

**SVEUČILIŠTE U ZAGREBU  
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA  
EKONOMSKI FAKULTET**

**SVEUČILIŠTE J.J. STROSSMAYERA U OSIJEKU  
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I  
INFORMACIJSKIH TEHNOLOGIJA**

**SVEUČILIŠTE U SPLITU  
FAKULTET ELEKTROTEHNIKE, STROJARSTVA I BRODOGRADNJE**

# **Pogled u budućnost 2020**

---

**Projekt suradnje s  
Hrvatskom regulatornom agencijom za mrežne djelatnosti**

***1.9.-31.12. 2017***



Zagreb, siječanj 2018.

## Sadržaj

<b>1. LTE-M.....</b>	<b>3</b>
1.1. Uvod.....	3
1.2. Obilježja LTE-M.....	3
1.2.1. LTE PSM.....	5
1.2.2. LTE eDRX.....	5
1.3. Prednost i mane LTE-M.....	6
1.4. Slučajevi uporabe LTE-M.....	7
1.5. Raširenost LTE-M.....	8
1.6. Literatura.....	9
<b>2. Poboljšanje kvalitete života osoba s invaliditetom kroz harmonizaciju društvene osviještenosti i usluga telekom operatora.....</b>	<b>10</b>
Izveštaj sa skupa i okruglog stola „Osobe s invaliditetom u digitalnom društvu“.....	10
<b>3. Širokopolasni pristup Internetu u ruralnim područjima.....</b>	<b>14</b>
3.1. Širokopolasni ekosustav ruralnih područja.....	14
3.2. Pregled obilježja novih telekomunikacijskih širokopolasnih rješenja.....	15
a) Širokopolasne tehnologije.....	15
b) Širokopolasne usluge.....	18
3.3. Primjena tehnologija i usluga Interneta stvari u poljoprivredi.....	20
3.4. Literatura.....	24
<b>4. Odabrani pravno-regulatorni aspekti interneta stvari.....</b>	<b>25</b>
Izvešće o istraživanju započetom u zadnjem kvartalu 2017.g. ....	25
<b>5. Internet stvari: studijski primjer pametnog grada.....</b>	<b>34</b>
5.1. Uvod.....	34
5.2. Pametni sustavi - funkcijske komponente pametnog grada.....	34
5.3. Domena pametnog grada s motrišta Interneta stvari.....	36
5.4. Lanac vrijednosti Interneta stvari.....	38
5.5. Normizacijski i regulatorni aspekti.....	39
5.6. Literatura.....	41

## 1. LTE-M

### 1.1. Uvod

LTE-M je kratica za LTE Cat-M1 (engl. *Long Term Evolution Category M1*) ili prevedeno, kategorija M1 dugoročne evolucije mreže. Riječ je o tehnologiji za omogućavanje Interneta stvari (engl. *Internet of Things*, IoT) u okviru javne pokretne mreže LTE, bez potrebe za korištenjem mrežnog pristupnika i samo korištenjem pokretnog uređaja na baterije [1]. LTE-M dugoočekivani je odgovor standardizacijske organizacije 3GPP (*3rd Generation Partnership Project*) na rastuću potražnju za mrežnim tehnologijama velikog dometa uz malu potrošnju baterije (engl. *Low-Power Wide-Area Network*, LPWAN). LTE-M omogućuje spajanje uređaja putem jeftinih i jednostavnih radijskih modula na postojeću mrežu LTE, što tu tehnologiju uz upotrebu inovacija poput LTE eDRX (*Extended Discontinuous Reception*) i LTE PSM (*Power Saving Mode*) čini vrlo potentnim rješenjem za uspostavu IoT mreža [2].

### 1.2. Obilježja LTE-M

LTE-M podržava relativno brzi prijenos podataka, pokretljivost, prelaženje (engl. *roaming*) i potencijalno glasovne usluge. Mreže LTE-M će, podržane od strane proizvođača opreme i proizvođača čipova i komunikacijskih modula, postojati uz postojeće 2G, 3G i 4G pokretne mreže. Na taj će način imati korist od svih postojećih tehnika za zaštitu sigurnosti i privatnosti javnih pokretnih mreža, kao što su podrška za povjerljivost korisnika (engl. *user identity confidentiality*), autentifikaciju entiteta (engl. *entity authentication*), integritet podataka (engl. *data integrity*) i identifikaciju pokretne opreme (engl. *mobile equipment identification*) [3].

Osnovna obilježja mreža LTE-M za koja se smatra da će privući veliki broj korisnika [1]:

- Niski troškovi: Uređaji će se moći spajati na mrežu 4G pomoću cjenovno pristupačnih komunikacijskih modula koji koriste pola frekvencijskog dupleksa (engl. *half-duplex*) i zauzimaju uži frekvencijski pojas od postojećih 4G uređaja, a to uz smanjenje cijene za 20-25% u odnosu na postojeće EGPRS modeme [3].
- Dugo trajanje baterije: Tehnologija LTE-M omogućiti će trajanje baterija uređajima od barem 10 godina za čitav niz slučajeva uporabe (engl. *use cases*). To se planira postići slanjem uređaja u stanje „dubokog sna“ u okviru štednog načina rada (engl. *Power Savings Mode*, PSM) ili periodičnim buđenjima dok je uređaj spojen na mrežu u okviru načina rada produženog diskontinuiranog prijema (engl. *extended discontinuous reception*, eDRX). Više detalja o ove dvije tehnologije štednje energije dostupno je na kraju ovog poglavlja.

- Niža cijena usluga: Maksimalna brzina prijenosa koja se očekuje od LTE-M uređaja je red veličine 100 kbit/s, zbog čega će ti uređaji biti puno manji teret za 4G mrežu. Mrežni operatori će moći ponuditi cijene puno bliže starijim 2G uslugama nego trenutnim 4G uslugama.

LTE-M je tehnologija dizajnirana za rad na postojećim 4G mrežama. Njene glavne karakteristike prikazane su u Tablici 1 [1]. Ona koristi širinu frekvencijskog pojasa sustava od 1.08 MHz za dolazni i odlazni smjer. U dolaznom smjeru, prijenos podataka temelji se na ortogonalnom frekvencijskom višestrukome pristupu (engl. *Orthogonal frequency-division multiple access*, OFDMA) uz 15 kHz tonske pojaseve, modulaciji 16 QAM (*Quadrature Amplitude Modulation*) te turbo kodiranju za zaštitu podataka u prijenosu. U odlaznom smjeru, prijenos podataka temelji se na frekvencijskom višestrukome pristupu zasnovanom na jednom nositelju (engl. *Single-Carrier Frequency-Division Multiple Access*, SC-FDMA). Maksimalna izlazna snaga pokretnog uređaja ograničena je na 23 dBm, što je višestruko poboljšanje od maksimalne izlazne snage pokretnih uređaja u 2G mreži. Dopuštena je uporaba FDD-a s potpunim i polovičnim dupleksiranjem. Uz potpuno dupleksiranje, maksimalna prijenosna brzina u dolaznom i odlaznom smjeru je 1 Mbit/s, dok je uz polovično dupleksiranje maksimalna brzina u dolaznom smjeru 375 kbit/s, a u odlaznom smjeru 300 kbit/s.

LTE-M potiče poboljšani vijek trajanja baterije. Koristi štedni način rada (PSM), tehniku predloženu u izdanju 3GPP Release 12 [4]. Uređaj s PSM štednim načinom rada zahtijeva mrežu na određeno vrijeme, tijekom kojeg je uređaj dostupan pozivanjem (engl. *paging*), a zatim se prebacuje u način rada za uštedu energije tijekom kojeg je nedostupan. Dodatna poboljšanja u vijeku trajanja baterije postižu se korištenjem produženog diskontinuiranog prijema (eDRX), predstavljenog u izdanju 3GPP Release 13 [5]. eDRX se može koristiti kada dolazni promet ne podržava odgodu u prijemu ili u ekstremnim scenarijima pokrivenosti, kada se fizički kanali ponavljaju mnogo puta.

**Tablica 1.** LTE Cat M1 [1]

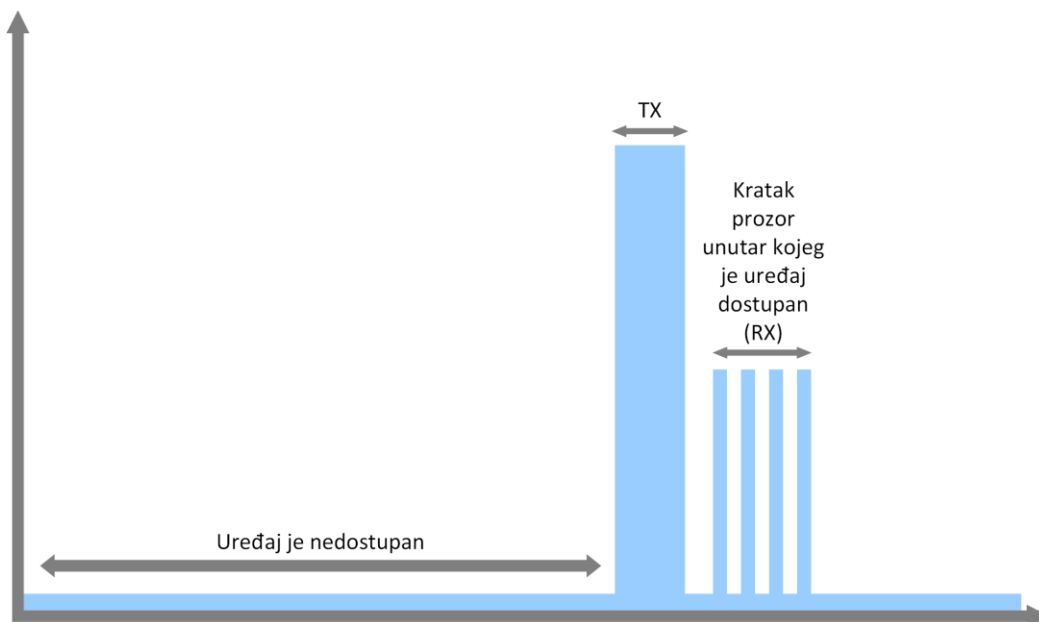
<b>Deployment</b>	In-band LTE
<b>Coverage</b>	155.7 dB
<b>Downlink</b>	OFDMA, 15 kHz tone spacing, Turbo code, 16 QAM, 1 Rx
<b>Uplink</b>	SC-FDMA, 15 kHz tone spacing, Turbo code, 16 QAM
<b>Bandwidth</b>	1.08 MHz
<b>Peak data (DL/UL)</b>	For FD: 1 Mbps DL and UL For HD: 300 kbps for DL, 375 kbps for UL
<b>Duplexing</b>	FD & HD (type B), FDD & TDD
<b>Power saving</b>	PSM, ext I-DRX, C-DRX
<b>Power class</b>	23 dBm, 20 dBm

### 1.2.1. LTE PSM

U štednom načinu rada (*Power Saving Mode*, PSM) [2], prikazanom na Slici 1.1., uređaj najavi mreži da na neodređeno vrijeme odlazi u stanje spavanja te postaje nedostupan. U onom trenutku kada uređaj odluči, na temelju ranije definirane logike ili postavljenog brojača, da je vrijeme za slanje podataka (TX), budi se i šalje podatke te ostaje dostupan u prijemnom načinu rada (RX) u 4 okvira mirovanja, nakon čega ponovno odlazi u stanje spavanja.

Budući da je LTE-M uređaj nedostupan u stanju spavanja za vrijeme trajanja LTE PSM okvira, njegova potrošnja baterije je iznimno niska. Dapače, čak je niža od konkurentnih LPWAN tehnologija poput Sigfox-a ili LoRaWAN-a, jer LTE-M ostvaruje nešto više brzine prijenosa podataka. Razlog tome je korištenje licenciranog frekvencijskog spektra u kojem nema toliko interferencija koliko ima u nelicenciranom spektru koji koriste ostale spomenute tehnologije.

LTE-M uređaj koji šalje podatke jednom dnevno koristeći opisani štedni način rada, trebao bi moći raditi bez prestanka punih 10 godina na napajanje od dvije AA baterije.



Slika 1.1. LTE PSM [2]

### 1.2.2. LTE eDRX

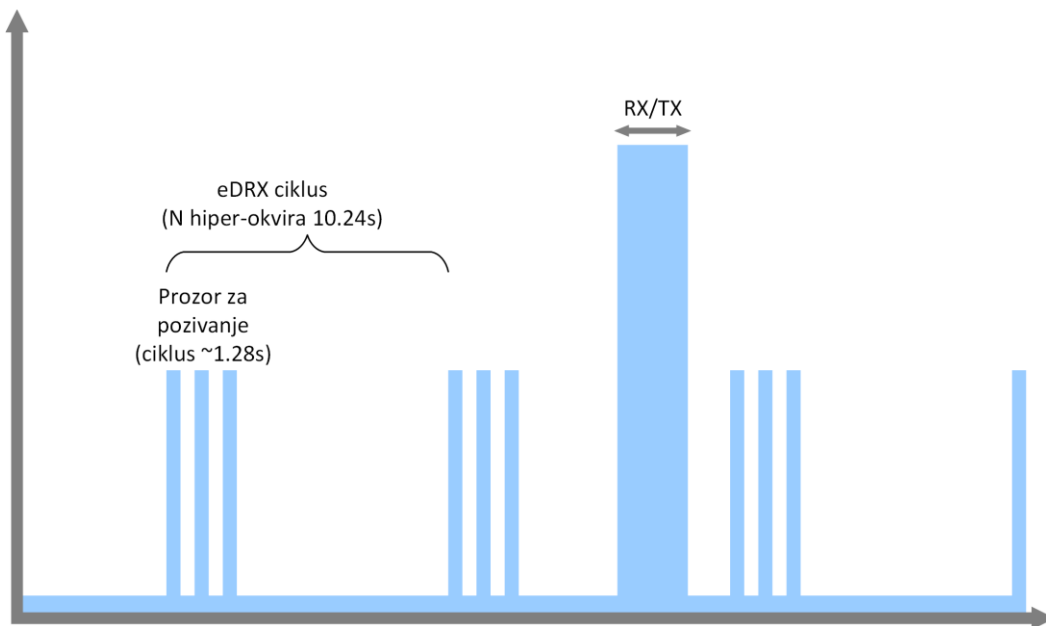
Uobičajeni okvir pozivanja u okviru mreže LTE iznosi 1.28s, tijekom kojega mreža može pozvati uređaj. Druga vrsta štednje baterije korištenje je diskontinuiranog prijema (*Discontinuous Reception*, DRX) i proširenog diskontinuiranog prijema (*Extended Discontinuous Reception*, eDRX) [2].

LTE DRX omogućuje uređaju ulazak u fazu spavanja u trajanju od 10.24s između ciklusa pozivanja, što pomaže u smanjenju potrošnje baterije, ali još uvijek nije dovoljno za

omogućavanje višegodišnjeg rada baterije. LTE-M dodatno produljuje uobičajenu fazu mirovanja s 1.28s na 5.12s.

Glavna inovacija u kontekstu štednje baterije je postupak LTE eDRX, prikazan na Slici 1.2., koji omogućuje da LTE-M uređaj kaže mreži koliko hiper-okvira u trajanju od po 10.24s želi „spavati“ prije povratka u dostupno stanje. Maksimalan broj hiper-okvira određuje mrežni operator javne pokretne mreže, a minimalno bi trebao iznositi barem 40 minuta.

LTE-M uređaji koji šalju podatke jednom dnevno i „bude se“ odnosno vraćaju u dostupno stanje svakih 60 hiper-okvira kako bi provjerili je li ih netko treba, što je otprilike svakih 10 minuta, mogu raditi 4.7 godina bez prestanka na napajanje od dvije AA baterije.



