

**UNIVERZITET PRIVREDNA AKADEMIJA U NOVOM SADU
FAKULTET ZA EKONOMIJU I INŽENJERSKI MENADŽMENT U NOVOM SADU**

„Digitalna transformacija poslovanja i njene bezbednosne implikacije“

Doktorska disertacija

MENTOR:

Prof. dr Dragan Soleša

KANDIDAT:

mr Petar Čelik

Novi Sad, 2020. godine

**UNIVERSITY BUSINESS ACADEMY IN NOVI SAD
FACULTY OF ECONOMICS AND ENGINEERING MANAGEMENT IN NOVI SAD**

"Digital Transformation of Business and its Safeness Implications"

Doctoral dissertation

MENTOR:

Prof. dr Dragan Soleša

CANDIDATE:

mr Petar Celik

Novi Sad, 2020

UNIVERZITET PRIVREDNA AKADEMIJA U NOVOM SADU

FAKULTET ZA EKONOMIJU I INŽENJERSKI MENADŽMENT U NOVOM SADU

KLJUČNI PODACI O ZAVRŠNOM RADU

Vrsta rada:	Doktorska disertacija
Ime i prezime autora:	mr Petar Čelik
Mentor (titula, ime, prezime, zvanje, institucija)	Prof. dr Dragan Soleša, redovni profesor, uža naučna oblast Kvantitativne metode i informacioni sistemi, izabran 27.04.2010. godine, Fakultet za ekonomiju i inženjerski menadžment u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu
Naslov rada:	„Digitalna transformacija poslovanja i njene bezbednosne implikacije“
Jezik publikacije (pismo):	Srpski, latinica
Fizički opis rada:	Uneti broj: Stranica <u>339</u> Poglavlja <u>VIII</u> Referenci <u>244</u> Tabela <u>11</u> Slika <u>17</u> Grafikona <u>17</u>
Naučna oblast:	Kvantitativne metode i informacioni sistemi
Predmetna odrednica, ključne reči:	Digitalna transformacija poslovanja, digitalna ekonomija, disruptivne inovacije, digitalizacija, sajber bezbednost
Izvod (apstrakt ili rezime) na jeziku završnog rada:	U novije vreme, pod pritiskom ubrzanih, široko disperzovanih i diverzifikovanih digitalnih inovacija kao generatora sveopšteg društvenog i privrednog razvoja, dve recentne pojave, procesa i

	<p>fenomena: digitalna transformacija poslovanja i sajber bezbednost izazivaju veliko interesovanje i to ne samo poslovnih i političkih krugova, već i naučno-istraživačkog sektora. Nezavisno od toga što su proizašli iz različitih izvora, njihov zajednički vremenski kontekst jasno implicira stav da su ovi procesi međusobno uslovljeni, da jedan drugi prožimaju i da njihovi izazovi deluju podudarno i da imaju konvergentan smisao. Prema problemskom i razvojnom zahvatu, ti izazovi su veoma slični, kao i po svojim diskurzivnim formacijama. Mada nastupaju iz različitih, a ponekad i veoma sličnih i graničnih disciplinarnih područja - jedan iz oblasti informatičkih, a drugi iz bezbednosnih sfera, oni u tematskom smislu imaju izukrštan referentni okvir i najčešće upućuju na potrebu sinergetskog delovanja koje svoju rezultatnu uspostavlja u domenu ekonomije. Na osnovu vizuelizacije potpuno merljivih performansi i algoritama, digitalna tehnologija je poslednjih godina dramatično promenila i nastavlja da ubrzanim tempom redizajnira način poslovanja, obrazovanja, zabave, javnog sektora, kao i drugih društvenih segmenata. Konfiguracija i obim promena, uz neizbežnu disrupciju odvijaju se na tri nivoa: individualnom, organizacionom i društvenom.</p>
Datum odbrane: (Popunjava naknadno odgovarajuća služba)	
Članovi komisije: (titula, ime, prezime, zvanje, institucija)	<p>1. Prof. dr Dragan Soleša, redovni profesor, uža naučna oblast: Kvantitativne metode i informacioni sistemi, izabran 27.04.2010. godine, Fakultet za ekonomiju i inženjerski menadžment u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu - mentor.</p> <p>2. Prof. dr Vladimir Šimović, redovni profesor, uža naučna</p>

	<p>oblast: Kvantitativne metode i informacijski sistemi, izabran 27.02.2018. godine, Fakultet za ekonomiju i inženjerski menadžment u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu - predsednik komisije.</p> <p>3. Prof. dr Siniša Fajt, redovni profesor, uža naučna oblast: Elektrotehnika, izabran 27.02.2018. godine, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu - član komisije.</p>
Napomena:	<p>Autor doktorske disertacije potpisao je sledeće izjave:</p> <ol style="list-style-type: none">1. Izjava o autorstvu,2. Izjava o istovetnosti štampane i elektronske verzije doktorskog rada i3. Izjava o korišćenju. <p>Ove izjave se čuvaju na fakultetu u štampanom i elektronskom obliku.</p>
UDK	004.738:339]::005 33:004.738

UNIVERSITY BUSINESS ACADEMY IN NOVI SAD
FACULTY OF ECONOMICS AND ENGINEERING MANAGEMENT
IN NOVI SAD

KEY WORD DOCUMENTATION

Document type:	Doctoral Dissertation
Author:	MsC Petar Čelik
Menthor (title, first name, last name, position, institution)	Dragan Soleša, Ph.D., Full Professor at the Faculty of Economics and Engineering Management in Novi Sad, University Business Academy in Novi Sad, scientific area: Quantitative Methods and Information Systems
Title:	Digital Transformation of Business and its Safeness Implications
Language of text (script):	Serbian language (latin)
Physical description:	Number of: Pages <u>339</u> Chapters VIII References <u>244</u> Tables <u>11</u> Illustrations <u>17</u> Graphs <u>17</u>
Scientific field:	Quantitative Methods and Information Systems
Subject, Key words:	Digital transformation of business, Digital economy, Disruptive innovations, Digitization

Abstract (or resume) in the language of the text:	More recently, under the pressure of accelerated, widely dispersed and diversified digital innovations as generators of overall social and economic development, two recent phenomena of processes: Digital Transformation of Business and Cyber Security cause great interest, not only in business and political circles, but also within the scientific and research sector. Regardless of the fact that they came from different sources, their common time context clearly implies that these processes are mutually conditioned, that each other is intermingled and that their challenges act coincidentally and have a convergent meaning. According to the problem and its development, these challenges are very similar, as well as in their discursive formations. Although they come from different and sometimes very similar and boundary disciplinary areas - one in the field of informatics, and the other in the security spheres - they have in the thematic sense a fractured reference frame and most often point to the need for synergetic action that establishes its resultant in the domain of economy. Based on the visualization of fully measurable performance and algorithms, digital technology has dramatically changed in recent years and continues to accelerate the pace of redesigning business, education, entertainment, the public sector, and other social segments. Configuration and scope of changes, along with inevitable disruption, take place at three levels: individual, organizational and social.
Defended: (The faculty service fills later.)	
Thesis Defend Board: (title, first name, last name, position, institution)	1. Ph.D. Dragan Soleša, full professor at the Faculty of Economics and Engineering Management in Novi Sad, University Business Academy in Novi Sad, scientific area - Quantitative Methods and Information Systems - Mentor. 2. Ph.D. Vladimir Šimović, full professor at the Faculty of

	<p>Economics and Engineering Management in Novi Sad, University Business Academy in Novi Sad, scientific area: Quantitative Methods and Information Systems, Chairman of the Commission.</p> <p>3. Ph.D. Siniša Fajt, full professor at the Faculty of Electrical Engineering and Computing, University of Zagreb, scientific area: Electrotechnics - Member of the Commission.</p>
Note:	<p>The author of doctoral dissertation has signed the following Statements:</p> <ol style="list-style-type: none">1. Statement on the authority,2. Statement that the printed and e-version of doctoral dissertation are identical, and3. Statement on copyright licenses. <p>The paper and e-versions of Statements are held at the faculty.</p>
UDC	<p>004.738:339]::005 33:004.738</p>

APSTRAKT	14
ABSTRACT	15
SPISAK SLIKA	16
SPISAK TABELA	16
SPISAK GRAFIKONA	17
UVOD	18
1. Dispozicija teze	21
2. Opšta razmatranja	22
3. Specifična razmatranja	24
4. Rezime uvodnih razmatranja	25
Poglavlje I: Konceptualna osnova i metodološki okvir istraživanja	26
1. Problem istraživanja	26
1.1 Prethodni pristup problemu istraživanja	27
1.2 Lociranje problemskog sklopa	28
1.3 Markiranje centralnog problema	28
1.3.1 Osnovno istraživačko pitanje	29
1.4 Postavka istraživanja	29
1.4.1 Predmet istraživanja	30
1.4.2 Ciljevi istraživanja	30
1.5 Hipotetički okvir	31
1.6 Dizajn istraživanja	32
1.6.1 Nacrt istraživanja	33
1.6.2 Metode istraživanja	33
1.7 Značaj, opravdanost i relevantnost istraživanja	33
Poglavlje II: Konfiguracija digitalnih tehnologija i trendovi razvoja	35
1. Obeležja i dometi tehnološke revolucije	35
1.1 Razvoj i mogućnosti primene novih tehnologija	40
2. Disruptivne tehnologije	42
2.1 Bazične digitalne tehnologije i njihov kontekst	46
2.1.1 Prvi talas disruptivnih tehnologija	48
2.1.2 Big Data	48
2.1.3 Internet stvari	50
2.1.4 Mobilna telefonija	54

2.1.5 Društvene mreže	57
2.1.6 Računarstvo u oblaku (Cloud tehnologija)	62
2.2 Drugi talas	66
2.2.1. 3D printeri	67
2.2.2. Robotika	70
2.2.3. Dronovi	75
2.2.4. Nosive tehnologije	78
2.2.5. Veštačka inteligencija	80
3. Kvantne tehnologije	82
4. Značaj, uloga i primena Industrije 4.0	86
4.1 Suština i karakteristike Industrije 4.0.....	93
5. Obuhvat i područja primene interneta pametnih stvari.....	95
5.1 Pametni gradovi	99
5.2 Pametne mašine i uređaji	102
5.3 Uticaj na poslovanje	107
5.4 Horizontalna i vertikalna integracija.....	108
6. Napredni i inovativni proizvodni procesi	109
6.1 Pametne fabrike	110
6.2 Pametne kuće	112
7. Ključni digitalni trendovi.....	113
Poglavlje III: Teorijske paradigme, koncepti i modeli digitalne ekonomije	118
1. Pojam i sadržaj digitalne ekonomije	118
2. Razvoj i komponente digitalne ekonomije	121
3. Izazovi digitalne ekonomije i temeljni principi	125
4. Najznačajniji pravci kretanja digitalne ekonomije u bliskoj budućnosti.....	127
4.1 Fiksni 5G i 5G mobile.....	127
4.2 Chatbots tehnologija	129
4.3 Povezani oblaci (javni, privatni i hibridni)	132
4.4 Blockchain koji se konačno razume	133
4.5 Data to Analytics – Machine Learning to Artificial Intelligence (AI) - Analitika podataka, mašinsko učenje i veštačka inteligencija.....	133
4.6 GDPR (General Data Protection Regulation)	134
4.7 Zakon o zaštiti privatnosti potrošača u Kaliforniji (Carnifornia Consumer Privacy Act)	136
4.8 Zakon o Internetu stvari u Kaliforniji (Internet of Things Law)	144

4.9 Kina i Internet stvari	146
5. Digitalna ekonomija u Srbiji, prilike i ograničenja.....	150
Poglavlje IV: Digitalizacija poslovanja	157
1. Terminološko i semantičko određenje digitalne transformacije.....	157
2. Digitalne mogućnosti, dometi i ograničenja	160
3. Promene koje generiše digitalna transformacija.....	160
3.1 Novi model strateškog upravljanja	162
3.2 Promena poslovanja kompanija/preduzeća i kreiranje novih ekonomskih modela.....	163
3.2.1 Ekonomija deljenja	164
3.2.2 Ekonomija saradnje.....	164
3.2.3 Zelena ekonomija.....	165
3.2.4 Cirkularna ekonomija.....	165
3.2.5 Bihevioralna ekonomija.....	166
3.2.6 Ekonomija utemeljena na znanju.....	166
3.3 Poboljšanje korisničkog iskustva.....	167
4. Savremeni sistemi upravljanja odnosima sa kupcima (CRM).....	170
5. Prednosti i vrednosti koje stvara digitalno poslovanje	178
6. Uticaj digitalizacije na ekonomske efekte - rast produktivnosti i tržište rada i zapošljavanje	179
Poglavlje V: Strateško povezivanje poslovanja i informaciono-digitalnih tehnologija.....	190
1. Sinergija informacionih tehnologija i poslovanja.....	192
1.1 Prednosti i očekivanja.....	193
2. Uticaj informacionih sistema na proizvodnu efikasnost poslovanja.....	194
3. Informacioni sistemi kao generator inovativnosti u poslovanju	195
4. Strategija primene digitalnih tehnologija u poslovanju	204
4.1 Faze izrade strateškog plana primene digitalnih tehnologija.....	206
4.2 Tehnologija izrade strateškog plana.....	209
5. Oblikovanje digitalnog poslovnog modela	210
6. Analitički kontekst funkcionisanja informacione infrastrukture postojećeg poslovnog modela.....	213
6.1 Ciljevi i smernice primene digitalnih tehnologija.....	214
7. Razrada strategije, sistem etabliranja i pozicioniranje uloge digitalnih tehnologija u poslovanju.....	215
7.1 Podrška poslovanju.....	222
7.2 Proaktivna strategija.....	223

7.3 Predlog strateškog plana informacionog sistema kao podrške poslovnom procesu	224
Poglavlje VI: Upravljanje rizicima u digitalnom poslovanju	226
1. Pojam i sadržaj informatičkog rizika	226
2. Osnovne vrste i obeležja rizika	228
2.1. Strateški rizici	228
2.2. Rizici sprovođenja informacionih programa i projekata	230
2.3. Rizici sprovođenja poslovnih procesa	231
2.4. Infrastrukturni informatički rizici	231
3. Plan upravljanja informatičkim rizicima	234
3.1 Identifikacija i klasifikacija rizika	236
3.2 Procena težine rizika	237
3.3. Određivanje protivmera i scenariji upravljanja rizicima	241
3.4 Omeđivanje odgovornosti i provera sprovođenja kontrole.....	242
3.5. Stalni nadzor i revizija plana.....	243
4. Ranjivost informacionih sistema.....	246
5. Postupak optimizacije rizika	248
6. Savremene pretnje i modaliteti ugrožavanja digitalnog poslovanja	250
6.1 Zero-Day napadi	254
6.2 Reciklirane cyber pretnje.....	255
6.3 Napredne uporne pretnje.....	255
Poglavlje VII: Dizajniranje i kontekstura informacione bezbednosti u digitalnom poslovanju.	257
1. Određenje pojma i sadržaja informacione bezbednosti	258
2. Tri stuba bezbednosti	259
2.1 Poverljivost.....	259
2.2 Integritet.....	260
2.3 Dostupnost	260
3. Bezbednost Cloud-a.....	263
4. Strateški, institucionalni i regulatorni okvir informacione bezbednosti u Evropskoj Uniji: rešenja, iskustva i pouke	267
5.1. Evropska strategija i politika informacione bezbednosti.....	271
4.2. Evropski odgovor na slučaj cyber krize velikih razmera.....	276
4.3. CSIRT - Mreža nacionalnih timova za odgovor na sajber incidente	277
5. Koordinisani odgovor na prekogranične cyber incidente/krize	281
6. Da li je iko bezbedan?.....	283
Poglavlje VIII: Rezultati istraživanja.....	288

1. Prikaz rezultata istraživanja	288
2. Diskusija rezultata istraživanja	295
3. Preporuke za dalja istraživanja	301
ZAKLJUČNA RAZMATRANJA	305
Korišćena literatura:	319
Bibliografski izvori:	319
Elektronski izvori:.....	336

APSTRAKT

U novije vreme, pod pritiskom ubrzanih, široko disperzovanih i diverzifikovanih digitalnih inovacija kao generatora sveopšteg društvenog i privrednog razvoja, dve recentne pojave, procesa i fenomena: digitalna transformacija poslovanja i sajber bezbednost izazivaju veliko interesovanje i to ne samo poslovnih i političkih krugova, već i naučno-istraživačkog sektora. Nezavisno od toga što su proizašli iz različitih izvora, njihov zajednički vremenski kontekst jasno implicira stav da su ovi procesi međusobno uslovljeni, da jedan drugi prožimaju i da njihovi izazovi deluju podudarno i da imaju konvergentan smisao. Prema problemskom i razvojnom zahvatu, ti izazovi su veoma slični, kao i po svojim diskurzivnim formacijama. Mada nastupaju iz različitih, a ponekad i veoma sličnih i graničnih disciplinarnih područja - jedan iz oblasti informatičkih, a drugi iz bezbednosnih sfera - oni u tematskom smislu imaju izukrštan referentni okvir i najčešće upućuju na potrebu sinergetskog delovanja koji svoju rezultatnu uspostavlja u domenu ekonomije. Na osnovu vizuelizacije potpuno merljivih performansi i algoritama, digitalna tehnologija je poslednjih godina dramatično promenila i nastavlja ubrzanom tempom da redizajnira način poslovanja, obrazovanja, zabave, javnog sektora, kao i drugih društvenih segmenata. Konfiguracija i obim promena, uz neizbežnu disrupciju odvijaju se na tri nivoa: individualnom, organizacionom i društvenom nivou.

Ključne reči: digitalna transformacija poslovanja, digitalna ekonomija, disruptivne inovacije, digitalizacija, sajber bezbednost

ABSTRACT

More recently, under the pressure of accelerated, widely dispersed and diversified digital innovations as generators of overall social and economic development, two recent phenomena of processes: Digital Transformation of Business and Cyber Security cause great interest, not only in business and political circles, but also within the scientific and research sector. Regardless of the fact that they came from different sources, their common time context clearly implies that these processes are mutually conditioned, that each other is intermingled and that their challenges act coincidentally and have a convergent meaning. According to the problem and its development, these challenges are very similar, as well as in their discursive formations. Although they come from different and sometimes very similar and boundary disciplinary areas - one in the field of informatics, and the other in the security spheres - they have in the thematic sense a fractured reference frame and most often point to the need for synergetic action that establishes its resultant in the domain of economy. Based on the visualization of fully measurable performance and algorithms, digital technology has dramatically changed in recent years and continues to accelerate the pace of redesigning business, education, entertainment, the public sector, and other social segments. Configuration and scope of changes, along with inevitable disruption, take place at three levels: individual, organizational and social level.

Key words: digital transformation of business, digital economy, disruptive innovations, digitization, cyber security

SPISAK SLIKA

Slika br. 1 DSI infrastruktura

Slika br. 2 Uticaj disruptivnih tehnologija na društvo, poslovanje i ekonomije

Slika br. 3 Prikaz razlika između binarnog i kvantnog računara

Slika br. 4 Prikaz Industrije 4.0

Slika br. 5 Industrija 4.0

Slika br. 6 Četiri osnovne karakteristike Industrije 4.0

Slika br. 7 Generička arhitektura IoT rešenja

Slika br. 8 Primena IoT

Slika br. 9 Agentski sistemi

Slika br. 10 Pametne kuće

Slika br. 11 Gartnerov „Hype“ ciklus za nove tehnologije, 2016

Slika br. 12 Indeks digitalne transformacije

Slika br. 13 Prikaz Omnichannel koncepta

Slika br. 14 Model CRM – 360° View

Slika br. 15 Koraci i faze postupka dizajniranja i primene strategije digitalne poslovne transformacije

Slika br. 16 Faze i Koraci u upravljanju informatičkim rizicima

Slika br. 17 Raspberry Pi - Single board computer

SPISAK TABELA

Tabela br. 1 Poslovi u digitalnoj ekonomiji

Tabela br. 2 Biznis model Canvas - metoda za analizu biznis modela

Tabela br. 3 Izvođenje informatičke strategije iz strategije poslovanja

Tabela br. 4 Delovi poslovnog plana određuju delove strateškog plana informatike

Tabela br. 5 Defanzivna i ofanzivna strategija

Tabela br. 6 Primer procene nivoa informacionih rizika i utvrđivanja strategije odgovora na rizike

Tabela br. 7 Podela informatičkih kontrola

Tabela br. 8 Hipotetički primer pregleda rezultata plana upravljanja informacionim rizicima

Tabela br. 9 Primeri informatičkih incidenata

Tabela br. 10 5 najvećih rizika za mala preduzeća sa trendovima razvoja

Tabela br. 11 Uzroci prekida poslovanja koji najčešće izazivaju strah kod kompanija

SPISAK GRAFIKONA

- Grafikon br. 1 Rast kapitalnih investicija u duboke tehnologije u Evropi
- Grafikon br. 2 Najpopularnije društvene mreže u svetu na dan 18.07.2019. godine prema broju aktivnih korisnika (u milionima)
- Grafikon br. 3 Rast AM industrije na globalnom planu
- Grafikon br. 4 Rast AM industrije i proizvodnje po zemljama u svetu
- Grafikon br. 5 Procenjena godišnja ponuda industrijskih robota
- Grafikon br. 6 Broj industrijskih robota na 10.000 zaposlenih u proizvodnji u 2017.godini
- Grafikon br. 7 Procenjene investicije u proizvodnju hardvera za dronove
- Grafikon br. 8 Norme za pametne gradove
- Grafikon br. 9 Prodaja pametnih uređaja po tržištima u 2016.godini
- Grafikon br. 10 Rast Internet povezanih uređaja do 2020. godine
- Grafikon br. 11 Tehnološka mapa: Internet stvari
- Grafikon br. 12 Disruptivne tehnologije i njihov procenjeni potencijalni uticaj u 2025. godini, u trilionima dolara, godišnje
- Grafikon br. 13 DESI 2018- Indeks digitalne ekonomije po zemljama
- Grafikon br. 14 DESI kategorije
- Grafikon br. 15 Indeks DESI za Srbiju 2017.
- Grafikon br. 16 Prikaz stepena mrežne spremnosti i ostalih pokazatelja Srbije
- Grafikon br. 17 Udeo radnika pod visokim rizikom od automatizacije u OECD zemljama (%)

UVOD

Kako bi istraživačka ideja i konceptualni okvir istraživanja koji je postavljen u ovom radu dobili svoje ključne odrednice, tj. svoje fundamentalne elemente, u cilju razrade teme kroz istraživački proces, bilo je neophodno definisati bitne istraživačke segmente metodološkog okvira, analizirati dosadašnja istraživanja, postojeće stavove i objavljene rezultate, kako bi se na toj osnovi uspostavio skladan odnos između definisanog problema, predmetnog okvira, ciljeva i postavljenih hipoteza istraživanja.

Budući da naznačeni problemsko-predmetni kompleks pripada onima koji su do sada sporadično i po obimu nedovoljno istraživački opservirani, odnosno "neadekvatno definisani" zapravo "meki", moguće su veće nedorečenosti. Da bi se ova nepoželjna pratilja istraživanja minimizirala, najpre će se dati širi kontekstualni prikaz, tj. konceptualizacija istraživanja (izbor i markiranje problemskog sklopa, lociranje centralnog problema, definisanje i dimenzionisanje predmetno-istraživačkog okvira, određivanje dispozicije ciljeva istraživanja, oblikovanje hipoteza, izrada idejnog nacrt, itd.), kao i operacionalizacija koja uključuje: izbor i izradu dizajna i nacrt istraživanja, izbor i razradu metoda i tehnika istraživanja i na kraju plan obrade rezultata istraživanja.

Definisanje svih metodoloških elemenata, omogućiće elaboriranje i razumevanje suštine i namere osnovne istraživačke ideje. Ovim delom rada objasniće se svi elementi istraživačkog konceptualnog okvira, kao i odnosi i veze pojedinih delova i podcelina. Takođe, na ovom mestu se nastoji staviti naglasak i akcenat na ulogu i značaj svakog elementa naučne zamisli, što doprinosi boljem razumevanju osnovne problemske orijentacije i istraživačke namere ovog rada.

Sveobuhvatna digitalna transformacija ne predstavlja samo primenu novih tehnologija u poslovanju i radu kompanija, već znači i uvođenje novih digitalnih modela poslovanja, te i značajne promene u načinu povezivanja preduzeća sa kupcima i dobavljačima, što podrazumeva kreiranje novog lanca i sistema vrednosti, kao i niza promena u oblasti marketinga, menadžmenta, zapošljavanja, pristupa tržištu i njihovim interakcijama, uključujući tu i promenu interpersonalnih odnosa unutar svake kompanije.

Osim toga, digitalna transformacija, stimulišući promene u očekivanjima krajnjih korisnika dobara, istovremeno stvara potpuno nova korisnička i poslovna iskustva, čime se kompanije

usmeravaju na personalizaciju proizvoda i usluga u skladu sa preferencijama i zahtevima korisnika.

Stepen digitalizacije u savremenom poslovnom okruženju najčešće se procenjuje praćenjem sledećih parametara (D'Souza&Williams, 2017:80-86).

Prisutnost – u kojoj meri preduzeća i potrošači ostvaruju raznovrsni pristup digitalnim aplikacijama i uslugama (Stojanović, 2017:86);

Pristupačnost – do kog nivoa digitalne usluge cenovno optiraju u domenu koji omogućava da što veći broj ljudi može da ih koristi;

Pouzdanost – kvalitet digitalnih dostupnih servisa;

Brzina – u kojoj meri se može pristupiti digitalnim uslugama u realnom vremenu;

Upotrebljivost – lakoća korišćenja digitalnih usluga i sposobnost povećanja lokalnih usvajanja ovih usluga;

Veština – sposobnost korisnika da digitalne usluge ugrade u privatne i poslovne prilike.

Ako se akceptira prethodni stav, proizilazi da su promene u poslovanju, a u širem smislu i u društvu, zapravo konstante koje neprekidno ispoljavaju uticaj, kako na ekonomske, tako i na opšte društvene procese. Pri tome, posebno treba naglasiti, da brzina kojom se menja korisničko ponašanje, znanje i iskustvo, kao i brzina evoluiranja njihovih očekivanja, stoji u direktnoj zavisnosti od brzine razvoja i uvođenja disruptivnih tehnologija.

Savremena globalna ekonomija sve je više pogođena digitalizacijom. Digitalne tehnologije transformišu sve ekonomske sektore, od infrastrukture do poljoprivrede i već su imale ogroman uticaj na tradicionalne industrije poput proizvodnje i transporta. Budući rast ekonomije SAD zavisi od uspeha njene digitalne ekonomije (Burwell, 2018).

Primenjujući prvi talas disruptivnih tehnologija: računarstvo u oblaku, mobilne tehnologije, big data, društvene mreže i internet stvari, većina kompanija iz svih industrija koje su među prvima zakoračile u svet digitalnih tredova, nastoje da među prvima iskoriste i sve prednosti i mogućnosti novih i naprednih tehnološki rešenja kao što su: roboti, dronovi, veštačka inteligencija, 3D print, skladištenje energije, kompjuterske simulacije, nove materijale i nano-tehnologije koje velikom dolaze brzinom pod uticajem „Četvrte industrijske revolucije“, tj. „Industrije 4.0“.

Analizirajući dosadašnji razvoj, dinamiku i tendencije razvoja disruptivnih tehnologija i inovacija, pojedini autori (kao npr. Varian, 2016) jasno trasiraju pravce i označavaju smerove u kojima će digitalno ekonomsko okruženje ostvariti uticaj na razvoj i fizionomiju poslovnih aktivnosti, kao npr:

Prikupljanje i analiza podataka – Kompanije bi o klijentima trebalo da prikupe veliki broj informacija, najpre onih putem kojih bi mogle predvideti njihovo ponašanje, sve u cilju unapređenja usluga koje im se pružaju;

Personalizacija i prilagođavanje – Kompanije bi trebalo da obezbede prilagođene proizvode i usluge, jer klijenti u savremenom svetu očekuju potpunu posvećenost koja obuhvata relevantne informacije o prethodnim kupovnim navikama klijenata, načinima na koje vrše plaćanja, njihovoj adresi i ostalim detaljima od značaja;

Eksperimentisanje i stalni progres – Kompanije će dostići nivo da mogu koristiti i analizirati ogromne količine podataka i da uz pomoć specijalno strukturisanih algoritama za usluge predikcije i posredstvom potpuno automatizovanih sistema donose važne odluke i za proizvodnju i za realociranje resursa;

Inovacije i ugovaranje – Kompanije i njihovi klijenti biće u mogućnosti da prate, nadgledaju i utvrđuju identitet onih kojima posluju. Ovo će učiniti lakšim nove vrste transakcija u ekonomiji (na primer plaćanje elektronskim novcem);

Koordinacija i komunikacija – Komunikaciona sredstva (kao što su aplikacije za razmenu dokumenata, videokonferencijski sistemi, bežični mobilni uređaji i dr.), omogućiće ljudima interakciju povećane fleksibilnosti, nevezano od toga gde se oni nalaze. Kompanije će usled toga biti u prilici da mnogo lakše učestvuju na svetskom tržištu sa ponudom svojih proizvoda i usluga.

Rezimirajući navedeno, jasno je da digitalna transformacija u današnje vreme više nije pitanje izbora, već imperativ postojanja, opstanka i pozicioniranja kompanija i javnih servisa na jednom izuzetno konkurentnom i turbulentnom tržištu, koje samim tim više nije geografski određeno, već se praktično neograničeno prostire u sajber prostoru i po njegovoj širini i dubini.

1. Dispozicija teze

Aktuelne pretnje i rizici u oblasti digitalnog poslovanja iziskuju redefinisane postojećih strateških agendi i redizajniranje operativnih mehanizama zaštite, kako u sferi digitalne ekonomije, tako i u sferi države.

Sistematika i kompozicija doktorske disertacije u celosti je upodobljena metodološkom zahtevu da se u istraživačkom smislu obuhvati kompletna, iako izuzetno složena i dispergovana predmetno-problemska tematika vezana za nastanak, razvoj i funkcionisanje digitalne ekonomije u savremenom poslovnom okruženju i sa aspekta bezbednosti. To je, u prvom redu odredilo i postupak strukturisanja predmetnog sadržaja disertacije, tako da ona sadrži sve relevantne tematske celine, odnosno blokove povezane sa naslovljenom temom.

U uvodnom delu i prvom poglavlju, dat je bliži prikaz lajtmotiva, izraženih potreba i teorijsko-praktičnih razloga za bliže opserviranje navedene teme s obzirom na njenu relevantnost, opravdanost i aktuelnost u postojećem poslovnom ambijentu. Takođe, prezentovani su metodološki okvir i konceptualne osnove koje detaljnije razrađuje problemski sklop, i u okviru toga centralni problem istraživanja. Istovremeno, dato je dimenzionisanje predmeta istraživanja, koordinate, dispozicija ciljeva, sistem hipoteza, kao i dizajn istraživanja sa metodološkim instrumentarijem, sa primenjenim metodama i tehnikama i na kraju ostvarenim i očekivanim rezultatima istraživanja.

U drugom poglavlju data je i razmotrena konfiguracija digitalnih tehnologija i trendova njihovog razvoja, kroz obeležja i domete tehnološke revolucije i inovativne poslovno-proizvodne procese.

U trećem poglavlju, istraživački fokus je usmeren na teorijske paradigme, koncepte i modele digitalne ekonomije, njene izazove i najznačajnije pravce kretanja, kako na globalnom novou, tako i u R. Srbiji.

Četvrto poglavlje, razmatra digitalizaciju poslovanja, promene generisane digitalizacijom poslovnog modela, sisteme za upravljanje odnosima sa kupcima, uticaj digitalizacije na ekonomske efekte kroz rast produktivnosti i disrupciju na polju rada i zapošljavanja.

U petom poglavlju, razrađene su relevantne podteme vezane za strateško povezivanje poslovanja i informaciono-digitalne tehnologije, koje između ostalog uključuju analitički kontekst

funkcionisanja informacione infrastrukture u poslovnim modelima, pojam informacionih sistema u kompaniji ili preduzeću i najzad učinjen je pokušaj razrade strategije poslovanja u uslovima masovne primene informacionih tehnologija.

U šestom poglavlju, prikazane su vrste i obeležja informatičkih rizika, njihova klasifikacija i procena rizika, zatim, ranjivost informacionih sistema i postupak optimizacije rizika.

U sedmom poglavlju, razrađen je postupak dizajniranja informacione bezbednosti u digitalnom poslovanju, sa prikazom evropskog i američkog regulatornog okvira i opsega, kao integralnog odgovora na sajber incidente i krize velikih razmera. U nastavku poglavlja, sa osloncem na noviju evropsku i američki pravnu regulativu, prikazani su mehanizmi za upravljanje sajber krizama koji predstavljaju referentni okvir i standard, ne samo za SAD, već i države članice EU, a samim tim i za države koje se nalaze u procesu pridruživanja EU, kao što je Republika Srbija.

U osmom poglavlju, dati su rezultati istraživanja, kao i diskusija o rezultatima istraživanja i date su opširne preporuke za dalja istraživanja.

Zaključna razmatranja objedinjuju istraživačke rezultate, analitičke predloge i druge istraživačke doprinose i rezultate do kojih se došlo tokom istraživanja. Formulirane su i smernice za prevazilaženje postojećih prepreka i ograničenja kada je reč o uvođenju i operacionalizaciji koncepta i modela digitalne ekonomije, uključujući i bezbednosni aspekt.

2. Opšta razmatranja

Digitalna transformacija je, svojim neposrednim uticajem na svest, ideje, ponašanje i promenu paradigme, fokusa i načina poslovanja, nesumnjivo dovela do stvaranja i ekspanzije digitalne ekonomije, kao potpuno novog i do tada nepoznatog modela tržišnog poslovanja.

Paralelno sa razvojem ovih poslovnih modela i novih načina privređivanja, disruptivne tehnologije su u kompleksnom globalnom okruženju postale veliki izazov i svojevrsna pretnja i samom modelu digitalnog poslovanja, zbog neograničenih mogućnosti zloupotrebe tehnologija i njihovih slabih strana i tako nastalog disbalansa između veoma brzog razvoja tehnoloških inovacija i njihove implementacije, sa jedne, i pratećih mehanizama zaštite i bezbednosnih izazova, sa druge strane (Čelik, P. 2019:61-68).

Navedeni nesklad, u korelaciji sa gubitkom značaja geografskog prostornog integriteta, otvorio je prostor za brojne forme i modalitete ugrožavanja razvojnih potencijala i mogućnosti koje

pružaju digitalne tehnologije, usled manjih mogućnosti iznalaženja adekvatnih operativnih i proaktivnih odgovora na širok spektar stalno inovirajućih pretnji, upravo jer bezbednosni odgovori prema svim dosadašnjim iskustvima nastaju sa objektivno uslovljenim vremenskim zakašnjenjem.

Kako bi unapredili poslovne procese, autor (Page, 2016) ističe deset koraka koje treba preduzeti u cilju poboljšanja efektivnosti, efikasnosti i prilagodljivosti. Prvi korak je identifikovanje organizacionih procesa odlučnih za obavljanje poslovnih aktivnosti i definisanje prioriteta, dok poslednji korak predstavlja obavezu da se sa procesom nikada ne prekida, što se u potpunosti poklapa sa savremenim principom menadžmenta da su promene konstanta koja stalno zahteva adekvatan i pravovremen odgovor u sistemu upravljanja. Navedeni stav u potpunosti potvrđuje rezultate novijih istraživanja koja sugerišu da je ljudski faktor u najvećoj meri presudan u menadžmentu poslovnih procesa, uprkos nespornoj činjenici da nikada ranije nismo imali u aktuelnom vremenskom okviru na raspolaganju toliku količinu znanja i informacija i ujedno tehnoloških rešenja zasnovanih na inteligentnim, tj. pametnim digitalnim tehnologijama (Wong, Tseng&Tan, 2014).

U referentnoj domaćoj i stranoj literaturi dominira stav, da u situaciji aktuelne proliferacije različitih digitalnih inovacija i disruptivnih tehnologija, nedostaje sistemski pristup, posebno sa aspekta zaštite digitalne ekonomije i prateće infrastrukture, kako na institucionalnom, tako i na funkcionalnom planu. U skladu sa tim, gotovo sve zemlje zapada, bez izuzetka, učinile su značajne korake na iskorišćavanju svih prednosti koje pružaju digitalne tehnologije, uz razvijanje pratećih bezbednosnih agendi, razvijanja bezbednosnih procedura, obrazovanje specijalizovanih timova i agencija za reagovanje u slučaju sajber kriza i incidenata, kao i uspostavljanja prekograničnih i nadnacionanih mehanizama koordinacije, podrške i zajedničkog nastupa.

Jedna od ključnih karakteristika poslovnih modela u digitalnoj ekonomiji jeste stalna integracija, odnosno prožimanje ili istovremena promena svih, primarnih i sekundarnih, međusobno nezavisno razvijanih, digitalnih tehnologija, kojima je moguće stvoriti inovativne, do tada nepostojeće usluge, proizvode, tržišta i modele poslovanja.

Novo poslovno okruženje, koga karakterišu zasebni ili simultani procesi inoviranja i promena na svim razvojnim poljima, počev od proizvodnje, organizacije rada, upravljanja, marketing miksa, uključujući i neizostavnu procenu rizika i ranjivosti digitalnih poslovnih modela i korisničkog

lanca stvorene vrednosti, omogućava digitalnim tehnologijama, podržanim od strane disruptivnih inovacija, da se etabliraju kao najznačajniji pokretači razvoja, rasta, konkurentnosti i prestiža, za preduzeća svih veličina i delatnosti.

Međutim, uspostavljanje i razvoj digitalne ekonomije zasnovane na primeni savremenih i sofisticiranih digitalnih tehnologija i rešenja, zbog otvorenog ili prikrivenog delovanja brojnih turbulentnih činilaca i dejstvujućih faktora, strateških vektora i varijabli, postaje sve kompleksnije, sveobuhvatnije i složenije, a samim tim i neizvesnije i teže predvidivo. U vezi sa tim, otvara se i pitanje rizika i bezbednosti u svim fazama i segmentima delovanja digitalne ekonomije.

3. Specifična razmatranja

Sajber rizici su posebna vrsta informatičkih rizika, koji su u vezi sa intenzivnom primenom digitalnih tehnologija u poslovanju. Po svojoj suštini, ili bolje reći konteksturi, ti rizici imaju dvostruki karakter. Prvo, oni su neizbežni, stalno su prisutni i njihova pojava i intenzitet stvaraju probleme u poslovanju, dok bolji kvalitet upravljanja istim čuva vrednosti informatičkih investicija.

Ovim se došlo do centralnog problemskog spleta na koji je fokusiran i oko koga se organizuje ceo postupak istraživanja. U sklopu toga, ključni problem ogleda se u nepostojanju analitičke podloge, kao i opšteprihvaćenog jedinstvenog pristupa, a time i metodologija i standarda za primenu digitalnih tehnologija u poslovnom procesu, što u praksi stvara čestu konfuziju i na taj način izaziva brojne nedoumice, dileme, čak i pogrešna rešenja.

Osim toga, na prostoru Republike Srbije, zapadnog Balkana, pa i šireg okruženja, ne postoji jedinstvena baza podataka o veličini, obimu, obuhvatu, dinamici, intenzitetu digitalizacije ekonomije i celokupnog društva, koji bi omogućili potpuniji uvid u trendove razvoja, aktuelnog stanja i stepena implementirane digitalizacije u cilju strateškog planiranja i upravljanja ravnomernom digitalizacijom, kao i preveniranja i saniranja posledica ugrožavanja. Pored toga, preovlađujući korpus operativno važnih komponenti problema, lociran je u sferi traganja za efikasnim metodologijama procene rizika i izgradnje mehanizama zaštite, kako bi se predupredile i smanjile eventualne štete, gubici i zaštitio ugled kompanije i štićeni podaci.

4. Rezime uvodnih razmatranja

Kroz predmetno istraživanje se traži odgovor na pitanje: kako i na koji način uspešno transformisati preduzeća i javni sektor, kontrolisano primenjujući savremene tehnologije u cilju uspostavljanja modela digitalne ekonomije i društva, uz istovremeno razvijanje preventivnih i operativnih mehanizama zaštite.

Iz navedenog proizilazi da je definisani problem izuzetno razuđen, difuzno strukturiran, te zbog toga istraživanje i prateći analitički kontekst predstavljaju duboko zalaženje u oblast koja je izuzetno široka, duboka i bogato iznijansirana. Postojeće, a naročito implikacije koje se mogu javiti na osnovu naznačenog problema, nisu dovoljno sagledane ili specifikovane, uprkos brojnim iskustvima i novim podacima, koji kao takvi pokazuju koje i kakve štete mogu nastati po kompaniju i njene zaposlene, ukoliko primena tehnologija i razvoj digitalnih poslovnih modela ne prate odgovarajući bezbednosni aspekti i aranžmani, koji se stalno moraju usklađivati sa nastupajućim promenama.

Poglavlje I: Konceptualna osnova i metodološki okvir istraživanja

Tematika digitalne transformacije u celini, a naročito digitalne ekonomije, iako nesporno vrlo aktuelna i relevantna za dalji razvoj teorijske misli i ekonomije, nije bila kod nas u fokusu širih naučnih opservacija, a još manje teorijsko-empirijskih istraživanja, kao što je to slučaj u akademskim krugovima na zapadu, što predstavlja jedan eklatantan primer neracionalne alokacije naših naučno-istraživačkih resursa.

