazove. Prema Georgakopoulosu i Jayaramanu (2022), potrebno je osigurati

sigurnu isporuku uređaja do krajnjih korisnika, s mjerama zaštite kako bi se spriječilo neautorizirano manipuliranje uređajima tijekom transporta. Naposljetku, kao što Marasović, Bugarinović i Jovanović (2023) ističu, zaštita opskrbnog lanca ne završava kada uređaj dođe do krajnjeg korisnika. Uređaji bi trebali biti dizajnirani na način da omogućavaju redovita sigurnosna ažuriranja kako bi ostali sigurni tijekom cijelog svog životnog vijeka.

Dakle, učinkovita zaštita opskrbnog lanca zahtijeva sveobuhvatni pristup koji se proteže kroz cijeli životni ciklus IoT uređaja, od dizajna i proizvodnje, preko distribucije, sve do krajnjeg korisnika. Privatnost predstavlja još jedan važan aspekt regulative IoT-a, naročito s obzirom na to da IoT uređaji često prikupljaju i obrađuju velike količine osobnih podataka. Rad *Designing privacy-aware internet of things applications* (2022) naglašava nužnost integracije zaštite privatnosti od samog početka dizajna IoT sustava, pristup koji je poznat kao *Privacy by Design*. *Privacy by Design* koncept, kako ističu Rajivan, Camp i McGill (2022), odnosi se na uključivanje mjera zaštite privatnosti u početnoj fazi razvoja proizvoda ili sustava. U kontekstu IoT-a, to može značiti korištenje pseudonimizacije ili anonimizacije podataka, ograničavanje prikupljanja podataka samo na ono što je neophodno za funkcionalnost uređaja, i osiguranje da su podaci adekvatno zaštićeni tijekom prijenosa i pohrane.

S obzirom na to da IoT uređaji često funkcioniraju u mreži s drugim uređajima i sustavima, pitanja o prenosivosti i interoperabilnosti podataka također su bitna. Morabito (2022) naglašava važnost razvijanja standarda koji omogućavaju siguran i efikasan prijenos podataka između različitih uređaja i platformi, uz poštivanje prava na privatnost. Kao što Miorandi, Sicari i Pellegrini (2023) sugeriraju, regulacija IoT-a također bi trebala obuhvatiti i pitanja pristupa i kontrole podataka. Korisnici bi trebali biti u mogućnosti kontrolirati koji podaci se prikupljaju, kako se koriste, i s kim se mogu dijeliti. Ukupno gledano, zaštita privatnosti u IoT-u zahtijeva sveobuhvatni pristup koji počinje integracijom mjera zaštite privatnosti u samoj fazi dizajna, ali se također bavi pitanjima prikupljanja, prijenosa, pohrane i kontrole podataka.

Regulacija IoT-a podrazumijeva i implementaciju efikasnih strategija za adresiranje potencijalnih prijetnji i ranjivosti, kako je istaknuto u radu *A Comprehensive and Systematic Survey on the Internet of Things* (Sharma et al., 2023). Regulatorni okviri trebali bi biti usmjereni na minimiziranje ovih rizika i osiguravanje robustnih mjera zaštite za IoT sustave. Prema Sharma i suradnicima (2023), potencijalne prijetnje i ranjivosti mogu se javiti u različitim dijelovima IoT infrastrukture, uključujući uređaje, mreže i cloud servise. Ove ranjivosti mogu biti iskorištene od strane napadača kako bi se narušila sigurnost IoT sustava,

što može dovesti do ozbiljnih posljedica, uključujući gubitak privatnosti, financijsku štetu ili čak fizičku štetu u slučaju uređaja koji kontroliraju fizičke sustave.

U tom kontekstu, regulatorni okviri trebali bi se usmjeriti na razvoj standarda i smjernica koje će osigurati visoku razinu sigurnosti kroz cijeli opskrbni lanac IoT-a, od proizvodnje i implementacije uređaja do njihovog korištenja i održavanja. To bi moglo uključivati zahtjeve za sigurnosne značajke kao što su enkripcija, autentifikacija i kontrola pristupa, kao i smjernice za sigurnu konfiguraciju i upravljanje uređajima.

Osim toga, kako ističu Chiang i Zhang (2023), važno je i osigurati postojanje efikasnih mehanizama za detekciju i reagiranje na sigurnosne incidente. To bi moglo uključivati razvoj alata za kontinuirano praćenje sigurnosnog stanja IoT sustava, kao i postupaka za brzo i efikasno reagiranje na identificirane prijetnje ili incidente. Ukupno gledano, efikasna regulacija IoT-a zahtijeva holistički pristup koji obuhvaća različite aspekte sigurnosti, od prevencije i zaštite do detekcije i odgovora na incidente.

Važno je istaknuti i to da preporučeni omjer regulacije može varirati ovisno o kontekstu i specifičnoj primjeni IoT-a. Kao što rad *Resource-Efficient Parallelized Random Access for Reliable Connection Establishment in Cellular IoT Networks* (Lee et al.., 2021) ističe, za neke aplikacije, poput onih u telekomunikacijskim mrežama, može biti potrebno više regulative kako bi se osigurao pouzdan i stabilan rad sustava. U kontekstu telekomunikacijskih mreža, pouzdanost i stabilnost iznimno su bitni za ispravno funkcioniranje sustava. Kako bi se osigurao ovaj nivo pouzdanosti, Lee i suradnici (2021) sugeriraju da se regulatorni okvir treba usmjeriti na optimizaciju upravljanja resursima i pristupom mreži. To bi moglo uključivati razvoj standarda i smjernica za upravljanje mrežnim resursima, uključujući tehnikama za učinkovit paralelizirani pristup kako bi se poboljšala pouzdanost povezivanja. Osim toga, autori ističu da regulacija može imati bitan značaj u postizanju ravnoteže između učinkovitosti resursa i pouzdanosti sustava. To bi moglo uključivati uspostavljanje pravila za pravičnu raspodjelu resursa između različitih korisnika i aplikacija, kao i mehanizme za kontrolu opterećenja mreže kako bi se izbjegle situacije preopterećenja koje bi mogle narušiti pouzdanost sustava.

Regulacija IoT-a također može biti učinkovita u pružanju odgovarajućih pravnih okvira za suočavanje s etičkim pitanjima koja proizlaze iz primjene IoT-a D'Adamo, Di Vaio, Formiconi i Soldano (2022) u svojem radu naglašavaju složenost pravnih pitanja koja proizlaze iz primjene Internet of Things (IoT) tehnologija. Posebno se bave pitanjima poput vlasništva nad podacima,

odgovornosti za sigurnosne propuste, kao i zaštitom privatnosti korisnika. Pitanje vlasništva nad podacima posebno je složeno u kontekstu IoT-a, s obzirom na to da podaci često teku kroz različite uređaje, sustave i platforme. D'Adamo i suradnici (2022) ističu da su tradicionalni pravni okviri često neadekvatni za rješavanje ovih pitanja, budući da oni pretpostavljaju jasno definirane granice vlasništva koje su u svijetu IoT-a često zamagljene. Isto tako, autori navode da pitanje odgovornosti za sigurnosne propuste također predstavlja veliki izazov. U slučaju sigurnosnog incidenta, nije uvijek jasno tko bi trebao biti odgovoran - proizvođač IoT uređaja, pružatelj usluga, krajnji korisnik, ili neka druga strana. Prema mišljenju autora, potrebno je razviti nove pravne i regulativne okvire koji će se adekvatno baviti ovim pitanjima, uzimajući u obzir složenu i dinamičnu prirodu IoT ekosustava.

Što se tiče zaštite privatnosti korisnika, D'Adamo i suradnici (2022) naglašavaju da IoT uređaji često prikupljaju i obrađuju osjetljive osobne podatke, što postavlja ozbiljna pitanja o privatnosti. U tom smislu, autori sugeriraju da bi regulatorni okviri trebali sadržavati jasne smjernice i pravila o prikupljanju, obradi i pohrani osobnih podataka u kontekstu IoT-a.

U svojem radu iz 2023. godine, Taherdoost ističe da regulativa povezana s IoT-om mora biti fleksibilna i adaptirana brzom razvoju tehnologije. IoT ekosustav je dinamičan, stalno se mijenja i evoluira, stoga se mora postaviti regulatorni okvir koji je u mogućnosti pratiti te promjene (Taherdoost, 2023). Taherdoost (2023) tvrdi da tradicionalni pristupi regulaciji možda neće biti dovoljni, budući da su često rigidni i nisu prilagođeni brzoj evoluciji tehnoloških trendova. Naprotiv, potrebni su agilni i dinamični regulatorni okviri koji mogu reagirati na nove izazove, kao što su novi oblici sigurnosnih prijetnji, problemi s privatnošću ili etička pitanja koja se pojavljuju kako tehnologija napreduje. Na primjer, IoT uređaji sve više ulaze u privatne domove i postaju integralni dio svakodnevnog života. Ova integracija dovodi do novih izazova kada je u pitanju zaštita privatnosti korisnika i sigurnosti podataka. Stoga Taherdoost (2023) sugerira da bi regulatorni okviri trebali anticipirati i adresirati ove nove izazove, kako bi se održala zaštita korisnika i povjerenje u IoT tehnologije. Osim toga, Taherdoost (2023) naglašava da bi regulacija IoT-a trebala uzeti u obzir i potencijale koje ova tehnologija donosi. U tom smislu, regulativa ne bi smjela biti prepreka inovacijama, već bi trebala omogućiti sigurno i učinkovito korištenje IoT-a, potičući istovremeno napredak i inovacije.

Song, Tu i Qin (2022) donose zanimljivu perspektivu na problematiku regulacije Internet of Things (IoT) okruženja, naglašavajući ulogu naprednih tehnologija poput blockchaina. U

njihovom konceptualnom pristupu, blockchain tehnologija se koristi za stvaranje transparentnog, decentraliziranog sustava za kontrolu pristupa i regulaciju ponašanja u IoT okruženju. Razlog zašto blockchain može biti posebno koristan u ovom kontekstu leži u njegovim inherentnim karakteristikama. Kao distribuirana baza podataka, blockchain omogućuje transparentno praćenje svih transakcija (u ovom kontekstu, interakcija s IoT uređajima) koje su javno dostupne i nemoguće promijeniti nakon što su zabilježene (Song, Tu i Qin, 2022).

Blockchain može pružiti učinkovit i siguran način za autentifikaciju IoT uređaja i korisnika, omogućavajući decentralizirani pristup kontroliranju i reguliranju IoT okruženja. Song, Tu i Qin (2022) predlažu korištenje takvog blockchain temeljenog sustava za kontrolu pristupa kako bi se smanjila mogućnost neovlaštenog pristupa ili manipulacije IoT uređajima. Osim toga, blockchain može poboljšati privatnost i sigurnost podataka u IoT okruženju. Budući da svaka transakcija (ili interakcija s IoT uređajem) mora biti potvrđena od strane mreže prije nego što se zabilježi u blockchainu, ovaj proces dodatno otežava neovlaštene aktivnosti i napade na podatke (Song, Tu i Qin, 2022). Također, ova tehnologija može olakšati regulaciju ponašanja IoT uređaja, omogućujući učinkovito praćenje i provjeru usklađenosti s utvrđenim pravilima i standardima. Na primjer, ako IoT uređaj djeluje izvan utvrđenih parametara, njegovo ponašanje može se lako identificirati i provjeriti putem blockchaina, što olakšava brzo i učinkovito rješavanje problema (Song, Tu i Qin, 2022). Ipak, primjena blockchaina u regulaciji IoT-a nosi i određene izazove, poput pitanja skalabilnosti, energetske učinkovitosti i interoperabilnosti s postojećim sustavima. Unatoč ovim izazovima, Song, Tu i Qin (2022) smatraju da blockchain nudi obećavajuće mogućnosti za unaprjeđenje sigurnosti, privatnosti i regulacije IoT okruženja.

U svom izvješću *U.S. Federal and State Regulation of Internet of Things (IoT) Devices*, Beyer i Su (2023) opisuju odredbe IoT Cybersecurity Improvement Acta 2020. koje je usvojila američka vlada. Ovaj zakon se usredotočuje na uspostavljanje minimalnih sigurnosnih standarda za IoT uređaje koje koristi američka vlada. Pod odredbama ovog zakona, američka vlada nije ovlaštena kupovati ili koristiti IoT uređaje koji ne ispunjavaju određene sigurnosne standarde. Ovi standardi, između ostalog, zahtijevaju da uređaji mogu biti sigurno ažurirani, da ne sadrže poznate sigurnosne propuste i da koriste sigurne metode za autentifikaciju i komunikaciju. Izuzetno, ovaj zakon predstavlja važan korak prema poboljšanju sigurnosti IoT-a na nacionalnoj razini (Beyer i Su, 2023).

S druge strane Atlantika, britanska vlada je također poduzela mjere za regulaciju IoT-a. Godine 2021., uvela je Zakon o sigurnosti proizvoda i povezanih sistema (Product Security and Telecommunications Infrastructure Bill), koji ima za cilj osigurati da su svi proizvodi na britanskom tržištu, uključujući IoT uređaje, sigurni za uporabu. Zakon propisuje obvezne sigurnosne zahtjeve za pametne uređaje, uključujući IoT uređaje, kao što su zahtjevi za jedinstvene lozinke za svaki uređaj i pružanje transparentnih informacija o minimalnom vremenskom razdoblju tijekom kojeg će proizvod primati sigurnosna ažuriranja. Ove mjere su dizajnirane da smanje rizik od napada na IoT uređaje i da poboljšaju sigurnost korisnika. Ovim zakonom, Britanska vlada namjerava stvoriti okruženje u kojem će potrošači moći imati puno povjerenje u sigurnost proizvoda koje kupuju (UK Government, 2021).

Ove inicijative na globalnoj razini pokazuju rastuću svijest o potrebi za učinkovitom regulacijom IoT-a. Kako se tehnologija nastavlja razvijati, očekuje se da će se i regulativni okviri nastaviti prilagođavati kako bi se osigurala zaštita korisnika i održivost IoT ekosustava.

U EU-i su donesene određene regulative vezane za Internet of Things (IoT). Posebno se ističe Uredba o kibernetičkoj sigurnosti (EU) 2019/881, koja predstavlja značajan korak prema jačanju sigurnosti IoT-a na razini EU. Uredba o kibernetičkoj sigurnosti, kako je opisano u službenom sažetku Uredbe (European Union, 2019), uspostavlja europski okvir za certifikaciju proizvoda i usluga za kibernetičku sigurnost. Ova Uredba ima za cilj standardizirati sigurnosne mjere koje se primjenjuju na proizvode i usluge uključujući IoT uređaje. Svrha je omogućiti visoki, jednaki nivo kibernetičke sigurnosti širom EU i olakšati slobodan protok takvih proizvoda i usluga unutar Unije. Uredba također predviđa uspostavljanje EU Agencije za kibernetičku sigurnost (ENISA), koja je zadužena za pripremu shema certifikacije za proizvode i usluge kibernetičke sigurnosti. Ove sheme certifikacije igraju ključnu ulogu u osiguranju da IoT uređaji koji se prodaju unutar EU ispunjavaju određene sigurnosne standarde. Pored toga, Uredba predviđa mehanizme za suradnju između država članica u pogledu kibernetičke sigurnosti. Ova suradnja uključuje razmjenu informacija o prijetnjama i ranjivostima, kao i koordinaciju odgovora na velike kibernetičke incidente. Uredba o kibernetičkoj sigurnosti predstavlja značajan korak prema uspostavi sveobuhvatnog i koordiniranog pristupa kibernetičkoj sigurnosti na razini EU. S obzirom na brzi razvoj i širenje IoT tehnologija, očekuje se da će ovaj okvir imati ključnu ulogu u zaštiti europskih građana i poduzeća od kibernetičkih prijetnji.

U izgradnji regulativnog okvira za IoT, postoji nužna potreba za uravnoteženim pristupom. U radu *Securing the Internet of Things (IoT): A Security Taxonomy and Survey* autori Obaidat, Obeidat, Holst, Al Hayajneh i Brown (2020) ističu važnost postizanja pravilnog omjera regulacije. Prekomjerna regulacija, kako autori naglašavaju, može biti kontraproduktivna, jer može ometati inovacije i rast IoT industrije. Striktna regulacija može stvoriti prepreke za ulazak na tržište, ograničiti konkurenciju, usporiti razvoj novih proizvoda i usluga, i na taj način usporiti ukupni napredak industrije. S druge strane, nedostatak regulacije može dovesti do sigurnosnih rizika i kršenja privatnosti. Ako se IoT uređaji ne reguliraju dovoljno, mogu postati lakim metama za hakerske napade, što može dovesti do kompromitacije osobnih podataka, krađe identiteta, neautoriziranog pristupa do informacija i drugih sigurnosnih prijetnji. Iz ove perspektive, autori sugeriraju da je neophodno pronaći ravnotežu koja omogućuje održiv i siguran razvoj IoT-a. Uređaji i sustavi IoT-a trebali bi biti adekvatno regulirani kako bi se osigurala njihova sigurnost i zaštita privatnosti, ali ta regulacija ne bi smjela biti tako stroga da ometa inovacije i rast industrije. Ovo je izazov koji regulatori širom svijeta trenutno pokušavaju riješiti kako bi se omogućio napredak IoT-a, ali i osigurala zaštita korisnika (Obaidat et sl., 2020).

3.5. Opća uredba o zaštiti podataka (GDPR) u svijetu Interneta stvari i umjetne inteligencije

U kontekstu IoT-a i AI-a, regulacija zaštite podataka postaje iznimno važna, s obzirom na velike količine osobnih podataka koji se koriste i obrađuju. Uredba (EU) 2016/679, poznatija kao Opća uredba o zaštiti podataka (GDPR), postavlja značajne standarde u pogledu zaštite podataka u Europskoj uniji. Paolone, Iachetti, Paesani, Pilotti, Marinelli i Di Felice (2022) ističu kako se IoT često koristi za prikupljanje velikih količina podataka iz različitih izvora, uključujući osobne podatke korisnika. To postavlja brojne izazove u pogledu zaštite podataka, posebno s obzirom na širok spektar uređaja, aplikacija i usluga koje su uključene u IoT ekosustav. GDPR propisuje da obrada osobnih podataka mora biti zakonita, pravična i transparentna, što postavlja važne standarde za IoT operatore. S druge strane, Hölbl, Kežmah i Kompara (2021) navode kako GDPR utječe na praksu obrade podataka u AI-u. Oni ističu kako su, prema GDPR-u, subjekti podataka obdareni različitim pravima, uključujući pravo na pristup, ispravak, brisanje (*pravo na zaborav*) i pravo na ograničenje obrade. To znači da AI

sustavi moraju biti dizajnirani tako da poštuju ova prava, što može zahtijevati znatne tehničke i operativne prilagodbe.

Georgiou i Lambrinoudakis (2020) navode kako GDPR ima poseban utjecaj na zdravstvene sustave, posebno one koji koriste cloud tehnologiju. Oni ističu kako GDPR zahtijeva posebne mjere zaštite za osobne podatke vezane za zdravlje, što uključuje strogu kontrolu pristupa i korištenje naprednih tehnika šifriranja. To može biti posebno relevantno u kontekstu AI-a i IoT rješenja u zdravstvu, koja često koriste cloud tehnologije za obradu podataka.

GDPR evidentno ima velik značaj u postavljanju standarda za zaštitu podataka u svijetu IoT-a i AI-a. Bez obzira na izazove u njegovoj primjeni, važno je da se pravila i norme koje on postavlja striktno prate kako bi se osigurala zaštita osobnih podataka korisnika.

Ekosustav IoT-a predstavlja globalnu mrežu uređaja povezanih putem interneta, od kućanskih aparata do industrijskih strojeva. Ovi uređaji generiraju i prenose velike količine podataka, često uključujući osjetljive informacije, što ističu Paolone, Iachetti, Paesani, Pilotti, Marinelli i Di Felice (2022). Stoga, potreba za odgovarajućim mjerama zaštite podataka u ovom kontekstu postaje neophodna kako bi se izbjegli rizici nesankcioniranog pristupa ili zlouporabe ovih informacija.

U skladu s GDPR-om, Hölbl, Kežmah i Kompara (2021) navode da obrada podataka mora biti transparentna, ograničena na specifične svrhe, minimalna i točna. Također se mora provesti na način koji osigurava odgovarajuću sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade, gubitka, uništenja ili oštećenja. Također, ističu da subjekti podataka moraju biti informirani o obradi i imati pravo pristupa svojim podacima. Diamantopoulou, Androutsopoulou, Gritzalis i Charalabidis (2020) ističu važnost poštivanja prava na privatnost u digitalnom prostoru, osobito u pogledu GDPR-a. Naglašavaju kako je važno osigurati da su svi procesi obrade podataka u skladu s načelima privatnosti od početka do kraja, kako bi se zaštitila privatnost subjekata podataka. Ataei, Degbelo, Kray i Santos (2018) dodatno naglašavaju važnost očuvanja privatnosti lokacije u skladu s GDPR-om. Kako IoT uređaji često koriste podatke o lokaciji korisnika, potrebno je poduzeti dodatne mjere kako bi se osigurala zaštita ovih podataka. To uključuje informiranje korisnika o tome kako se podaci koriste i osiguranje mogućnosti korisnika da kontroliraju upotrebu svojih podataka.

Uz to, Georgiadou, de By i Kounadi (2019) naglašavaju važnost zaštite privatnosti lokacije u svjetlu GDPR-a. Pojašnjavaju da GDPR nudi značajan okvir zaštite privatnosti u kontekstu

prikupljanja i obrade podataka o lokaciji, što je od posebne važnosti za IoT aplikacije koje se sve više oslanjaju na geolokacijske podatke. Na temelju ovih spoznaja, jasno je da je GDPR od iznimnog značaja za osiguranje zaštite podataka u svijetu IoT-a, posebno s obzirom na veliku količinu osobnih podataka koji se generiraju i obrađuju. Ta količina podataka uključuje i osjetljive informacije poput podataka o lokaciji, koje je nužno zaštititi od nesankcioniranog pristupa ili zlouporabe. U vezi s ovim, regulativa GDPR pruža značajne smjernice i zahtjeve za upravljanje takvim podacima, uključujući ograničenja na obradu podataka, zahtjeve za transparentnost i informiranje korisnika te pravo korisnika na pristup i kontrolu nad njihovim podacima. To naglašava i rad Ziccardija (2020), koji se posebno bavi problematikom zaštite podataka u kontekstu nosive tehnologije, često integralnog dijela ekosustava IoT-a. U ovom kontekstu, primjena AI-a donosi dodatne izazove za zaštitu podataka. Kao što Georgiou i Lambrinoudakis (2020) ističu, važno je osigurati da se AI sustavi koji koriste podatke iz ekosustava IoT-a usklade s odredbama GDPR-a. To uključuje ne samo zaštitu podataka na svim razinama obrade, već i osiguranje da AI sustavi ne krše prava pojedinaca, poput prava na privatnost ili prava na nediskriminaciju.

Također, kako se ističe u radu Taylora i Whittona (2020), od velikog je značaja osigurati pravilnu ravnotežu između prava pojedinaca na kontrolu nad vlastitim podacima i potreba za pristupom podacima za istraživačke svrhe. Primjerice, u kontekstu istraživanja u zdravstvu, važno je osigurati da se osobni podaci koriste na način koji je u skladu s GDPR-om, dok se istovremeno omogućava da istraživači pristupe neophodnim podacima. Kao što su naveli Hölbl, Kežmah i Kompara (2021), GDPR je iznimno važan za IoT i postavlja visoke standarde zaštite podataka. S obzirom na to, organizacije koje koriste IoT tehnologije moraju poduzeti odgovarajuće korake kako bi osigurale da se u potpunosti pridržavaju ovih propisa. U svijetu IoT-a, ove mjere često uključuju implementaciju robusnih sigurnosnih sustava, uključujući kriptografiju i anonimizaciju podataka, kako bi se osigurala sigurnost podataka (Paolone et al., 2022).

Prema GDPR-u, organizacije su obvezne dobiti informirani pristanak korisnika prije obrade njihovih osobnih podataka. Ovaj pristanak mora biti jasno izražen i korisnici moraju biti u potpunosti informirani o svrsi obrade njihovih podataka. Ovo je posebno važno u kontekstu IoT-a, gdje uređaji često prikupljaju i obrađuju velike količine osobnih podataka, ponekad bez izravnog znanja korisnika (Diamantopoulou, Androutsopoulou, Gritzalis i Charalabidis, 2020). Uz to, GDPR pruža korisnicima pravo na pristup svojim podacima, pravo na ispravak netočnih

podataka, pravo na brisanje (pravo na zaborav) i pravo na ograničenje obrade. To znači da korisnici imaju kontrolu nad svojim podacima i mogu zahtijevati da se njihovi podaci izbrišu ili ograniče za daljnju obradu. Ovo je posebno važno u kontekstu IoT-a, gdje se osobni podaci često pohranjuju i obrađuju na udaljenim poslužiteljima (Ataei, Degbelo, Kray i Santos, 2018). Ovi autori naglašavaju da GDPR zahtijeva jasno informiranje korisnika o načinu korištenja njihovih podataka o lokaciji. Korisnici moraju dati izričit pristanak za takvu obradu, čime se osigurava njihovo sudjelovanje u odlučivanju o načinu korištenja njihovih osobnih podataka.

Prema Georgiou i Lambrinoudakisu (2020), jedan od bitnijih elemenata GDPR-a je potreba za procjenom utjecaja na zaštitu podataka (Data Protection Impact Assessment - DPIA) prilikom uvođenja novih tehnologija. DPIA je sistematski proces identificiranja i minimiziranja rizika povezanih s obradom osobnih podataka. Kada je riječ o IoT-u i AI-u, ova procjena postaje posebno važna. IoT uređaji su često povezani i generiraju velike količine podataka, što može uključivati i osjetljive osobne podatke. AI, s druge strane, često koristi te podatke za stvaranje preciznih modela i predviđanja. Bez odgovarajućih mjera zaštite, ovi procesi mogu izložiti korisnike rizicima, uključujući neautorizirani pristup podacima i potencijalne povrede privatnosti. U skladu s GDPR-om, DPIA bi trebala utvrditi kakav utjecaj nove tehnologije mogu imati na zaštitu osobnih podataka, te kakve mjere zaštite treba poduzeti. Ovaj proces može uključivati procjenu rizika povezanih s obradom podataka, analizu načina na koje se podaci prikupljaju, pohranjuju i obrađuju, te evaluaciju mjera zaštite koje su na mjestu. DPIA također može zahtijevati konzultacije s regulatorima za zaštitu podataka i, u nekim slučajevima, s korisnicima čiji se podaci obrađuju. Kroz ovaj proces, organizacije mogu identificirati potencijalne rizike i odrediti najbolje načine za mitigaciju tih rizika. Time se osigurava da IoT i AI tehnologije poštuju propise o zaštiti podataka i štite prava i slobode korisnika, čime se pomaže održati povjerenje korisnika i osigurati uspjeh ovih tehnologija na tržištu. Georgiadou, de By i Kounadi (2019) dodatno ističu pravo korisnika na prigovor, koje je također bitan element GDPR-a. Ovo pravo omogućava korisnicima da se usprotive obradi svojih podataka o lokaciji. Ovo je posebno relevantno u kontekstu IoT-a, gdje podaci o lokaciji mogu biti stalno prikupljani i obrađivani. Ti autori sugeriraju da bi provedba ovih mjera mogla biti izazovna, ali je važna za očuvanje prava korisnika na privatnost i zaštitu podataka. Važno je naglasiti da je održavanje transparentnosti i poštovanje prava korisnika od visoke važnosti za stvaranje povjerenja među korisnicima, što je neophodno za daljnji razvoj i usvajanje IoT tehnologija. Bez tog povjerenja, korisnici možda neće biti voljni koristiti ove tehnologije, što bi moglo ograničiti njihov potencijal.

Fedeli, Scendoni, Cingolani, Compagnucci, Cirocchi i Cannovo (2022) istaknuli su poseban aspekt zaštite podataka u kontekstu genetskih istraživanja. Prema GDPR-u, genetski podaci spadaju u kategoriju osjetljivih podataka, za koje se zahtijeva posebna zaštita. U kontekstu pandemije COVID-19, genetska istraživanja igraju ključnu ulogu u razumijevanju virusa i razvoju učinkovitih mjera za borbu protiv njega. No, prikupljanje i obrada genetskih podataka, uključujući podatke relevantne za istraživanje COVID-19, podliježe strogim pravilima GDPR-a.