Slika 1.2. LTE eDRX [2]

### 1.3. Prednost i mane LTE-M

Tehnologija LTE-M jedan je od odgovora standardizacijske organizacije 3GPP na rastuću potražnju za komunikacijskim tehnologijama koje omogućuju implementaciju IoT sustava. Druga tehnologija je NB-IoT (*Narrowband IoT*) koja se u potpunosti zasniva na jednostavnijoj pristupnoj shemi, na frekvencijskom višestrukome pristupu zasnovanom na jednom nositelju (SC-FDMA). Međutim, možda i nepremostivi nedostatak kod NB-IoT-a je postojanje dvije konkurentne tehnologije koje najvjerojatnije neće biti međusobno kompatibilne [6]. Osnovna razlika između NB-IoT i LTE-M je što LTE-M ostvaruje višu brzinu prijenosa podataka i omogućuje brži izlazak na tržište (engl. *time-to-market*), dok NB-IoT pruža veću fleksibilnost u dostupnom frekvencijskom spektru i načinima rada. Od ostalih brzo rastućih tehnologija u području LPWAN mreža svakako valja izdvojiti SigFox i LoRaWAN. Sigfox [7] je zatvorena implementacija ultra uskopojasne (engl. *Ultra Narrow Band*) radijske komunikacije u otvorenom ISM (*Industrial, Scientific, Medical*) frekvencijskom pojasu (u Europi je riječ o 868 MHz). LoRaWAN [8] je protokolni sloj

razvijen nad fizičkim slojem LoRa zasnovanom na modulaciji CSS (*Chirp Spread Spectrum*) koji također koristi ISM sloj za radijsku komunikaciju.

Osnovni ciljevi tehnologije LTE-M definirani su u izdanju 3GPP Release 13 [5]:

- trajanje baterije energije od 5Wh barem 10 godina,
- cijena uređaja usporediva s IoT uređajima koji koriste mrežu GPRS (*General Packet Radio Service*),
- proširena pokrivenost ( $> 156$  dB MCL),
- varijabilne brzine prijenosa podataka kako bi se poboljšala pokrivenost.

Iako je specifikacija LTE-M kao komunikacijske tehnologije dostupna, niz detalja oko implementacije još uvijek nije razriješeno. Primjerice, detalji oko izvedbe štednih načina rada PSM i eDRX još uvijek nisu jasno koordinirani između mrežnih operatora, proizvođača opreme i infrastrukturnih operatora.

Ograničenja koja treba uzeti u obzir prilikom razmatranja LTE-M kao tehnologije prikladne za uspostavu IoT mreže [1]:

- Uređaji spojeni na mrežu LTE-M za napajanje koriste baterije, pa s obzirom na to ograničenje za prijenos podataka koriste jednostavne UDP/TCP naredbe. Malen i energetski efikasan uređaj spojen na mrežu LTE-M zbog ograničene procesorske moći nije u mogućnosti uspostavljati konekcije zasnovane na protokolu PPP (*Point-to-Point Protocol*).
- Punokrvni operacijski sustav iz obitelji Linux može vrlo dobro rukovati sa složenim sigurnosnim zahtjevima usluga poput primjerice MQTT (*Message Queuing Telemetry Transport*) pokrenutima na platformi kao što je AWS IOT [9]. Međutim, malen i energetski efikasan uređaj spojen na mrežu LTE-M vrlo vjerojatno neće biti u mogućnosti na isti način izaći na kraj s takvim izazovima. Stoga je potrebno posvetiti dodatnu pozornost pitanjima sigurnosti i privatnosti na takvim uređajima.
- Ostvariti maksimalnu izlaznu snagu od 23 dBm zahtijeva struju od barem 500 mA prema LTE-M modulu. Uzevši u obzir da je napajanje baterijsko, a istodobno se očekuje višegodišnji neometani rad uređaja bez potrebe za njenom promjenom, planiranje ispravnog omjera između vrste baterije i njenog kapaciteta postaje jedan od glavnih zadataka prilikom uspostave mreže LTE-M.

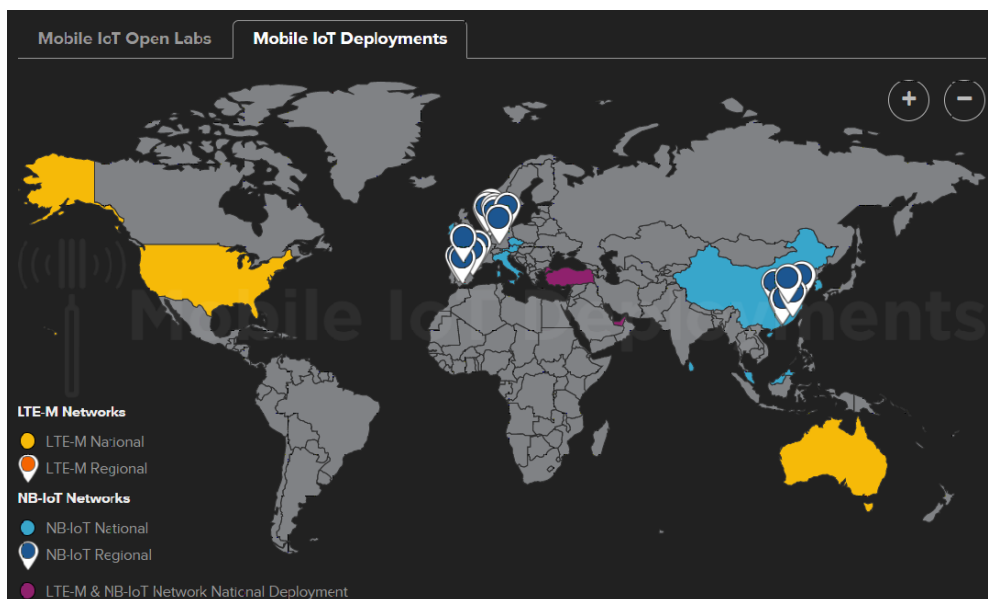
#### 1.4. Slučajevi uporabe LTE-M

LTE-M kao jedna od LPWAN komunikacijskih tehnologija ima vrlo dobre predispozicije za korištenje u sljedećim slučajevima uporabe [1]:

- Široko rasprostranjeni senzori (engl. *Low Density Sensors*): U slučajevima kada tvrtka mora uspostaviti mrežu senzora na velikom geografskom području, „klasične“ tehnologije poput WiFi-a ili neke od tehnologija koje koriste mrežne pristupnike nisu nužno najbolji izbor. LTE-M zbog vrlo dobre pokrivenosti koju pruža, dugotrajnosti baterije uređaja koju garantira, ali i jednostavnosti jer ne zahtijeva spajanje i konfiguriranje pristupnika, značajno pojednostavljuje uspostavu mreže senzora.
- Automatska očitavanja na daljinu (engl. *Automated Meter Reading, AMR*): Prijašnje javne pokretne mreže korištene u svrhu automatskog očitavanja mjernih postaja na daljinu nisu bila popularna, ponajprije zbog dosta visoke cijene. Kako LTE-M u odnosu na njih konkurira nižim troškovima, što zbog niže cijene komunikacijskih modula, što zbog manjih troškova za pokretnu mrežu, pretpostavka je da bi AMR mogao čest slučaj uporabe u mrežama LTE-M.
- Praćenje paketa (engl. *Asset Tracking*): U ovom slučaju, LTE-M bi se mogao upariti s nekom od komunikacijskih tehnologija malog dometa (npr. Bluetooth) i u tom smislu u pozadini pružati podršku za komunikaciju na velike udaljenosti.

### 1.5. Raširenost LTE-M

U tijeku je utrka u izgradnji mreža zasnovanih na različitim LPWAN komunikacijskim tehnologijama. Bez obzira što se LTE-M zasniva na postojećim mrežama LTE, svejedno je potrebno izvršiti nadogradnju prije nego li postanu sposobne spajati LTE-M uređaje i pružati im usluge. Udruženje GSMA (*GSM Association*) na svojim web-stranicama vodi evidenciju uspostavljenih mreži LTE-M na nacionalnoj i regionalnoj razini. Osim prikaza aktualnih LTE-M projekata, na istoj karti prate se i projekti iz područja NB-IoT tehnologija.



Slika 1.3. LTE-M diljem svijeta [10]



Ono što je evidentno na prvi pogled na Sliku 1.3., u ovom trenutku su na nacionalnoj razini uspostavljene mreže LTE-M u Sjedinjenim Američkim Državama i Australiji, dok je u Turskoj i Ujedinjenim Arapskim Emiratima uz LTE-M uspostavljena i nacionalna pokrivenost mrežom NB-IoT [10]. Svi vodeći mrežni operatori javnih pokretnih mreža, poput AT&T-a, KPN-a, Orangea, Telefónica, Telstre i Verizona trenutno sudjeluju u različitim zemljama u implementaciji LTE-M mreža različite geografske pokrivenosti [3].

U ovom trenutku u Hrvatskoj ne postoji javno poznati projekt uspostave IoT mreže zasnovane na tehnologiji LTE-M, ali postoji projekt razvoja mreže NB-IoT pod vodstvom Deutsche Telekomu [11].

## 1.6. Literatura

[1] Brian Ray, What is LTE-M, Link Labs, <https://www.link-labs.com/blog/what-is-lte-m>, 11.12.2017.

[2] Brian Ray, LTE eDRX and PSM Explained for LTE-M1, Link Labs, <https://www.link-labs.com/blog/lte-e-drx-psm-explained-for-lte-m1>, 11.12.2017.

[3] Long Term Evolution for Machines: LTE-M, <https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/>, 12.12.2017.

[4] 3GPP Release 12, <http://www.3gpp.org/specifications/releases/68-release-12>, 12.12.2017.

[5] 3GPP Release 13, <http://www.3gpp.org/release-13>, 12.12.2017.

[6] Iain Morris, Ericsson, Huawei Incompatibility Threatens NB-IoT – Sources, [http://www.lightreading.com/iot/nb-iot/ericsson-huawei-incompatibility-threatens-nb-iot---sources/d/d-id/732345?page\\_number=3](http://www.lightreading.com/iot/nb-iot/ericsson-huawei-incompatibility-threatens-nb-iot---sources/d/d-id/732345?page_number=3), 13.12.2017.

[7] Sigfox, <https://www.sigfox.com/en/sigfox-iot-technology-overview>, 13.12.2017.

[8] LoRa Alliance™ Technology, <https://www.lora-alliance.org/What-Is-LoRa/Technology>, 13.12.2017.

[9] AWS IOT, <https://aws.amazon.com/iot/>, 13.12.2017.

[10] GSMA LTE Deployment map, <https://www.gsma.com/iot/deployment-map/#deployments>, 14.12.2017.

[11] Deutsche Telekom to launch NB-IoT in eight markets in 2017 , <https://www.mobileeurope.co.uk/press-wire/deutsche-telekom-to-launch-nb-iot-in-eight-markets-in-2017>, 14.12.2017.

## **2. Poboljšanje kvalitete života osoba s invaliditetom kroz harmonizaciju društvene osviještenosti i usluga telekom operatora**

### **Izveštaj sa skupa i okruglog stola „Osobe s invaliditetom u digitalnom društvu“**

Dana 29. studenog 2017. u sklopu/okviru projekta „Pogled u budućnost“ na kojem surađuju Fakultet elektrotehnike i računarstva i Hrvatska regulatorna agencija za mrežne djelatnosti održan je Okrugli stol pod nazivom „Osobe s invaliditetom u digitalnom društvu“.

U okviru istog projekta provedeno je istraživanje o percepciji korisnika o mogućnostima pristupa javnim komunikacijskim uslugama koje je ukazalo na potrebu dodatnih inicijativa, a jedna od njih je i organizacija navedenog događaja.

Iako je skup trebao biti održan u Saboru, zbog bolje prilagođenosti prostora, održan je na Fakultetu elektrotehnike i računarstva.

Prije samog skupa održani su pripremni sastanci organizatora s predstavnicima operatora (12. lipnja 2017.) i s predstavnicima osoba s invaliditetom (16. studenog 2017.) te pripremni sastanak članova organizacijskog tima HAKOM-a i FER-a (12. listopada 2017.).

Pozdravni govor održan je od strane domaćina, prodekana za nastavu prof. dr. sc. Marka Delimara, ravnatelja HAKOM-a, mr. sc. Maria Webera te predstavnika Ureda pravobraniteljice za osobe s invaliditetom, Darija Jurišića, mag. iur. univ. spec. admin. publ., zamjenika Pravobraniteljice.

Aktivnosti vezane za Zaštitu i promicanje prava osoba s invaliditetom kao korisnika elektroničkih komunikacijskih usluga predstavila je Tanja Zaninović, dipl. iur. iz HAKOM-a.

Nakon toga, članica Laboratorija za asistivne tehnologije i potpomognutu komunikaciju FER-a, Ivana Rašan, dipl. oec., predstavila je rezultate provedenog istraživanja *Percepcija korisnika o mogućnostima pristupa javnim komunikacijskim uslugama* koji su i svojevrsna podloga za organizaciju ovog skupa.

EU Direktiva o pristupačnosti internetskih stranica i mobilnih aplikacija tijela javnog sektora, predstavljena je od strane Marije Livajušić, dipl. ing. računarstva, koja je članica Up2date, Centar za istraživanje, edukaciju i primjenu novih znanja.

Zatim je gospođa Vanda Šagovac, dipl. turist. menadžer, predsjednica udruge „Svijet tišine“, iznijela primjere pozitivne prakse u inozemstvu vezano za komunikacijske usluge.

Članica CeDePe-a, Društva osoba s cerebralnom i dječjom paralizom Zagreb, gospođa Iva Ražanković, koja je sudjelovala u terenskom istraživanju vezano za pristupačnost poslovnica

operatora, prezentirala je trenutnu situaciju u poslovnicaama te ju usporedila s idealnom situacijom. Također je ukazala na elemente koji su lako prilagodljivi (npr. nagnuti cjenici, a ne oni koji su postavljeni ravno, snižen pult, edukacija djelatnika za razgovor s osobom koja sjedi u kolicima – npr. ne stajati iza pulta, već izaći i doći do osobe koja je u kolicima, itd.) i koji bi znatno utjecali na poboljšanje razine kvalitete usluga koje pružaju operatori.

Nakon prezentacija uslijedila je konstruktivna rasprava, okrugli stol između predstavnika operatora Marijana Grubešić, Tele2, Lidija Varga Trgovec, Vipnet, Vice Jakovljević, HT te predstavnika osoba s invaliditetom, Marija Livajušić, Up2date, Centar za istraživanje, edukaciju i primjenu novih znanja, Josip Koštan, CeDePe – Društvo osoba s cerebralnom i dječjom paralizom Zagreb, Vanda Šagovac, predsjednica udruge „Svijet tišine“ i Mirjana Dobranović, Udruga za promicanje istih mogućnosti (UPIM). Skup i okrugli stol je moderirala izv. prof. dr. sc. Željka Car.

Pitanja za poticanje diskusije upućena predstavnicima osoba s invaliditetom:

- S kojim se problemima susrećete pri analizi ponude i u komunikaciji s telekom operatorom? Osim problema, jeste li imali i kakvih pozitivnih iskustava (zadovoljavajuće usluge, uređaji, djelatnici službe za korisnike)?
- Jeste li upoznati s iskustvima i praksom koje imaju osobe s invaliditetom u ostalim zemljama EU?
- Kako treba izgledati pristupačno prodajno mjesto telekom operatora te koja znanja trebaju posjedovati prodajni djelatnici kako bi nesmetano komunicirali s osobama s invaliditetom?
- Imate li kakav prijedlog kako poboljšati dostupnost informacija o uslugama i proizvodima te komunikaciju s korisničkom službom operatora?
- Smatrate li da inicijative i suradnje poput ove (u okviru ovog projekta/skupa/istraživanja) mogu doista poboljšati položaj osoba s invaliditetom u digitalnom društvu?