Nasuprot evropskim i svetskim trendovima, u našoj akademskoj zajednici - naučnoj produkciji i referentnoj literaturi se već duže vreme oseća deficitarnost produbljenih i na sistemskoj osnovi zasnovanih teorijskih i analitičkih pristupa ovoj tematici. Među malobrojnim, ali vrlo inspirativnim i naučno fundiranim radovima, posebno se ističu radovi i istraživačke studije dr Marijane Bujanje Vidas, koja se na ovim prostorima među prvima počela baviti pitanjima digitalne transformacije, odnosno digitalne ekonomije.

Ključni stav koji ovaj autor zastupa u svom radu iz 2017. godine, polazi od premise da se "Savremeno poslovno okruženje menja pod uticajem drugog talasa "uznemirujućih" digitalnih tehnologija kao što su „Cloud computing“ tj. računarstvo u oblaku, mobilne aplikacije, „Big data“ analitika, društvene mreže, Internet stvari i dr.

Posebnost navedenih digitalnih inovacija, često nazivanih „Četvrta industrijska revolucija“ ili „Industrija 4.0“ ogleda se kroz to što su one uzrok promena u celom spektru industrijskih sektora, a koje na ovaj način postaju ulaznica za održanje konkurentnosti na globalnom nivou. Ovaj rad stoga analizira uticaj i doprinos savremenih digitalnih tehnologija u rastu ekonomija i ostvarivanju višeg nivoa produktivnosti i time konkurentnosti preduzeća uz prateće bezbednosne implikacije.

1. Problem istraživanja

Da bi dostigla potrebni nivo konkurentnosti, savremena preduzeća moraju otpočeti sa procesom digitalne poslovne transformacije, tj. transformacijom koja zahteva nove načine komuniciranja sa partnerskim preduzećima, nove modele saradnje sa kupcima i potrošačima, redizajn poslovnih procesa i uspostavljanje sasvim novih organizacionih modela.

Sudeći po stavovima pojedinih autora, proces digitalne transformacije predstavlja jednu od najsveobuhvatnijih transformacija poslovnog okruženja koja se odigrala u poslednjih sto godina,

usled čega njegovi potencijali koji mogu biti iskorišćeni u okviru novih digitalnih inovacija, predstavljaju značajan izazov za sve industrijske grane, ali i nacionalne ekonomije. Iskustva EU u razvoju digitalnog preduzetništva, kao i izazovi digitalnih promena kod domaćih preduzeća, takođe su predmet analize (Vidas-Bubanja, M. 2017).

Približno sličan stav po pitanju neophodnosti i urgentne potrebe razvoja digitalne ekonomije na prostoru Republike Srbije, imaju i drugi ekonomisti: dr Trninić J., dr Đurković, J. sa Ekonomskog fakulteta u Subotici, dr Jasna Soldić-Aleksić sa Ekonomskog fakulteta u Beogradu, Svetlana Sokolov-Mladenović sa Ekonomskog fakulteta u Nišu, a u bližem okruženju, i dr Branko Krsmanović, Fakultet poslovne ekonomije Bijeljina i dr Mario Spremić, sa Ekonomskog fakulteta, Sveučilišta u Zagrebu.

1.1 Prethodni pristup problemu istraživanja

Temeljna postavka koju dr Mario Spremić kao autor kroz svoje radove obrazlaže, polazi od toga da: "Okruženje digitalne ekonomije donosi vizionarske i inspirativne scenarije primene digitalnih tehnologija kojima će se svi poslovni subjekti morati prilagoditi. Digitalna transformacija i opsežna digitalizacija poslovanja sigurno će biti važne strateške aktivnosti kojima će poslovni subjekti pokušati osnažiti svoju konkurentsku poziciju. Povodi za razmišljanja o poslovnom okruženju digitalne ekonomije u kojoj živimo i radimo, ukazuju na činjenicu da nam tek predstoji izuzetno intenzivno i sveobuhvatno korišćenje potpuno novih - digitalnih tehnologija koje će kao takve (zauvek) promeniti naše životne i poslovne navike, ali nas izložiti i brojnim novim rizicima - sajber rizicima".

U stranoj, najpre zapadnoj literaturi, a prevashodno etabliranim publikacijama iz ove oblasti, zbog svoje sveobuhvatnosti, interdisciplinarnog, sistematskog i holističkog pristupa, posebno treba izdvojiti radove kanadskih naučnika Chris-a D'Souza-e i David-a Williams-a, koji ističu: "Digitalizacija bi mogla imati širok opseg efekata u ekonomiji. Sve više poslovnih zadataka koje trenutno obavljaju ljudi u bliskoj budućnosti biće izvršavani elektronski. Prednosti digitalizacije verovatno će biti najveće među preduzećima sa visokim nivoom organizacionog potencijala i ljudskog kapitala koji intenzivno koriste znanje.

Da bi uspešno upravljali tranzicijom ka digitalizaciji, kreatori politike bi trebalo da osiguraju da ekonomija bude prilagodljiva; da su firme podstaknute tržištem agilne; da je ekonomska dobit

široko rasprostranjena; da različiti obrazovni, pripravnički, imigracioni i programi osiguranja zapošljavanja zajedno dobro funkcionišu sa obavezama poslodavaca za obuku na poslu.

1.2 Lociranje problemskog sklopa

Američki ekspert Hal Varian, glavni ekonomista u kompaniji Gugl, zastupa tezu da "Digitalne aplikacije dominantno utiču na sve aspekte svakodnevnog života i rada, a uticaj na ekonomiju treba da pomogne da se živi pametnije i bolje", dok na drugoj strani, Henning Kagermann, Hubert Osterle i John M. Jordan kao grupa autora, u svojoj istraživačkoj studiji naglašavaju da se "optimizacija procesa proizvodnje, pružanja usluga i uopšte poslovanja odvija pod snažnim pritiskom digitalnih tehnologija i inovacija, radi čega tržišni uslovi sve više omogućavaju zadovoljavanje širokog spektra potreba različitih korisnika."

Suštinu digitalne transformacije, prednosti i nedostatke uvođenja tehnologije i inovacija u poslovne procese, kao i buduće trendove razvoja, najsazetije je izneo Klaus Schwab, izvršni direktor Svetskog ekonomskog foruma (WEF) i jedan od glavnih entuzijasta „Revolucije 4.0“. U svom poznatom delu "Četvrta industrijska revolucija" koje je promovisano prilikom održavanja ovog foruma 2016. godine. Schwab se istakao: „Nalazimo se na početku tehnološke revolucije koja ima potencijal da iz korena promeni naš celokupni način života, način na koji obavljamo svakodnevne radne aktivnosti, kao i način koji određuje kako ćemo se odnositi jedni prema drugima. Posledice ove revolucije promeniće i način poimanja kakvi smo mi zapravo, kakav je naš interaktivni odnos prema drugim ljudima, bez razlike da li je reč i o najudaljenijim delovima sveta: revolucija će uticati na poslovno tržište, budućnost posla, nejednake prihode, dok će poslednji trzaji revolucije uticati na etičke odrednice i geopolitičku sigurnost.“ Schwab pored toga ističe da se „Revolucija 4.0 ne definiše kroz dijapazon inovativnih tehnologija, već njihovom transformacijom u nove sisteme koji su sagrađeni na infrastrukturi prethodne, digitalne revolucije“.

1.3 Markiranje centralnog problema

U smislu iznetih vladajućih stavova i shvatanja u literaturi, vezano za područje istraživanja, predmet istraživanja ovog rada je fokusiran na utvrđivanje digitalnih trendova, stanje i razvoj digitalnih tehnologija i disruptivnih inovacija, kao i uticaj tih trendova na razvoj poslovnih modela, kao i način uspostavljanja digitalne ekonomije i njenih osnovnih funkcionalnih obeležja.

Pored toga, u predmetno-tematskom pogledu, istraživanje je usmereno na identifikovanje, lociranje i fiksiranje svih realnih potencijalnih opasnosti, pretnji, hazarda i rizika koji prate proces digitalne transformacije kao celine.

Pretežno teorijski karakter predmetnog istraživanja, kompleksnost istraživačkog područja, hipotetički okvir sa postavljenim deskriptivnim, eksplikativnim i eksplorativnim ciljevima, prioritarno opredeljuju izbor i primenu adekvatnog nacrt istraživanja i komplementarnu primenu više istraživačkih metoda za prikupljanje iskustvene evidencije i njenu kontekstualnu i konceptualnu analizu.

1.3.1 Osnovno istraživačko pitanje

Precizno omeđeno problemsko područje, kao i postavljeni ciljevi istraživanja, upućuju nas na istraživačke pretpostavke definisane u formi hipoteza, koje će svoje utemeljenje naći u rezultatima dosadašnjih istraživanja iz ove oblasti, kao i u navedenim stavovima iz analizirane literature.

Pri svemu tome, važno je razmotriti i prethodna iskustva i dosadašnje metodološke pristupe u sličnim istraživanjima. Obzirom na pretežno kvalitativni i eksplorativni karakter ovog istraživanja, ono je zasnovano na jednom širokom i nespecifičnom hipotetičkom okviru koji obuhvata ispitivanje i proveravanje pretpostavljenih odnosa, različitog nivoa opštosti. Navedeno sugeriše da hipoteze realno ne mogu biti na takvom nivou metodološke oblikovanosti da neposredno usmeravaju istraživanja na indikativna i relevantna teorijska i empirijska područja na osnovu kojih bi se te tvrdnje mogle verifikovati bez posredovanja.

1.4 Postavka istraživanja

Istraživački pristup koji se koristi u ovoj disertaciji, jeste princip komplementarnosti koji zahteva različite izvore i načine prikupljanja, analizu podataka, njihovu obradu, istraživačke strategije, kao i poseban istraživački dizajn. U prvom redu, reč je o dominantno kvalitativno i primenjeno istraživačkom pristupu koji podrazumeva uobičajeni metodološki postupak induktivnog izvođenja zaključaka sa ciljem provere postavljenih hipoteza. Nedovoljna teorijska izgrađenost navedene tematike, uslovlila je pretežno eksplorativnu prirodu uspostavljenih istraživačkih zahteva, što je u istraživačkom smislu zahtevalo primenu deskriptivnog nacrt istraživanja.

Predmetna tematika, sa aspekta razvoja i primene digitalnih tehnologija i disruptivnih inovacija s jedne i bezbednosnih implikacija sa druge strane, usled povećanog rizika i ranjivosti, a naročito sve većih šteta i gubitaka koje izazivaju, jeste po svom karakteru i fizionomiji u turbulentnom okruženju, što uvek znači visok stepen nepredvidivosti i neizvesnosti i drastično redukovanu mogućnost strateškog i planskog upravljanja rizicima, iz čega proističe da je ova tematika izuzetno aktuelna, značajna i atraktivna.

Obzirom da je ova tema neretko bila direktni, a često i uzgredni predmet brojnih naučnih konferencija, kongresa, seminara, sesija i sl., uključujući tu i sam Svetski ekonomski forum koji je 2016. godine bio bezmalo u celosti posvećen ovoj temi, njenim implikacijama i izazovima, to jasno ukazuje da ova tema ima objektivnu globalnu relevantnost i široku društvenu opravdanost, budući da tretira, po opštoj oceni, jedno od najvažnijih pitanja, kako aktuelnog, tako i još više budućeg razvoja, kako ekonomije, tako i društva u celini.

1.4.1 Predmet istraživanja

U pogledu nivoa naučne spoznaje, realno je planirati ostvarenje nivoa naučne deskripcije, pri čemu se teorijski nalazi pretežno opisuju, obrađuju, analiziraju, sistematizuju i klasifikuju, saobrazno teorijskom i konceptualnom pristupu i hipotetičkoj šemi.

Za pojedina tematska područja može se postići nivo objašnjenja, odnosno nivo eksplikacije na kojem se fond dobijenih istraživačkih nalaza objašnjava u odnosu na ostvarena ili započeta kretanja ili procese u ovoj oblasti i oblasti digitalizacije, kako na prostorima EU, SAD, NR Kine, tako i tranzicionih zemalja u koje spada i Republika Srbija.

U tom smislu, sagledavanje će biti usmereno i na registrovane trendove, posebno u domenu ugrožavanja i bezbednosti.

1.4.2 Ciljevi istraživanja

Kompleksnost predmetnog područja, kao i definisani problem istraživanja, direktno određuju i dispoziciju ciljeva. Shodno tome, ciljevi istraživanja ove teme su:

- utvrđivanje smera i intenziteta uticaja digitalnih tehnologija na razvoj poslovnih modela, ali i na organizacione i poslovne performanse unutar kompanije;
- sagledavanje novog načina poslovanja baziranog na znanju i inovacijama;

- razumevanje transformacije ključnih poslovnih procesa;
- utvrđivanje stepena međusobne zavisnosti i povezanosti digitalnih tehnologija i poslovnih modela;
- ukazivanje na neiskorišćene potencijale i resurse, ali i trendove u razvoju i primeni digitalnih tehnologija, posebno u domenu digitalne ekonomije;
- markiranje faktora i elemenata koji doprinose povećanju poslovne agilnosti;
- sagledavanje mogućnosti i pravaca korisničkog iskustva, i
- izvršavanje klasifikacije i sistematizacije primarnih rizika, pretnji i opasnosti u digitalnoj ekonomiji.

1.5 Hipotetički okvir

Istraživanje se usmerava na sistem hipoteza koji uključuje dva nivoa: opšte i posebne hipoteze. Uzimajući u obzir sve napred navedeno, glavna hipoteza glasi:

U složenoj konfiguraciji prilagođavanja neprestanim i silno izdiferenciranim promenama koje dolaze iz spoljnog okruženja, kompanije/preduzeća, kako bi opstale u savremenom poslovnom i tržišnom okruženju, primenjuju savremene disruptivne inovacije i tehnologije u cilju povećanja rasta, produktivnosti, konkurentnosti i svog ukupnog tržišnog održanja i pozicioniranja.

Digitalne tehnologije, a pre svega internet stvari, „cloud“ tehnologija, robotika, 3D printing, kvantna informatika i sl., u potpunosti menjaju način poslovanja, poslovne modele i način upravljanja, pristup tržištu, odnose sa kupcima i dobavljačima, sistem unutrašnjih odnosa u kompaniji po vertikali i horizontali, sistem poslovnih komunikacija i umrežavanja, budući da imaju transformativnu moć, stvaraju ambijent i polazište za razvoj i integraciju kompanija u tokove digitalne ekonomije koji otvaraju prostor za poboljšanje poslovne efikasnosti, uz paralelno smanjenje troškova poslovanja i maksimiziranje racionalnosti korišćenja dostupnih resursa.

Navedene prednosti i gledišta koje pruža aktuelna proliferacija digitalne transformacije, sa sobom nose i ogromne rizike i pretnje. Postojeća iskustva prikazuju da kompanije, bez obzira na svoju pripremljenost i predostrožnost, nisu u stanju da prate brzinu razvoja inovativnih

tehnologija bez upuštanja u rizik, dok države ne uspevaju da tekuće tehnološke promene i inovacije adekvatno i pravovremeno regulišu (Čelik, P. 2019:61-81).

Posebne hipoteze:

Efikasno upravljanje novim poslovnim modelima i na tim osnovama izgrađenog lanca vrednosti, baziranih na digitalnim tehnologijama i disruptivnim inovacijama, u značajnoj meri povećavaju performanse, konkurentnost i razvojne kapacitete kompanije.

Digitalna tehnologija u uslovima razvoja digitalne ekonomije značajno skraćuje vreme od poslovne ideje do finalne realizacije proizvoda ili usluge, smanjuje troškove proizvodnje uz istovremeno povećanje zadovoljstva potrošača tih proizvoda i usluga.

Rastuća primena i zavisnost kompanija od savremenih tehnologija, povećava njihovu ranjivost i izloženost savremenim, digitalnim pretnjama i rizicima.

1.6 Dizajn istraživanja

Kada se posmatra kao deo istraživačkog projekta, način istraživanja se najčešće tretira kao naučni dokument ili istraživačko-operativni plan koga čini niz međusobno povezanih elemenata složenih po tačno utvrđenom redosledu. Po pravilu, ovaj segment obuhvata izbor nacrtu istraživanja, metode, tehnike i instrumente istraživanja, odabir uzorka, analizu i odabir podataka, izvore istraživanja i značaj istraživanja.

Kroz proces planiranja, praktično se sinhronizuju sve predviđene aktivnosti, sredstva i učesnici u istraživanom prostoru i vremenu. U sklopu toga, svi planovi istraživanja moraju biti determinisani prostornim i vremenskim određenjem istraživanja. Rezultat planiranja je operativni plan u kome se određuje: ko, šta, kada, kako i čime realizuje istraživanja; vreme trajanja; prostor u kome će se obaviti istraživanje, kao i materijalno tehnička i finansijska sredstva koja su potrebna da se istraživanje realizuje, itd.

Teorijsko-empirijski karakter predmetnog područja, složenost istraživačkog fenomena i postupka u celini, hipotetički okvir sa postavljenim deskriptivnim, eksplikativnim i eksplorativnim ciljevima, opredeljuju primenu više metoda za prikupljanje iskustvene evidencije, njenu analizu, kao i izbor i razradu adekvatnog nacrtu istraživanja.

1.6.1 Nacrt istraživanja

Na osnovu svega iznetog, osnovni istraživački princip u ovoj disertaciji jeste princip komplementarnosti koji zahteva različite izvore i metode prikupljanja, obrade i analize podataka, istraživačke strategije i dizajn. Radi se o dominantno kvalitetnom i istraživačkom pristupu, a nedovoljna teorijska izgrađenost uslovila je pretežno eksplorativnu prirodu istraživačkih zahteva. To je osnovni razlog da se u radu primeni deskriptivni nacrt istraživanja.

1.6.2 Metode istraživanja

Priroda istraživačke teme nametnula je primenu različitih metoda i postupaka, uključujući tu i istraživačke tehnike i instrumente. Radi uspostavljanja što većeg nivoa obuhvatnosti i pouzdanosti, u istraživanju je primenjen standardni metodološki instrumentarij koji je postao nezamenjiv u istraživanju sličnih tema, uz komplementarno korišćenje sledećih istraživačkih metoda:

- metoda analize sadržaja;
- istorijska metoda;
- metoda analize, sinteze, dedukcije i indukcije;
- metoda klasifikacije i sistematizacije;
- deskriptivna metoda;
- komparativna metoda; i
- kvantitativne i kvalitativne metode.

Teorijska zasnovanost problema istraživanja, kao i istraživačka elaboracija svih relevantnih pitanja vezanih za digitalnu transformaciju, digitalnu ekonomiju, ranjivost digitalnih entiteta, ranjivost digitalnog poslovanja, a posebno aktuelne i potencijalne bezbednosne pretnje i rizike, temelji se na pregledu i analizi savremene domaće i strane referentne literature, istraživačkih nalaza, studija i analitike budućih trendova.

1.7 Značaj, opravdanost i relevantnost istraživanja

Prilikom koncipiranja teme, a naročito oblikovanja metodološkog okvira, pošlo se od nesporne ocene da u naučno-stručnoj, ali i široj društvenoj javnosti, postoji jasno profilisan interes i

etabliran imperativ za bližim, dubljim i sveobuhvatnijim rasvetljavanjem i opservacijom svih izazova, koristi, prednosti, rizika i njihovih dolazećih efekata, koje digitalna transformacija nosi sa sobom u uslovima uspostavljanja digitalne ekonomije, pametnih tehnologija i društva znanja.

Upravo je taj interes sadržan gotovo u svim, bez izuzetka, razvojnim projekcijama i strateškim dokumentima, najpre stimulisao, a zatim i usmerio naučno-stručnu produkciju, što je rezultiralo imponantnim brojem naučnih projekata, studija, udžbenika i drugih pisanih materijala.

Imajući u vidu ukupan značaj ove tematike, njenu aktuelnost, a naročito deficitarnost naučnih izvora, dobijeni rezultati ove disertacije mogu poslužiti da se popune postojeće praznine, da se otklone prisutne dileme, kontroverze i različiti i neujednačeni pristupi, kao i pogrešne precepcije koje se tiču digitalne transformacije kao celine, tj. ključne osnove za bezbedan razvoj digitalne ekonomije.

Poglavlje II: Konfiguracija digitalnih tehnologija i trendovi razvoja

1. Obeležja i dometi tehnološke revolucije

Digitalna revolucija, u akademskim krugovima, političkom, a naročito poslovno-informatičkom okruženju i diskursu, poprima transformativnu moć koja zahvata sve aspekte društva, od pojedinca, preko kompanija, pa do svih državnih sektora, pri čemu se u potpunosti menja, ne samo konfiguracija i pejzaž poslovanja, proizvodnje, pružanja usluga, odvijanja tržišne utakmice, način komunikacije, već i model upravljanja i organizacije poslovanja i rada, ne samo privrednih, već i javnih servisa.

U suštini, dinamičan i ubrzan razvoj disruptivnih tehnologija i inovacija, generišu visok stepen umrežavanja, nepoznat u dosadašnjoj istoriji između ljudi s jedne i informaciono-fizičkih sistema sa druge strane. U okviru ovog procesa, vidljivi su trendovi ubrzanja primene „Interneta pametnih stvari“, kao i njihove integracije u kompleksne sisteme na globalnom nivou. Tehnološki ciklusi koji se pritom odvijaju, odvijaju se tako velikom brzinom, da oni transformišu celo društvo i ekonomiju svojim eksponencijalnim rastom. Društvo i ekonomija se izlažu strukturnim promenama, te naglašenim kvantnim skokovima u inovacijama, što omogućava u kvalitativnom smislu kreativno oblikovanje inoviranih proizvoda i usluga, a time i korespondentnih proizvodnih potencijala čije je ishodište digitalna ekonomija.

Informaciono-komunikacione tehnologije zasnovane na disruptivnim inovacijama, omogućavaju, kako to brojni stručnjaci ističu, potpuno novu interakciju društva i tehnologije, što otvara široke prostore za rešavanje, kako starih problema, tako i novih izazova u širokom rasponu, od proizvodnje i usluga, preko medicine, umetnosti, nauke, tehnologije, bezbednosti, energetike, telekomunikacija, marketinga, bankarstva, brojnih privrednih sektora, kao i javne uprave.

Masovnom primenom digitalnih tehnologija, brojne kompanije na različite načine prolaze sopstvenu digitalnu transformaciju vođene novim digitalnim korisničkim iskustvom koje deluje kao spoljni vektor, menjaju operativne modele, te shodno tome redizajniraju, prilagođavaju postojeće ili izgrađuju nove digitalne i poslovne tržišne mogućnosti.

Ogroman broj promena koje nastaju u tom procesu, iziskuje i nov način razmišljanja o tome kako maksimizirati pozitivne efekte tehnoloških dostignuća, kako u odnosu na postojeće tehnološke baze, tako i potpuno nove nadolazeće inovacije disruptivnog karaktera. Istovremeno, takav

razvoj, kao i način promišljanja, nameće potrebu uspostavljanja procesa kontinuirane izgradnje modela odnosa između proizvođača, partnera, korisnika i kupaca u agilnom stvaranju novog lanca vrednosti.

Izuzetno dramatične, kompleksne i teško predvidljive promene u brojnim tehnologijama i njihov uticaj na poslovne procese, poslednjih godina postaju daleko izraženije nego ranije. Naime, disruptivne tehnologije u najširem smislu u potpunosti menjaju cele industrije, a u okviru toga i sve unutrašnje sektore, a posebno one koji su po svojoj prirodi tehnološki zavisni od inovativnih modela razvoja. Stoga je od izuzetne važnosti za razumevanje celokupnog poslovnog okruženja, kao i predviđanja budućih trendova, realna analiza disruptivnog potencijala postojećih tehnologija i kompanija koje te tehnologije primenjuju u svom svakodnevnom poslovanju.

U takvom turbulentnom i dinamičnom poslovnom ambijentu, paralelno se odvija nekoliko makro procesa ili revolucija, koje ne samo da jedna drugu podstiču, već se međusobno prepliću i ukrštaju. U prvom planu, to se odnosi na globalizaciju koja se ubrzava u svim segmentima, rast kompanija i tržišta koji uvećava poslovne mogućnosti, održivost koja se koncentriše na iznalaženja novih načina upravljanja ograničenim prirodnim resursima i najzad digitalnu revoluciju, kao megatrend i proces globalnih razmera. Nakon ubrzanja protoka informacija i povećanja kapaciteta komunikacijske umreženosti i značajnog pojednostavljenja i olakšanja procesa proizvodnje i pružanja usluga, informacione i digitalne tehnologije ulaze u svoju poslednju ili završnu fazu - digitalizaciju stvari (Jovković, Čelik, 2017).

Naglašavajući brzinu i širinu ove nove tehnološke revolucije, pojedini autori ističu da su promene toliko duboke, da iz temelja menjaju našu percepciju, ne samo opštu, nego i biznisa u celini, budući da se javljaju novi načini proizvodnje, komunikacije, transporta, isporuke, saradnje, itd., čime se uspostavlja novi tržišni sistem sa potpuno izmenjenim standardima i pravilima igre (Schwab K; 2016:7-8).

Uporedo sa razvojem digitalnih tehnologija i njihovim napretkom, poslovanje i pružanje usluga postaju sve više zavisni od informacija s jedne, ali i umreženih informacionih sistema sa druge strane, čiji je zadatak da informacije obrade, analiziraju i daju nova saznanja za definisanje ili inoviranje postojeće poslovne strategije rada, razvoja i upravljanja, te izradu aplikacija za njihovu podršku. Na taj način posmatrano, digitalna transformacija nije opcija, već imperativ

svake države, ekonomije, kompanije, sektora, službe, servisa i sl. ukoliko žele opstati na tržištu, odnosno steći ili zadržati kompetitivnu prednost u odnosu na konkurenciju.

Savremeno doba je donelo da tehnološki napredak vodi do kvalitativnog skoka i informatizacije koja ima sve karakteristike nove industrijske i društvene revolucije (Đoković, Milunović, Čelik, 2016). Takve ideje se čvrsto oslanjaju na poslovnu intuiciju, spremnost na tržišnu borbu i ubacivanje inovacija na tržište na novi ili drugačiji način, a kroz poslovne preduzetničke ideje nastale na tim inovacijama (Đoković, Pavićević, Čelik, 2014). Razvoj preduzetništva u informaciono-komunikacionom pravcu definitivno je podstaknut novim ekonomskim tendencijama, na kojima su se razvile i paradigme konkurentnosti i posebnosti modernih preduzetnika. Neke od tih paradigmi su, kreiranje specijalizovanih timova, odnosno malih i fleksibilnih preduzeća, umrežavanje i koordinacija timova pomoću informacione i komunikacione tehnologije, smanjenje hijerarhijskih nivoa i demokratizacija u poslovnom odlučivanju, kao i povećanje autonomije zaposlenih i samostalnosti u donošenju odluka (Đoković, Milunović, Čelik, 2016).

Koliko je primena digitalnih tehnologija uzela maha i kako pojedine države nastoje da održe ili uhvate korak sa digitalnim trendovima, to najbolje ilustruju napori Evropske Unije i njenih država članica. Pojedine države članice EU su veoma rano prepoznale potrebu uvođenja digitalne transformacije, najpre u ključne privredne sektore, a zatim i u ostale segmente društva.

Nakon usvajanja novog regulativnog okvira, podstaknut je trend digitalizacije evropske industrije koji ujedno definiše i paket ostalih podsticajnih mera namenjenih iskorišćavanju svih potencijala i pogodnosti zaokruženog i unificiranog Evropskog digitalnog tržišta. Razvoj digitalnih tehnologija, zajedno sa drugim naprednim tehnologijama, kako se ističe u zvaničnom dokumentu Evropske Komisije (EK) „menja način na koji se oblikuju i proizvode proizvodi i povezane usluge, te način trgovanja istim, uključujući način stvaranja nove vrednosti. Zbog napretka u tehnologijama, počev od internet stvari, tehnologije 5G, računarstva u oblaku, analitike velikih podataka i robotike, drastično se menjaju proizvodi, procesi i poslovni modeli u svim sektorima, što uz pomeranje globalnih vrednosnih lanaca u konačnom vodi do kreiranja novih industrijskih modela“ (EK, COM 2016, 180 final, 2).

Prema istom izvoru, najveći izazov za evropsku industriju jeste kako brzo i u potpunosti iskoristiti te digitalne mogućnosti, odnosno digitalne prilike koje se pružaju preduzećima, kako

bi u potpunosti usvojila digitalizaciju kao sredstvo jačanja i osiguranja sopstvene konkurentnosti na jedinstvenom digitalnom tržištu. Konvergencija brojnih tehnologija pokretač je digitalne evolucije, pre svega robotike, veštačke inteligencije i 3D print-a i stoga omogućava preduzećima svih veličina i u svim regijama i sektorima da mogu iskoristiti prednosti evropskog sektora IKT formiranjem digitalnih industrijskih platformi sa ciljem razvijanja različitih tehnologija od komponenti i uređaja do softvera - za potrošačka tržišta i informatičke i web platforme, kao i odgovarajuće aplikacije i usluge.

Prema procenama iz studije PWC (PricewaterhouseCoopers), mreže kompanija za pružanje profesionalnih i konsultantskih usluga koja funkcioniše u 158 država širom sveta, evropski IKT sektor čini oko 4% BDP-a, upošljava više od 6 miliona radnika, njegova novostvorena vrednost iznosi više od 580 milijardi evra, dok se u narednih 5 godina procenjuje da će taj sektor doneti više od 110 milijardi evra prihoda na godišnjem nivou. Digitalizacija industrije u Nemačkoj, prema istim predviđanjima dovešće do povećanja produktivnosti za 8% i rast prihoda od 30 mlrd. eura godišnje“.

Tokom 2017. godine, EK je donela Strategiju za jedinstveno digitalno tržište, čiji je cilj da omogući svakom preduzeću u Evropi da u potpunosti iskoristi dostupne digitalne inovacije za poboljšanje svojih proizvoda, usluga i procesa, kao i za prilagođavanje aktuelnog poslovnog modela digitalnoj transformaciji. Poseban značaj ima pokretanje Evropske platforme koja uključuje 12 postojećih i 9 narednih nacionalnih inicijativa u području digitalizacije industrije. U sklopu toga, institucije EU, zajedno sa Svetskim ekonomskim forumom (WEF) pokrenule su tzv. Inicijativu o iskorišćavanju digitalnih mogućnosti. Kroz ovu inicijativu, osnivači nastoje svojim angažmanom doprineti ubrzanom razvoju digitalne ekonomije i društva znanja u saradnji sa vladama i proaktivnim visokoškolskim institucijama.

Budući da se za potrebe digitalne transformacije primenjuju slična znanja, tehnologije, rešenja i iskustva, bez obzira na to da li je reč o digitalnom preduzeću ili pametnim gradovima, DTI inicijativa akcentat daje zajedničkim infrastrukturnim elementima, kako bi se kroz umreženu saradnju omogućilo delovanje na nacionalnom nivou.

Praktični značaj i doprinos ove inicijative ogleda se u nastojanju da se podrži razvoj sposobnosti gradova i preduzeća, a paralelno sa tim ubrza razvoj preduslova i uklanjanje barijera u poslovnom okruženju. Kroz digitalne tehnologije poput računarstva u oblaku, mobilne i

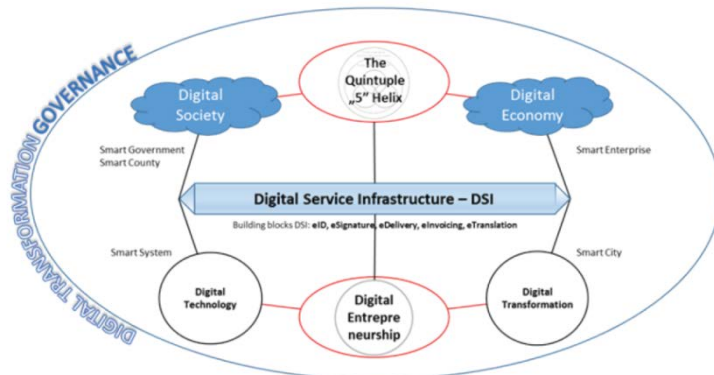
društvene mreže, BigData i interneta stvari, razradiće se „programi i obrazovne jedinice kao bi se na poslovnom nivou omogućilo:

- povećanje poslovne agilnosti
- ubrzanje inovacija
- nov način poslovanja
- transformisanje ključnih poslovnih procesa
- poboljšanje korisničkog iskustva“ (Infodom grupa; 2016:1).

Iz navedenog proizilazi, da digitalizacija podrazumeva, osim potpune transformacije poslovanja kroz stalno učenje, inoviranje modela poslovanja, procesa i proizvoda i otvorenost za promenu organizacione kulture, opredeljenost ka poslovnoj izuzetnosti kao dominantnom načinu mišljenja, te razvoj istraživačko-razvojnih kapaciteta, primenu prednosti otvorenih inovacija i novi tip liderstva.

Preporuka ove inicijative je više nego očigledna. Ekonomije svih država moraju se podvrgnuti ubrzanju transformaciji pod pritiskom inovacija i novih tehnologija, kao i sve veće prisutnosti elemenata četvrte industrijske revolucije na globalnom nivou. Na nacionalnom nivou, konceptualni okvir za digitalnu transformaciju podrazumeva i razvoj DSI infrastrukture (Digital Service Infrastructure), čije se komponente koje su u isključivoj nadležnosti država (e-identitet, e-potpis, e-račun, e-ispоруka...) stavljaju na raspolaganje svim zainteresovanim subjektima u ekonomskom sektoru.

Slika 1: DSI infrastruktura



Izvor: InfoDom konceptualizacija Digital Transformation Framework, Zagreb 2016.

U cilju povećanja brzine širenja inovacija, te osiguranja jednostavnosti primene rešenja, primenjuju se novi pristupi i arhitekture. Istovremeno, takav pristup zahteva uvođenje interoperabilnosti i standarda, a to će sve zajedno pospešiti poslovni kontinuitet, smanjiti rizike i povećati stepen bezbednost u sajber prostoru.

1.1 Razvoj i mogućnosti primene novih tehnologija

U akademskoj zajednici i diskursu, kao i u samom poslovnom okruženju, opšte je prihvaćeni stav da je digitalna tehnologija do sada dramatično promenila i nastaviće da menja konfiguraciju i pejzaž poslovanja, obrazovanja, zabave i funkcionisanja javnog sektora i servisa. Poslednjih nekoliko godina zabeležene su krupne promene koje predstavljaju dalekosežni iskorak, a tempo tih promena se ubrzava, dok je krajnji ishod veoma teško predvideti, usled opšte disperzije i razuđenosti inovativnog spektra tehnološkog razvoja.

Tehnološke promene obeležavaju tri temeljna faktora i to: brzina, obim i uticaj promene na sisteme i okruženje. Potpuno je izvesno da se promene i disrupcija dešavaju na tri nivoa, i to: individualnom, društvenom i organizacionom.

Brzina tehnoloških prodora čiji smo savremenici, istorijski je presedan. Naime, kada se postojeća brzina, dinamika i intenzitet promena uporedi sa prethodnim tehnološkim talasima, proizilazi da se aktuelna tehnološka revolucija razvija eksponencijalno, a ne ujednačenim tempom.

Iz navedenog proizilazi da su opseg disperzije i dubina opisanih promena u stvari vesnici, odnosno akceleratori dubinske promene svih proizvodnih sistema, sistema upravljanja i državne uprave, koja usled tehnološko-inovativnog pritiska mora da redefiniše i redizajnira, ne samo poslovni ambijent u kome se odvija tržišna utakmica u digitalnom prostoru, već i sam način vlastitog funkcionisanja.

Kako ove tehnologije utiču na poslovanje i tržišne odnose, najbolje ilustruje podatak iz jednog od novijih izveštaja McKinsey Global Instituta (2016.), u kome je data ocena „da je međunarodna razmena podataka u 2015. godini po prvi put u istoriji međunarodne trgovine generisala više vrednosti nego razmena roba i usluga. Od 8 uređaja trenutno povezanih na internet, samo jedan neposredno koristi čovek, dok su preostalih 7 deo interneta stvari, odnosno IoT“ (McKinsey Global Institute, 2016).

U istom izveštaju, predviđa se da će se u narednih 5 godina broj IoT uređaja povećavati 3 ili 4 puta brže nego broj internet korisnika. Ako taj trend predstavimo brojčano, dolazimo do toga da će do 2020. godine broj IoT uređaja porasti sa 22 na 50 milijardi jedinica, dok će se istovremeno broj internet korisnika uvećati sa 3,3 na 4,6 milijardi, budući da se predviđa da će do tada približno 2/3 svetske populacije ostvariti pristup Internetu. Ovakav dinamičan razvoj generisaće podatke daleko većim tempom nego što će se iz njih moći dobiti primenjiva saznanja, najpre u poslovne, a zatim i u medicinske, obrazovne i druge svrhe.

Nije teško ustanoviti jednu novu pravilnost: brzina kojom se menja ponašanje korisnika i kojom evoluiraju njihova očekivanja, u direktnoj je zavisnosti od brzine razvoja tehnologije. U praksi nailazimo na brojne primere kako nove tehnologije transformišu ili remete (disrupuju) različite industrije, poput autonomnih uređaja, npr. automobila, 3D štampe u proizvodnji, robota u logistici i mrežne ekonomije u turističkim uslugama.

Ovi akceleratori tehnološkog napretka i inovacija obuhvataju internet stvari (IoT), virtuelnu i proširenu stvarnost i kognitivno računarstvo. Upravo takve inovativne i kvantne skokove, tehnološki svesne i u tom pravcu usmerene kompanije u značajnoj meri koriste za optimizovanje poslovnih procesa, poboljšanje korisničkog iskustva i razvoj inoviranih ili potpuno novih digitalnih servisa i proizvoda u cilju opstanka na tržištu ili povećanja konkurentskog potencijala.

Slično prethodnim, i aktuelna tehnološka revolucija ima potencijal, ili kako se to u zvaničnom vokabularu ističe „transformativnu i inovativnu moć“ da uveća globalni nivo prihoda, osigura proizvodnju i pristup egzistencijalnim resursima i ujedno poboljša kvalitet života, uslove rada i privređivanja, unapredi načine komunikacije i najzad promeni, ne samo percepcije, već i shvatanja uloge, značaja i potrebe interaktivnosti čoveka sa mašinama, drugim ljudima i globalnim okruženjem. Najveću korist, prema mišljenju stručnjaka, od ovakvog tehnološkog razvoja i široke primene novih digitalnih i disruptivnih tehnologija i inovacija, imaju potrošači i korisnici digitalnih servisa i usluga, jer ta konstelacija stvari uvećava mogućnost zadovoljavanja njihovih potreba i preferencija, usled čega kod njih stvara i osećaj ličnog zadovoljstva i digitalnog komfora.

Ubrzanje inovacija i njihova široka primena predstavljaju izvor stalnog iznenađenja, tim pre što nove tehnologije imaju snažan i kontinuirani uticaj na sve aspekte ljudskog rada i delovanja.

Glavne promene na strani „potražnje ispoljavaju se kao:

- Rastuća transparentnost;
 - angažovanje potrošača;
 - novi obrasci potrošačkog ponašanja usled pristupa mobilnim mrežama i podacima.“
- (WEF, 2016)

Započeta tehnološka revolucija, direktno ili indirektno ostvaruje uticaj na način poslovanja, uticaj na vlade i njihovo delovanje, a samim tim i uticaj na ljude. Time nije iscrpljena lista ovih uticaja, obzirom da se ona proteže i na našu saosećajnost i saradnju, privatnost i mogućnost rasuđivanja, te prilagođavanje ukupnom turbulentnom okruženju koje je opet od snažnog uticaja i na našu sposobnost oblikovanja budućnosti. Jednom rečju, nove tehnologije i sa njima spregnute disruptivne inovacije, uveliko redefinišu, ne samo savremeni način života, već i način na koji je ljudski um umrežen.

Pored navedenih, značajno obeležje novih tehnologija jeste i u tome što su one danas postale dostupne širokom broju korisnika, praktično svakome ko ima pristup internetu i pratećim informaciono-komunikacionim sredstvima. Ipak, sam pristup ovim tehnologijama ne daje konkurentsku prednost, već to daje način na koji koristimo tehnologiju.

2. Disruptivne tehnologije

Iako postoje brojne, više ili manje celovite i uglavnom konvergentne definicije, disruptivne tehnologije se u konceptualno-teorijskom smislu, a prvenstveno u poslovnoj teoriji, najjednostavnije definišu kao „inovacija koja stvara novu i istovremeno narušava postojeću tržišnu i vrednosnu mrežu, pomerajući do tada uspostavljene odnose na tržištu, pozicije kompanija, strukturu proizvoda i partnerstva“ (Rahman, 2017).

Pojednostavljeno, „digitalna disrupcija je izmena kapitalizacije ponude (proizvoda ili usluge) za korisnike, koja je kreirana putem korišćenja digitalnih tehnologija ili digitalnih poslovnih modela, koja je dovela do značajne promene na tržištu. Ne mogu se sve promene nazvati disruptivnim. Da bi promena bila disruptivna, neophodno je da ona bude prihvaćena od korisnika i da značajno poremeti postojeće snage na tržištu, tj. da dovede do preuzimanja velikog broja klijenata, odnosno preuzimanja velikog dela prihoda“ (Vujović; B., 2017:62).

Prema vodećim stručnjacima na zapadu, sve inovacije se razvrstavaju u dve glavne kategorije: održive i ometajuće.