GDPR zahtijeva jasno obrazloženje svrhe obrade genetskih podataka. Drugim riječima, istraživači moraju jasno navesti zašto prikupljaju genetske podatke i kako će ih koristiti. Ova pravila osiguravaju transparentnost u obradi podataka i omogućuju sudionicima istraživanja da razumiju kako će se njihovi podaci koristiti. Osim toga, obrada genetskih podataka mora se provesti uz striktno pridržavanje pravila o pristanku. Ovo znači da sudionici istraživanja moraju dati izričit pristanak za prikupljanje i obradu svojih genetskih podataka. Istraživači moraju osigurati da su sudionici istraživanja u potpunosti informirani o prikupljanju i obradi njihovih genetskih podataka, te da im je dano pravo da povuku svoj pristanak u bilo kojem trenutku. Naposljetku, obrada genetskih podataka mora se provesti uz striktno pridržavanje pravila o povjerljivosti. Istraživači su dužni zaštititi povjerljivost genetskih podataka sudionika istraživanja i osigurati da se podaci ne koriste na način koji bi mogao naštetiti sudionicima. Kroz ova pravila, GDPR ima bitan značaj u održavanju povjerenja javnosti u genetska istraživanja. Pravila o transparentnosti, pristanku i povjerljivosti omogućuju sudionicima istraživanja da imaju kontrolu nad svojim podacima i osiguravaju da se njihova prava poštuju. Ovo je od velikog značaja za održavanje povjerenja u genetska istraživanja i omogućavanje njihovog daljnjeg razvoja.

U AI-u, zaštita osobnih podataka postaje sve važnija. Diamantopoulou, Androutsopoulou, Gritzalis i Charalabidis (2020) detaljno su raspravljali o tome kako GDPR postavlja okvir za zaštitu podataka u kontekstu AI-a. Prvo, prema GDPR-u, svaki algoritam koji se koristi za obradu osobnih podataka mora biti transparentan. To znači da korisnici imaju pravo znati kako se njihovi podaci koriste i obrađuju. U kontekstu AI-a, to može uključivati objašnjenje kako algoritam radi i kako donosi odluke na temelju podataka koje koristi, što je iznimno bitno za osiguranje povjerenja korisnika u AI tehnologije. Drugo, GDPR predviđa *pravo na objašnjenje*. Ovo pravo omogućava korisnicima da traže objašnjenje odluka koje su donesene automatski, uključujući one koje su donesene kroz AI. Ako je, na primjer, korisnik odbijen za kredit na

temelju automatskog algoritma, ima pravo zatražiti objašnjenje o tome kako je algoritam došao do te odluke. Treće, GDPR zahtijeva da se osobni podaci zaštite tijekom cijelog životnog ciklusa AI sustava. To uključuje mjere zaštite podataka tijekom prikupljanja, pohrane, obrade, dijeljenja i brisanja podataka. AI sustavi često koriste i obrađuju velike količine osobnih podataka, stoga je važno osigurati da se ti podaci zaštite u svim fazama životnog ciklusa sustava. Ovi aspekti GDPR-a osiguravaju da se AI tehnologije razvijaju na način koji poštuje prava na privatnost i štiti osobne podatke. Ovo je ključno za održavanje povjerenja javnosti u AI i omogućavanje njenog daljnjeg razvoja.

IoT AI stvaraju kompleksna okruženja u kojima se podaci neprestano prikupljaju, obrađuju i dijele između različitih entiteta. Ova složena dinamika može stvoriti izazove kada je riječ o poštovanju GDPR-a, kako Taylor i Whitton (2020) naglašavaju. GDPR zahtijeva jasnu definiciju uloga i odgovornosti svih onih koji obrađuju podatke. To znači da svaka organizacija koja prikuplja, obrađuje ili čuva podatke mora razumjeti svoje obaveze prema GDPR-u. Međutim, u okruženjima kao što su IoT i AI, podaci često prolaze kroz mnoge različite sustave i organizacije. Definiranje uloga i odgovornosti može biti posebno izazovno kada podaci putuju kroz takve složene mreže. Na primjer, IoT uređaj može prikupljati podatke koji se zatim šalju na servere tvrtke za analizu. Ti se podaci zatim mogu dijeliti s drugim tvrtkama za daljnje analize ili za marketinške svrhe. U tom procesu, nije uvijek jasno tko je odgovoran za zaštitu podataka u svakoj fazi.

Ovo je područje koje zahtijeva dodatno razmatranje i smjernice kako bi se osigurala učinkovita zaštita podataka u složenim okruženjima poput IoT-a i AI-a. Taylor i Whitton (2020) sugeriraju da će biti potrebne daljnje studije i možda zakonske izmjene kako bi se ovaj problem u potpunosti riješio.

Nosive tehnologije i pametna odjeća postaju sve uobičajeniji u našim svakodnevnim životima. Bilo da je riječ o pametnim satovima koji prate naše zdravstvene parametre, kao što su otkucaji srca i razina tjelesne aktivnosti, ili pametnoj odjeći koja može pratiti našu temperaturu i postotak tjelesne masnoće, te tehnologije prikupljaju vrlo osjetljive i osobne podatke. U kontekstu GDPR-a, Ziccardi (2020) ističe da su ti podaci posebno zaštićeni. Prema GDPR-u, podaci o zdravlju su posebna kategorija osobnih podataka koja je podložna strogim zahtjevima zaštite. To znači da tvrtke koje proizvode i prodaju nosive tehnologije moraju poduzeti dodatne mjere kako bi osigurale zaštitu tih podataka. Ziccardi (2020) navodi nekoliko specifičnih izazova povezanih s ovom temom. Prvi je da se podaci o zdravlju često prikupljaju i obrađuju

bez eksplicitnog pristanka korisnika. Drugi izazov je sigurnost podataka, budući da ove tehnologije često koriste bežične mreže za prenošenje podataka, što može predstavljati rizik od neovlaštenog pristupa. Konačno, korisnici često nisu dovoljno informirani o tome kako i zašto se njihovi podaci prikupljaju i koriste. Za rješavanje ovih izazova, Ziccardi (2020) predlaže veću transparentnost i bolje informiranje korisnika, kao i strožu regulaciju i nadzor nad tvrtkama koje proizvode ove tehnologije. Ovo uključuje pružanje jasnih informacija korisnicima o tome kako se njihovi podaci koriste, kao i pridržavanje najboljih praksi za sigurnost podataka.

Slijedom svega navedenog, evidentno je da Uredba (EU) 2016/679 ili GDPR ima izniman značaj u osiguranju zaštite osobnih podataka u kontekstu IoT-a i AI-a. Ona propisuje visoke standarde zaštite podataka, uključujući pravila o pristanku, transparentnosti i povjerljivosti, kao i specifične zahtjeve za obradu osjetljivih podataka kao što su podaci o lokaciji i genetski podaci. Usprkos izazovima, postizanje usklađenosti s GDPR-om od iznimnog je značaja za održiv i odgovoran razvoj IoT-a i AI-a.

4. ANALIZA TRŽIŠTA ELEKTRONIČKIH KOMUNIKACIJA U KONTEKSTU NOVOG ZAKONODAVSTVA I KIBERNETIČKE SIGURNOSTI U REPUBLICI HRVATSKOJ

U dinamičkom svijetu elektroničkih komunikacija, razumijevanje tržišta u kontekstu novog zakonodavstva i kibernetičke sigurnosti postaje ključno. U Republici Hrvatskoj, kao i širom svijeta, tehnološke inovacije poput Interneta stvari (IoT) donose nove mogućnosti, ali i izazove. U poglavlju 4. ovoga rada pružit će se sveobuhvatan prikaz tržišta elektroničkih komunikacija u Hrvatskoj, istražujući kako IoT utječe na ovaj sektor i kako je novo zakonodavstvo oblikovalo pejzaž. Poseban naglasak bit će na NIS 1 i NIS 2 direktivama, čijim se uvođenjem pokušava pružiti odgovor na povećane kibernetičke prijetnje.

Kibernetička sigurnost postala je iznimno bitna tema u diskursu elektroničkih komunikacija. Poglavlje 4.4. detaljno će se baviti ovim pitanjem, pružajući uvid u najčešće vrste kibernetičkih napada, razinu svijesti o potencijalnim rizicima, kao i mjere zaštite koje su poduzete za zaštitu od tih napada.

Osim toga, zaštita privatnosti i podataka dobiva na važnosti u svijetu IoT-a. U poglavlju 4.5. istraživat će se kako regulatorna obilježja usluga pametnih gradova i nacionalno zakonodavstvo utječu na zaštitu privatnosti i podataka.

Ova analiza omogućuje dublje razumijevanje dinamičnog tržišta elektroničkih komunikacija u Hrvatskoj, te donosi uvid u to kako novo zakonodavstvo i povećana svijest o kibernetičkoj sigurnosti mijenjaju način na koji komuniciramo i poslujemo.

4.1. Prikaz tržišta elektroničkih komunikacija

Tržište elektroničkih komunikacija u Republici Hrvatskoj prolazi kroz dinamičan period promjena, gdje glavnu ulogu igraju novi Zakon o elektroničkim komunikacijama (dalje u tekstu: ZEK), stupio na snagu u srpnju 2022. godine, kao i direktive Europskog parlamenta i Vijeća koje se odnose na elektroničke komunikacije. ZEK donosi brojne inovacije u regulativnom okviru, uključujući konsolidaciju pravnih smjernica elektroničkih komunikacija koje su od ključne važnosti za ostvarenje ambicioznih ciljeva Europske Unije do 2030. godine.

Među tim ciljevima su gigabitna povezanost na razini cijele Unije i potpuna pokrivenost 5G mrežom na svim naseljenim područjima.

ZEK pokriva širok spektar područja u kontekstu elektroničkih komunikacija, uključujući pružanje mrežnih usluga, upravljanje radiofrekvencijskim spektrom, zaštitu podataka i prava korisnika, kao i sigurnost mreža i usluga. Na ovaj način, ZEK pokušava uskladiti kompleksnu stvarnost tržišta elektroničkih komunikacija sa novim tehničkim i tehnološkim zahtjevima, uz poticanje tržišne konkurencije i zaštite prava sudionika na tržištu. ZEK, iako donosi brojne novine, ipak ne mijenja temeljne regulatorne obveze operatera u pružanju elektroničkih komunikacijskih usluga i upravljanju elektroničkim komunikacijskim mrežama. Te obveze ostale su većinom nepromijenjene u odnosu na ranije uređenje.

Važne promjene koje uvodi novi regulatorni okvir odnose se na tehničke aspekte pružanja elektroničkih komunikacija, uključujući koordinaciju korištenja radiofrekvencijskog spektra i pristupa infrastrukturi na razini cijele EU. Osim toga, ZEK uvodi i diferencirane regulatorne obveze za različite vrste operatora, uz uvođenje novih pojmova kao što su maloprodajni/veleprodajni operateri i mikropoduzeća. Na prvom mjestu, operatori su obvezni pružiti univerzalnu uslugu. To znači da su dužni omogućiti pristup uslugama elektroničkih komunikacija na cijelom teritoriju Republike Hrvatske, po razumnoj cijeni i odgovarajuće kvalitete. Ova obveza ima za cilj osigurati da svaki građanin, bez obzira na njegovu lokaciju, ima pristup osnovnim uslugama komunikacije. Sljedeća značajna obveza je obveza pristupa. Operatori, koji kontroliraju pristup do krajnjeg korisnika, obvezni su omogućiti pristup svojoj infrastrukturi drugim operatorima na pravednim, objektivnim i nediskriminirajućim uvjetima. Ova obveza omogućuje konkurenciju na tržištu i potiče inovacije.

Važna je i obveza zaštite podataka korisnika. Operatori moraju poduzeti odgovarajuće tehničke i organizacijske mjere za zaštitu podataka korisnika od neovlaštenog pristupa, obrade, gubitka ili oštećenja. Osim toga, postoji obveza zaštite prava korisnika. Operatori su dužni informirati korisnike o uvjetima korištenja usluga, cijenama i tarifama, pravima korisnika u slučaju kvara ili prekida usluge, te o mjerama koje korisnici mogu poduzeti kako bi zaštitili svoje interese.

Na kraju, ali ne manje važno, jest obveza osiguranja sigurnosti elektroničkih komunikacijskih mreža i usluga. Operatori su dužni poduzeti odgovarajuće mjere kako bi osigurali integritet i sigurnost svojih mreža i usluga. Sve navedene obveze su bitne za rad operatora na tržištu elektroničkih komunikacija i doprinose stvaranju konkurentnog i pravičnog okruženja za sve

sudionike. Važno je napomenuti da je svaki operator odgovoran za poštivanje ovih obveza i da bi nepridržavanje moglo dovesti do značajnih sankcija od strane regulatornih tijela.

U ZEK-u, Republika Hrvatska se uskladila s Direktivom Europskog parlamenta i Vijeća, čime je omogućeno jače povezivanje hrvatskog tržišta s europskim, ali i unaprijedila zaštita prava korisnika. Pored prethodno navedenih promjena u regulatornom okviru, ZEK je donio nekoliko tehničkih promjena koje se tiču uvjeta i postupaka izdavanja odobrenja za pružanje elektroničkih komunikacijskih usluga i mreža, kao i uvjeta upravljanja i korištenja brojevnih resursa.

Ostale promjene uključuju preciznije reguliranje uvjeta za ostvarivanje prava pristupa i sučeljavanja, uključujući uvjete za pristup fizičkoj infrastrukturi, što je posebno važno za operatora u svjetlu planiranog razvoja novih generacija mreža, poput 5G. HAKOM-u je dano više ovlasti za upravljanje frekvencijskim spektrom, što je također bitan element za razvoj 5G mreža. Iz tog razloga, zakonodavac je prepoznao potrebu za pojačanjem regulatornih ovlasti kako bi se osigurala pravična i učinkovita alokacija spektra. Također, ZEK uključuje poboljšanja koja se odnose na zaštitu potrošača, kao što je obvezno informiranje potrošača o uvjetima pružanja usluga, uključujući cijene i druge uvjete, te pravo na jednostrani raskid ugovora. To je dio opće orijentacije prema povećanju transparentnosti tržišta elektroničkih komunikacija i poboljšanju zaštite prava potrošača.

Sve te promjene su pokazatelj jasne tendencije da se regulatorni okvir prilagodi brzo razvijajućim tehnologijama i novim poslovnim modelima u sektoru elektroničkih komunikacija, pružajući bolji okvir za inovacije i konkurenciju. Isto tako, zakonodavac nastoji postići ravnotežu između poticanja inovacija i konkurencije s jedne strane, i zaštite potrošača s druge strane.

Očekuje se da će te promjene dovesti do značajnijih promjena na tržištu elektroničkih komunikacija u Hrvatskoj, s više konkurencije i inovacija, što bi trebalo koristiti potrošačima. Pored toga, one bi trebale pomoći u stvaranju povoljnijeg okruženja za investicije i razvoj novih tehnologija i usluga.

S obzirom na sve ove promjene, može se zaključiti da novi ZEK donosi niz značajnih inovacija koje imaju za cilj unaprijediti prava korisnika i potaknuti razvoj tržišta elektroničkih komunikacija.

Tržište elektroničkih komunikacija nastavilo je s rastom tijekom 2022. godine, s ukupnim prihodima koji su dosegnuli 1.6 milijardi eura, što predstavlja povećanje od 3,6 posto u odnosu na prethodnu godinu (HAKOM, 2023). Operatori su nastavili s ulaganjima u mreže pokretnih i nepokretnih komunikacija, uz poseban naglasak na mreže vrlo velikog kapaciteta (VHCN), gdje su ulaganja viša za šest posto u odnosu na isto razdoblje prethodne godine.

Tijekom 2022. godine, prihodi od usluga širokopojasnog pristupa internetu rasli su za devet posto, od najma mreže i vodova za pet posto, a od naplatne televizije za četiri posto. Suprotno tome, prihodi od telefonskih usluga u nepokretnoj mreži smanjeni su preko devet posto. Prikaz tržišta ne bi bio potpun bez analize korisničkih navika. U četvrtom tromjesečju 2022. nastavljena je migracija korisnika na svjetlovodnu tehnologiju, što je utjecalo na rast takvih priključaka za 27,5 posto u godini dana. Ukupan podatkovni promet putem nepokretnih i pokretnih mreža rastao je u prosjeku za 15,7 posto. Interesantno je primijetiti kako je udio korisnika širokopojasnih priključaka s brzinom većom od 100 Mbit/s također rastao i iznosi 35,7 posto. Analiza tržišta otkriva i značajne podatke o korištenju roaming usluga. Strani državljani su u posljednjem tromjesečju 2022. godine potrošili preko 95 milijuna roaming minuta razgovora, što je rast od 8,9 posto u odnosu na isto razdoblje 2021. godine. S druge strane, broj poslanih SMS i MMS poruka značajno je niži u odnosu na prethodnu godinu, s padom od 21,6 posto, odnosno 27,7 posto (HAKOM, 2023).

Kada je u pitanju naplatna televizija, 62,3 posto kućanstava koristilo je neki oblik televizije s naplatom usluge, a prihodi od ove usluge nastavili su rasti. Ukupni prihodi od usluga televizije povećali su se za 4,3 posto u odnosu na prethodnu godinu. Najzastupljeniji oblik televizije je IPTV s više od 52 posto priključaka. Ovaj podatak ukazuje na to da korisnici sve više cijene visokokvalitetan sadržaj i napredne usluge koje IPTV nudi, kao što su interaktivnost, prilagođavanje sadržaja, pristup različitim platformama i sl.

Međutim, nije sve na tržištu elektroničkih komunikacija bilo u znaku rasta. Na tržištu telefonskih usluga u nepokretnoj mreži nastavljen je trend smanjenja broja korisnika, ukupnih prihoda i odlaznog prometa. U usporedbi s istim razdobljem prethodne godine, broj korisnika manji je za 1,8 posto, ukupni odlazni promet operatora niži je za 22,5 posto, a ukupni prihod za 9,4 posto. Ovi podaci jasno ukazuju na to da korisnici sve više prelaze na mobilne mreže i usluge širokopojasnog pristupa internetu, posebno s obzirom na širenje i unaprjeđenje svjetlovodne tehnologije. U cjelini, 2022. godina bila je godina rasta i unaprjeđenja na tržištu elektroničkih komunikacija. Operatori su nastavili s ulaganjima u infrastrukturu, a korisnici su

pokazali jasnu preferenciju za naprednije tehnologije i usluge. Unatoč izazovima, kao što su smanjenje broja korisnika nepokretnih telefonskih usluga, tržište je pokazalo sposobnost prilagodbe i inovacije, što ukazuje na svijetlu budućnost za sektor elektroničkih komunikacija u Hrvatskoj (HAKOM, 2023).

Kako bi se potpunije moglo prikazati značajke dinamičnog tržišta elektroničkih komunikacija vrijedi ukazati i na spoznaje sa Dana tržišta elektroničkih komunikacija održanog u listopada 2022. godine u Zagrebu. Na ovom događanju okupili su se predstavnici različitih dionika tržišta elektroničkih komunikacija, tijela državne uprave, predstavnici gospodarstva, znanstvene zajednice te medija. Ovaj događaj koji se održava svake godine, pružio je priliku za prezentaciju najvažnijih aktivnosti na tržištu te ciljeva i zadataka HAKOM-a za buduće razdoblje. Četiri panel rasprave obuhvatile su različite tematske okvire, od zemljopisnog pregleda dostupnosti i korištenja elektroničkih komunikacijskih mreža, preko simetrične regulacije kao nadopune SMP regulacije, do novih pravila za transparentno ugovaranje usluga i raskid ugovora. Također, otvorena je diskusija o potrebi sufinanciranja razvoja mreža od strane OTT pružatelja, koji te mreže koriste u svom poslovanju.

Rasprave su bile osnažene uvidima i znanjem stručnjaka iz različitih područja, među kojima su predstavnici A1 Hrvatska d.o.o., Hrvatskog Telekoma d.d., Ministarstva mora, prometa i infrastrukture Republike Hrvatske, Telemach Hrvatska d.o.o., Pro-Ping d.o.o. te Googlea, a sve je koordinirano pod vodstvom moderatora iz HAKOM-a. Prema izvorima dostupnim na HAKOM-ovom webu, Agencija redovito prikuplja i objavljuje podatke s tržišta elektroničkih komunikacija, poštanskih i željezničkih usluga, prateći time trendove razvoja tržišta. Ovaj Dan tržišta elektroničkih komunikacija poslužio je kao važan mehanizam za iznošenje i raspravljanje o takvim podacima, omogućujući stoga bolje razumijevanje stanja i kretanja na tržištu. na minimalnoj razini. Naglasio je važnost ravnoteže između zaštite korisnika i slobodnog tržišnog natjecanja.

Dakle, iz pristupa svih panelista, jasno je da je opća suglasnost o tome da je simetrična regulacija potrebna kao alat za uravnoteženje tržišne konkurencije. Međutim, postoji jasan oprez kada je u pitanju stupanj regulacije, s obzirom da prekomjerna regulacija može imati potencijalno štetne učinke na investicije i tržišnu dinamiku. Jasno je da će biti potrebna daljnja rasprava kako bi se došlo do rješenja koje će zadovoljiti sve strane. Sveukupno, *Dan tržišta elektroničkih komunikacija* pružio je vrijedne uvide u trenutne izazove i mogućnosti na hrvatskom tržištu elektroničkih komunikacija. Izražena je potreba za daljnjim dijalogom i

suradnjom između operatora, regulatora i ostalih relevantnih dionika kako bi se osiguralo da hrvatsko tržište elektroničkih komunikacija nastavi napredovati i pružati kvalitetnu uslugu korisnicima. Sve ove spoznaje su prema informacijama izviještenim od strane HAKOM-a i vodećih operatora na hrvatskom tržištu.

Na suvremenom tržištu elektroničkih komunikacija, značaj transparentnosti i jasne komunikacije s korisnicima sve je veći. Kako je Petra Nakić navela, korisnici cijene mogućnost da na jednom mjestu dobiju sve potrebne informacije i pisane potvrde onoga što im je ponuđeno od strane operatora. Ova praksa doprinosi smanjenju nejasnoća, povećanju transparentnosti, i na koncu, većoj sigurnosti za korisnike. U pogledu amortizacije opreme, pristup Hrvatskog Telekoma d.d. (HT) odnosi se na podjelu uređaja po vrijednosti u klastere i postupno smanjenje njihove vrijednosti na godišnjoj razini. Kako bi se izbjegla situacija u kojoj korisnici moraju platiti za uređaje, potrebno je da ih vrate. S druge strane, A1 Hrvatska d.o.o. (A1), osim obveze propisane pravilnikom o povratu, dodatno korisniku šalje dva dopisa nakon isporučenog računa, omogućujući tako vraćanje opreme bez dodatnih troškova. Kako je istaknula Erslan, cilj A1 je prikupljanje opreme koju će, ako je potrebno, uništiti na propisani način. Kada je riječ o korištenju vlastite opreme, zakon predviđa takvu mogućnost, ali je uvjet da oprema bude kompatibilna s mrežama operatora. U situacijama kada korisnik koristi opremu koja nije prošla sva testiranja, operator ne može imati nadzor nad tim uređajem, ne može pružiti daljinsku pomoć u otklanjanju kvarova, niti može biti odgovoran za kvalitetu usluge pristupa ili garantirati minimalnu brzinu. Kao što je rečeno tijekom skupa, korisnici trebaju biti informirani o tome što mogu očekivati od svoje opreme, a što od opreme operatora, kako bi na kraju sami mogli donijeti odluku.

Jedno od važnih pitanja koje se raspravljalo na četvrtoj panel raspravi bilo je trebaju li OTT pružatelji usluga financijski doprinositi razvoju mreža koje koriste. Stavovi su se križali, a u raspravi su sudjelovali predstavnici Googlea, HAKOM-a, HT-a i odvjetničkog društva Hrdalo&Krnić. Diskusija je otvorila pitanje uloge i obaveza tehnoloških giganta poput Googlea, Mete, NetF lixa i sličnih u pokrivanju troškova razvoja i korištenja komunikacijskih mreža putem kojih pružaju svoje usluge. Ova rasprava se odvija na razini EU, te sukladno ciljevima *Digitalne dekade*, posebno se razmatra u kontekstu potpune pokrivenosti 5G i gigabitnim pristupom do 2030. godine.

S jedne strane, tehnološki giganti poput Googlea smatraju da su kroz DSA (*Digital Services Act*) i DMA (*Digital Markets Act*) već prekomjerno regulirani, te da su im nametnute značajne

obveze i potencijalne kazne. S druge strane, pružatelji usluga poput HT-a se suočavaju s poteškoćama u namirenju troškova, a kako je Iva Cibulić Blažević istaknula, pojedini OTT pružatelji čak odbijaju plaćanje operatorima. Izazov je pružiti korisnicima nesmetan pristup uslugama, ali istovremeno osigurati pravednu raspodjelu troškova.

Zanimljivu perspektivu pružio je Igor Zgrabljić iz Googlea, naglašavajući da korisnici trebaju biti u središtu svih diskusija. Tvrdi da Google već pridonosi infrastrukturi, ukazujući na investicije od 23 milijarde eura samo prošle godine u Europi, uključujući ulaganja u podmorske kabele i ostale infrastrukturne projekte.

Vlaho Hrdalo, odvjetnik, naglasio je da je prilagodba ključna, izrazivši stajalište da bi operatori trebali biti fleksibilniji u prilagođavanju novonastalim okolnostima. S druge strane, Mislav Hebel iz HAKOM-a upozorio je na potrebu za odgovarajućim opravdanjima za svaku regulativnu mjeru, potvrđujući da će BEREC (Body of European Regulators for Electronic Communications) nastaviti sa svojim analizama.

U svojoj završnoj riječi, ravnatelj HAKOM-a, Miran Gosta, naglasio je važnost dijaloga sa svim dionicima kako bi se postiglo zadovoljstvo korisnika. Ovaj skup pružio je važan forum za raspravu o pitanjima koja su ključna za budući razvoj tržišta elektroničkih komunikacija.

Proučavajući izvještaj Dan HAKOM-a iz 2022. godine, postaje jasno koliko je tržište elektroničkih komunikacija otporno i dinamično. Unatoč globalnoj neizvjesnosti uzrokovanom pandemijom i političkim nemirima, tržište je pokazalo iznimnu izdržljivost. Međutim, postavlja se pitanje kada i u što ulagati, i kako će regulator reagirati na takve odluke.

4.2. Uloga Interneta stvari na tržištu elektroničkih komunikacija

Transformacija tržišta elektroničkih komunikacija pod utjecajem IoT tehnologije postaje sve izraženija. Ova tehnologija, koja je revolucionirala svijet informacija, drastično mijenja način prikupljanja, obrade i prijenosa informacija. IoT uređaji postaju ključni igrači u ovom procesu, nudeći niz mogućnosti za unapređenje komunikacije. IoT uređaji, koji uključuju sve od pametnih telefona do kućanskih aparata i industrijske opreme, opremljeni su senzorima i softverom koji omogućavaju prikupljanje, obradu i razmjenu podataka putem interneta. Ova sposobnost prikupljanja i razmjene podataka u stvarnom vremenu omogućava niz inovacija koje dovode do bolje povezanosti, veće učinkovitosti i poboljšane kvalitete usluga. U studiji

koju su proveli Abdel-Basset et al. (2019), autori ističu da IoT tehnologija ima značajan utjecaj na tržište elektroničkih proizvoda. Primjena IoT-a na ovom tržištu rezultira moćnim sustavom za podršku odlučivanju koji može pružiti korisnicima informacije temeljene na analizi velikih količina podataka prikupljenih s različitih IoT uređaja. Ovaj sustav pomaže korisnicima da donose informirane odluke o odabiru proizvoda, što u konačnici dovodi do boljeg korisničkog iskustva. Osim toga, IoT tehnologija doprinosi stvaranju personaliziranih proizvoda i usluga koje su bolje prilagođene specifičnim potrebama korisnika. Prikupljanje podataka s IoT uređaja omogućava proizvođačima da bolje razumiju ponašanje korisnika i da na temelju tih spoznaja razviju proizvode i usluge koje bolje zadovoljavaju njihove potrebe.

IoT ne samo da transformira tržište elektroničkih komunikacija, već otvara i nove mogućnosti za telekomunikacijsku industriju. Povezanost koju IoT donosi premašuje koncept povezivanja ljudi i proširuje se na povezivanje različitih uređaja i sustava. Kako su Nistor i Zadobrischi (2022) naglasili, integracija IoT-a i telekomunikacija zajedno preoblikuje regionalni medijski pejzaž, a ovo je posebno važno u kontekstu evolucije elektroničkih tržišta.

Prisutnost IoT-a mijenja pravila igre u telekomunikacijama. Telekomunikacijske mreže su ključne za IoT ekosustav jer pružaju infrastrukturu koja omogućava povezanost među uređajima. IoT uređaji generiraju ogromne količine podataka, što povećava potražnju za visokokvalitetnim, brzim i pouzdanim mrežama za prijenos tih podataka. Ovaj porast u korištenju podataka potiče telekomunikacijsku industriju da kontinuirano poboljšava svoje usluge, unaprjeđujući brzine prijenosa podataka, pokrivenost mreže i kvalitetu usluge. S druge strane, IoT otvara nove poslovne prilike za telekomunikacijske operatere. Na primjer, operatori mogu pružati usluge upravljanja podacima i analitike za tvrtke koje koriste IoT uređaje, omogućavajući im da bolje koriste prikupljene podatke. Također, operatori mogu razvijati i pružati specijalizirane IoT usluge za određene sektore, kao što su zdravstvo, poljoprivreda ili transport.