Pitanja za poticanje diskusije upućena predstavnicima operatora:

- Prezentirajte trenutnu ponudu usluga i uređaja za osobe s invaliditetom?
- Kako poboljšati diseminaciju informacija o ponudi za osobe s invaliditetom?
- Smatrate li da bi se razina zadovoljstva osoba s invaliditetom povećala nakon provedene marketinške kampanje vezano za dostupne usluge i proizvode?
- Kako općenito poboljšati položaj osoba s invaliditetom u digitalnom društvu?
- Smatrate li da inicijative i suradnje poput ove u okviru ovog projekta/skupa/istraživanja mogu doista poboljšati položaj osoba s invaliditetom u digitalnom društvu?

Tijekom okruglog stola, operatori su iznijeli svoje trenutne mogućnosti i aktivnosti vezano za poboljšanje kvalitete usluga te ponude proizvoda za osobe s invaliditetom. Predstavnici osoba s invaliditetom, ali i ostali sudionici skupa iznijeli su probleme s kojima se susreću prilikom sklapanja ugovora (s naglaskom na sklapanje ugovora preko udruga), zatim vezano za ponudu uređaja koji su trenutno dostupni i onih koji bi im trebali biti dostupni te arhitekturu poslovnica. Naglašeno je kako je Internet nekim osobama s invaliditetom nužni preduvjet za ostvarivanje komunikacije s vanjskim svijetom te bi trebao biti cjenovno dostupan svim osobama koje su u toj skupini.

Sudionici okruglog stola su iskazali zadovoljstvo vezano za održani skup i susret jer je isti otvorio mogućnosti za buduću konstruktivnu suradnju. Naglasak je na tome da su operatori mogli iz prve ruke dobiti informacije koje su im potrebne kako bi mogli kroz svoje aktivnosti poboljšati trenutno stanje, a predstavnici osoba s invaliditetom su također dobili direktno povratne informacije od operatora i njihova objašnjenja vezano za pojedine probleme.

Zaključeno je kako je za poboljšanje stanja i razine kvalitete usluga i proizvoda nužna harmonizirana suradnja svih prisutnih dionika koja će osigurati transparentan prijenos informacija između operatora i osoba s invaliditetom, a upravo su informacije ključne u kontekstu prediktora za pozitivno djelovanje u okviru ove suradnje. Uz to, naglašena je i važnost marketinškog djelovanja za ciljanu populaciju.

Bitno je još napomenuti kako je naglašena važnost univerzalnog dizajna koji omogućuje korištenje određenog proizvoda ili bivanje u određenom okruženju svim ljudima bez potrebe za dodatnim prilagodbama (npr. sudionik skupa naglasio je kako je ulazna vrata poslovnice jednog operatora vrlo teško otvoriti i osobi koja nema nikakve teškoće, a za osobu koja je u kolicima nemoguće – u ovom slučaju bi vrata koja se otvaraju uz pomoć senzora mogla biti promatrana kao univerzalni dizajn).

Nakon što je završio formalni dio skupa, sudionici su se još bolje upoznali tijekom neformalnog dijela te su razmijenili iskustva i razmotrili ideje za buduću suradnju.

Dogovoreno je da će projektni tim održati interni sastanak početkom prosinca te će na istom utvrditi koji su daljnji koraci vezao za sve navedeno.

Zaključci skupa:

1. Ispraviti naziv „poremećaj“ u „teškoća“ u okviru Kviza na sjedištu weba HAKOM-a (ovo je već provedeno u djelo i naziv „poremećaj“ je uklonjen sa web i mobilne verzija Kviza);
2. Na prodajnim mjestima operatora povećati pristupačnost informacija o cijeni i performansama izloženih uređaja;

3. Na prodajnim mjestima operatora s otežanim prilazom implementirati zvono za pomoć kod ulaska u prostor osoba s invaliditetom ili drugih osobama (npr. roditelji s kolicima, osobe starije dobi, djeca i sl.);
4. Definirati model komunikacije operatora s tumačem znakovnog jezika koji bi se mogao primijeniti kod pojedinih operatora;
5. Predstavnici osoba s invaliditetom/udruge/centri formulirati svoje potrebe s obzirom na elektroničke komunikacije koristeći jedinstvenu web-stranicu/portal koja će biti u tu svrhu implementirani (i o kojoj će biti pravovremeno obaviješteni);
6. Operatori trebaju odrediti odgovorne osobe za komunikaciju i upite vezano uz osobe sa složenim komunikacijskim potrebama;
7. HAKOM će prilagoditi sadržaj i dizajn svojeg sjedišta weba kako bi bili pristupačniji i odražavali aktivnosti koje se provode u ovom području.

Navedene aktivnosti po prethodnim točkama treba implementirati u prvoj polovini 2018. godine, pri čemu bi se drugi sastanak predstavnika OSI, operatora i regulatora te svih ostalih zainteresiranih za ovu temu održao sredinom 2018. godine.

### 3. Širokopojasni pristup Internetu u ruralnim područjima

#### 3.1. Širokopojasni ekosustav ruralnih područja

Ruralna područja već se duže vrijeme suočavaju se s problemom „dvostrukog digitalnog jaza“. Dok na strani ponude ruralna područja zaostaju za urbanima u pogledu pružanja osnovne potrebne infrastrukture, na strani potražnje nedostaju adekvatne digitalne usluge. Stoga smanjenje ovakvih postojećih negativnih trendova, odnosno digitalnog jaza, mora postati osnovni razvojni prioritet.

Trenutno su programi ruralnog razvoja koji imaju za cilj poboljšanje životnih uvjeta u ruralnim područjima definirani na različitim hijerarhijskim razinama.

Na globalnoj razini, ITU Agenda [1], inicijativa čiji je cilj usmjeravanje budućeg razvoja informacijsko-komunikacijskog sektora, ističe važnost unaprjeđenja i prilagodbe postojećeg okruženja na telekomunikacijskim tržištima ubrzanim trendovima razvoja novih tehničkih rješenja.

Nadalje, i na europskoj razini brojne inicijative i programi razmatraju načine na koje se u ruralnim područjima digitalne usluge u sektorima kao što su zdravstvo, socijalni sustav, obrazovanje, energetika, promet, trgovina i drugo mogu poboljšati kroz implementaciju ICT alata i / ili kroz podupiranje aktivnosti koje se provode za pojedine ili od strane pojedinih ruralnih zajednica.

Na nacionalnoj razini postojeće strategije su usmjerene na:

- širi kontekst ruralnog razvoja i poboljšanje kvalitete života u ruralnim područjima i to s posebnim nalaskom na obrazovanju, mobilnosti, zapošljavanju, zdravstvu, njezi i energiji, te
- razvoj ICT-a i potrebnih kapaciteta, posebno širokopojasne infrastrukture i digitalnih usluga [2].

Dakle, kako bi se u što većoj mjeri umanjio postojeći digitalni jaz između pojedinih ruralnih i urbanih područja te omogućio daljnji razvoj ruralnih područja, nužna je daljnja implementacija širokopojasnih rješenja u tim područjima.

Procesi razvoja i implementacije širokopojasnih rješenja usmjereni su na ujednačavanje postojećih razlika u razinama i mogućnostima pristupa i primjene naprednih digitalnih informacijsko-komunikacijskih tehnologija i usluga. S obzirom na postojeće razlike u razinama i mogućnostima korištenja digitalnih tehnologija i usluga na razini države, digitalni jaz je moguće razmatrati na različitim razinama – regionalnoj, županijskoj ili lokalnoj. Stoga je uz razmatranje cjeline, potrebno razmotriti svaki segment u određenom području zasebno.

Načelo tehnološke neutralnosti nalaže omogućavanje podjednakog razvoja svih tehnoloških rješenja, bilo žičnih ili bežičnih. Stoga je potrebno precizno procijeniti zahtjeve i pronaći adekvatna pristupna rješenja za svaki pojedini tip područja [3]. Izbor adekvatnih rješenja potrebno je načiniti s obzirom na:

- veličinu tržišta, odnosno broj potencijalnih korisnika usluga - uvjetuje isplativost rješenja;
- postojeće infrastrukturne preduvjete za razvoj (npr. za ruralna naselja u blizini pristupa fiksnoj jezgrenoj mreži - primjena žičnih pristupnih rješenja; za udaljena i teže dostupna područja poput brdsko-planinskih područja - primjena bežičnih pristupnih rješenja) [4].
- vrstu korisnika - rezidencijalni korisnici (uglavnom manji zahtjevi - osnovne pristupne brzine) ili poslovni korisnici (veći zahtjevi - brzi i ultrabrzi pristup uz dodatne poticaje);
- vrste digitalnih usluga.

### **3.2. Pregled obilježja novih telekomunikacijskih širokopojasnih rješenja**

#### **a) Širokopojasne tehnologije**

Postojeće stanje na telekomunikacijskom tržištu može se promatrati i uspoređivati s obzirom na udio fiksnih i mobilnih priključaka u ukupnom broju širokopojasnih priključaka [5]. Dok fiksne širokopojasne pristupne tehnologije korisnicima osiguravaju pakete s velikim pristupnim brzinama, mobilne tehnologije omogućuju fleksibilnost te mogućnost pristupa Internetu neovisno o mjestu i vremenu pristupa. U dinamici budućeg razvoja i implementacije širokopojasnih rješenja izvjesno je da će veći naglasak u idućem periodu biti na supstituciji pojedinih vrsta širokopojasnih rješenja drugima.

Kako bi se koristile mogućnosti koje proizlaze iz primjene pojedinih širokopojasnih usluga, u svim je područjima bitno osigurati dostupnu širokopojasnu infrastrukturu. Proširenje dostupnosti širokopojasnih rješenja na nova ruralna područja, odnosno naselja i izgradnja pristupne infrastrukture može predstavljati problem. Stoga je nužno analizirati postojeće infrastrukturne preduvjete za izgradnju.

U ruralnim naseljima koja su dovoljno blizu fiksne jezgrene mrežne infrastrukture, predlaže se implementacija žičnih pristupnih rješenja koja osiguravaju velike pristupne brzine (brzi i ultrabrzi priključci), kakva su i pristupna rješenja zasnovana na optici (FTTx). Pri tome je moguća primjena predviđenih potpora za financiranje izgradnje pristupnih mreža. Ovakva rješenja su opravdana jer omogućuju daljnji gospodarski razvoj i revitalizaciju ovih područja.

Za razliku od područja u blizini pristupa fiksnoj jezgrenoj mrežnoj infrastrukturi, u područjima jako udaljenima od fiksne jezgrene mreže, kao što je većina vrlo malih ruralnih naselja s pretežno rezidencijalnim korisnicima, predlažu se tehnološka rješenja koja

zahtijevaju manje investicijske troškove, uglavnom temeljena na bežičnom pristupu. Kada se bazne stanice postavljaju na lokacije na kojima je dostupna jezgrena mrežna infrastruktura, tada se u spojnoj mreži mogu koristiti iznajmljene linije, vlakna ili mikrovalne veze. Također, i satelitska veza može osigurati pokrivenost u ovim područjima.

Kako bi ostali konkurentni na telekomunikacijskim tržištima operatori se moraju pripremati za prihvaćanje i razvoj novih tehnoloških rješenja. Nova širokopolasna pristupna rješenja danas se razvijaju u smjeru konvergencije različitih tehnologija. Primjenom heterogenih mreža nastoje se iskoristiti prednosti više postojećih tehnoloških rješenja koja se koriste u pristupnim mrežama. Jedan od takvih primjera je i primjena Fi-Wi (*Fiber-Wireless*) mreža, koje u radu koriste prednosti dviju tehnologija - veliki propusni opseg optičkih vlakana te mobilnost svojstvenu bežičnim mrežama. Također, jedan od novijih koncepata koji se u sve značajnijoj mjeri implementira je i Internet objekata (eng. *Internet of Things*, IoT).

### *IoT rješenja*

IoT sustav čini mreža međusobno povezanih i jednoznačno označenih objekata koji mogu razmjenjivati prikupljene podatke unutar mreže bez potrebe za ljudskom intervencijom pri provedbi pojedinih komunikacijskih procesa. Objektima se u ovom kontekstu smatraju živa bića, uređaji ili stvari s ugrađenim senzorom/senzorima koji omogućuju prikupljanje određenih vrsta podataka. Kroz postupke napredne obrade i analize prikupljenih podataka omogućuje se:

- bolji uvid u stanje sustava / komponenti u sustavu
- lakše upravljanje sustavom
- kvalitetnije održavanje sustava.

U IoT sustavima potrebno je razmotriti različite situacije koje mogu nastupiti u mreži, a koje utječu na komunikaciju između objekata, kao i na ukupne performanse IoT sustava. Performanse IoT sustava vezane su uz određene mrežne parametre. Praćenjem performansi IoT sustava kroz analizu mrežnih parametara u različitim mrežnim okruženjima omogućuje se:

- kontrola procesa u sustavu / sustava
- upravljanje procesima / sustavom
- održavanje sustava.

Kako je IoT rješenja moguće primjenjivati u različitim mrežnim okruženjima i imaju vrlo široku primjenu, kontinuirano se uvodi i primjenjuje sve više različitih IoT sustava. Brojne provedene analize ukazuju na sljedeće činjenice vezane uz IoT sustave:

- u implementiranim sustavima broj IoT objekata dosegnut će nekoliko desetaka milijuna do 2020. godine;



- implementirana IoT rješenja generirat će veliku količinu podataka koja bi već 2020. godine mogla iznositi i nekoliko desetaka zeta bajta.

Kako je osnovna svrha umrežavanja razmjena i efikasnije korištenje resursa - informacija, aplikacija i opreme, s porastom ukupnog broja IoT rješenja povećavat će se i izazovi vezani uz:

- upravljanje IoT sustavima, kao i
- upravljanje prikupljenim podacima / dostupnim resursima.

Kao trenutno aktualna istraživačka tematika vezana uz probematiku u području IoT mrežnih sustava može se izdvojiti:

1) Zaštita dostupnih resursa

- zaštita podataka, tj. rizici vezani uz ugrozu integriteta i privatnosti podataka pri njihovoj razmjeni mrežom

2) Efikasno prikupljanje, pouzdana pohrana i napredno korištenje raspoloživih resursa

- efikasno prikupljanje (*crowdsensing*), pouzdana pohrana (*blockchain*) i napredna obrada (*data mining*) velikih količina podataka (*big data*)

3) Pouzdano upravljanje resursima

- optimalno prosljeđivanje velikih količina prikupljenih podataka kroz mrežu s obzirom na zahtjeve za potrebnom energijom

4) Pouzdana razmjena resursa

- interoperabilnost i uspješna provedba komunikacijskih procesa u heterogenim mrežnim sustavima

5) Optimalna namjena resursa

- optimalna raspodjela dostupnih resursa uz ostvarivanje definiranih razina kvalitete usluga (QoS).

Primjeri rješenja navedene problematike u IoT mrežama obuhvaćaju metode za:

- omogućavanje uspješnog slanja dostupnih podataka kroz fizički medij
- omogućavanje efikasne razmjene podataka dijeljenim medijem
- omogućavanje optimalnog prosljeđivanja podataka kroz mrežu uz efikasnu potrošnju raspoložive energije
- omogućavanje pouzdanog prijenosa podataka s kraja na kraj heterogene mreže
- izbor mrežnih rješenja koja omogućuju ostvarivanje definiranih razina kvalitete usluga.