Tvorac ometajuće (disruptivne) inovacije, odnosno jedan od vodećih stručnjaka iz ove oblasti, Christensen Clayton, profesor Poslovnog fakulteta na Univerzitetu Harvard, praktično je „udario“ temelje disruptivnom pristupu i tako omogućio pronalaženje potpuno novih izvora rasta i razvoja.¹

Na osnovu brojnih predviđanja ovog profesora, tek je nakon objavljivanja njegove knjige 1997. godine „*The Innovator’s Dilemma*“ postalo jasno da je on u potpunosti bio u pravu u pogledu datih predviđanja vezanih za buduća dešavanja, a u prvom redu kada je reč o razvoju inovativnih tehnologija koje neprekidno preuzimaju primat u smislu njihove uvećane efikasnosti. Stoga, planiranje i projektovanje ometajućih, tj. disruptivnih promena zahteva od menadžera stalno stvaranje novih mogućnosti, bilo da je u pitanju preuzimanje kompanije čiji su procesi i vrednosti u skladu sa inoviranim zadatkom, ili pak stvaranje nove kompanije čiji će razvoj biti baziran na primeni novih inovativnih rešenja i tehnologija.

Disruptivne tehnologije se često u literaturi nazivaju i tehnologijama u nastajanju ili konvergirajućim tehnologijama. Tehnologije u nastajanju su tehničke inovacije koje po pravilu krše već uspostavljene paradigme, pravila i standarde. Konvergentne tehnologije nastaju iz konvergencije različitih sistema koji se razvijaju prema sličnim ciljevima. Primeri tehnološke konvergencije mogu biti spoj mobilnog telefona i interneta, dizajn hibridnih vozila, kombinacija industrije filmova i igara, sinergija nauke o nano i makro skali u biologiji, poljoprivredi i dizajnu materijala, online obrazovanje, itd.

Za razliku od novih tehnologija, konvergentne tehnologije nisu nužno bazirane na tehničkim otkrićima, nego uključuju razvijene i komercijalizovane tehnologije kako bi se postigao novi nivo primene ljudskih sposobnosti, društvenih rezultata, nacionalne produktivnosti i kvaliteta života.

Implementacija nove tehnologije često uključuje ekonomski rizik, ali ako je implementacija uspešna, ona nudi značajnu kompetitivnu prednost kompaniji. Neke od novih tehnologija razvijaju se kroz teorijska istraživanja, dok se druge temelje na komercijalnom istraživanju i razvoju.

¹ Christensen je do sada objavio pet knjiga, bestselera iz ove oblasti i to: „*The Innovator’s Dilemma*“ (1997.), „*The Innovator’s Solution*“ (2003.), „*Seeing What’s Next*“ (2004.), „*Disrupting Class*“ (2008.) i „*The Innovator’s Prescription*“ (2009.)

Ometajuće ili disruptivne inovacije nesumnjivo mogu izmeniti načine na koje ljudi žive i rade, redefinisati vrednosti na tržištima i dovesti do stvaranja potpuno novih proizvoda i usluga. Otkrivanje i identifikacija disruptivnih tehnologija, stoga, od istraživača zahteva da istovremeno razmišlja i kao inovator i kao preduzetnik, kako bi u potpunosti bio sposoban da iskoristi trenutak u kome je došao do spoznaje da novo i potencijalno rešenje u potpunosti ili delimično menja prethodnu tehnologiju i do tada primenjeno rešenje.

S tim u vezi, poslednjih godina se jako puno raspravlja, a u istraživačkom smislu opserviraju i nove tehnologije i trendovi koji će verovatno imati ometajući učinak na ekonomije, poslovne modele, kompanije i ljude. Digitalna disrupcija se najčešće zasniva na inovacijama ili novoj ideji, mada se može u određenim slučajevima zasnivati i samo na inovativnim poslovnim modelima koji značajno uvećavaju vrednost ponude.

Nakon skoro dve decenije upotrebe, termin disruptivne tehnologije i/ili inovacije postao je visoko frekventan, tako da danas u svakodnevnom, a naročito poslovno-tehnološkom diskursu nailazimo i na fraze poput „disruptiraj ili ćeš biti disruptiran“, „big-bang disrupcija“ i sl.

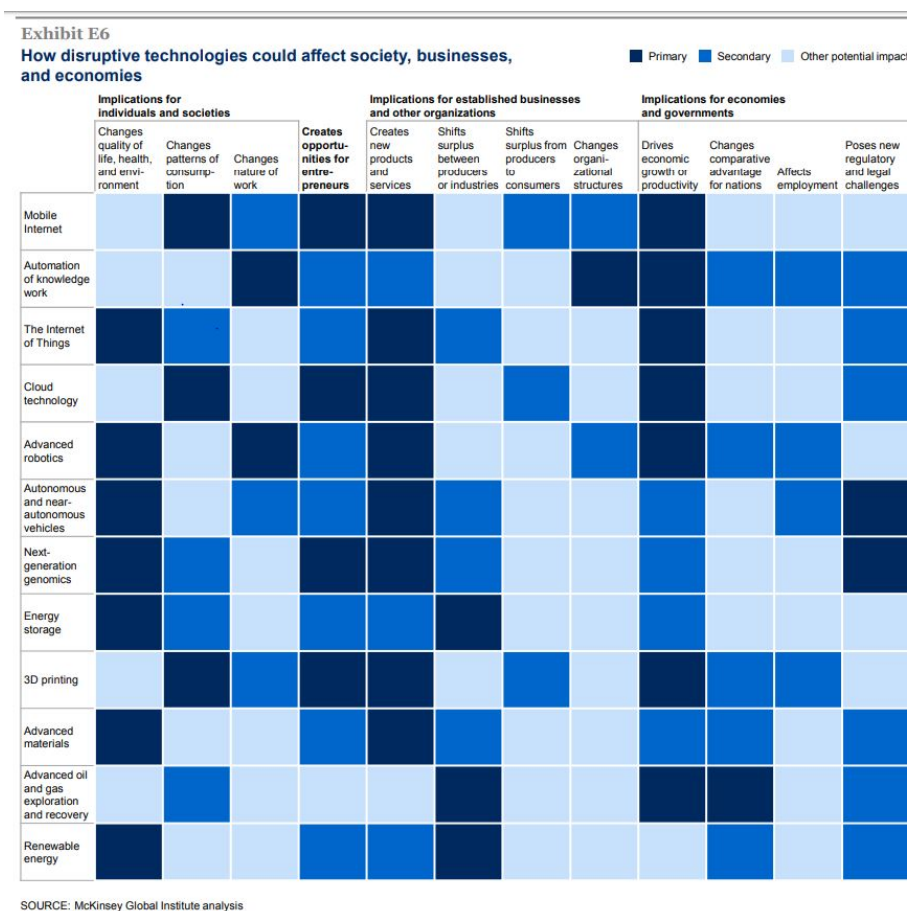
Kako bi ilustrovali značenje ovog termina, pojedini autori, primerima iz prakse pokazuju višeznačnost i brojne dimenzije i aspekte ovog termina. Tako na primer, e-mail je disruptivna inovacija koja je bezmalo uništila poštansku službu, dok je Amazon najpoznatija globalna knjižara. Ovakve disruptivne inovacije nisu mogli prenebregnuti čak ni najveći svetski trgovinski lanci poput Walmart-a u svom poslovanju.

Nesporno je da sintagma disruptivne inovacije zaista zvuči atraktivno, tim pre što podseća na kreativnu destrukciju, definisanu od strane čuvenog austrijskog ekonomiste J. Schumpeter-a, a to posebno ako se ima u vidu da obe konstrukcije imaju destruktivno-disruptivni i kreativno-inovativni momenat.

Istraživanja novijeg datuma ukazuju, da je teorija disruptivnih inovacija zapravo deo poslovne kulture svoga doba u kojoj učesnici digitalne ekonomije kreću u novi tehnološki poduhvat, ne uzimajući u obzir do koje mere je on i izvestan i rizičan. Ovakav trend doveo je do rata na planu inovacija između velikih kompanija i time direktnih konkurenata na tržištu. U ekonomskom pogledu, na savremenom tržištu, proizvodi i proizvođači se faktički ne takmiče sa cenama, nego sa inovacijama. Stoga su inovacije, ne samo neizvesne, već i veoma skupa igra koju ne mogu sebi priuštiti sve kompanije, već samo one u datom momentu finansijski sposobne da do kraja

isprate trend „serviran“ od strane konkurencije. U prevodu to znači, da kompanije ili ekonomije, kako bi osigurale sredstva za nastavak inovacija radi osiguranja što povoljnije pozicije na tržištu, bivaju prisiljene eksploatisati cene iznad marginalnog troška, bilo u obliku diskriminatornih cena, oligopolnih cena ili čak monopola (Lepore; J, The New Yorker, 2014.).

Slika 2. Uticaj disruptivnih tehnologija na društvo, poslovanje i ekonomije



Izvor: McKinsey Global Institute analysis str. 20, 2013

Disruptivnim tehnologijama najčešće se smatraju one tehnologije koje menjaju uvrežene poslovne procese, pa i cele industrije, na taj način što uvode potpuno novi način poslovanja baziran na tehnologiji. Među najpoznatijim primerima „disrupcije“ su „Uber“ i „Airbnb“ čija je zajednička crta pokazala da se započete disruptivne promene događaju brzo, tačnije daleko brže nego što to naša očekivanja mogu digestirati.

U domaćoj, a još više u stranoj stručnoj javnosti, najčešće se postavljaju sledeća dva pitanja:

- Koje to tehnologije danas prete disrupcijom, tj. nasilnom promenom postojećih paradigmi?

- Koji poslovni modeli postaju prevaziđeni, a koje su industrije ili njeni pojedini sektori prepoznali priliku i sada na tim osnovama ostvaruju značajan rast, zahvaljujući pre svega primeni savremenih tehnoloških rešenja?

Pojedini autori smatraju „da disruptivna inovacija kreira proizvod koji pronalazi jednostavnu primenu u donjem tržišnom segmentu, a onda nezaustavljivo napreduje ka vrhu, što za posledicu ima potiskivanje postojećih konkurenata sa tržišta“ (Lajović, Vulić, 2010:73).

Napredak na planu razvoja veštačke inteligencije, nanotehnologija, kvantne informatike i sl., tipični su primeri kako nove tehnologije generišu promene u radu i poslovnom okruženju, ponašanju zaposlenih i sl. Prema dostupnim podacima, približno 20% kompanija se uključilo u neki oblik primene veštačke inteligencije u svoje poslovne procese, dok 40% kompanija ima strategiju za njeno uvođenje. Osim toga, u segmentu prodaje, predviđa se da će 60% prodajnih timova povećati primenu analitičkih alata i veštačke inteligencije kako bi lakše prepoznali potrebe i želje kupaca.

2.1 Bazične digitalne tehnologije i njihov kontekst

U naučnoj i stručnoj javnosti, kao i poslovnom svetu, velika pažnja se poklanja bazičnim, odnosno dubokim digitalnim tehnologijama, za razliku od tzv. plitkih ili površnih tehnologija čiji razvoj ne izaziva toliko interesovanje, usled njihovog manje izraženog disruptivnog potencijala.

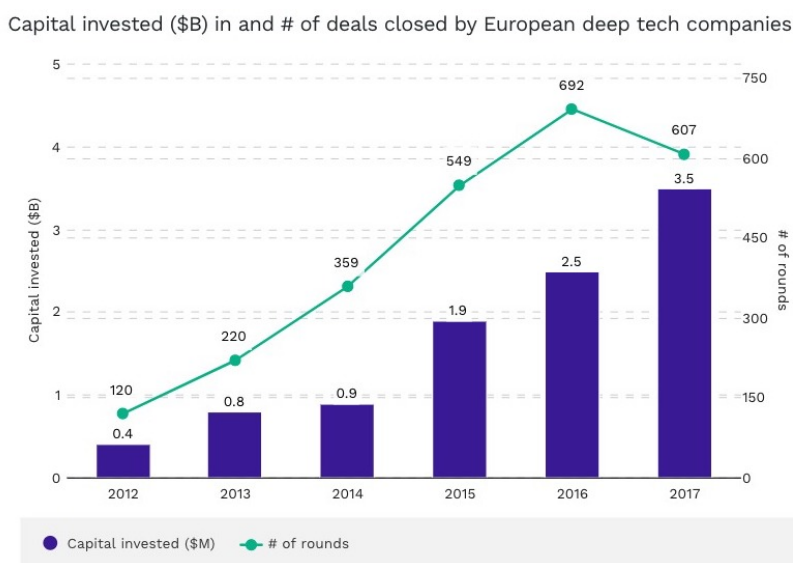
Bazične ili duboke tehnologije, skup su najsavremenijih i najrazornijih tehnologija, utemeljenih na velikim naučno-istraživačkim dostignućima i visokotehnološkim inženjerskim inovacijama u domenu matematike, fizike, medicine i sl. One često iziskuju dugoročna razvojna istraživanja, velike investicije i po pravilu duži vremenski interval priprema za uvođenje proizvoda u komercijalnu upotrebu.

Za 2019. i 2020. godinu, stručnjaci označavaju da glavna područja, segmenti i pravci razvoja i primene bazičnih tehnologija uključuju, veštačku inteligenciju, poljoprivredu, nauku o životu, hemiju, vazduhoplovnu industriju, energetiku i zelenu energiju. Osim toga, duboke tehnologije obuhvataju između ostalog i duboko i mašinsko učenje. Sam izraz „duboka tehnologija“ prvi je upotrebio Swati Chaturvedi, osnivač prve platforme u svetu koja je posvećena „digitalnom anđelu koji ulaže u duboke tehnološke startup-ove“. Duboku tehnologiju u najširem kontekstu određujemo kao kompanije zasnovane na naučnom otkriću ili smislenoj inženjerskoj inovaciji, a

sa druge strane, duboke tehnološke kompanije pokušavaju rešiti određene životne probleme, kao što su na primer novi medicinski uređaj ili tehnika za borbu protiv kancera, analitika podataka kako bi se pomoglo poljoprivredi da uzgaja više hrane ili rešenje za čistu energiju koja nastoji smanjiti ljudski uticaj na klimatske promene, itd.

Gotovo sva područja bazične, odnosno duboke tehnologije, imaju isti izazov, tj. izazov: kako pronaći investitora za početno finansiranje razvoja inovativnog tehnološkog rešenja, imajući u vidu složenu prirodu i neizvesnost koja prati takav pristup. Suštinski, to znači da postoji niz poteškoća, nepremostivih prepreka ili ograničenja u razumevanju potencijala dubokog tehnološkog pokretanja, jer je izuzetno teško, kako je to napred i istaknuto, pronaći pouzdanog i spremnog investitora koji je istovremeno i kompetentan za određenu oblast, pa zaista razume početnu inovativnu tehnologiju i istraživačku ideju.

Grafikon br.1 Rast kapitalnih investicija u duboke tehnologije u Evropi



Izvor: Startup Business, 2018

Prema istraživanju kompanije Wavestone, u Evropi je od 2015. godine ulaganje rizičnog kapitala u duboke tehnologije raslo tri puta brže nego u svetu. Francuska je globalno vodeća zemlja u pogledu talenata, dok je Velika Britanija, što se tiče pristupa finansijama i ulaganjima u 2017. godini, na prvom mestu (Wavestone, 2017).

Ubrzani rast B2C, kao forme elektronskog poslovanja, tehnoloških divova poput Google, Amazon, Facebook, Spotify, WhatsApp, itd., praktično su trasirali put za hiljade manjih

kompanija koje primenjuju digitalne tehnologije u cilju izgradnje inovativnih poslovnih rešenja, baziranih na internet aplikacijama. Sa razvijanjem sposobnosti rešavanja globalnih pitanja, kao što su: energetska tranzicija, bezbednost, starenje, klimatske promene kroz najsavremenije tehnologije, uključujući i nove materijale, veštačku inteligenciju, bio i nano tehnologiju, nove kompanije na tržištu rastu poput novog propulzivnog talasa privlačeći investitore koji upravo na tom polju traže prostor za pozicioniranje i rast investiranog finansijskog uloga.

2.1.1 Prvi talas disruptivnih tehnologija

Iako se proces razvoja disruptivnih tehnologija odvija veoma brzo, po nekim merilima čak i prebrzo, ipak, taj se proces realizuje u talasima, gde se najpre pojavljuju one tehnologije koje su u startu imale obećavajući potencijal, a onda nakon određenog vremena na „scenu“ stupaju inovativnija rešenja bazirana na nadgradnji postojećih tehnologija i rešenja.

Uvidom u postojeću stručnu literaturu koja sa teškoćom i velikim zaostatkom prati sve savremene digitalne i tehnološke tokove, proizilazi zaključak da prvi talas disruptivnih tehnologija obuhvata: cloud tehnologiju, mobilnu tehnologiju, big data, društvene mreže i internet stvari. U nastavku, daće se kratak pregled svih ovih pet tehnologija prvog disruptivnog talasa.

2.1.2 Big Data

Big data podrazumeva velike skupove podataka, koji zbog svog obima i složenosti nisu pogodni za to da ih tradicionalni softverski proizvodi preuzmu, upravljaju njima i obrađuju ih u vremenski prihvatljivom roku radi dobijanja novih saznanja.

Iz tih razloga, svi veliki skupovi podataka moraju uključivati strukturisane, delimično strukturisane i nestrukturisane podatke, od kojih svi mogu da se pretražuju i analiziraju radi uvida.

Big data ili tzv. veliki podaci, karakterišu se sa tri „V“:

- Ekstremni obim podataka (Data Volume)
- Širok spektar tipova podataka (Data Variety) i na kraju
- Brzina kojom se podaci moraju obraditi i analizirati (Data Velocity).

U stručnoj literaturi se navodi da koncept Big data sadrži skup interkonektovanih komponenti koje omogućavaju organizacijama da upotrebe dostupne podatke za praktične potrebe i tako

rešavaju niz poslovnih izazova i problema. To između ostalog obuhvata IT infrastrukturu potrebnu za podršku, analitiku koja se primenjuje na podatke, tehnologiju potrebnu za Big data projekte, povezane skupove kompetencija i stvarne slučajeve za koje je potrebno da se koristi Big data (Violino, 2018). Praktična vrednost, ili jedna od najvećih vrednosti Big data jeste analitika primenjena na podatke i njihovo temeljno razumevanje.

Kompanije i sektori koji su uveli digitalizaciju, imaju potrebu nesmetanog, jeftinog i fleksibilnog skladištenja podataka, a rešenje ovog problema upravo nudi primena Cloud-a. Skladištenje u Cloud-u omogućava svim zainteresovanim subjektima snimanje strukturiranih i nestrukturiranih podataka bilo koje vrste u izvornom formatu. Na taj način, centralizovani podaci u oblaku osnova su, kako za sadašnju, tako i za buduću analitiku. Sa tog aspekta, Big Data se percipira kao prilika za poslovni uspeh, ali samo za one kompanije koje imaju jasnu viziju i znaju kako da rešavaju problem sa ogromnom količinom i raznovrsnošću podataka. Trenutno, većina kompanija sakuplja podatke, međutim one i dalje nemaju razvijenu analitiku, upravo usled prakse da se ti podaci samo deponuju, a odluke se i dalje donose na bazi delimičnog uvida u njih.

Mali je broj kompanija koje uspevaju da kreiraju znanje i rade na primenama i transferu tog znanja na osnovu velike količine analiziranih podataka. U novije vreme, pojavljuju se i tržišta podataka radi pojednostavljivanja procesa pretraživanja, nudeći različite izvore i tipove podataka zajedno sa potencijalnom grupom njihovih kupaca.

Analizirajući podatke, menadžment može donositi bolje i kvalitetnije poslovne odluke, kao što su: kada i gde pokrenuti marketinšku kampanju ili kada uvesti novi proizvod ili uslugu.

Najčešće se analitika odnosi na osnovne primene poslovne inteligencije (BI) ili naprednije analitike predviđanja, nalik onima koje se koriste u cilju poboljšanja zdravstvenih usluga. Ipak, među najnaprednije vrste analitike podataka spada takozvano rudarenje podataka, putem koga data analitičari vrše estimaciju velikih skupova podataka kako bi kroz njih identifikovali međusobne odnose, kao i trendove i obrasce posmatranih pojava.

U pojedinim slučajevima, analitika podataka uključuje i njihovu verifikacionu analizu u cilju utvrđivanja da li je pretpostavka o određenom skupu podataka istinita. Osim toga, treba razlikovati kvantitativnu od kvalitativne analize podataka, s tom razlikom da prva obuhvata analizu numeričkih podataka, a druga se fokusira na nenumeričke podatke kao što su slike, tekst ili video zapisi.

Mada se Big data koncept koristi u različitim oblastima poslovanja, stručnjaci smatraju da ova tehnologija postiže najveću aplikativnu vrednost u sledećim slučajevima:

Analitika korisnika – daje mogućnost kompanijama da pregledaju korisničke podatke kako bi poboljšale korisničko iskustvo, uvećale stopu promena i podigle nivo zadržavanja korisnika;

Operativna analitika - označava operativnu uspešnost i bolji stepen iskorišćenja korporativne imovine. Analitika Big data može pomoći kompanijama u iznalaženju načina za efikasnije poslovanje i poboljšanje performansi;

Prevenција prevara – duboka analiza podataka pomaže ranom otkrivanju sumnjivih i nedozvoljenih aktivnosti i registrovanju obrazaca koji mogu ukazivati na potencijalno kriminalno ponašanje, što je vid pomoći u redukciji rizika;

Optimizacija cena – kompanije mogu koristiti Big data analitiku kako bi, ako je to u njihovom interesu, optimizovale cene za proizvode ili usluge u cilju podizanja nivoa profitabilnosti.

Imajući u vidu kompleksnost i razuđenost, kao i širinu i obim Big data, te neophodnu profesionalnu analitiku, nastala je potreba za profesionalnim i stručnim ljudskim resursima koji imaju sveobuhvatne menadžerske sposobnosti da upravljaju značajnim Big data projektima od njihovog početka do kraja, čime se obezbeđuje konzistentnost postupka i kvalitet krajnjih rezultata.

Obzirom na hronični deficit kadrova sa ovakvim vrstama veština, umeća i znanja, potpuno je izvesno da će pronalaženje iskusnih profesionalaca i njihovo angažovanje na ovim poslovima biti jedan izuzetan izazov za sve kompanije u kontekstu efikasne primene Big data koncepta.

Sve češće se u stručnim krugovima dovodi u pitanje stav da pristup većoj količini podataka nudi više informacija, što pojedini autori smatraju da nije uvek slučaj. Naime, „postoji ogromna razlika između same količine i potpunosti velikog broja podataka“(Boyd&Crawford; 2011).

Iz tih razloga, određivanje „test uzoraka“ u ovom kontekstu nosi jednu kompleksniju dimenziju, koja, kako se tumači, vodi do potpunog prestanka potrebe za statističkim uzorkovanjem.

2.1.3 Internet stvari

Internet povezanih stvari ili Internet inteligentnih uređaja (eng. Internet of Things) kao pojam, odnosi se na milijarde fizičkih uređaja opremljenih sensorima i softverima, instaliranih širom

sveta i povezanih na internet, kako bi sakupljali i razmenjivali podatke. Upotrebom ovih uređaja, uvodi se tzv. digitalna inteligencija u mrežne sisteme, odnosno daje mogućnost ovim uređajima da bez učešća čoveka koriste potrebne podatke u određeno vreme i da na taj način regulišu svoj rad i interakciju. Sam termin Internet stvari ili IoT, već u prvoj aproksimaciji asocira na opštu međusobnu povezanost svih elektronskih uređaja. Pod tim terminom podrazumeva se sistem fizičkih uređaja povezanih preko interneta, opremljenih sensorima, organizovanih tako da mogu prikupljati podatke, razmenjuju ih i mrežno komuniciraju. Ova tehnologija, omogućava da svaki fizički objekat koji ima mogućnost povezivanja na internet može biti pretvoren u IoT uređaj.

Prema procenama specijalizovane web stranice „Business Insider“, do 2023. godine IoT će biti dominantna tehnologija, kako u privatnoj sferi, tako i u domenu biznisa.

U izveštaju ovog portala, data su prilično utemeljena predviđanja da će Internet stvari u narednih 5 godina u velikoj meri preobraziti konzumerizam, kompanije i vlade time što će:

- podstaći ekonomiju baziranu na podacima i tako premostiti jaz između fizičkog i digitalnog sveta;
- omogućiti da potrošači, kompanije i vlade širom sveta instaliraju više od 40 milijardi IoT uređaja do 2023. godine, što će označiti početak i ubrzati ključnu transformaciju u načinu poslovanja kompanija i dovesti do uspostavljanja novog regulativnog okvira, kao i načina na koji će potrošači percipirati svoje potrebe i okruženje.

Za ostvarenje ovog ambicioznog cilja, potrebna su velika ulaganja, koja se kreću u zoni triliona dolara do 2026. godine. (Business Insider, The Internet of things 2019.)

U svetu IoT-a, koji se neprestano menja, kroz ovu ekskluzivnu studiju i detaljna istraživanja na tom području, temeljno se opisuju komponente koje čine „IoT ekosistem“. U tom izveštaju, daje se i sveobuhvatna analiza i na njoj razrađena projekcija „kako internet stvari nastavljaju da transformišu poslovanje, domaćinstva i gradove kroz sledeću generaciju digitalnih rešenja“ (Ibid).

U knjizi prognoza za IoT 2018. godine, dat je prikaz globalne proliferacije IoT u narednih 5 godina, koji uključuje obuhvat primene IoT kod potrošača, kompanija i vlada. Prema toj prognozi, može se očekivati sledeći trend:

Internet stvari za potrebe potrošača – Samo u SAD broj pametnih kućnih uređaja premašiće broj od milijardu do 2023. godine. Potrošači će prosečno izdvajati oko 725 dolara po domaćinstvu u ovu svrhu, što će u ukupnom iznosu doneti više od 90 milijardi dolara potrošnje samo na ovom tržištu IoT.

IoT u biznis sektoru – Kompanije će nastaviti trend ulaganja u povezane uređaje i automatizaciju. Do 2023. godine, ukupna industrijska baza robota u svetu približiće se broju od 6 miliona, dok će godišnja potrošnja na proizvodna rešenja IoT biti oko 450 milijardi dolara.

Internet stvari za potrebe Vlada – Na globalnom nivou vlade uvode IoT uređaje kako bi pokrenule razvoj pametnih gradova koji bi bili opremljeni inovativnim tehnologijama kao što su povezane kamere, pametna ulična svetla i povezana brojila, kako bi se ostvario uvid u saobraćaj, korišćenje komunalnih usluga, kriminal i ekološku zaštitu. Predviđa se da će godišnje ulaganje u ovo područje dostići 900 milijardi dolara.

Opisane tehnologije će na različite načine, kako se procenjuje, promeniti budućnost poslovanja i fizionomiju biznisa. U prvom digitalnom talasu, doći će do ekspanzije pametnih telefona, toster, klima uređaja, kreveta, vrata, frižidera, štednjaka, sijalica, sistema navodnjavanja, kontejnera i sl., zapravo svega onoga što sada smatramo običnim neinteligentnim hardverom.

Iako postoje svega nekoliko godina, ove tehnologije su već našle široku primenu u brojnim sektorima industrije, pa stručnjaci predviđaju da bi njihova primena dovela do povećanja produktivnosti, smanjenja troškova proizvodnje, proširenja proizvodnog asortimana i delokruga usluga, a to bi se odrazilo i na otvaranje novih tržišta i redefinisanje tradicionalnih.

Pored biznis sektora, ove tehnologije našle su primenu i u oblastima funkcionisanja javne uprave. Obzirom na opšti trend smanjenja državne administracije, a time i troškova državnog aparata, predviđa se da će upravo u ovom segmentu IoT naći svoju masovnu primenu, a to će se po inerciji preliti i na javna preduzeća i njihov način rada sa korisnicima usluga.

Poslednjih godina, veliki broj tehnoloških kompanija, nezavisno od svoje veličine i finansijske moći, ulaže ogromna finansijska sredstva koja se mere u milijardama u razvoj IoT tehnologije poput pametnih frižidera, pametnih brava, pametnih prekidača, pametnih termoregulacionih uređaja, pametnih svetlosnih sistema, pametnih kućnih aparata itd., kako bi se pre konkurencije

što bolje i brže pozicionirale na tržištu i svoj finalni proizvod plasirale i distribuirale što širem broju korisnika.

Prvenstveno zbog primene ovih tehnologija, veliki broj poslova u bliskoj budućnosti biće potpuno automatizovan, čime se povećava efikasnost i produktivnost poslovanja, i na kraju i sam profit kompanije. Međutim, automatizacija prema nekim predviđanjima neće i pored svih podozrivih očekivanja dovesti do smanjenja broja radnih mesta, nego će usled masovne primene IoT rešenja doći zapravo do veće uposlenosti radnika, ali sa potpuno drugačijim veštinama, kompetencijama i specijalnostima.

U prilog tome, mogu se navesti brojni primeri koji potvrđuju navedeni pravac i trend razvoja. U tom kontekstu, General Electric je u saradnji sa Intel-om kreirao IoT sistem za industrijska postrojenja, tzv. „Predix“ kako bi što veći broj industrija naveli na upotrebu njihovog tehnološkog rešenja u domenu pametnih industrijskih tehnologija.

Ukoliko bi se IoT integrisao u ceo lanac proizvodnje i snabdevanja, a ne samo u neke njegove delove i ne samo u pojedine kompanije, uticaj IoT na sektor industrije bio bi daleko veći i izraženiji.

Široka i masovna primena IoT ima dva primarna cilja:

- povećanje produktivnosti radne snage i
- uštedu na troškovima.

U praksi, industrijski IoT može ostvariti nove izvore prihoda, kao na primer u proizvodnji motora, gde proizvođač može da vrši prodaju motora i njihovo tehničko, inteligentno prediktivno održavanje. U celini posmatrano, prednosti IoT u poslovnom svetu su ogromne i direktno su zavisne od načina implementacije. Kako bi se stvorile veće mogućnosti za inovativne promene koje inače donose željene rezultate, od posebne je važnosti da kompanije od starta imaju potpun pristup većoj količini podataka o sopstvenim proizvodima i uslugama i unutrašnjem sistemu poslovne organizacije.

Najveći stepen iskorišćavanja primene IoT je evidentan u dva segmenta:

U industriji specifične namene - senzori koji olakšavaju proces proizvodnje u industrijskim postrojenjima, medicinski aparati za lečenje pacijenata i dijagnostikovanje bolesti, itd;

IoT uređaji koji su primenjivi u svim oblastima poslovanja - pametna klimatizacija, pametni bezbednosni sistemi (nadzorne kamere, senzori, alarmi i sl.)

Na tržištu globalnih IoT “igrača“ postoji nekoliko stotina kompanija. Međutim, globalni lideri i u ovoj oblasti su Google, Cisco, IBM, INTEL, Microsoft, Samsung, Apple, Oracle i dr.

Gotovo svaka od ovih kompanija, svoju viziju i misiju i pristup tržištu proizvoda i usluga bazira na IoT, usled čega marketinški afirmiše svoje proizvode „kao inteligentne sisteme, pametne uređaje, autonomne sisteme i sl.“, kako bi na taj način ostvarili tržišnu dominaciju i pobedili konkurenciju na temeljima svog rešenja.

U pogledu daljeg razvoja IoT tehnologije, stručna očekivanja idu u pravcu njenog povezivanja sa drugim naprednim tehnologijama, a u prvom redu sa 5G mrežom, preko koje je moguće povezati veliki broj senzora na relativno malom prostoru, što implicira uvećanje potrebe i efikasnosti IoT tehnologije. Vizija 5G predviđa mrežu koja nudi ultra širokopolasne i inteligentne mrežne komponente koje će smanjiti udaljenost u povezivanju ljudi i mašina na nulu, bez obzira gde se nalazili.

2.1.4 Mobilna telefonija

Početak razvoja mobilne tehnologije datira od poslednje decenije prošlog veka. Potrebe i razlozi nastanka ovog vida komunikacione tehnologije jesu povezivanje mobilnih uređaja kao što su ruteri i telefoni na mobilnu mrežu telekomunikacionog provajdera ili mobilnog operatera. Nakon povezivanja mobilne mreže i interneta, počeo je razvoj suštinske nadgradnje ove tehnologije koja se kao takva u nekoliko generacija razvijala u više pravaca.

Kao i sve druge bežične tehnologije, tako i mobilna tehnologija funkcioniše na sličan način. Osnovna svrha ove tehnologije jeste bežični prenos audio i vizuelnih signala sa jednog uređaja na drugi putem radiotalasne infrastrukture. Prenos signala se ostvaruje preko tzv. baznih stanica, odnosno primopredajnika instaliranih na tornjevima i visokim objektima. Jedna od temeljnih prednosti mobilne telefonije ogleda se u njenoj „prenosivosti“ i premošćavanju prostornih barijera. Način funkcionisanja ove tehnologije vrlo je jednostavan: mobilni primopredajnici emituju signale različitih jačina, frekvencija i standarda što omogućava mobilnu komunikaciju sa uređajima koji se nalaze u njihovom opsegu pokrivenosti.

Ukoliko je uređaj udaljeniji od bazne stanice, tj. ako su mobilni predajnici na većim rastojanjima, onda će i signal biti slabiji, što će direktno uticati na performanse IKT infrastrukture u pogledu prijema i slanja signala, odnosno brzine protoka.

U literaturi, mobilna telefonija se često poistovećuje sa celularnom tehnologijom iz razloga što se celularna mreža deli na hiljade preklapajućih geografskih zona i ćelija, gde se u centru svake ćelije praktično nalazi bazna stanica. Prednost ove tehnologije je u tome, što se umesto ulaganja u velike i skupe projekte tzv. „žičane“ tehnologije, koje podrazumevaju fizičku infrastrukturu nadzemnog i podzemnog tipa, danas može uz niži nivo troškova uspostaviti direktna veza između korisnika i provajdera, nezavisno od topografske konfiguracije područja i geografskih veličina.

U razvojnom smislu, mobilna telefonija se uporedo razvijala sa 0G tehnologijom (mobilna radio telefonija) iz koje je ubrzo nastala mobilna bežična telefonija 1G, koja je kompletno bila analogna i isključivo se koristila za prenos audio signala u komunikaciji.

Nakon jedne decenije razvoja te tehnologije, pojavila se 2G mreža u kojoj je signal postao digitalan i enkriptovan, a to je doprinelo i razvoju zaštićene komunikacije. U okviru 2G tehnologije, u široku upotrebu su ušle i kratke „SMS“ i slikovne „MMS“ poruke, a kasnije i internet servisi (GPRS) kao posledica direktnog povezivanja mobilne mreže i interneta.

Početak novog milenijuma, počinje razvoj treće generacije mobilne tehnologije, tzv. 3G. Ključna novina kod ove tehnologije je u tome što je njen fokus u potpunosti premešten sa „voice“ komunikacije na internet razmenu podataka. Osim toga, 3G tehnologija donela je i niz drugih novina: mogućnost video i konferencijskih poziva, IPTV usluge, „surfing“ i sl.

Krajem prve decenije 21. veka, na scenu stupa četvrta generacija mobilne tehnologije (4G) koja je učinila veliki iskorak u pravcu razvoja mobilnog širokopojasnog interneta bez ograničenja, što je do tada bilo isključivo rezervisano za optičke, kablovske i DSL mreže, organizovane od strane internet provajdera. To je doprinelo povećanju brzine u mobilnim mrežama u rasponu i do 100 Mbit/s, što spada u brzinski standard prisutan u najvećem broju zemalja širom sveta.

U toku je razvoj nove generacije mobilne telefonije poznatije kao 5G. Trenutno se ova tehnologija nalazi u eksperimentalnoj fazi, a početak njene primene očekuje se nakon 2020. godine. U odnosu na sve ranije generacije mobilnih mreža, 5G tehnologija ili 5G mreža ima

unapređene performanse čiji će kapacitet biti 10.000 puta veći od kapaciteta sadašnje mreže, a maksimalna brzina prenosa podataka i 10Gb/s, dok će brzina prenosa podataka na rubu prenosne ćelije biti 100 Mb/s uz kašnjenje prenosa manjeg od 1ms. (Electronics notes; 2019)

U okviru ove tehnologije, uporedo se razvijaju i različiti koncepti za mobilni sistem pete generacije, gde se posebno izdvajaju:

Sveprisutne mreže - u okviru ove tehnologije korisnik može biti povezan sa nekoliko bežičnih pristupnih tehnologija i bez prekida se kretati među njima.

Grupno kooperativno prosleđivanje - omogućava visoke brzine prenosa podataka u širem području ćelije, odnosno veći nivo interferencije sa manjim nivoom signala.

Kognitivna radio tehnologija - tehnologija koja pretražuje radio spektar, pri čemu bira optimalnu mrežu za radio pristup, modulacionu mrežu i ostale parametre za vlastito konfigurisanje radi uspostavljanja veze sa optimalnim performansama po inteligentnom kognitivnom principu.

Bežično mrežasto umrežavanje i dinamičko ad-hoc umrežavanje - sa primenom različitih pristupnih šema, moguće je uspostaviti vezu sa drugim obližnjim mrežama uz mnogo brži protok podataka.

Pametne antene - primena ovih antena omogućava da se menja smer signalnog snopa, što će doprineti uspostavljanju više paralelnih direktnih komunikacija i ujedno smanjiti interferenciju, a povećati sveukupni kapacitet ćelije.

Što se tiče rokova predviđenih za projektna istraživanja, uvođenje standarda i konačno razvijanje proizvoda, nisu fiksirani rokovi, ali pojedine kompanije koje pretenduju da budu lideri u ovoj oblasti samostalno su odredile vlastitu vremensku osu za 5G mrežu, kako bi mogle da pre drugih planski realizuju zacrtani projektni zadatak.

Prema predviđanjima nekih stručnjaka, korisni vek trajanja za 5G tehnologiju verovatno neće biti dug. Osnov za takva predviđanja predstavlja činjenica da je ova tehnologija primarno usmerena na uspostavljanje opšte povezanosti, kao i za komunikaciju IoT i M2M (machine to machine), usled čega će samo neke od ovih primena nakon uspostavljanja ipak opstati određeni niz godina.

U najboljem slučaju, procene za životni vek ove tehnologije dosežu do 2040. godine, za kada se očekuje naredna generacija mobilne tehnologije.

2.1.5 Društvene mreže

Društvene mreže predstavljaju online servise koji različitim korisnicima omogućavaju različite vidove komunikacije i lične prezentacije. Početak razvoja društvenih mreža vezuje se za 2002. godinu, kada su i zvanično započele sa radom kompanije Facebook i MySpace. To je danas jedan od najpopularnijih načina komunikacije posredstvom interneta i u velikoj meri zamenjuje pisanje e-mail poruka.

Pojedini teoretičari smatraju da društvene mreže predstavljaju „najmoćniji faktor uticaja na razvoj savremenog društva, pri čemu je taj fenomen poznat kao WEB 2.0 - računarska komunikacija“ (Bubanja, 2015:157).

Uvođenje tehnološke mogućnosti za komunikacije putem računara „Computer Mediated Communication - CMC“ zapravo je postavilo temelj na kome moderno doba i doba kompanija - društvenih mreža počiva. Prva komunikacija koja je utemeljila razmenu pisanih poruka bila je uspostavljena na asinhronom modelu, tj. modelu u kome komunikacija nije bila direktna i mogla je da se odvija u različito vreme između slanja i odgovora na poruku. E-mail komunikacija je primer asinhronog modela. Kasnije je razvijen i sinhroni model CMC-a, tj. online pisana komunikacija koja je evoluirala do nivoa koji danas razvijaju kompanije-društvene mreže i slične platforme za pojedinačne i masovne komunikacije između poznatih i nepoznatih osoba.

Unutar društvenih mreža treba razlikovati strukturu sastavljenu od pojedinaca koji se nazivaju „čvorovi“ koji su povezani specifičnim tipovima međuzavisnosti, kao što su vizije, ideje, finansijski interesi, prijateljstvo, zajednički interesi, znanje, prestiž, itd.

Značajno obeležje društvenih mreža u savremenom poslovanju zapravo je da su one provajderi različitih koncepata socijalnog povezivanja i udruživanja i da kao takve profilišu i ciljne grupe i interese. Time ove mreže istovremeno predstavljaju i kompanije sa svojevrsnim poslovnim modelom, koji kao takav ima veću nematerijalnu (intelektualnu), nego materijalnu (imovinsku) vrednost na tržištu, usled čega su ovi poslovni koncepti bitno izmenili sistem vrednovanja kompanija, pa se njihova vrednost više ne određuje prema fizičkoj imovini u nepokretnostima, tj. zakonima fizike, već vrednostima nastalim kao proizvod broja i aktivnosti njihovih korisnika i tako nastale intelektualne vrednosti.

Prema Leif Edvinssonu, nematerijalna imovina danas čini oko 90% vrednosti svih svetskih kompanija. Koliko god da se fokus virtuelne ekonomije u prethodnom periodu stavljao samo na nivo tehnološke promene, porast značaja i vrednosti informacija kao robe i značaj primene intelektualnog kapitala, dali su sasvim drugačije ključne dugoročne trendove i odrednice unutar ekonomije kakvu imamo danas, od one zasnovane na klasičnim principima i postulatima.