Konvergencija tehnologije i telekomunikacija IoT-a otvara vrata revolucionarnim promjenama u svijetu digitalne komunikacije. Ova sinergija ne samo da olakšava komunikaciju i povezivanje različitih uređaja, već utire put za razvoj novih poslovnih modela i otvara neviđene prilike u telekomunikacijskom sektoru. Prva i najizraženija transformacija dolazi kroz unapređenje infrastrukture koja podržava IoT. Kako bi se omogućila efikasna komunikacija među IoT uređajima, neophodna je brza i pouzdana mrežna infrastruktura. Telekomunikacijske tvrtke igraju ključnu ulogu u osiguravanju ovih mreža, koje uključuju nove generacije mobilnih

mreža poput 5G, te posebne mreže poput LoRaWAN i NB-IoT. Ova poboljšanja u mrežnoj infrastrukturi ne samo da omogućavaju IoT uređajima da se efikasno povežu i komuniciraju, već također omogućuju telekomunikacijskim tvrtkama da prošire svoje poslovanje i pruže nove usluge. Primjerice, pružanje usluga upravljanja i analize podataka prikupljenih od IoT uređaja može postati važan dio poslovnog modela telekomunikacijskih tvrtki. Također, integracija umjetne inteligencije i mašinskog učenja s IoT uređajima otvara nove mogućnosti za razvoj naprednih usluga i aplikacija. Osim toga, konvergencija IoT-a i telekomunikacija također omogućuje razvoj novih poslovnih modela. Na primjer, modeli temeljeni na podacima, gdje se prikupljeni podaci koriste za pružanje personaliziranih usluga, mogu donijeti dodatne prihode telekomunikacijskim tvrtkama.

IoT tehnologija, u kombinaciji sa strojnim učenjem, preoblikuje način na koji se energija koristi, posebno u kontekstu pametnih zgrada. Prema istraživanju koje su proveli Shah et al. (2022), ove dvije tehnologije igraju ključnu ulogu u poboljšanju energetske učinkovitosti, što je sada važnija nego ikad s obzirom na rastuće globalne energetske potrebe i ekološke izazove. Pametne zgrade, koje su opremljene IoT uređajima, omogućuju precizno praćenje i kontrolu potrošnje energije. Senzori i uređaji prikupljaju podatke o različitim aspektima zgrade, poput temperature, vlažnosti, osvjetljenja i prisutnosti ljudi, a zatim te podatke koriste za prilagodbu uvjeta i optimizaciju potrošnje energije. Primjerice, sustav za upravljanje energijom može automatski prilagoditi grijanje ili hlađenje na temelju broja ljudi u sobi ili vremenskih uvjeta. Međutim, samo prikupljanje i upotreba podataka nije dovoljno da bi se postigla optimalna energetska učinkovitost. Ovdje dolazi do izražaja uloga mašinskog učenja. Algoritmi mašinskog učenja mogu analizirati podatke prikupljene od IoT uređaja, prepoznati obrasce i trendove, i na temelju toga donositi informirane odluke o upravljanju energijom. Na primjer, algoritam strojnog učenja može predvidjeti potrošnju energije na temelju povijesnih podataka i trenutnih uvjeta, omogućujući sustavu da unaprijed prilagodi potrošnju kako bi se izbjegli vrhovi u potrošnji. To ne samo da vodi do značajnih ušteda energije, već i smanjuje trošak energije za korisnike.

Slijedom navedenog, IoT predstavlja središnju sastavnicu modernog tržišta elektroničkih komunikacija. Njegova sposobnost prikupljanja, obrade i prenošenja velikih količina podataka omogućuje bolje povezivanje uređaja, efikasniju komunikaciju i optimizaciju resursa. Kako tehnologija napreduje, očekuje se da će IoT nastaviti oblikovati tržište elektroničkih komunikacija na načine koji su trenutno možda i nezamislivi.

4.3. Novi pravno-regulatorni okvir elektroničkih komunikacija: NIS 1 i NIS 2 Direktiva

Kao odgovor na sveprisutnost i rastući utjecaj digitalnih tehnologija u svakodnevnom životu, Europska unija je donijela direktive NIS 1 i NIS 2, uspostavljajući tako novi pravno-regulatorni okvir za elektroničke komunikacije. Transformacija digitalne topografije koju smo svjedočili posljednjih godina, kao što su ubrzani razvoj 5G tehnologije (Rogalski, 2021; Gur, 2022), rast cyber prijetnji i sve veća ovisnost o digitalnim sustavima za ključne usluge, ukazala je na hitnu potrebu za jačanjem cyber sigurnosti na razini EU.

U ovom kontekstu, direktive NIS 1 i NIS 2 izdane su s ciljem stvaranja jedinstvenog pristupa zaštiti kritične infrastrukture od cyber prijetnji na razini EU. Prema Claus Nielsen (2022), ove direktive predstavljaju ključni korak u tom smjeru. One ne samo da uspostavljaju obvezne mjere zaštite i obvezu izvješćivanja o incidentima za ključne pružatelje usluga i digitalne pružatelje usluga, već također šire njihovu primjenu na velik broj sektora i uvode strože mjere nadzora na razini EU. Ove promjene u pravnom i regulatornom okviru pokazuju prepoznavanje od strane EU o sve većoj važnosti digitalne sigurnosti u suvremenom svijetu. Kako ističe Schmitz-Berndt i Cole (2022), ovakav sveobuhvatni i koordinirani pristup cyber sigurnosti unutar EU neophodan je za efikasnu zaštitu digitalnih sustava i infrastrukture od potencijalnih prijetnji.

Ove direktive predstavljaju snažan korak naprijed u uspostavi efikasnijeg i koherentnijeg okvira za cyber sigurnost unutar EU. Međutim, kako ističe Markopoulou (2021), implementacija ovih direktiva također stavlja izazove pred organizacije koje moraju prilagoditi svoje operacije novim zahtjevima. To uključuje uspostavu odgovarajućih mehanizama za ocjenu i upravljanje rizikom, razvoj efikasnih sustava za izvještavanje o incidentima i postizanje usklađenosti s novim regulatornim zahtjevima. S obzirom na složenost digitalnog okruženja i stalno mijenjajuće prijetnje cyber sigurnosti, važno je kontinuirano praćenje i ažuriranje ovog pravno-regulatornog okvira. Kao što de Hert, Papakonstantinou i Markopoulou (2019) naglašavaju, uočavajući neumoljiv rast i sveprisutnost digitalnih tehnologija u svakodnevnom životu, EU je uvela prvu Direktivu o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava u Uniji, poznatiju kao NIS 1 Direktiva. Ova Direktiva, kako ističu de Hert i suradnici (2019), predstavljala je prvi značajan pokušaj EU da na sveobuhvatan način regulira pitanje cyber sigurnosti na razini Unije. Uvela je niz mjera koje su se odnosile na pružatelje ključnih usluga i digitalnih usluga, te je postavila temelje za suradnju između država članica u ovom

ključnom području. Međutim, s obzirom na dinamičnu i stalno evoluirajuću prirodu digitalne sfere, pokazalo se da je NIS 1 Direktiva brzo postala nedovoljna za pružanje odgovarajuće zaštite. Stalni razvoj tehnologije, poput brzog razvoja 5G mreže (Rogalski, 2021; Gur, 2022), donio je nove izazove i složenosti koje originalna Direktiva nije mogla u potpunosti riješiti.

Schmitz-Berndt i Cole (2022) prepoznali su ovu prazninu i istaknuli potrebu za uvođenjem efikasnijeg i koherentnijeg regulatornog okvira koji bi se mogao prilagoditi ovim promjenjivim uvjetima. Potreba za novim pristupom kojim bi se osigurao odgovarajući nivo cyber sigurnosti, rezultirala je uvođenjem NIS 2 Direktive. Ova revizirana Direktiva cilja na proširenje opsega sektora obuhvaćenih regulativom, jačanje mjera nadzora i uvodnjenje strožijih zahtjeva za izvještavanje o incidentima. Pored toga, prepoznavanje koncepta *securability* kao ključnog za zaštitu digitalnih sustava od rastućih cyber prijetnji (Maglaras, Janicke, Ferrag, 2022), dodatno naglašava nužnost stalnog ažuriranja i prilagodbe pravno-regulatornog okvira za elektroničke komunikacije. Kao što ističu Markopoulou i Papakonstantinou (2021), ova kontinuirana evolucija je neophodna kako bi se osigurala adekvatna zaštita u sve složenijem digitalnom pejzažu.

Kao odgovor na navedene nedostatke i kontinuirane izazove koje digitalna era donosi, EU je predložila drugu verziju Direktive o sigurnosti mrežnih i informacijskih sustava - NIS 2 Direktivu. Ova revizija nije samo prepoznala i riješila pitanja koja su se pojavila nakon provedbe NIS 1 Direktive, već je također postavila i strože zahtjeve za razne organizacije. Kako Cullen International (2022) ističe, jedan od važnih aspekata NIS 2 Direktive je uvođenje obveznog izvještavanja o incidentima. Ova mjera je osmišljena da unaprijedi transparentnost i olakša pravodobno reagiranje na sigurnosne incidente. Uz to, Direktiva uvodi i poboljšane mjere za upravljanje rizicima, usmjerene na osiguranje da organizacije aktivno upravljaju svojim cyber sigurnosnim rizicima. Osim što je pojačala već postojeće zahtjeve, NIS 2 Direktiva je također proširila svoj doseg na širi raspon sektora. Osborne Clarke (2023) navodi da su sada obuhvaćeni pružatelji digitalnih usluga poput online tržišta, online tražilica i usluga cloud computinga. Ovaj prošireni opseg odražava sve veću ulogu koju digitalne usluge igraju u društvu i gospodarstvu, te priznaje da je njihova sigurnost jednako važna za opću cyber sigurnost.

U sveobuhvatnom prepoznavanju novih digitalnih trendova, NIS 2 Direktiva dodatno naglašava važnost sposobnosti da se kritična infrastruktura zaštiti od cyber prijetnji (Maglaras, Janicke, Ferrag, 2022). Kroz ovu širu perspektivu i sveobuhvatniji pristup, NIS 2 Direktiva predstavlja

značajan korak naprijed u stvaranju učinkovitijeg i koherentnijeg pravno-regulatornog okvira za elektroničke komunikacije unutar Europske unije. Naime, unaprijeđena cyber sigurnost ne odnosi se samo na zaštitu digitalnih sustava od prijetnji, već i na održavanje stalne operativnosti i pouzdanosti tih sustava, čak i u slučaju potencijalnih napada ili problema.

Koncept *securability*, odnosno osigurivost stoga prepoznaje potrebu za robustnim mjerama koje ne samo da štite sustave od napada, već osiguravaju i njihov kontinuirani rad. Ovaj pristup prepoznaje da su prekidi u radu kritične infrastrukture gotovo jednako štetni kao i izravni cyber napadi, a ponekad i više. Posebno je važno primijeniti koncept *securability* na nove tehnologije poput 5G. Kako Rogalski (2021) i Gur (2022) ističu, razvoj 5G tehnologije donosi nove izazove kada je riječ o cyber sigurnosti. S obzirom na to da 5G omogućava veću povezanost i brži prijenos podataka, potencijalni cyber napadi mogu imati dalekosežne i devastirajuće posljedice. Ova priznanja i poboljšanja u NIS 2 Direktivi, poput fokusa na *securability* i prihvaćanja izazova koje donose nove tehnologije, pokazuju kako EU aktivno prati razvoj digitalne sfere i prilagođava svoj pravno-regulatorni okvir kako bi osigurala najvišu razinu cyber sigurnosti. Izazovi digitalne sfere su brojni i raznovrsni, od brze promjene tehnologija i pristupa do konstantne prijetnje cyber napadima. Prema tome, Markopoulou i Papakonstantinou (2020) ističu da je neophodan jedinstven i koherentan pristup zaštiti kritične infrastrukture. NIS 2 Direktiva ima velik značaj u oblikovanju takvog pristupa unutar EU. Ova Direktiva ne samo da prepoznaje i adresira prijetnje i izazove koje donosi digitalno doba, već i postavlja obvezne mjere zaštite i odgovornosti za različite sektore, potičući tako integriran pristup cyber sigurnosti. Posebno je važno istaknuti ulogu NIS 2 Direktive u sektorima poput zdravstva, koji su se pokazali posebno ranjivima na cyber prijetnje. Kako Markopoulou i Papakonstantinou (2020) ističu, regulacija kibernetičke sigurnosti u ovom sektoru je od iznimnevažnosti, a nedostatak adekvatne zaštite može imati dalekosežne posljedice ne samo za zdravstvene sustave, već i za opće dobro. Direktiva NIS 2 postavlja visoke standarde zaštite u sektoru zdravstva, uključujući obavezno izvještavanje o incidentima, stroge mjere za upravljanje rizicima i zahtjeve za redovito testiranje sigurnosti. Ove mjere pružaju osnovu za stvaranje jakog i otpornog zdravstvenog sektora koji može odgovoriti na stalno evoluirajuće cyber prijetnje. Sve ove navedene mjere ukazuju na to kako se NIS 2 Direktiva bavi složenošću i raznolikošću izazova s kojima se susreće digitalna sfera, i kako njen integrirani pristup ima potencijal osigurati visoku razinu sigurnosti mrežnih i informacijskih sustava na razini cijele Unije.

Iako predstavljaju bitan korak prema poboljšanoj cyber sigurnosti na razini EU, Direktive NIS 1 i NIS 2 donose sa sobom brojne izazove kada je riječ o njihovoj implementaciji.

Ducuing (2021) naglašava kompleksnost primjene pravila o prevalenciji unutar NIS direktiva, koja se odnosi na situacije kada se dvije ili više direktiva odnose na isto pitanje. U takvim situacijama, pravilo prevalencije propisuje koja će direktiva imati prednost. Ducuing koristi Cooperative Intelligent Transport Systems (C-ITS) kao studiju slučaja, pokazujući kako primjena pravila prevalencije može biti složena i zahtijevati pažljivo razmatranje, posebno kada je riječ o sektorima koji se brzo razvijaju kao što je transport. S druge strane, Markopoulou (2021) ističe potrebu za daljnjim regulacijama u području cyber osiguranja. Iako NIS 2 Direktiva predstavlja važan korak naprijed u regulaciji cyber sigurnosti, Markopoulou argumentira da će biti potrebne dodatne mjere kako bi se osigurao adekvatan nivo cyber osiguranja, a time i zaštitio integritet digitalnih sustava i mreža na razini cijele EU.

Nadalje, Papakonstantinou (2022) prepoznaje potrebu za priznavanjem novog prava na cyber sigurnost. Prema njemu, ovakav pravni okvir bi osigurao bolju zaštitu pojedinaca i organizacija od cyber prijetnji i omogućio efikasnije sudjelovanje svih dionika u stvaranju sigurnijeg digitalnog okruženja. Sve ovo ukazuje na to da, iako Direktive NIS 1 i NIS 2 predstavljaju izniman napredak, još uvijek postoje brojni izazovi i pitanja koja treba riješiti kako bi se osigurala potpuna i učinkovita zaštita kritične infrastrukture u digitalnoj sferi na razini EU.

U kontekstu energetskog sektora, Mateska, Krstevski i Borozan (2021) ističu važnost poboljšanja postupaka i praksi operatora sustava za prijenos električne energije u jugoistočnoj Europi kako bi se ublažile cyber sigurnosne prijetnje, a Naarttijärvi (2018) naglašava potrebu za uravnoteženjem zaštite podataka i privatnosti, posebno u slučaju sustava senzora za sigurnost informacija. Implementacija politike i zakonodavstva EU u vezi s cyber sigurnosti nije samo tehničko pitanje, već i pitanje institucionalnog dizajna i strateškog nadzora. Prema ENISI, 2023 godine, potpora ovim implementacijskim procesima ključna je za ostvarenje ciljeva NIS 2 Direktive. Izgradnja učinkovitog institucionalnog okvira za ovu svrhu zahtijeva kombinaciju tehničke ekspertize, zakonodavne stručnosti i strateškog pristupa. Ova potreba za institucionalnim inovacijama još je više naglašena u izvještaju Montija i de Streela (2022) za Centre on Regulation in Europe (CERRE). Autori naglašavaju kako poboljšanje dizajna institucija EU nije samo nužno za efektivniji nadzor digitalnih platformi, već i za postizanje veće digitalne suverenosti u Europi. Digitalna suverenost se odnosi na sposobnost države ili

regije da samostalno kontrolira svoju digitalnu ekonomiju i infrastrukturu, te se štiti od cyber prijetnji.

U tom kontekstu, institucionalni dizajn igra ključnu ulogu. Uspostavljanje učinkovitih mehanizama nadzora, jasno definirane regulative i snažnih institucija može pružiti stabilan okvir za upravljanje digitalnom sferom. Također, može omogućiti EU da se bolje nosi s izazovima cyber sigurnosti, unaprijedi svoju digitalnu autonomiju i zaštiti prava svojih građana u digitalnom dobu. Bez obzira na tehničke aspekte sigurnosnih mjera, institucionalna struktura i mehanizmi nadzora koji podržavaju implementaciju tih mjera su od ključne važnosti za postizanje dugoročne cyber sigurnosti.

Ukupno gledajući, NIS 1 i NIS 2 Direktive predstavljaju ključni korak prema postizanju veće cyber sigurnosti na razini EU, ali također predstavljaju izazov za organizacije koje moraju prilagoditi svoje operacije kako bi ispunile nove zahtjeve i standarde. No, unatoč ovim izazovima, jasno je da ovakav pravno-regulatorni okvir ima iznimno bitan značaj u zaštiti digitalne infrastrukture i promicanju povjerenja u digitalno okruženje.

4.4. Pravno-regulatorni okvir u Republici Hrvatskoj

Kako bi se adekvatno razumjelo stanje i budućnost elektroničkih komunikacija i kibernetičke sigurnosti u Republici Hrvatskoj, nužno je razmotriti relevantni pravno-regulatorni okvir. Iako se važnost globalnih regulativa poput Direktiva NIS 1 i NIS 2 ne može zanemariti, uspješna implementacija i primjena tih direktiva uvelike ovisi o nacionalnom zakonodavstvu i regulatornim tijelima.

Pravni okvir koji oblikuje kibernetičku sigurnost u Republici Hrvatskoj temelji se na nekoliko važnih zakona. To uključuje Zakon o kibernetičkoj sigurnosti ključnih usluga i davatelja digitalnih usluga i Zakon o elektroničkim komunikacijama, koji predstavljaju dvije glavne osi regulative na ovom području. Osim toga, određene odredbe Kaznenog zakona također igraju bitnu ulogu u regulaciji i sankcioniranju cyber kriminaliteta.

Uz to, u kontekstu elektroničkih komunikacija ne smije se zanemariti uloga HAKOM-a. Kao regulatorno tijelo, HAKOM igra ključnu ulogu u provedbi relevantnih zakona i politika, te osigurava stabilno i funkcionalno okruženje za razvoj tržišta elektroničkih komunikacija.

Daljnje poglavlje će detaljno analizirati svaku od ovih komponenti pravno-regulatornog okvira, kako bi se pružio dublji uvid u trenutno stanje i izazove s kojima se Republika Hrvatska susreće na putu prema boljoj kibernetičkoj sigurnosti.

4.4.1. Analiza ključnih usluga i davatelja digitalnih usluga prema Zakonu o kibernetičkoj sigurnosti

Zakon o kibernetičkoj sigurnosti koji je donesen u Hrvatskoj 2018. godine, ujedno je i transpozicija *tzv*. NIS direktive Europske unije na nacionalnu razinu. Temeljna svrha ovog zakona jest osigurati visoku razinu kibernetičke sigurnosti prilikom pružanja usluga koje su od vitalne važnosti za funkcioniranje ključnih društvenih i gospodarskih aktivnosti. Ovaj zakon konkretno se primjenjuje na dva segmenta i to kako operatorima ključnih usluga, tako i davateljima digitalnih usluga. Operatori usluga uključuju institucije i organizacije iz kritičnih sektora, kao što su energetika, prijevoz, bankarstvo, infrastruktura financijskog tržišta, zdravstveni sektor, opskrba vodom za piće i njena distribucija. Davatelji digitalnih usluga uključuju pružatelje online tražilica, online trgovina i cloud computing usluga.

Svrha ovog zakona jest osigurati da su operatori ključnih usluga i davatelji digitalnih usluga uspostavili i održavaju odgovarajuće mjere kibernetičke sigurnosti. To uključuje, između ostalog, mjere za identifikaciju, zaštitu, otkrivanje, reagiranje i oporavak od kibernetičkih incidenata. Operatori i davatelji moraju također imati sustave za upravljanje rizicima i redovito provoditi procjene rizika. Osim toga, Zakon o kibernetičkoj sigurnosti utemeljuje i mrežu za suradnju u području kibernetičke sigurnosti, koja omogućuje razmjenu informacija o prijetnjama i incidentima između država članica EU, kako bi se osigurala koordinirana i učinkovita reakcija na kibernetičke prijetnje.

Nova NIS2 direktiva, koju je EU donijela, proširuje opseg ove obveze, te uvodi dodatne zahtjeve za subjekte obveznike. Vlada Republike Hrvatske trenutno radi na izradi novog Zakona o kibernetičkoj sigurnosti, koji će transponirati odredbe NIS2 direktive u nacionalno zakonodavstvo.

Analiza tvrtke Deloitte iz 2021. godine naglasila je koliko je Zakon o kibernetičkoj sigurnosti bitan za zaštitu i održavanje integriteta digitalnih infrastruktura. Zakon daje strukturu za osiguranje digitalnih resursa na koje društvo uvelike ovisi, poput energetske mreže, financijskih usluga, zdravstvenog sektora i ostalih ključnih sektora.

Obveze koje taj Zakon nameće od vitalne su važnosti za osiguranje kibernetičke sigurnosti. Između ostalog, Zakon propisuje mjere za sprječavanje kibernetičkih incidenata, ali i načine na koje se organizacije moraju odazvati u slučaju da dođe do takvih incidenata. Osim toga, važno je naglasiti da državne institucije, pravne osobe i institucije koje provode ovaj zakon imaju priliku natjecati se za sredstva iz Fonda za povezivanje Europe (CEF - Connecting Europe Facility). Ovaj fond osigurava financiranje za projekte unutar Europske unije koji promiču rast, radna mjesta i konkurentnost kroz ciljana infrastrukturna ulaganja. Sredstva iz ovog fonda mogu biti posebno korisna za pomoć u pokrivanju troškova implementacije mjera kibernetičke sigurnosti koje Zakon zahtijeva. Na primjer, sredstva se mogu koristiti za kupnju potrebne opreme, unapređenje postojeće infrastrukture, obuku osoblja ili zapošljavanje stručnjaka za kibernetičku sigurnost.

Zakon o kibernetičkoj sigurnosti i njegova provedba od vitalne su važnosti za održavanje stabilnosti i sigurnosti digitalnih usluga na koje se danas uvelike oslanja društvo, a sredstva dostupna kroz CEF fond mogu pomoći u ostvarivanju tih ciljeva.

Međutim, primjena Zakona o kibernetičkoj sigurnosti u Republici Hrvatskoj naišla je na brojne izazove. Između ostalog, uočen je nedostatak resursa među tijelima odgovornim za provedbu ovog zakona. To se odnosi kako na financijske resurse, tako i na ljudske resurse, odnosno, na stručnjake za kibernetičku sigurnost koji mogu pratiti i provoditi mjere koje zakon propisuje. Također, evidentirano je da se mjere kibernetičke sigurnosti koje propisuje Zakon ne primjenjuju u dovoljnoj mjeri na strani obveznika, to jest, kod operatora ključnih usluga i davatelja digitalnih usluga. To znači da su mjere zaštite od kibernetičkih napada i prijava takvih incidenata na neodgovarajućoj razini. Uz to, postoji izazov u pogledu transparentnosti i obavještavanja nadležnih tijela o kibernetičkim incidentima. Isto tako je primijećeno da se Zakon primjenjuje prilično usko, konkretno na onaj dio poslovnog procesa i pripadajući informacijski sustav operatora koji predstavlja ključnu uslugu. Ovakva uska primjena Zakona može rezultirati neadekvatnom zaštitom na nacionalnoj razini, jer ne obuhvaća sve aspekte poslovanja i digitalne infrastrukture koji mogu biti podložni kibernetičkim napadima.

Sve navedeno ukazuje na potrebu za daljnjim usklađivanjem i prilagođavanjem Zakona o kibernetičkoj sigurnosti, s ciljem njegove efikasnije provedbe. Pritom bi se trebalo voditi računa o osiguranju dodatnih resursa, jačanju kapaciteta obveznika za primjenu mjera zaštite, kao i širenju opsega primjene Zakona, kako bi se postigla potrebna razina kibernetičke sigurnosti na nacionalnoj razini.

Nova NIS2 direktiva koju je donijela EU predstavlja značajan korak naprijed u pogledu kibernetičke sigurnosti. Uzimajući u obzir probleme s kojima su se suočile države članice tijekom primjene prethodne direktive, NIS2 unosi brojne novine s ciljem poboljšanja postojećeg stanja. Prvo, NIS2 direktiva proširuje broj sektora i podsektora koji se smatraju ključnim za održavanje kibernetičke sigurnosti. Time se osigurava da se šira paleta industrija i usluga bavi ovom važnom temom. Ovo proširenje pridonosi jačanju otpornosti čitave digitalne ekonomije na kibernetičke prijetnje, a ne samo pojedinih sektora koji su ranije bili identificirani kao ključni. Drugo, NIS2 direktiva uvodi promjenu pristupa kibernetičkoj sigurnosti. Umjesto da se fokus stavlja isključivo na ključne usluge, nova direktiva naglašava važnost kibernetičke sigurnosti u cjelokupnom poslovanju svakog subjekta obveznika. To znači da se više ne promatraju samo pojedini, ključni segmenti poslovanja, već se procjenjuje kibernetička sigurnost cijelog poslovnog procesa. Ovaj integrativni pristup omogućuje bolje prepoznavanje i rješavanje potencijalnih slabosti u sigurnosnim sustavima. Također, NIS2 direktiva uvodi strože zahtjeve za incident management i obavezno izvješćivanje o incidentima, kao i veće kazne za neusklađenost sa zahtjevima direktive. Cilj ovih mjera je osigurati brže i učinkovitije reagiranje na kibernetičke incidente te ohrabriti subjekte obveznike da pojačaju svoje napore na području kibernetičke sigurnosti.

NIS2 direktiva predstavlja temeljni okvir na temelju kojeg će države članice razvijati i primjenjivati svoje nacionalne propise, uključujući i Republiku Hrvatsku koja već radi na novom Zakonu o kibernetičkoj sigurnosti.

U skladu s novom NIS2 direktivom, Vlada Republike Hrvatske započela je rad na izradi novog Zakona o kibernetičkoj sigurnosti. Ova značajna zakonodavna aktivnost ima za cilj prevesti odredbe NIS2 direktive u kontekst nacionalnog zakonodavstva, usklađujući time hrvatski pravni okvir s najnovijim europskim standardima na području kibernetičke sigurnosti.

Novi Zakon o kibernetičkoj sigurnosti predstavljat će sveobuhvatan i učinkovit okvir za upravljanje kibernetičkom sigurnošću, kojim će se obuhvatiti sve relevantne sektore i podsektore unutar nacionalnih granica. Zakon neće biti usmjeren samo na ključne usluge, već će obuhvatiti cjelokupno poslovanje subjekata obveznika, naglašavajući pritom važnost kontinuiranog rada na održavanju i unaprjeđenju kibernetičke sigurnosti.

Novim Zakonom o kibernetičkoj sigurnosti osigurat će se detaljni okviri za sigurnosne procese unutar organizacija, od identifikacije i procjene rizika, do uspostave sigurnosnih mjera i

postupanja u slučaju kibernetičkih incidenata. Također, planira se jačanje kapaciteta nadležnih tijela za nadzor nad provedbom zakona, uključujući i bolje resursiranje tih tijela.

Kroz novi Zakon, Republika Hrvatska će osnažiti svoju sposobnost zaštite kritične infrastrukture od kibernetičkih prijetnji i osigurati učinkovito upravljanje kibernetičkom sigurnošću, u skladu s direktivama EU-a. Na taj će način zemlja unaprijediti svoj nacionalni kibernetički prostor, ali i pridonijeti stvaranju sigurnijeg kibernetičkog okruženja unutar cijele EU-e.

Vlada Republike Hrvatske već je prepoznala potrebu za povećanjem kibernetičke sigurnosti u zemlji i pokrenula je niz inicijativa usmjerenih na postizanje tog cilja. Izrada novog Zakona o kibernetičkoj sigurnosti samo je jedan dio ovog šireg napora. Novi Zakon o kibernetičkoj sigurnosti cilja na kreiranje robusnog i učinkovitog okvira za upravljanje kibernetičkom sigurnošću u Hrvatskoj, u skladu s novim zahtjevima NIS2 direktive. Pored toga, novi zakon će obuhvatiti široki spektar sektora i podsektora, proširujući tako domet kibernetičke sigurnosti na nacionalnoj razini.

Zakon će također poticati jaču suradnju između različitih dionika u području kibernetičke sigurnosti, uključujući javni i privatni sektor. Ovo će omogućiti bolje dijeljenje informacija i najbolje prakse, kao i koordinirani odgovor na kibernetičke prijetnje. S obzirom na rastuću važnost digitalne ekonomije i potencijalne prijetnje koje kibernetički napadi predstavljaju, novi Zakon o kibernetičkoj sigurnosti je od iznimne važnosti. Očekuje se da će novi zakon znatno pridonijeti jačanju kibernetičke sigurnosti u Hrvatskoj, pružajući jaču zaštitu ključnih digitalnih infrastruktura i usluga, kao i osiguravajući usklađenost s najnovijim EU standardima i direktivama.