### *Optimalna pristupna rješenja*

Primjena adekvatnih *backhaul* rješenja predstavlja značajan faktor rizika u poslovnim modelima. Stoga je pravilan izbor *backhaul* rješenja ključan za implementaciju optimalnih pristupnih rješenja. Kao optimalna *backhaul* rješenja mogu se izdvojiti rješenja zasnovana na nelicenciranom spektru koji će u narednom periodu postati iznimno bitan i zbog implementacije velike količine budućih mobilnih (4G) M2M (*Machine-to-Machine*) i IoT rješenja.

Rad u nelicenciranom spektru omogućuje implementaciju pristupnih mrežnih rješenja uz niže troškove te primjenu LPWA (*Low-Power Wide-Area*) baziranih IoT rješenja. U pravilu LPWA mreže imaju niže troškove implementacije u odnosu na tradicionalne mobilne mreže koje omogućuju isporuku M2M usluga. U usporedbi sa mobilnim mrežama, LPWA mreže zahtijevaju i manji broj baznih stanica za pokrivanje područja signalom. Također, one omogućuju korištenje već postojeće mrežne infrastrukture uz njenu nadogradnju.

U područjima u kojima nije adekvatno riješena širokopojasna pristupna infrastruktura, što je uglavnom često slučaj u ruralnim područjima, nastoji se dodatno inicirati njen razvoj. U tom smjeru postavljeni su i ciljevi inicijative WiFi4EU. Uredba WiFi4EU propisuje mogućnost subvencioniranja projekata jedinicama lokalne samouprave i pružateljima javnih usluga vezanih uz instaliranje WiFi bežičnih pristupnih točaka i pružanje besplatne povezivosti u centrima javnog života. Pri tome se subvencije odnose samo na slučajeve u kojima nema slobodnih dostupnih javnih ili privatnih pristupnih točaka koje mogu pružati pristup internetu velikih brzina.

Iako navedena uredba WiFi4EU ide u prilog pokrivanju dodatnih zemljopisnih područja širokopojasnim pristupom, pokrivanje dodatnih kućanstava (tj. pristup do pojedinih kućanstava) nije izravno obuhvaćeno ovom mjerom. Također, ostaje i problem pristupa u područjima koja nemaju pristup do jezgre mreže, tj. nisu u blizini jezgre mreže niti jednog operatora. Stoga je potrebno proučiti i druge postojeće koncepte implementacije širokopojasnog pristupa, kao što je i osiguranje dodatnih pristupnih rješenja kroz slobodni UHF pojas te satelitski pristup.

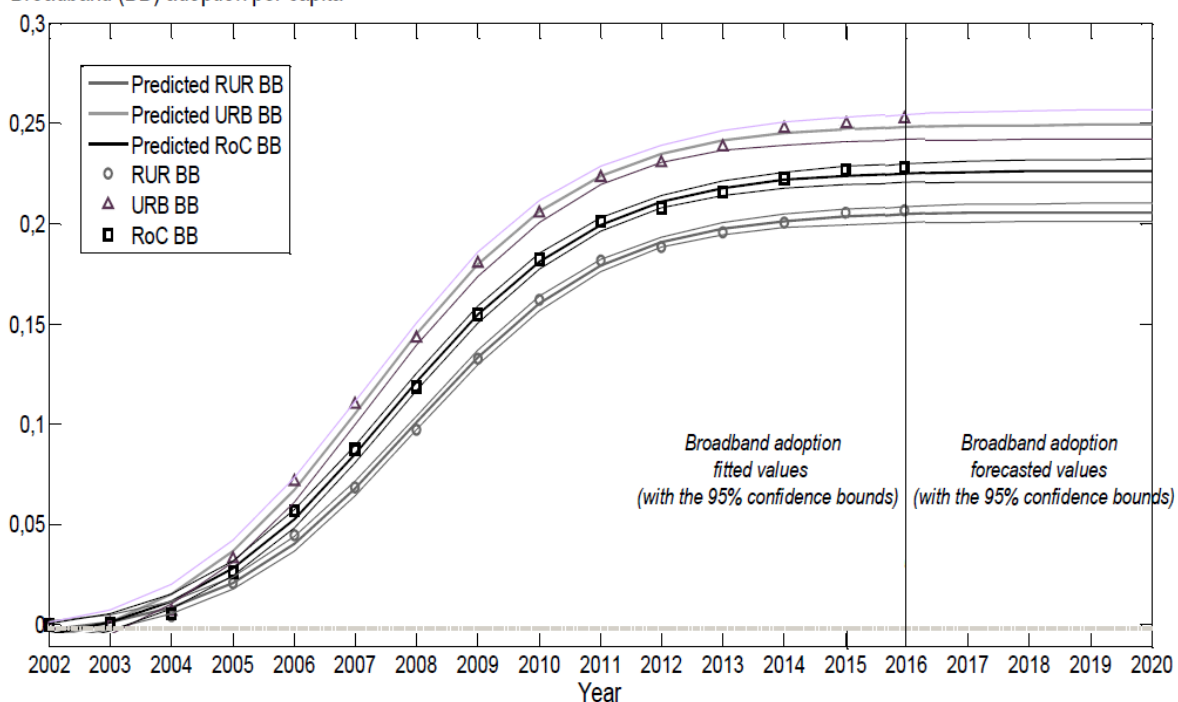
#### b) Širokopojasne usluge

Jedna od ključnih metoda za smanjenje digitalnog jaza je i razvoj i implementacija digitalnih usluga. Ova metoda je bitna za socio-ekonomsku koheziju stanovništva te utječe na kvalitetu života ruralnog stanovništva. S obzirom na njihova različita obilježja, procesi usvajanja svake telekomunikacijske usluge odvijaju se drugačijim intenzitetom, dok u dinamici razvoja i implementacije širokopojasnih rješenja sudjeluje veliki broj čimbenika [6]. Ovi se čimbenici razlikuju u ruralnim i urbanim područjima, pa se pri analizama procesa usvajanja usluga područja klasificiraju kao ruralna ili urbana (tablica 3.1.).

**Tablica 3.1.** Klasifikacija hrvatskih (RoC) županija prema EU kriteriju gustoće naseljenosti (PopDen) prema podacima popisa stanovništva iz 2001. i 2011. godine

The case study area (RoC)				
Number of counties	Average population density in 2001 (PopDen <sub>2001</sub> )	Average population density in 2011 (PopDen <sub>2011</sub> )	Changes in the average population densities (PopDen <sub>2011</sub> -PopDen <sub>2001</sub> )	EU's Criterion of rurality
15	58	54	<i>Negative</i>	RURAL
6	175	171	<i>Negative</i>	URBAN
21 (RoC)	78	76	<i>Negative</i>	RURAL

Broadband (BB) adoption per capita



**Slika 3.1.** Modeliranje i predviđanje broja korisnika (BB) u ruralnoj (RUR) i urbanoj (URB) skupini županija u Republici Hrvatskoj (RoC)

Najčešće korištene kvantitativne metode predviđanja u obzir uzimaju vremenske nizove podataka. Vremenski nizovi primjenjuju se za modeliranje i predviđanje budućih vrijednosti broja korisnika na osnovu povijesnih podataka o stvarnom broju korisnika u prethodnom razdoblju (slika 3.1.).

Proces razumijevanja i predviđanja usvajanja širokopojsnih usluga, kao i njihovog životnog ciklusa vrlo je bitan pri kreiranju poslovnih modela. Zato je bitno dovoljno pozornosti posvetiti metodama koje omogućuju preciznu analizu procesa usvajanja širokopojsnih usluga.

Razvijene usluge treba prilagoditi zahtjevima i potrebama ruralnih stanovnika. Takve usluge trebaju omogućiti korisnicima u ruralnim područjima povećanu produktivnost i povećanje kvalitete života. Primjer usluga koje tome mogu doprinijeti su upravo i IoT i M2M usluge.

Ukoliko se u obzir uzme budući ubrzani razvoj novih usluga temeljenih na novim komunikacijskim konceptima, poput IoT i M2M usluga, izgledan je rastući trend prihvaćanja novih vrsta usluga i od strane operatora i od strane korisnika. Ovakve usluge za svoj rad zahtijevaju odgovarajuću količinu mrežnih resursa. Tako je, na primjer, za implementaciju novih bežičnih telekomunikacijskih rješenja nužno osigurati odgovarajući dio frekvencijskog spektra. Time se osigurava mogućnost daljnjeg usvajanja novih rješenja te definiranja optimalnih poslovnih modela operatora.

### **3.3. Primjena tehnologija i usluga Interneta stvari u poljoprivredi**

U Republici Hrvatskoj poljoprivredno zemljište čini oko 40% ukupne površine, dok je u poljoprivrednim djelatnostima zaposleno više od 10% stanovništva. Ovi podaci pokazuju kako poljoprivreda ima značajnu ulogu u razvoju hrvatskog gospodarstva.

Postojeća problematika vezana uz nedostatak adekvatne opreme te uz nepravovremene informacije, karakteristična za tradicionalni pristup provedbi poljoprivrednih djelatnosti, uzrokuje primjenu nedovoljno efikasnih metoda i postupaka u radu. Stoga implementacija naprednih digitalnih tehnologija i usluga usmjerenih na razvoj poljoprivrede postaje jedan od razvojnih prioriteta.

Primjena digitalnih usluga u poljoprivredi trebala bi omogućiti:

- jednostavnije naručivanje sirovina
- prikupljanje podataka o prinosima
- praćenje cijene proizvoda
- pravovremene informacije o vremenskim prilikama
- lakši pristup stručnim informacijama
- smanjenje poslovnih rizika te povećanje prihoda.

Iako se prikupljanje i analiza podataka o okolišu obavlja kontinuirano već desetljećima, ubrzani su procesi klimatskih promjena potaknuli, a suvremeni trendovi razvoja informacijsko-komunikacijskih tehnologija omogućili kreiranje inovativnih tehničkih rješenja primjenjivih u poljoprivredi.

Tako je omogućen razvoj i primjena IoT sustava zasnovanih na senzorskim mrežama i umreženim uređajima te postupci prikupljanja i obrade podataka za specifične zahtjeve koji se primjenjuju u poljoprivredi. Prikupljanje podataka putem senzora, njihova pohrana uz primjenu računarstva u oblaku i analiza velikih količina podataka omogućuju implementaciju rješenja za efikasno upravljanje i nadzor poljoprivrednih površina.

Implementirani IoT sustav omogućuje prikupljanje podataka vezanih uz tlo i klimatske parametre i to iz različitih izvora. Nad prikupljenim podacima moguće je zatim provesti postupke napredne obrade kako bi se iz velike količine informacija razlučili podaci koji su bitni u praktičnoj primjeni. Navedene podatke moguće je naknadno analizirati i primjenjivati putem praktičnih aplikacija namijenjenih različitim sudionicima uključenima u različite poljoprivredne djelatnosti.

### *Implementacija senzorskih mreža u realna okruženja*

Sustav Interneta stvari koji omogućuje praćenje agrometeoroloških parametara i procjenu fiziološkog stanja usjeva u stvarnom vremenu omogućuje praćenje i planiranje provedenih agrotehničkih mjera u cilju njihove optimizacije. Pri implementaciji takvih sustava potrebno je posebnu pozornost posvetiti tehničkim aspektima koji omogućuju ostvarivanje pouzdane komunikacije između čvorova u senzorskim mrežama namijenjenima prikupljanju okolišnih parametara sa poljoprivrednih usjeva.

Stoga je nužno analizirati ponašanje implementirane bežične senzorske mreže u realnim uvjetima rada kako bi se mogla izvršiti optimizacija parametara bežične komunikacije u takvoj mreži. Optimizacija je moguća i pri određivanju parametara koji opisuju fiziološko stanje biljki na temelju podataka prikupljenih pomoću senzora.

Pri ispitivanju i analizi aspekata komunikacije u realnim uvjetima, a u cilju optimizacije radnih parametara senzorskih mreža, analizirati se mogu različiti scenariji, odnosno:

- mrežne topologije s obzirom na moguće lokacije i razmještaj implementiranih senzora
- načini prosljeđivanja i usmjeravanja prikupljenih senzorskih podataka do krajnjeg odredišta
- načini prikupljanja podataka ovisno o definiranom periodu uzorkovanja te o broju uzoraka koji će se koristiti pri obradi i analizi
- načini obrade i agregacije podataka u stvarnom vremenu
- sigurnosni mehanizmi za postizanje visoke razine sigurnosti u radu.

Kako se postojeće komunikacijske tehnologije uvelike razlikuju prema svojim obilježjima, bitno je odrediti konkretne zahtjeve vezane uz ostvarivanje komunikacije u svakom pojedinom scenariju. Pri izboru pojedinih rješenja uspoređuje se njihova brzina, pouzdanost, sigurnost i energetska učinkovitost. Komunikacijske tehnologije i standardi koji se primjenjuju razlikuju se s obzirom na veličinu razmatranog područja (veličinu područja rasprostiranja signala) i konkretne scenarije primjene (npr. ruralna/urbana područja).

- U LPWA (*Low Power Wide Area Network*) mrežama u kojima je domet rasprostiranja signala veći moguće je primjenjivati više različitih rješenja naznačenih prema prikazu iz tablice 3.2.

Tablica 3.2. usporedba LPWA rješenja

Technical capabilities	Low Power Wide Area Networks (LPWAN)						
	LoRaWAN	Neul	NWave	SigFox	Weightless -N	Weightless -P	Cellular
Range (km/m)	2-5 urban; 15 suburban; 45km rural	up to 10km	up to 10km	up to 10km urban; 50km rural	5km	2km	35km GSM; 200km 3G/4G
Deep Indoor Performance	Yes	ISM yes, Whitespace no	Yes	Yes	Yes	Yes	No
Freq. Band	Varies, Sub-GHz	ISM or Whitespace	Sub-GHz	Frequency independent; 868/902MHz	Sub-GHz	Sub-GHz	900/1800/1900/2100MHz
ISM?	Yes	Yes, depends on base-station	Yes	Yes	Yes	Yes	Depends
Fully Bi-Directional	Yes, depends on mode	Yes	No	No	Uplink only	Yes	Yes
Data Rate	0.3 - 50 kbps adaptive	10 - 100kbps	100bps	10 - 1000bps	30kbps - 100kbps	up to 100kbps adaptive	35-170kbps GSM/ 3 - 10Mbps LTE
Power Profile	Low	Low	Low	Low	Low	Low	Medium
Authentication	Yes	-	Yes	Yes	Yes	Yes	High security, back by major telecoms
E2E Encryption	Yes	-	Yes	Yes	Yes	Yes	Yes
Over the Air Software Upgrades	Yes	-	No	No	No	Yes	Yes
Supports sensors moving between hubs	Yes	-	No	No	Yes	Yes	Yes
Location Aware	Yes	-	No	No	No	-	Yes
Operational Model	Public or private	-	Public or private	Public	Public or private	Public or private	Public or private
Standard	LoRaWAN	Weightless	Weightless	No	Weightless	Weightless	GSM, LTE etc
Scalability	Yes	Yes	Yes	Yes	Limited	Yes	Yes

Izvor: <https://publisher.opensensors.io/connectivity>

Pojedina LPWA rješenja razlikuju se i s obzirom na frekvencijska područja u kojima rade.

Tablica 3.3. Prikaz frekvencijskog spektra kojeg primjenjuju pojedina LPWA rješenja

Name of Standard	Weightless			SigFox	LoRaWAN
	-W	-N	-P		
Frequency Band	TV whitespace (400-800 MHz)	Sub-GHz ISM	Sub-GHz ISM	868 MHz/902 MHz ISM	433/868/780/915 MHz ISM
Name of Standard	LTE-Cat M	IEEE P802.11ah (low power WiFi)	Dash7 Alliance Protocol 1.0	Ingenu RPMA	nWave
Frequency Band	Cellular	License-exempt bands below 1 GHz, excluding the TV White Spaces	433, 868, 915 MHz ISM/SRD	2.4 GHz ISM	Sub-GHz ISM

Izvor: <https://www.cnx-software.com/2015/09/21/comparison-table-of-low-power-wan-standards-for-industrial-applications/>

- U SRN (*Short Range Networks*) mrežama u kojima je domet rasprostiranja signala manji moguće je primjenjivati neka od rješenja prikazanih u tablici 3.4.