Ne tako davno, WEF je u saradnji sa web portalom *Visual Capitalist* izneo podatke o zastupljenosti društvenih mreža u 2018. godini, pri čemu glavni kriterijum nije bio ukupan broj registrovanih članova, već broj aktivnih korisnika na mesečnom nivou. (WEF; 2018)

Istraživački podaci iz ove studije pokazuju da je društvena mreža Facebook i dalje najpopularnija, a slede ga Youtube, WhatsApp, Facebook messenger, WeChat, Instagram, itd.

Dominacija Facebook-a bi mogla biti ugrožena, ili pak dovedena u pitanje zbog ekspanzije novih aplikacija za besplatno komuniciranje, kao i platformi zasnovanih na isključivo vizuelnim sadržajima. Upravo ovi novi „igrači“ na internetu stavljaju telekomunikacione gigante pred velike izazove, ukoliko žele da zadrže sadašnju poziciju. Primetan je povratak „grafičke“ komunikacije na štetu tekstualnih sadržaja, tako da se opravdano može postaviti pitanje: Da li se uz digitalnu tehnološku revoluciju odvija i svojevrsna komunikaciona „kontrarevolucija“ i degradacija?

U smislu iznetog, posebno zabrinjava „oskudica“ jezika praćena oskudicom razmišljanja o sadržajima koji se plasiraju na društvenim mrežama. Naime, danas korisnici radije kucaju poruke sa nepravilnim jezičkim skraćenicama, umesto obavljanja razgovora uživo, te isti najčešće šalju vizuelne, umesto tekstualnih sadržaja. U ovom pravcu, evidentna je prevlast raznih animacija, „smajlija“ i fotografija nad rečima, što prema mišljenju lingvista i pedagoga drastično utiče na povećanje opšte funkcionalne nepismenosti, ali i urušavanje pravilnih jezičkih formi i stila kulturnog ophođenja i izražavanja u sferi društvenog komuniciranja.²

² Zahtevi za brzim dopisivanjem uticali su na to da je jezik sadržavao dosta skraćenic, a znaci interpunkcije i veliko slovo sve manje poštuju. Na pravopis se obraća manja pažnja, jer je najvažnije brzo saopštiti svoje misli i ideje. Takav način dopisivanja se među mladima proširio i u svakodnevnom pisanju, pa je došlo i do slovno-numeričkih kombinacija, koje se u čitanju izgovaraju kao reč ili grupa reči, na primer, 4U umesto for you, 2gether umesto together, 2U umesto to you, sk8 umesto skate, itd. Obrazovni nivo i uzrast korisnika mnogo utiču na način korišćenja jezika. Kada tome dodamo i to da govornici kojima engleski nije maternji jezik prave greške iz neznanja i koriste jednostavan vokabular i gramatiku, dobijamo engleski kao sajber jezik koji je simplifikovana verzija standardnog engleskog jezika, bez konzistentne upotrebe gramatičkih pravila, interpunkcije i pravopisa. Sloboda u sajber prostoru znači i slobodan odnos prema jeziku. Posebne skraćnice vezane za internet nastale su zbog potrebe za brzim kucanjem poruka, ali takođe i iz želje da se objasni šta osoba oseća ili šta radi u trenutku kucanja poruke. I u telefonskoj komunikaciji nije bilo moguće preneti one male signale koji toliko doprinose kvalitetu razgovora oči u oči, facijalne ekspresije,

Među brojnim društvenim mrežama, na globalnom planu se posebno izdvajaju one koje prednjače po broju korisnika, a koje se izdvajaju i po različitom dijapazonu koncepata sadržaja, gde ti sadržaji zapravo predstavljaju generatore privlačenja korisnika. Iz tog širokog i razuđenog konglomerata, posebno se po osnovu navedenih kriterijuma i parametara izdvajaju sledeće društvene mreže: Facebook, LinkedIn, Twitter, Google+, Pinterest, Youtube, Instagram, WhatsApp, WeChat i dr.

Prvo mesto po broju aktivnih korisnika u svim starosnim grupama zauzima Facebook sa oko 1,56 milijardi logovanja na dnevnom nivou. Facebook je i društvena mreža sa najvećom globalnom popularnošću. Sa praktičnog aspekta, ova društvena mreža predstavlja virtuelno mesto gde svaki pojedinac može postaviti i organizovati svoj profil, razmenjivati poruke, objaviti statuse, ali i izabrati način predstavljanja i izražavanja svojih stavova, bilo pojedinačno ili u okviru grupa. U tom smislu, Facebook je idealno mesto za javno izlaganje, promociju i razvijanje „PR“ odnosa sa ciljnim grupama i pojedincima iz domena geografski i virtuelno široko rasprostranjene Facebook zajednice.

LinkedIn je po broju korisnika društvena mreža koja ima oko 590 miliona korisnika. Osnovna namena LinkedIn-a je povezivanje poslovne zajednice i zapošljavanje. Takođe, LinkedIn poseduje opciju za preporuke, pa je moguće zatražiti preporuku od partnera, kupaca i klijenata, kao i ponuditi svoje preporuke drugima. Osim toga, na ovoj društvenoj mreži se može otvoriti i poslovna stranica za kompaniju, tražiti novi radnici, predstaviti marketinški profil kompanije, itd.

Naredna je društvena mreža je Twitter sa preko 575 miliona korisnika. Twitter funkcioniše tako što omogućava korisnicima komunikaciju na temelju kratkih i jezgrovitih objava, takozvanih tvitova, od maksimalno 140 karaktera. Pored toga, Twitter je takođe pogodno mesto za pružanje korisničke podrške, jer se preko Twitter pretraživača mogu pretraživati svi javni tvitovi

ton glasa, grimase, govor tela, itd., a na internetu je smišljen način da se to brzo opiše. Postoje čitave liste ovih skraćenica, koje su se, budući da nisu ušle u neki standardni rečnik, menjale i proširivale vremenom. Uporedo sa tim razvijen je i ceo fond takozvanih emotikona koji vizuelno prikazuju ekspresije vezane za jezičke skraćenice, čime se ovaj fenomen dodatno usložnjava učiniivši to da je tako zapravo zaživela upotreba vizuelnih sredstava koja zamenjuju reči. Skraćenice koje smo pomenuli, a koje izražavaju osećanja i uopšte emocije koje hoćemo da naglasimo u vezi sa temom o kojoj se piše, sve više zamenjuju crteži lica koja prikazuju osećanja o kojima je reč. Kako su kasnih devedesetih godina SMS i internet postali raširena pojava, tako su se razvili i emotikoni. Reč emoticon nastala je od engleskih reči emotion i icon. Emotikoni su brzo postali popularni i koriste se u SMS porukama, imejlovima i internet forumima. Oni imaju formu grubog crteža nasmejanog ili tužnog lica dobijenog znacima interpunkcije - :-)) i :-(. Ove prve emotikone je predložio svom univerzitetu još 1982. Skot Falman, koji se bavio kompjuterskom naukom. Kasnije su dodavana nova osećanja, raspon emocija se povećao na nekoliko desetina i oni su postalajali sve složeniji. U Japanu, Koreji i Kini razvija se njihov stil crtanja emotikona. Upravo se na japanskim mobilnim telefonima 1999. godine razvija nova forma koja je danas dominantna, a to su emodži. Reč je poreklom japanska i znači piktograf (e - slika, moji - simbol). (Petković, 2018)

ogromnog broja korisnika, što podiže sposobnost brzog reagovanja između objavljiivača i njegovih pratilaca.

Google+ je društvena mreža u vlasništvu kompanije Google sa 395 miliona aktivnih korisnika na mesečnom nivou i preko 2 milijarde registrovanih korisnika. Najveća prednost ove društvene mreže jeste lakoća i jednostavnost njenog korišćenja, kao i efekatan vizuelni identitet. U prednosti ove društvene mreže možemo uključiti kvalitetnu interakciju klijenata i korisnika, budući da su korisnici podeljeni u krugove, tako da je kreirano više ciljnih grupa, što značajno olakšava komunikaciju među njima. Google+ društvena mreža ima odličnu integraciju sa Google pretraživačem, što daje poseban kvalitet i informativnost ovoj mreži korisnika uz jedan od najboljih načina da se izgradi brend kroz tutorijale i video blogove.

Pinterest je osnovan 2010. godine. Prema novijim istraživanjima i empirijskim pokazateljima, pinterest je najbrže rastuća društvena mreža za deljenje i slanje fotografija i video dokumenata i direktno je povezana sa Facebook-om i Twitter-om. Pinterest ima oko 200 miliona aktivnih korisnika na mesečnom nivou i oko milijardu kreiranih „tabli“, dok je do sada u okviru ove mreže kreirano preko 100 milijardi „pin“- ova.

Youtube je društvena mreža izuzetne popularnosti. Youtube na mesečnom nivou ima oko 1,5 milijardi aktivnih korisnika, 30 miliona aktivnih korisnika na dnevnom nivou i oko 5 milijardi video pregleda na dan, uz prosečan boravak korisnika na mreži od oko 40 minuta.

Instagram je društvena mreža, odnosno online platforma koja beleži izuzetan rast. Trenutno ima oko 800 miliona aktivnih korisnika na mesečnom nivou i oko 500 miliona dnevno aktivnih korisnika. Na dnevnom nivou na ovu platformu se aplouduje preko 95 miliona fotografija i oko 250 miliona priča (stories).

WhatsApp je takođe visoko rangiran po rastu kada su u pitanju online platforme sa svojih 700 miliona korisnika na mesečnom nivou, dok je na dnevnom nivou kod WhatsApp aktivno oko 320 miliona korisnika. Dnevno se registruje oko milion novih članova i putem ove platforme se razmenjuje oko 43 milijarde poruka dnevno.

WeChat je kineska aplikacija koja je nastala 2011. godine i spada u one platforme koje beleže izuzetno dinamičan rast i razvoj. O prethodnim platformama je već puno rečeno, dok se o aplikaciji, odnosno platformi WeChat u javnosti malo zna, pa ćemo joj se posebno posvetiti.

Nakon samostalnog početnog proboja na tržištu, WeChat se poslednjih godina nalazi u sastavu velike kineske tehnološke kompanije Tencent Holdings, pete po veličini kompanije na svetu, vredne oko 500 milijardi dolara. Vrednost ove kompanije beleži konstantan rast. Kao i WhatsApp, aplikacija WeChat se razvija u nekoliko pravaca i to: video isečci, glasovne poruke i video zapisi, kao i „Moments feeds“, što su objave nalik na one kakve ima Facebook.

Koristeći Tencent-ovu uključenost u „gaming“ sektor, odnosno sektor koji ima veliku perspektivu, WeChat je u svoju postojeću ponudu dodao i gaming integraciju, uz šta se WeChat uključio i u oblast digitalnih plaćanja, odnosno oblast u kojoj WhatsApp pokušava da ih prati na indijskom tržištu. Ukratko, raspon usluga kompanije WeChat osigurava funkcionalnost celog paketa aplikacija za svoju ogromnu korisničku bazu. Između ostalog, ta ponuda je proširena i između sudija i parničara u kineskim sudskim predmetima. Obzirom da ne mogu istisnuti sa zapadnog tržišta već izuzetno dobro pozicionirane mreže kao što su Facebook i Twitter, ova kineska kompanija u svojim razvojnim strategijama i planovima fokus daje na veliko tržište jugoistočne Azije i dalekog istoka. Drugi pravac prodora ove kompanije je ogromno i mnogoljudno tržište južne Azije koje obuhvata područje Indije, Bangladeša, Pakistana i Irana, gde po procenama menadžera ove kompanije postoje velike mogućnosti za ekspanziju, uprkos prisustvu mnogih drugih globalnih igrača iz Rusije, Evrope, SAD, itd.

Pored najvećih poznatih globalnih društvenih mreža, postoji čitav spektar manjih mreža lokalnog ili nacionalnog karaktera. Takve mreže najčešće imaju usko profilisane sadržaje, npr. muzičke, poslovne, zatim one namenjene objavljivanju kratkih poruka, pa sve do onih koje služe za razmenu informacija, video zapisa, fotografija, aplikacija i sl.

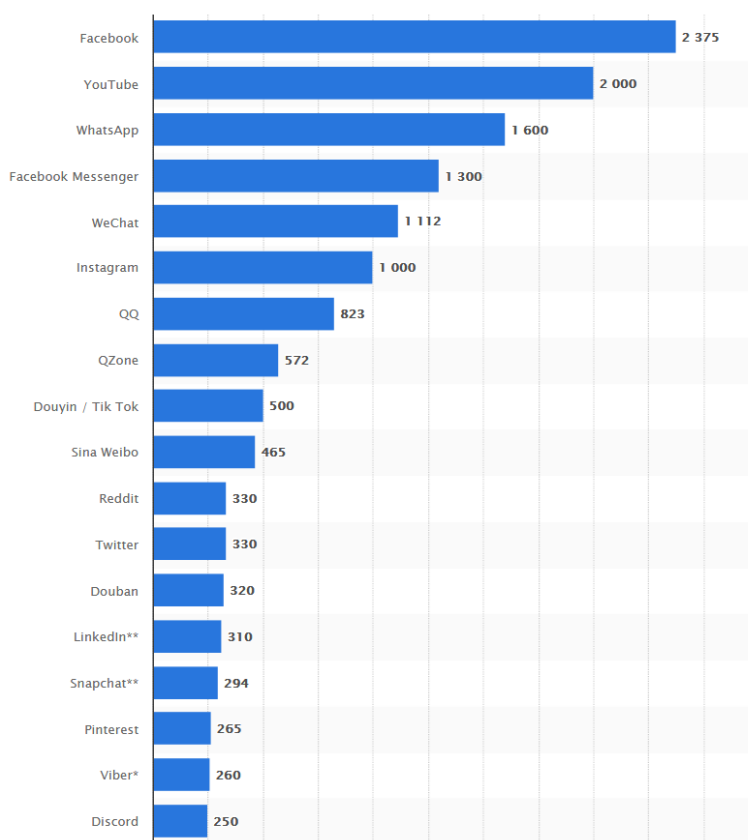
Među društvenim mrežama ovog tipa i nivoa, treba izdvojiti i Friendfeed koji predstavlja agregator, nalik klasičnim RSS čitačima i objedinjuje aktivnost kontakata sa različitih društvenih mreža, blogova i mikro-blogova. Najkraće rečeno, Friendfeed predstavlja način komunikacije gde korisnik bez posebnog adresiranja određenoj osobi šalje poruku ili obaveštenje svima.

Zanimljivo je istaći da se i starosna struktura korisnika društvenih mreža uveliko menja, tako da mladi nisu više jedini i najbrojniji korisnici, već im se priključuje i starija populacija, a u tom segmentu se po brojnosti posebno ističe generacija između 35 i 42 godine života.

Da se radi o veoma turbulentnim kretanjima po pitanju korisnika društvenih mreža i stalnom rastu broja aktivnih korisnika, pokazuje i statistički grafikon preuzet sa web

prezentacije www.statista.com iz koga se jasno vidi trend rasta u broju aktivnih korisnika, čak i u kratkom periodu između istraživanja urađenog juna 2018. godine i ovog istraživanja iz jula 2019. godine.

Grafikon br.2 Najpopularnije društvene mreže u svetu na dan 18.07.2019. godine prema broju aktivnih korisnika (u milionima)



Izvor: www.Statista.com

2.1.6 Računarstvo u oblaku (Cloud tehnologija)

Sušтина razvoja i primene Cloud tehnologije polazi od toga da se svi podaci koji su potrebni korisniku, bilo da su to aplikacije, dokumenti, hardver ili sl. budu dostupni u svakom trenutku, ukoliko je prethodno uspostavljena internet veza. Drugim rečima, Cloud tehnologija pruža mogućnost dostavljanja servisa umesto samog proizvoda. Zapravo, računarstvo u oblaku je podskup uslužnog računarstva sa konsekventnim prednostima resursa skalabilnosti i pouzdanosti, što se više smatra modelom poslovanja, nego određenom tehnologijom, jer se u klasičnom IKT okruženju, sve ono što se smatra proizvodom u uslužnom računarstvu tretira kao usluga.

Najširu definiciju, odnosno opis karakteristika, značenja isporuka usluga i modela primene računarstva u oblaku, data je u opisu Američkog Nacionalnog Instituta za standarde NIST. Prema NIST definiciji, računarstvo u oblaku je model za omogućavanje sveprisutnog, prikladnog, na zahtev, mrežnog pristupa zajedničkom prostoru podesivih računarskih resursa, (npr. mreže, davalaca skladištenja, aplikacije i usluge) koji mogu biti brzo alocirani i otpušteni sa minimalnom upravljačkom aktivnošću ili interakcijom davaoca usluge. Radi dodatnog obrazloženja, NIST navodi 5 ključnih karakteristika koje infrastruktura računarstva u oblaku mora posedovati:

- Samoposluživanje na zahtev
- Širok mrežni pristup
- Objedinjavanje resursa
- Rapidnu elastičnost
- Merljivu uslugu.

Verovatno najvažnija poslovna prednost upotrebe računarstva u oblaku jeste mogućnost „da platiš koliko troši“, gde korisnik plaća samo one resurse (procesori, radna memorija, kapacitet skladištenja, itd., koje stvarno koristi i u količini koju koristi).

Obzirom da analitički sistemi postaju sve više heterogeni, na cloud-u nisu samo tehnologije čija je osnovna funkcija skladištenje podataka, već i druge tehnologije vezane za analitike, reporting tehnologiju, serverless tehnologiju i tehnologiju obrade podataka. Iako se navedene tehnologije ubrzano razvijaju, stručnjaci smatraju da će upotreba cloud-a najviše dolaziti do izražaja kod prediktivne analitike. Smatra se da će „deep learning“, tj. u osnovi neuronske mreže sa višestrukim brojem skrivenih slojeva, drastično promeniti buduće poslovanje. Oblast u kojoj će primena ove tehnologije doći do svog maksimalnog izražaja jeste prepoznavanje slika.

Za razliku od brojnih naučnika i institucija, američki Nacionalni institut za standarde i tehnologiju dao je jednostavnu definiciju ovog fenomena koja se često citira i navodi u stručnoj literaturi. Prema ovom institutu: „Računarski oblak je model koji omogućava svuda prisutan pogodan mrežni pristup deljivim računarskim resursima (mrežnim serverima, skladištu podataka, servisima i aplikacijama), koji na zahtev korisnika i uz minimalnu interakciju sa isporučiocem mogu biti brzo stavljani na raspolaganje korisniku ili biti otkazani“ (NIST, 2011:2).

Primenom i razvojem pametnih telefona, e-mail servisa, društvenih mreža i sl., došlo je do naglog razvoja i široke primene Cloud tehnologije u različitim oblastima, ali i u različite svrhe. Razvoj koncepta računarstva u oblacima ili tzv. Cloud tehnologije, iako nije u potpuno nov, u velikoj meri je promenio tehnološku stvarnost usled svoje široke primene. Ova tehnologija omogućava korišćenje različitih, ponekad i raznorodnih informatičkih usluga na fizički udaljenim serverima, uz podršku internet mrežne infrastrukture i odgovarajućih internet protokola. Značajna prednost ove tehnologije u odnosu na klasičnu, jeste u tome što ona omogućava kompanijama i fizičkim licima da umanje početna ulaganja u opremu i aplikacije.

U stručnoj literaturi se navodi da suštinu ove tehnologije čini složena infrastruktura sastavljena od različitih informacionih, odnosno informatičkih tehnologija koje su po principu sinergetskog efekta povezane u jednu logičko-funkcionalnu celinu. U tehnološkom smislu, opisani sistem čine dva fizički odvojena dela: korisnički deo interfejsa ili „front end“ i drugi, infrastrukturni deo iz domena pružaoca usluga, odnosno dobavljača, koji predstavlja tzv. „back end“. Da bi sistem funkcionisao oba dela moraju biti povezana internet vezom.

U poređenju sa drugim tehnologijama, ova tehnologija ima pet ključnih karakteristika i to:

Pružanje usluge na zahtev korisnika – korisnik može samostalno da bira i pokreće izabrane računarske resurse, s tim da će usluge biti naplaćene u zavisnosti od vremena i obima korišćenja;

Širok mrežni pristup – sve usluge su praktično dostupne preko mreže, tako da im se može pristupiti preko različitih uređaja sa različitim operativnim sistemima;

Udruživanje resursa – infrastruktura koju obezbeđuje provajder može da kombinuje različite fizičke i virtuelne resurse, tako da može opslužiti više korisnika istovremeno;

Brza elastičnost – funkcionalnosti na oblaku mogu biti brzo aktivirane za potrebe povećanja ili smanjenja resursa za korisnika, po principu skalabilnosti;

Izmerena usluga – primenom odgovarajućih sistema moguće je proveriti i optimizovati upotrebu resursa u oblaku.

Računarstvo u oblaku se deli prema tipu i vrsti oblaka. Postoje tri tipa računarstva u oblaku i to:

- Softver kao usluga (SaaS)

- Platforma kao usluga (PaaS) i
- Infrastruktura kao usluga (IaaS).

Prema vrsti oblaka razlikujemo:

Javni oblak – reč je o oblaku putem koga provajder usluga iznajmljuje njegove resurse korisnicima i po obimu upotrebe naplaćuje korišćenje;

Privatni oblak – radi se o oblaku koji je napravljen isključivo za potrebe jednog klijenta, odnosno korisnika;

Zajednički oblak – sličan je javnom oblaku, a razlika je u tome što je on napravljen kao rešenje zatvorenog tipa za određenu zajednicu, odnosno grupu preduzeća koja imaju zajedničke zahteve, potrebe i ciljeve; i

Hibridni oblak – to je kombinovani oblak koji daje mogućnost korisniku koji je oformio svoj privatni oblak da postojeću infrastrukturu proširi uslugama iz javnog oblaka stvarajući jedinstven entitet (NIST, 2011:2-3).

Pored brojnih navedenih prednosti, Cloud tehnologija ima i niz slabosti i ograničenja koja se moraju uzeti u razmatranje prilikom donošenja odluke ili razvoja strategije poslovanja, a tiče se primene ove tehnologije u okviru postojećeg poslovnog modela. Analizirajući sve aspekte ove tehnologije, ključne slabosti Cloud tehnologije uključuju:

Zavisnost – kompanije koje koriste javni Cloud se oslanjaju isključivo na kompanije koje pružaju te usluge i oni su potpuno zavisni od prodavca ili distributera Cloud tehnologije;

Bezbednost – Cloud tehnologija je izuzetno ranjiva na spoljne pretnje, jer se podacima koji se nalaze u oblaku može pristupiti izvan virtuelnih bezbednosnih zidova sistema. Podaci pohranjeni u oblaku u slučaju nemarnih korisnika Web browsera postaju laka meta za krađu podataka i nastanak nenadoknadive štete i gubitaka. Osim toga, prodavac Cloud-a mora dati garancije korisniku u pogledu zaštite privatnosti podataka, kao i preuzeti obavezu da ti podaci ne smeju biti na bilo koji način kompromitovani ili izgubljeni;

Nedostatak referenci – zbog izraženog rizika po bezbednost podataka, kompanije pružaoci i primaoci Cloud usluga ne iznose detalje ili reference o upotrebi i dometima Cloud tehnologije koje koriste, niti o svojim poslovnim poduhvatima.

Od svih mana i slabosti vezanih za Cloud tehnologiju, pitanje bezbednosti podataka je najosetljivije i to je ključni faktor koji stvara rezerve i nedoumice kod korisnika prilikom opredeljivanja za pristup ovom tehnološkom rešenju u ovirima poslovne strategije. U tom smislu posebno se ističe jedan izuzetno važan aspekt bezbednosti, obzirom da nema garancija da pružalac usluga neće ukrasti, prodati ili na drugi način zloupotrebiti dokumente, podatke korisnika, logove o ponašanju i korišćenju aplikacija od strane korisnika na Cloudu.

U sklopu sprovođenja strategije jedinstvenog digitalnog tržišta i razrade planova digitalizacije evropske industrije, Evropska komisija (EK) je početkom 2016. godine donela niz mera radi uspostavljanja takozvanog „Evropskog oblaka“. Osnovni cilj ove inicijative jeste da omogući evropskim istraživačima i istraživačko-tehnološkom sektoru da dobije virtuelno okruženje za skladištenje, razmenu i ponovno korišćenje podataka, bez obzira na granice i područje nauke kojim se bave. Time se uspostavlja evropska informaciona infrastruktura koja će obuhvatati brze „broadband“ mreže, velike kapacitete skladištenja i superračunarske kapacitete za efikasan pristup velikim data bazama smeštenim u oblaku.

Kroz upotrebu savremene i sofisticirane tehnološke infrastrukture, Evropa će osigurati svoju poziciju u globalnoj trci sa drugim tehnološki jakim igračima na svetskom tržištu u skladu sa svojim ekonomskim i inovativnim potencijalom. U početku je predviđeno da će razvoj te infrastrukture obuhvatiti samo naučnu zajednicu u Evropi, kao i njene globalne partnere, ali sa tim da će se vremenom proširiti i na javni sektor i industriju. Navedena inicijativa je deo paketa mera EK za poboljšanje položaja Evrope na polju inovacionih informacija, za jačanje konkurentnosti i kohezije, te stvaranje jedinstvenog digitalnog tržišta u Evropi podržanog Cloud tehnologijom.

Praktični doprinos ove inicijative ogleda se u tome što će ona inovatorima i istraživačima značajno olakšati pristup potrebnim podacima, kao i njihovo ponovno korišćenje, a to će istovremeno smanjiti i troškove skladištenja podataka i napredne analize. Veliku korist od otvaranja pristupa u istraživačkom smislu imaju i novonastala preduzeća, kao i brojne javne službe na području medicine i javnog zdravstva, itd.

2.2 Drugi talas

Digitalno doba podržano naprednim digitalnim tehnologijama, nezadrživo ulazi u sve pore društva, ekonomije, javnog sektora, ali i sve oblasti ljudskog rada i delovanja. Sveopšti trend

digitalizacije, osim brojnih koristi na praktičnom planu, podstiče u inovativnom smislu razvoj novih naprednih tehnologija u odnosu na dosadašnje, sa različitim obuhvatima i nivoima primenljivosti.

Pod uticajem tzv. Industrije 4.0, odnosno digitalne transformacije, odvija se u širokom rasponu i na različitim tehnološkim nivoima i kontekstima, drugi tehnološki talas koji obuhvata 3D print, robotiku, dronove, nosive tehnologije, veštačku inteligenciju (AI), proširenu realnost (AR), itd.

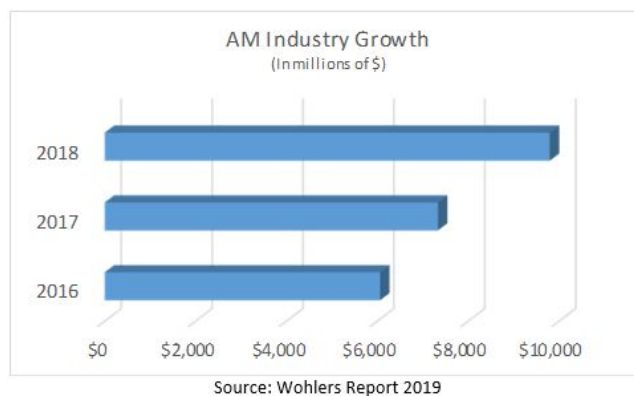
2.2.1. 3D printeri

Među tehnološkim dostignućima, poslednjih godina 3D štampa privlači sve veću pažnju, kako naučne i akademske javnosti, tako i poslovnog sveta. Perspektiva 3D print mašina koje mogu da štampaju predmete na isti način kao što to rade klasični InkJet štampači, inspirisala je brojne inovatore da ovu tehnologiju proglase začetnikom i nosiocem sledeće industrijske revolucije. Na drugoj strani, istraživači su reagovali skeptično i ukazali na trenutna ograničenja ove tehnologije i relativno nizak nivo njenog usvajanja.

Iako 3D štampa ima potencijal da „ometa“ način na koji se proizvodi projektuju, grade, distribuiraju i prodaju, može potrajati godinama pre nego što se taj uticaj oseti iznad ograničenog opsega robe. U razvijenim zemljama, 3D štampači su postali uobičajena pojava i alat za inženjere, dizajnere i arhitekte koji ih koriste za kreiranje dizajna proizvoda i njihovih prototipova (Wohlers Report 2012). U ovom izveštaju su po prvi put date iscrpne dubinske analize aditivne proizvodnje (Additive Manufacturing - AM) i 3D štampe u svetu, pri čemu se težište daje istorijatu ove tehnologije, aplikacijama, procesima, proizvodima i materijalima. Najkraće rečeno, AM je proces spajanja materijala za izradu objekata iz podataka 3D modela, obično „sloj po sloj“, za razliku od metoda izdvajanja iz proizvodnje.

AM proizvodnja najčešće se koristi za izradu fizičkih modela, prototipova, uzoraka, komponenti alata i delova proizvodnje u plastičnim, metalnim i kompozitnim materijalima, s tim da AM sistemi koriste tanke vodoravne preseke od kompjuterski podržanog dizajna (CAD), 3D-skeniranja sistema, medicinskih skenera i video igara za proizvodnju delova koje je jako teško ili nemoguće proizvesti na bilo koji drugi način.

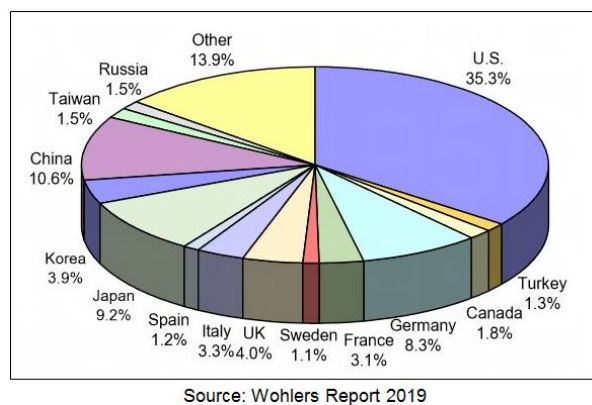
Grafikon br.3. Rast AM industrije na globalnom planu



U novije vreme, 3D štampa, podržana pratećom pametnom tehnologijom, dobija sve više na značaju u sektoru proizvodnje alata, kalupa, pa čak i finalnih proizvoda. Stručnjaci procenjuju da upotreba 3D štampača može dovesti do neviđenog porasta nivoa masovne potrošnje, smanjenja cena u lancima snabdevanja, pa čak i do svojevrsne „demokratizacije“ proizvodnje u kojoj potrošači i preduzetnici počinju da „štampaju“, odnosno proizvode svoje proizvode.

Broj kompanija koje proizvode industrijske AM sisteme je u porastu i to može biti zanimljiva metrika iz razloga što je to samo jedan od nekoliko korišćenih alata za merenje položaja zemlje u AM industriji. Najnoviji izveštaji potvrđuju da se u SAD proizvodi više od trećine svih proizvedenih industrijskih AM sistema. Takođe, SAD je „u vrhu istraživanja i razvoja u vezi sa hardverom, softverom, aplikacijama i AM uslugama u poređenju sa drugim zemljama u svetu: 10,6% u Kini i 8,3% u Nemačkoj, Japan 9,2%“, itd. (Wohlers Report, 2019).

Grafikon br. 4 Rast AM industrije i proizvodnje po zemljama u svetu



Dugoročno gledano, već nakon 2025. godine, pojedini tipovi i generacije 3D printera, npr. Bioštampanje živih organa, ima potencijal da produži ili spase mnoge živote. Sa ekonomskog

aspekta, procenjuje se da bi 3D štampa mogla da generiše ekonomski uticaj od 230-550 milijardi dolara godišnje do 2025. godine u aplikacijama koje su uveliko u primeni. Najveći iskorak i ujedno napredak u Bio-print tehnologiji ostvaren je u istraživanju matičnih ćelija. Uz pomoć ove tehnologije, matične ćelije se mogu oblikovati na način koji je visokoporozan na fleksibilne primene na planu regeneracije tkiva ili na substrate radi pristupa kapsularnim matičnim ćelijama značajnim za genomsku analizu u biomedicinskim naukama (Tasoglu, Demirci, 2013:1).

Danas 3D štampa može da kreira objekte iz različitih materijala, nezavisno od toga da li su u obliku praha, filamenata, tečnosti ili listova. Postoje različite tehnike 3D štampe od kojih svaka ima prednosti i nedostatke.

U pogledu masovne upotrebe, glavne tehnike uključuju selektivno lasersko sinterovanje, direktno lasersko sinterovanje metala, fuzionisano modeliranje taloženja, stereolitografiju, InkJet bio štampu i druge aditivne tehnike proizvodnje.

Prednosti 3D štampe u odnosu na konvencionalne metode su višestruke:

- Ideja može ići direktno iz datoteke sa kompjutera dizajnera do gotovog dela ili proizvoda, potencijalno preskačući mnoge tradicionalne proizvodne korake;
- Smanjuje se količina materijala koja se gubi u proizvodnji;
- Kreiraju se objekti koje je nemoguće proizvesti tradicionalnim tehnikama, a posebno objekti sa složenim unutrašnjim strukturama koje ojačavaju konstrukciju, smanjuju težinu i/ili povećavaju funkcionalnost.

Prema tumačenju Ministarstva energetike SAD, 3D štampa „ima potencijal da revolucionarno promeni proizvodnju, omogućavajući kompanijama (i pojedincima) da dizajniraju i proizvode proizvode na nove načine, istovremeno smanjujući materijalni otpad, štedeći energiju i skraćujući vreme potrebno za plasiranje proizvoda na tržište“(US Department of Energy, 2014).

Sadašnja ograničenja 3D štampe uključuju relativno malu brzinu gradnje, ograničenu veličinu objekata, ograničen detalj objekta ili rezoluciju, visoke troškove materijala, a u nekim slučajevima i ograničenu snagu predmeta. Međutim, poslednjih godina napravljen je veliki skok u redukciji ovih ograničenja.

2.2.2. Robotika

Robotika je jedan od temelja četvrte industrijske revolucije, iako se roboti u proizvodnji primenjuju više od 15 godina. Novina je u tome što nova generacija robota u umreženoj fabrici ima veći stepen veštačke inteligencije, usled čega roboti mogu putem pametnih uređaja komunicirati sa drugim mašinama i radnicima. Roboti su već opštepristupni gotovo u svim industrijskim sektorima, a posebno u auto i mašinskoj industriji, bolnicama, trgovinskim lancima, restoranima, pa čak i u ratom zahvaćenim područjima, dok nagli napredak u oblastima poput veštačke neuronske mreže, drastično smanjuje barijere između ljudi i mašina.

Tehnologija koja omogućava robotizaciju, temelji se na razvoju veštačke inteligencije koja u kombinaciji sa poboljšanim sensorima, nanotehnologijom i uopšte automatikom, dobija sve više na zamahu i primenjuje se u različitim oblastima. U praksi, uz pomoć te tehnologije, roboti mogu da naprave kompleksne proizvode i nauče da samostalno izvršavaju zadatke, pri čemu mogu i da funkcionišu i u neizvesnim i fluidnim situacijama. Kako se predviđa, do 2025. godine roboti će biti sposobni proizvoditi robu sa visokim kvalitetom i pouzdanošću, ispravljajući svoje greške u hodu.

Napredak u interfejsu, sensorima, aktuatorima u kombinaciji sa poboljšanim materijalima i ergonomskim dizajnom, unapređuje robotizovanu hirurgiju i dramatično povećava kvalitet i korisnost ljudskih proteza. Ultrapecizni hirurški roboti izvode najsloženije hirurške zahvate, čime doprinose razvoju novih oblika minimalno invazivne hirurgije koja može smanjiti postoperativne komplikacije, te pomoći bržem oporavku pacijenata i time smanjiti stope smrtnosti iz domena medicinskih, a naročito hirurških procedura. Približno 200 miliona velikih operacija se na ovaj način može obaviti svake godine u državama sa razvijenim zdravstvenim sistemima do 2025. godine.

Robotska protetika i egzoskeleti su u stanju da preduzmu precizne pravce, a time i preciznije i delikatnije pokrete. Razvoj novih interfejsa koji mogu da upravljaju robotskim udovima koristeći slabe električne signale, koriste u stvari signale iz nervnih završetaka, ili čak moždanih talasa. Sposobnost ove protetike može uskoro nadmašiti motoriku uobičajenih ljudskih pokreta.

Tehnološki napredak u ovoj oblasti, u kombinaciji sa opadajućim troškovima, daje potpuno nove mogućnosti za upotrebu robota. Brzina i stepen usvajanja naprednih robota određeni su mnogim faktorima, koji uključuju i uslove na tržištu rada.

Nova generacija sofisticiranih robota postaje komercijalno dostupna velikom broju korisnika u različitim sektorima. U odnosu na prethodnu generaciju, napredni roboti imaju veću pokretljivost, spretnost, fleksibilnost, prilagodljivost, ali i sposobnost da uče od ljudi i komuniciraju sa njima, uveliko proširujući svoj opseg potencijalnih primena. Takođe, ovi roboti imaju napredni softver za prepoznavanje slika koji im omogućava da pozicioniraju objekte za delikatne operacije i da raspoznaju konkretan deo među velikim brojem uzoraka.

Američka agencija za napredne istraživačke projekte (DARPA) „uveliko istražuje i primenjuje robote koji mogu u potpunosti automatizovati proces šivenja odeće, koristeći pri tome proces koji prati kretanje pojedinačnih niti i precizno pokreće tkaninu, kako bi se izvršilo precizno šivenje“ (Device Plus, 2018).

U skorije vreme, prema procenama Međunarodne federacije robotike, mnogi radnici u fabrikama biće zamenjeni automatizovanim uređajima, odnosno pametnim robotima, obzirom da će proizvodno biti efikasniji od ljudi i da će manje koštati. Roboti kao radnici su mnogo jeftiniji od ljudi: nema isplate zarada, toplog obroka, troškova prevoza, poreza i doprinosa, regresa, odsustva sa posla, godišnjih odmora, sindikata, itd.

Kako će se započeti trend automatizacije odvijati, najbolje ilustruju podaci da u fabrici u SAD radnik poslodavca košta 25 USD na sat, dok su troškovi za robota koji obavlja isti posao samo 8 USD po satu. Taj trošak do 2030. godine mogao bi zajedno sa proizvodnjom da padne na svega 2USD po satu. Stoga, nije teško zaključiti za koga će se poslodavci u budućnosti odlučiti: da li da ulože 35000 dolara u robota, ili da skupo plaćaju neefikasnog radnika na istom radnom mestu.

Niz drugih primera, naročito iz oblasti industrije, beleži trend robotizacije, tako da brojni proizvođači automobila kao što su američki Ford, General Motors, Chrysler (FCA), japanska Toyota, Mazda, Nissan, Mitsubishi, Honda, Suzuki, koreanski Hyundai i Kia, nemački Mercedes Benz, BMW, VW, Opel, francuski Renault, Peugeot, Citroen, italijanska FIAT grupa i dr. uvode potpuno automatizovane linije sa minimalnim brojem radnika, gde najveći deo poslova obavljaju roboti, ali još uvek pod nadzorom ljudi, što je slučaj i sa Fiat-ovom fabricom automobila poslednje generacije stacioniranom u Kragujevcu.

Iako robotika ostaje relativno mali deo globalnih ekonomija, ona je značajno doprinela rastu svetskog BDP-a. Čak 10% ukupnog svetskog rasta u poslednje 22 godine doprinos je robotike. CEBR studija (Redwood Software and the Centre for Economic and Business Research) iz marta

2017. godine, pokazala je da ulaganje u robotiku ima veći pozitivan uticaj na ekonomiju, nego razvoj sektora kao što su informaciona tehnologija, građevinarstvo ili nekretnine, čak iako se uzme u obzir da svi ti sektori imaju koristi od ekonomije obima sa kojom se robotika ne može porediti.

Prema analizi WEF koja je urađena u 15 razvijenih zemalja koje zapošljavaju 65% svetske radne snage, procenjuje se da će do 2020. godine više od 7 miliona radnih mesta nestati zbog uvođenja automatizacije i robotizacije u proizvodnju, u kojoj je već do sada angažovano oko 1,8 miliona robota. U istom periodu procenjuje se da će 2 miliona poslova biti otvoreno, dok će preko 7 miliona radnih mesta zameniti tehnološka rešenja ili će postati nepotrebna, što znači da će 5 miliona radnih mesta biti ugašeno. Istovremeno, nestaće više od 15 današnjih zanimanja, prvenstveno u medicinskom i finansijskom sektoru. Gledano po sektorima, najveći udarac može očekivati zdravstveni sektor zbog eskpanzije telemedicine, a onda slede energetska i finansijske usluge. Takav trend izazvaće velike promene na tržištu rada, pa se očekuje da će čak 65% učenika u osnovnim školama u budućnosti raditi u zanimanjima koja sada ne postoje.