4.4.2. Zakon o elektroničkim komunikacijama

U ovom poglavlju, fokus je stavljen na Zakon o elektroničkim komunikacijama (ZEK). Ovaj zakon, koji služi kao temelj za regulaciju elektroničkih komunikacija na nacionalnoj razini, obuhvaća širok spektar pitanja vezanih za elektroničke komunikacijske mreže, usluge i korisnike. Potrebno je naglasiti da su početne teme ZEK-a već obrađene u okviru poglavlja 4.1. pod nazivom *Prikaz tržišta elektroničkih komunikacija*. Poglavlje 4.1. pružilo je sveobuhvatan

pregled trenutačnog stanja na tržištu elektroničkih komunikacija, analizirajući trendove, aktere i izazove.

No, unatoč tome što su neke teme već obrađene, ZEK nudi daljnje uvide u načine na koje se reguliraju elektroničke komunikacije. To uključuje, ali nije ograničeno na, odredbe o pristupu i međusobnoj povezanosti mreža, pravima korisnika, upravljanju spektrom, sigurnosti mreža i privatnosti korisnika. ZEK postavlja i okvir za nadzor nad provođenjem i poštivanjem pravila, navodeći mehanizme za kontrolu i sankcioniranje povreda.

4.4.3. Analiza zakonskih članaka vezanih za cyber sigurnost u novom Kaznenom zakonu

U Glavi XXV. Novog Kaznenog zakona (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22) detaljno su opisana kaznena djela koja se odnose na cyber sigurnost. Prema izvorima Škrtića (2012), stari Kazneni zakon iz 1997. godine zamijenjen je ovim novim, čija primjena počinje 2013. godine. Novi Kazneni zakon donosi nekoliko bitnih odredbi koje se odnose na zaštitu računalnih sustava, programa i podataka. Članak 266. opisuje kaznena djela koja uključuju neovlašteni pristup računalnim sustavima ili podacima, s mogućom kaznom zatvora do jedne godine, a do tri godine ukoliko se djelo odnosi na sustave državne vlasti ili javne ustanove.

Članak 267. se odnosi na ometanje rada računalnih sustava, dok članak 268. postavlja pravni okvir za kaznena djela koja uključuju oštećenje računalnih podataka. Prema Škrtiću (2012), ranije kaznene odredbe su bile smještene u Glavi XVII., no sada su izdvojene i uvrštene u ovu novu Glavu XXV. koja se bavi cyber sigurnošću.

Članci 269. i 270. definiraju neovlašteno presretanje računalnih podataka i računalno krivotvorenje, dok članak 271. tretira računalnu prijevaru. U članku 272. se opisuje zloporaba naprava, a članak 273. se bavi teškim kaznenim djelima protiv računalnih sustava, programa i podataka.

Važno je napomenuti da, iako Novi Kazneni zakon donosi novine u kontekstu cyber sigurnosti, Škrtić (2012) navodi da ne uvodi bitne promjene u definiranju kaznenih djela računalnog kriminaliteta, niti značajniju usklađenost s međunarodnim pravnim izvorima.

U svakom slučaju, ova Glava XXV. Kaznenog zakona predstavlja važan okvir za pravnu zaštitu računalnih sustava i podataka u Republici Hrvatskoj, postavljajući jasne pravne granice koje štite integritet i sigurnost cyber prostora.

4.4.4. Uloga i nadležnosti HAKOM-a

HAKOM je nacionalna regulatorna agencija sa sjedištem u Zagrebu. Agencija djeluje kao nezavisna i neprofitna pravna osoba s javnim ovlastima, a njen rad je javan. Osnivač HAKOM-a je Republika Hrvatska, a osnivačka prava ostvaruju Hrvatski sabor i Vlada Republike Hrvatske, kojima HAKOM odgovara za svoj rad.

Upravljačku funkciju u HAKOM-u ostvaruje Vijeće HAKOM-a, sastavljeno od pet članova, uključujući predsjednika i zamjenika predsjednika. Članovi Vijeća imenuju se na prijedlog Vlade Republike Hrvatske, a mandat im traje pet godina. Ravnatelja stručne službe, zadužene za stručne, administrativne i tehničke poslove, imenuje Vijeće HAKOM-a.

HAKOM-ove nadležnosti propisane su Zakonom o elektroničkim komunikacijama, Zakonom o poštanskim uslugama i Zakonom o regulaciji tržišta željezničkih usluga i zaštiti prava putnika u željezničkom prijevozu. Jedan od bitnih zadataka HAKOM-a jest dodjela RF spektra za mreže pokretnih komunikacija, posebno u kontekstu implementacije 5G tehnologije. Kao regulatorno tijelo, HAKOM je nadležan za planiranje i dodjelu radiofrekvencijskog spektra, uključujući i odabir načina dodjele za 5G mreže. Također, određuje uvjete koje će budući nositelji dozvola morati ispunjavati. Kontinuirano radi na identifikaciji mogućih izazova i prepreka za uspješnu implementaciju 5G-a u Republici Hrvatskoj, s ciljem njihovog rješavanja.

Tijekom 2021. godine, HAKOM je proveo proces javne dražbe za dodjelu frekvencijskih pojaseva 700 MHz, 3600 MHz i 26 GHz za 5G uporabu. Izdane dozvole vrijede 15 godina za sva područja, osim za Međimursku i Varaždinsku županiju, gdje su iznimno izdane na 13 godina.

Kada trenutno važeće dozvole isteknu 2024. godine, HAKOM će pokrenuti novi postupak javne dražbe za njihovu ponovnu dodjelu. Ovim postupcima osigurava se kontinuitet rada mreža javnih pokretnih komunikacija i pružanja usluga krajnjim korisnicima uz regulatornu predvidljivost.

Dodjela frekvencija za 5G uporabu je od iznimnog značaja za podršku daljnjem razvoju digitalnih usluga i infrastrukture u Republici Hrvatskoj. Ova frekvencija omogućava brzi bežični pristup internetu s velikim kapacitetima podataka, niskim kašnjenjem i visokom pouzdanošću. To je od velikog značaja za podršku razvoju digitalne ekonomije, uključujući IoT, autonomna vozila, telemedicinu, pametne gradove i druge napredne tehnologije.

Kada dozvole za upotrebu frekvencijskih pojaseva 800 MHz, 900 MHz, 1800 MHz, 2100 MHz i 2600 MHz isteknu 2024. godine, HAKOM planira provesti novi postupak javne dražbe za dodjelu prava uporabe ovih frekvencijskih pojaseva. Očekuje se da će se ovim postupkom potaknuti dodatna konkurencija na tržištu, pružajući veći izbor usluga za krajnje korisnike i omogućavajući daljnje unapređenje mrežne infrastrukture u Republici Hrvatskoj. U tom kontekstu, HAKOM će nastaviti obavljati svoju regulatornu ulogu, nadgledajući ispravan tijek dražbi i provođenje uvjeta dozvola. Također će nastaviti s praćenjem performansi operatera kako bi se osiguralo da su korisnici adekvatno zaštićeni i da dobivaju usluge koje zadovoljavaju regulatorne standarde.

U okviru uloge i nadležnosti HAKOM-a, proces dodjele radiofrekvencijskog (RF) spektra za mreže pokretnih komunikacija predstavlja ključnu točku interesa. Taj proces je rezultat šestotjednog natjecanja koje je započelo 16. siječnja 2023. Dozvole za RF spektar su izdane na 15 godina za sva područja dodjele, s mogućnošću produljenja za najviše pet godina, sukladno nadnacionalnim pravilima EU-a. HAKOM-ova uspješna provedba javne dražbe frekvencijskih pojaseva 800 MHz, 900 MHz, 1800 MHz, 2100 MHz i 2600 MHz na nacionalnoj razini rezultirala je ukupnim iznosom naknada za uporabu RF spektra od 339 milijuna eura. Kroz ovaj proces, HAKOM je također odredio obvezu pokrivenosti od 99,4% stanovništva Republike Hrvatske do 31. prosinca 2029. godine, s najmanjom prijamnom razinom signala od -110 dBm.

Rezultati nadmetanja u postupku javne dražbe za frekvencijski pojas 800 MHz, 900 MHz, 1800 MHz, 2100 MHz i 2600 MHz na nacionalnoj razini navedeni su u sljedećoj tablici:

Tablica 1. Rezultati nadmetanja

Frekvencijski pojas	Operator	Količina spektra (MHz)	Iznos početne cijene(EUR)	Ukupni iznos naknade(EUR)
800 MHz	A1 Hrvatska	2x10	14.000.000,00	19.600.000,00
	Hrvatski Telekom	2x10	14.000.000,00	19.616.011,00
	Telemach Hrvatska	2x10	14.000.000,00	20.011.011,00
900 MHz	A1 Hrvatska	2x15	21.000.000,00	28.840.000,00
	Hrvatski Telekom	2x15	21.000.000,00	28.840.202,50
	Telemach Hrvatska	2x5	7.000.000,00	9.520.200,50
1800 MHz	A1 Hrvatska	2x25	10.000.000,00	27.340.000,00
	Hrvatski Telekom	2x30	12.000.000,00	33.020.385,00
	Telemach Hrvatska	2x20	8.000.000,00	21.910.902,00
2100 MHz	A1 Hrvatska	2x15	6.000.000,00	30.000.000,00
	Hrvatski Telekom	2x25	10.000.000,00	50.240.000,00
	Telemach Hrvatska	2x20	8.000.000,00	40.162.883,00
2600 MHz	A1 Hrvatska	2x25	3.500.000,00	3.500.000,00
	Hrvatski Telekom	2x25	3.500.000,00	3.598.000,00
	Telemach Hrvatska	2x20	2.800.000,00	2.800.000,00

Ovaj je postupak bio od posebnog značaja jer su trenutno dodijeljene dozvole za navedene frekvencijske pojaseve istjecale 2024. godine. Kroz ovu dodjelu, HAKOM je osigurao

kontinuitet rada mreža javnih pokretnih komunikacija i pružanja usluga krajnjim korisnicima uz regulatornu predvidljivost.

Ishod dražbe prikazan je u sljedećoj tablici:

Tablica 2. Ishod dražbe

Odabrani ponuđač	Područje dodjele	Količina spektra (MHz)	Iznos početna cijene (EUR)	Ukupni iznos naknade (EUR)
Digicom	Brodsko-posavska	20+10	19.000,00	19.000,00
	Krapinsko-zagorska	20	19.000,00	19.000,00
	Grad Zagreb	10+10	38.000,00	38.000,00
Markoja	Bjelovarsko-bilogorska	30+10	28.500,00	28.500,00
	Karlovačka	30	28.500,00	29.450,00
	Ličko-senjska	10	1.900,00	1.900,00
	Osječko-baranjska	30	28.500,00	28.500,00
	Požeško-slavonska	30	11.400,00	11.400,00
	Virovitičko-podravska	30+10	11.400,00	11.400,00

Također je bitno napomenuti kako je HAKOM u ovom procesu dodijelio spektar u frekvencijskom pojasu 3600 MHz koji nije bio dodijeljen u dražbi iz 2021. godine. Ova dodjela, koja se odvijala na regionalnoj (županijskoj) razini, omogućila je stvaranje poslovnih prilika za manje, regionalne operatore, te potakla raznolikost usluga i pružila veće mogućnosti izbora za krajnje korisnike.

Ukupan iznos naknada za uporabu RF spektra koji je postignut na javnoj dražbi za frekvencijski pojas 3600 MHz na regionalnoj razini iznosi 187.150 eura. Nadmetanje na regionalnoj razini odvilo se u tri kruga u glavnoj fazi nadmetanja, bez potrebe za provođenjem faze dodjele. Ukupno gledano, iznos naknada za uporabu RF spektra na nacionalnoj i regionalnoj razini koji je postignut na javnoj dražbi iznosio je 339.186.745,00 EUR. Svi prikupljeni iznosi s javne dražbe u potpunosti se uplaćuju u državni proračun, čime je HAKOM-ova uloga u regulaciji RF spektra značajno doprinijela financijskoj snazi države.

Ukupan iznos naknada za uporabu RF spektra na nacionalnoj i regionalnoj razini koji je postignut na javnoj dražbi prikazan je u tablici 3.

Tablica 3. Ukupan iznos naknada za uporabu RF spektra na nacionalnoj i regionalnoj razini koji je postignut na javnoj dražbi

Osim toga, HAKOM će nastaviti rad na promicanju konkurencije na tržištu, transparentnosti u radu operatora, i zaštiti prava korisnika. To uključuje rad na propisima koji će dodatno podržati razvoj digitalne ekonomije, kao što su pravila o dijeljenju infrastrukture, interoperabilnosti, net-neutralnosti, zaštiti podataka i sigurnosti mreže.

Jasno proizlazi da je kontinuirani rad HAKOM-a na regulaciji frekvencijskog spektra i digitalne infrastrukture od iznimne važnosti podršku digitalnoj transformaciji u Republici Hrvatskoj. Ovaj rad će omogućiti brži razvoj novih usluga, poticanje inovacija, jačanje konkurencije, poboljšanje kvalitete usluga, zaštitu korisnika, te podršku ekonomskom rastu i društvenom razvoju.

4.5. Kibernetička sigurnost u elektroničkim komunikacijama

Kako su se elektroničke komunikacije razvijale, tako su i kibernetičke prijetnje postale sve složenije i sofisticiranije. Podaci koje komuniciramo i pohranjujemo na elektronički način postali su najvažniji resursi, a time i meta kibernetičkih napada. Prema istraživanju Lia i Liu (2021), takvi napadi sve su učestaliji i sve sofisticiraniji, a uz to se šire i na nove tehnološke sfere, poput IoT-a. Kroz svoj rad, Raimundo i Albérico Travassos Rosário (2022) istaknuli su specifične izazove kibernetičke sigurnosti u kontekstu industrijskog upravljanja i primjene Iot-a. Posebno su se fokusirali na potrebu za novim sigurnosnim strategijama koje mogu efikasno se suočiti s izazovima koji dolaze s rastućom povezanošću i kompleksnošću IoT uređaja.

U sferi zaštite podataka, posebno je važan rad Malcolma Dowdena i Lucije Rubio Robustillo (2022). Oni su naglasili potrebu za povećanjem obveza i odgovornosti na razini uprave u zaštiti elektroničkih komunikacijskih mreža i usluga od kibernetičkih napada i gubitka podataka. Ovaj rad ukazuje na važnost pravnog i organizacijskog okvira u održavanju kibernetičke sigurnosti, uz tehnološke mjere.

Kada govorimo o tehnološkim mjerama, potrebno je spomenuti rad Krzysztofa Szczypiorskog (2022) koji se bavi tematikom sigurnosti u kontekstu IoT-temeljenog *cloud computinga*-računarstva u oblaku. Szczypiorski naglašava potrebu za sveobuhvatnim pristupom sigurnosti koji obuhvaća kako tehničke mjere (poput enkripcije i sigurnosnih protokola), tako i organizacijske (poput politika pristupa i edukacije korisnika).

Na kraju, ali ne manje važno, ističe se rad Waqasa Ahmada, Aamira Rasoola, Abdul Rehmana Javeda, Thara Bakera i Zunere Jalil (2022). Ovaj rad pruža opsežan pregled izazova i rješenja u području kibernetičke sigurnosti u kontekstu IoT-temeljenog cloud computinga. Autori ističu kako je unapređenje sigurnosti u ovom kontekstu kontinuiran proces koji zahtijeva stalna istraživanja, razvoj novih tehnika i strategija te suradnju među svim dionicima u svijetu informacijskih tehnologija.

U svjetlu ovih radova, može se zaključiti da je kibernetička sigurnost u elektroničkim komunikacijama višedimenzionalan i kompleksan izazov koji zahtijeva interdisciplinarni pristup. Osim što su neophodne sofisticirane tehnološke mjere, potrebna je i odgovarajuća pravna regulativa, edukacija korisnika, kao i odgovornost na svim razinama upravljanja.

U kontekstu sve veće primjene IoT-a, ovaj izazov postaje još složeniji. IoT uređaji sve su prisutniji u našim životima, a njihova povezanost s internetskim uslugama i cloud computingom otvara nove mogućnosti za kibernetičke napade. Stoga je unapređenje sigurnosti u ovom kontekstu kontinuiran proces koji zahtijeva stalna istraživanja, razvoj novih tehnika i strategija te suradnju među svim dionicima u svijetu informacijskih tehnologija, kako su to istaknuli Ahmad, Rasool, Javed, Baker i Jalil (2022). Sve ove spoznaje potiču na daljnje promišljanje i istraživanje ove teme, kao i na razvoj novih metoda, tehnika i strategija u borbi protiv kibernetičkih prijetnji. Važno je da svi dionici u ovom procesu, od pojedinaca i tvrtki do regulatornih tijela i pružatelja usluga, budu svjesni ovih izazova i aktivno sudjeluju u njihovom rješavanju.

Holistički pristup sigurnosti, kojeg su istaknuli Fischer i Walters (2019), sugerira sveobuhvatan, integriran način razmišljanja o sigurnosti. Umjesto da se fokusiraju samo na pojedinačne aspekte ili određene prijetnje, ovaj pristup zagovara da se sigurnost mora promatrati u kontekstu cijelog sustava. To uključuje tehničke mjere zaštite, ali i strategije upravljanja rizicima, politike sigurnosti, edukaciju zaposlenika i druge aspekte poslovanja. Pritom, tehnologija sama po sebi ne može osigurati potpunu zaštitu, bez obzira na to koliko je sofisticirana. Kako se tehnologija razvija, tako se razvijaju i kibernetički napadi. Stoga je važno pratiti najnovije trendove, istraživanja i razvoj na području kibernetičke sigurnosti, kako bi se na vrijeme detektirale potencijalne prijetnje i osmislile adekvatne mjere zaštite.

Istodobno, kibernetička sigurnost u elektroničkim komunikacijama postaje sve više regulirana. Primjerice, Zakon o privatnosti elektroničkih komunikacija, kako su to objasnili Malcolm Dowden i Lucia Rubio Robustillo (2022), postavlja određene obveze na dionike u ovom području, uključujući i obvezu zaštite mreža i usluga elektroničkih komunikacija od kibernetičkih napada i gubitka podataka.

Ovakav regulativni okvir postavlja novi nivo odgovornosti, posebno na razini upravljanja. Kako Dowden i Robustillo (2022) ističu, povećane obveze uključuju i odgovornost na razini upravljačkih struktura. Dakle, uključivanje uprave u procese kibernetičke sigurnosti, kao i svjesnost o njenoj važnosti, ključni su faktori u očuvanju integriteta elektroničkih komunikacija.

IoT predstavlja rastući segment digitalne tehnologije koji naglašava povezivanje svakodnevnih uređaja s internetom. Ova tehnologija donosi velike pogodnosti, ali također i nove izazove za

kibernetičku sigurnost. U radu Ricarda Jorge Raimunda i Albérica Travassosa Rosária (2022) ističe se kako sveprisutnost IoT uređaja može predstavljati potencijalne sigurnosne rizike. Svaki uređaj povezan s internetom je potencijalna točka ulaza za kibernetičke napade, a broj takvih uređaja raste eksponencijalno s razvojem IoT-a. Stoga je od vitalnog značaja osigurati robusnu kibernetičku sigurnost koja može zaštititi ovu mrežu uređaja. Waqas Ahmad i njegovi kolege (2022) posebno su istraživali izazove kibernetičke sigurnosti u kontekstu IoT-omogućenog cloud computinga. Cloud computing, ili računarstvo u oblaku, pruža brojne pogodnosti, poput povećane efikasnosti i smanjenja troškova, ali također predstavlja i izazove za sigurnost, pogotovo kada je povezan s IoT uređajima.

U svom istraživanju, Ahmad i suradnici (2022) ističu kako je osiguranje robustne kibernetičke sigurnosti u ovom kontekstu kontinuirani proces. Potrebna su stalna istraživanja i razvoj novih tehnika zaštite, kao i suradnja među svim dionicima u svijetu informacijskih tehnologija kako bi se pružila adekvatna zaštita od prijetnji koje donosi sveprisutnost IoT-a.

Krzysztof Szczypiorski je renomirani stručnjak u polju kibernetičke sigurnosti čiji rad pokriva širok spektar tema. U svom radu iz 2020. godine, Szczypiorski se bavi općim pitanjima kibernetičke (ne)sigurnosti, ističući složenost tog polja i nužnost konstantne adaptacije na novonastale izazove (Szczypiorski, 2020). S obzirom na brzi razvoj tehnologije i sofisticiranost potencijalnih napadača, sigurnosne mjere se moraju kontinuirano ažurirati i prilagođavati. Jedan od specifičnih izazova u polju kibernetičke sigurnosti na koji Szczypiorski ukazuje je mrežna steganografija, tehniku koja omogućuje prikriveno slanje informacija unutar legitimnog mrežnog prometa. U suradnji sa Smolarczykom i Pawlukom, Szczypiorski (2020) proučava ove metode i ističe potrebu za razvijanjem novih detekcijskih mehanizama kako bi se otkrile i neutralizirale ove prijetnje.

Nadalje, u kontekstu sigurnosti IoT-a, Szczypiorski u suradnji sa Chmielom, Koronom, Koziołom i Rawskim (2021) vodi diskusiju o sigurnosnim preporukama u usporedbi sa najnovijim rješenjima. Autori ističu kako su IoT uređaji posebno ranjivi na napade zbog svoje povezanosti i interaktivnosti, što zahtijeva posebne mjere zaštite.

Njihov rad naglašava važnost stalne revizije i ažuriranja sigurnosnih mjera, ali i svijesti o potencijalnim prijetnjama koje se stalno mijenjaju i evoluiraju. Kroz ovu vrstu istraživanja, jasno je da je kibernetička sigurnost dinamično i složeno polje koje zahtijeva stalnu pažnju, Analiza i implementacija profila prijetnji u realnom vremenu ključni su elementi suvremenih

strategija kibernetičke sigurnosti. Sharma, Vidalis, Menon, Anand i Kumar (2021) ističu kako poluautomatizirani pristupi omogućuju brže i učinkovitije identificiranje i neutraliziranje prijetnji. Ova vrsta pristupa pruža bolje razumijevanje aktivnosti unutar mreže, omogućuje pravovremenu detekciju neobičnih obrazaca ponašanja i potencijalnih prijetnji.

Daljnje unapređenje metoda za analizu prometa mreže temeljene na konvolucijskim neuronskim mrežama istražili su Krupski, Graniszewski i Iwanowski (2021). Ove tehnike koriste napredne algoritme za obradu velikih količina podataka, omogućujući dubinsku analizu i identifikaciju potencijalno štetnih aktivnosti. Upotrebom takvih sofisticiranih tehnika, moguće je bolje predvidjeti, detektirati i reagirati na kibernetičke prijetnje.

Ova istraživanja naglašavaju važnost inovacija i razvoja naprednih tehnika u borbi protiv kibernetičkih prijetnji. Istovremeno, ona potvrđuju kako kibernetička sigurnost u elektroničkim komunikacijama zahtijeva stalnu pažnju, investicije u tehnologiju i ljudske resurse, kao i interdisciplinarni pristup koji obuhvaća tehničke, pravne, organizacijske i druge aspekte.

Sve ovo ukazuje na to da je kibernetička sigurnost u elektroničkim komunikacijama ključna za zaštitu osjetljivih podataka, te da održavanje iste zahtijeva kontinuiran napredak u tehnologijama i strategijama. Prema istraživanju Grzesiaka, Piotrowskog, Kelnera (2021), sofisticirane taktike poput prljave konstelacije s faznim pomacima mogu biti korištene za stvaranje bežičnih prikrivenih kanala. Ovakve suptilne metode iziskuju napredne mehanizme za otkrivanje i obranu, posebno u kontekstu IoT-a.

Nadalje, rad Rastenisa, Ramanauskaite, Suzdaleva, Tunaityte, Janulevičiusa, i Čenysa (2021) pokazuje kako automatizirane metode analize mogu biti korisne u identifikaciji potencijalno štetnih poruka, poput spam-a ili phishing-a. Ovo istraživanje ističe važnost automatizacije u procesu održavanja sigurnosti elektroničkih komunikacija.

Uputno je podsjetiti se i rada Malcolma Dowdena i Lucije Rubio Robustillo (2022) koji naglašavaju ulogu obveza i odgovornosti na razini uprave u zaštiti elektroničkih komunikacijskih mreža i usluga od kibernetičkih napada i gubitka podataka. Ova perspektiva ističe kako, iako tehnologija ima ključnu ulogu u zaštiti elektroničkih komunikacija, ljudski faktor, uključujući organizacijske politike i procedure, ostaje od vitalnog značaja. S obzirom na kontinuirani rast broja uređaja povezanih na mrežu i složenost kibernetičkih prijetnji, neophodno je razvijanje strategija koje uključuju sve segmente elektroničkih komunikacija.

Kako ističu Yuchong Li i Qinghui Liu (2021), to uključuje sve od razvoja tehnoloških rješenja do obuke i edukacije korisnika o potencijalnim rizicima i najboljim praksama.

Evidentno je da je zaštita elektroničkih komunikacija od kibernetičkih napada složen i stalno evoluirajući zadatak. Kroz integraciju tehnologije, politika i praksi, te stalno unapređenje i edukaciju, može se postići viši stupanj kibernetičke sigurnosti u elektroničkim komunikacijama.

4.5.1. Najčešće vrste kibernetičkih napada

Kibernetička sigurnost je postala bitan element suvremenog digitaliziranog svijeta. Način na koji se suočavamo s kibernetičkim prijetnjama oblikuje naše društvo, ekonomiju i politiku. Između raznih oblika kibernetičkih napada, nekoliko ih se posebno ističe svojom učestalošću i potencijalnom štetom. Phishing napadi su jedan od najčešćih oblika kibernetičkih napada. Prema Valerie Thomas (2014), phishing napadi često uključuju pokušaje prijevare putem elektroničke pošte ili drugih online komunikacijskih kanala, s ciljem prikupljanja povjerljivih informacija poput korisničkih imena, lozinki ili kreditnih kartica. Naprednija forma phishing napada, poznata kao *spear-phishing*, cilja specifične pojedince ili organizacije, često s detaljno proučenim i personaliziranim pristupom.

Ransomware napadi, gdje napadači koriste maliciozni softver za šifriranje podataka žrtve i potom traže otkupninu za dešifriranje, su drugi oblik kibernetičkog napada koji je postao sve učestaliji. Kao što je opisano u radu Aslana i suradnika (2023), ovaj tip napada može uzrokovati značajnu financijsku i operativnu štetu, posebno za velike organizacije.

Napadi na IoT uređaje su također brzo rastući problem. Kako Tsiknas i suradnici (2021) navode, brojni uređaji koji su sada povezani na internet, od pametnih kućanskih uređaja do industrijske opreme, predstavljaju potencijalne ciljeve za kibernetičke napade. Ova vrsta napada može rezultirati krađom podataka, oštećenjem uređaja ili čak fizičkom štetom u slučaju napada na kritičnu infrastrukturu.

Osim toga, sve veći broj napada provodi se kroz tzv. *supply chain*, gdje napadači ciljaju dobavljače i partnere glavnih ciljeva kako bi došli do njih. Kao što Mazhar i suradnici (2023) ističu, ova strategija je posebno zlokobna jer često omogućuje napadačima da zaobiđu tradicionalne obrambene mjere ciljane organizacije.

Potrebno je spomenuti i sofisticirane APT (Advanced Persistent Threat) napade, koji često uključuju dugotrajne i ciljane kampanje koje provode vrlo sposobni napadači, ponekad čak i uz potporu države. Prema Yildirim Yayilgan i suradnicima (2022), ovi napadi su posebno opasni zbog njihove upornosti, sofisticiranosti i visokog stupnja prilagodbe. APT napadi nisu samo usmjereni na krađu podataka, već i na špijunažu ili sabotiranje kritičnih informacijskih sustava. Oni obično počinju s fazom istraživanja, gdje napadači temeljito proučavaju svoje ciljeve, slijedi faza proboja, gdje napadači koriste različite metode da prodru u mrežu cilja, a zatim faza održavanja pristupa, gdje napadači uspostavljaju "backdoors" i druge načine da ostanu u mreži unatoč pokušajima otklanjanja.