Tablica 3.4. Usporedba SNR rješenja

Short Range Networks				
BLE	WIFI	Thread	ZigBee	Z-Wave
80m	50m	Mesh	100m/Mesh	30m/Mesh
No	No	No	-	-
2.4GHz	2.4GHz	2.4GHz	915MHz/2.4GHz	900MHz
Yes	Yes	Yes	Yes	Yes
Yes	Yes	-	Yes	Yes
< 1mbps	600mbps max	-	250kbps	10 - 100kbps
High	High	Low	Low	Low
Trusted devices problematic	Yes	Yes	Yes	Yes
Yes	Yes	Yes	Yes	Yes
Yes	Yes	-	Yes	Yes
Yes	Yes	No	Yes, mesh-based	Yes, mesh-based
No	Yes	-	-	-
Public or private	Public or private	Private/WIFI backbone	Public or private	Public or private
Bluetooth 4.0	IEEE802.11	Thread, based on 6LoWPAN IEEE802.15.4	ZigBee	Z-Wave
Yes		Yes	Yes	Limited

Izvor: <https://publisher.opensensors.io/connectivity>

Za primjenu senzorskih mreža u poljoprivredi naglasak je svakako potrebno staviti na pouzdanu i sigurnu bežičnu komunikaciju uz minimalnu potrošnju energije. Stoga se u takvim mrežama predlaže usporedba različitih koncepata za osiguravanje komunikacije, prema sljedećem konceptu.

- Za komunikaciju između postavljenih senzorskih čvorova i bazne stanice (*gatewaya*) moguće je ispitivanje optimizacije pri primjeni rješenja koja se koriste u SNR mrežama:
  - Wi-Fi
    - pogodan za brzi bežični prijenos velikih količina podataka
    - rad u 2,4 GHz i 5 GHz frekvenzijskim područjima
  - ZigBee
    - pogodan za primjene u kojima je bitan siguran prijenos podataka, ali nije nužna velika brzina prijenosa

- rad u 2,4 GHz frekvencijskom području
- Za komunikaciju između gateway-a i poslužitelja koji je namijenjen za upravljanje IoT ekosustavom/skladištenje senzorskih podataka predlaže se ispitivanje parametara komunikacije pri primjeni rješenja koja se koriste u LPWA mrežama:
  - 3G/4G/GPRS
    - omogućuje velike prijenosne brzine
    - rad u više frekvencijskih područja 800/900/1800/1900/2100 MHz
  - LoRa/LoRaWAN
    - podržava dvosmjernu komunikaciju uz niže prijenosne brzine
    - rad u 868/900 MHz frekvencijskom području

Optimalnost rješenja u pojedinim primjenama ovisit će o samim karakteristikama scenarija, pa ih je potrebno detaljnije razmotriti za svaki pojedini slučaj.

### 3.4. Literatura

[1] „Connect 2020 Agenda for Global Telecommunication / ICT Development“, ITU, 2014.

[2] „Broadband Development Strategy in the Republic of Croatia in 2011 – 2015“, Ministry of the Sea, Transport and Infrastructure of the Republic of Croatia, Zagreb, 2010.

[3] „Proposal for a Regulation of the European Parliament and of the Council on measures to reduce the cost of deploying high-speed electronic communications networks“, European Commission, 2013/0080 (COD), Brussels, 2013.

[4] „National Programme for the Development of Broadband Aggregation Infrastructure in Areas Lacking Sufficient Commercial Interest for Investments, as precondition for the Development of Next Generation Access Networks“, Ministry of Maritime Affairs, Transport and Infrastructure, Republic of Croatia, Zagreb, August 2014.

[5] „Croatian Quarterly Electronic Communications Market Dana“, Reports, Croatian Regulatory Authority for Network Industries, 2004 - 2016.

[6] „Usage of Information and Communications Technologies in Households and by Individuals“, Reports, Croatian Bureau of Statistics, Zagreb, 2007-2016



## 4. Odabrani pravno-regulatorni aspekti interneta stvari

### Izješće o istraživanju započeto u zadnjem kvartalu 2017.g.

Internet stvari (engl. *Internet of Things – IoT*) je infrastruktura u kojoj su milijarde senzora ugrađeni u standardne, svakodnevne uređaje ili predmete koji su povezani i putem jedinstvenog identifikatora komuniciraju s drugim uređajima, predmetima ili osobama, a namijenjeni su snimanju, obradi, pohrani i prijenosu podataka te komunikaciji s drugim uređajima ili sustavima putem Interneta ili drugih komunikacijskih mreža.

Golemi potencijal tržišta interneta stvari (u daljnjem tekstu i skraćeno kao „IoT“) uočen je već neko vrijeme, pa se prema predviđanjima tvrtke Gartner očekuje da će do 2020. godine više od 25 milijardi IoT uređaja biti online, dok će ukupne usluge na tom području doseći 263 milijarde dolara.<sup>1</sup>

Na razini EU-a jasno su izraženi ciljevi uspostave odgovarajućih uvjeta za razvoj jedinstvenog IoT tržišta. Pored fokusirane standardizacije i interoperabilnosti ključni čimbenici pritom su (*inter alia*) svakako mrežna povezanost te numeriranje i adresiranje (razvoj mreža nove generacije - 5G, prema komercijalnoj uporabi, raspodjela frekvencijskog spektra i dr.), čemu treba doprinijeti i daljnji razvoj regulatornog okvira EU-a u elektroničkom komunikacijskom sektoru.<sup>2</sup>

Velike prednosti od razvoja tržišta interneta stvari imaju korisnici takvih uređaja ali i brojne inovativne i kreativne tvrtke u EU i RH koje pružaju usluge i inovacije na području informacijsko-komunikacijskih tehnologija. Mnoge od njih morati će promijeniti poslovnu politiku te svoj fokus od razvoja i ponude tradicionalne informatičke tehnologije usmjeriti prema novim potrebama i zahtjevima tržišta interneta stvari.

Promjene koje donosi nagla ekspanzija interneta stvari nudi goleme financijske i druge mogućnosti takvim tvrtkama na brzo rastućem tržištu, ali istovremeno, takav prijelaz prate i brojne opasnosti za korisnike takvih uređaja i usluga. Da bi se izbjegle moguće greške i spriječile eventualne zloporabe treba stvoriti takav pravni okvir koji će obvezati ponuditelje

---

<sup>1</sup> Gartner Says 4.9 Billion Connected „Things“ Will Be in Use in 2015, 11.11.2014., <http://www.gartner.com/newsroom/id/2905717>.

<sup>2</sup> Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Digitalizacija europske industrije: Iskorištavanje svih prednosti jedinstvenog digitalnog tržišta, {SWD(2016) 110 final}, COM(2016) 180 final, Bruxelles, 19.4.2016.; Commission Staff Working Document, Advancing the Internet of Things in Europe, SWD/2016/0110 final, SWD(2016) 110 final, Brussels, 19.4.2016. (priležeci dokument).

takvih tehnologija i/ili usluga da pri izradi, ponudi i implementaciji takvih „svari“ vode računa o sigurnosti svojih proizvoda, intelektualnom vlasništvu, zaštiti potrošača i privatnosti krajnjih korisnika.

Kada je riječ o sigurnosti IoT uređaja, brojni stručnjaci već godinama ukazuju na sigurnosne propuste kada je riječ o IoT uređajima i nedovoljna ulaganja u tom vitalnom području te se sve više smatra da to tržište ne smije biti prepušteno samo sebi već da se vlade moraju izravno uključiti na prvome mjestu u reguliranje minimalnih sigurnosnih standarda za uređaje interneta stvari.<sup>3</sup> Ukazuju na to i rezultati najnoviji istraživanja tržišta. Tako je nedavno istraživanje (*Gemalto*)<sup>4</sup> pokazalo da čak 90% potrošača nema povjerenja u sigurnost IoT uređaja. Nedvojbena je stav anketiranih tvrtki da je potrebno donošenje propisa kako bi se regulirala sigurnost IoT-a. Potrebno je da vlade s jasnoćom definiraju tko je odgovoran za osiguravanje IoT uređaja i podataka u svakom trenutku na njihovu putu (61%), kao i posljedice njihova neusklađenog postupanja (55%). Čak 96% anketiranih tvrtki i 90% anketiranih potrošača traži provedivu regulaciju u području IoT sigurnosti. Iako potrošači očekuju da im IoT uređaji dolaze zaštićeni kao standard, tijela koja pohranjuju podatke, odnosno koriste IoT uređaje to ne čine. U tom su pogledu poražavajući rezultati ovog istraživanja. Naime, tek 57% njih kriptira sve podatke koje pohranjuju ili primaju. Nadalje, tek 6 od 10 njih koji kriptiraju, kriptiraju podatke čim IoT uređaj dohvati podatke (kada se radi o podacima koje pohranjuju: 62%; kada se radi o podacima koje šalju: 59%). Kada je riječ o osviještenosti i samozaštiti samih potrošača, tek 45% njih koji posjeduju IoT uređaj promijenilo je početnu lozinku na svim svojim IoT uređajima (onda kada ih uređaji uopće imaju).

Treba istaknuti i okolnosti koje predstavljaju najveći strah za potrošače pri korištenju IoT uređaja. To je na prvome mjestu preuzimanje kontrole nad njihovim uređajima povezanim s internetom (66% ispitanika), potom istjecanje podataka (60%), te neovlašteni pristup njihovim osobnim podacima (54%).

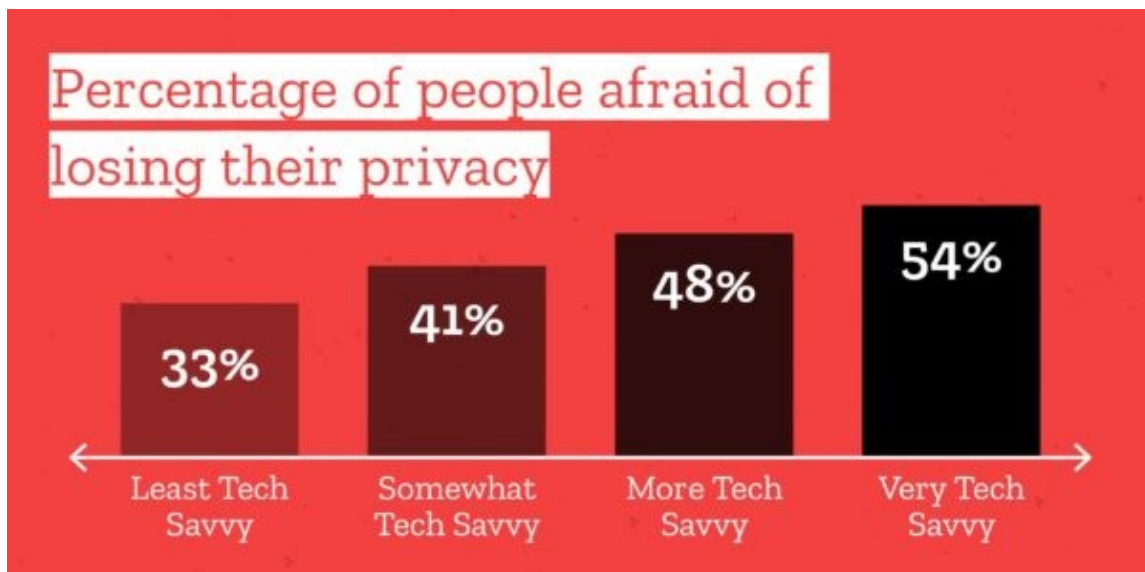
Valja navesti i nedavno objavljene rezultate *Mozilline* ankete o „povezanoj budućnosti korisnika.“<sup>5</sup> Kada je riječ o čimbenicima koji utječu na potrošače da kupe određeni IoT uređaj, cijena i značajke uređaja najvažniji su, dok su u odnosu na to pitanja sigurnosti i privatnosti od manjeg značaja. S druge strane anketirani korisnici interneta na globalnoj razini navodili su strah od gubitka privatnosti (45%) kao primarnu i najveću bojazan u viziji povezane budućnosti.

---

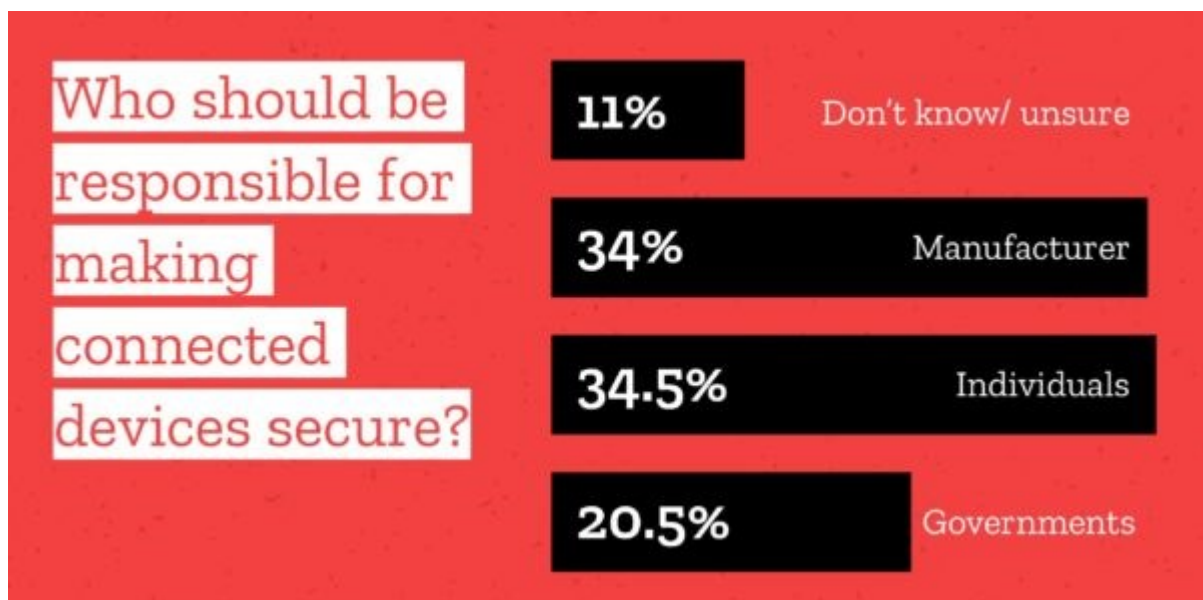
<sup>3</sup> Vidi npr. Schneier, Bruce, Your WiFi-connected thermostat can take down the whole Internet. We need new regulations., 3.11.2016., <https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/>.

<sup>4</sup> Gemalto, The state of IoT security, Security takes a back seat, Is it time for government-mandated IoT security regulations?, 2017., dostupno na: <http://www6.gemalto.com/state-of-iot-security-2017-press-release;> <http://www2.gemalto.com/iot/iot-security.html>.

<sup>5</sup> Caltrider, Jen, 10 Fascinating Things We Learned When We Asked The World ‘How Connected Are You?’, 1.11.2017., <https://blog.mozilla.org/blog/2017/11/01/10-fascinating-things-we-learned-when-we-asked-the-world-how-connected-are-you/>,



Zanimljivi su rezultati i u pogledu toga tko bi trebao snositi odgovornost za to da povezani uređaji budu privatni i sigurni. Tako trećina ispitanika smatra kako odgovornost trebaju snositi proizvođači IoT uređaja. Druga trećina smatra da se sami pojedinci moraju zaštititi online. Zadnja trećina anketiranih podijeljena je između toga da vlade trebaju snositi odgovornost za online privatnost i između onih koji na to pitanje ne znaju odgovor.