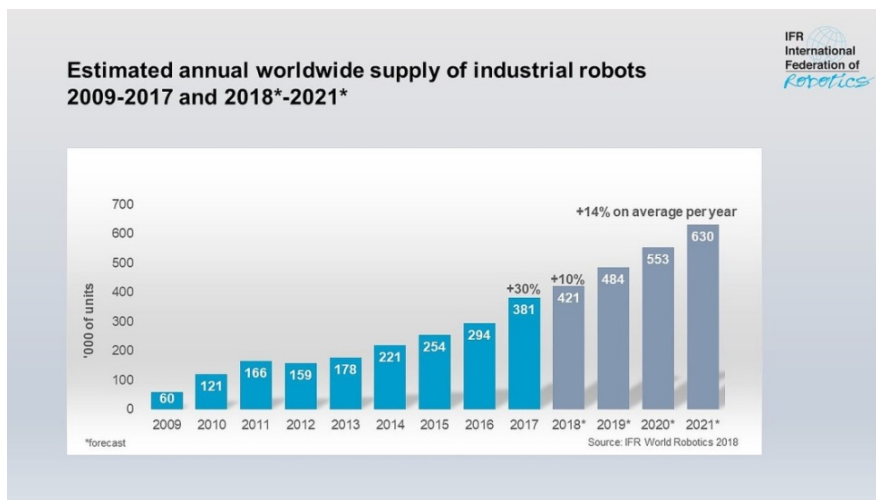
Dubinska istraživanja Univerziteta Oxford jasno ukazuju da će zbog razvoja robotike u narednih 20 godina čak 35% poslova biti pod rizikom opstanka. Najugroženija su ona radna mesta na kojima se ponavljaju radnje rutinski, a pre svega to se odnosi na poslove gde će roboti uveliko zameniti ljude u građevinarstvu, mesnoj industriji, transportu, obezbeđenju, administraciji i sl.

Za sada nisu ugroženi poslovi u kojima je potreban veći stepen kreativnosti, poput umetnosti, muzike, dizajna, zabave i sl. Na simpozijumu o budućim trendovima u razvoju robotike održanom 2015. godine u Međunarodnom izložbenom centru u Tokiju, predstavljena je strategija sa planom sprovođenja razvoja robotike, sa ciljem da se steknu prednosti nad drugim vodećim ekonomijama, među kojima su i SAD i Nemačka, čime će se otvoriti vrata za potpunije uvođenje četvrte industrijske revolucije. Istraživački institut Micuho Katcujukija Hasegave smatra da Japan u svetu predvodi u razvoju i primeni industrijskih robota, a japanska vlada je strategiju rasta postavila kao „Robotsku revoluciju“. Japan je jedan od najvećih proizvođača robota i robotske tehnologije u svetu. Vlada Japana je koncentrisala napore u pravcu razvoja robota koji će međusobno moći da kontaktiraju preko interneta.

Novi izveštaj „World Robotics - Industrial Robot Report 2018“ registruje povećanje od 30% isporučenih robota u odnosu na prethodnu godinu, kao i da se godišnji obim prodaje industrijskih

robota povećao za 114% u poslednjih 5 godina. Ukupna vrednost prodaje robota porasla je za 21% u poređenju sa 2016. godinom, što je rezultirano novim rekordom od 16,2 milijarde dolara u 2017. godini.

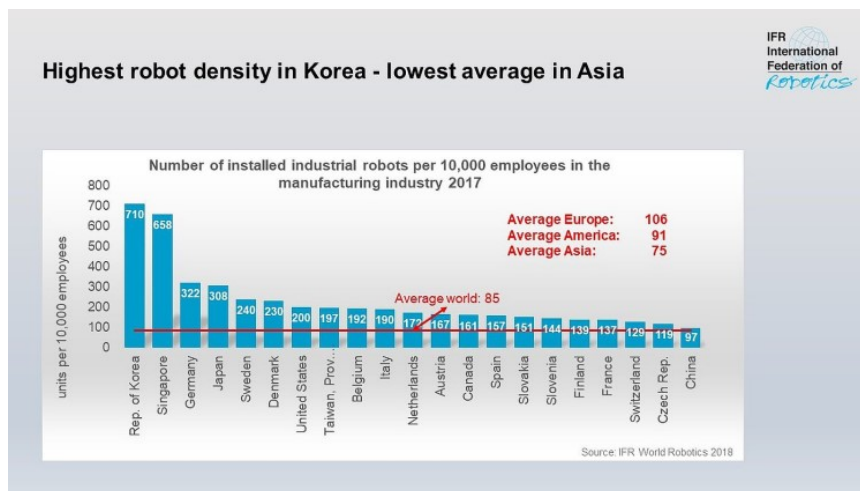
Grafikon br.5. Procenjena godišnja ponuda industrijskih robota



Izvor: IFR, World Robotics 2018

Rezultat takve ekspanzije u proizvodnji i distribuciji robota doveo je do potpuno nove gustine primene ove tehnologije u proizvodnim delatnostima. Na globalnom planu, ustanovljen je novi prosek koji iznosi 85 robota na 10000 zaposlenih, a regionalno, u Evropi ta gustina iznosi 106 jedinica, SAD 91 i Aziji 75, što potvrđuje paradoks da regija koja najviše proizvodi robote ima nižu prosečnu gustinu u primeni industrijskih robota.

Grafikon br. 6 Broj industrijskih robota na 10.000 zaposlenih u proizvodnji u 2017. godini



Izvor: IFR World Robotics 2018

U odnosu na druga područja, mogu se izdvojiti četiri najveća tržišta u svetu koja čine 73% ukupnog nivoa prodaje robota u 2017. godini:

- Kina
- Japan
- Južna Koreja i
- Nemačka.

Kada se razmatraju industrijski sektori gde su najviše primenjeni roboti, izdvajaju se tri industrijska sektora i to:

Automobilska industrija - sa udelom od 33% ukupne ponude u 2017. godini, gde je zabeležen porast prodaje za 22%;

Elektronska industrija – sustiže auto industriju, pri čemu je prodaja povećana za 33%, dok udeo u ukupnoj ponudi 2017. godine iznosi 32%

Metalna industrija – nalazi se u usponu. Procenat ukupne ponude dostigao je 10%, uz izuzetan rast prodaje od 55% u 2017. godini (IFR World Robotics, 2018).

Između ostalog, nedavno su prikazani i roboti najnovije generacije koji automatski vrše merenje telesne temperature i krvnog pritiska putem zgloba prislonjenog na internet terminal, uključujući i nove robote koji gase požar, deminiraju prostor ili izvršavaju posebne borbene zadatke u realnim ratnim uslovima.

Usvajanje napredne robotike u narednom periodu, nailazi na različite izazove i prepreke. I pored smanjenja troškova, većina industrijskih robota, kao i mnogi komercijalni, za usluge ostaju i dalje skupi. Za usvajanje industrijskih i uslužnih robota u velikom obimu, treba izdvojiti 1,1-1,6 triliona dolara do 2025. godine.

Mogućnost nabavke hirurških robota je još više sužena, obzirom na njihovu visoku cenu, kao i nedostatak stručnih kadrova za njihovo opsluživanje. Nasuprot tome, koristi od napredne robotike su nemerljive, obzirom da će njihova primena doneti veliku vrednost za proizvođače robota, pružaoce zdravstvenih i drugih usluga, preduzetnike, potrošače i konačno celo društvo.

Za mnoge kompanije, napredna robotika pruža priliku za veliko smanjenje troškova rada, veću fleksibilnost i smanjenje vremena za isporuku proizvoda i usluga na tržište. Među kompanijama i dalje će postojati dilema da li da se suoče sa izazovima punog poboljšanja produktivnosti i

kvaliteta koje donose napredni roboti, ili se držati starih oprobanih načina i modela privređivanja. Neizvesnost oko toga i dalje postoji, tim pre što robotika zahteva značajna kapitalna ulaganja, a menadžmentu kompanija će biti potrebni jasni dokazi o pozitivnom povratu investicija. Bilo koja forma rekonfigurisanja poslovnih procesa, kanala za isporuku usluga i lanaca snabdevanja je teška i dugotrajna, a obuka zaposlenih složena, dugotrajna i skupa.

Za ekonomije i kreatore politika, mogućnosti savremenih tehnologija i inovativnih rešenja, a posebno u domenu upotrebe napredne robotike, donose brojne potencijalne koristi. Rastuća produktivnost, povećana konkurentnost, kvalitetniji proizvodi i usluge, sigurnije operacije i bolji kvalitet života starijih i invalida, benefiti su ove tehnologije. Primetan je trend da širenje robotike stvara nove mogućnosti za zapošljavanje radnika sa visokim stepenom stručnosti, prvenstveno onih koji imaju tehnološko-informatička i inženjerska znanja i veštine.

2.2.3. Dronovi

Dron je sofisticirana bespilotna letelica koja može da se kreće, ili daljinski upravljana, ili korišćenjem računara i veštačke inteligencije. U početku, dronovi su isključivo korišćeni u vojne svrhe, ali vremenom njihova primena se razgranala u pravcu zaštite i spasavanja, topografskog snimanja i merenja prostora, zatim u policijskom radu, u radu vatrogasnih službi, agrokulture i sl.

Sa mogućnošću dosezanja nepristupačnih mesta ili destinacija, koje uzgred rečeno mogu biti rizične ili udaljene, dronovi su omogućili ljudima da ipak mogu da snimaju, kontrolišu ili obavljaju određene operacije širom planete. Porast broja bespilotnih letelica je toliko brz da se novijim studijama predviđa rast globalnog tržišta za poslovne usluge koje koriste dronove u visini od 127 milijardi dolara.

Zbog brojnih prednosti koje omogućavaju svojim korisnicima, dronovi se sve više koriste u korporativnom pejzažu, omogućavajući masovno prikupljanje podataka, nabavljanje slika i drugih osetljivih informacija u gotovo realnom vremenu. Spisak kompanija koje koriste tehnologiju drona se stalno širi. Na primer, „telekomunikacione kompanije koriste dronove da bi obezbedile privremeno pokrivanje internetom bojnih polja, zona katastrofa i oblasti do kojih se teško stiže radi operacija potrage i spasavanja“ (Internet ogledalo, DATA, 2019:22).

Međutim, sve češća primena drona je u sektoru isporuke i transporta za dostavljanje različitih pošiljki u udaljene i nepristupačne destinacije. Pored toga, i aviokompanije koriste tehnologiju

drona za obavljanje ispitivanja oštećenja mašina i infrastrukture, a pametnu navigaciju i kompjuterski prikaz koriste za dobijanje preciznih podataka sa teško dostupnih mesta.

Zahvaljujući ogromnom napretku tehnologije, dronovi se danas koriste za prikupljanje podataka, mapiranje, isporuku robe, igre i mnoge druge radne procese. Istraživanja sugerišu da postoji „deset potencijalnih područja gde se dronovi koriste u većem obimu:

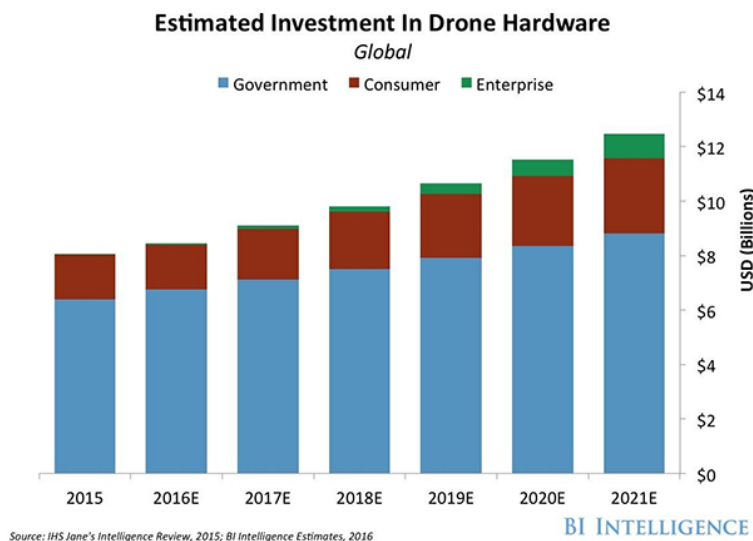
- Odbrani
- Upravljanju zaštitom i spasavanjem u slučaju prirodnih nesreća ili katastrofa
- Urbanom planiranju
- Praćenju ugroženih vrsta i biodiverziteta
- Zdravstvenoj zaštiti
- Poljoprivredi
- Prognozi vremena
- Upravljanju otpadom
- Rudarstvu
- Telekomunikacijama“, itd. (Geospatial World; 2018).

U novom izveštaju Business Insider, date su prognoze za prihode od prodaje dronova za vodeće proizvođače i kompanije u svetu. Pored toga, data je i projekcija predviđenog rasta u isporukama bespilotnih letelica do 2021. godine, koji uključuju sledeće parametre:

- Prihodi od prodaje dronova do 2021. godine dostići će 12 milijardi dolara, što je daleko više od 8 milijardi dolara kojiko je to bilo u 2017. godini;
- Isporuka dronova tokom sledećih 5 godina će se učetvorostručiti zbog sve veće tržišne konkurencije i novih tehnologija koje olakšavaju proizvodnju dronova;
- Rast preduzetničkog sektora premašiće potrošački sektor, kako u isporukama, tako i u prihodima, budući da regulatorni okvir otvara široke mogućnosti upotrebe dronova u SAD i EU;
- Tehnologije kao što su „geo-fencing“ i „collision avoidance“ učiniće letove dronovima bezbednijim, a regulatorni okvir dostupnijim za masovnu upotrebu dronova;
- Federalna vazduhoplovna agencija (FAA) ograničava komercijalne letove za nekoliko odabranih industrija i aplikacija, kao što su snimanje iz vazduha u sektoru poljoprivrede, rudarstva, nafte i gasa;

- Vojni sektor i dalje prednjači u odnosu na druge sektore u upotrebi dronova, zahvaljujući visokim troškovima i sve većem broju zemalja koji dronove žele imati u svom vojnom arsenalu.

Grafikon br.7 Procenjene investicije u proizvodnju hardvera za dronove



Izvor: BI inteligence, 2016

U sklopu vojno-industrijskog kompleksa, ubrzano se razvija posebna vrsta dronova, tzv. trutova, koji se u vojnoj leksici poistovećuju sa letećim robotima. Prema dostupnim podacima, u SAD ima više od 11000 takvih aparata, ali se tehnologija širi velikom brzinom i postaje cenovno pristupačna, kako vojnim, tako i policijskim i drugim bezbednosnim subjektima, ali i ostalim zainteresovanima. Zanimljivo je istaći, kako pokazuju policijski izveštaji u SAD, da se u novije vreme ovi sofisticirani aparati koriste i u kriminalnim krugovima radi špijuniranja ili eliminisanja konkurencije.

Uporedo sa vojnom, raste i komercijalna upotreba dronova. U novije vreme, dronovi, naročito u zapadnoj hemisferi, našli su široku primenu u agrokulturi, građevinskoj industriji, te industriji prostornog upravljanja. Štaviše, dronovi su brzo postali jedna od galopirajućih industrija koju investitori rado prate i u koju ulažu kapital, znajući da će se on vratiti.

Ako se uzme u obzir skokovit rast ove tehnologije, može se očekivati da će cena dronova postepeno padati, čineći tu tehnologiju još dostupnijom širem potrošačkom krugu. Najveće ograničenje za masovnijiu primenu dronova predstavljaju međunarodni nacionalni regulatorni

okviri koji ne dopuštaju letenje iznad određenih područja u kojima su vojni objekti i instalacije, razvojni centri, ključni objekti kritične infrastrukture, urbani centri, vladine institucije, itd.

Obim zabrana i ograničenja u ovom segmentu varira od jedne do druge države, što nameće potrebu integrisanog pristupa, a to znači usvajanja međunarodnih standarda i propisa iz ove oblasti koji će biti primenjivi i obavezujući za sve.

2.2.4. Nosive tehnologije

Među različitim i sve popularnijim tehnološkim trendovima koji će obeležiti godine pred nama, jeste i trend takozvanih „Nosivih tehnologija“, odnosno proizvoda koji su kombinacija sa odevnim predmetima i ugradnim elektronskim tehnologijama.

Pojedini analitičari smatraju da bi takvi pametni uređaji mogli zameniti pametne telefone kao glavne komunikacione uređaje, te predviđaju i da će za par godina sve veći broj ljudi, umesto mobilnih telefona koristiti satove i naočare.

Specijalno dizajnirane naočare o kojima se sve više diskutuje i piše u stručnoj, ali i široj javnosti, mogle bi u budućnosti promeniti način na koji ljudi komuniciraju ili pretražuju informacije na internetu i društvenim mrežama, upravo zbog činjenice da ova tehnologija omogućava prikazivanje sadržaja na ekranu ugrađenom u sočivo naočara.

Druga tehnologija je vezana za uređaje za prepoznavanje govora sa kojih se odmah putem glasa može odgovoriti na poziv direktno iz naočara, bez pomoći drugih tehnoloških sredstava. Veliko interesovanje izaziva i pametni sat, koji, kada je povezan sa mobilnim telefonom, omogućava prikazivanje informacija poput SMS poruka, obaveštenja sa društvenih mreža, mejlova i poziva, tako da nema potrebe uzimati mobilni telefon, već se na ekranu sata može videti aktuelni poziv ili poruka.

Pored gedžeta, očekuje se da će se nosiva (wearable) tehnologija najčešće primenjivati u sklopu odeće, kao na primer: majice sa čipovima i sensorima koji prate otkucaje srca, pritisak i te informacije šalju na obližnji mobilni uređaj putem bežične tehnologije, kako bi taj uređaj izvršio softversku analizu putem posebnih i specijalizovanih aplikacija.

Ove tehnologije našle su široku primenu u oblasti zdravstva, pri čemu će aplikacija odmah obavestiti korisnika i zakazati mu pregled kod lekara i istovremeno lekaru poslati sve obrađene

podatke i analize vezane za korisnikovo zdravstveno stanje koje je softverski ocenjeno kao adekvatno za angažovanje lekara.

Pored primene u zdravstvu, nosiva tehnologija, odnosno odeća sa sensorima, ima širok spektar primene i u oblasti sporta, obzirom da može pratiti aktivnosti sportista u realnom vremenu i tako ih upozoravati na pogrešno izvedene vežbe ili poteze i putem mobilne aplikacije im pokazati kako pravilno to treba uraditi.

Američka kompanija Motorola, nedavno je predstavila pilule i posebne tetovaže koje šalju signale koji služe kao pristupne šifre za računare, smart telefone i online servise, ali je ta tehnologija još uvek u eksperimentalnoj fazi.

Veliku pažnju i interes primene uređaja iz kategorije nosive tehnologije predstavlja i I-watch kompanije Apple koji se nedavno pojavio na tržištu. Kako očekuju pojedini analitičari, ovaj proizvod bi mogao pokrenuti trend razvoja ovih uređaja, obzirom na njihovu pristupačnu cenu. Zanimljiva tema u vezi sa tržištem nosive tehnologije je i to koliko će ona daleko odvesti računarsku industriju od zone komfora i kakve će rezultate to doneti. U suštini, 4 tehnologije u nastajanju odvešće tržište nosive tehnologije daleko napred i tako učiniti značajan doprinos kvalitetu života ljudi.

Ključni korak koji će omogućiti nosivoj tehnologiji da napreduje, jeste da ona pređe na bežično punjenje – jednostavnije rečeno, bežični talasi biće i više nego što je dovoljno za pristup.

Drugi tehnološki korak predstavljaju savitljivi ekrani koji omogućavaju da prenosivi proizvodi budu podesivi tankom zglobu, širokom vratu i kratkom torzou.

Treći stub razvoja su snažniji senzori – dizajnirani da mogu u svakom trenutku brojati korake, meriti otkucaje srca, i dr.

Najzad, četvrti, veliki upozoravajući prikazi podataka, gde se predviđa više moćnih senzora koji bi prikazali daleko veće količine informacija i iste obradili i prosledili korisniku.

U većini slučajeva, tehnološka strana tržišta prenosivih uređaja jednostavno zahteva ono što tehnološka industrija u ovom trenutku najbolje radi: minijaturizaciju, integraciju i inovaciju. Gledajući napred, inženjering povratne sprege uključivaće npr. modne dizajnere i vlasnike butika. Tehnološka industrija će time praktično biti gurnuta na tržište čiji je osnovni moto i prvo

pitanje: „da li mi ovo dobro stoji?“, a tek posle toga će se razmišljati na način „da li mi ovo treba?“

Idući talas inovacija ne odnosi se na prebacivanje podataka sa jednog mesta na drugo, već na povezivanje fizičkih objekata sa internetom na do sada nezabeleženom nivou. Sve je veći broj uređaja povezan sa košuljama, naočarima, satovima, nakitom i sl., što omogućava širok bežični spektar ili takozvani mrežni kapacitet na planu rasta mobilnog saobraćaja. S tim u vezi, Scott R. Peppet, profesor na pravnom fakultetu univerziteta Colorado, u tekstu objavljenom u Texas Law Review 2014. godine (Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent) upozorava da brojni mali i masovno proizvedeni uređaji koji sadrže IoT ne doprinose većoj zaštiti bezbednosti i privatnosti.

Nosiva tehnologija (Wearable Technology) zapravo obuhvata svu elektronsku tehnologiju sa pratećim softverom koja je nosiva na ljudskom telu. Početni razvoj ove vrste tehnologije činili su pametni satovi i narukvice. Kompanija Google je među prvima lansirala nosivi uređaj, odnosno „Android wear“ verziju operativnog sistema koji je prilagođen i optimizovan upravo za ove uređaje. Najveći stepen tržišne penetracije zabeležen je kod nosivih uređaja koji sadrže rešenja koja prate aktivnosti čoveka (broje korake, mere puls i sl.).

U pogledu razvoja nosive tehnologije, velike korporacije kao što su Huawei, Samsung, Sony, LG i dr., izbacili su na tržište veliki broj raznih sprava, Gadget-a kojima je softver na mobilnim uređajima omogućio perspektivu i ubrzani razvoj. Nakon nekoliko godina, mnoštvo manjih firmi vođenih uspehom velikih kompanija, kreirće nove gedžete i na taj način se probijati na tržištu.

2.2.5. Veštačka inteligencija

Veštačka inteligencija (Artificial Intelligence-AI) podrazumeva računarske sisteme koji prikupljaju, interpretiraju i uče iz unetih podataka, kako bi izvršili specifične zadatke i ostvarili postavljene ciljeve. U odnosu na prirodnu ljudsku inteligenciju, AI je veštačka forma inteligencije ispoljena kroz rad mašina. Kako se računarska snaga ubrzano povećava tokom poslednjih godina i sposobnosti AI su takođe dramatično porasle. Istraživači sa Univerziteta Oxford i Univerziteta Eindhoven u svom istraživanju koje su sproveli tokom 2016. godine ukazuju da postoji 50% verovatnoće da će sposobnosti AI premašiti ljudsku inteligenciju u periodu 2040-2050. godine (Muller, Bostrom, 2016:553-571).

Ciljevi veštačke inteligencije su mnogobrojni, a među njima su najvažniji sledeći: „da odmeni ljudski mozak u svim funkcijama koje mogu da se obavljaju uz pomoć mašina, pri čemu se ove funkcije izvršavaju neuporedivo brže i tačnije nego kada bi to radio čovek“ (Branković, 2017:17).

Drugi tehnološki eksperti predviđaju da će se to dogoditi mnogo ranije. Budući da AI stalno uči i napreduje, novi oblik AI super inteligencije može se pojaviti već tokom naredne decenije i predstavljaće u postojećim razmerama pravi kvantni skok. AI tehnologije su značajno napredovale tokom poslednjih godina i njihov dalji razvoj takođe prati taj trend, ali primena prilično zaostaje za inovacijama. Brojni primeri iz prakse pokazuju da AI može transformisati brojne poslovne aktivnosti i da ima potencijal da fundamentalno promeni druge. Isto tako, AI može oblikovati različite funkcije u celom lancu vrednosti u potpuno različitim sektorima.

Za primenu AI tehnologije, pored korporacija, start-up(ova), veoma su zainteresovane i vlade i društvene institucije. Uzimajući u obzir iskustva, kompanije koje usvajaju AI u obimu i u ključnom delu svog poslovanja, već registruju potencijal ove tehnologije, a one koje sprovode proaktivne AI strategije očekuju još veće koristi.

Navedene činjenice sugerišu da AI može dati kompanijama značajne konkurentske prednosti, ali samo za one koje su potpuno posvećene punoj primeni ove tehnologije. Međutim, da bi ispunila očekivanja kompanija, AI će morati da pruži ekonomske efekte primene koji značajno smanjuju troškove, povećavaju prihode i iskorišćenost imovine, infrastrukture i uopšte biznis kapaciteta kompanije.

U postojećem izuzetno tehnološki razuđenom poslovnom svetu, sa različitim nivoom tehnološke situiranosti, AI ima i različite stepene relevantnosti za pojedine sektore industrije, sa različitim spektrom mogućnosti da se AI tehnologija primeni.

Stvaranje vrednosti AI tehnologija ostvaruje u nekoliko oblasti:

Projekcija i prognoza – kompanije moraju stalno da predviđaju budućnost da bi stekle konkurentsku prednost. U tom smislu AI omogućava kompanijama bolje prognoze za njihov lanac snabdevanja i bolje dizajnirane ponude. Očekuje se „da će se troškovi vezani za transport i skladištenje smanjiti za 5-10%, a za administraciju lanca snabdevanja za 25-40%.

Sa primenom AI ukupna smanjenja zaliha od 25-50% su izvodljiva“(McKinsey&Company; April 2017).

Proizvodnja ili transformacija inputa u rezultate - AI može da pomogne kompanijama da proizvode kontinuirano, optimizujući sredstva i procese, organizujući najbolje timove ljudi i mašina, poboljšavajući kvalitet i pouzdanost i sprečavajući zastoje u održavanju, a sve to zajedno povećava produktivnost. Očigledna uloga AI je da zameni ljude kroz proces poslovne automatizacije.

Kreiranje vrednosti - je treća oblast u kojoj AI dolazi do izražaja putem promocija i marketinških ponuda, po pravoj ceni, sa ciljanom porukom, usmerenom prema ciljnoj grupi.

Poboljšanje korisničkog iskustva i stvaranje novih izvora vrednosti - četvrta je oblast u kojoj AI omogućava da korisnici budu bogatiji, prilagođeniji i praktičniji.

Stvaranje baze lojalnih klijenata - je jedan od načina da se podstaknu i povećaju prihodi, a to se jedino može postići uz podršku AI tehnologije kao što je kompjuterski vid i mašinsko učenje, obzirom da povećava korisnička iskustva za širi krug ljudi.

Mogući uticaji veštačke inteligencije na društvo i radnu snagu poslednjih godina su opsežno istraživani i proučavani sa različitih aspekata. Iako AI ima potencijal da fundamentalno preoblikuje društvo i ekonomiju, ostaje značajna neizvesnost oko toga kako će se sama tehnologija razvijati, u kom pravcu i sa kakvom dinamikom.

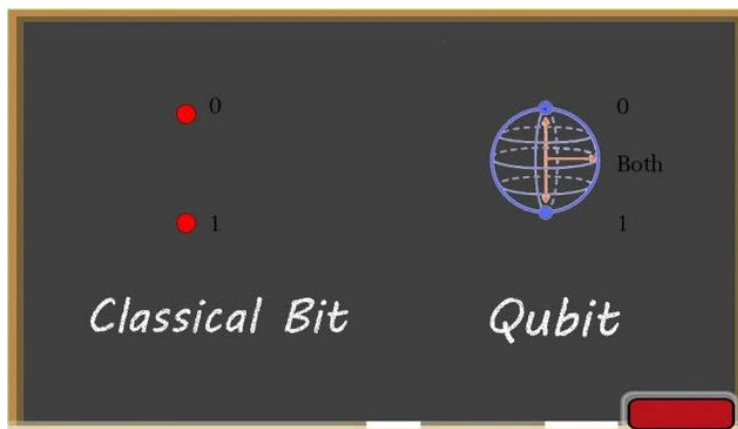
Nezavisno od toga što je ukupni uticaj AI do sada u mnogim industrijama veoma mali, njegov potencijal za „poremećaje“ je veoma visok. Smatra se da AI može ići dalje od promene poslovnih procesa, pa do promene celokupnih poslovnih modela sa dinamikom „Winner take all“, a da se u međuvremenu prašina veštačke inteligencije slegne, kako bi rizik uvođenja ove tehnologije bio izbegnut.

3. Kvantne tehnologije

Naučnici iz različitih regiona sveta smatraju da će kvantna tehnologija, za razliku od već postojećih, radikalno i revolucionarno promeniti IT svet kakav poznajemo, a naročito malo poznatu oblast koju obuhvata kvantna fizika, jer je ona duži niz decenija veliki naučni i tehnološki izazov.

Razlike između klasičnog i kvantnog računara su vidljive i ogromne po tehničkim parametrima. Na klasičnom računaru za izvođenje proračuna procesor koristi tranzistore i binarni sistem, dok kvantni računari koriste „Kubite“ koji imaju jednu dodatnu funkciju u odnosu na bitove. Najkraće rečeno, oni nisu predstavljeni kao jedinice i nule, već zapravo mogu biti i jedno i drugo u isto vreme.

Slika br. 3 Prikaz razlika između binarnog i kvantnog računara



Izvor: The next web; 2018, Amsterdam

Uvođenjem kvantnih računara u IK sisteme, uspostavljena je tzv. kvantna nadmoć u odnosu na dosadašnje generacije računara, obzirom da kvantni računari mogu obraditi više informacija istovremeno, budući da poseduju takozvanu kvantnu superpoziciju u kubitima, dok binarni računari to ne mogu. Kvantna nadmoć daje mogućnost da ovi računari, kada bude uspostavljena njihova potpuna funkcionalnost, da čak i oni slabiji od 100 kubita, mogu bez posebnih teškoća zaobilaziti bezbednosne sisteme kod svih binarnih računara.

Na osnovu saznanja i razvoja kvantne fizike i kvantne mehanike i uopšte kvantne informatike, istraživački napor i inovativni potencijali podržani opštim tehnološkim trendom, težišno su usmereni na razvoj kvantnog računarstva kao jednog od brojnih segmenata iz domena kvantne tehnologije radi njene primene u praksi.

Prvi talas kvantne revolucije doneo je kvantnu mehaniku, tj. teoriju koja daje deskripciju mikroskopskog sveta sa neverovatnom preciznošću i revolucionarnom tehnologijom poput tranzistora, lasera, GPS-a i magnetne rezonance. Drugi talas se trenutno bavi mikroskopskim svetom kvantnih tehnologija koje nose potencijal za inovacije na osnovnom nivou i za svakodnevne primene. Na tom planu ostvaren je ogroman napredak u pripremi, manipulaciji,

kontroli i detekciji kvantnih pojava u materijalima i supstancama, kvantnim elektronskim sistemima, hladnim atomima, kvantnim tačkama i isprepletenim fotonima. Kvantne tehnologije, trenutno uključuju kvantne atomske satove, kvantne senzore, simulatore komunikacije i kvantne računare.

U odnosu na druga tehnološka rešenja, kvantni računari su najzahtevniji i imaju verovatno najširu oblast primene kvantnih tehnologija, jer poseduju mogućnosti i performanse za rešavanje najšireg spektra problema.

Prema Microsoft-u, procesi optimizacije koje izvodi kvantni računar predstavljaju važan i odlučujući korak u daljem razvoju robotike, automatizma, fabrika budućnosti, transportu i mašinskom učenju.

Iako se kvantni računari još uvek nisu pojavili na tržištu, drugi uređaji iz ove tehnologije, prema oceni stručnjaka, mogu biti za kratko vreme dostupni za savršeno sigurnu komunikaciju, dakle bez mogućnosti prisluškivanja. Ti uređaji se baziraju na fenomenu kvantnog ispreplitavanja gde se uspostavljaju posebno jake veze između dve prostorno odvojene kvantne čestice.

Primena tih sofisticiranih uređaja vidljiva je u nekoliko područja. Između Šangaja i Pekinga konstruiše se 2000 km duga veza sa kvantnom enkripcijom za bezbedan prenos podataka. U Evropi i SAD slične veze takođe su uspostavljene, ali na manjim rastojanjima.

Sudeći po najavama vodećih tehnoloških inovatora, uz dovoljno sredstava za nastavak istraživanja, proizvodnja, a time i upotreba kvantnih računara može se očekivati za 5-10 godina. Još osamdesetih godina prošlog veka, poznati fizičar Richard Feynman objavio je svoju teoriju o kvantnom računaru. Generacije naučnika posle njega nastavile su istraživanja o računaru koji koristi kvantno stanje radi rešavanja određenih problema koji su klasičnim računarima nerešivi.

Najdalje u tom pravcu otišao je Mikhail Lukin sa Univerziteta Harvard, budući da je sa svojim timom razvio kvantni računar koji koristi 51 kvantni bit da bi obavljao proračune i pravio algoritme, što ga čini najsnažnijim kvantnim računarom koji je do sada proizveden.

Jedan od najvećih rezultata u stvaranju kvantnog računara zabeležen je u novoj Microsoft-ovoj laboratoriji koja radi istraživanje i razvoj na tehnološkom univerzitetu Delft u Holandiji. Ernst-Jan Stigter, generalni direktor „Microsoft Netherlands“ smatra da su ulaganja u resurse i

infrastrukturu putem javno-privatnog partnerstva ključni za kvantnu budućnost i da će ova laboratorija biti ključna za razvoj kvantne ekonomije (Microsoft, 2019).

Za razliku od sadašnjih, kvantni računari će moći obavljati proračune i zadatke na daleko većoj brzini i višem nivou složenosti, nego čak i današnji najmoćniji superkompjuteri. Primena ove računarske moći ima potencijal da revolucionira društvo i svet u kome živimo.

Razvoj kvantnih računara ide u dva pravca:

Prvi – otkrivanje i primena novih tretmana protiv bolesti; i

Drugi – rešavanje izazova u ekološkoj oblasti, kao što su efikasno korišćenje oskudnih materijala ili ekonomično korišćenje prirodnih resursa, što bi moglo pomoći u borbi protiv globalnog zagrevanja.

Kvantne tehnologije, a pre svega kvantni računari, nude revolucionarna i kvalitativna poboljšanja u pogledu kapaciteta, osetljivosti i brzine, tako da će biti primarni faktor uspeha u mnogim industrijama i na mnogim tržištima.

Pre komercijalizacije ovih računara, potrebno je izgraditi platformu kroz osnovna i primenjena istraživanja, koja će ključnim idejama i inovacijama društva omogućiti znanje o tome kako izgraditi sigurnije, brže i sa višim stepenom kapaciteta pametnije uređaje, proizvode i protokole.

Sumirajući dosadašnje rezultate, naučnici, obzirom na revolucionarnost pojedinih rešenja, ocenjuju da svaki ozbiljniji pomak ili korak u razvoju kvantne tehnologije, u stvari predstavlja jedan svojevrsni kvantni skok.

Evropska Unija, nastojeći da održi korak sa najrazvijenijim zemljama na zapadu i istoku, veoma je rano prepoznala potrebu za velikim ulaganjima, a zatim i razvijanju istraživačkih kapaciteta u oblasti kvantne tehnologije. Iz tih razloga, institucije EU pokrenule su inicijativu pod nazivom „Quantum Technologies Flagship“, vrednu više od milijardu eura, koja će kroz sledećih 10 godina finansirati više od 5000 istraživača u naučnim institucijama i sve projekte usmerene na razvoj kvantne tehnologije. U tom kontekstu predstavljen je i manifest koji opisuje značaj novih tehnoloških projekata, te važnost novih tehnologija u čijem se središtu nalazi kvantna revolucija. Koliki je značaj ove tehnologije, vidi se i po tome što se ona upoređuje sa otkrićem tranzistora 1940-ih i uvođenjem interneta 1990-tih. Realizacija programa počinje 2018. godine i obuhvata 22 države članice, dok istraživačke projekte podržavaju globalni tehnološki giganti poput:

Google, Intel, Microsoft, Airbus Defense i Space, Alcatel Lucent, ASML, Bosch, IBM, Nokia, IMEC, Safran, Siemens i Thales. Time je postalo jasno da je Evropa odlučila da bude predvodnik u razvoju kvantne tehnologije u svetu.

Pojedine kompanije, kao na primer Microsoft, iznele su svoje razvojne i opsežne planove, od istraživanja u hemiji, biohemiji, ekologiji, kvantnim sensorima, mašinskom učenju i iznad svega obradi velike količine podataka koje prikupljaju svi inteligentni uređaji interneta stvari (IoT).

Druge kompanije, kao što je Intel, intenzivno rade zajedno sa holandskim naučnim institucijama na izgradnji širokog spektra kvantnih i pratećih klasičnih tehnologija, dok Bosch ističe svoju orijentaciju prema IoT sensorima, kvantnim sensorima, kvantnoj kriptografiji i kvantnom računarstvu.

Otvarajući naučnu konferenciju „Kvantna Evropa 2016“ u Amsterdamu, Evropski komesar za digitalnu ekonomiju i društvo Günther H. Oettinger, naglasio je „da će kvantna tehnologija imati ogroman uticaj na društvo i ekonomiju, a od ovih tehnologija se, pre svega, očekuje da unaprede kapacitete računara do neslučenih razmera. To će Evropi omogućiti da preuzme vođstvo u globalnoj trci u razvoju kvantnih tehnologija, dok će industriju podstaći da ove tehnologije iskoristi u svim segmentima proizvodnje i pružanja usluga“.

Prema dosadašnjim istraživačkim dostignućima, može se bez većih rizika zaključiti da kvantna tehnologija osigurava veliki tehnološki napredak u područjima kao što su računarstvo, simulacije, kriptografija, telekomunikacije, dok se konkretne koristi od njene primene već vide kroz veoma precizne senzore u medicini, proizvodnji lekova i farmaciji, energetici, ekologiji i ostvarivanju veće bezbednosti digitalnih podataka.

Pored navedenih, posebna vrednost kvantne tehnologije i mogućnost šire primene, ogleda se u njenoj kompatibilnosti sa drugim naprednim tehnologijama, što će otvoriti širok prostor za razvoj nove generacije naprednih tehnologija čiji se obrisi samo naziru, ali još uvek ne i konkretna rešenja i mogućnosti primene.

4. Značaj, uloga i primena Industrije 4.0

Termin Industrija 4.0 ili digitalna transformacija industrije četvrte generacije, novijeg je datuma i prvi put je upotrebljen u javnom diskursu pre nekoliko godina, tokom održavanja sajma tehnologije u Hanoveru 2011. godine. Tom prilikom pokrenuta je sa najvišeg nivoa platforma

Industrije 4.0, a tokom 2012. godine je na predlog nemačkog Saveznog ministarstva obrazovanja i istraživanja, formiran naučno-industrijski konzorcijum koji je objavio strategiju uvođenja sa jasnim preporukama nemačkoj vladi, ali i poslovnom svetu, „pri čemu se navodi osam prioriteta, odnosno ključnih područja na kojima se temelji koncept Industrije 4.0:

Referentna arhitektura i standardizacija – podrazumevaju povezivanje i integraciju određenog broja kompanija kroz vrednosnu mrežu i poslovno partnerstvo, koje će biti održivo samo ako je uspostavljen set zajedničkih standarda, dok će referentna arhitektura obezbediti tehnički opis tih zajedničkih standarda i time olakšati njihovo sprovođenje;

Upravljanje kompleksnim sistemima – sistemi proizvodnje i proizvodi njihovog delovanja ispostavljaju se sve složenijim, usled čega to iziskuje adekvatno planiranje i tehničko-tehnološku opremljenost proizvodnih inženjera, kako metodama, tako i alatima nužnim za razvoj tih modela;

Sveobuhvatna širokopojasna industrijska infrastruktura – sveobuhvatne, kvalitetne i pouzdane širokopojasne mrežne komunikacije, ključni su uslov za Industriju 4.0;

Bezbednost i zaštita – kritični su za uspeh sistema pametne proizvodnje. Važno je obezbediti da objekti, proizvodnja i proizvodi nisu opasnost, ni za ljude, niti njihovu okolinu, dok istovremeno pogoni za proizvodnju i proizvodi koji u sebi integrišu podatke i informacije moraju biti podvrgnuti zaštiti od zloupotreba i neautorizovanog pristupa;

Organizacija i dizajn rada – u pametnim fabrikama uloga zaposlenih značajno će se promeniti, najpre usled postojanja kontrole u realnom vremenskom okviru koja kao takva teži transformaciji radnog sadržaja, procesa rada i radnog okruženja;

Usavršavanja i premanentni profesionalni razvoj - Industrija 4.0 drastično će promeniti sam princip angažovanja radnika i njihove kompetencije, usled čega će biti neophodno implementiranje odgovarajuće strategije osposobljavanja i organizovanja rada na način koji podstiče učenje i omogućava celoživotni ciklus usavršavanja učenjem;

Regulativni okvir - postojeće zakonodavstvo mora se adaptirati tržišnoj situaciji i utakmici, najpre time što će regulativa uzeti u obzir poslovne inovacije zbog zaštite poslovnih podataka, a onda i pitanja odgovornosti u vezi sa njima. Pored toga, regulativa mora uzeti u obzir i pitanja u vezi sa rukovanjima ličnim podacima, pitanja u vezi sa trgovinskim

ograničenjima, poslovnim smernicama, modelima ugovora, sporazumima između kompanija i samoregulacione inicijative kao što su revizije;

Efikasnost resursa – pored izuzetno visokih troškova, velike količine sirovina i energije koje se troše, takođe predstavljaju pretnju za životnu sredinu i bezbednost snabdevanja. U tom smislu Industrija 4.0 donosi uvećanu produktivnost i poslovnu efikasnost koja zahteva procenu kompromisa između dodatnih ulaganja koja se moraju izvršiti u pametne fabrike i potencijalne uštede koje će taj potez generisati“ (Kagermann, Wahlster, Helbig 2013:6-7).