S obzirom na gore navedeno, jasno je da je kibernetička sigurnost izuzetno važna za sve aspekte suvremenog društva. Kao što navode Mishra i suradnici (2022), stvaranje učinkovitih politika kibernetičke sigurnosti složen je zadatak koji zahtijeva razumijevanje ne samo tehničkih aspekata kibernetičke sigurnosti, već i socijalnih, psiholoških i političkih čimbenika. Ovaj posao postaje sve teži s obzirom na stalnu evoluciju kibernetičkih napada. Međutim, radovi kao što su oni koje su proveli Chng i suradnici (2022), Alawida i suradnici (2022) i Varga i suradnici (2021) pružaju vrijedne uvide u ovo područje, ukazujući na potrebu za sveobuhvatnim pristupom koji uključuje ne samo tehničke mjere zaštite, već i edukaciju korisnika, regulative i zakone, te suradnju na globalnoj razini. S obzirom na široku prirodu kibernetičke sigurnosti, potrebno je neprestano istraživanje i inovacije kako bi se ostalo ispred kibernetičkih prijetnji. Alguliyev, Imamverdiyev i Sukhostat (2018) ističu važnost istraživanja i razvoja u području kibernetičke sigurnosti, posebno u kontekstu zaštite kritične infrastrukture. Ben-Asher i Gonzalez (2015) dodatno naglašavaju ulogu korisničkog obrazovanja i svijesti o kibernetičkoj sigurnosti kao ključne komponente u borbi protiv kibernetičkih prijetnji.

Tehseen Mazhar i njegov tim (2023) u svojoj studiji detaljno proučavaju specifične prijetnje koje se odnose na pametne mreže, posebno ukazujući na složenost i ozbiljnost takvih napada. Pametne mreže, kao integralni dio moderne infrastrukture, uvelike povećavaju učinkovitost i fleksibilnost isporuke energije, ali su s druge strane i iznimno atraktivan cilj za kibernetičke napadače. Svjesni ovog problema, Mazhar i njegov tim ističu potencijal metoda strojnog učenja i blockchain tehnologije u obrani od ovakvih napada. Strojno učenje može pružiti snažne alate za detekciju anomalija i potencijalnih napada, dok blockchain tehnologija može pružiti robustan i transparentan način za evidentiranje transakcija, čime se smanjuje rizik od manipulacija.

U isto vrijeme, Sule Yildirim Yayilgan i suradnici (2022) istražili su digitalne trafostanice u Norveškoj, fokusirajući se na potencijalne kibernetičke prijetnje kojima su izloženi. Njihova studija ukazuje na to da su sofisticirane infrastrukture, poput digitalnih trafostanica, posebno osjetljive na kibernetičke napade. Digitalne trafostanice su važan dio energetske infrastrukture, omogućavajući distribuciju električne energije na velika područja. Međutim, njihova digitalna priroda ih čini ranjivima na različite vrste kibernetičkih napada, od krađe podataka do potencijalno katastrofalnih napada na samu operativnost trafostanica. Yayilgan i njegov tim ukazuju na nužnost kontinuiranog razvoja i primjene sofisticiranih obrambenih mjera kako bi se očuvala sigurnost ovih kritičnih infrastruktura.

Ove studije ukazuju na to da kibernetičke prijetnje predstavljaju ozbiljan rizik za moderne infrastrukture, ali također ističu i mogućnosti koje moderne tehnologije pružaju u borbi protiv ovih prijetnji. Potrebno je stalno istraživanje i inovacija kako bi se održao korak s kibernetičkim napadačima i osigurala sigurnost naših digitalnih infrastruktura.

Alshaibi i suradnici (2022) pružili su ključan doprinos u razumijevanju kako setovi podataka mogu utjecati na efikasnost obrane kibernetičke sigurnosti. U svojoj su studiji usporedili dostupne setove podataka o kibernetičkoj sigurnosti, s ciljem određivanja njihove korisnosti u sprječavanju kibernetičkih napada. Kroz ovu analizu, tim je dokazao da kvaliteta i sveobuhvatnost informacija imaju ključnu ulogu u pravovremenom otkrivanju i sprječavanju napada. Stoga, setovi podataka koji se koriste u kibernetičkoj sigurnosti moraju biti ažurirani, precizni i sveobuhvatni kako bi se pravilno identificirale i sprječavale prijetnje.

S druge strane, Tsiknas i suradnici (2021) usmjerili su se na prijetnje koje industrijski Internet stvari (IIoT) donosi. IIoT, koji obuhvaća sve od pametnih proizvodnih linija do automatiziranih sustava upravljanja, donosi brojne prednosti u smislu učinkovitosti i fleksibilnosti, ali također otvara vrata za nove vrste kibernetičkih napada. Tsiknas i njegov tim naglašavaju potrebu za razvojem specifičnih mjera sigurnosti koje su prilagođene ovom rastućem segmentu tehnologije. Oni ističu da je razumijevanje specifičnih prijetnji koje IIoT donosi, ključno za razvoj učinkovitih metoda zaštite. Iz ovih studija vidljivo je da je zaštita od kibernetičkih napada složen proces koji zahtijeva pravovremeno i precizno informiranje, kao i razumijevanje specifičnosti tehnoloških domena koje treba zaštititi. Bez toga, obrana od kibernetičkih napada može biti neučinkovita, ostavljajući sustave ranjivima na prijetnje.

Ahmad i suradnici (2022) pružili su opsežnu analizu problema kibernetičke sigurnosti u kontekstu Internet of Things (IoT) i cloud computinga. Njihova studija upućuje na niz izazova koji proizlaze iz ovog spoja tehnologija. IoT uređaji, s njihovom sve većom prisutnošću i povezanošću, predstavljaju potencijalne točke ulaza za kibernetičke napade. S druge strane, cloud computing, iako omogućuje fleksibilnost i skalabilnost, također predstavlja potencijalne ranjivosti, pogotovo kada je u pitanju zaštita podataka.

Ahmad i suradnici istaknuli su važne izazove u ovom kontekstu, uključujući potrebu za boljim strategijama autentifikacije, jačanjem sigurnosti podataka u tranziciji i skladištenju, kao i potrebu za unapređenjem sigurnosnih protokola u kontekstu IoT uređaja. Ovi izazovi, prema autorima, zahtijevaju sveobuhvatni pristup koji uključuje tehničke, organizacijske i pravne mjere. Studija Ahmada i suradnika naglašava složenost kibernetičke sigurnosti u doba IoT-a i cloud computinga, ali isto tako nudi moguće strategije za rješavanje ovih izazova. Njihov rad služi kao korisna polazna točka za daljnje istraživanje i implementaciju mjera zaštite u ovom dinamičkom području.

Istraživanja koja su proveli Yuchong Li i Qinghui Liu (2021), Kathrin Reibelt i Veit Hagenmeyer (2020), Maria Bada i Jason R.C. Nurse (2020), Andreea Bendovschi (2015) te Julian Jang-Jaccard i Surya Nepal (2014) pružaju daljnje bitne uvide u suvremene kibernetičke prijetnje i strategije zaštite.

Yuchong Li i Qinghui Liu (2021) istražuju kako kibernetički napadači koriste sofisticirane metode poput deep learninga da unaprijede svoje napadačke taktike. Prepoznajući ove strategije, istraživači mogu razviti učinkovite protumjere i obrambene mehanizme.

Kathrin Reibelt i Veit Hagenmeyer (2020) pružaju analizu sigurnosti kritične infrastrukture, posebno usmjerenu na energetski sektor. Njihova studija naglašava važnost zaštite ovih ključnih resursa od kibernetičkih napada i predlaže nove pristupe za njihovu obranu.

Maria Bada i Jason R.C. Nurse (2020) usredotočuju se na ljudski faktor u kibernetičkoj sigurnosti. Njihova studija ističe koliko je važna edukacija i svijest korisnika u sprječavanju kibernetičkih napada.

Andreea Bendovschi (2015) proučava ekonomski aspekt kibernetičke sigurnosti. U svom radu naglašava kako su kibernetički napadi postali ne samo tehnološka, već i ekonomska prijetnja, ukazujući na potrebu za boljom ekonomskom analizom u ovoj sferi.

Julian Jang-Jaccard i Surya Nepal (2014) istražuju pitanja privatnosti i sigurnosti u cloud computingu. Uz brojne prednosti koje cloud computing pruža, postoje i ozbiljne sigurnosne prijetnje koje moraju biti adresirane. Ova istraživanja zajedno pružaju sveobuhvatan pregled trenutnih kibernetičkih prijetnji i obrambenih strategija, pokazujući koliko je važno konstantno ažuriranje znanja i praksi u ovom dinamičkom polju.

Uistinu, kibernetička sigurnost nije samo tehničko pitanje, već i kompleksna problematika koja obuhvaća psihološke, socijalne i druge aspekte.

Samuel Chng i suradnici (2022) provode detaljno istraživanje o ljudskom faktoru u kibernetičkoj sigurnosti. Razmatraju ulogu ljudskog ponašanja, odlučivanja i percepcije rizika u kontekstu kibernetičkih napada. Njihova studija ukazuje na potrebu za boljom edukacijom i osvješćivanjem o sigurnosnim prijetnjama.

Moatsum Alawida i suradnici (2022) bave se problematikom socijalnih medija kao kanala za kibernetičke napade. Njihova studija istražuje kako napadači koriste socijalne mreže za širenje zlonamjernog softvera i za krađu podataka. Naglašavaju važnost poboljšane zaštite korisnika na ovim platformama.

Stefan Varga i suradnici (2021) istražuju kako su novi razvoji u tehnologiji poput interneta stvari (IoT) i cloud computinga otvorili nove prilike za kibernetičke napadače. S druge strane, ove tehnologije također omogućuju nove strategije obrane.

Rasim Alguliyev, Yadigar Imamverdiyev i Lyudmila Sukhostat (2018) istražuju kako se informacijski sustavi mogu zaštititi od različitih vrsta napada. Njihov rad ukazuje na raznolikost tehnika koje napadači koriste i na potrebu za sveobuhvatnom strategijom zaštite.

Noam Ben-Asher i Cleotilde Gonzalez (2015) usredotočuju se na ljudski aspekt kibernetičke sigurnosti, istražujući kako se ljudska pogreška i zloupotreba mogu minimizirati kroz bolje obrazovanje i dizajn interfejsa.

Sve ove studije skupa ukazuju na širinu i kompleksnost problematike kibernetičke sigurnosti. Od tehnologije i infrastrukture do ljudskog ponašanja i socijalnih medija, svaki aspekt predstavlja potencijalnu metu i zahtijeva stalno praćenje i poboljšanje strategija obrane.

Studija koju su proveli Samuel Chng i suradnici (2022) predstavlja temeljitu analizu različitih tipova hakera, uključujući njihove motive, strategije i tehniku napada. Cilj ovog istraživanja je

produbiti razumijevanje potencijalnih prijetnji u kibernetičkom prostoru, što je bitno za izgradnju učinkovitih obrambenih strategija.

Autori su klasificirali hakere prema različitim kategorijama uključujući njihove motivacije, koje mogu varirati od financijske dobiti, političkih ciljeva, pa do jednostavno želje za demonstracijom svojih tehničkih vještina. Razumijevanje ove motivacije može pomoći u predviđanju mogućih napada i izgradnji prilagođenih obrambenih mehanizama. Također, Chng i njegovi suradnici istražili su strategije koje koriste različiti tipovi hakera. To uključuje tehnike kao što su spear-phishing, gdje napadači ciljaju specifične individue ili organizacije, ili napade na usluge, gdje je cilj preopteretiti mrežu ili server kako bi se onemogućila njegova usluga. U svjetlu ovog istraživanja, jasno je da razumijevanje hakera - njihovih motivacija, strategija i tehnika ima bitan značaj u razvoju učinkovitih obrambenih strategija. Ovo istraživanje pruža temelje za razumijevanje ove složene problematike i potiče daljnja istraživanja u ovoj domeni.

U studiji koju su proveli Moatsum Alawida i suradnici (2022), autori detaljno analiziraju utjecaj pandemije Covid-19 na pitanja kibernetičke sigurnosti. Razmatrajući kako hitne i neočekivane globalne situacije mogu dramatično promijeniti krajolik kibernetičke sigurnosti, autori osvježavaju naše razumijevanje prirode kibernetičkih prijetnji i izazova. Njihova studija se posebno usredotočuje na način na koji pandemija Covid-19 stvara nove mogućnosti za kibernetičke napade. S obzirom na to da su mnoge organizacije tijekom pandemije brzo prešle na rad na daljinu, postojeće mrežne infrastrukture često nisu bile adekvatno prilagođene da se nose s povećanim sigurnosnim rizicima. Ovaj nagli prijelaz na online radne procese, prema autorima, otvorio je nove prilike za napade, uključujući phishing, malware i napade na konferencijske platforme. Studija ističe koliko je važno za organizacije da budu spremne na brze promjene koje mogu imati veliki utjecaj na kibernetičku sigurnost. Autori naglašavaju važnost planiranja za krizne situacije, uključujući pandemije, prirodne katastrofe ili druge neočekivane događaje koji bi mogli prisiliti organizacije da brzo prenesu svoje operacije na internet. Ova studija pruža važan uvid u prilagodljivost kibernetičkih prijetnji i potrebu za stalnim nadzorom i ažuriranjem sigurnosnih strategija.

U radu Stefana Varge i suradnika (2021), autori analiziraju percepciju kibernetičkih prijetnji i upravljanje rizikom unutar švedskog financijskog sektora. Ova specifična studija ilustrira koliko sektorske specifičnosti mogu utjecati na prirodu kibernetičkih napada i potrebne strategije zaštite. Financijski sektor, zbog svoje važnosti u svjetskoj ekonomiji i visoke vrijednosti podataka koji se u njemu obrađuju, posebno je privlačna meta za kibernetičke

napadače. Varga i suradnici ukazuju na to da se u ovom sektoru susrećemo s jedinstvenim izazovima u pogledu kibernetičke sigurnosti, među kojima su sofisticirani ciljani napadi, potreba za visokom dostupnošću sustava i strogi regulatorni zahtjevi. Autori također ističu da je upravljanje rizicima bitan aspekt borbe protiv kibernetičkih prijetnji u financijskom sektoru. Kako bi uspješno upravljali rizicima, financijske institucije moraju provesti temeljite procjene rizika, razviti sveobuhvatne planove zaštite, redovito provoditi revizije i testove te kontinuirano pratiti i ažurirati svoje sigurnosne mjere (2021).

Na kraju, ova studija naglašava potrebu za prilagođenim strategijama zaštite. Kako se kibernetičke prijetnje neprestano mijenjaju i evoluiraju, strategije zaštite moraju biti fleksibilne i prilagodljive. To znači da se moraju temeljiti na dubokom razumijevanju specifičnih prijetnji s kojima se suočava svaki sektor, kao i na tehnologijama i postupcima koje taj sektor koristi (Varga et al., 2021).

Rasim Alguliyev, Yadigar Imamverdiyev i Lyudmila Sukhostat (2018) u svojoj studiji posvećuju pažnju sigurnosnim problemima cyber-fizičkih sustava (CPS). Cyber-fizički sustavi predstavljaju integraciju računalnih resursa s fizičkim procesima, stvarajući složene mreže koje donose brojne pogodnosti, ali i predstavljaju potencijalne mete za kibernetičke napade. Njihov rad ukazuje na to da suvremena digitalna infrastruktura, iako donosi značajne prednosti u pogledu efikasnosti i povezanosti, također nosi sa sobom i brojne sigurnosne izazove. Autori naglašavaju da su CPS-ovi posebno ranjivi zbog svoje inherentne kompleksnosti i sveobuhvatnosti, kao i zbog velike raznolikosti ugrađenih uređaja i sustava.

Alguliyev, Imamverdiyev i Sukhostat analiziraju različite vrste prijetnji koje se odnose na CPS, uključujući fizičke napade, napade na komunikacijske kanale, napade na softver i druge. Također razmatraju različite strategije zaštite koje se mogu primijeniti na CPS, uključujući metode detekcije napada, kriptografske tehnike, tehnike autentifikacije i autorizacije, kao i metode za povrat podataka. Studija naglašava važnost multidisciplinarnog pristupa u zaštiti CPS-a, uključujući stručnost iz područja računalnih znanosti, inženjeringa, fizike i drugih relevantnih disciplina. Također ističe važnost razvijanja novih metoda i tehnologija za zaštitu ovih kompleksnih sustava, kao i potrebu za stalnim usavršavanjem i ažuriranjem sigurnosnih mjera kako bi se održao korak s brzim razvojem tehnologije (2018).

Studija koju su proveli Noam Ben-Asher i Cleotilde Gonzalez (2015) istražuje kako znanje o kibernetičkoj sigurnosti utječe na otkrivanje i odgovor na kibernetičke napade. Autori su se

posebno usredotočili na razumijevanje kako se informirana osoba može suprotstaviti sofisticiranim kibernetičkim napadima u usporedbi s onima koji imaju manje znanja. U sklopu svog istraživanja, Ben-Asher i Gonzalez su primijenili kognitivne i modele ponašanja kako bi analizirali kako ljudi prepoznaju i reagiraju na kibernetičke prijetnje. Njihova studija sugerira da su ljudi s većim razumijevanjem kibernetičke sigurnosti bolje opremljeni za otkrivanje i sprječavanje napada. Ova otkrića imaju značajne implikacije za dizajniranje obrazovnih programa i politika usmjerenih na povećanje svijesti o kibernetičkoj sigurnosti. Autori također naglašavaju važnost stalnog obrazovanja i treninga u ovom području. Budući da se kibernetičke prijetnje neprestano razvijaju i mijenjaju, kontinuirano učenje i ažuriranje vještina ključno je za održavanje visoke razine sigurnosti. Ova studija pruža snažan argument za ulaganje u obrazovanje i svijest o kibernetičkoj sigurnosti kao ključnoj komponenti strategija obrane od kibernetičkih prijetnji.

Sve ove studije zajedno stvaraju sliku kibernetičkih prijetnji kao složenog i dinamičnog problema koji zahtijeva multidisciplinarni pristup i stalnu prilagodbu. Bez obzira na to koristimo li se suvremenim tehnologijama kao što su strojno učenje ili blockchain, ili se oslanjamo na tradicionalnije metode obrane, jedno je jasno: kibernetička sigurnost mora biti prioritet za sve nas u digitalnom dobu (Ben-Asher i Gonzalez, 2015).

4.5.2. Osviještenost o rizicima kibernetičkih napada

Osviještenost o rizicima kibernetičkih napada ima visok značaj u suvremenom društvu koje se sve više oslanja na digitalne tehnologije. S razvojem interneta i sveprisutnošću tehnologije, kibernetička sigurnost postala je vitalno važna u svim sektorima društva, od poslovnog do obrazovnog.

Rastuća potreba za kibernetičkom sigurnošću ne može se zanemariti. U eri u kojoj se sve više oslanjamo na digitalne tehnologije, kibernetički napadi postaju ozbiljna prijetnja. Studija Shouq Alrobaian, Saif Alshahrani i Abdulaziz Almaleha (2023) proučava svijest o kibernetičkoj sigurnosti među polaznicima tehničkog i strukovnog obrazovanja, ističući važnost obrazovanja kao prvog koraka u obrani od kibernetičkih prijetnji. Daljnje studije Tibora Póse i Jens Grossklagsa (2022) ističu utjecaj radnog iskustva na svijest o rizicima kibernetičke sigurnosti.

Njihova studija sugerira da iskustvo može igrati ključnu ulogu u oblikovanju naše percepcije i reakcije na kibernetičke prijetnje.

Osim toga, Keyong Wang, Xiaoyue Guo i Dequan Yang (2022) proučavali su učinkovitost svijesti o kibernetičkoj sigurnosti u okvirima procjene rizika industrijskih kontrolnih sustava. Njihova studija naglašava kako je svijest o kibernetičkoj sigurnosti ključna u održavanju sigurnih operativnih okruženja.

Nisha Rawindaran, Ambikesh Jayal i Edmond Prakash (2022) istraživali su utjecaj svijesti o kibernetičkoj sigurnosti na male i srednje poduzetnike u Walesu. Otkrili su da su tvrtke koje su bile svjesne kibernetičkih rizika bile bolje pripremljene za obranu od kibernetičkih napada.

Studija Mohammeda Khadera, Marcela Karama i Hanne Fares (2021) razvila je okvir za osvješćivanje kibernetičke sigurnosti za akademsku zajednicu. Njihov rad pokazuje da obrazovne institucije mogu imati bitan značaj u povećanju svijesti o kibernetičkoj sigurnosti.

Daljnji rad Talala Alharbija i Asife Tassaddiq (2021) ocijenio je svijest o kibernetičkoj sigurnosti među studentima na Sveučilištu Majmaah. Njihovo istraživanje pokazuje da je svijest o kibernetičkoj sigurnosti na visokom nivou među studentima, što ukazuje na važnost edukacije u ranoj fazi.

Konačno, studija Noor Suhani Sulaiman, Muhammada Ashrafa Fauzija, Suhaidah Hussain i Waltona Widera (2022) proučava ponašanje kibernetičke sigurnosti među vladinim zaposlenicima. Njihov rad ističe ulogu teorije motivacije zaštite i odgovornosti u ublažavanju kibernetičkih napada. Uvidi iz ove studije pokazuju da pojedinci mogu djelovati kao prva linija obrane protiv kibernetičkih napada, ako su pravilno motivirani i obučeni.

U sklopu istraživanja o oštećenju ugleda organizacija zbog kibernetičkih napada, Srinath Perera, Xiaohua Jin, Alana Maurushat i De-Graft Joe Opoku (2022) analizirali su faktore koji utječu na reputacijsku štetu. Njihov rad pokazuje kako svijest o potencijalnoj šteti od kibernetičkih napada može pridonijeti formiranju boljih strategija zaštite.

Studija koju su proveli Mohammad Hijji i Gulzar Alam (2022) razvila je okvir za obuku i osvješćivanje o kibernetičkoj sigurnosti (CAT) za zaposlenike koji rade na daljinu. Ova studija pokazuje važnost pružanja odgovarajuće obuke o kibernetičkoj sigurnosti u trenutnom kontekstu sve većeg rada na daljinu.

Rad Aleksandre Kuzior, Pauline Brożek, Olhe Kuzmenko, Hanne Yarovenko i Tetyane Vasilyeva (2022) bavi se rizicima kibernetičkog kriminala u financijskim institucijama. Predviđanje informacijskih trendova u ovom kontekstu ključno je za razumijevanje budućih prijetnji i pripremu za njih.

Rad Konstantinosa Ntafloukasa, Daniela P. McCruma i Liliane Pasquale (2022) predstavlja pristup procjeni kibernetičko-fizičkog rizika za transportnu infrastrukturu omogućenu Internetom stvari. Uz svijest o mogućim prijetnjama, ova studija ističe važnost uvođenja sofisticiranih metoda procjene rizika za očuvanje infrastrukture.

Rad Yuchong Lija i Qinghui Liu (2021) nudi opsežan pregled studije o kibernetičkim napadima i kibernetičkoj sigurnosti. Ova studija ističe najnovije trendove i razvoj u području kibernetičkih napada, naglašavajući potrebu za stalnom sviješću o ovom rastućem području prijetnji.

Studija Noam Ben-Asher i Cleotilde Gonzalez (2015) proučava učinke znanja o kibernetičkoj sigurnosti na otkrivanje napada. Ovaj rad ukazuje na ključnu ulogu koju znanje i obrazovanje igraju u povećanju naše sposobnosti detekcije kibernetičkih napada. Autore sugeriraju da veće razumijevanje tehničkih aspekata kibernetičke sigurnosti može značajno pomoći u ranom prepoznavanju potencijalnih napada.

Stephen Hart, Andrea Margheri, Federica Paci i Vladimiro Sassone (2020) razvili su igru pod nazivom Riskio, koja služi za podizanje svijesti i obrazovanje o kibernetičkoj sigurnosti. Ovaj inovativni pristup koristi gamifikaciju kao sredstvo za poboljšanje razumijevanja kibernetičkih prijetnji i načina na koje se možemo boriti protiv njih.

Edward G. Amoroso (2011) u svom radu naglašava važnost svijesti o kibernetičkim napadima. On ističe da je svijest ključna u borbi protiv kibernetičkih prijetnji, s obzirom na stalno mijenjanje i razvoj tehnologija koje koriste napadači.

Taufik Mohammad, Nur Atikah Mohamed Hussin i Mohd Heikal Husin (2022) proučavali su svijest o online sigurnosti i ljudskim faktorima primjenom teorije ljudske ekologije. Oni su došli do zaključka da je važno razumjeti kako ljudski faktori utječu na svijest o online sigurnosti, kako bi se stvorile učinkovite strategije zaštite.

Ulrik Franke i Joel Brynielsson (2014) proveli su sustavni pregled literature o kibernetičkoj situacijskoj svijesti. Njihov rad pruža dubinsko razumijevanje trenutnog stanja znanja u ovoj

oblasti i ističe važnost kontinuiranog istraživanja za unapređenje metoda detekcije i prevencije kibernetičkih napada.

Svijest o kibernetičkim rizicima nije samo stvar znanja, već i pripravnosti na različite vrste napada. Studija Šarūnasa Grigaliūnasa, Rase Brūzgienė i Algimantasa Venčkauskasa (2023) predlaže metodologiju za identificiranje opsega faza kibernetičkih napada u odnosu na njihov utjecaj na kontrolu kibernetičke održivosti nad sustavom.

Bitno je istaknuti da osviještenost o kibernetičkim rizicima nije samo stvar individualne odgovornosti. Institucije na svim razinama - od obrazovnih do poslovnih i državnih - moraju prepoznati važnost ovog pitanja i uložiti sredstva u razvoj strategija, alata i programa za edukaciju i podizanje svijesti o kibernetičkim rizicima. Samo tako može se postići sveobuhvatna i učinkovita zaštita od kibernetičkih prijetnji.

4.5.3. Mjere zaštite od kibernetičkih napada

Mjere zaštite od kibernetičkih napada važne su kako za pojedince, tako i za organizacije različitih veličina i sektora. Kibernetički napadi mogu uzrokovati značajnu štetu, uključujući gubitak povjerljivih podataka, prekid usluga, financijski gubitak, kao i oštećenje reputacije. S obzirom na složenost i stalnu evoluciju kibernetičkih prijetnji, potrebne su složene i sveobuhvatne mjere zaštite kako bi se ublažili rizici i osigurala otpornost na kibernetičke napade.

Studija Jian Chen i suradnika (2021) upućuje na sofisticiranu prirodu kibernetičkih prijetnji, posebno u kontekstu pametnih mreža, koje su vitalne za moderno društvo i ekonomiju. S obzirom na složenost i veličinu ovih mreža, jednostavne i uske sigurnosne mjere često su nedovoljne za pružanje sveobuhvatne zaštite. Stoga se fokus prebacuje na integrirani pristup zaštiti kibernetičke sigurnosti.

Chen i suradnici predlažu višeslojni sigurnosni okvir, što znači da se koristi niz međusobno povezanih sigurnosnih mjera kako bi se ojačala ukupna zaštita. Ovaj pristup uključuje tehničke, proceduralne i organizacijske aspekte sigurnosti. Tehnički aspekti odnose se na hardver, softver i mrežne komponente, dok proceduralni i organizacijski aspekti obuhvaćaju sigurnosne politike, standarde i procedure, kao i ljudske resurse i njihovu edukaciju. Konkretno, u njihovom okviru, primjenjuju se različiti alati i tehnike za detekciju, obranu i oporavak od

kibernetičkih napada. Ova slojevita strategija omogućuje bržu detekciju napada, efikasnije reagiranje na incidente i brži oporavak sustava nakon napada (Chen et al., 2021).

Osim toga, višeslojni okvir nudi više razine zaštite od različitih vrsta prijetnji. Na primjer, ako napadač uspije proći kroz jedan sloj zaštite, sljedeći sloj može ga zaustaviti. Ovo stvara dubinu u obrani i povećava ukupnu sigurnost sustava. Ukratko, studija Chen i suradnika (2021) naglašava važnost integriranog i sveobuhvatnog pristupa zaštiti kibernetičke sigurnosti. Svijest o ovom pristupu može bitno pridonijeti smanjenju ranjivosti i poboljšanju otpornosti na kibernetičke napade.

Studija Šarūnasa Grigaliūnasa i suradnika (2023) donosi novi uvid u razumijevanje kibernetičkih napada, promatrajući ih kroz različite faze i analizirajući njihov utjecaj na kontrolu kibernetičke održivosti nad sustavom. Ovaj istraživački rad pruža temeljitiji i detaljniji pogled na dinamiku kibernetičkih napada, što omogućuje izradu specifičnijih i ciljanih mjera zaštite.

Kibernetički napadi često nisu jednostavni ili trenutačni događaji. Umjesto toga, oni se obično odvijaju u različitim fazama, od početnog istraživanja i pronalaženja slabosti, preko probijanja i infiltracije u sustav, do eksploatacije i moguće eskalacije privilegija. Svaka od ovih faza nosi sa sobom specifične rizike i izazove za kibernetičku sigurnost. Grigaliūnas i njegov tim razvili su metodologiju koja omogućuje identificiranje i analizu ovih faza. Uzimajući u obzir specifične značajke i utjecaje svake faze, ova metodologija može pomoći u prepoznavanju slabih točaka, predviđanju mogućih napada i stvaranju učinkovitijih strategija zaštite.

Osim toga, ova metodologija također omogućuje bolje razumijevanje utjecaja kibernetičkih napada na kontrolu kibernetičke održivosti nad sustavom. Kibernetička održivost odnosi se na sposobnost sustava da održava svoju funkcionalnost i performanse unatoč kibernetičkim prijetnjama i napadima. Shvaćanje kako različite faze napada mogu utjecati na ovu kontrolu može biti ključno za osiguranje dugoročne sigurnosti i održivosti informacijskih sustava (Grigaliūnas et al., 2023).