*Forresterovo* istraživanje pokazalo je predviđanja za 2018. godinu<sup>6</sup> da sigurnosni aspekti IoT-a nastavljaju biti ključan problem za razvoj navedenog tržišta. Radi se o ključnoj brizi svih tijela koja žele koristiti IoT uređaje ali i velikoj brizi onih koji ih proizvode (iako većina potonjih nema uspostavljen sustav konzistentnog upravljanja rizicima kada je o tome riječ, te poslovni pritisak značajno nadvladava nad pitanjima tehničke sigurnosti IoT uređaja). Predviđa se i to da će u 2018. godini biti još napada vezanih za IoT poput Mirai botneta<sup>7</sup>, no ti će napadi biti veći i kada je riječ o njihovu opsegu i kada je riječ o njihovim učincima.

Uspješan razvoj IoT tržišta ovisi o uspješnoj provedbi mjera kibersigurnosti, razvoju i implementaciji obvezujućih minimalnih standarda za IoT uređaje, adekvatnom uređenju pitanja pristupa podacima i uvjetima njihova korištenja, kao i o uspješnoj provedbi regulacije zaštićenih podataka. Osim toga, imajući u vidu kompleksno IoT okruženje važno je i adekvatna regulacija zaštite prava potrošača, napose kada je riječ o aspektu odgovornosti za štetu u slučaju malfunkcije IoT uređaja.

Kibersigurnost, uspostava čim sigurnijeg okruženja od kibernetičkih napada i sigurnosnih incidenata te zaštita kritične komunikacijske i informacijske infrastrukture predstavlja ključan preduvjet za razvoj interneta stvari. Zabrinjava podatak da je tijekom prošle (2016.) godine čak 80 % europskih kompanija imalo barem jedan incident u tom području.<sup>8</sup> Stoga je, kada je riječ o području kibersigurnosti naše istraživanje obuhvatit će ispitivanje mjera koje se poduzimaju u svrhu jačanja otpornosti EU-a i RH u tom području. Na EU razini treba istaknuti u rujnu ove godine objavljeni novi paket kibersigurnosti od strane Europske komisije, kojeg sačinjavaju:

- a) Prijedlog Uredbe Europskog parlamenta i Vijeća o ENISA-i (agenciji EU-a za kibersigurnost) i stavljanju izvan snage Uredbe (EU) 526/2013 te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Akt o kibersigurnosti”) {SWD(2017) 500 final} {SWD(2017) 501 final} {SWD(2017) 502 final}, COM(2017) 477 final 2017/0225 (COD), Bruxelles, 4.10.2017.;
- b) Zajednička komunikacija Europskom parlamentu i Vijeću, Otpornost, odvratanje i obrana: jačanje kibersigurnosti EU-a, JOIN(2017) 450 final, Bruxelles, 13.9.2017.;
- c) Preporuka Komisije od 13.9.2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera, C(2017) 6100 final, Bruxelles, 13.9.2017.;

---

<sup>6</sup> Voce, Chris (Forrester Research), In 2018, IoT will move beyond experimentation: The Internet of Things extends beyond devices and connectivity. Here's how Forrester predicts IoT will reshape businesses in 2018., 16.11.2017., <http://www.zdnet.com/article/in-2018-iot-will-move-beyond-experimentation/>.

<sup>7</sup> U.S. Department of Justice, Press Release, Justice Department Announces Charges And Guilty Pleas In Three Computer Crime Cases Involving Significant Cyber Attacks, 13.12.2017., <https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases>.

<sup>8</sup> PWC, Global State of Information Security Survey, 2016., i: <http://news.sap.com/pwc-study-biggest-increase-in-cyberattacks-in-over-10-years/>. Preuzeto sa: European Commission, Cybersecurity Factsheet, State of the Union 2017, Resilience, Deterrence and Defence: Building strong cybersecurity in Europe.

- d) Prijedlog Direktive Europskog parlamenta i Vijeća o borbi protiv prijevara i krivotvorenja bezgotovinskih sredstava plaćanja i zamjeni Okvirne odluke Vijeća 2001/413/PUP {SWD(2017) 298 final} {SWD(2017) 299 final}, COM(2017) 489 final, 2017/0226 (COD), Bruxelles, 13.9.2017., i
- e) Komunikacija Komisije Europskom parlamentu i Vijeću - Optimalno iskorištavanje potencijala Direktive NIS – prema učinkovitoj provedbi Direktive (EU) 2016/1148 o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, s Prilogom., COM(2017) 476 final, Bruxelles, 4.10.2017., s Prilogom.

Kada je riječ o kaznenopravnom zakonodavnom okviru i sankcioniranju kibernetičkog kriminala potrebno je istaknuti recentnije prilagodbe Kaznenog zakona<sup>9</sup> u svrhu provedbe *Direktive o napadima na informacijske sustave*<sup>10</sup>. S time u svezi potrebno je razmotriti i izvješće koje je Europska komisija u rujnu ove godine donijela o ocjeni mjere u kojoj su države članice poduzele mjere potrebne za usklađivanje s tom direktivom.<sup>11</sup>

Kada je riječ o provedbi mjera sigurnosti mrežnih i informacijskih sustava, u domaćem zakonodavnom okviru mora se čim hitnije (rok: svibanj 2018) provesti NIS Direktiva - *Direktiva 016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije*<sup>12</sup>. Ta provedba mora uzeti u obzir odredbe postojećih propisa, napose odredbe *Zakona o kritičnim infrastrukturama* (Narodne novine br. 56/13) i *Zakona o informacijskoj sigurnosti* (Narodne novine 79/07). Kako se navodi u nedavno usvojenom *Izvješću o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti*<sup>13</sup>, ključan problem predstavljat provedba zahtjeva za operatore ključnih usluga u okviru sektora kritične infrastrukture te utvrđivanje i usklađivanje kriterija i uvjeta za davatelje digitalnih usluga. Vezano za što bolju provedbu NIS Direktive nužno je analizirati i ispitati nedavno donesenu *Komunikaciju Komisije za učinkovitu provedbu NIS Direktive* (ranije navedenu u točki e ) i njezin Prilog.

---

<sup>9</sup> Narodne novine br. 125/11, 144/12, 56/15; 61/15 i 101/17.

<sup>10</sup> Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, SL L 218, 14.8.2013, str. 8–14.

<sup>11</sup> Izvješće Komisije Europskom parlamentu i Vijeću kojim se ocjenjuje u kojoj su mjeri države članice poduzele mjere potrebne za usklađivanje s Direktivom 2013/40/EU o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, COM(2017) 474 final, Bruxelles, 13.9.2017.

<sup>12</sup> SL L 194, 19.7.2016, str. 1–30.

<sup>13</sup> Nacionalno vijeće za kibernetičku sigurnost, *Izvješće o provedbi Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti*, rujna 2017. godine (prihvaćeno Zaključkom Vlade Republike Hrvatske, klasa: 022-03/17-07/376, Ur.br.: 50301-29/23-17-2 od 22. rujna 2017.).

Pored navedenog važno je ispitati i pratiti realizaciju *Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za njezinu provedbu*<sup>14</sup> kada je riječ o prepoznatim nužnim pravno-regulatornim mjerama u svrhu jačanja otpornosti na različite napade u kibernetičkom prostoru, osobito kada je riječ o napadima na kritičku infrastrukturu. Provedba mjera zaštite sigurnosti i cjelovitosti mreža i usluga u elektroničkom komunikacijskom sektoru regulirana je Zakonom o elektroničkim komunikacijama (Zakon o elektroničkim komunikacijama, Narodne novine br. 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17) i Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga (NN br. 109/12, 33/13, 126/13 i 67/16).

Okruženje interneta stvari generira iznimno velike količine podataka. Primjerice, kada je riječ o autonomnim vozilima, prema izjavi predsjednika uprave Intela iz 2016. godine ta vozila će u usporedbi s prosječnom osobom koja će uskoro koristiti oko 1.5. gigabajta podataka dnevno, koristiti oko 4000 gigabajta.<sup>15</sup> Stoga je razvoj tržišta interneta stvari neostvariv bez odgovarajućeg upravljanja podacima i o kojima IoT sustavi u osnovi ovise, te nužnih preduvjeta za otvaranje pristupa podacima. U tom kontekstu istraživanje bi se usredotočilo na utvrđivanje i analizu postojećih pravno-regulatornih ograničenja pri obradi i protoku podacima (ovisno o vrsti podataka o kojima je riječ) na nacionalnoj razini te na razini EU-a u mjeri u kojoj isto utječe na razvoj jedinstvenog podatkovnog tržišta i time na razvoj tržišta interneta stvari. Tako, na primjer, na domaćoj razini se to primjerice odnosi na regulatorna ograničenja prijenosu podataka s obzirom na njihovu lokaciju, te zahtijeva identifikaciju i analizu svih relevantnih propisa (npr. odredbe *Zakona o državnoj informacijskoj infrastrukturi*, Narodne novine br. 92/14 i *Uredbe o organizacijskim i tehničkim standardima za povezivanje na državnu informacijsku infrastrukturu*, Narodne novine br. 60/17 i dr.). Otvaraju se ovdje i pitanja „vlasništva“ nad neosobnim podacima u IoT okruženju (npr. nad podacima koje generiraju senzori), kao i pitanje ponovne uporabe podataka i pristupa podacima vezano za koje treba ispitati odredbe domaćeg *Zakona o pravu na pristup informacijama* (Narodne novine br. 25/13 i br. 85/2015) i relevantnih akata EU-a (*Direktiva o ponovnoj uporabi informacija javnog sektora*<sup>16</sup>). Od posebne je važnosti i ažurno praćenje aktualnih inicijativa u tom pogledu za daljnje otvaranje podataka (moguća revizija Direktive o ponovnoj uporabi informacija javnog sektora u tom smjeru, razmatranje i mogućnosti otvaranja pristupa i uporabe podataka privatnog sektora ako bi to bilo u javnom interesu).<sup>17</sup>

---

<sup>14</sup> Odluka o donošenju Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, Narodne novine br. 108/15.

<sup>15</sup> Beres, Damon, Autonomous cars may one day be data hogs, 17.8.2016., <http://mashable.com/2016/08/17/intel-autonomous-car-data/#CC5GTdRq0qqC>.

<sup>16</sup> Direktiva 2003/98/EZ Europskog parlamenta i Vijeća od 17. studenoga 2003. o ponovnoj uporabi informacija javnog sektora, SL L 345, 31.12.2003, str. 90–96., - posebno izdanje na hrvatskom jeziku: 13/Sv. 047, str. 141 – 147; Direktiva 2013/37/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o izmjeni Direktive 2003/98/EZ o ponovnoj uporabi informacija javnog sektora, SL L 175, 27.6.2013, str. 1–8., posebno izdanje na hrvatskom jeziku: 16/Sv. 4, str. 27-34.

<sup>17</sup> Upravo su dovršene javne konzultacije o reviziji Direktive o ponovnoj uporabi informacija, koje su trajale od 12. rujna do 12. prosinca 2017.: Commission launches public consultation on the review of the Directive on the

Kada je riječ o *neosobnim podacima*, imajući u vidu potencijal koje donosi razvoj podatkovnog tržišta Europske unije i nužne preduvjete da se isto realizira 2017. godine donesena je komunikacija “Stvaranje europskog podatkovnog gospodarstva”<sup>18</sup>, nastavno na koju je Komisija sredinom rujna 2017. godine podnijela prijedlog *Uredbe o okviru za slobodan protok neosobnih podataka u Europskoj uniji*<sup>19</sup>. Ciljevi su predložene Uredbe:

1. poboljšanje prekogranične mobilnosti neosobnih podataka na jedinstvenom tržištu, koja je danas ograničena u mnogim državama članicama ograničenjima uvedenima u svrhu lokalizacije podataka ili pravnom nesigurnošću na tržištu;
2. osiguravanje da ovlasti nadležnih tijela da zatraže i dobiju pristup podacima radi regulatorne kontrole, primjerice za potrebe inspekcijskih pregleda i revizija, ostanu nepromijenjene; i
3. olakšavanje promjene pružatelja usluga i prijenosa podataka za profesionalne korisnike usluga pohrane ili ostale obrade podataka, ali bez stvaranja prevelikog opterećenja za pružatelje usluga i narušavanja tržišta.

Istraživanjem bi se obuhvatila dubinska analiza predložene Uredbe (i prateće dokumentacije kao i studija specifičnih za Republiku Hrvatsku), praćenje tijeka zakonodavnog postupka u tom kontekstu i anticipiranje implikacija koje ista ima za razvoj tržišta IoT-a na lokalnoj i EU razini.

Kada je riječ o osobnim podacima novodonesena Opća uredba o zaštiti podataka<sup>20</sup>, koja će se primjenjivati diljem EU-a pa tako i u Hrvatskoj od kraja svibnja iduće godine, donosi brojne nove obveze koje su relevantne za tržište interneta stvari (npr. načelo pouzdanosti, odgovornosti izvršitelja obrade, integrirana i tehničke zaštita podataka, prijave povreda osobnih podataka, upravljanje rizicima; procjene učinaka na zaštitu osobnih podataka, profiliranje, postroženi uvjeti za dobivanje privole kod obrade osobnih podataka,

---

re-use of Public Sector Information, <https://ec.europa.eu/digital-single-market/en/news/commission-launches-public-consultation-review-directive-re-use-public-sector-information>. Komisija je najavila i javno saslušanje na temu (19. siječnja, 2018., .: Public hearing on the review of the Directive on the reuse of public sector information, <https://ec.europa.eu/digital-single-market/en/news/public-hearing-review-directive-reuse-public-sector-information>.

<sup>18</sup> Europska komisija, Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija „Stvaranje europskog podatkovnog gospodarstva”, {SWD(2017) 2 final}, COM(2017) 9 final, Bruxelles, 10.1.2017.

<sup>19</sup> Europska komisija, Prijedlog Uredbe Europskog parlamenta i Vijeća o okviru za slobodan protok neosobnih podataka u Europskoj uniji {SWD(2017) 304 final} {SWD(2017) 305 final}, COM(2017) 495 final, 2017/0228 (COD), Bruxelles, 13.9.2017.

<sup>20</sup> Uredba 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka, Službeni list Europske unije (dalje: SL) L 119, 04.5.2016, str. 1–88.

pseudonimizacija i dr.). Uspješna provedba ovog novog regulatornog režima osobito je važna za podizanje povjerenja potrošača i time za uspješan razvoj (i široko prihvaćanje) IoT tržišta. U tom je kontekstu nužno utvrditi i analizirati najrelevantnije nove i/ili postrožene obveze u tom području u odnosu na dosadašnji okvir. Osim toga nužno je pratiti daljnji razvoj domaćeg pravno-regulatornog okvira koji se donosi radi provedbe Uredbe, odnosno na temelju Uredbe (potonje u kontekstu mogućih iznimaka od primjene Uredbe i ograničenja koja se u pojedinim područjima mogu propisati domaćim zakonodavnim okvirima sukladno uvjetima propisanim u Uredbi).