Ogroman podstrek na planu popularizacije, ali i konceptualne razrade Industrije 4.0, dao je Svetski ekonomski forum (WEF) u Davosu 2016. godine, gde se o ovom fenomenu i esencijalno važnom pitanju za budućnost ekonomije i biznisa, raspravljalo čak na 20 različitih panela. Tim povodom, predsednik ovog foruma i jedan od vodećih stručnjaka u ovoj oblasti Klaus Schwab, predstavio je svoju knjigu pod nazivom „Četvrta industrijska revolucija“.

Nakon Svetskog ekonomskog foruma, digitalizacija industrije postaje ključna tema na svim velikim političkim skupovima, naučnim konferencijama i međunarodnim tehnološkim sajmovima, dok u naučnoj produkciji ona postaje neizostavni deo naučnih debata i istraživačkih napora. Razmatrajući načine i modalitete njenog uvođenja, kao i pozadinu koja stoji iza svega toga, pojedini autori smatraju da je „Industrija 4.0 u stvari preuzeta Nemačka vizija napredne industrijske proizvodnje koja se danas uveliko ostvaruje, a obuhvata primenu savremenih tehnologija za automatizaciju proizvodnje, obradu i razmenu podataka i dr.“ (Smokvina; 2016:30).

Zaključak je vrlo jasan: Industrija 4.0 povezuje dva dosad potpuno odvojena, ali brzorastuća digitalna područja – robotiku i e-poslovanje u jednu homogenu celinu čiji je krajnji rezultat pametna fabrika. Stvarajući novi vrednosni lanac, Industrija 4.0 se primarno oslanja na „Kibernetičko-fizički sistem“, odnosno „Cyber-Physical-Systems(CPS)“, a to je istovremeno i drugi naziv za IoT i njemu pripadajuće internet sisteme, najčešće smeštene u „oblaku“. Prema nemačkim stručnjacima sa Univerziteta u Dortmundu, moguće je „razlikovati 6 projektnih principa na kojima se temelje scenariji za implementaciju industrije 4.0:

Interoperabilnost – sposobnost međusobnog povezivanja i komunikacije sajber fizičkih sistema (CPS), ljudi i pametnih fabrika, pri čemu je primena normi presudna za uspešno povezivanje različitih proizvođača CPS-a;

Virtuelizacija – Omogućava da CPS nadzire fizičke sisteme povezivanjem podataka dobijenih preko senzora sa virtuelnim i simulacionim proizvodnim modelima;

Decentralizacija – sa povećanim zahtevima za individualizovanim proizvodima, strateško upravljanje sistemom postaje sve teže. Ugrađeni računari omogućavaju da CPS sam donosi proizvodne odluke u okviru pametne fabrike i nema više potrebe za strateškim planiranjem i nadzorom;

Sposobnost rada u realnom vremenu – potrebno je prikupljati i istovremeno obrađivati podatke. Stanje pogona je pod stalnim nadzorom i analizom, tako da se u slučaju kvara ili zastoja mašina, proizvodi automatski preusmeravaju na druge, odnosno rezervne ili alternativne proizvodne sisteme;

Servisna orijentacija – Internet usluga obuhvata sve učesnike u okvirima proizvodnog pogona, kao i one izvan njega. Servisna arhitektura preduzeća je sveobuhvatna kroz zatvorene web servise;

Modularnost – zahvaljujući standardizovanom hardveru i softveru omogućeno je fleksibilije prilagođavanje pametne fabrike promenljivim zahtevima, zamenom ili proširenjem pojedinih modula.“ (Hermann, Pentek, Otto, 2015)

Obzirom na svoju razuđenost, uticaj Industrije 4.0 na pojedine aktere i segmente poslovnog procesa je višestruk. Kada su u pitanju kompanije, uticaj Industrije 4.0 uključuje:

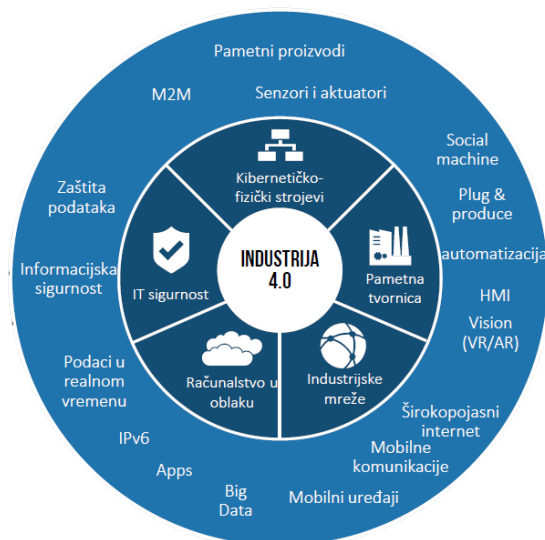
- Lokalizovane i identifikovane proizvodne serije omogućavaju više saznanja o proizvodnom procesu;
- Povezanost unutar organizacije;
- Prilagodljivost i mogućnost optimizacije proizvodnog procesa putem kontinuiranog prikupljanja spoljnih i unutrašnjih podataka;
- Kompetitivna prednost;
- Individualizacija proizvodnje prema zahtevima kupca i veća povezanost sa kupcima.

Industrija 4.0 ispoljava i uticaj na radnike i njihov status:

- Dodatni zahtevi za zaposlene, obuka (IT znanja i veštine);
- Veća uključenost u inovacioni proces;
- Nova vrsta interakcije između čoveka i mašina uz manje prisustvo radnika unutar fabrike;

- Podrška za pametne potpomognute sisteme;
- Decentralizovane strukture i upravljačke forme; i
- Više prostora za odlučivanje (Perić, 2017:5).

Slika br.4. Prikaz Industrije 4.0



Izvor: Perić, Industrija 4.0, Hrvatska gospodarska komora, Zagreb, 2017, str. 3

Kada je u pitanju tehnološki razvoj, naročito u jako promenjivim, turbulentnim i krajnje neizvesnim globalnim okolnostima, u tehnološkoj utakmici učestvuje veliki broj aktera sa različitim ambicijama, od kojih će neki biti dobitnici, a neki gubitnici. Obzirom da će u najrazvijenijim zemljama tehnološke promene zaživeti najbrže, one su u isto vreme, zajedno sa ekonomijama u razvoju i najveći dobitnici.

Prema navodima Klause Schwab-a, četvrta industrijska revolucija ima latentnu moć da podigne nivo globalno stvorenih vrednosti i kvalitativno utiče na živote i standard čitavih populacija. U tom kontekstu, stručnjaci ocenjuju da će postupak transformacije doneti pozitivne efekte samo onim ekonomijama ili kompanijama koje su sposobne za inovaciju i prilagođavanje u ranoj fazi uvođenja digitalne transformacije. Svi oni koji u tom pogledu zakasne ili postupe neodlučno, ne mogu očekivati uspehe, bar ne u punoj meri, usled vremensko-tehnološkog zaostatka na globalnoj ekonomsko-tehnološkoj sceni. Pored navedenog, korist ili dobra strana revolucije mogla bi biti cenovno pristupačnije robe i usluge, što će dovesti do novog trenda ekonomskog rasta, a najveća pretnja uvođenja novih tehnologija, prema mišljenju naučnika, jeste masovna nezaposlenost i sve veći jaz između korporacija i populacije. Upravo navedeni parametri,

verovatno će uticati na pozicioniranje država ili njihovih ekonomija i načina prilagođavanja novom robotizovanom, tj. digitalnom svetu. Među onima koji će sigurno biti gubitnici, posebno se izdvajaju nerazvijene, tranzicione ili tzv. target ekonomije, tehnološki i inovativno zaostale kompanije i drugi javni i profesionalni servisi okrenuti tradicionalnim poslovnim modelima.

Bez obzira što se nalazi tek na početku implementacije, kako po državama, tako i po sektorima, Industrija 4.0 još nije dostigla svoj vrhunac u smislu potpune primene. Industrija 4.0 ispoljava niz prednosti, ali istovremeno i određene nedostatke, ograničenja i prepreke za širu ekspanziju. U prednosti ove industrije „ubrajamo:

- Orijentaciju na individualne zahteve kupca;
- Prilagodljivu proizvodnju;
- Smanjen pritisak na radnike;
- Novu vrednost inovirane B2B usluge;
- Povećanu konkurentnost;
- Usmerenost na produktivnost i efikasnu upotrebu resursa;
- Spremnost na nove izazove na domaćem i stranim tržištima.

Nedostaci Industrije 4.0 obuhvataju:

- Manjak zaštite podataka;
- Olakšanu udaljenu manipulaciju proizvodnim sistemima;
- U ruralnim područjima nedostatak i slaba pokrivenost širokopojasnim internetom;
- Kontinuirana nabavka i održavanje infrastrukture;
- Složeni i skupi tehnički standardi, i
- Dodatna oprema za zaposlene“ (Perić, 2017:12).

Nedavna istraživanja sugerišu da će mašine sa veštačkom inteligencijom u narednoj deceniji, zahvaljujući eksplozivnom razvoju veštačke neuronske mreže, obavljati za sada niz nezamislivih poslova rezervisanih isključivo za ljude, kao na primer: humanoidni roboti sedeće u upravnim odborima, obavljace najsloženije hirurške operacije, te brojne i složene poslove u farmaceutskoj, mašinskoj, prerađivačkoj, kosmičkoj industriji, ali i u domenu menadžmenta i marketinga, itd.

Tipičan primer koji ilustruje napred navedeni stav jeste korporacija IBM koja razvija sofisticirani sistem „Watson“ dizajniran da uči iz informacija i iskustva ljudi, namenjen prvenstveno u

medicinske svrhe, tako da njegov računar ima pohranjene informacije o 2 miliona stranica medicinskih publikacija i 1,5 miliona kliničkih podataka, što daje mogućnost da analizira i ispita simptome pacijenta i da preporuke lekarima za lečenje.

U poređenju sa prethodnim, četvrta industrijska revolucija se razvija eksponencijalno, tako da dubina i širina započetih ili ostvarenih promena preoblikuje čitave proizvodne sisteme, menadžment i javnu upravu. Iz tog razloga, veoma je teško, ponekad čak i nemoguće predvideti kompletan spisak potencijalnih ishoda ili finalni scenario, do kakvih će promena zapravo dovesti. U budućnosti će inovativnost i tehnološki napredak biti važniji od kapitala. Oni koji više troše na nauku i tehnička istraživanja imaju tendenciju da rastu brže nego oni koji akumuliraju više kapitala, ali troše manje na tehnološke inovacije i razvoj, pa se čini da će to biti od presudne važnosti za buduću proizvodnju (Economic Discussions, 2015).

U digitalnoj eri, praktično se sve može digitalizovati. Svi do sada urađeni scenariji budućeg razvoja digitalizacije, prilično su ambiciozni i međusobno divergentni. Uprkos razlikama, načini uticaja Industrije 4.0 na kompanije i ekonomske sektore, pa i društvo u celini mogu se „sažeti u tri kategorije:

Prekid – Industrija 4.0 omogućava potpuno nove poslovne modele i načine stvaranja vrednosti, koji će sa vremenom zameniti stare tehnologije i modele;

Napredak – Ona rešava probleme današnjice sa tehnologijama budućnosti;

Destrukcija – Iako retka, postoje mišljenja da Industrija 4.0 nije nova, nema inovativni pristup i usled toga u nepripremljenim uslovima i ekonomskom okruženju može izazvati tzv. poremećaje destruktivnog tipa (Buhr, 2015:6).

U ovom trenutku, teško je potvrditi koja će od kategorija ostvariti dominantni uticaj, ali svi su izgledi da stručna javnost, tehnološki sektor i uopšte poslovne strukture, prednost daju konceptima napretka i prekida.

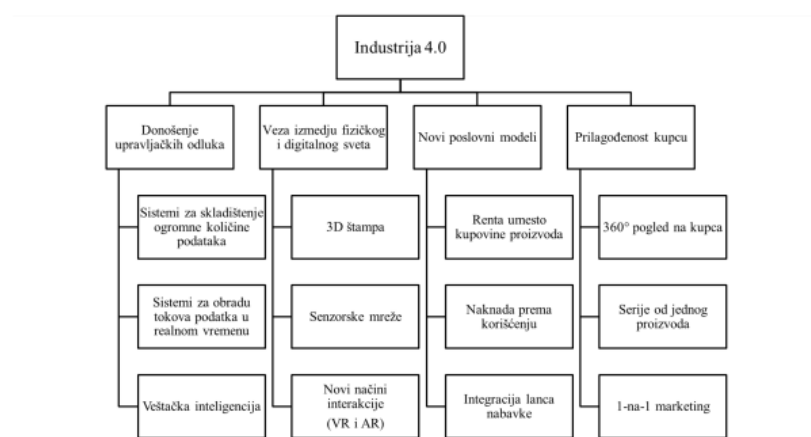
Novije ekonomske analize i istraživački nalazi potvrđuju, da je za razvoj Industrije 4.0 od presudnog značaja politička podrška. Od kreatora politike, posebno u domenu ekonomskog i tehnološkog razvoja, očekuje se da obezbedi ambijent, pravni i institucionalni okvir, definišu politiku i obezbede finansijska sredstva, kako bi tehnološke inovacije zauzele u skladu sa mogućnostima i potrebama zemlje svoje mesto u tehnološkoj konfiguraciji, koristeći obilato pri

tome iskustva, dobru praksu i rešenja već digitalizovanih kompanija i ekonomija. To između ostalog podrazumeva kreiranje savremene inovacione politike, formiranje istraživačkih centara i naučnih instituta i tesno povezivanje ekonomije i nauke radi uspostavljanja različitih vrsta javno-privatnog partnerstva.

4.1 Suština i karakteristike Industrije 4.0

Stručnjaci iz različitih oblasti, čiji se fokus odnosi na digitalnu tehnologiju (npr. Bornemann, D., Kagermann, H., Smit, J., Wahlster, W., Helbig, J., Buhr, D., Lodder, J., Bretel, M., Berger, R., Hirsch-Kreinsen, Hartmut., Klein, Michael., Ganz, Walter., Renn, Ortwin., Stephan, Peter., Schneider, H., Schwab, K., Degryse, C., Krueger, A., Huws, U., Katz, L., Ford, M., i dr.) istražujući i sagledavajući digitalne tehnologije iz više uglova i aspekata, pozitivno ocenjuju dosadašnji trend razvoja i primene naprednih digitalnih tehnologija, disruptivnih inovacija, a time i Industrije 4.0, naglašavajući da je to ireverzibilan tehnološki proces i da savremene ekonomije nemaju izbora pred dolazećim disruptivnim talasom.

Iz njihovih izlaganja proizilaze generalizujući stavovi da digitalna transformacija nije opcija, već imperativ. Fundamentalne karakteristike i specifičnost Industrije 4.0 sadržane su u posve vidljivoj činjenici da ona u potpunosti menja i redizajnira postojeće poslovne modele, način proizvodnje i distribucije, odnose između proizvođača i kupaca, promenu strateških paradigmi i projekcija, odnos radnika, mašina i poslodavaca, te upravljanja poslovnim procesima, jednom rečju transformiše ceo sistem poslovanja i sve njegove mreže. U sadržajnom pogledu, Industrija 4.0 obuhvata umrežavanje pametnih digitalnih uređaja sa proizvodima, mašinama, alatima, robotima i ljudima u domenu poslovanja, ali i u drugim sektorima javnog života.

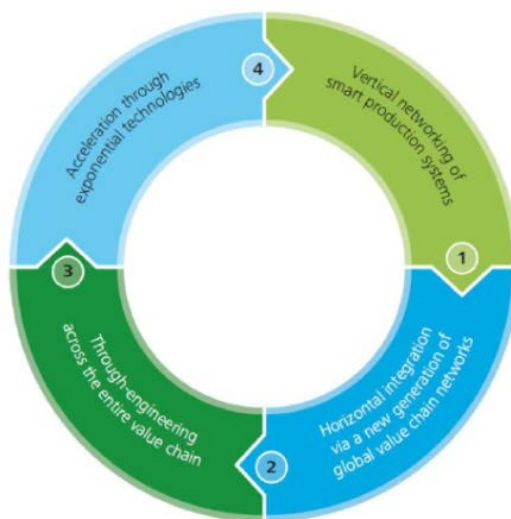


Slika br. 5. Industrija 4.0

Prema podacima kompanije za pružanje profesionalnih usluga Deloitte, „treba razlikovati 4 osnovne karakteristike industrije 4.0 i to:

- Vertikalnu mrežu pametnih proizvodnih sistema;
- Horizontalne integracije putem nove generacije globalne mreže vrednosnog lanca;
- Posredovani inženjering preko celog lanca vrednosti; i
- Akceleraciju posredovanjem eksponencijalnih tehnologija“ (Deloitte, 2015:6-8).

Slika br. 6. Četiri osnovne karakteristike Industrije 4.0



Izvor: Deloitte (2015) Industry 4.0 Challenges and solution for the digital transformation and use of exponential technologies, The Creative Studio of Deloitte, 6

Prema nedavno objavljenoj Dell EMC studiji „Digital Transformation Index Survey“, disrupcija je opšte prisutna u svim granama industrije. Više od polovine učesnika studije primetilo je da se u njihovom sektoru rada u poslednje 3 godine dogodile ozbiljne promene, približno polovina je iznela da ne znaju kako će njihova industrija izgledati u naredne tri godine, dok 45% veruje da postoji ozbiljna opasnost da će njihov biznis postati „zastareo“ u naredne 3 godine. (Dell EMC, 2016).

Prema procenama, u narednih 5 godina, Evropska Unija će širenjem digitalizacije povećati godišnji prihod industrijskog sektora za više od 110 milijardi evra. Bivši komesar za digitalnu ekonomiju i društvo Gunther Oettinger, u vezi namera Evropske Unije za razvijanje programa digitalne evropske industrije, ističe: „da bi Evropa zadržala vodeći položaj, a to znači i leaderski poziciju, mora uspešno i brzo da digitalizuje svu svoju industriju i u tu svrhu EU do 2030. godine

planira investicije u Industriju 4.0 u visini od 1350 milijardi evra, što znači da je ona u praksi potpuno posvećena procesu i napretku digitalizacije“ (Oettinger; PC Press, 2016).

U aktuelnom, tesno povezanom, globalnom poslovnom ambijentu, brzina penetracije na tržište i spremnost organizacije na promene, ubrzano postaju ključevi uspeha. Pritisci za snažnijom orijentacijom ka korisniku, nova očekivanja menadžmenta i zaposlenih od digitalne transformacije, aktuelni trend uvođenja i primene Industrije 4.0, obeležavaju sledeći prioriteti: kompetitivnost, prostor za poboljšanje kvaliteta proizvoda i usluga i njihovog kvaliteta, eliminisanje barijera, opstanak i tržišno prilagođavanje najbržih ekonomija i kompanija i rapidan razvoj korisničkog iskustva.

5. Obuhvat i područja primene interneta pametnih stvari

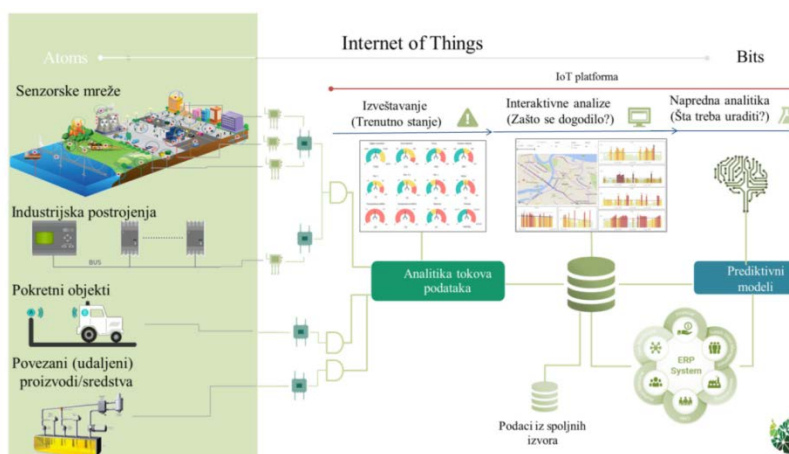
Internet stvari najčešće označavaju sposobnost komunikacije čoveka sa svojim fizičkim okruženjem, pri čemu je ta komunikacija dvosmerna ili višesmerna. Teško je pronaći neku oblast društvenog rada i života u kojoj internet stvari nemaju aplikativni kapacitet. Često se u javnosti ističe da većina načina primene interneta stvari za brojne delove populacije, osim stručne i naučne javnosti i poslovnog sveta, predstavlja i dalje naučnu fantastiku.

Osim navedene primene u sektoru industrije, IoT je već našao svoju primenu i u drugim sektorima, kao što su zdravstvo, farmaceutska industrija, transport (geolociranje, nadgledanje potrošnje i brzine kretanja, regulisanje saobraćaja), energetike, nadgledanja i redukovanja potrošnje radi uštede energije, vode i drugih resursa, prehrambenoj industriji (kontrola kvaliteta i porekla namirnica u realnom vremenu), vojna industrija (primena dronova i drugih pametnih autonomnih i hibridnih uređaja specijalno dizajniranih za obavljanje rizičnih poslova, kao što su deminiranje, boravak u kontaminiranim područjima i sl.), infrastruktura, itd. Iz navedenog je moguće zaključiti da potencijalne koristi IoT skoro nemaju granice, a odgovarajuće aplikacije konstantno utiču na načine života i rada, sabirajući pritom vreme i resurse i otvarajući nove pristupe za dalji razvoj i uvođenje inovacija. IoT je „vitalni instrument koji omogućava razvijenom društvu da usavrši načine korišćenja energije i optimizuje sve vrste prevoza i transporta. Očigledna je komplementarnost sa Cloud-om, Big Data i budućim mobilnim mrežama kao što je 5G“ (Drajić, 2017:13).

Polazeći od svojih performansi i konfiguracija, IoT nalazi primenu u različitim društvenim oblastima, a posebno u industrijskim sektorima. Tehnološka rešenja i proizvodi zasnovani na

inovativnoj tehnologiji interneta stvari, velikom brzinom osvajaju širok dijapazon oblasti. I sasvim letimičan pogled na IoT uređaje pokazuje da su oni našli primenu u vidu: pametnih satova, pametnih zgrada, preko rešenja za pametne automobile, gradove, medicinu, poljoprivredu, saobraćaj, zaštitu životne sredine i oblast zaštite i spasavanja. Prikupljanje informacija „na IoT platformama pruža celovit uvid u proizvodne kapacitete i predstavlja virtuelni model fabrike“ (Damnjanović, 2016:117). Povezivanjem sa drugim tehnologijama, IoT pruža velike mogućnosti na planu upravljanja resursima kompanije, budući da podrazumeva integraciju IoT rešenja sa upravljanjem, održavanjem, magacinima, zaštitom na radu, zaštitom životne sredine, kao i praćenjem transportnih sredstava.

Slika br. 7 Generička arhitektura IoT rešenja



Izvor: Damnjanović, D., (2016)., Primena Internet of Things (IoT) rešenja u upravljanju održavanjem u proizvodnji, Atom Bits d.o.o., str. 117

IoT kao suštinska revolucionarna tehnologija, sve više nalazi primenu i u nekim drugim oblastima, kao što je agrarni sektor, bezbednost prehrambenih proizvoda, stočarstvo i veterina. Naime, poslednjih godina razvijen je niz IoT rešenja u stočarstvu i veterini kojima se omogućavaju telemedicina, totalno praćenje lanaca snabdevanja prehrambenim proizvodima, te informacije o praćenju zdravstvenog stanja životinja, itd. (Marković, Nedić, 2016:58).

Analizirajući savremene digitalne trendove, a posebno kako IoT digitalizuje društvo, odnosno kako se razvijaju IoT rešenja koja odgovaraju zahtevima budućnosti i šta sve donosi nova tehnologija povezivanja i kako se IoT danas primenjuje i služi kao generator za razvoj budućih nadolazećih tehnologija, jedan od pionira modernih telekomunikacija i IoT-a, Jan Willem Smeenk, smatra da je IoT danas našao masovnu primenu gotovo u svim tehnološkim sektorima i

da će to biti generalni trend u budućnosti koja dolazi. Konačan uspeh primene IoT zavisi od razvoja ključnih faktora ekosistema, od pravnih normi, atmosfere poverenja, gde su, pored ostalog, važni i aspekti identifikacije, privatnosti i bezbednosti.

U stručnoj literaturi sve se češće govori o tzv. “pametnim prostorima“, koji obuhvataju pametne gradove, pametne kuće, pametne fabrike, itd. Postoji 5 ključnih dimenzija u kojima se pametni prostori razvijaju: otvorenost, povezanost, koordinacija, inteligencija i opseg. U osnovi, pametni prostori se razvijaju kao pojedinačne tehnologije kombinovane na stvaranju okruženja za saradnju i interakciju. Najopsežniji primer pametnih prostora su pametni gradovi, gde se područja koja kombinuju poslovne, stambene i industrijske zajednice projektuju koristeći okvire inteligentnih urbanih sistema, sa svim sektorima koji se povezuju na planu društvene i lokalne saradnje. Mnoge industrije uvode IoT i na njima zasnovane nove tehnologije kao deo razvoja poslovne strategije. Primenom tih tehnologija dolazi do značajnih promena, obzirom da one potiču od preduzimljivih i inovativnih konkurenata, koji zahvaljujući pristupima globalnim inovativnim istraživačkim platformama usmerenim na razvoj, prodaju, distribuciju i marketing, mogu eliminisati sa tržišta čak i dobro pozicionirane konkurente brže nego ikada pre, pritom poboljšavajući cenu, kvalitet i brzinu po kojoj je novostvorena vrednost isporučena.

Na strani potražnje javljaju se tri ključne promene i to:

- Rastuća transparentnost;
- Angažovanje potrošača; i
- Novi obrasci ponašanja potrošača.

Navedene promene podstiču kompanije da se adaptiraju na novonastalu situaciju i da menjaju način na koji generišu i isporučuju proizvode i usluge. Polazna tačka za takav trend je razvoj platformi koje vrše kombinovanje potražnje i ponude, koje su jednostavne za korišćenje na pametnim telefonima i koje kreiraju inovativne načine konzumiranja roba i usluga.

Nove tehnologije predvođene IoT-om ispoljavaju 4 glavna efekta na poslovanje:

- Očekivanje kupaca;
- Unapređenje proizvoda;
- Inovativnu saradnju; i
- Organizacione forme.

Ekspanzija i implementacija modernih tehnologija doveli su potrošače/kupce/korisnike u epicentar ekonomije, a kompanije se praktično takmiče u dizajniranju i isporučivanju proizvoda po želji i meri kupca.

U narednih nekoliko godina, prema prognozama, svetska industrija uložiće 6 biliona dolara u Internet stvari. Sudeći po interesovanju, uređaji i oprema zasnovani na ovoj tehnologiji najveću primenu će imati u kompanijama, dakle u korporativnom sektoru, zbog toga što će im IoT smanjiti troškove, povećati produktivnost i omogućiti širenje na nove oblasti, kako u oblasti proizvodnje, tako i u oblasti distribucije i prodaje. Drugi najveći korisnik ovih tehnologija će biti vlade država, kako bi povećale kvalitet života građanima i ujedno smanjile troškove administracije. Na kraju, pojedinci će zadnji prihvatiti ovu promenu, zbog dužeg perioda prilagođavanja novim tehnološkim rešenjima.

Danas više nego ikada, usluge i fizički proizvodi mogu biti unapređeni primenom digitalnih tehnologija i rešenja koja uvećavaju njihovu vrednost, a da pritom ove nove tehnologije čine primenjena sredstva dugotrajnijim i rezistentnijim, dok se povratna informaciona sprega kompanija obezbeđuje putem podataka i njihove analize.

Ovo znači da postepeno ulazimo u svet „potrošačkih/korisničkih iskustava“ i usluga zasnovanih na podacima i radnim karakteristikama sredstava, a to sve zajedno iziskuje i potpuno nove forme saradnje zbog dinamike kojom inovacije ulaze u svet biznisa i poslovanja.

Inovativne promene ne dovode samo do pojave novih platformi, već iniciraju dizajniranje i izgradnju potpuno novih poslovnih modela, budući da su kompanije prisiljene da konstantno ispituju načine na koje posluju i da postojeće poslovne modele stalno inoviraju ili uvode nove.

IoT tehnologije, sa druge strane, ispoljavaju značajni uticaj građana na rad vlade i drugih državnih institucija. Pod digitalnim pritiskom, vlade su suočene sa potrebom da izmene model i metod upravljanja javnim poslovima, kao i postupak kreiranja i implementacije javne politike i uspostavljanja efikasnije, operativnije i racionalnije javne administracije, uključujući tu i jačanje njenih kapaciteta radi ostvarenja konačnog cilja, a to je – uspostava javne uprave kao servisa građana.

Na kraju, IoT ispoljava i značajan uticaj na ljude. Naime, nove tehnologije zasnovane na IoT-u neposredno utiču i na identitet čoveka i njegov osećaj za privatnost, pri čemu radikalno menjaju

uvreženi pojam vlasništva, obrasce potrošnje, radno vreme, slobodno vreme, razvoj karijere, način razvijanja veština, upoznavanje i komunikaciju sa ljudima, percepciju i promenu našeg zdravlja.

Na individualnom planu, najveći izazov uvođenja tehnologije jeste ugrožavanje privatnosti. Pojedini stručnjaci navode brojne primere kako IoT sa novim tehnologijama doprinosi i utiče na oblikovanje budućnosti: naše živote, ekonomiju, društvo i okruženje.

Povodom toga, može se u stručnim krugovima naići na različite scenarije, od onih potpuno optimističnih, do onih koji daju pesimističku viziju i nehumanu sliku daljeg tehnološkog razvoja. Upravo ta najmračnija prognoza mogla bi imati potencijal, ukoliko se poremete ili izgube vrednosne i humane granice, da se robotizuje čovečanstvo i na taj način preuzme sve ono što je za čoveka suštinsko i bez čega bi čovek izgubio svaki smisao, odnosno bio dehumanizovan.

Potpuno suprotno gledište iznosi tezu, da tehnologija može poslužiti kao dopuna najboljim delovima ljudske prirode, kao što su kreativnost, humanost, empatija, odgovornost, posvećenost i sl., a takođe može da podigne i celokupno čovečanstvo na sledeći nivo moralne i kolektivne svesti, bazirane na zajedničkim vrednostima za dalji opstanak života na planeti.

5.1 Pametni gradovi

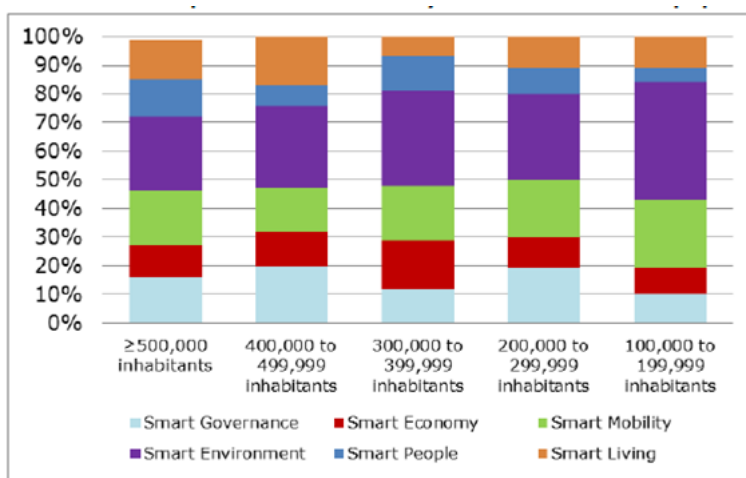
Uprkos različitim i brojnim interpretacijama i tumačenjima, pametni gradovi se najčešće definišu kao generički izraz koji obuhvata niz elemenata. U osnovi, gradove pametnim čini korišćenje modernih tehnologija kako bi poboljšali kvalitet života svojih građana, odnosno stanovnika i omogućili lakše upravljanje pojedinim javnim službama.

Paradigma pametnog grada nije potpuno nova, kao što se često u javnosti ističe. Ona se, doduše u različitim oblicima i sintagmama može pronaći i u ranijem periodu, u smislu rešenja koja se zasnivaju na iskustvu održivog razvoja gradova. Koncept pametnih gradova, pored ostalog, ima za cilj da uz pomoć interneta stvari gradski život prilagodi „novim digitalnim navikama“ njegovih stanovnika, ali i da gradskoj infrastrukturi starije generacije omogući nove funkcije zasnovane na novim rešenjima.

Jednostavno rečeno, pametni gradovi koriste IoT uređaje, senzore, svetla i brojila za prikupljanje podataka i njihovu analizu, a ti podaci služe gradskoj upravi ili gradskom menadžmentu za poboljšanje infrastrukture, servisa i komunalnih usluga.

Stručnjaci ističu da je potencijal pametnih gradova, obzirom na razvoj IoT i pratećih tehnologija skoro neograničen, tako da će rast pametnih gradova svoju punu ekspanziju tek doživjeti u bliskoj budućnosti.

Grafikon br. 8. Norme za pametne gradove



Izvor: Ericsson - Norme za pametne gradove – što primijeniti u Hrvatskoj?

Nije redak slučaj da se razvoj i koncept pametnog grada vezuje za realizaciju sledećih projekata: pametne ekonomije, pametnog stanovništva, pametne javne uprave, pametnog saobraćaja, pametne okoline i pametnog življenja.

Primeri implementacija IoT aplikacija u pametnim gradovima najčešće su: sistemska kontrola saobraćaja, pametna rešenja za parkiranja vozila, detekcija nivoa zagađenosti vazduha, preuzimanje informacija vezanih za nivo i vrstu zagađenja vazduha (smog, CO2 i sl.).

Istovremeno, postoji niz kategorija u više domena za primenu inteligentnih rešenja u pametnim gradovima, kao što su:

- zdravstvo
- administracija
- pametne zgrade
- javna bezbednost
- saobraćaj
- programi učešća
- energetika
- životna sredina

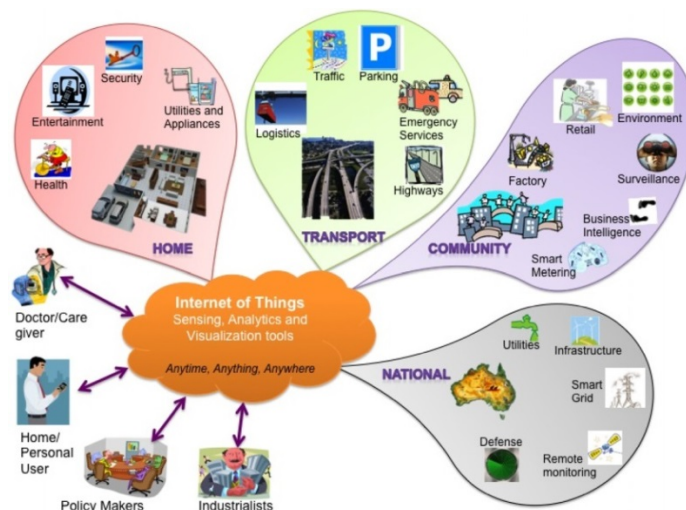
U tehnološko inovativnom smislu, za razvoj IoT infrastrukture u pametnim gradovima, pretežno se koriste: razvojne platforme, pristupne tehnologije, skladišta podataka, servisi za data analitiku i bezbednost podataka.

Jedna od vodećih svetskih kompanija, Bosch, pokrenula je 14 projekata vezano za pametne gradove, od kojih 7 uključuju rešenja urbane mobilnosti, kao što je povezano parkiranje i upravljanje voznim parkovima, multimodalni transport i elektromobilnost.

Osim primene u gradovima, Bosch-ova tehnologija, sudeći po brojnim potpisanim sporazumima i partnerstvima, veliku primenu nalazi i u pametnim lukama, aerodromima, železničkom transportu i sl.

Osnovna svrha primene IoT-a jeste da se najpre obezbedi, a zatim i primeni tzv. pametna infrastruktura u različitim oblastima koje omogućavaju normalno funkcionisanje gradskih i javnih službi u saobraćaju, električnoj energiji, stambenoj izgradnji i javnim servisima.

Slika br. 8 Primena IoT



Izvor: Okano, Marcelo. (2017). IOT and Industry 4.0: The Industrial New Revolution.

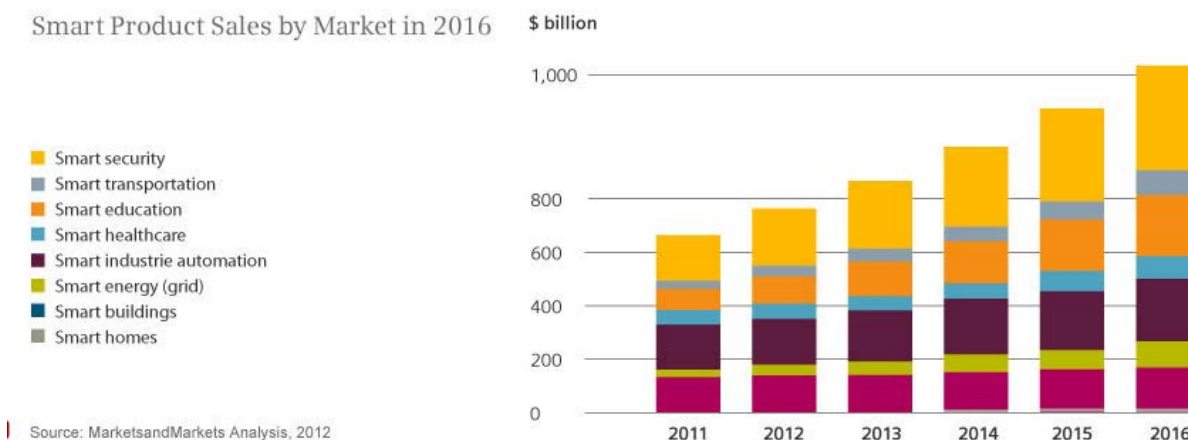
Tehnološki trend uvođenja pametnih gradova prisutan je u celom svetu, sa jasno unapred definisanim ciljem da se gradovi, a naročito velike metropole, transformišu u inteligentnije i efikasnije urbanističke celine koje će dati vidljive benefite, ne samo građanima, već i gradskoj upravi u smislu uštede na polju troškova funkcionisanja gradskih službi.

Prema tome, pametan grad, digitalne i komunikacione tehnologije prvenstveno koristi radi zadovoljenja potreba svojih građana, kao i radi unapređenja efikasnosti gradskih usluga. Takve urbane celine smanjuju troškove i potrošnju energije, a to kao krajnji rezultat ima čistiju životnu sredinu i podizanje životnog standarda građana.

5.2 Pametne mašine i uređaji

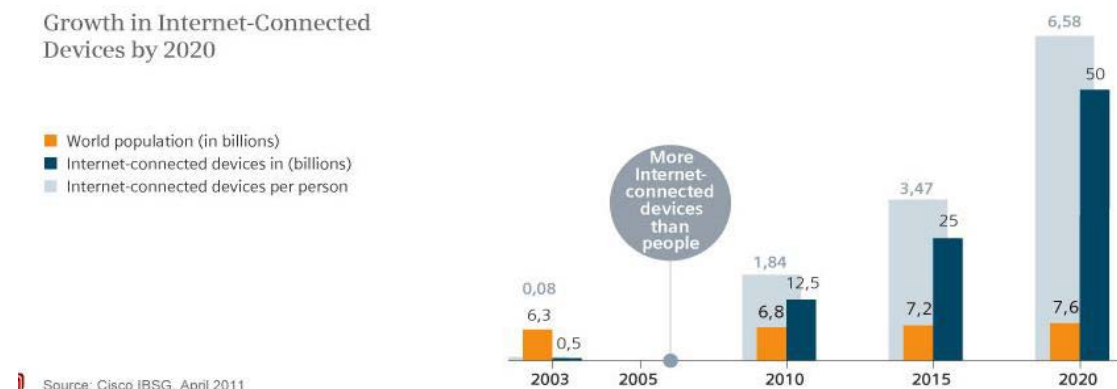
Naučnici predviđaju da će tri tehnološka pravca presudno uticati na dalji razvoj poslovanja i uopšte primene sofisticirane tehnologije u svakodnevnom životu. Prvi je razvoj BlockChain tehnologije, drugi je mašinsko učenje, dok je treći razvoj i primena autonomnih stvari. Na prestižnom MIT univerzitetu (The Massachusetts Institute of Technology), krajem novembra prošle godine, grupa naučnika laboratorije za računarske nauke i veštačku inteligenciju, iznela je rezultate razvoja tehnologije koji omogućavaju izradu vernih reprodukcija slika uz pomoć veštačke inteligencije i 3D štampe.

Grafikon br. 9 Prodaja pametnih uređaja po tržištima u 2016. godini



Izvor: Siemens, http://www.siemens.com/innovation/apps/pof_microsite/pof-fall-2012/html_en/facts-and-forecasts-growth-market-of-the-future.html

Grafikon br. 10 Rast Internet povezanih uređaja do 2020. godine



Source: Siemens, http://www.siemens.com/innovation/apps/pof_microsite/pof-fall-2012/html_en/facts-and-forecasts-growth-market-of-the-future.html

Sa tehnološkog stanovišta, Blockchain je kompjuterski registar (fajl) koji služi za skladištenje podataka, odnosno informacija. Slično drugim fajlovima, on postoji u bazi nekog digitalnog skladišta kao što je hard disk. Blockchain kao takav ima oblik niza binarnih bitova koje računari mogu da obrađuju i pojednostavljaju do mere da su razumljivi i čitljivi za ljude. Svi Blockchain fajlovi imaju tri univerzalne karakteristike, koje, kada se sastave, funkcionišu na drugačiji način od svih ostalih tipova kompjuterskih fajlova:

- Klasifikacija Blockchain-ova;
- Kriptografija; i
- Dostupnost, odnosno otvorenost Blockchain-a.