Studija Fawaza Alharbija i njegovih suradnika (2021) donosi važne uvide u odnos između praksi kibernetičke sigurnosti i potencijalne štete od kibernetičkih napada, posebno u kontekstu malih i srednjih poduzeća (MSP). Ova vrsta poduzeća često je izložena visokim rizicima od kibernetičkih napada, s obzirom na njihovu relativnu ranjivost i ograničene resurse za sigurnost. Prema nalazima studije, primjena pravilnih praksi kibernetičke sigurnosti ima značajan utjecaj

na smanjenje štete uzrokovane kibernetičkim napadima. To uključuje različite aspekte, od tehničkih mjera poput instaliranja antivirusnih programa i redovitog ažuriranja softvera, do organizacijskih mjera poput edukacije zaposlenika o opasnostima i najboljim praksama za kibernetičku sigurnost.

Alharbijeva studija otkriva kako pravilna primjena ovih praksi može biti od iznimnog značaaj za zaštitu MSP-a od kibernetičkih napada. Na primjer, redovita edukacija zaposlenika može pomoći u sprečavanju uobičajenih taktika kao što su phishing napadi, dok tehničke mjere mogu pružiti snažnu zaštitu protiv različitih vrsta malwarea. Osim toga, studija također ističe važnost razvijanja kulture kibernetičke sigurnosti unutar organizacije. To znači da kibernetička sigurnost treba biti integralni dio svakodnevnih operacija i procesa poduzeća, a ne samo dodatak ili naknadna misao. Kroz ovaj pristup, poduzeća mogu stvoriti snažan sustav obrane protiv kibernetičkih prijetnji i minimizirati potencijalnu štetu od napada (Alharbi et al., 2021).

Istraživanje Yuchong Lia i Qinghui Liua (2021) daje sveobuhvatan pregled kibernetičkih napada i mjera kibernetičke sigurnosti, ističući ključne trendove i nedavna dostignuća u ovom području. Ova studija može poslužiti kao temelj za razumijevanje šireg konteksta kibernetičke sigurnosti i za razvoj učinkovitih mjera zaštite.

Ercan Nurcan Yılmaz i Serkan Gönen (2018) razvili su sustav za detekciju / prevenciju napada protiv kibernetičkih napada u industrijskim kontrolnim sustavima. Njihov rad ilustrira važnost razvoja specifičnih rješenja za određene sektore i vrste infrastrukture.

U radu Yu Zhenga i suradnika (2022) istražene su dinamičke obrane u kibernetičkoj sigurnosti, tehnike, metode i izazovi. Autorski tim naglašava kako je potrebno konstantno ažuriranje i prilagođavanje obrambenih strategija kako bi se nosile s stalno mijenjajućim kibernetičkim prijetnjama.

Joe Kim (2017) bavi se pitanjem kibernetičke sigurnosti u vladinom sektoru, posebno usredotočujući se na smanjenje rizika. Kroz ovu studiju, razvidna je važnost sektorski specifičnih rješenja, te pristup *najbolje prakse* unutar određenih industrijskih i institucionalnih okvira.

Bekkers i suradnici (2023) istražili su kako poduzetnici mogu bolje zaštititi svoje poslovanje od napada ransomware-a koristeći prošireni model motivacijske teorije zaštite. Ova studija pokazuje kako je razumijevanje motivacija i ponašanja ključno u razvijanju učinkovitih mjera zaštite.

Studija Guoliang Donga i suradnika (2022) analizira napade na mrežu web mjesta i sigurnosne protumjere. Rezultati istraživanja pokazuju kako precizno razumijevanje specifičnih napada može voditi učinkovitim protumjerama.

Xirong Ning i Jin Jiang (2022) proučavaju obranu u dubini protiv unutarnjih napada u kibernetičko-fizičkim sustavima, dok rad Michela Dacorogne i suradnika (2023) ističe važnost izgradnje kibernetičke otpornosti kroz bolje razumijevanje kibernetičkog rizika putem novog algoritma za modeliranje podataka s teškim repovima.

U radu Chrisa McIntosha (2015) raspravlja se o problemu kibernetičke sigurnosti: tko će pružiti zaštitu? Ova studija ukazuje na važnost međuinstitucionalne suradnje i koordinacije u osiguranju kibernetičke sigurnosti.

Studija Huga Riggsa i suradnika (2023) detaljno se bavi utjecajem, ranjivostima i strategijama ublažavanja za kibernetički sigurnu kritičnu infrastrukturu, dok rad Esrae Altulaihan i suradnika (2022) predstavlja prijetnje kibernetičke sigurnosti, protumjere i tehnike ublažavanja na Internetu stvari.

Eric C. K. Cheng i Tianchong Wang (2022) proučavaju institucionalne strategije za kibernetičku sigurnost u visokoškolskim institucijama, dok rad Tehseena Mazhara i suradnika (2023) analizira napade na kibernetičku sigurnost i njihova rješenja za pametnu mrežu koristeći metode strojnog učenja i blockchaina. Ove studije naglašavaju važnost raznolikosti strategija i pristupa u borbi protiv kibernetičkih prijetnji, s obzirom na različite sektore, tehnologije i vrste prijetnji.

U svim ovim studijama vidljiva je hitnost učinkovite kibernetičke zaštite, ali isto tako i kompleksnost ovog problema. Kibernetičke prijetnje se stalno razvijaju i mijenjaju, što zahtijeva konstantnu pažnju, istraživanje i inovaciju. Samo kroz detaljno razumijevanje prirode prijetnji i pravovremeno djelovanje može se osigurati učinkovita zaštita. Bez obzira radi li se o kritičnoj infrastrukturi, malim poduzećima, visokoškolskim institucijama ili IoT-u, svi sektori moraju razviti i primijeniti učinkovite mjere zaštite kako bi osigurali svoju kibernetičku sigurnost.

Pored toga, važno je promicati međuinstitucionalnu suradnju i koordinaciju. Kibernetička sigurnost nije samo problem pojedinačnih organizacija, već i cijelih društava i država. Iz tog razloga, potrebno je poticati dijalog, suradnju i razmjenu znanja na svim razinama.

Konačno, u svijetu u kojem tehnologija sve više oblikuje našu svakodnevnicu, pitanje kibernetičke sigurnosti postaje sve važnije. Kroz ove i brojne druge studije, jasno je da su stalna istraživanja, edukacija i inovacije ključni u postizanju sigurnog kibernetičkog prostora.

4.6. Zaštita privatnosti i podataka u kontekstu Interneta stvari

Prema istraživanju autora Hillary Brill i Scotta Jonesa u *Little Things and Big Challenges: Information Privacy and the Internet of Things* (2017), IoT je prisutan u našem životu na bezbrojne načine, od dobrodošlih i namjernih, poput fitnes uređaja i sustava za sigurnost doma, do onih nenamjernih i potencijalno uznemirujućih, poput igračaka povezanih s internetom koje mogu slušati našu djecu ili tehnologija koje nas mogu pratiti bez našeg znanja.

U današnjem digitalnom svijetu, privatnost i sigurnost podataka postaju sve važnije, posebno s obzirom na sveprisutnu upotrebu IoT tehnologija. Kroz različite uređaje i aplikacije, IoT prikuplja ogromne količine podataka, stvarajući potencijalne izazove za zaštitu privatnosti korisnika i sigurnost njihovih osobnih podataka.

Zaštita privatnosti i podataka u kontekstu IoT-a važna je tema u suvremenom digitalnom svijetu. IoT, kako ga definira Bijela kuća, jest sposobnost uređaja da komuniciraju jedni s drugima koristeći ugrađene senzore povezane kroz žičane i bežične mreže (Bodenheimer, 2016). Međutim, s obzirom na njegovu sveprisutnost, IoT sa sobom donosi brojne sigurnosne i rizike koji se tiču prava privatnosti.

Prema istraživanju koje je izveo Fabiano (2017), glavni rizik za privatnost u IoT-u je profiliranje, što omogućava identifikaciju fizičkih osoba kroz njihove osobne informacije. Sustav IoT omogućuje prijenos podataka, uključujući osobne podatke, putem interneta, čime se otvaraju mogućnosti za potencijalne sigurnosne prijetnje i pitanja odgovornosti. Kako bi se takvi rizici minimalizirali, neophodno je obratiti posebnu pozornost na analizu zakona, kako bi se procijenili rizici i spriječila pogrešna upotreba osobnih podataka i informacija.

U tom kontekstu, Weber (2017) sugerira da rješenje za brojne odgovornosti koje se javljaju u kontekstu IoT-a ne može se postići samo kroz jedan pravni instrument niti kroz tehničko rješenje. Klasični pravni instrumenti, kao što su ugovorne obveze, odgovornost za proizvode i

odštetni zahtjevi, nisu više dovoljni u okruženju IoT-a. Umjesto toga, potreban je kombinirani pristup koji stvara praktičnu stvarnost na koju se zakon može primijeniti.

Uvođenje GDPR-a predstavlja važan korak prema rješavanju ovih problema. Fabiano (2017) naglašava da GDPR, koji se primjenjuje od 25. svibnja 2018., ima bitan značaj u zaštiti podataka u kontekstu IoT-a. Uredba uvodi procjenu utjecaja zaštite podataka (DPIA), obavijesti o povredama podataka i vrlo visoke administrativne kazne za kršenje odredbi uredbe.

Osim toga, Fornasier (2019) upozorava na neizvjesnosti i rizike koje IoT donosi za ostvarivanje osnovnih prava na zdravstvo i privatnost. IoT ima veliki potencijal za poboljšanje zdravstvene skrbi, ali sigurnost prikupljanja i pohrane osjetljivih podataka treba biti prva briga u razvoju sustava koji uključuju takve tehnolog ologije. Naime, postoji veliki potencijal nepoštovanja temeljnog prava na privatnost pojedinaca kroz njihovu upotrebu, ne samo od strane privatnih trećih strana, već i od strane države. U ovom kontekstu, Fornasier naglašava važnost uspostave dobrih praksi, učinkovitih tehnologija sigurnosti podržanih javnim politikama i pravnim praksama.

Upravo se tu uklapa Weber (2017), koji raspravlja o složenosti rješavanja pitanja odgovornosti u kontekstu IoT-a i novih oblika ugovora. Weber ističe kako se problemi odgovornosti ne mogu riješiti jednim pravnim instrumentom niti tehničkim rješenjem. Tradicionalni pravni instrumenti, kao što su ugovorni lijekovi, proizvođačeva odgovornost i tužbe zbog štete, više nisu dovoljni u okruženju IoT-a. Stoga je potreban kombinirani pristup koji stvara praktičnu stvarnost na koju se može primijeniti zakon. Bez te interakcije, ostaje praznina, a jaz između prava i tehnologije raste, što dovodi do značajnog nedostatka izvršivosti u online svijetu.

Ovi argumenti dalje dovode do rasprave Bodenheimera (2016), koji tvrdi da IoT predstavlja tsunami pravnih dilema. Iz perspektive privatnosti i sigurnosti, IoT, s milijardama uređaja, predstavlja raznolikost potencijalnih rizika, kako je naglašeno na različitim kongresnim saslušanjima i saveznim izvješćima. Bodenheimer naglašava da su izazovi osiguranja svijeta IoT-a složeni, s obzirom na raznoliku i široko rasprostranjenu prirodu IoT-a i brojne načine na koje se uređaji i mreže mogu povezati s IoT sustavima.

U skladu s ovim, Fabiano (2017) objašnjava da fenomen IoT-a mora uzeti u obzir pravna pitanja povezana s pravom na zaštitu podataka. Glavni rizik za privatnost u IoT-u je profiliranje koje omogućuje identifikaciju fizičkih osoba putem njihovih osobnih podataka. Fabiano dodatno naglašava važnost razmatranja novog europskog Općeg propisa o zaštiti podataka (GDPR) koji

se primjenjuje od 25. svibnja 2018. godine. GDPR uvodi procjenu utjecaja zaštite podataka (DPIA), obavijest o povredi podataka i vrlo visoke administrativne kazne u slučaju kršenja propisa.

U svjetlu svih ovih argumenata i dokaza, jasno je da IoT, dok pruža ogromne potencijale za napredak i inovacije, također donosi sa sobom brojne pravne, etičke i sigurnosne izazove.

Ovi izazovi, koji uključuju privatnost, sigurnost podataka, odgovornost i pravnu izvršivost, zahtijevaju dubinsko razumijevanje i pravni okvir koji je sposoban upravljati kompleksnošću IoT-a. Fabiano ukazuje na važne elemente GDPR-a kao načine za poboljšanje zaštite podataka i privatnosti u IoT-u, ali oni su tek prvi koraci. Potreban je sveobuhvatan, višedimenzionalan pristup koji uključuje javnu politiku, zakonodavstvo, korporativnu odgovornost i razvoj novih tehnologija za zaštitu podataka. Daljnje istraživanje ove teme od velike je važnosti kako bi se osiguralo da se prava na privatnost i zdravstvo adekvatno štite dok se istovremeno iskorištavaju prednosti koje IoT pruža. Vlade, pravna zajednica, tvrtke i tehnolozi trebaju surađivati u razvijanju rješenja koja omogućuju razvoj IoT-a, a da pritom ne ugrožavaju temeljna prava i slobode pojedinaca.

U tom smislu, akademska zajednica treba nastaviti s istraživanjem i raspravama o ovim pitanjima. Kroz konstruktivan dijalog i razmjenu ideja, moguće je razviti strategije i alate koji će omogućiti da se tehnološki napredak događa uz puno poštovanje ljudskih prava i zaštite podataka. Bez sumnje, IoT donosi izazove, ali s pravim pristupom, ti se izazovi mogu prevladati.

U svom radu iz 2020. godine, Jeremy Siegel istražuje problematiku privatnosti i sigurnosti podataka u kontekstu IoT-a s perspektive potrošača, posebno u Sjedinjenim Američkim Državama. Siegel ukazuje na sve veći broj IoT uređaja s kojima se ljudi svakodnevno susreću i time otvaraju sve više mogućih pristupnih točaka za sigurnosne prijetnje. On ističe da mnogi potrošači nisu ni svjesni rizika koji prate korištenje ovih uređaja, a problemi se protežu kroz sve socioekonomske i demografske skupine širom svijeta. Osim što su potrošači izloženi opasnostima, Siegel također upozorava na rizike s kojima se suočavaju tvrtke kada su njihovi IoT uređaji hakirani, s obzirom na velike količine korisničkih podataka koje pohranjuju. Uprkos sve češćim slučajevima kršenja sigurnosti podataka, Siegel ukazuje da su potrošači često neosjetljivi na ovu problematiku, ne shvaćaju ozbiljnost rizika i ne znaju kako se zaštititi.

Rizici povezani s kršenjem sigurnosti podataka putem IoT uređaja su ozbiljni, a Siegel ističe da postoje brojne prepreke koje otežavaju korisnicima da ostvare pravnu zaštitu. Nedostatak uspješnih pravnih teorija na koje se potrošači mogu osloniti kako bi podigli tužbu protiv proizvođača IoT-a je jedna od glavnih prepreka, a tu se nalazi i problem zadovoljenja uvjeta za pokretanje tužbe prema članku III Ustava SAD-a. Prema Siegelu, iako kompanije nastavljaju ulagati u sigurnosnu infrastrukturu kako bi spriječile kršenje podataka, još uvijek ne postoji široko prihvaćena ili prepoznata definicija što bi trebalo biti nepažnja ili standard dužne pažnje za tvrtke koje se bave IoT-om. Ovo dovodi do velike nesigurnosti oko toga kako se potrošači mogu zaštititi (2020).

U odnosu na američko federalno zakonodavstvo koje se odnosi na kibernetičku sigurnost, Siegel naglašava da su propisi razbacani i nedostaju jasnoće. S druge strane, GDPR donesen od strane Europske unije 2018. godine, prema Siegelu, daje dugotrajan odgovor na mnoga pitanja o zaštiti privatnosti podataka.

Larisa-Antonia Capisizu, u svojoj publikaciji *Legal Perspectives on the Internet of Things*, ističe brojne izazove koje sa sobom donosi IoT, uključujući potrebu za zaštitom privatnosti i podataka. Kao jedan od ključnih izazova, ističe se postizanje povjerljivosti i sigurnosti podtakvi međusobno povezani sustavi prikupljaju i šire ne traže uvijek izriččime se postizanje povjerljivo

Pored toga, izazov predstavlja i zaštita podataka. Slobodan protok podataka izložen (2021) ukazuju, IoT donosi brojne mogućnosti, ali istovremeno i brojne rizike. Jedan od najvećih izazova je određivanje odgovornosti među različitim akterima u IoT ekosustavu, posebno s obzirom na složenu prirodu i interakciju tih aktera. Ti autori predlažu identifikaciju IoT aktera prema novom petoslojnom modelu računalstva u IoT-u, koji i *dew* računarstvo. Njihov je zaključak da bi identifikacija IoT aktera u svjetlu odgovarajućih uloga upravitelja podacima IoT-a mogla biti korisna u određivanju odgovornosti IoT aktera za njihovu usklađenost s pravilima zaštite podataka i privatnosti.

Tanczer et al. (2019) također ističu da je, s obzirom na rastući utjecaj IoT-a, upravljanje ovim područjem postalo važan zadatak i odgovornost koju vjerojatno neće preuzeti samo privatni sektor. Oni tvrde da će efikasno upravljanje suprotstavljenim zahtjevima biti ključno za temeljnu integritet i otpornost ekosustava IoT-a. Različite tehnologije koje čine IoT, kao što su senzori, akceleratori i mrežne komponente, predstavljaju potencijalne slabosti u lancu sigurnosti, što zahtijeva sveobuhvatno i dinamično razumijevanje sigurnosti. Mirai botnet, na

primjer, bio je primjer potencijalnog rizika od IoT-a, koristeći globalno raspršene IoT uređaje kao što su video kamere ili baby monitore kao daljinski kontrolirane uređaje koji su korišteni u jednom od najdestruktivnijih napada ometanja usluge (DDoS) 2016. godine.

Kako bi se osigurala zaštita podataka i privatnosti u kontekstu IoT-a, potrebno je razviti odgovarajuće strategije i politike, uključujući identifikaciju i upravljanje odgovornostima različitih IoT aktera, te razvijanje sveobuhvatnih i dinamičnih pristupa upravljanju sigurnošću.

4.7. Regulatorna obilježja usluga pametnih gradova

Pametni gradovi su suvremeni urbanistički koncept koji se temelji na korištenju tehnologije za poboljšanje kvalitete života građana i održivog razvoja gradova. No, kako se tehnologija razvija, raste i potreba za regulacijom usluga pametnih gradova, osobito s obzirom na pitanja poput privatnosti, sigurnosti, održivosti i pristupačnosti. U tom kontekstu, potrebno je rasvijetliti regulatorna obilježja usluga pametnih gradova temeljena na različitim studijama.

Weber i Podnar (2019) naglašavaju važnost regulatornih okvira za upravljanje uslugama pametnih gradova, ukazujući na potrebu za boljim integracijom tehnologija i usluga. Pandemija je pokazala važnost takvih okvira, gdje su Petrova i Tairov (2022) istakli ulogu pametnih gradova u upravljanju rizicima u vrijeme krize.

U kontekstu upravljanja i sociotehničkih sustava, rad Kim i Yang (2023) nudi vrijednu analizu važnosti povezanih usluga u pametnim gradovima. Autori naglašavaju kako integrirane usluge unutar pametnih gradova imaju bitan značaj u povećanju učinkovitosti i poboljšanju kvalitete života građana. Ova perspektiva pruža korisne uvide u složenost sociotehničkih sustava unutar pametnih gradova, gdje interakcija između ljudi, tehnologija i procesa stvara dinamično okruženje koje zahtijeva promišljeno i fleksibilno upravljanje.

S druge strane, Malik i sur. (2022) donose sveobuhvatnu analizu pametnih usluga unutar pametnih gradova kroz znanstvenu analizu. Njihov rad identificira elemente i trendove u razvoju pametnih usluga, uzimajući u obzir različite aspekte poput tehnologije, održivosti i korisničkog iskustva. Ovaj pristup omogućava dublje razumijevanje načina na koje pametne usluge oblikuju i mijenjaju pejzaž pametnih gradova, pružajući važne uvide za strateško planiranje i razvoj. Oba istraživanja pružaju važne uvide u regulatorna obilježja usluga pametnih gradova, naglašavajući složenost i interdisciplinarnost ove teme. Pritom ističu

važnost razumijevanja kako tehnološki napredak i socijalne promjene međusobno utječu jedni na druge u kontekstu pametnih gradova, što predstavlja ključni izazov za regulatorne okvire.

U kontekstu održivosti i planiranja pametnih gradova, istraživanje Choi i Song (2023) donosi značajne uvide. Autori analiziraju postojeće planove za pametne gradove i nude smjernice za tranziciju prema modelu pametnih održivih gradova. Ovaj rad naglašava važnost strateškog planiranja i dijagnoze kako bi se osiguralo da inicijative pametnih gradova pridonose dugoročnoj održivosti. Isto tako, analiza Choi i Song nudi praktične smjernice za kritičnu ocjenu i poboljšanje postojećih planova, naglašavajući važnost kontinuirane evaluacije i prilagodbe.

Miguelez i sur. (2023), s druge strane, fokusiraju se na kritičnu infrastrukturu pametnih gradova. Autori ističu ključnu ulogu IoT tehnologije u obnovi i securitizaciji kritične infrastrukture. Pritom pružaju smjernice za integraciju IoT-a u procese obnove i zaštitu, podupirući razvoj otpornih i sigurnih urbanih sustava. Oba rada naglašavaju složenost i interdisciplinarnost izazova s kojima se suočavaju pametni gradovi. Istovremeno, oni ukazuju na potencijal inovativnih tehnoloških rješenja, poput IoT-a, u rješavanju ovih izazova i promicanju održivosti. Njihovi nalazi pružaju dragocjene uvide u mogućnosti i izazove koje pametni gradovi predstavljaju za održiv razvoj i sigurnost, dok naglašavaju važnost integriranih i strateški usmjerenih pristupa.

Istraživanje Fabrèguea i Bogonija (2023) bacilo je svjetlo na složenu problematiku sigurnosnih pitanja u kontekstu pametnih gradova, posebice u domeni privatnosti. Autori su se detaljno bavili izazovima i mogućim rizicima koje pametni gradovi nose u pogledu zaštite privatnih podataka svojih građana. Ovo istraživanje ukazuje na važnost pažljivog razmatranja sigurnosnih mjera prilikom razvoja i implementacije usluga pametnih gradova, ali i na potrebu za razvojem normativnih okvira koji bi regulirali ovu problematiku.

U svjetlu zaštite podataka, Vandercruysse, Buts i Dooms (2020) su napravili važan doprinos kroz istraživanje usluga pametnih gradova. Autori su razvili tipologiju usluga pametnih gradova s obzirom na ocjenu utjecaja zaštite podataka, ističući kako su pitanja privatnosti i zaštite podataka ključni elementi u konstrukciji i upravljanju pametnim gradovima. Tipologija koju su predložili pruža koristan okvir za analizu i razumijevanje različitih aspekata usluga pametnih gradova, a ujedno naglašava važnost ocjene utjecaja zaštite podataka u kontekstu razvoja i implementacije takvih usluga. Oba istraživanja ističu da je zaštita privatnosti neophodna

komponenta razvoja pametnih gradova. Sigurnost i privatnost podataka moraju biti u središtu svake politike i strategije, a istovremeno pružaju važan okvir za razumijevanje kompleksnosti i multidimenzionalnosti usluga pametnih gradova.

Lee (2023) pristupa temi pametnih gradova iz perspektive prihvaćanja modela usluga. Njegovo istraživanje, koje se posebno fokusira na Seul, analizira kako su građani prihvatili i koristili različite usluge pametnih gradova. Autor raspravlja o različitim faktorima koji utječu na to prihvaćanje, uključujući tehnološku spremnost, dostupnost infrastrukture, razumijevanje i svijest o korisnosti tih usluga, te kvalitetu i efikasnost usluga koje se pružaju. Ova studija pruža važne uvide u proces prihvaćanja i upotrebe usluga pametnih gradova od strane građana.

S druge strane, Beştepe i Özkan Yildirim (2022) bave se pitanjem prihvaćanja IoT-a i usluga pametnih gradova s naglaskom na održivost. Njihova analiza pokazuje da je prihvaćanje ovih usluga ključno za ostvarenje ciljeva održivosti. Autori ističu da tehnologija IoT-a i usluge pametnih gradova mogu imati značajan utjecaj na održivost, uključujući poboljšanje energetske učinkovitosti, smanjenje emisija ugljika, poboljšanje kvalitete zraka i vode, te promicanje ekološki prihvatljivih praksi. Ovo istraživanje naglašava važnost integriranja održivosti u razvoj i primjenu usluga pametnih gradova. Obje studije pružaju vrijedan doprinos razumijevanju kako tehnologija i usluge pametnih gradova mogu biti učinkovito implementirane i prihvaćene, istovremeno naglašavajući važnost održivosti u kontekstu pametnih gradova.

Studije o regulatornim mehanizmima pametnih gradova otvaraju novu perspektivu na način na koji pravni, sigurnosni i informacijski sustavi utječu na funkcioniranje pametnih gradova. Peoples (2021) nudi sveobuhvatnu analizu pravnih i sigurnosnih aspekata pametnih gradova. Fokusirajući se na različite razine regulative, autor iznosi argumente o utjecaju zakonodavstva na razvoj i implementaciju tehnologija pametnih gradova. Kroz njegov rad, dolazimo do boljeg razumijevanja kako se pravna regulativa oblikuje i primjenjuje u kontekstu naprednih urbanih tehnologija.

Ranchordás i Goanta (2020) pružaju dublji uvid u ulogu informacijskih sustava u pametnim gradovima. Njihova analiza obuhvaća važnost informacijskih sustava u podršci operativnim funkcijama pametnih gradova, naglašavajući kako tehnološka rješenja igraju ključnu ulogu u omogućavanju održive i učinkovite urbane infrastrukture.

Ismagilova i sur. (2019) idu korak dalje, analizirajući interakciju između informacijskih sustava i regulatornih mehanizama. Njihov rad pokazuje kako su informacijski sustavi ključni u implementaciji regulative i potiču diskusiju o budućim smjernicama za integraciju tehnologije i regulative u kontekstu pametnih gradova.

Saborido i Alba (2020) pružaju posebno zanimljiv uvid u softverske sustave koji se koriste u pametnim gradovima. Ističu važnost regulacije ovih sustava, posebno s obzirom na dobavljače usluga pametnih gradova. Autori argumentiraju da su dobavljači softvera ključni akteri u ekosustavu pametnih gradova te da je stoga važno osigurati odgovarajuće regulatorne mehanizme za nadzor njihovih aktivnosti. Ukupno, ove studije pružaju dublji uvid u kompleksnost regulativnih mehanizama pametnih gradova, ističući važnost razumijevanja uloge pravne regulative, informacijskih sustava i softverskih dobavljača u ovom kontekstu. Razvoj urbanog infrastrukturnog razvoja i njegovu ključnu ulogu u uspostavljanju i održavanju pametnih gradova istražuju Ercan i Kutay (2021). Njihov rad je usmjeren na identifikaciju i analizu ključne infrastrukture pametnih gradova, s posebnim naglaskom na mogućnosti poboljšanja učinkovitosti i održivosti. Ercan i Kutay pružaju brojne preporuke koje se odnose na optimizaciju infrastrukture, uključujući primjenu novih tehnologija, integraciju različitih urbanih sistema, te poticanje inovacija. Njihova studija potvrđuje važnost strateškog i holističkog pristupa razvoju infrastrukture pametnih gradova, koja uključuje razumijevanje specifičnih potreba grada, ali i širih društvenih, ekonomskih i okolišnih aspekata.

S druge strane, Chong i sur. (2018) pružaju inovativan pristup otkrivanju i rješavanju urbanističkih problema koristeći dinamičke kapacitete pametnog grada. Autori se fokusiraju na razvoj metodologije koja omogućuje identifikaciju i analizu urbanističkih problema u realnom vremenu, koristeći napredne tehnologije i algoritme za obradu podataka. Njihova studija ističe potencijal pametnih gradova da prepoznaju i rješavaju urbanističke probleme na proaktivni i učinkovit način, koristeći se dinamičnim kapacitetima koje pružaju tehnologija i veliki podaci. Ovaj rad doprinosi sve većem korpusu istraživanja koja naglašavaju važnost kontinuirane inovacije i fleksibilnosti u upravljanju pametnim gradovima.