Pored navedenog značajan utjecaj na razvoj tržišta interneta stvari imaju i pravila o zaštiti privatnosti i obradi osobnih podataka u elektroničkom komunikacijskom sektoru. Posebno je važno pratiti i kritički analizirati predložena rješenja nove *Uredbe o privatnosti i elektroničkim komunikacijama* (prijedlog Komisije iz siječnja o.g.)<sup>21</sup>, koja će staviti van snage važeću *Direktivu o privatnosti i elektroničkim komunikacijama*<sup>22</sup>, a koji je prijedlog Uredbe danas u zakonodavnom postupku. Osobito s obzirom na pravnu prirodu predloženih novih pravila te široko područje njihove primjene kao i novu kategorizaciju podataka koji se štite, nova pravila o povjerljivosti i (ne)dopuštenoj obradi elektroničkih komunikacijskih podataka, na prvome je mjestu važno analizirati mogućnost i ako da implikacije primjene novih pravila i na M2M komunikaciju te na okruženje interneta stvari. Radi se o posebno hitnom pitanju i s obzirom na nužnost usklađivanja predložene Uredbe s već donesenim pravilima Opće uredbe o zaštiti osobnih podataka, odnosno najavljenim hitnim donošenjem te Uredbe kako bi se u roku početka primjene u što manjoj mjeri „kaskalo“ za Općom uredbom o zaštiti osobnih podataka. U ranijim istraživanjima u okviru projekta apelirali smo na to da se na nacionalnoj razini provede hitno savjetovanje domaće javnosti vezano za reviziju Direktive o privatnosti. U međuvremenu je Europska komisija službeno objavila prijedlog novih pravila (Uredbe) i Republika Hrvatska donijela Stajalište o tom prijedlogu (čiji su nositelji Ministarstvo mora, prometa i infrastrukture i HAKOM<sup>23</sup>), koje su podržali Odbor za ljudska prava i prava nacionalnih manjina<sup>24</sup> kao i Odbor za europske poslove (Odbor za pravosuđe nije raspravljao).<sup>25</sup> Vlada Republike Hrvatske dužna je do usvajanja navedenog prijedloga Uredbe

---

<sup>21</sup> Prijedlog Uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama), {SWD(2017) 3 final} {SWD(2017) 4 final} {SWD(2017) 5 final} {SWD(2017) 6 final}, COM(2017) 10 final, 2017/0003(COD), Bruxelles, 10.1.2017.

<sup>22</sup> Direktiva o 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama, SL L 201, 31.7.2002., str. 37-47. - posebno izdanje na hrvatskom jeziku: 13/Sv. 52, str. 111-121. Ta je direktiva mijenjana Direktivom 2006/24/EZ i Direktivom 2009/136/EZ.

<sup>23</sup> Stajalište Republike Hrvatske o Prijedlogu uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama) COM (2017) 10, <http://edoc.sabor.hr/DocumentView.aspx?entid=2004295>.

<sup>24</sup> <http://www.sabor.hr/misljenje-odbora-za-ljudska-prava-i-prava-naci0002>.

<sup>25</sup> [edoc.sabor.hr/DocumentView.aspx?entid=2004874](http://edoc.sabor.hr/DocumentView.aspx?entid=2004874).



u Europskom parlamentu i Vijeću redovito izvješćivati Sabor o značajnijim izmjenama prijedloga Uredbe kao i o izmjenama Stajališta Republike Hrvatske.

Naposljetku, ukoliko opseg istraživanja to dopusti, moguće je utvrđivanje te ispitivanje i drugih legislativnih inicijativa na razini EU-a s potencijalnim utjecajem na razvoj tržišta interneta stvari u svrhu procjene učinka istih u tom kontekstu i na razvoj tog tržišta nacionalnoj razini (npr. nedavno izmijenjeni prijedlog Direktive o određenim aspektima ugovora o prodaji robe na internetu i drugoj prodaji robe na daljinu<sup>26</sup>, moguća revizija<sup>27</sup> *Direktive o pravnoj zaštiti baza podataka*<sup>28</sup>). U istom je kontekstu korisno i praćenje studija i drugih aktualnosti vezano za moguću ocjenu (i/ili reviziju) važećeg regulatornog okvira EU-a u vezi s odgovornosti za neispravne proizvode (*Direktiva o odgovornosti za neispravne proizvode*<sup>29</sup> i *Direktiva o strojevima*<sup>30</sup>). To osobito s obzirom na to da se u kompleksnom lancu IoT-a i među-povezanih uređaja mogu pojaviti i posve novi aspekti odgovornosti za štetu, uključujući, ali ne ograničavajući se na pitanja identifikacije uzroka štete i onih koji su u proizvodnom i/ili dostavnom lancu odgovorni (npr. ako je šteta u vezi s uslugom ili proizvodom nastala u vezi s dostavom pogrešnih podataka ili općenito zbog ne-dostave podataka, ranjivosti softvera, nestabilnosti mreže i dr.).

---

<sup>26</sup> Izmijenjeni prijedlog Direktive Europskog parlamenta i Vijeća o određenim aspektima ugovora o prodaji robe na internetu i drugoj prodaji robe na daljinu, izmjeni Uredbe (EZ) br. 2006/2004 Europskog parlamenta i Vijeća i Direktive 2009/22/EZ Europskog parlamenta i Vijeća te stavljanju izvan snage Direktive 1999/44/EZ Europskog parlamenta i Vijeća {SWD(2017) 354 final}, COM(2017) 637 final, 2015/0288(COD)., Bruxelles, 31.10.2017.

<sup>27</sup> Javne konzultacije o toj direktivi Europska je komisija provela u razdoblju od 24. svibnja do 30. kolovoza ove godine, vidi: Commission launches public consultation on Database Directive, <https://ec.europa.eu/digital-single-market/en/news/commission-launches-public-consultation-database-directive>.

<sup>28</sup> Direktiva 96/9/EZ Europskog parlamenta i Vijeća od 11. ožujka 1996. o pravnoj zaštiti baza podataka, SL L 77, 27.3.1996, str. 20–28.; posebno izdanje na hrvatskom jeziku: 13/Sv. 024, str. 36–44.

<sup>29</sup> Direktiva Vijeća od 25. srpnja 1985. o približavanju zakona i drugih propisa država članica u vezi s odgovornošću za neispravne proizvode, 85/374/EEZ, SL L 210, 7.8.1985, str. 29–33 - posebno izdanje na hrvatskom jeziku: 15/Sv. 22, str. 3–7.

<sup>30</sup> Direktiva 2006/42/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o strojevima o izmjeni Direktive 95/16/EZ (preinaka), SL L 157, 9.6.2006, str. 24–86. – posebno izdanje na hrvatskom jeziku: 13/Sv.039, str. 74–136.

## 5. Internet stvari: studijski primjer pametnog grada

### 5.1. Uvod

Pojam pametni grad (*smart city*) opisuje razvoj urbane sredine kojim se pridonosi njenoj održivosti i unapređuje kvaliteta življenja. Upotrebljava se u različitim kontekstima i okolnostima, često reduciran na neki specifični problem, bez sustavnog sagledavanja tehnoloških rješenja, posebice onih zasnovanih na informacijskoj i komunikacijskoj tehnologiji. Izdvojiti će se nekoliko izvornih definicija pametnog grada:

“A smart sustainable city is an innovative city that uses information and communication technologies (ICTs) and other means to improve quality of life, the efficiency of urban operation and services and competitiveness, while ensuring that it meets the needs of present and future generations with respect to economic, social and environmental aspects.” (International Telecommunication Union, Telecommunication Standardization Sector, ITU-T)

“A smart city is one where the government and citizens are using the best available means, including the ICT, to achieve their shared goals. This often includes economic development, environmental sustainability, and improved quality of life for citizens. A connected city is one where all relevant city systems – transportation, utilities, employment, health care, public safety, education, and others – are capable of communicating with each other to allow coordination and reduce waste.” (US Department of Transportation)

Elektroničke komunikacije omogućitelj su ovakvog razvoja urbanih sredina čija je temeljna pretpostavka umreženost bez prostornih, vremenskih i resursnih ograničenja. Pritom specifičnu ulogu ima Internet stvari [1].

### 5.2. Pametni sustavi - funkcijske komponente pametnog grada

Za cjelovit obuhvat elektroničkih komunikacija i Interneta stvari predlažu se sljedeće funkcijske komponente pametnog grada (Slika 5.1.), pri čemu se digitalna infrastruktura smatra dijelom rješenja i kao takva ne uvodi u ovaj model:

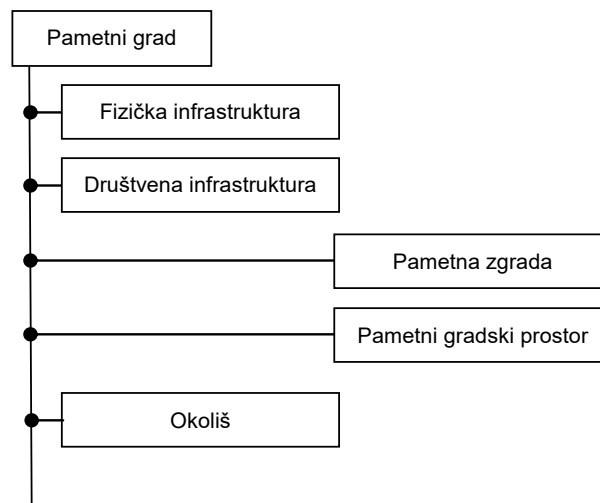
- Fizička infrastruktura (energija, transport, voda, otpad, ...);
- Društvena infrastruktura (zdravlje, starenje, obrazovanje, kultura, zabava, način života, ...);
- Okoliš (klimatske promjene, onečišćenje i zagađenje, prirodne i druge katastrofe i incidenti, ...).

Izdvojene su zatvorene (zgrade) i otvoreni prostori (ulice, trgovine, parkovi, ...) sa specifičnim rješenjima fizičke infrastrukture, odnosno ulogom u ostvarivanju društvene infrastrukture.

Kako bi se ostvario pomak od automatizacije (karakteristična danas za fizičku infrastrukturu) prema autonomnom načinu rada te od informacijskih sustava (karakteristični danas za društvenu infrastrukturu) prema uslugama informacijskog društva, „gradski“ sustavi trebaju poprimiti obilježja povezanih pametnih sustava (*smart system*), uključujući kibernetičko-fizičke sustave (*cyber-physical system*). I ovdje se navode izvorne definicije:

*Smart systems* are “self-sufficient intelligent technical systems or subsystems with advanced functionality, enabled by underlying micro- nano- and bio-systems and other components. They are able to sense, diagnose, describe, qualify and manage a given situation, their operation being further enhanced by their ability to mutually address, identify and work in consort with each other.” (EpoSS – The European Technology Platform on Smart Systems Integration)

*Cyber-physical systems* are “smart systems that include engineered interacting networks of physical and computational components. Cyber-physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfil time-sensitive functions with varying degrees of interaction with the environment, including human interaction.” (National Institute of Standards and Technology, US Department of Commerce)



Slika 5.1. Osnovne funkcijske komponente pametnog grada

Pametni sustavi sadrže povezane pametne entitete – objekte (*Connected Smart Object, CSO*) koji namijenjene im zadaće provode samostalno ili u interakciji s drugim objektima ili ljudima. Pojam „objekta“ ima različito značenje u pojedinim istraživačkim zajednicama (*Cyber-physical system: “component”, Internet of Things: “thing”, Machine-to-Machine*

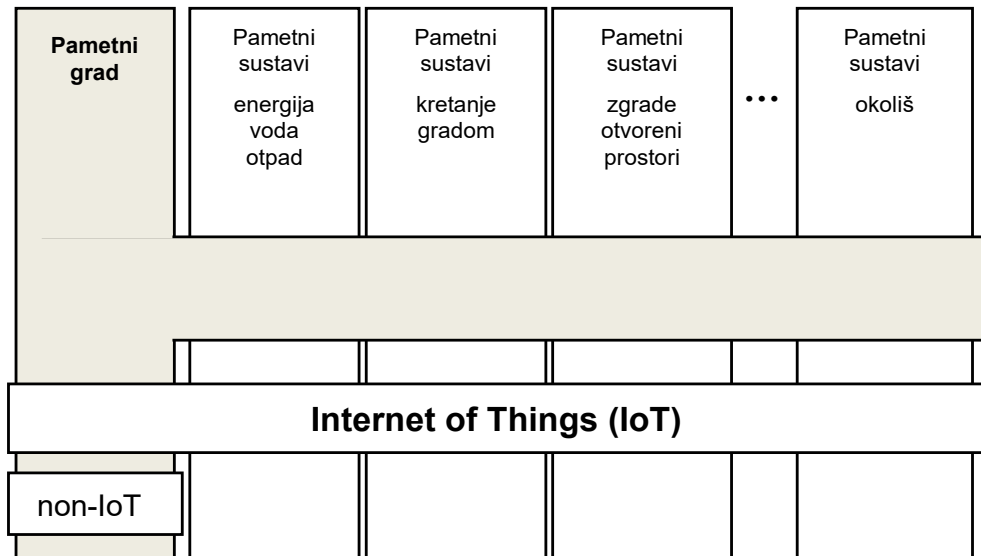
*Communications: "machine"*). Naravno da svi objekti u nekom sustavu ne trebaju biti "pametni", ali moraju se moći povezati i umrežiti.

Osnovna obilježja povezanih (pametnih) objekata potrebna za evaluaciju njihovih komunikacijskih i mrežnih zahtjeva slijede:

- Pojavni oblik: fizički (senzor, mjerac, aktuator) ili virtualni (reprezentant fizičkog objekta ili isključivo virtualni objekt)
- Fizička izvedba: samostalni uređaj (senzor, mjerac, aktuator) ili ugrađen u komunikacijski ili računalni uređaj (npr. pametni telefon), kućanski aparat (npr. frižider), ili medijski uređaj (npr. pametni televizor)
- Interaktivnost: međusobna, ili interakcija s čovjekom (izravna ili posredna, mogući problemi s privatnošću)
- Povezanost: stacionarna, nomadska i pokretna komunikacija zasnovana na IP-mreži, mrežna pokrivenost uključujući širokopolasni pristup Internetu (nije i ne smije biti problem u gradovima)
- Osnovna nefunkcijska obilježja: raspoloživost (*availability*), pouzdanost (*reliability*), zaštita (*safety*), cjelovitost (*integrity*), mogućnost održavanja (*maintainability*) [2]
- Osnovna obilježja sigurnosti: raspoloživost, cjelovitost, povjerljivost/tajnost (*confidentiality*) [2]
- Količina informacije koju objekt šalje/prima: ekstremne varijacije, od pojedinačnog podatka (paket, poruka, ...) do struje podataka (video, audio, ...), u stvarnom vremenu ili uz vremensku relaksaciju, uzimajući u obzir zahtijevano vrijeme odgovora ili provedbe akcije.

### **5.3. Domena pametnog grada s motrišta Interneta stvari**

Pametni grad kao domena primjene Interneta stvari obuhvaća tehničke sustave izvedene kao pametni sustavi vezane uz upravljanje energijom, vodom, otpadom, kretanjem, zgradama i otvorenim prostorima, kao i nadzorom okoliša (slika 5.2.).



Slika 5.2. Medusektorski prikaz domene pametnog grada

Ovakav horizontalan pogled na pametni grad odgovara ulozi Interneta stvari, uz napomenu da i druga “non-IoT” rješenja zasnovana na ICT-u pridonose, posebice društvenoj infrastrukturi pametnog grada (zdravlje i starenje, socijalnu skrb, obrazovanje, kulturu, zabavu, rekreaciju, turizam, ...).

Nova vrijednost koju unosi Internet stvari može se karakterizirati ovako:

- Poboljšane mogućnosti (npr. mjerenje potrošnje u stvarnom vremenu koje omogućuje dinamičku naplatu i bolje uravnoteženje potrošnje).
- Mogućnost objedinjenog upravljanja (npr. integracija posebnih sustava automatizacije u zgradi kako bi se postiglo učinkovito korištenje raspoloživih sredstava, poboljšalo korisničko iskustvo i smanjila potrebna ulaganja i troškovi).
- Iskorištenje mogućnosti samo-prilagodbe (npr. upravljanje prometom zasnovano na različitim izvorima prometnih i okolišnih podataka u cilju smanjenja gužve i zagađenja zraka).
- Potpuno nove usluge i aplikacije koje ne mogu pružiti postojeći sustavi te nove usluge i aplikacije s kojima se oni mogu transformirati u pametne sustave i usluge.