Najveći nedostatak vezan za Blockchain jeste što on zahteva ogromnu procesorsku moć, zbog izuzetno kompleksne kriptografske zaštite koju računari moraju da razreše da bi mogli da rešavaju pitanje skladištenja i pristupa podacima. Blockchain tehnologija podrazumeva i velike ekološke troškove, usled čega pristalice ove tehnologije to pravdaju time da se ti troškovi mogu kompenzovati prelaskom na obnovljivu tj. čistiju energiju. Neke zemlje poput Islanda, koje poseduju velike zalihe geotermalne energije postale su glavna čvorišta tzv. Bitcoin rudarenja.

Tokom jeseni 2018. godine, Brookings institucija iz Vašingtona je, u okviru serijala analitičkih tekstova „Plan za budućnost veštačke inteligencije“, detaljno analizirala i prikazala različite aspekte uticaja AI na razvoj društva, izazove i moguće nove politike kojima se ti izazovi rešavaju, čime je pokrenuta široka naučna, ali i društvena debata o gorućim pitanjima vezanim za tehnološki progres i rizike koje on nosi sa sobom.

Krajem decembra 2018. godine, svetski priznati stručnjaci u oblasti ekonomije i veštačke inteligencije, dr. Kai Fu Lee, Susan Athey i Erik Brynjolfsson sa Stanford univerziteta u Kaliforniji, predstavili su svoju knjigu pod nazivom „AI Superpowers: China, Silicon Valley and the New World Order“, u kojoj se razmatra odnos SAD i Kine u okviru razvoja tehnologija AI, uključujući i napredak novih tehnologija koje će u budućnosti oblikovati ekonomije, kompanije, ali i područje rada. Po prvi put u javnosti, dr Lee ističe svoju perspektivu o „Četiri talasa AI“: „Internet AI“, „Biznis AI“, „Percepciona AI“ i „Autonomna AI“ (Lee; 2018) i za svaki od ovih talasa navodi i kompanije koje pokazuju potencijal tog oblika veštačke inteligencije da revolucionarno promeni svaku industriju sa kojom dođe u kontakt. U svom izlaganju, dr Lee težište stavlja na brz rast i razvoj AI, neophodnosti saradnje SAD i Kine na tom planu,

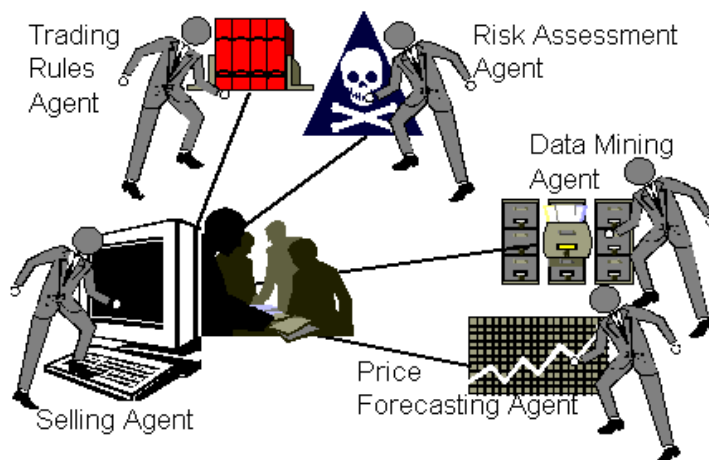
neizbežnoj automatizaciji rutinskih poslova i projektu koegzistencije između ljudi i veštačke inteligencije (Lee; AI Superpowers: 2018).

Prema Susan Athey, AI je sjajna prilika u ovom prostoru, jer ima puno fiksnih troškova, a ne previše marginalnih troškova, pa je optimistična u našoj sposobnosti da kanališemo filantropie, kao i vodeće univerzitete i istraživačke zajednice na rešavanju konkretnih, pre svega egzistencijalnih problema sadašnjice. Athey dalje ističe da naučna i tehnološka istraživanja „mogu doneti drastična poboljšanja u zdravstvu, obrazovanju i uopšte, ali premalo inovacija dospeva do ljudi kojima one najviše trebaju, jer uprkos tolikom napretku u nauci i tehnologiji nismo videli velikih primena na rešavanje problema siromašnih.“ (Athey; 2018)

Analizirajući koliko su moderni AI algoritmi široko primenjivi, a trenutna tehnologija „preuska“ Erik Brynjolfsson navodi da se novija dostignuća ne mogu tako lako generalizovati na rešavanje komercijalnih problema i realnog sveta i ističe važnost preduzetnika koji stvaraju nove kategorije poslova, naglašavajući pritom kreativnost u odnosu na rutinski način rada (Brynjolfsson, Mitchell, Rock, 2018).

Autonomne stvari koriste veštačku inteligenciju za obavljanje brojnih poslova koji su do sada bili tradicionalno rezervisani za ljude. Iako softiciranost inteligencije varira, sve autonomne stvari koriste AI za prirodnu interakciju sa svojim okruženjem. Moderni inteligentni uređaji i mašine, popularno nazvani autonomne stvari, postoje u 5 oblasti: robotika, vozila, trutovi, pametni uređaji i agenti, odnosno sofisticirana posrednička digitalna struktura.

Slika br.9 Agentski sistemi



Izvor: <https://www.w3.org/WAI/PF/SVG/examples/agent.gif>

Napred navedeno prikazuje široku sliku potencijalnih primena, a praktično i svaki program usluga, obzirom da IoT objekt može biti inkorporiran u neki oblik veštačke inteligencije za automatizaciju ili proširenje procesa ili ljudskih akcija. Pojedine, tzv. kolaborativne autonomne stvari kao što su „drono rojevi“ sve češće će podstaći, a time i podržati budućnosti AI sistema.

Opšti je imperativ da se ovi pametni uređaji koriste za usko definisane svrhe i namene, čime će uveliko olakšati i ubrzati proizvodnju, a posebno angažovanje ljudi u teškim radnim uslovima.

U kontekstu razvoja modernih pametnih mašina i uređaja, posebno se izdvaja Blockchain, odnosno lančani spisak svih izvršenih transakcija u okviru jedne valute. Drugim rečima, Blockchain je tehnologija po kojoj radi Bitcoin, ali i sve ostale kriptovalute, odnosno to je jedna digitalna finansijska knjiga gde je apsolutno pouzdano evidentirano ko ima koliko novca i ko je kome novac transferisao u prošlosti. Ključni razlog zašto je Blockchain postao jako popularan i široko primenjiv, jeste da se u njega mogu zabeležiti svi lični podaci o imovini, a upravo to rešenje daje mogućnost da se ova tehnologija, osim za potrebe prikupljanja i obrade finansijskih podataka, koristi i u druge različite svrhe, pa i one bezbednosno analitičke u kontekstu otkrivanja finansijskog kriminala globalnih razmera.

Blockchain je relativno nova tehnologija koja omogućava decentralizovanje, skladištenje i prenos informacija i predstavlja upotrebljiv alat za praćenje svih vrsta transakcija. Ova tehnologija može smanjiti napetosti, korupciju, povećati poverenje i osnažiti korisnike. Gotovo svi sektori, od finansija, energetike, brodogradnje, medija, itd., mogu koristiti ovu revolucionarnu tehnološku aplikaciju. Izazov je otvoriti taj potencijal na način koji osigurava uključenost, bezbednost, interoperabilnost i sveobuhvatnost. Tehnologija ovog tipa unapređuje načela dobrog upravljanja, kako bi se podržala infrastruktura na kojoj se temelji, a aplikacija izgrađena na distribuiranoj tehnologiji čini glavna područja primene. Konkretno, oblast primene je široka, poput digitalnog prepoznavanja, sertifikovanja, integracije lanca snabdevanja, pametnih ugovora, te valutnih i monetarnih sistema.

Blockchain je, dakle, neka vrsta raspodeljene knjige, širi hronološki urađen popis kriptografskih potpisanih neopozivih transakcijskih zapisa, koje dele svi učesnici u mreži. Kompanijama koje koriste sofisticiranu tehnologiju Blockchain, ona služi za praćenje transakcija u slučaju kada rade sa nepoverljivim strankama, ali bez potrebe za centralizovanom strankom, tj. bankom. Primenom ovog sistema kompanije smanjuju troškove, što znači da smanjuju i vreme transakcije i

poboljšavaju finansijske tokove. Iako predstavlja novinu u tehnološkom smislu, Blockchain polako preuzima mesto i poslove koje su u ranijem periodu obavljale mašine sa nižim stepenom veštačke inteligencije. Najkraće rečeno, Blockchain predstavlja distribuirani elektronski registar koji primenjuje softverske algoritme radi pouzdanog i anonimnog evidentiranja i potvrđivanja izvršene transakcije.

Posebno interesovanje poslovnog sveta, pored stručne javnosti, izazivaju tehnologije: proširena stvarnost (AR) i virtuelna realnost (VR). Koncept virtuelne realnosti nije nov. Brojni uređaji iz ovog domena postojali su i bili dostupni i ranije, ali je njihova primena bila usko ograničena na akademske i vojne krugove. Međutim, u skorije vreme, ova tehnologija je počela da ostvaruje eksponencijalni napredak i donosi razne pojavne oblike. Ti pojavni oblici se mogu sresti od virtuelne realnosti pohranjene u jednostavne i jeftine kartonske kutije, do veoma naprednih sistema virtuelne realnosti čija je cena u rasponu od par desetina do stotina hiljada evra. Veliko interesovanje za ovim uređajima stvorilo je kritičnu masu za njihovu široku ili serijsku proizvodnju i široku prodaju. Zanimljiv, atraktivan i nadasve jedinstven sadržaj privlači ljude da nabavljaju takvu opremu, a ta povratna sprega doprinosi njenom nezaustavljivom usponu.

Prvi ozbiljniji primeri omasovljavanja tehnologije virtuelne realnosti beleže se u oblasti zabave, najpre u industriji računarskih igara, ali i video 360°, međutim, VR tehnologija svoju primenu sve češće nalazi u oblasti poslovanja, obrazovanja, trgovine, zabave, kulture itd.

VR koncept i koncept interneta stvari povezani su u koncept „realnosti stvari“ (Reality of Things), obzirom da je to dovelo do promene definicije pojma stvari. Obzirom da se ove tehnologije uporedo razvijaju, prognoze su da će se taj proces dalje intenzivirati, a realnost stvari biti pomerena do mere da će biti veoma teško većini ljudi da razluče i naprave razliku između fizičkih stvari napravljenih od atoma i nacrtanih stvari sačinjenih od fotona i elektrona. Konkretno, osim za stručna lica, biće jako teško razdvojiti naučnu fantastiku od realnosti.

U odnosu na druge tehnologije, proširena stvarnost omogućava nadogradnju informacija i vizuelnih elemenata fizičkom svetu putem grafičkog, odnosno audio sloja u cilju poboljšanja korisničkog iskustva u odnosu na neki proizvod ili zadatak. Naznačeno „proširenje“ realnog sveta postiže se posredstvom dodatnih uređaja koji pružaju i prikazuju takve informacije. Za razliku od navedenog, virtuelna realnost omogućava trodimenzionalnu simulaciju slike ili čitavog okruženja koju generiše računar u okviru unapred određenog i kontrolisanog prostora sa

kojim korisnici mogu da postanu interaktivni. Dakle, cilj virtuelne stvarnosti je pružanje potpunog iskustva posredstvom prateće opreme bez koje ne može da funkcioniše.

5.3 Uticaj na poslovanje

Svaka tehnologija u svom domenu, pojedinačno ili u celini, stimuliše revoluciju u načinu na koji se posluje. Međutim, konkretan napredak u tom smislu zavisi od stvari koje su njome zahvaćene, a u prvom redu onih koji kreiraju strateško okruženje, odnosno donose ključne poslovne odluke. Nova generacija digitalizovanih fabrika u razvijenim zapadnim, ali i istočnim zemljama, u mnogome je promenila, transformisala i rekonfigurisala način rada i života, najpre tako što su najteže poslove preuzeli roboti i mašine, dok se od masovne proizvodnje, odustalo. Prelazak na digitalnu platformu u funkcionisanju kompletne privrede, sa osloncem na pametne fabrike u različitim sektorima, nije jednostavan, a još manje jeftin način poslovanja. Pojedine procene ističu da će Evropska Unija do kraja 2030. godine u industriju 4.0 investirati najmanje 350 mlrd. evra. Digitalna tehnologija podrazumeva zaokruženu digitalizaciju svih proizvodnih procesa i njenu primenu prilikom kreiranja ideja o nekom proizvodu ili izradi prototipa, proizvodnom inženjeringu, proizvodnoj organizaciji, realizaciji proizvodne aktivnosti, kontroli proizvodnog procesa i pružanja usluga u industriji.

Referentne studije potvrđuju stav da većina stanovnika očekuje da će tehnologija doneti dubinske, pa čak i revolucionarne promene u njihovim delatnostima u predstojećih 10 godina, dok samo 2% ispitanika smatra da one neće izvršiti nikakav uticaj.

Razne tehnologije će imati bitan uticaj na industrijske ili uslužne sektore, na različite načine, dok se ti uticaji u zavisnosti od kriterijuma mogu različito kategorisati. Nezavisno od toga u kom se sektoru ove tehnologije primenjuju, one generalno utiču na promene stavova, kako radnika, tako i menadžmenta i zahtevaju njihovo suštinsko razumevanje i pripremu kompanija za njih. To pored ostalog znači i razvijanje posebne discipline ili segmenta menadžmenta koji je usmeren na upravljanje informatičkim i digitalnim promenama u kompanijama.

Iako postoje izražene razlike između tržišta, zajednička im je otvorenost radne snage da bez većih otpora usvoje novu tehnologiju i način rada. Navedeni optimizam i spremnost neće dati očekivane rezultate, ako same kompanije ne budu spremne da iskoriste sve šanse koje im pruža nova tehnologija i naredna razvojna generacija. Na prostoru Evropske Unije čak 57% radnika smatra da će organizacioni modeli i delatnosti imati ozbiljnih poteškoća zbog nezadržive

digitalizacije u predstojećoj deceniji. Dakle, nesposobnost ili nespремnost kompanija da se pripreme ili prilagode eri digitalizacije, sprečiće dalju integraciju i implementaciju tehnologije u proizvodne procese.

Svako organizaciono, poslovno i tržišno adaptiranje novim tehnologijama, opterećenje je za poslovanje, prvenstveno bog povećanja troškova rada. U tom smislu veoma su indikativni rezultati studije McKinsey Instituta, koji pokazuju da 79% ispitanika veruje da tehnologija ima potencijal da unapredi organizacionu efikasnost, dok 77% smatra da će tehnološka transformacija u zavisnosti od sektora povećati prihode.

Primena interneta stvari do 2025. godine može ostvariti potencijalni globalni uticaj u iznosu od 6,2 mlrd. US dolara. Visok procenat ispitanika, čak 76% veruje da će tehnologija stvoriti nove izvore rasta, dok 74% tvrdi da može povećati konkurentnost u određenom sektoru. Da smo duboko zašli u fazu promena, potvrđuje i 81% ispitanika, koji smatraju da će nova tehnološka transformacija usloviti ispitivanje tradicionalnog načina poslovanja. Isto tako, održavanje koraka sa promenama potrebno je, ne samo zbog konkurentnosti kompanija, nego i zbog stvaranja ogromnog prostora za budući rast. Može se bez zadržke zaključiti da tehnologija više ne “statira”, već osvaja ključnu ulogu u poslovnim procesima i trendovima.

5.4 Horizontalna i vertikalna integracija

Značajna dimenzija i karakteristika industrije 4.0, pored umreženosti, primene novih kibernetičko-fizičkih sistema, fleksibilnosti pametnih uređaja i mašina je i horizontalna i vertikalna integracija.

Horizontalna integracija se uglavnom odnosi na integraciju različitih IT sistema, korišćenih u različitim fazama proizvodnje ili planiranja proizvodnje, koji kao takvi uključuju razmenu materijala, energije i informacija, bilo unutar jednog preduzeća, bilo između različitih preduzeća.

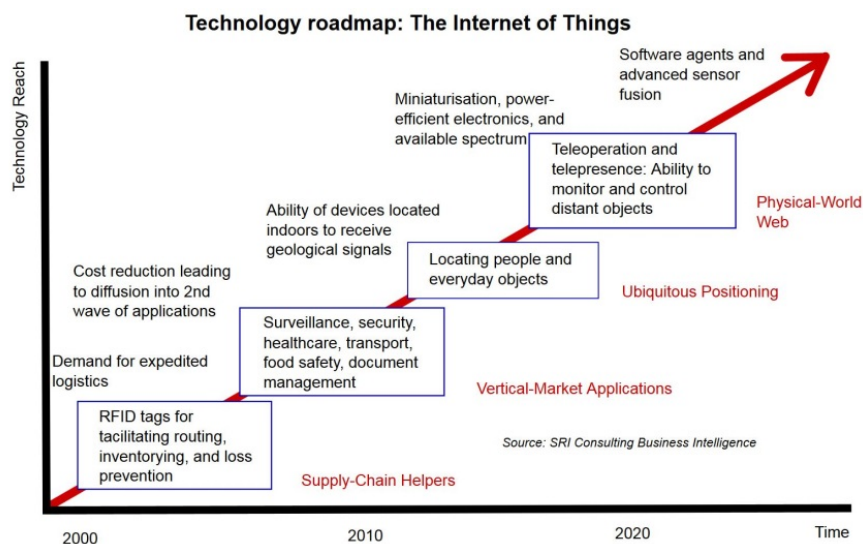
Za razliku od toga, vertikalna integracija se odnosi na povezivanje različitih IT sistema na različitim hijerarhijskim nivoima (senzori - kontrolni sistem, menadžment proizvodnje, planiranje strategije preduzeća i dr.) sa ciljem postizanja optimalnog rešenja. Najkraće rečeno, horizontalna i vertikalna integracija spajaju u kompanijama elemente kao što su: proizvodnja, održavanje i inženjering u skladnu celinu, a izvan preduzeća spajaju i sinhronizuju dobavljače, proizvođače i potrošače.

6. Napredni i inovativni proizvodni procesi

Ugrađeni hardverski i softverski sistemi značajno i suštinski proširuju funkcionalnost i konkurentnost vozila, medicinske opreme, vazduhoplova, proizvodnih postrojenja i aparata za domaćinstvo. Upravo, povezivanje ovih sistema sa virtuelnim okruženjem globalno umreženih servisa i informacionih sistema generiše potpuno nove oblasti inovacija i novih poslovnih platformi.

Imajući u vidu započete trendove, sajber fizički sistemi će doprineti bezbednosti, efikasnosti, udobnosti i zdravlju ljudi i uopšte rešavanju ključnih izazova današnjice. Takvi izazovi su starenje populacije, ograničeni resursi, mobilnost i naponi ka osvajanju i usvajanju obnovljivih izvora energije. Tehnike kombinovanja inovacionih tehnologija u praksi, sasvim je izvesno, mogu ostvariti efektivno upravljanje fizičkim stanjem uređaja i postrojenja.

Grafikon br. 11 Tehnološka mapa: Internet stvari



Izvor: SRI Consulting Business Intelligence

Istraživanja u oblasti RFID tehnologije (Radio Frequency Identification), omogućila su njenu praktičnu primenu u oblasti elektro-energetike. Ako se uzme u obzir da ova tehnologija zahteva kombinovanje sa drugim tehnologijama i konceptima inovativnog projektovanja, postoje veliki izgledi za uspešno rešavanje različitih problema u oblasti upravljanja. Pored toga, ova tehnologija omogućava konvergenciju tehnologija CPS (Cyber Physical Systems) i ERP (Enterprise Resource Planning).

6.1 Pametne fabrike

Industrija 4.0 donosi brojne koristi i rezultate putem digitalizacije, od kojih centralno mesto zauzimaju tzv. pametne fabrike. Zahvaljujući automatizaciji i veštačkoj inteligenciji, uvođenje pametnih fabrika ima za cilj optimizaciju procesa nabavke, proizvodnje i plasiranja proizvoda uz podizanje kvaliteta. Vodeća svetska industrija na tom planu je Nemačka, obzirom da je veoma rano prepoznala ovaj trend i uložila ogromna sredstva u promociju i inovacije. U zapadnoj hemisferi, razvijajući koncept 4.0, američki gigant, General Electric, koncipirao je termin „industrijski internet“ koji u suštini označava isti sadržaj. U naučno-stručnim krugovima, s pravom se ističe da budućnost pripada pametnim fabrikama. Naime, sveopšta digitalizacija u proizvodnim pogonima dovešće do značajnih promena na tržištu radne snage, pojavi novih zanimanja, odnosno nestajanju postojećih, razvoju pratećih grana i uopšte potpuno će redizajnirati, ne samo način proizvodnje, nego i ekonomiju u celini.

Brojni korporativni procesi su već sada kontrolisani i koordinisani u realnom vremenu, zavisno od opreme, čak i na velikim udaljenostima. Nove tehnologije omogućavaju da robusne mreže obezbeđuju razmenu podataka radi automatskog prilagođavanja procesa proizvodnje i njenih parametara. Više ne postoji potreba da kontrola procesa bude striktno centralizovana. Ona sada može biti upravljana prema CPS-u. Bazični uslovi za stvaranje inteligentne fabrike delom su već realizovani ili se nalaze u fazi finalizacije. Između ostalog, to podrazumeva da nabavka novih softvera i mašina za kreiranje novih saveza i kupovinu profesionalnih usluga mora već sada biti orijentisana ka budućim načinima rada.

Na praktičnom planu, to pretpostavlja:

- „spremnost da se uključe proizvođači i potrošači u svojim kompanijskim procesima i da automatski razmenjuju informacije;
- nove mašine za IPv6 (internet protokol ver. 6), i komunikaciju sa komponentama omogućavaju fleksibilnu proizvodnju;
- novi softver za planiranje, kontrolu, vizuelizaciju ili analizu, takođe mora biti prilagođen fleksibilno ili individualno, a to znači da se ergonomski upravlja;
- umrežavanje mora omogućiti komunikaciju van korporativnih granica, ali da ipak ostane bezbedna“ (Industrija br. 54, 2015:16).

Digitalizovana fabrika omogućava inteligentnu spregu procesa proizvodnje, gde se direktno povezuje fizički i virtuelni, odnosno digitalni svet. Pored digitalizovanih mašina, digitalno preduzeće mora da ima odgovarajući industrijski softver koji objedinjuje procese u proizvodnji, infrastrukturu za komunikacije, sistem bezbednosti i industrijske servise koji su digitalizovani. Konkretna ili namenska softverska rešenja mogu biti podvrgnuta razvoju u sopstvenom okruženju, međutim, najveći broj kompanija na tržištu kupuje takva rešenja od specijalizovanih proizvođača.

U nedavno objavljenoj studiji pod nazivom „Automatizacija 2020.“ udruženja Nemačkih inženjera, pokrenuto je esencijalno pitanje: sa čime njihovi članovi treba da se bave u industriji, odnosno koji profil kadrova u budućnosti treba obezbediti da bi pametne fabrike mogle da postignu maksimalnu primenu? Kako bi IoT i pametne fabrike bile uspešne, pored tehničkih zahteva i standarda u implementaciji, fokus treba usmeriti i na pripremu kadrova, tj. stručnjaka za automatizaciju i rad u fabrici u skladu sa digitalnim zahtevima vremena koje dolazi.

Osim toga, neophodno je instalirati softver koji je u stanju da učini brzu analizu i pošalje podatke u razumljivom obliku, a pre svega da se sa tim softverom može lako i brzo upravljati. Trenutno, razvoj pametne fabrike ide u 7 pravaca:

Spajanje ljudi u tim - najveći izazov u ovom trenutku nije, kao što se često pretpostavlja, tehnološki, nego organizacioni. Postavlja se imperativ da se u kompanijama formiraju disciplinovani timovi u čiji sastav ulaze predstavnici iz različitih oblasti proizvodnje uključujući automatizaciju, IT, marketing i prodaju, upravljanje lancem snabdevanja, koji zajednički, dakle timski, mogu doprineti boljem funkcionisanju pametnih fabrika.

Pronaći zajednički jezik - između različitih tržišnih uslova i proizvodnih uređaja, kao što su internet stvari za automatizaciju, računarsko-fizički sistemi, PLC-ovi (programabilni logički kontroleri), informacioni tokovi, ergonomija, ukupni trošak vlasništva, povrat uložene investicije, investicionih ciklusa i dr. treba:

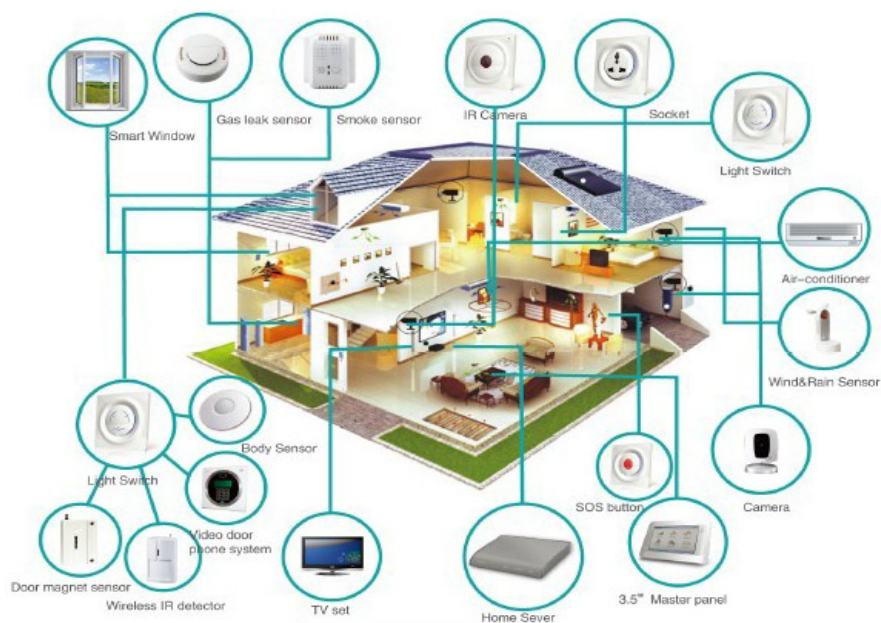
- Definisati poslovne ciljeve;
- Odrediti idealno stanje;
- Uraditi Cost/benefit analizu;
- Uskladiti tehnologije;
- Izvršiti implementaciju i stalno usavršavanje (Industrija br. 54, 2015:16-17).

Prema rezultatima istraživanja renomirane kompanije specijalizovane za ekonomski konsalting: „PriceWaterhouseCoopers“ (PWC), umrežavanje industrijskih pogona pokreće novu industrijsku revoluciju, tzv. industriju 4.0, gde je pametna fabrika ona koja kod većine fabrika iz industrijskog sektora u Nemačkoj postaje sastavni deo takve poslovne strategije. I pored svih napora, i dalje tek svaka 5. kompanija u Nemačkoj upravlja svojim pogonima za proizvodnju i poslovnim jedinicama putem umreženih informacionih sistema. Ovakav vid proizvodnje omogućava drastično skraćanje perioda od početka razvoja do izlaska na tržište novih proizvoda.

6.2 Pametne kuće

Savremene tehnologije su tokom poslednje dekade, našle na masovnu primenu u domaćinstvu, kroz razvoj tzv. „pametne kuće“. Novi model stanovanja, baziran na širokoj primeni električnih uređaja i instalacija, nameće potrebu za razvojem integrisanih elektronskih komponenti i sistema. Rastuće potrebe korisnika prostora s jedne, i moderni uslovi stanovanja sa druge strane, otvaraju mogućnost primene različitih tehnologija radi zaštite životne sredine, racionalnije potrošnje energije i osiguranja bezbednosti imovine. Kako bi se zadovoljile navedene potrebe, neophodno je stvoriti inteligentniji ambijent koji će biti sposoban upravljati komforom (definisanim i kvantifikovanim na određeni propisan način), da garantuje bezbednost, štedi energiju i izlazi u susret starijima, mladima i drugim zainteresovanim grupama.

Slika br.10 Primer pametne kuće



Izvor: Heetae Yang, Wonji Lee, Hwansoo Lee Published in J. Sensors 2018

Tako projektovani sistem omogućava izvršavanje komandi korisnika, počev od uključivanja svetala, podizanja roletni, pa sve do kompleksnih scenarija uslovljenih vremenskim prilikama, identitetom korisnika, neprekidnim praćenjem parametara kao što su temperatura, vlažnost vazduha, potrošnja energije, itd., automatska regulacija kućnih parametara, kao i slanje određenih signala u slučaju potrebe, kao i usluge podrške na daljinu.

Savremeni „In house“ pametni sistemi najčešće su u poziciji da obavestavaju korisnika audiovizuelnog signala, a u novije vreme moguća je i komunikacija sa objektom putem internet protokola posredstvom SMS poruka ili e-mail poruka.

7. Ključni digitalni trendovi

Prilikom analize postojećeg stanja digitalizacije, vodeći stručnjaci iz ove oblasti ističu da je transformacija digitalnog poslovanja jedan od najizraženijih trendova u oblasti informacionih tehnologija (IT), ali i poslovanju uopšte. Stručnjaci posebno ističu da se ovde ne radi o isključivo tehnološkom trendu, već se radi o središtu poslovnih strategija gotovo u svim industrijskim segmentima i tržištima.

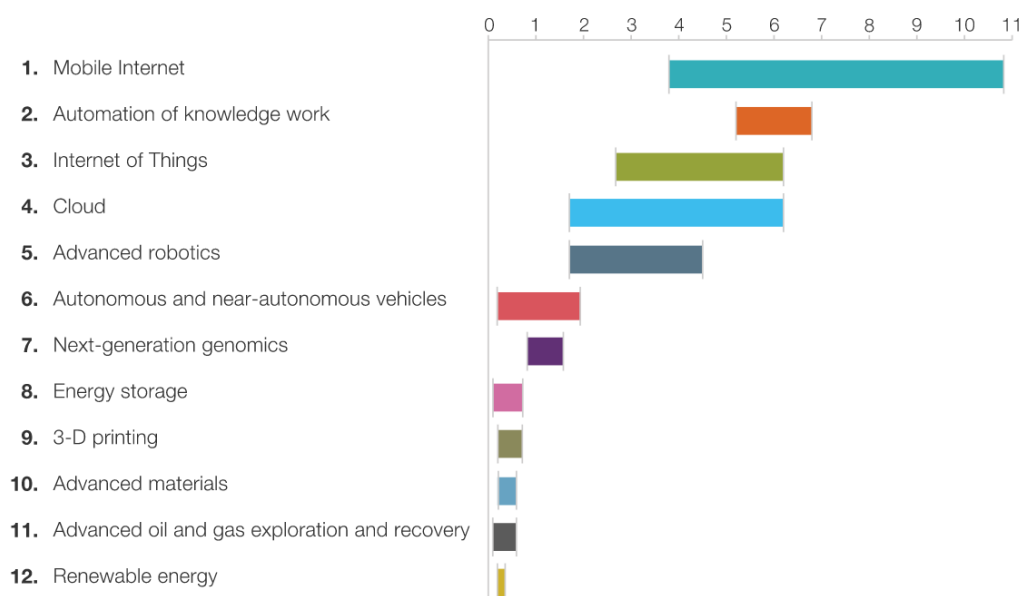
Novija istraživanja, međutim, sugerišu da je veoma teško u ovom trenutku predvideti koje će tehnologije, a samim tim i tehnološki trendovi u skorijoj budućnosti dominantno uticati na ekonomska i opšta društvena kretanja. Širok dijapazon razvoja novih tehnologija zasnovanih na disruptivnim inovacijama, već duži niz godina odvija se na više koloseka gde se njihove granice često prepliću, a u nekim aspektima i prožimaju. Praksa je u više navrata do sada pokazala da brojne nadolazeće tehnologije, čak i one koje su u startu favorizovane, nemaju kreativni potencijal da se relativno brzo i lako pozicioniraju i sebi osiguraju praktičnu primenu. Nasuprot tome, samo mali broj tehnoloških inovacija i rešenja ima mogućnost da promeni „status quo“ i da na taj način utiču i menjaju ekonomske, industrijske i finansijske tokove, smerove i pravce.

Pronalaženje odgovora na pitanje u kom pravcu će se odvijati dalji tehnološki razvoj, koje tehnologije će uticati na promenu u načinu proizvodnje, kako će se odvijati komunikacije i buduće ponašanje ljudi, tj. kakvi tehnološki trendovi će biti dominantni u lokalnim, regionalnim i globalnim okvirima, bez sumnje iziskuje jednu holističku projekciju inovativnih rešenja, koja se istovremeno bazira i na korisničkim iskustvima i raznovrsnim istraživačkim i naučnim naporima, kako bi se istim došlo do rešavanja konkretizovanih društvenih, privrednih, životnih i sličnih pitanja, ali i problema koji u današnje vreme

predstavljaju balast za gotovo sve zemlje, bez obzira na njihov razvojno-tehnološki status (Čelik, P. 2019:61-81).

Brojne istraživačke studije, nastale kao rezultat opsežnih empirijskih istraživanja, urađene od strane različitih referentnih i u ovoj oblasti etabliranih naučno-istraživačkih institucija, iako polaze od različitih metodoloških pristupa i kriterijuma za podelu, imaju niz približno sličnih zaključaka, posebno kada se radi o ključnim tehnološkim trendovima. U tom pogledu, izuzetno je zanimljiv i ilustrativan izveštaj instituta McKinsey u kome se taksativno navodi lista od 12 tehnologija koje će imati značajan uticaj na ekonomiju, obzirom da će doneti dobit iz među 14 i 33 triliona dolara godišnje do 2025. godine.

Grafikon br. 12 Disruptivne tehnologije i njihov procenjeni potencijalni uticaj u 2025. god. u trilionima dolara



Izvor: McKinsey Global Institute, 2013

U navedenom izveštaju, detaljno je opisano i egzaktnim podacima podržano stanovište o tome kako će ove tehnologije izgledati, koje su njihove dobre i loše strane, kao i izazovi sa kojima će se kompanije i državni organi suočavati u vezi sa njima. Iznete ocene u izveštaju bazirane su prvenstveno na dubinskoj analizi i suptilnoj proceni koliko će ove tehnologije biti korisne na više polja, kako će uticati na različite ekonomske sektore, uključujući i dodatnu vrednost potrošača koja će biti ostvarena boljim kvalitetom proizvoda/usluga, smanjenjem troškova, nižim cenama, čistijom i održivom životnom sredinom i poboljšanim zdravstvom.

Autori izveštaja navode sledeće tehnološke trendove:

- Mobilni internet
- Automatizacija rada znanja
- Internet stvari
- Cloud tehnologija
- Napredna robotika
- Autonomna i skoro autonomna vozila
- Sledeća generacija genomike
- Skladištenje energije
- 3D štampa
- Napredni materijali
- Napredna istraživanja nafte i gasa i oporavak
- Obnovljiva energija.

Na narednom grafikonu prikazane su nove tehnologije i njihov ekonomski potencijalni koji može proizvoditi novu vrednost kompanijama i tako značajno doprineti rastu BDP.

Potpuno je izvesno, kako se navodi u izveštaju, da će pojedine tehnologije poput robotike, automatizacije znanja i posla, Cloud tehnologije, mobilnog interneta, 3D štampe, autonomnih vozila i uređaja, napredno istraživanje fosilnih goriva i pronalaženje načina za razvoj obnovljivih energija, naprednih materijala i dr., u bliskoj budućnosti direktno uticati na gotovo sve aspekte života i rada.

Za razliku od ove projekcije, novija studija koju je nedavno objavio WEF sa odborom savetnika časopisa „Scientific American“ utvrđuje potpuno drugačiju listu najvažnijih tehnologija u nastajanju (emerging technologies) kreiranu na osnovu tri glavna kriterijuma:

- Potencijal poboljšanja života ljudi;
- Veličina transformacije jedne ili više industrija (disrupt);
- Step en održivog razvoja, odnosno očuvanja planete korišćenjem ovih tehnologija.

U studiji je prikazana lista od deset novih tehnologija koje će nepovratno, dakle ireverzibilno promeniti život na planeti.

Navedena lista uključuje sledeće tehnologije u nastajanju:

1. Tečna biopsija
2. Dobijanje čiste vode iz vazduha
3. Duboko vizuelno učenje
4. Tečna goriva od energije sunca
5. Atlas ljudskih ćelija
6. Precizna poljoprivreda
7. Isplativi katalizatori za „Zelena goriva“
8. Genetske vakcine
9. Održivo kreiranje naselja i gradova
10. Kvantni kompjuteri

Veliki iskorak u predviđanju budućnosti u tehnološkom smislu predstavlja i najnoviji Gartnerov izveštaj za 2019. godinu, u kome se decidirano ističe deset strateških tehnoloških trendova za 2019. godinu. Nove tehnologije poput Blockchain, kvantnog računanja, proširene analitike i veštačke inteligencije izazvaće, prema mišljenju vodećih stručnjaka ove referentne konsultantske kompanije, velike disrupcije, a kao odgovor na taj izazov i nove poslovne modele.

Prema mišljenju zamenika predsednika Gartner-a, Davida Cearley-a „vreme koje dolazi biće u znaku pametnih uređaja koji će, u zavisnosti od preferencija i potreba korisnika, pružati sve jasnije i dostupnije digitalne tehnološke usluge bilo gde u svetu“.

Taj razvoj se u savremenom informatičkom diskursu naziva „inteligentna digitalna mreža“ zasnovana na tri komponente i to:

Inteligentno – veštačka inteligencija se nalazi u gotovo svakoj postojećoj tehnologiji i stvara potpuno nove kategorije;

Digitalno – kombinovanje digitalnih i fizičkih sistema radi stvaranja tehnološki zarobljenog sveta;

Mesh – Iskorišćavanje veza između proširenih grupa ljudi, kompanija, uređaja, sadržaja i usluga.

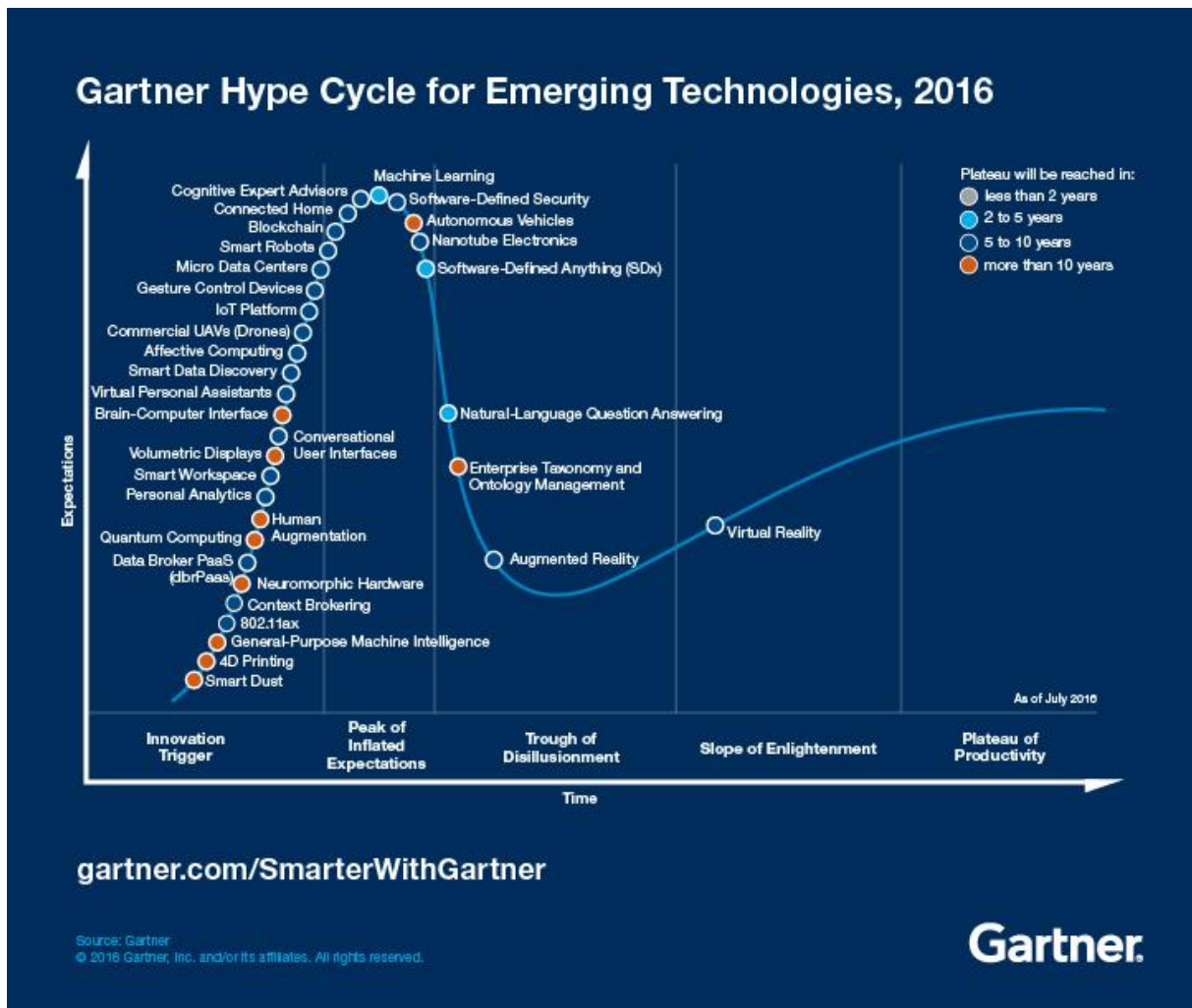
U svim ovim komponentama, trendovi su integralni deo u vođenju kontinuiranog inovacionog procesa, a to je u širem smislu deo kontinuirane buduće strategije.