Oba ova rada pružaju važne uvide u izazove i mogućnosti koje se javljaju u kontekstu urbanog infrastrukturnog razvoja pametnih gradova, ukazujući na važnost strategijskog planiranja, inovacija i fleksibilnosti u ovom procesu. Razumijevanje i mapiranje složene mreže dionika unutar pametnih gradova je važno za uspješnu implementaciju i regulaciju ovih sistema. U svojoj studiji iz 2021. godine, Hadzovic, Mrdovic i Radonjic napravili su značajan korak prema

tome, istražujući model vrijednosti IoT-a za pametne gradove. Oni identificiraju dionike i pružaju duboko razumijevanje njihovih uloga i međusobnih odnosa. Njihov rad predstavlja novi pristup kroz razvoj taksonomije koja kategorizira i navodi relevantne tehnološke i regulatorne karakteristike usluga pametnih gradova. Taksonomija obuhvaća širok spektar faktora, uključujući različite tipove dionika, tehnologije koje koriste, regulatorni kontekst u kojem djeluju, kao i međusobne odnose i interakcije. Ova sveobuhvatna perspektiva omogućuje bolje razumijevanje kompleksnosti pametnih gradova i pruža temelj za razvoj učinkovitijih politika i strategija. Osim toga, autori pružaju detaljno mapiranje IoT dionika iz različitih perspektiva. Oni identificiraju nove uloge upravitelja podacima povezane s različitim oblicima računalstva, uključujući dew, mist, edge, fog i cloud računalstvo. Ovaj segment rada pokazuje kako se razvoj tehnologije odražava na strukturu i dinamiku pametnih gradova, dovodeći do pojave novih uloga i odgovornosti.

U konačnici, Hadzovic, Mrdovic i Radonjic kompiliraju sve ove nalaze u novi model IoT-a sa pet računalnih slojeva temeljen na cloud, fog, edge, mist i dew računalstvu. Ovaj model ne samo da daje detaljan prikaz tehnološke infrastrukture pametnih gradova, nego također ukazuje na ključne regulatorne izazove i pitanja. Njihov rad predstavlja značajan doprinos literaturi o pametnim gradovima, pružajući dragocjene uvide i alate za akademske istraživače, donositelje odluka i praktičare u polju. Ovaj sveobuhvatni pristup identifikaciji dionika i komponenti IoT-a posebno je važan u kontekstu regulatornih obilježja usluga pametnih gradova, jer pruža dublji uvid u složenost i dinamičnost tehnološkog okruženja unutar kojeg se te usluge pružaju. Nadalje, ističe se važnost regulative poput GDPR-a, što je od posebne važnosti u kontekstu privatnosti i sigurnosti podataka u pametnim gradovima. Identificirane nove uloge upravitelja podacima potvrđuju neophodnost kontinuirane adaptacije regulatornih okvira kako bi se učinkovito upravljalo rastućom složenošću i dinamičnošću digitalnog okruženja pametnih gradova. Ovaj model može poslužiti kao vrijedna podrška u razjašnjavanju IoT komponenti, IoT dionika i odgovarajućih GDPR uloga.

Svaka od ovih studija pruža bitan uvid u regulatorna obilježja usluga pametnih gradova. Kroz pregled literature, postaje jasno da su važni aspekti regulacije pametnih gradova vezani uz integraciju tehnologija i usluga, upravljanje rizicima, održivost, privatnost i sigurnost te prihvaćanje i prilagodba tehnologija od strane korisnika. Također, istraživanja pokazuju da su fleksibilnost i dinamikat regulatornih okvira presudni za uspjeh implementacije i upravljanja uslugama pametnih gradova.

5. STAVOVI KLJUČNIH DIONIKA PO PITANJU RAZUMIJEVANJA PRAVNIH ASPEKATA REGULACIJE INTERNETA STVARI (IoT) NA TRŽIŠTU

Fokus grupe su korisna metoda u društvenim i tržišnim istraživanjima, jer omogućuju da se istraže i razumiju složene teme kroz interakciju i raspravu. Ova metoda pruža dublje razumijevanje problema, pri čemu svaki sudionik može izraziti svoje mišljenje i iskustvo, a zatim to mišljenje raspraviti i obogatiti kroz diskusiju s drugim sudionicima.

U fokus grupi koju je autorica osmislila i provela, sudjelovali su kako muški tako i ženski ispitanici. Međutim, zbog olakšanja čitanja i jednostavnosti izraza, u ovom radu sve izjave i odgovori fokus grupe izneseni su u muškom gramatičkom rodu. To, naravno, ne umanjuje ni na koji način doprinos ili perspektive ženskih sudionika, čiji su uvidi bili jednako važni i relevantni za ovu studiju.

5.1. Uvodno o fokus grupi

Ovaj sastanak fokus grupe organiziran je kao dio istraživanja o pravnim aspektima regulacije Interneta stvari (IoT) na tržištu. Cilj je prikupiti gledišta, ideje i stručno mišljenje kako bi se bolje razumjeli trenutne izazove, potrebe i mogućnosti u ovoj dinamičnoj i sve važnijoj domeni tehnologije.

Sastav ove fokus grupe odabran je tako da se predstavi što širi raspon stručnosti i iskustva. Imamo predstavnike iz HAKOM-a, inženjere, pravnike, odvjetnike i druge stručnjake koji se bave ovom tematikom. Također smo angažirali stručnjake iz različitih sektora kako bismo osigurali raznolikost perspektiva.

Fokus grupa sastojala se od:

1. Predstavnik HAKOM-a
2. Pravnik HAKOM-a
3. Inženjer telekomunikacija
4. Pravni stručnjak za IoT
5. Korisnik IoT uređaja

6. Odvjetnik 1
7. Odvjetnik 2
8. Inženjer za kibernetičku sigurnost

Tijekom ove fokus grupe, postavit ću seriju pitanja koja će služiti kao polazna točka za našu diskusiju. Cilj nam je razviti dubinsko razumijevanje tema i identificirati zajedničke i divergentne stavove.

5.2. Predstavljanje rezultata fokus grupe

Molimo vas da se slobodno uključite u diskusiju, dijelite svoja iskustva i mišljenja i slušate druge sudionike. Vaša povratna informacija bit će od presudne važnosti za naše istraživanje i oblikovanje našeg budućeg rada u ovom području.

Dobro došli na ovaj krug naše fokus grupe. Izuzetno smo zahvalni što ste odlučili podijeliti svoje vrijeme i stručnost s nama

Hvala vam što ste ovdje danas s nama. Počnimo s našom prvim temom

Pitanje: Kako trenutna pravna regulacija utječe na sigurnost i privatnost IoT uređaja i koji su glavni izazovi s kojima se suočavamo?

- Predstavnik HAKOM-a: Regulacija je nužna kako bi se osigurala sigurnost IoT uređaja. Izazovi uključuju brzi razvoj tehnologije i pronalaženje ravnoteže između sigurnosti, inovacija i privatnosti korisnika.
- Pravnik HAKOM-a: Regulacija mora biti fleksibilna kako bi se prilagodila stalnoj evoluciji IoT tehnologija. Izazov je u tome što se zakoni često ne mogu brzo prilagoditi tehnološkim promjenama.
- Inženjer telekomunikacija: Sigurnost IoT uređaja nije uvijek prioritet u dizajnu, a regulacija može pomoći u postavljanju standarda. Izazovi su u tome što je teško postići globalni konsenzus o tim standardima.
- Pravni stručnjak za IoT: Regulacija pomaže u zaštiti korisnika i podataka, ali može ograničiti inovacije. Izazovi uključuju usklađivanje s međunarodnim pravilima i prilagodbu brzo mijenjajućem digitalnom krajoliku.

- Zastupnik korisnika IoT uređaja: Regulacija mora zaštititi prava i privatnost korisnika. Izazovi su u tome što korisnici često nisu svjesni potencijalnih rizika povezanih s IoT uređajima.
- Odvjetnik 1: Uključivanje kibernetske sigurnosti u regulativu IoT je ključno. Izazovi su u usklađivanju zakonodavstva i tehnologije te određivanju tko je odgovoran kada se dogode sigurnosni propusti.
- Odvjetnik 2: Regulacija mora biti proaktivna, a ne reaktivna. Izazovi su u stvaranju zakona koji su tehnološki neutralni, a pružaju dovoljnu zaštitu.
- Inženjer za kibernetičku sigurnost: Regulacija je potrebna za postavljanje standarda sigurnosti koje IoT uređaji moraju ispunjavati. Izazov je što su cyber napadi sve sofisticiraniji, stoga je teško predvidjeti sve moguće scenarije i uključiti ih u regulativu.

Slijedeće pitanje: **Kako biste poboljšali trenutnu regulativu u pogledu IoT-a?**

- Predstavnik HAKOM-a: Bilo bi korisno razviti regulativu koja bi bila specifičnija za različite vrste IoT uređaja i njihove jedinstvene sigurnosne potrebe.
- Pravnik HAKOM-a: Trebali bismo tražiti veću harmonizaciju s međunarodnim pravilima kako bi tvrtke lakše mogle poslovati na globalnoj razini.
- Inženjer telekomunikacija: Regulacija bi trebala uključivati jasne smjernice za dizajn sigurnosti uređaja od samog početka, a ne samo postavljanje minimalnih standarda.
- Pravni stručnjak za IoT: Trebalo bi postojati više obrazovanja i osvješćivanja o sigurnosnim rizicima i važnosti zaštite podataka među korisnicima i proizvođačima IoT uređaja.
- Zastupnik korisnika IoT uređaja: Povećanje transparentnosti oko toga kako IoT uređaji koriste i dijele korisničke podatke moglo bi pomoći korisnicima da donesu informirane odluke.
- Odvjetnik 1: Potrebne su strože sankcije za one koji ne uspiju zaštititi IoT uređaje od kibernetičkih napada.
- Odvjetnik 2: Regulativa bi trebala naglasiti etičke obveze proizvođača IoT uređaja, uključujući poštivanje privatnosti i zaštite podataka.
- Inženjer za kibernetičku sigurnost: Ja bih uveo obvezne redovite revizije sigurnosti IoT uređaja kako bi se osiguralo da oni ostaju sigurni tijekom cijelog vijeka trajanja.

Treće pitanje: Kakva je vaša perspektiva o ravnoteži između regulacije i inovacije u kontekstu IoT-a?

- Predstavnik HAKOM-a: Regulacija i inovacija moraju ići ruku pod ruku. Pravilna regulacija može potaknuti inovacije poticanjem konkurencije i zaštitom potrošača.
- Pravnik HAKOM-a: Regulacija može biti dvosjekli mač. Ako je previše stroga, može ograničiti inovacije, ali ako je previše labava, može ugroziti zaštitu podataka i sigurnost.
- Inženjer telekomunikacija: Snažan regulatorni okvir može potaknuti inovacije jer će tvrtke težiti pronalaženju novih rješenja unutar postavljenih pravila.
- Pravni stručnjak za IoT: Potrebno je pravilno balansirati kako bi se potaknula inovacija, ali i osigurala zaštita korisnika. Ova ravnoteža je ključna za dugoročno održiv rast IoT sektora.
- Zastupnik korisnika IoT uređaja: Iako inovacije donose nove mogućnosti, zaštita potrošača kroz pravilnu regulaciju mora biti na prvom mjestu.
- Odvjetnik 1: Potrebna nam je prilagodljiva regulacija koja može pratiti brze promjene u tehnologiji.
- Odvjetnik 2: Važno je pružiti prostor za inovacije, ali nikada na štetu prava i sigurnosti korisnika.
- Inženjer za kibernetičku sigurnost: Inovacije u sigurnosti IoT-a trebale bi biti istaknuti prioritet. Pravilna regulacija može stimulirati razvoj naprednih sigurnosnih tehnologija.

Četvrto pitanje: Kako vidite ulogu umjetne inteligencije (AI) u IoT-u i koja bi trebala biti regulatorna strategija?

- Predstavnik HAKOM-a: AI ima važnu ulogu u analizi podataka generiranih kroz IoT. Regulatorni okvir bi trebao osigurati etičku upotrebu AI-a i zaštitu podataka.
- Pravnik HAKOM-a: Potrebno je razviti regulatorni okvir koji razumije specifičnosti AI-a i IoT-a, kako bi se riješila pitanja odgovornosti, transparentnosti i prava na privatnost.
- Inženjer telekomunikacija: AI može dramatično poboljšati funkcionalnost IoT-a. Regulacije bi trebale biti fleksibilne kako bi omogućile brzi napredak, ali i zaštitile korisnike.

- Pravni stručnjak za IoT: Uloga AI-a u IoT-u je neizbježna i može donijeti mnogo koristi. Međutim, regulacija mora biti jasna u pogledu etičkih smjernica, transparentnosti i odgovornosti u vezi s korištenjem AI-a.
- Zastupnik korisnika IoT uređaja: AI u IoT-u može pružiti bolju uslugu korisnicima, ali također nosi rizik od kršenja privatnosti i sigurnosnih problema. Regulacija bi trebala biti usredotočena na zaštitu korisnika.
- Odvjetnik 1: AI će imati ključnu ulogu u upravljanju sigurnošću u IoT ekosustavu. Regulacija mora jasno definirati odgovornosti tvrtki koje koriste AI u svojim proizvodima i uslugama.
- Odvjetnik 2: AI i IoT su međusobno povezani. Regulacija bi trebala biti usmjerena na osiguranje transparentnosti, zaštitu podataka i utvrđivanje pravila o odgovornosti.
- Inženjer za kibernetičku sigurnost: AI će biti ključna za obradu i analizu podataka generiranih putem IoT-a. Regulacije bi trebale biti usmjerene na zaštitu podataka, privatnosti i sigurnosti.

Peto pitanje: Kako možemo osigurati da regulacija IoT-a uključuje zaštitu prava korisnika i sigurnost podataka?

- Predstavnik HAKOM-a: Regulacija mora biti usmjerena na zaštitu prava korisnika, posebno kada je u pitanju privatnost i sigurnost podataka. Također, potrebna je i edukacija korisnika o njihovim pravima.
- Pravnik HAKOM-a: Potrebno je uspostaviti stroga pravila o pristupu i korištenju podataka korisnika, uz obvezno osiguranje transparentnosti o tome kako se podaci koriste.
- Inženjer telekomunikacija: Tehnologija za zaštitu podataka mora biti integralni dio svih IoT uređaja i usluga, a regulacija treba osigurati primjenu tih tehnologija.
- Pravni stručnjak za IoT: Uspostava pravnih okvira koji jasno definiraju prava korisnika, obveze tvrtki i mehanizme zaštite podataka ključni su za regulaciju IoT-a. Obvezujuće smjernice i provedba prava korisnika na zaborav i prijenos podataka trebaju biti sastavni dio ovog okvira.

- Zastupnik korisnika IoT uređaja: Regulacija IoT-a mora biti transparentna, korisnički centrirana i omogućiti lako razumljive uvjete korištenja. Također, mora se promicati digitalna pismenost kako bi korisnici bili bolje informirani o svojim pravima.
- Odvjetnik 1: Važno je razviti jasan regulatorni okvir koji nalaže tvrtkama da implementiraju najbolje prakse zaštite podataka i sigurnosne standarde. To uključuje i redovite revizije i provjere usklađenosti.
- Odvjetnik 2: Snažna regulacija u kombinaciji s obrazovanjem korisnika može biti najučinkovitiji način za zaštitu prava korisnika i sigurnosti podataka. Potrebno je jasno definirati koji su korisnički podaci zaštićeni i kako se oni mogu koristiti.
- Inženjer za kibernetičku sigurnost: Uvođenje *security by design* koncepta u razvoj IoT uređaja ključno je za zaštitu prava korisnika i sigurnosti podataka. Regulacija mora naložiti tvrtkama da uključe sigurnosne mjere u sve faze razvoja proizvoda.

Šesto pitanje: Kako možemo osigurati usklađenost IoT uređaja i usluga s domaćim i međunarodnim regulativama?

- Predstavnik HAKOM-a: Pomoću rigoroznih postupaka certifikacije i provjere usklađenosti, uz redovite revizije. Moramo raditi s međunarodnim tijelima kako bismo osigurali da su naše regulative u skladu s globalnim standardima.
- Pravnik HAKOM-a: Stroge sankcije za nepoštivanje pravila i propisa ključne su za osiguranje usklađenosti. Također, važno je edukacija tvrtki o važnosti usklađenosti i posljedicama nepoštivanja.
- Inženjer telekomunikacija: Uz stroge regulative, trebamo razvijati tehnologije koje omogućuju automatsku provjeru usklađenosti IoT uređaja i usluga.
- Pravni stručnjak za IoT: Usklađenost se može osigurati uspostavljanjem jasnih pravila i smjernica, kao i kroz redovite provjere i revizije. Trebali bismo surađivati s međunarodnim tijelima kako bi se osiguralo da su naši standardi usklađeni.
- Zastupnik korisnika IoT uređaja: Važno je da korisnici imaju povjerenje u IoT uređaje i usluge koje koriste. Da bi se to postiglo, tvrtke moraju jasno pokazati da poštuju sve regulative.
- Odvjetnik 1: Usklađenost bi trebala biti uvjet za dobivanje licence za rad. Nepoštivanje bi trebalo rezultirati strogim kaznama, uključujući povlačenje licence.

- Odvjetnik 2: Usklađenost može biti osigurana uspostavljanjem jasnog regulatornog okvira koji je u skladu s međunarodnim standardima, uz stroge provjere i sankcije za nepoštivanje.
- Inženjer za kibernetičku sigurnost: Integracija sigurnosnih funkcija direktno u dizajn IoT uređaja može pomoći u osiguranju usklađenosti. Tvrtke bi trebale biti obvezne da to učine.

Sedmo pitanje: Kako uskladiti brzi tehnološki napredak IoT-a s potrebom za sveobuhvatnim i pravodobnim regulativama?

- Predstavnik HAKOM-a: Regulacije bi trebale biti fleksibilne da se mogu prilagoditi brzom razvoju tehnologije. Također, potrebno je blisko surađivati s tehnološkim tvrtkama kako bi se razumjeli novi trendovi i prilagodili regulative.
- Pravnik HAKOM-a: Moramo razvijati propise koji su tehnološki neutralni, ali koji učinkovito štite prava korisnika i sigurnost podataka.
- Inženjer telekomunikacija: Ključno je razumjeti kako tehnologija funkcionira kako bi se razvila učinkovita regulativa. Potrebna je stalna edukacija i komunikacija s industrijskim sektorom.
- Pravni stručnjak za IoT: Regulacije bi trebale biti dovoljno općenite da pokrivaju širok spektar tehnologija, ali i dovoljno specifične da rješavaju ključne probleme.
- Zastupnik korisnika IoT uređaja: Potrebno je redovito pregledavati i ažurirati regulative kako bi ostale relevantne i u skladu s najnovijim tehnološkim napretkom.
- Odvjetnik 1: Regulacije bi trebale anticipirati tehnološke trendove i unaprijed osigurati odgovarajuću zaštitu."
- Odvjetnik 2: Moramo raditi na regulativama koje su fleksibilne i prilagodljive, ali koje pružaju čvrst okvir za zaštitu prava i sigurnosti.
- Inženjer za kibernetičku sigurnost: Bitno je uključiti stručnjake za sigurnost u proces razvoja IoT uređaja. Oni mogu pružiti dragocjene uvide za stvaranje učinkovitih regulativa.

Osmo pitanje: Kako osigurati transparentnost u upotrebi IoT uređaja i podataka koje generiraju?

Predstavnik HAKOM-a: Ključna je uloga regulacije. Propisi bi trebali zahtijevati od tvrtki da jasno objasne kako koriste podatke i kakvu vrijednost donose korisnicima.

Pravnik HAKOM-a: Potrebna je robusna regulacija koja traži od kompanija da pruže jasne i razumljive informacije korisnicima o tome kako se njihovi podaci koriste i štite.

Inženjer telekomunikacija: Transparentnost se mora integrirati u dizajn uređaja. Na primjer, uređaji bi mogli imati sučelje koje korisnicima omogućuje da vide koje se informacije prikupljaju.

Pravni stručnjak za IoT: Transparentnost bi trebala biti dio ugovora o korisničkom usluzi. Kompanije bi trebale biti jasne o tome što prikupljaju, kako koriste podatke i s kim ih dijele.

Zastupnik korisnika IoT uređaja: Regulacije bi trebale zahtijevati od kompanija da redovito obavještavaju korisnike o prikupljenim podacima i njihovoj upotrebi.

Odvjetnik 1: Transparentnost je ključna za zaštitu prava korisnika. Regulacija bi trebala osigurati da korisnici imaju pristup podacima o tome kako se njihovi podaci koriste i zašto.

Odvjetnik 2: Transparentnost treba biti ugrađena u IoT tehnologije i podržana odgovarajućim zakonodavstvom.

Inženjer za kibernetičku sigurnost: Tehnologija može pomoći u poboljšanju transparentnosti, omogućujući korisnicima da lako vide i kontroliraju podatke koje IoT uređaji prikupljaju.

5.3. Analiza rezultata

Nakon provedene fokus grupe na temu *Pravni aspekti regulacije Interneta stvari (IoT) na tržištu*, uočeni su značajni uvidi i stavovi među sudionicima koji dolaze iz različitih sektora - od predstavnika HAKOM-a, preko inženjera, pravnika, do odvjetnika.

Svi sudionici su prepoznali važnost pravne regulative u kontekstu IoT-a. Pojedinci iz pravne sfere naglasili su potrebu za stvaranjem tehnološki neutralnih zakona koji će osigurati zaštitu korisnika, a inženjeri su podržali ovu perspektivu uz dodatak da regulativa mora biti fleksibilna kako bi omogućila brzi tehnološki napredak.

Uloga AI-a u IoT-u prepoznata je kao ključna, ali i povezana s izazovima u pogledu etike i zaštite podataka. Konsenzus među sudionicima bio je da regulativa treba uspostaviti jasna pravila o transparentnosti i odgovornosti u kontekstu korištenja AI-a u IoT-u.

Zaštita prava korisnika i sigurnost podataka prepoznate su kao osnovni prioriteti. Sudionici su istaknuli potrebu za strogim pravilima o pristupu i korištenju podataka korisnika, ali su također prepoznali važnost edukacije korisnika o njihovim pravima.

U pogledu odgovornosti za moguće štete uzrokovane IoT uređajima, sudionici su izrazili različite stavove. Dok su neki zauzeli stajalište da bi proizvođači trebali snositi odgovornost, drugi su naglasili potrebu za suradnjom različitih strana, uključujući proizvođače, pružatelje usluga i korisnike.

Na temelju ovih uvida, jasno je da postoji zajednički stav o potrebi za sveobuhvatnom i pravno utemeljenom regulativom koja balansira između poticanja inovacija u IoT-u i zaštite interesa korisnika. To je signal regulatorima da je potrebno daljnje usmjeravanje i angažman u ovom području.

6. ZAKLJUČAK

U eri digitalne transformacije, Internet stvari (IoT) postaje neizbježan dio svakodnevnog života. Integracija IoT-a u tržište elektroničkih komunikacija otvara niz novih mogućnosti, ali istovremeno postavlja i niz pravnih izazova koji zahtijevaju sveobuhvatnu regulativu. Pravni aspekti regulacije IoT-a na tržištu elektroničkih komunikacija obuhvaćaju pitanja privatnosti podataka, sigurnosti, intelektualnog vlasništva, međunarodnih ugovora i etičkih standarda. Izazov je u tome što IoT uređaji generiraju goleme količine podataka koje se mogu koristiti za poboljšanje usluga, ali istovremeno mogu predstavljati rizik za privatnost korisnika ako nisu adekvatno zaštićeni.

Europska unija (EU) predstavlja pionira u kreiranju pravnih okvira koji se odnose na IoT. Jedan od najistaknutijih pravnih dokumenata koji je donijela jest Uredba (EU) 2016/679, široko prepoznata kao Opća uredba o zaštiti podataka (GDPR). Ova uredba postavlja rigorozne kriterije u pogledu zaštite podataka građana i, s obzirom na svoju sveobuhvatnost i strogoću, postala je inspiracija i uzor za slične regulative diljem svijeta. Iako GDPR pruža solidnu osnovu u kontekstu zaštite podataka, specifična priroda i složenosti povezane s IoT-om ukazuju na potrebu za dodatnim, ciljanim regulativama. Takve bi regulative trebale rješavati izazove i pitanja koja su jedinstvena za tehnologije bazirane na IoT-u.

Važan aspekt regulacije IoT-a je i sigurnost. Kako broj povezanih uređaja raste, tako raste i površina za potencijalne napade. Regulacija bi stoga trebala postaviti stroge standarde sigurnosti za IoT uređaje i usluge, kako bi se osigurao integritet mreža i zaštitili korisnici.

S druge strane, pravni okvir mora također uvažavati dinamičnost tržišta elektroničkih komunikacija. Treba osigurati dovoljnu fleksibilnost da omogući inovacije, ali i pružiti sigurnost koja će korisnicima omogućiti da s povjerenjem koriste IoT tehnologije.

U kontekstu pravne regulacije IoT-a na tržištu elektroničkih komunikacija u Republici Hrvatskoj, postoji niz zakona koji se već bave pitanjima kibernetičke sigurnosti i zaštite podataka. No, kontinuirani napredak u tehnologiji i promjene na tržištu zahtijevaju stalno prilagođavanje i unaprjeđenje pravnog okvira.

U svjetlu pažljivo provedene analize, točka konsenzusa jest da je ovdje riječ o iznimno kompleksnom području koje zahtijeva daljnju dublju analizu i sveobuhvatan pristup. Regulacija IoT-a predstavlja izazov, koji se prostire od tehničkih pitanja poput arhitekture i implementacije

tehnologija poput 5G i umjetne inteligencije, do pravnih i etičkih pitanja vezanih za zaštitu podataka, privatnost i sigurnost.

Proučavajući međunarodne pristupe, uočene su određene zajedničke teme kao i razlike. Iz takve analize proizlazi zaključak da postoji žurna potreba za koherentnim međunarodnim odgovorom na izazove koji se javljaju, sa ciljem zaštite korisnika, ali i kako bi se potaknuo kontinuirani rast i inovacije unutar sektora IoT-a.

U kontekstu Republike Hrvatske, posebna pažnja bila je posvećena tržištu elektroničkih komunikacija i regulativi vezanoj za kibernetičku sigurnost. Analiza ukazuje na važnost proaktivnog pristupa i potrebu za adaptacijom u svjetlu novih izazova koje donosi IoT.

S obzirom na proučavanje regulativa EU-a, kao i globalnih pravnih standarda, moguće je zaključiti da postoji imperativ kreiranja regulativa koje su u stanju pratiti dinamičan tehnološki razvoj, a da pritom osiguravaju zaštitu temeljnih prava i osiguravaju sigurnost pojedinaca.

Smatrajući da je teorija sama po sebi nedostatna, provedena je i fokus grupa koja omogućava dublji uvid u mišljenja i stavove ključnih dionika. Sudionici fokus grupe, uključujući predstavnike Hrvatske regulatorne agencije za mrežne djelatnosti (HAKOM), inženjere, pravnike i odvjetnike, pružili su korisne informacije i uvide koji su obogatili analizu. Iz provedene fokus grupe, uočeni su vrijedni uvidi iz prakse i stavova relevantnih dionika. Unatoč različitosti njihovih pozicija i perspektiva, postoji zajednička želja za kreiranjem regulative koja će omogućiti razvoj i inovacije, ali i osigurati adekvatnu zaštitu korisnika. Svaki od sudionika donio je jedinstvenu perspektivu, bilo da se radi o tehničkim aspektima IoT-a, pravnim izazovima, ili čak etičkim pitanjima. Ovi različiti stavovi pomogli su u stvaranju složene, ali sveobuhvatne slike o tome kako se različiti sektori nose s pitanjima koja donosi IoT.

Kroz ovaj rad jasno je da će izazovi regulacije IoT-a biti multidisciplinarni i da će zahtijevati sveobuhvatni pristup kako bi se ostvario balans između inovacija, zaštite korisnika i sigurnosti.

Također, kroz ovaj sveobuhvatni pristup, dani su ne samo teorijski uvidi o pravnim aspektima regulacije IoT-a, već su pružene i praktične, stvarne perspektive koje mogu pomoći u daljnjem razumijevanju i rješavanju izazova koje pred nas stavlja IoT.

Iz zaključaka ovog rada, jasno je da je pitanje regulacije IOT-a, složeno i zahtjeva multidisciplinarni pristup. Izazovi sežu od tehničkih aspekata, poput arhitekture i

implementacije tehnologija poput 5G i AI-a, do pravnih i etičkih pitanja vezanih za zaštitu podataka, privatnost i sigurnost.

Tehnički aspekti su od ključnog značaja. Arhitektura i implementacija tehnologija poput 5G i AI-a postavljaju temelje za funkcioniranje IoT-a. Ove napredne tehnologije donose brojne prednosti, uključujući povećanu brzinu prijenosa podataka, veću efikasnost i mogućnost za implementaciju sofisticiranih IoT rješenja. No, istodobno, predstavljaju i izazove za inženjere i stručnjake u području IT-a. Kako se te tehnologije brzo razvijaju, stručnjaci moraju biti u koraku s najnovijim dostignućima kako bi osigurali sigurnost, stabilnost i učinkovitost ovih sistema.

No, izazovi nisu ograničeni samo na tehničke aspekte. Pravna i etička pitanja su jednako bitna. Na primjer, pitanja zaštite podataka, privatnosti i sigurnosti su sve važniji u svijetu gdje su digitalne tehnologije sveprisutne. Kako bi se zaštitili korisnici IoT-a, potrebno je razviti pravni okvir koji će omogućiti odgovarajuću regulaciju ove tehnologije, ali i omogućiti njen daljnji razvoj.

Sve ove različite komponente stvaraju složenost koja zahtijeva multidisciplinarni pristup, pokazujući da rješavanje izazova regulacije IOT-a, zahtijeva integrirani napor koji uključuje tehničko znanje, pravnu stručnost i visoku etičku osviještenost, što priznat ćemo, nije nimalo jednostavno za ostvariti.