Prve tri kategorije obilježavaju prethodno spomenuti pomak od automatizacije prema autonomnom radu. Upravo to tretira većina analiza tržišta Interneta stvari – tu postoje iskustva s tradicionalnim poslovanjem, javnim uslugama i njihovom naplatom.

Četvrta kategorija je prijelomna novost, ne samo po potencijalnoj širini primjene (ŠTO), već i po samom nastanku (KAKO): tko sve može biti i tko će sve biti *kreator*, *izvođač*, *proizvođač*, ili *davatelj* usluga i aplikacija Interneta stvari?

#### 5.4. Lanac vrijednosti Interneta stvari

Kao polazne postavke pri definiranju lanca vrijednosti odabiru se ove:

- Fizički objekt može biti izveden: a) kao samostojeći ili dio nekog uređaja sastavljen od komponenata koje omogućuju njihovu senzorsku ili aktivacijsku funkciju, ili b) objekt ugrađen u pametnom telefonu.
- Fizički objekt izveden kao samostojeći ili dio nekog uređaja može komunicirati stacionarno ili u pokretu, javnom ili privatnom mrežom, izravno ili putem pametnog telefona koji osigurava prihvata i izmjenu podataka (*Bluetooth* ili druge tehnologije).
- IoT-usluga može biti izvedena: a) kao usluga koja zahtijeva određeni fizički objekt ili b) kao usluga koja se oslanja isključivo na (senzorske) mogućnosti pametnog telefona.
- IoT-aplikacija dostupna putem aplikacijskog spremišta (*store*): a) obavlja neku specifičnu funkcionalnost u okviru IoT-sustava ili b) predstavlja samo korisničko sučelje neke IoT-usluge.

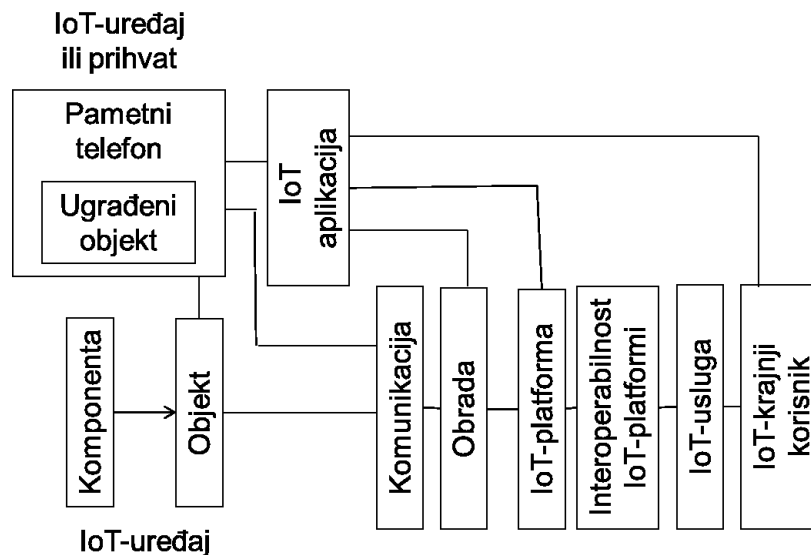
Lanac vrijednosti predočen je na slici 5.3. sa svoje četiri središnje komponente kojima se ostvaruju komunikacija, obrada, IoT-platforma i interoperabilnost IoT-platformi, oko kojih se razvijaju i pružaju usluge i aplikacije.

Ovakav pristup zagovara otvoreno distribuirano rješenje s više davatelja usluga (više IoT platformi – više sustava), u odnosu na centralizirano rješenje s jednim davateljem usluga (jedna IoT-platforma – više ili svi sustavi), ili s više njih, ali bez međusobne suradnje.

Iskustvo pametnih telefona i pokretnih aplikacija pokazuje da se nikoga ne smije isključiti u lancu vrijednosti Interneta stvari, a posebice ne osobe – građane. Građani se mogu očekivati u više uloga u IoT, kao:

- krajnji korisnici usluga i aplikacija, što će biti većina,
- davatelji podataka i informacija za usluge i aplikacije, što će biti mnogi i
- kreatori i razvijatelji usluga i aplikacija, što će biti poneki.

Uz građane potrošače (*consumer*), očekuju se građani koji su ujedno i proizvođači (*prosumer*), prvenstveno podataka raspoloživih iz pametnog telefona i u njega ugrađenih fizičkih objekata (raznovrsni senzori) te virtualnih objekata kojima mogu pristupiti. Uz to, pametni telefon služi za prihvata i izmjenu podataka s drugim fizičkim objektima kojima raspolaže korisnik [3], primjerice nosivi uređaj (*wearable*), ili uređaj vezan uz prijevozno sredstvo.



Slika 5.3. IoT-lanac vrijednosti za domenu pametnog grada

### 5.5. Normizacijski i regulatorni aspekti

Elektroničke komunikacije i Internet stvari u pametnom gradu i za pametni grad elaborirani su detaljnije u [4, 5], tako da se u nastavku razmatraju samo neka opća pitanja normizacije i regulacije. Normizacija i regulativa vezana uz pametni grad je u nastajanju, a obuhvaća tehnološke i organizacijske aspekte, uključujući ICT u širem smislu, elektroničke komunikacije i sam Internet stvari. Elektroničke komunikacije imaju dvostruku ulogu u pametnom gradu:

- brzi i ultra brzi pristup Internetu te
- povezivanje objekata, stacionarno ili u pokretu, trajno ili na zahtjev.

Prva je u potpunosti pokrivena normizacijom i regulatornim okvirom, uključujući mjere za smanjenje troškova uvođenja i izvedbe takvih mreža. Druga je uloga u mnogome složenija i manje uređena – riječ o složenom ekosustavu Interneta stvari koji obuhvaća više tradicionalnih sektora, s elektroničkim komunikacijama kao omogućiteljem. U Europskoj uniji pametni grad predmet je političkog interesa koji se očituje u okvirnim programima istraživanja i inovacija [6, 7]. S motrišta sudjelovanja Hrvatske ističu se ovi projekti:

- Open IoT – Open Source cloud solution for the Internet of Things  
([www.openiot.eu](http://www.openiot.eu)) [8].
- symbIoTe – symbiosis of smart objects across IoT environments  
([www.symbiote-h2020.eu](http://www.symbiote-h2020.eu))

Normizacijski i regulacijski procesi vezani uz Internet stvari u pametnom gradu mogu se razložiti na nekoliko slojeva, od tehnoloških i organizacijskih aspekata pametnog grada i horizontalnih obvezujućih smjernica koje se odnose na sva područja djelovanja i poslovanja pa tako i pametni grad, preko onih za elektroničke komunikacije, do posebnih za pojedine sektore.

Različite aspekte pametnog grada razrađuju Međunarodna organizacija za normizaciju (*International Organisation for Standardisation, ISO*) i Međunarodno elektrotehničko povjerenstvo (*International Electrotechnical Commission, IEC*), o čemu su objavili zajedničko izvješće [9]. Obuhvaćene su norme vezane uz ICT, zgrade i fizičku infrastrukturu, usluge pametnog grada te upravljanje pametnim gradom.

Od horizontalnih mjera s posebnim utjecajem na pametni grad su zaštita podataka i privatnost, uključujući elektroničke komunikacije i Internet stvari s pridruženim računarstvom u oblaku (*cloud computing*) te obradom velike količine podataka (*Big Data*) [10, 11].

Nadalje, opće reguliranje elektroničkih komunikacija, mreža i usluga, Interneta stvari i komunikacije strojeva (*Machine to Machine, M2M*) razmatraju Međunarodna telekomunikacijska unija (*International Telecommunication Union, ITU*) i Tijelo europskih regulatora za elektroničke komunikacije (*Body of European Regulators for Electronic Communications, BEREC*) [12, 13].

Na kraju, tu je i sektorska regulacija, sa sljedeća dva primjera vezana uz elektroničke komunikacije i Internet stvari:

- „Direktiva o energetske učinkovitosti“: očekuje se da će 80% domaćinstava do 2020. imati instalirana pametna električna brojila, uz uvođenje inteligentnih mjernih sustava za druge energente [14].
- „Uredba eCall“: sva nova vozila trebaju imati instaliran uređaj koji automatski bira 112 u slučaju nesreće, pri čemu bi trebalo promicati opremanje vozila proizvedenih nakon 31. ožujka 2018. sustavom eCall [15].

Dodatno, za razvoj usluga i aplikacija Interneta stvari važna je otvorenost javnih podataka [16, 17]. Kako bi se pospješilo europsko podatkovno gospodarstvo postavlja se jedan od novih ciljeva: pristup gospodarstva strojno generiranim podacima kako bi se potaknule inovacije i digitalno gospodarstvo [18].

Složenost problema normizacije i regulatornog okvira je očevidna. Internet stvari je Europska komisija definirala jednim od ključnih područja standardizacije, uz tehnologiju 5G, računarstvo u oblaku, kibernetičku sigurnost i podatkovne tehnologije, a koji su povezani s Internetom stvari [19-22]. Razvoj regulatornog okvira nije definiran tako „precizno“ – pretežno se naglašavaju pravni aspekti zaštite podataka i privatnosti, a kao moguće prepreke navode raspoloživost frekvencijskog spektra i sustava numeracije.

Normizacija nije i neće biti dovoljna za iskorištenje inovacijskog potencijala Interneta stvari i pridruženih tehnologija, ne samo za rješavanje društvenih izazova, već i za industrijski razvoj



i nastajanje novih industrija. Smanjit će probleme vezivanja uz jednog i promjenu proizvođača ili davatelja usluga, ali sama po sebi neće stvoriti konkurentno IoT-okruženje u kojem djeluju poduzeća svih veličina, od mikro poduzeća do globalnih kompanija, s građanima kao aktivnim sudionicima.

Manjim gospodarstvima kao što je hrvatsko može se dogoditi da u zemlji budu samo fizički objekti – stvari kojima se omogućuju usluge Interneta stvari i krajnji korisnici – potrošači koji ih plaćaju (fizičke i pravne osobe), a da sustavi kojima se usluge ostvaruju i davatelji usluga budu „bilo gdje“, uz obrazloženje da „to omogućuje Internet“, uz „puno manje troškove zbog ekonomije razmjera“ (poznati model iz materijalne proizvodnje: izvoz sirovina (podataka), uvoz proizvoda više dodane vrijednosti (usluga i aplikacija)). Može se dogoditi da normizacijska otvorenost Interneta stvari ne unese stvarnu otvorenost, od programskih platformi i rješenja otvorenog koda, do društva i tržišta koji potiču i omogućuju kreativnost, inovativnost i kompetitivnost, industrijski razvoj i nastajanje nove industrije.

Stoga je potrebno uspostaviti otvoreno distribuirano okruženje s davateljima usluga i aplikacija Interneta stvari s različitim IoT-plattformama, otvorenima i vlasničkim, i rješenjima za njihovu interoperabilnost koja mikro, malim i srednjim poduzećima omogućuju i olakšavaju razvoj inovativnih usluga i aplikacija korištenjem sredstava obuhvaćenih s jednom i više IoT-plattformi [1].

Regulatorni procesi u području Interneta stvari trebaju voditi računa o dinamici uvođenja, inovacijama, ulaganjima, pravnoj sigurnosti te društvenom i poslovnom okruženju. U područjima koja nisu harmonizirana na razini Europske unije primjereni su postupci meke regulacije (*soft regulation*). Međutim, za njihovu učinkovitost potrebna je nacionalna strategija inovacija i industrijske politike u domeni Interneta stvari. Regulatorna tijela tad mogu usmjeravati i poticati provedbu strateških ciljeva, nadzirati razvoj i pridonositi razumijevanju Interneta stvari.

## 5.6. Literatura

- [1] I. Lovrek, I. Podnar Žarko, M. Marjanović, “Internet stvari: stanje tehnologije i izazovi interoperabilnosti”, Projekt “Pogled u budućnost 2020”, Izvještaj Q2 2016, Zagreb, 2016.
- [2] A. Avizienis, J-C. Laprie, B. Randell, and C. Landwehr, „Basic Concepts and Taxonomy of Dependable and Secure Computing“, IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 1, 2004, pp. 11-33.
- [3] „Requirements of smartphone as sink node for IoT applications and services”, Recommendation ITU-T Y.4553, International Telecommunication Union, 2016.
- [4] D. Lučić, M. Weber, I. Lovrek, “Electronic Communications as Smart City Enablers”, Proceedings 2016 International Conference on Smart systems and Technologies (SST), Osijek, 2016., pp. 241-247.

- [5] M. Weber, D. Lučić, I. Lovrek, "Internet of Things Context of the Smart City", Proceedings 2017 International Conference on Smart systems and Technologies (SST), Osijek, 2017., pp. 187. – 193
- [6] "Smart cities and communities – European innovation partnership", Communication from the Commission, European Commission, C(2012) 4701 final, Brussels, 10.7.2012.
- [7] „Mapping Smart Cities in the EU“, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policies, January 2014.
- [8] I. Podnar Zarko, K. Pripuzic, and M. Serrano (eds.), "Interoperability and Open-Source Solutions for the Internet of Things", Lecture Notes in Computer Science, Vol. 9001, Springer, 2015.
- [9] "Smart cities, Preliminary Report 2014“, ISO/IEC JTC 1, Information technology, 2015.
- [10] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).
- [11] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama).
- [12] I. Brown, „Regulation and the Internet of Things“, GSR Discussion Paper, 15th Global Symposium for. Regulators, ITU International Telecommunication Union, 2015.
- [13] „Enabling the Internet of Things“, Report, BEREC – Body of European Regulators for Electronic Communications, BoR (16) 39, 12 February 2016.
- [14] Direktiva 2012/27/EU Europskog parlamenta i Vijeća od 25. listopada 2012. o energetske učinkovitosti, izmjeni direktiva 2009/125/EZ i 2010/30/EU i stavljanju izvan snage direktiva 2004/8/EZ i 2006/32/EZ
- [15] Uredba (EU) 2015/758 EU Europskog parlamenta i Vijeća od 29. travnja 2015. o zahtjevima za homologaciju za uvođenje sustava eCall ugrađenog u vozilo koji se temelji na službi 112 te o izmjeni Direktive 2007/46/EZ
- [16] „Digitalizacija europske industrije Iskorištavanje svih prednosti jedinstvenog digitalnog tržišta“ {SWD(2016) 110 final}, Komunikacija Komisije Europskom parlamentu, Vijeću Europskom i socijalnom odboru i Odboru regija, COM(2016) 180 final, Bruxelles, 19.4.2016.
- [17] Direktiva 2003/98/ Europskog parlamenta i Vijeća od 17. studenoga 2003. o ponovnoj uporabi informacija javnog sektora.
- [18] Direktiva 2013/37/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o izmjeni Direktive 2003/98/EZ o ponovnoj uporabi informacija javnog sektora.

[19] „Stvaranje europskoga podatkovnog gospodarstva“ {SWD(2017) 2 final, Komunikacija Komisije Europskom parlamentu, Vijeću Europskom i socijalnom odboru i Odboru regija, COM(2017) 9 final, Bruxelles, 10.1.2017.

[20] „Advancing the Internet of Things in Europe“, Commission Staff Working Document, SWD(2016) 110 final, Brussels, 19.4.2016

[21] „Roundtable on Digitising European Industry: Working Group 1 – Digital Innovation Hubs: Mainstreaming Digital Innovation Across All Sectors“, Final Version, European Union, June 2017

[22] „Digitising European Industry: Working Group 2 – Digital Industrial Platforms“, Final version, European Union, August 2017