LITERATURA

1. Alba, E., & Saborido, R. (2020). Software systems from smart city vendors. Cities, 101, 102690. https://doi.org/10.1016/j.cities.2020.102690
2. Aijaz, A., Simsek, M., Dohler, M., & Fettweis, G. (2017). Shaping 5G for the Tactile Internet. In 5G Mobile Communications (pp. 677-691). https://doi.org/10.1007/978-3-319-34208-5_25
3. Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. IEEE Internet Computing, 21(2), 34–42.
4. Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C. K., & Zhang, J. C. (2014). What will 5g be? IEEE Journal on selected areas in communications, 32(6), 1065–1082.
5. Al-Fuqaha, A., Guizani, M., Mohammadi, M., & Aledhari, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. IEEE Communications Surveys & Tutorials, 17(4), Fourthquarter 2015. https://doi.org/10.1109/COMST.2015.2444095
6. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010
7. Arkin, R. C. (2009). Governing Lethal Behavior in Autonomous Robots. CRC Press. https://doi.org/10.1201/9781420085952.
8. Brynjolfsson, E. (2017). AI and the Economy.
9. Bandyopadhyay, D., & Sen, J. (2011). Internet of Things - Applications and Challenges in Technology and Standardization. Wireless Personal Communications, 58(1), 49-69.
10. Beştepe, F., & Özkan Yildirim, S. (2022). Acceptance of IoT-based and sustainability-oriented smart city services: A mixed methods study. Sustainable Cities and Society, 80, 103794. https://doi.org/10.1016/j.scs.2022.103794
11. Bodenheimer, D. Z. (2016). The Internet of Things' Tsunami of Legal Conundrums. GPSolo, 33, 74.
12. Brill, H., & Jones, S. (2017). Little Things and Big Challenges: Information Privacy and the Internet of Things. American University Law Review, 66, 1183.
13. Capisizu, L.-A. (2018). Legal Perspectives on the Internet of Things.

14. Chih-Lin, I., Han, S., Xu, Z., Sun, Q., & Pan, Z. (2014). 5G: rethink mobile communications for 2020+. Philosophical Transactions of the Royal Society A, 372(2014). https://doi.org/10.1098/rsta.2014.0432
15. Chong, M., Habib, A., Evangelopoulos, N., & Park, H. W. (2018). Dynamic capabilities of a smart city: An innovative approach to discovering urban problems and solutions. Government Information Quarterly, 35(4), 682–692. https://doi.org/10.1016/j.giq.2018.07.005
16. Choi, H.-S., & Song, S.-K. (2023). Direction for a Transition toward Smart Sustainable Cities based on the Diagnosis of Smart City Plans. Smart Cities, 6(1), 156–178. https://doi.org/10.3390/smartcities6010009
17. Chowdhury, M. Z., Shahjalal, M., Hasan, M. K., & Jang, Y. M. (2019). The Role of Optical Wireless Communication Technologies in 5G/6G and IoT Solutions: Prospects, Directions, and Challenges.
18. Collotta, M., & Pau, G. (2014). A Solution Based on Bluetooth Low Energy for Smart Home Energy Management. Energies, 8(10), 11916-11938. https://doi.org/10.3390/en81011916
19. Coskun, V., Ozdenizci Kose, B., & Ok, K. (2013). A survey on Near Field Communication (NFC) technology. Wireless Personal Communications, 71(3). https://doi.org/10.1007/s11277-012-0935-5
20. Dang, S., Amin, O., Shihada, B., & Alouini, M-S. (2020). What should 6G be?
21. DeNardis, L. & Raymond, M. (2017). The Internet of Things as a Global Policy Frontier. UC Davis Law Review, 51(2).
22. Ercan, T., & Kutay, M. (2021). Smart cities critical infrastructure recommendations and solutions. In Solving Urban Infrastructure Problems Using Smart City Technologies (pp. 503-541). Handbook on Planning, Design, Development, and Regulation. https://doi.org/10.1016/B978-0-12-816816-5.00024-3
23. European Commission. (n.d.). Internet of Things policy. https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy
24. European Commission. (2021, April 21). Artificial Intelligence Act: Commission proposes a legal framework - questions and answers. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

25. EIT Digital. (2022). Artificial Intelligence Report. https://www.eitdigital.eu/fileadmin/2022/ecosystem/makers-shapers/reports/EIT-Digital-Artificial-Intelligence-Report.pdf
26. Fabiano, N. (2017). Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation. Athens Journal of Law, 3(3), 201–214. https://doi.org/10.30958/ajl.3-3-2
27. Fabrègue, B. F. G., & Bogoni, A. (2023). Privacy and Security Concerns in the Smart City. Smart Cities, 6(1), 586–613. https://doi.org/10.3390/smartcities6010027
28. Fornasier, M. de O. (2019). The Applicability of the Internet of Things (IoT) between Fundamental Rights to Health and to Privacy.
29. French Ministry of Higher Education, Research and Innovation. (n.d.). White Paper on Artificial Intelligence - A European approach to excellence and trust. https://www.ouvrirlascience.fr/white-paper-on-artificial-intelligence-a-european-approach-to-excellence-and-trust/
30. Gasser, U. (2015). Interoperability in the Digital Ecosystem. Berkman Klein Center for Internet and Society Research Publication No. 2015-13.
31. Goldsmith, J. (2019, March 18). Sovereign Difference and Sovereign Deference on the Internet. THE YALE
32. Goanta, C., & Ranchordás, S. (2020). The New City Regulators: Platform and Public Values in Smart and Sharing Cities. Computer Law & Security Review, 36, 105375. https://doi.org/10.1016/j.clsr.2019.105375
33. Greenfield, A. (2017). Radical Technologies: The Design of Everyday Life. Verso.
34. Große, C. (2022). Development and status of the European approach to AI: From ethics to regulation. Computer Law Review International, 23, 1–7. https://link.springer.com/article/10.1007/s44206-022-00025-z
35. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010
36. Guo, P., Qiao, W., Sun, Y., Liu, F., & Wang, C. (2019). Telemedicine Technologies and Tuberculosis Management: A Randomized Controlled Trial. Telemedicine and e-Health, 26(9), 1150-1156. https://doi.org/10.1089/tmj.2019.0190
37. Guinard, D., Fischer, M., & Trifa, V. (2010). Sharing using social networks in a composable Web of Things. Pervasive Computing and Communications Workshops

(PERCOM Workshops), 2010 8th IEEE International Conference on. https://doi.org/10.1109/PERCOMW.2010.5470524

38. Hadzovic, S., Mrdovic, S., & Radonjic, M. (2021). Identification of IoT Actors. Sensors, 21, 2093. https://doi.org/10.3390/s21062093
39. Hall, W. (2017, October 16). Professor Dame Wendy Hall calls for UK to extract value from AI in major review. https://www.ecs.soton.ac.uk/news/5478.
40. Hildebrandt, M. (2019, March). Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning. Theoretical Inquiries in Law, 20(1), 83-121. https://doi.org/10.1515/til-2019-0004.
41. Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019). Smart cities: Advances in research—An information systems perspective. International Journal of Information Management, 47, 88–100. https://doi.org/10.1016/j.ijinfomgt.2019.01.004
42. Jara, A. J., Alcolea, A. F., Zamora, M. A., & Skarmeta, A. F. G. (2010). Analysis of different techniques to define metadata structure in NFC/RFID cards to reduce access latency, optimize capacity, and guarantee integrity. IFAC Proceedings Volumes, 43(4), 192-197. https://doi.org/10.3182/20100701-2-PT-4011.00034
43. Kaminski, M. E. (2023). Regulating the Risks of AI. Boston University Law Review, 103. U of Colorado Law Legal Studies Research Paper No. 22-21. https://ssrn.com/abstract=3936686
44. Kaminski, M. E., & Urban, J. M. (2021). The Right to Contest AI. Columbia Law Review, 121(7). U of Colorado Law Legal Studies Research Paper No. 21-30. https://ssrn.com/abstract=3890205
45. Kahneman, D. (2021, May 16). Clearly AI is going to win. How people are going to adjust is a fascinating problem. https://www.theguardian.com/books/2021/may/16/daniel-kahneman-clearly-ai-is-going-to-win-how-people-are-going-to-adjust-is-a-fascinating-problem-thinking-fast-and-slow.
46. Kaplan, A., & Haenlein, M. (2018, November). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, 62(1). https://doi.org/10.1016/j.bushor.2018.08.004.
47. Kelion, L. (2021, April 26). The EU path towards regulation on artificial intelligence. Brookings Institution. https://www.brookings.edu/blog/techtank/2021/04/26/the-eu-path-towards-regulation-on-artificial-intelligence/

48. Kim, N., & Yang, S. (2023). Conceptually Related Smart Cities Services from the Perspectives of Governance and Sociotechnical Systems in Europe. Systems, 11(4), 166. https://doi.org/10.3390/systems11040166
49. Kortuem, G., Kawsar, F., Fitton, D., & Sundramoorthy, V. (2010). Smart Objects as Building Blocks for the Internet of Things. IEEE Internet Computing, 14(1), 44 - 51. https://doi.org/10.1109/MIC.2009.143
50. Larsson, E., Edfors, O., Tufvesson, F., et al. (2014). Massive MIMO for Next Generation Wireless Systems. IEEE Communications Magazine, 52, 186-195. https://doi.org/10.1109/MCOM.2014.6736761
51. Lee, S. (2023). The Acceptance Model of Smart City Service: Focused on Seoul. Sustainability, 15(3), 2695. https://doi.org/10.3390/su15032695
52. Li, F.-F., & Horvitz, E. (2023). AI and Human Values: A Conversation with Fei-Fei Li and Eric Horvitz. https://events.stanford.edu/event/ai_and_human_values_a_conversation_with_fei-fei_li_and_eric_horvitz.
53. Malik, R., Visvizi, A., Troisi, O., & Grimaldi, M. (2022). Smart Services in Smart Cities: Insights from Science Mapping Analysis. Sustainability, 14(11), 6506. https://doi.org/10.3390/su14116506
54. Miguelez, C. V., Baeza, V. M., Parada, R., & Monzo, C. (2023). Guidelines for Renewal and Securitization of a Critical Infrastructure Based on IoT Networks. Smart Cities, 6(2), 728-743. https://doi.org/10.3390/smartcities6020035
55. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, Applications and Research Challenges. Ad Hoc Networks, 10(7). https://doi.org/10.1016/j.adhoc.2012.02.016
56. NGIoT. (2022.). White Paper on Artificial Intelligence - Public Consultation. https://www.ngiot.eu/white-paper-on-artificial-intelligence-public-consultation/
57. Palattella, M. R., Dohler, M., Grieco, L. A., & Rizzo, G. (2016). Internet of Things in the 5G Era: Enablers, Architecture and Business Models. IEEE Journal on Selected Areas in Communications, 34(3), 1-1. https://doi.org/10.1109/JSAC.2016.2525418
58. Peoples, C. (2021). Solving Urban Infrastructure Problems Using Smart City Technologies. In Handbook on Planning, Design, Development, and Regulation (pp. 159-182). https://doi.org/10.1016/B978-0-12-816816-5.00008-5

59. Petrova, M., & Tairov, I. (2022). Solutions to Manage Smart Cities' Risks in Times of Pandemic Crisis. Risks, 10(12), 240. https://doi.org/10.3390/risks10120240
60. Poulsen, N. (2022.). Secure IoT Device Identities. Intertrust. https://www.intertrust.com/resources/secure-iot-device-identities/
61. Ranchordás, S., & Goanta, C. (2020). The New City Regulators: Platform and Public Values in Smart and Sharing Cities. Computer Law & Security Review, 36, 105375. https://doi.org/10.1016/j.clsr.2019.105375
62. Saborido, R., & Alba, E. (2020). Software systems from smart city vendors. Cities, 101, 102690. https://doi.org/10.1016/j.cities.2020.102690
63. Schneier, B. (2016). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (Reprint ed.). W. W. Norton & Company.
64. Sheng, Z., Wang, H., Yin, C., & Hu, X. (2015). Lightweight Management of Resource Constrained Sensor Devices in Internet-of-Things. IEEE Internet of Things Journal, 2(5), 1-1. https://doi.org/10.1109/JIOT.2015.2419740
65. Siekkinen, M., Hiienkari, M., Nurminen, J. K., & Nieminen, J. (2012). How low energy is Bluetooth low energy? Comparative measurements with ZigBee/802.15.4. https://doi.org/10.1109/WCNCW.2012.6215496
66. Siegel, J. (2020). When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers' Perspective. Journal of High Tech Law, 20, 189.
67. Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 37–56). Hoboken, New Jersey: Wiley.
68. Trachtman, J. P. (2019). Cybersecurity versus Trade in Internet of Things Products. Manchester Journal of International Economic Law, 16, 301.
69. van Schewick, B. (2010). Internet Architecture and Innovation. The MIT Press.
70. Vandercruysse, L., Buts, C., & Dooms, M. (2020). A typology of Smart City services: The case of Data Protection Impact Assessment. Cities, 104, 102731. https://doi.org/10.1016/j.cities.2020.102731
71. Viljoen, S. (2013). The socio-political implications of an Internet of Things. First Monday, 18(11). https://journals.sagepub.com/doi/10.1177/20539517231153811

72. Xiong, X., Dai, Y., Hu, Z., Huo, K., Bai, Y., Li, H., & Liu, D. (2021). Hardware Sharing for Channel Interleavers in 5G NR Standard. Security and Communication Networks, 2021, Article ID 8872140. https://doi.org/10.1155/2021/8872140
73. Wang, C., Di Renzo, M., Stanczak, S., Wang, S., & Larsson, E. G. (2020). Artificial Intelligence Enabled Wireless Networking for 5G and Beyond: Recent Advances and Future Challenges. IEEE Wireless Communications, 27(1), 16-23. https://doi.org/10.1109/MWC.001.1900292
74. Weber, M., & Žarko, I. P. (2019). A Regulatory View on Smart City Services. Sensors, 19(2), 415. https://doi.org/10.3390/s19020415
75. Weber, R. H. (2017). Liability in the Internet of Things. Journal of European Consumer and Market Law, 6. https://heinonline.org/HOL/LandingPage?handle=hein.kluwer/jeucml0006&div=53&id=&page=
76. Zanella, A., Bui, N., Castellani, A., & Vangelista, L. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), February 2014.
77. Zhang, H. E., Wong, K. H., & Chang, V. (2019). Patent Analysis in the 5G Network. Journal of Global Information Management, 29(6), 1-28. https://doi.org/10.4018/JGIM.20211101.oa28

OSTALI IZVORI

78. 5G.NRW. (2022, February 14). Elf neue EU-geförderte 5G-Forschungsprojekte.
79. 5G zvjezdarnica. (2022, February 21). 13. Quartalsbericht des 5G-Observatoriums.
80. Accenture. (2022, February 21). Utjecaj 5G na europsko gospodarstvo (EU-Studie im Auftrag von Qualcomm).
81. Bundesministerium für Digitales und Verkehr. (2022, February 21). Connecting Europe Facility 2 – Digital (CEF Digital).
82. Bundesministerium für Wirtschaft und Klimaschutz. (2022, February 15). Frankreich und Deutschland fördern gemeinsam vier Kooperationsprojekte zu 5G-Anwendungen für private Netzwerke.
83. Bundesnetzagentur. (2022, February 17). Bundesnetzagentur veröffentlicht Netzabdeckung mit 5G.

WEB IZVORI

84. AI and Human Values: A Conversation with Fei-Fei Li and Eric Horvitz. (2023). Stanford Institute for Human-Centered Artificial Intelligence (HAI). https://events.stanford.edu/event/ai_and_human_values_a_conversation_with_fei-fei_li_and_eric_horvitz.
85. Calo, R. (2021, April 22). The Regulation of Artificial Intelligence: A Conversation with Ryan Calo. https://techpolicy.press/the-regulation-of-artificial-intelligence-a-conversation-with-ryan-calo/.
86. Crawford, K. (2021, June 6). Microsoft's Kate Crawford: 'AI is neither artificial nor intelligent'. https://www.theguardian.com/technology/2021/j.
87. Ekonomija IHS / Tehnologija IHS. (2022, February 21). 5G gospodarstvo: Kako će 5G tehnologija doprinijeti globalnom gospodarstvu.
88. Europäischer Rechnungshof. (2022, February 15). Verzögerungen beim Mobilfunk: 5G in der EU braucht einen Booster.
89. Europska komisija. (n.d.). Akcijski plan za 5G. https://digital-strategy.ec.europa.eu/hr/policies/5g-action-plan.
90. Europska komisija. (2022, February 17). Alat za povezivanje.
91. Gartner. (2022, February 14). Gartner predviđa rast prihoda od svjetske 5G mrežne infrastrukture za 39% u 2021.
92. Lee, K.-F. (2017, June 24). The Real Threat of Artificial Intelligence. https://www.nytimes.com/2017/06/24/opinion/sunday/artificial-intelligence-economic-inequality.html.
93. Musk, E., et al. (2023, March 29). Elon Musk and Others Call for Pause on A.I., Citing 'Profound Risks to Society'. https://www.nytimes.com/2023/03/29/technology/ai-artificial-intelligence-musk-risks.html.
94. Qualcomm. (2022, February 15). 5G pokreće gospodarski rast, otpornost i održivost (Auftragsstudie eines Chipherstellers).
95. Russell, S. (2020, May 12). Why we need to rethink the purpose of AI: A conversation with Stuart Russell. https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-we-need-to-rethink-the-purpose-of-ai-a-conversation-with-stuart-russell.
96. Statista. (2022, February 17). Umsatz mit 5G-Netzwerktechnik weltweit im Jahr 2020 und Prognose bis 2022.

97. Thrun, S. (2016, September 14). Sebastian Thrun Talks Self-Driving Cars on Udacity Talks!
98. Vallor, S. (2022). An Introduction to Data Ethics. https://www.scu.edu/media/ethics-center/technology-ethics/IntroToDataEthics.pdf.
99. Wallach, W. (2018, December 7). Control and Responsible Innovation of Artificial Intelligence. Artificial Intelligence & Equality Initiative.
100. Yudkowsky, E. (2023, March 29). Pausing AI Developments Isn't Enough. We Need to Shut it All Down.https://digital-strategy.ec.europa.eu/en/policies/internet-things-policy,
101. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682, https://www.eitdigital.eu/fileadmin/2022/ecosystem/makers-shapers/reports/EIT-Digital-Artificial-Intelligence-Report.pdf
102. https://www.ouvrirlascience.fr/white-paper-on-artificial-intelligence-a-european-approach-to-excellence-and-trust/
103. https://link.springer.com/article/10.1007/s44206-022-00025-z
104. https://journals.sagepub.com/doi/10.1177/20539517231153811
105. https://www.ngiot.eu/white-paper-on-artificial-intelligence-public-consultation/
106. https://www.intertrust.com/resources/secure-iot-device-identities/
107. https://www.brookings.edu/blog/techtank/2021/04/26/the-eu-path-towards-regulation-on-artificial-intelligence/

PRAVNI IZVORI

Nacionalni pravni propisi:

1. Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/18)
2. Zakon o elektroničkim komunikacijama (NN br. 76/2022)
3. Kazneni zakon (NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22)

Eu regulativa:

GDPR - Opća uredbe o zaštiti podataka, 2018

AI Act - Zakon o umjetnoj inteligenciji, AI Act, 2021

NIS 1 i NIS 2 direktive

Međunarodna regulativa:

DSA - Digital Services Act

DMA - Digital Markets Act

ŽIVOTOPIS

Željka Grgec rođena je 03. rujna 1968. godine u Zagrebu, gdje je završila osnovnu i srednju školu. Na Pravnom fakultetu u Zagrebu diplomirala je 1993. godine.

Od listopada 1993. godine do ožujka 1995. godine, radila je kao vježbenica u Državnom zavodu za statistiku RH, u kojem je položila državni stručni ispit.

Od ožujka 1995. godine do prosinca 1996. godine, radila je kao vježbenica na Prekršajnom sudu u Zagrebu, te je u okviru toga obavljala praksu na Županijskom sudu u Zagrebu, Općinskom građanskom sudu u Zagrebu te Općinskom kaznenom sudu u Zagrebu.

Pravosudni ispit položila je 30. listopada 1996. godine.

Od prosinca 1996. godine do prosinca 1997. godine radila je kao sudske savjetnica na Prekršajnom sudu u Zagrebu.

U prosincu 1997. godine, imenovana je na dužnost sutkinje Prekršajnog suda u Zagrebu.

U siječnju 2011. godine, imenovana je Odlukom Državnog sudbenog vijeća na dužnost predsjednice Prekršajnog suda u Zagrebu, na kojoj dužnosti je bila do listopada 2013. godine.

Za vrijeme obnašanja dužnosti sutkinje i predsjednice suda, sudjelovala je u različitim radnim skupinama vezanim za donošenje zakona i podzakonskih propisa iz različitih područja prava, te na brojnim edukacijama iz različitih područja prava, kao i u projektima Europske unije .

Od veljače 2015. godine radi u Hrvatskoj regulatornoj agenciji za mrežne djelatnost (dalje: HAKOM) najprije na radnom mjestu Višeg stručnjaka za pravne poslove, a od veljače 2016. godine na radnom mjestu Rukovoditeljice Odjela željezničkih usluga (dalje: Odjel), koji je nastao pripajanjem Agencije za regulaciju tržišta željezničkih usluga HAKOM-u, 2014. godine. Navedeni Odjel, sada Sektor, bavi se regulacijom tržišta željezničkih usluga i pravima putnika u željezničkom prijevozu.

Kao Viši stručnjak za pravne poslove, osim obavljanja redovnih poslova pružanja pravne pomoći Vijeću i Ravnatelju HAKOM-a, aktivno je radila na projektu MAMEFORCE standarda kojeg je nositeljica Pravobraniteljica za ravnopravnost spolova Republike Hrvatske, sa kojom je surađivala na istom, a rezultat toga rada i suradnje je dodjela osnovnog te kasnije i naprednog MAMEFORCE standarda, kao i DADEFORCE standarda HAKOM-u., u prosincu 2017. godine u Hrvatskom saboru.

MAMEFORCE Standard je znak kvalitete kojim se potvrđuje da poslodavac raspolaže visokim stupnjem kompetentnosti u organizaciji rada koja omogućava kompatibilan odnos posla i privatnog života. Ujedno, organizacija koja posjeduje MAMFORCE© Standard služi kao dobar primjer ostatku tržišta u prilagodbi njihovih praksi usklađenja profesionalnog i privatnog života.

Kao Rukovoditeljica Odjela, između ostalog, započela je sa praksom organizacije tematskih Okruglih stolova s ciljem da HAKOM bude inicijator rješavanja izazova na tržištu željezničkih usluga u RH i to kroz zajedničku raspravu svih dionika na tržištu željezničkih usluga, kako bi se potaknuli svi dionici na tom tržištu, na stvaranje boljih uvjeta za funkcioniranje navedenog tržišta i kako bi se ukazalo na sve aktualnosti u željezničkom sektoru. Okruglim stolovima prethodili su tematski pripremni sastanci, na kojima su obrađivani konkretni izazovi,na kojima su sudjelovali i svi relevantni čimbenici na željezničkom tržištu, shodno problematici i području koje je obrađivano, te predstavnici resornih ministarstava ovisno o sadržaju teme koja je obrađivane na svakom pojedinom Okruglom stolu. U skladu s tim, prvi takav Okrugli stol održan je u rujnu 2016. godine u Rijeci na temu „Izazovi u prijevozu robe željeznicom iz morskih luka s posebnim osvrtom na luku Rijeka“, drugi je održan u Splitu, u svibnju 2017. godine na temu „Regija jug i važnost luka u navedenoj regiji- Šibenik, Split i Ploče“, te treći Okrugli stol, u rujnu 2017.godine u Vukovaru, na temu „Slavonija i važnost luka unutarnjih voda- Vukovar, Osijek i Slavonski Brod“.

Aktivno je sudjelovala kao članica Radne grupe u izradi Izmjena i dopuna Zakona o željeznici i u izradi novog Zakonu o regulaciji tržišta željezničkih usluga i zaštiti prava putnika u željezničkom prijevozu, pri Ministarstvu mora, prometa i infrastrukture.

Također je sudjelovala kao članica Radne grupe u okviru HAKOM-a, u izradi Izmjena i dopuna Zakona o elektroničkim komunikacijama, a u suradnji sa Ministarstvom mora, prometa i infrastructure te u izradi novog Zakona o željeznici, kao članica Radne grupe, pri Ministarstvu mora, prometa i infrastrukture.

U svom dosadašnjem redovnom radu aktivno je surađivala i surađuje s brojnim tijelima i organizacijama Europske komisije.

Članica je Hrvatskog društva za transportno pravo (HDTP), od njegovog osnutka na Pravnom fakultetu Sveučilišta u Zagrebu 2016. godine te Hrvatskog društva za pravo i politiku tržišnog

natjecanja (HDPPTN) od osnutka 2018. godine, također na Pravnom fakultetu Sveučilišta u Zagrebu.

Trenutno radi kao Viši stručnjak za pravne poslove u Odjelu pravnih poslova HAKOM-a.

BIOGRAPHY

Željka Grgec was born on September 3, 1968 in Zagreb where she finished elementary and high school. She graduated from the Faculty of Law in Zagreb in 1993.

From October 1993 until March 1, 1995, she worked as a trainee at the StateBureau of Statistics of the Republic of Croatia whereshe passed a state exam.

Between March 1995 and December 1996, she worked as an apprentice at the Zagreb Misdemeanour Court, and the County Court of Zagreb, the Municipal Civil Court in Zagreb and the Municipal Criminal Court in Zagreb.

On October 30, 1996 she passed the judicial exam.

From December 1996 to December 1997 she worked as judicial counsellor at the Misdemeanour Court in Zagreb.

In April 1997 she was appointed the Judge of the Misdemeanour Court in Zagreb.

In January 2011, she was appointed to serve as the President of the Misdemeanour Court in Zagreb by the Decision of the State Judicial Council where she stayed until October 2013.

She held office as judge and president of the court participating in various working groups relatedto the adoption oflaws and by-laws from different fields of law, as well as numerous education from different areas of law as well as the EU projects.

Since February 2015 she has been working at theCroatian Regulatory Authority for Network Industries (hereinafter: HAKOM). Ms. Grgec first served as Senior Legal Expert. Since February 2016 she has been holding position as Head of the Railway Services Department (hereinafter: Department) founded by merging Railway Service Regulatory Agency, 2014 to HAKOM. The afore -mentioned Departmentdeals with the regulation of the rail services market andtherights of passengers in the rail transport.

As a senior legal expert, in addition to carrying out regular legal aid tasks to the Council and Director of HAKOM she has been actively working on the MAMEFORCE project in cooperation with the project holder, the Gender Equality Ombudsperson of the Republic of Croatia and the result of that work and the co-operation is the award of the basic and later advanced MAMEFORCEstandards as well as theDADEFORCE standard HAKOM,in December 2017 in the CroatianParliament.

MAMFORCE ©Standard is a sign of quality that confirms that an employer has a high degree of competency in a work organization that enables a compatible relation between work and private life. At the same time, the organization that owns MAMFORCE © Standard serves as a good example of the rest of the market in adapting their practice of harmonizing professional and private life.

As the Head of Department, among other things, she began the practice of organizing Round Table Roundtables with the aim of making HAKOM the initiator for facing the challenges of the rail services market in Croatia through the joint discussion of all stakeholders in the railway service market, in order to encourage all stakeholders in this market to create better conditions for the operation of the said market and to point to all the actualities in the rail sector. The round tables were preceded by the thematic preparatory meetings addressing the concrete challenges that all relevant factors on the rail market were faced with , including issues and areas addressed, and representatives of the ministries depending on the topics dealt on each Round Table. Accordingly, the first Roundtable was held in September 2016 in Rijeka on the topic "Challenges in the transport system by sea from a sea port with a special focus on the port of Rijeka", the second was held in Split in May 2017 on the topic " Region south and the importance of ports in the mentioned region - Šibenik, Split and Ploče, and the third Round Table in Vukovar, September 2017, on "Slavonia and the Importance of Inland Waterways - Vukovar, Osijek and Slavonski Brod".

She has actively participated as a member of the Working Groupin drafting amendments to the Railway Act andin the drafting ofa new law regulating the railways marketand protecting the rights of passengers in rail transport at the Ministry of the Sea, Transport and Infrastructure. She also participated as a member of the Working Group within HAKOM in drafting the Amendments tothe Electronic Communications Act, in cooperation with the Ministry of the Sea, Transport and Infrastructure. She is currently participatingin the drafting of the

newRailway Act as a member of the Working Group in the Ministry of the Sea, Transport and Infrastructure.

In her regular work so far, she has actively cooperated with numerousbodies and organizations of the European Commission.

She is a member of HDTP (Croatian Transport Law Association) since its foundation at the Faculty of Law of the University of Zagreb, as well as HDPPTN (Croatian Competttition Law and Policy Association), also since its foundation at the Faculty of Law of the University of Zagreb.
She is currently employed as a Senior Expert in the Legal Affairs Department of HAKOM.