Prema Gartneru, 10 strateških tehnoloških trendova do 2023. godine uključuju:

- | | |
|---------------------------------------|------------------------------------|
| 1. Autonomne uređaje (stvari); | 6. Tekuće tehnologije; |
| 2. Proširenu analitiku; | 7. Blockchain; |
| 3. Razvoj baziran na AI; | 8. Pametne prostore; |
| 4. Digitalne blizance; | 9. Digitalnu etiku i privatnost; i |
| 5. Osnaživanje graničnih tehnologija; | 10. Kvantno računanje. |

U jednom od ranijih izveštaja Gartnera, prikazane su pojedinačne tehnologije i vreme njihovog razvoja i implementacije. Konkretno prikazane su tehnologije počev od 2016. za periode do dve godine (2018.), od dve do pet godina (do 2021.), od pet do deset godine (do 2026.) i više od deset godina (nakon 2026.).

Slika br. 11. Gartnerov „Hype“ ciklus za nove tehnologije, 2016



Izvor: Gartner, 2016

Poglavlje III: Teorijske paradigme, koncepti i modeli digitalne ekonomije

1. Pojam i sadržaj digitalne ekonomije

Termin „digitalna ekonomija“ nije u potpunosti nov, a još manje nepoznat u naučno-stručnim krugovima. On se prvi put pojavio u knjizi Don-a Tapscott-a 1994. godine kao ideja sa revolucionarnim načinima na koje bi savremene tehnologije, a u prvom redu internet, promenili svet biznisa i poslovanja.

U ekonomskoj nauci postoji niz različitih definicija digitalne ekonomije, tako da je danas veoma teško odlučiti se koja je od njih celovita i svrsishodna. Tako na primer, neki autori digitalnu ekonomiju određuju kao „ekonomiju zasnovanu na digitalnim tehnologijama, uključujući i digitalne komunikacione mreže i druge povezane informacione tehnologije“ (Krsmanović, 2014:4).

Drugi autori pod digitalnom ekonomijom podrazumevaju „novu naučnu paradigmu koja treba da objasni čitav niz ekonomskih, socijalnih i kulturnih promena koje sa sobom nosi IKT, gde počasno mesto pripada internetu“ (Ćuzović, Sokolov-Mladenović, 2014:144).

Strani autori imaju drugačiji pristup kada je u pitanju digitalna ekonomija, ili kako se u zapadnim krugovima naziva „nova ekonomija“. Prema njihovom shvatanju, najčešće taj termin uključuje: „skup ekonomskih pojava i međusobno uslovljenih procesa zasnovanih na informacionoj tehnologiji koji podrazumevaju nove načine poslovanja i daljeg privrednog razvoja i jednostavno predstavljaju kvalitativno drugačiji obrazac ekonomskog razvoja. Ovakva definicija povezuje „staru“ i „novu“ ekonomiju u smislu da je prva još uvek samo oblik ispoljavanja tehnološkog i ekonomskog razvoja“ (Milovanović, Veselinović, 2009:17-23).

Drugi teoretičari, na primer Gordon, smatra da pojam „nova ekonomija“ uvek treba pisati pod navodnicima, jer ona ne postoji kao celovita paradigma, u potpunosti definisan koncept ili razrađena praksa. Uporedo sa tim terminom, u etabliranim i referentnim publikacijama, često se koriste pojmovi kao što je internet ekonomija, web-ekonomija i nova ekonomija, a u novije vreme koristi se naziv „ekonomija znanja“. Po pravilu, digitalna ekonomija predstavlja ekonomiju utemeljenu na digitalnim inovacijama i tehnološkim rešenjima koja se baziraju na primeni IK tehnologija, hardvera, softvera i aplikacija posredstvom telekomunikacija u svim funkcionišućim oblicima ekonomije. Posebno, ona obuhvata unutrašnje aktivnosti (države,

neprofitnih i njima sličnih organizacija, kompanija, udruženja, itd.), zatim eksterne aktivnosti (različite vrste transakcija između samih organizacija, pojedinaca i organizacija, kao i pojedinaca kao potrošača i ostalih građana i njihovih struktura).

Digitalna ekonomija kroz dinamičan razvoj briše ranije granice između tradicionalne i savremene ekonomije, između ekonomije bazirane na resursima i ekonomije znanja, tj. ekonomije zasnovane na bit-ovima i bajt-ovima.

Među ekonomistima ipak postoji saglasnost da je moderna digitalna ekonomija vodeći pokretač ili generator inovacija u privredi i motor preduzetničke kompetitivnosti, usled čega omogućava većini kompanija i organizacija, rast, produktivnost, konkurentnost, stabilnost i što je najvažnije, opstanak na tržištu.

Trendovi koje „nova“ internet, odnosno digitalna ekonomija uspostavlja i nameće, naglo i fundamentalno menjaju način poslovanja, ali i funkcionisanja tržišta rada. Elektronska dimenzija nove ekonomije prisutna je u najrazličitijim granama poslovanja i biznisa – od trgovine, bankarstva, energetike, transporta, industrijskih sektora, ali i oblasti medija i izdavaštva, itd. Takođe, evidentan uticaj digitalne ekonomije vidi se i u osetljivim delatnostima javnog sektora, kao što su socijalna zaštita, obrazovanje, zdravstvo, informisanje, itd.

Digitalni stratezi najčešće navode 4 ključna uticaja koja digitalna ekonomija ispoljava na koncept i privredni sistem u celini: kreiranje novog sadržaja ili upotrebne vrednosti za proizvode i usluge koji ranije nisu postojali, zatim novi način i model poslovanja u okvirima novih poslovnih pravila, onda unapređenje postojećih biznis sadržaja (npr. Uber usluge i sl.), te novi način međusobne komunikacije, kako između proizvođača i pružaoca usluga, tako i potrošača.

U današnjem, sve više digitalnom dobu, savremene tehnologije su postale neizostavni element i pratilac svih nastojanja za promenama i njihovim upravljanjem, ali i kreiranje novih oblika uspešnog pozicioniranja svih učesnika (stakeholder-a) u procesu, od države, do pojedinca, malih, srednjih ili velikih preduzeća, kao i običnih preduzetnika. Osnovne karakteristike digitalne ekonomije su „elektronsko poslovanje, umrežavanje, globalizacija, virtuelizacija, digitalizacija, mobilnost, novi digitalni proizvodi i usluge, integracija, disintermedijacija, kao i nove organizacione forme i modeli“ (Mutula, 2010:17).

Sa uvođenjem digitalizacije, nova ekonomija više nema potrebu za posredovanjem, obzirom da robe i usluge više nisu samo materijalne, već se pojavljuje čitav niz digitalnih proizvoda. Preko toga, virtuelizacija je učinila nebitnim fizičku lokaciju i neposrednost poslovnih kontakata, tako da se poslovne transakcije obavljaju u potpuno virtuelnom kontekstu i okruženju.

Disintermeditacija tržišta, kao potpuno novi fenomen, preuzeta je iz američke ekonomske teorije i omogućila da potrošači mogu direktno pristupiti proizvođaču, čime su u mogućnosti da zaobiđu posrednike, trgovce i sl.

Takođe, novu, odnosno digitalnu ekonomiju, karakterišu znanje i informacija kao osnovne vrednosti za proizvodnju i potrošnju. Kompanije i javni servisi koji nastoje poboljšati svoje rezultate, najpre moraju raspolagati sa pravim informacijama, a zatim imati veštine za upravljanje znanjem. Efekat, odnosno uspešnost upravljanja znanjem, u velikoj meri je zavisno od alata kojima se olakšava proizvodnja znanja, njegova interpretacija, kontekstualizacija, rekonstrukcija i primena. Zapravo, osnova digitalne ekonomije leži na znanju koje suštinski utiče na konkurentnost kompanije, tj. organizacije, ili pojednostavljeno, količina i kvalitet znanja i informacija imaju direktni uticaj na poslovni pejzaž, a time i na ukupnu konfiguraciju poslovanja.

Kao što je već napred navedeno, digitalna ekonomija se primarno temelji na dodanoj vrednosti koju generišu nove tehnologije, kao i novi načini primene istih, koji kao takvi podstiču nove poslovne modele. Raznovrsna i masovna primena tehnologija u kompanijama značajno utiče na opštu primenu inovacija, ali i na rast produktivnog kapaciteta u drugim sektorima, gde upotreba tehnologija omogućava, ne samo poboljšanje poslovnih modela i strategija, već i istraživanje i mogućnosti stvaranja potpuno novih poslovnih formi koje značajno mogu promeniti budućnost postojećih kompanija i sektora na tržištu.

Prema tome, nema implementacije, niti razvoja digitalne ekonomije, ukoliko pre toga nije uspostavljena razvojna infrastruktura/platforma na kojoj se mogu graditi usluge ili procesi sa dodatom vrednošću, kako za informatičku, tako i za druge industrijske grane.

Za uvođenje digitalne ekonomije potrebno je osigurati znanje koje poseduju zaposleni i kreatori novog poslovnog nastupa, kao i znanje nastalo iz korisničkog iskustva, uključujući i iskustva svih onih koji mogu u bilo kom momentu ili fazi uzeti učešća u aktivnostima vezanim za digitalnu ekonomiju (mentori, savetnici, medijatori, eksperti, itd.).

Potpuno je izvesno da u tom kontekstu znanje predstavlja kapital čije obezbeđenje nije tako jednostavno ostvariti. Naime, tržište digitalne ekonomije, u širem smislu tržište IKT, faktički je u stalnoj potrazi za novim kadrovima i specifičnim profilima od kojih se naročito traži veliko i upotrebljivo iskustvo. Stoga je za većinu kompanija, stvaranje preduslova, izgradnja i održivost kapitala i tehnološkog znanja, imperativ prvog reda i pretpostavka većeg interesa ciljanih investitora, ciljanih i razvojnih kompanija, koje su spremne za te potrebe izdvojiti značajna finansijska sredstva. Ipak, izgradnja ovakvog „intelektualnog“ kapitala nije samo interes privatnog ili korporativnog sektora, već i celog društva, ukoliko u svojim strateškim i razvojnim projekcijama ima jasno definisano opredeljenje za uspostavljanje tzv. „društva znanja“ koje konvergira strategiju održivog razvoja.

Digitalna ekonomija danas nije samo koncept, inicijativa ili strategija, ona je primarno razmišljanje o tome kako digitalna transformacija utiče na naše okruženje, na koji način ga menja i kako će oblikovati njegovu budućnost.

Digitalna ekonomija je, iz navedenih razloga, osnovni pokretač gotovo svih industrija, a posebno onih koje su svoj budući portfolio odredile kao tehnološki profilisan. Gotovo bez izuzetka, svaka zemlja ima neku od tako ugrađenih smernica, bilo da je u pitanju digitalna ekonomija, internet ekonomija, digitalni rast, digitalna proizvodnja i sl., što samo po sebi potvrđuje da poslovni svet, nezavisno od geografskog područja ili vrste industrije, postepeno ulazi u digitalno doba, tj. u ireverzibilni ili bespovratni transformativni proces.

2. Razvoj i komponente digitalne ekonomije

Iz dosadašnjeg razvoja digitalne ekonomije, mogu se bez većih teškoća izdvojiti njene najvažnije komponente. U njih spadaju vlada, regulativa, politike, internet, World Wide Web (www), industrija telekomunikacija, pružaoci digitalnih usluga, e-poslovanje i e-trgovina, informacije i sistemi za upravljanje znanjem, prava iz domena intelektualne svojine, ljudski kapital i primenjiva znanja radnika, kao i istraživanje i razvoj novih tehnologija i rešenja (Krsmanović, 2014:4-10)

Ključna, ali ne i jedina uloga vlade kao komponente digitalne ekonomije, nije samo u izgradnji komunikacione infrastrukture, nego i na planu unapređenja tzv. e-spremnosti zemlje. Polazeći od normativnog okvira, konkretno nadležnosti i ovlašćenja, iako njihov opseg varira od države do države, vlade su prevashodno zadužene za izradu nacionalne strategije razvoja informacionog

društva, kao i za izgradnju infrastrukturne vizije sa ciljem unapređenja u domenu pružanja digitalnih usluga.

Od spremnosti i visine sredstava predviđenih budžetom za razvoj informacionog društva, zavisi i u kojoj meri će biti razvijen nivo poslovanja unutar kompanija, odnosno koliko su one tehnološki podržane i uopšte koliko se oslanjaju na digitalne tehnologije u svom poslovanju. Na strani potražnje, vlade se javljaju i kao veliki potrošači u segmentu informacionih tehnologija, prvenstveno kroz velike projekte IKT-a u javnom sektoru u cilju unapređenja javnih servisa koje država pruža preko svog javnog sektora. Na kraju, vlade kroz različite podsticaje, mehanizme ili instrumente privlače investicije u sektoru IKT-a, najčešće putem carinske politike (olakšicama), smanjenjem poreskih opterećenja za nabavku računarske i telekomunikacijske opreme, i sl.

Prilikom izgradnje informacionog društva koje se temelji na digitalnoj ekonomiji, veliki značaj imaju javne politike, a posebno politika o razvoju IKT. Jasno definisanje politike u toj oblasti podrazumeva usvajanje zakona i podzakonskih akata koji regulišu ključna pitanja iz ove oblasti, daju transparentan i otvoren poslovni okvir, jednostavnu i pristupačnu sa EU usklađenu korporativnu regulativu, kao i precizno uređen, stabilan pravni okvir za nesmetano odvijanje poslova, kako u nacionalnim, tako i prekograničnim elektronskim transakcijama.

Iz navedenog proizilazi da jasno formulisane politike i regulativa čine adekvatan sistem pravne zaštite za sve učesnike u digitalnim transakcijama. Pored toga, vlada ima obavezu da izgradi konkurentne telekomunikacije i tržište internet usluga, tj. da obezbedi poslovni ambijent za funkcionisanje tržišta, radi kasnijeg uključivanja u evropsko jedinstveno digitalno tržište.

Sa druge strane, internet i globalizacija su komponente bez kojih se ne može uspostaviti digitalna ekonomija. Opšteprihvaćena je činjenica da je danas internet „mreža svih mreža“ koja čini paradigmu savremenog poslovanja i metaforu novog digitalnog doba. Paralelno sa ključnim dostignućima interneta, odvija se i tzv. „poslovanje bez granica“, pri čemu je globalna razmena roba i usluga veoma jednostavna i lako usvojiva za sve kompanije koje se nalaze, ili planiraju izlazak na tržište. Uspostavljene Internet veze služe kao značajni pokazatelj nivoa e-spremnosti određene države, odnosno spremnosti njenih građana i preduzeća da učestvuju u visoko kompetitivnoj digitalnoj ekonomiji.

Pored interneta, od velikog značaja za preduzeća jesu i intranet i ektranet, jer omogućavaju bolju komunikaciju i razmenu podataka između poslovnih entiteta. Početak novog veka

obeležava i ekspanzija online bankarstva i finansija, online kupovine, online vesti, e-mail komunikacija i sl. U tom pogledu, internet je bio presudan faktor u globalizaciji svetske ekonomije, budući da se kupovina i prodaja može obavljati u cyber prostoru, bez ikakvih ograničenja. Iz tog razloga, često se ističe da je internet centralna komponenta digitalne ekonomije, dok World Wide Web čini integralni deo interneta koji obuhvata sistem servera na kojem se nalaze posebno formatirane informacije, kojima se neposredno može pristupiti preko web pretraživača.

U osnovi, hardver ili računarska oprema, predstavlja najširu i neizostavnu infrastrukturu za obradu, čuvanje i cirkulisanje poslovnog sadržaja u digitalnoj ekonomiji. Na tržištu, ali i u praksi, postoje različite hardverske platforme: mikroprocesori, neuronske mreže, klijent/server tehnologije, disk memorije, veštačka inteligencija i dr. (Krsmanović, 2014:4-10)

Specifičnost je u tome što svi ovi infrastrukturni segmenti deluju sinhronizovano, a neki i usklađeno i kompatibilno u digitalnoj ekonomiji. Poslednjih godina, evidentna je zastupljenost i novih tehnologija zasnovanih na bežičnoj i mobilnoj komunikaciji. Uzimajući u obzir te trendove, softverska industrija se težišno fokusirala na sledeće softverske proizvode od kojih su najvažniji: „ERP“ sistemi za planiranje resursa preduzeća, „CRM“ sistemi za upravljanje odnosima sa potrošačima, baze podataka, usluge kompjuterskog programiranja, kompjuterski integrisani sistemi, usluge preuzimanja informacija, kompjuterska obrada i dr. (Ibid)

Funkcionisanje digitalne ekonomije nije moguće bez komunikacionih proizvoda, a oni se generišu od strane industrije telekomunikacija. Globalna informaciona infrastruktura objedinjava, ili bolje reći integriše, nekoliko odvojenih komponenti: mobilnu telefoniju, satelitske mreže i informacionu opremu.

Nakon evoluiranja ove infrastrukture u mobilni i sveprisutni računarski sistem koji uključuje i lične digitalne asistente (PDA), mobilne (Smart) telefone, bežične kamere, laptopove, štampače, servere, internet, kućni intranet i dr., koji imaju uspostavljene tzv. „share interface“ (deljive interfejse), ulazimo u fazu njihove potpune integracije koja omogućava pored ostalog i razmenu informacija na globalnom planu putem svetske informacione infrastrukture.

Značajna i neizostavna komponenta digitalne ekonomije jesu digitalni pružaoci usluga koje čine internet provajderi, provajderi internet sadržaja i pružaoci aplikativnih usluga.

Komponente kao što su e-poslovanje i e-komerc industrija, predstavljaju kritične ili fokalne tačke za postavku savremenog u odnosu na tradicionalni vid poslovanja. Ako se uzme u obzir njegova širina i rasprostranjenost, e-poslovanje omogućava svim poslovnim „stakeholderima“ efikasnije uključivanje u komunikaciju sa domaćim i stranim klijentima, efikasniju obradu podataka ili transakcija i brže vreme odziva tj. uspostavljanja veze.

E-trgovina podrazumeva kupovinu i prodaju robe i usluga elektronskim putem kroz sistem kompjuterizovanih poslovnih „online“ transakcija koje se odvijaju putem interneta, mreža i drugih digitalnih medija. U pogledu sadržaja, e-trgovina obuhvata: naručivanje, fakturisanje, marketing, istraživanje tržišta, pronalaženje kupaca i dobavljača i sl.

Između učesnika e-poslovanja i e-trgovine, kontinuirano se razvijaju različite vrste interakcija, a pored ostalih, najčešće su: „e - poslovanje ka potrošaču (B2C), e - poslovanje između dva preduzeća (B2B), e - poslovanje tipa uprava prema korisniku (G2C), e - poslovanje uprava prema preduzeću (G2B), itd“ (Krsmanović, 2014:6).

Ostvarivanje funkcionalne digitalne ekonomije zahteva različite informacije i sisteme za upravljanje znanjem. Budući da poslovne organizacije postaju zavisne od znanja i informacija, upravljanje i razmena znanja postaje veliki izazov koji iziskuje edukovanje ili pronalaženje na tržištu adekvatnih kadrova koji imaju sposobnost razumevanja, sintetizovanja i razmenjivanja informacija i veština, kako bi kroz informacione kanale ti resursi postali podrška organizacionim, a time i proizvodnim procesima.

Izuzetno značajan aspekt digitalnog ekonomskog modela i infrastrukture čine autorska prava i širi kontekst intelektualne svojine, kako u segmentu e-trgovine, e-poslovanja, projektovanja i izgradnje web sajtova, tako i internet domena, patenata, distribucije sadržaja na internetu, partnerstva sa državnim i obrazovnim institucijama, a naročito razumevanje međunarodnih pravila i standarda vezanih za elektronsko poslovanje.

Stručnjaci se u potpunosti slažu, da ljudski kapital, odnosno njegovo kolektivno znanje i veštine, posebno kao radne snage, čini ponekad i zapostavljenu komponentu digitalne ekonomije. Ljudski kapital je i danas suštinski faktor konkurentnosti poslovnih sistema i na tom planu svi poslovni subjekti, pod pritiskom savremenih zahteva i masovne primene tehnologija, postaju prinuđeni da angažuju radnu snagu koja ima znanje i veštine za rad sa IKT, a u prvom redu IT stručnjake za web ekspertize, programiranje i elektronsko održavanje.

Bez istraživanja i razvoja, digitalna ekonomija ne može računati na dugoročni uspeh na izrazito dinamičnom i jako konkurentnom tržištu. Iz tih razloga postoji naglašena potreba za povezivanjem poslovnog sveta sa naučnim i istraživačkim institutima i centrima, kako radi uspostavljanja direktne komunikacije i saradnje, tako još više radi izrade projekata za dalje istraživanje i razvoj u oblasti IKT-a.

Za budući razvoj digitalne ekonomije, veliki značaj ima primena novih, nastupajućih i nadolazećih tehnologija. Za sada, veliki prodor u ovoj oblasti ostvaruju tehnologije Wi-Fi, Wi-Max, Bluetooth, Voice over internet protocol (VoIP), itd..

3. Izazovi digitalne ekonomije i temeljni principi

Široka i masovna primena informaciono-komunikacionih tehnologija (IKT), postali su globalni trend, ne samo u razvijenim, već i u tranzicionim ekonomijama. Prilikom nastojanja za sveopštom primenom interneta i e-poslovanja, kompanije se danas sa različitim intenzitetom suočavaju sa brojnim izazovima koji variraju od jedne do druge države, kao i između sektora.

U tekućim raspravama i naučnim analizama, često se navodi da je nemogućnost primene interneta u poslovanju primarno određeno nepovoljnim okruženjem, slabom infrastrukturom, nedostatkom IKT veština, visokim troškovima koji se odnose na fizičku opremu, mrežu i softver i na kraju, nepoverenjem u elektronske transakcije.

Generalno gledajući, najveći izazov u pogledu primene ovih tehnologija svodi se na „nemogućnost kupovine i održavanja širokopojasnog opsega i nemogućnosti sprovođenja bezbednosnih mera zbog ograničenih resursa“ (Krsmanović, 2014:8).

Pored toga, prisutne su različite vrste otpora kao posledice straha i deficita znanja o mogućnostima novih tehnologija. Najnovije pretnje u vidu cyber kriminala dodatno podižu nepoverenje, a situaciju dodatno otežavaju i usložnjavaju pitanja vezana za pravno obavezujuće sporazume izvršene putem interneta. Jednom rečju, prevlađuje mišljenje da još uvek ne postoji pravna garancija ili pouzdanost prilikom internet transakcija.

Drugi izazov je vezan za e-trgovinu. Ukoliko e-uprava ne obezbedi kvalitetne i razumljive, odnosno prihvatljive interfejse korisnicima, to će u praksi rezultirati značajnim uvećanjem troškova, što će dalje posledično uticati na ukupni nivo primene aplikacija iz domena e-trgovine.

Razvoj e-trgovine je u uskoj vezi sa uspostavljanjem jedinstvenog digitalnog tržišta. Taj prelazak ili napredak zahteva novi regulatorni okvir radi povezivanja računarstva u oblaku i mobilnih podataka, bez obzira na državne granice i geografske udaljenosti, što treba da dovede do pojednostavljenog pristupa informacijama i sadržajima uz zaštitu privatnosti, tj. ličnih podataka, odnosno ukupne cyber bezbednosti putem neutralne mreže.

Uklanjanje prepreka za transakcije putem interneta, suština je i cilj razvoja jedinstvenog digitalnog tržišta. Funkcionisanje takvog tržišta, npr. na prostorima EU za sada stvara mogućnost pristupu informacijama, poboljšanju efikasnosti u smislu smanjenja troškova transakcija, dematerijalizaciji potrošnje i smanjenju ekološkog traga, te mogućnosti uvođenja poboljšanih poslovnih i administrativnih modela. Razvoj e-trgovine donosi konkretnu korist potrošačima kroz nove proizvode koji se brže razvijaju, niže cene, veći izbor, te kvalitetniju robu, usluge i dr.

Postojeće virtuelno okruženje, usled različitih ograničenja i brojnih nedefinisanih pitanja, onemogućava korisnike, ali i druge aktere, da imaju jasne predstave o tome ko su ugovorne strane, koja je regulativa važeća i ko je konačno odgovoran za njenu primenu. Upravo te pravne praznine i neizvesnosti deluju destimulativno na potencijalne korisnike, usled čega ih takva situacija i udaljava od e-trgovine. Pitanje bezbednosti je takođe prisutno, a naročito prilikom plaćanja platnim, odnosno kreditnim karticama, te primenom elektronskog potpisa i sl. elektronskih dokumenata.

Treći izazov je u vezi politika, nadležnosti organa i same primene zakona. Ukoliko se e-transakcije odvijaju između dve ili više različitih država, iz napred iznetih razloga najčešće dolazi do krajnje složenih i komplikovanih situacija zbog primene različitih trgovinskih propisa.

Zbog neusklađenosti zakonskih propisa u ovoj oblasti, ali i njihovog različitog tumačenja, neretko dolazi do sporova između korisničkih strana, a u najtežim slučajevima, stranke traže zaštitu svojih prava na sudu.

Organizacija za ekonomsku saradnju i razvoj (OECD), usvojila je politiku koja omogućava državama članicama ove organizacije pristanak na neutralnost pri oporezivanju, efikasnost, bezbednost, te pravičnost i fleksibilnost. Normativni akti koji se odnose na potrošače, iz ovih razloga ne mogu se primenjivati u zemljama odakle potiče prodavac, što u praksi stvara ogromne barijere.

I pored navedenih izazova i ograničenja, mnoge vlade podržavaju internet kao tržišno vođenu, ali još uvek neuređenu platformu. Primetna je inertnost ili nespremnost vlada da u potpunosti uredi oblast poslovanja putem interneta, a dok su ta pitanja još uvek neuređena, u praksi se pojavio novi pristup koji polazi od toga da se odnosi između korisnika na internetu mogu urediti kroz privatno i zajedničko delovanje, a ne putem pravne regulative. Suština ovog predloga je u tome da korisnici zaštite svoju privatnost uz istovremenu kontrolu sadržaja elektronskih poruka, kao i zaštite od neprimerenog ponašanja nekih učesnika e-trgovine.

Prvi korak u rešavanju tih izazova, jeste obaveza vlade da stvori povoljan ambijent za neometano odvijanje elektronskih transakcija uz uklanjanje ograničenja u primeni IKT-a. Pored toga, vlade treba da donesu i usklađene politike i strategije, harmonizuju zakonodavstvo, kako bi učesnici elektronske trgovine mogli da bez ikakvih poteškoća uživaju prednostima digitalnog poslovnog modela i okruženja.

4. Najznačajniji pravci kretanja digitalne ekonomije u bliskoj budućnosti

Poslednjih nekoliko godina, veliki broj naučnika posvetio se proučavanju fenomena digitalne transformacije i njenih izazova, kao i tome koji će to biti najznačajniji trendovi u ovoj oblasti. Izučavanje ovog fenomena je utoliko teže iz razloga što digitalna transformacija, kao ekonomsko-tehnološki fenomen nije samo tehnološka promena, već tehnološka promena koja se odvija na raskršću koje obuhvata mnoge oblasti, počev od same tehnologije, preko poslovanja sve do samih ljudi, a što samo po sebi daje ne samo širok, već i dubok dijapazon mogućnosti.

Usled ovakvog razvoja, velikom broju kompanija je postalo jako teško predvideti koji je pravi put kojim treba krenuti, a samim tim i zašto je put koji bi se odabrao, zapravo onaj pravi, ako se u vidu imaju sada već dnevni poslovno-tehnološki pomaci. Ono što je važno inicijalno razumeti, jeste da tehnologija sama po sebi ne čini digitalnu transformaciju, jer digitalnu transformaciju čine i kupci, poslovna kultura i zaposleni u kompaniji, koji moraju biti deo srži svake tehnološke investicije, a koja opet ima za cilj održanje kontinuiteta poslovanja uz stalni rast i progres. S tim u vezi, predviđanja su da će trendovi digitalne ekonomije i dalje ići u različitim pravcima.

4.1 Fiksni 5G i 5G mobile

O 5G mreži, kao poslednjoj generaciji tehnologije, sve se više govori. Kako se radi o potpuno novoj tehnologiji, odnosno tehnologiji u eksperimentalnoj fazi razvoja, ona je prisutna samo

mestimično i u kontrolisanim uslovima. U slučaju putovanja po svetu, moguće je primetiti da mobilni uređaji s vremena na vreme „kliznu“ u zone mreža starijih generacija (kao što su 2G i 3G), međutim, iako se to desi, to ostaje bez nekog posebnog funkcionalnog problema po korisnika, osim eventualno promene brzine rada uređaja u tom periodu. Sa druge strane, na pojedinim mestima i u određenom prostoru 5G mreža funkcioniše i ima svoj pun kapacitet, međutim veliki broj korisničkih uređaja i dalje nema tehničke karakteristike koje bi omogućile korisnicima da iskoriste pun 5G mrežni potencijal.

Pokušavajući da reše ovaj problem, sve kako bi svuda i na svakom mestu postojala 5G mreža, u tehnološkoj zajednici je najpre osmišljen sistem fiksnih test mesta na kojima je ova tehnologija implementirana, pa su u tom domenu iskoračile kompanije kao što su Qualcomm, Nokia, Ericsson, Samsung, Huawei i Intel. Međutim, u prostoru koji je time ostao upražnjen, a to je mobilni 5G segment, sa ciljem osvajanja i zauzimanja ovog tehnološkog prostora, pojavile su se potuno nove kompanije koje su svoj poslovni koncept zasnovala na omogućavanju implementiranja 5G mreže na urbane, ali i ruralne lokacije. Jedna od takvih kompanija je Mimoso Networks, koja je razvila sopstveno tehnološko rešenje koje naziva „Spectrum Reuse Sinhronization“ (SRS).

Ovom tehnologijom otvoren je put da kompanije kao što su AT&T i Verizon počnu širiti ponudu novim, bržim i inovativnijim uslugama za mobilne korisnike. Samim tim već sada postoje test lokacije na kojima se testira fiksni 5G i može se reći da u tom smislu za ovu tehnologiju najveće interesovanje pokazuje akademska zajednica. Tako recimo AT&T već izvesno vreme u gradu Austin u Texasu testira ovu tehnologiju, a za nju su pokazala interesovanje još 2 grada u kojima se nalaze veliki univerziteti i studentski kampusi i to Univerziteta Baylor i Univerziteta Notr Dam. Istovremeno i kompanija Verizon Wireless pokrenula je testiranje fiksnog 5G u 11 američkih gradova.

U ovu tehnološku trku uključio se i jedan od najvećih mobilnih operatera u SAD, Sprint, kome se pridružila i svetski poznata telekomunikaciona kompanija T-Mobile. Ove kompanije, iako nisu izvorno razvijale segmente u poslovanju koji bi mogli da isprate 5G tehnologiju, odlučile su da te početne zaostatke kompenzuju akvizicijama manjih kompanija specijalizovanih za rešenja iz ove oblasti kako ne bi izgubile trku sa konkurencijom koja nezaustavljivo osvaja pozicije na ovom novom trendovskom polju.

Neke kompanije (kao što je AT&T) pribegle su i marketinškim „trik“ rešenjima u kojima su svojim korisnicima nudili tzv. 5G Evolution opciju, iako se ne radi o 5G standardu, već poboljšanoj verziji aktuelnog 4G LTE mobilnog internet standarda. Ovakav tehnološki trend u „zoni“ 5G zapravo je izazvao tektonske disruptivne poremećaje na tržištu, upravo jer se među konkurencijom pojavio određeni broj manjih kompanija sa krajnje svežim i inovativnim rešenjima, pa su te kompanije agilnije pristupile postojećim tržišnim nišama u jasnoj nameri da nametnu svoja rešenja i standarde i osvoje poziciju na tržištu.

4.2 Chatbots tehnologija

Do pre nekoliko godina, obavljanje „razgovora“ na jezicima ljudi sa mašinama bio je proces koji se kretao od frustrirajućeg do smešnog. Međutim, za samo nekoliko godina, situacija se i na tom polju drastično promenila, pa su mašine dobile algoritme za učenje, što je ovaj segment velikom brzinom približilo tome da će uskoro biti izuzetno teško razlikovati da li ste u razgovor stupili sa čovekom ili mašinom.

Iako je tzv. NLP (Natural Language Processing and Recognition) tehnologija još uvek daleko od savršenog, mnoge kompanije su ipak odlučile da kapitalizuju ovu tehnološku mogućnost, pa su u svom poslovanju uvećale broj angažovanih chatbot-ova i to najčešće u segmentu odnosa sa kupcima, ali i segmentu unutrašnjih poslovnih procesa u kojima chatbot-ovi mogu biti i trening asistenti tzv. „Training Assistants“. Ovaj način primene chatbot tehnološkog trenda, promeniće nesumnjivo mnoge poslovne segmente i domene u kojima su nam oni do sada bili poznati.

Na 6. Međunarodnoj Konferenciji ICLR koja je održana u Vankuveru u maju 2018. godine, glavna tema bila je prezentiranje dometa mašinskog učenja. Na ovoj konferenciji okupio se veliki broj naučnika, pa je među njihovim izlaganjima posebno interesantno bilo izlaganje šefa naučnog tima kompanije Sales Force, Richard-a Socher-a, koji je predstavio dostignuća u istraživanjima koja pokrivaju NLP (Natural Language Processing and Recognition), odnosno mašinsko prevođenje i odgovaranje mašina na postavljena pitanja. Tom prilikom je izneo da će NLP učiniti neverovatne pomake u određenim segmentima poslovanja, jer je kao tehnologija sposoban da iz temelja promeni načine na koje se pružaju usluge, načine na koje razumemo prodajne procese i načine na koje danas radimo marketing. On je takođe ukazao na izuzetan značaj društvenih medija, gde će biti jako važno da NLP ne samo razume jezik, već i sentiment

koji je inicijalno postavljen oko određene marketinške poruke, a pored toga, NLP mora razumeti kako ljudi uopšte percipiraju vaš brend. (Socher, 2018)

Iako sve ovo idilično zvuči, to i dalje ne znači da istovremeno sa „idilom“ ne otvara određena pitanja koja se kreću čak i do toga da li bi ljudi, ako bi to znali, stvarno želeli da razgovaraju sa mašinama o svojim potrebama i problemima?

Sa druge, tj. poslovne strane, sve ovo izuzetno ima smisla, pa za početak, kompanijama je nemerljivo jeftinije da se istovremeno dešava hiljadu simultanih „customers service“ razgovora sa mašinom, nego da se to dešava sa ogromnim call centrom u kome radi isto toliko ljudi na istim poslovima.

Sa druge strane, mora se postaviti i jedno pitanje koje sagledava i to, da li kroz ovu inicijativu postoji i nešto što time dobijaju i sami korisnici? Može se reći, da će, osim što usluga koju korisnici zahtevaju može biti brža, efikasnija i donekle korisnija, korisnici zapravo ostati bez bilo kakvog drugog dobitka, što donekle pokazuje da je ovakva digitalizacija poslovanja suštinski usmerenija na racionalizaciju poslovanja, nego na ostale povezane segmente u domenu korisničkih benefita. Na kraju krajeva, činjenica je da korisnici najpre zahtevaju brz odgovor na svoj zahtev, a sa druge strane, ako bi želeli da razgovaraju sa čovekom u korisničkom centru, alternativa chatbot opciji jeste da preslušaju desetominutni meni, da preslušaju desetine opcija koje automat nudi vrteći ih u krug, kako bi tek posle toga stekli mogućnost da pritisnu određeno dugme putem koga bi na kraju govornog menija mogli stupili u kontakt sa drugim čovekom, što zapravo nije ni brzo, ni efikasno, ni u skladu sa željama potrošača, a samim tim ni jeftino.

Da bi NLP tehnologija postigla svoju punu efikasnost, ona mora biti podvrgnuta konceptu agregacije i proširenja. Tako, pre nego što bi se razmišljalo o razgovoru između jednog čoveka i jedne mašine, chatbot-ovi u saradnji sa veštačkom inteligencijom (AI) mogu biti organizovani tako da nadgledaju i vrše uvid u svaku pojedinačnu konverzaciju, kako bi iz nje izvukli pouke i saznanja kako postići bolje performanse u narednim konverzacijama sa ljudima, odnosno korisnicima.

Kada je koncept proširenja u pitanju, to znači da mašine ne moraju voditi celokupnu konverzaciju, već će chatbot-i uskočiti po potrebi i izvršiti rutinske operacije, kao što su tipski odgovori na direktna pitanja iz baze znanja organizacije, ili govoriti o eventualnim detaljima plaćanja vezano za određenu uslugu.

Ovakav pristup može dovesti do rešavanja čak i onih slučajeva kada mašina nije u stanju da adekvatno sprovede celokupni razgovor. U takvom slučaju brzina mašinske analitike u realnom vremenu, kakva postoji danas, može učiniti da chatbot-ovi alarmiraju operatera u situaciji u kojoj otkriju, na primer, da je kupac uznemiren, u kom slučaju će zahvaljujući automatskoj analitici sentimenta kupca pozvati ljudskog operatera da preuzme aktuelni chat ili poziv.

U smislu iznetog, može se reći da su chatbot-ovi neka vrsta inteligentnih asistenata, odnosno predstavnici tehnologije koja omogućuje funkcionisanje „Siri“ ili „Google asistenta“ na mobilnom telefonu, odnosno „Microsoft Cortana-e“³, na desktop računaru.

Spiceworks studija iz 2018. godine, otkriva da će 40% velikih kompanija (sa više od 500 zaposlenih) implementirati tehnologiju inteligentnih asistenata ili chatbot tehnologiju do 2019. godine na uređajima u vlasništvu kompanija, nasuprot 25% kod kompanija srednje veličine i 27% kod malih biznisa. Ovaj nalaz daje indikaciju da iako je usvajanje ovih tehnologija u porastu, da su neke organizacije još uvek uzdržane, kako u nedostatku slučajeva u kojima bi ove tehnologije mogle primeniti u okvirima redovnog poslovanja, tako i radi očigledne zabrinutosti za bezbednost (Spiceworks Study, 2018).

Interesantno je napomenuti da ista studija u prezentiranju nalaza iznosi i zapažanja u delu primene ovih tehnologija po odeljenjima u kompanijama, precizirajući da rezultati studije kažu da 53% kompanija AI chatbot-ove i pametne asistente već koristi u svojim IT odeljenjima, 23% ih koristi kao podršku administrativnim odeljenjima, dok samo 20% koristi ove tehnologije pri odeljenjima za podršku korisnicima, a samo 16% organizacija koristi ove tehnologije u njihovim odeljenjima za prodaju i marketing.

Pretpostavlja se da će u budućnosti chatbot-ovi najverovatnije biti u mogućnosti da stvari odvedu čak i dalje od opisanog, pa čak i da predlože strategiju i taktiku za prevazilaženje poslovnih problema kompanija. Predviđa se takođe i da će ove tehnologije moći da pomognu u izradi efektnih marketinških poruka baziranih na razumevanju samog jezika, poruke i analitike prethodnih poslovnih uspeha i neuspeha.

Kao i sa ostalim primenama veštačke inteligencije, i razvoj NLP tehnologije je definitivno daleko od svog kraja, usled čega se čini da će nivo i kvalitet razgovora sa mašinama kakav

³ Studije su pokazale da je Microsoft Cortana najčešće korišćeni pametni asistent na radnim mestima iz razloga njene integrisanosti u Windows 10, nalik na to kako je prethodno bilo sa Internet Explorer-om.

imamo danas, nesumnjivo delovati arhaično i bukvalno, ali i krajnje neprirodno za samo nekoliko godina od danas. Jedan od razloga za to je i taj što organizacije sasvim jasno postaju sve više komotne u domenu integrisanja chatbot-ova i pametnih asistenata u svoje poslovne procese, verujući da će ih to dovesti do poboljšanja, kako efikasnosti poslovanja, tako i većeg broja zadovoljnih korisnika.

4.3 Povezani oblaci (javni, privatni i hibridni)

Od samog starta, Cloud tehnologija bila je u centru pažnje i izazivala razne kontroverze. Ono što se može reći za ovu tehnologiju, jeste da je ona u potpunosti zaživela i da već počinje da doživljava evolucije i širenje u obuhvatu i primeni. Bezbednost poslovnih podataka je od samog početka bila jedan od ključnih razloga koji je dovodio do uzdržanosti korisnika prema cloud tehnologiji. Međutim, smanjenje troškova poslovanja i masovna primena on-line digitalnih servisa, i u suštini značajna eksternalizacija poslovnih aktivnosti koncipiranih „na zahtev“, učinila je ovu tehnologiju primamljivijom od razloga koji su od nje odvrćali.

Tokom prakse primene računarstva u oblaku, ispostavilo se da su kompanije koje su prišle ovom rešenju, shvatile da korišćenje samo javnog, samo privatnog ili samo hibridnog cloud-a, nije uvek najbolja opcija, obzirom da je kompanijama s vremena na vreme potrebna mešavina dva ili svih ovih oblika cloud-a radi efikasnog vršenja poslovne funkcije. U tom smislu, cloud provajderi su počeli sa intenzivnim razvijanjem ovog segmenta poslovanja, kako bi u potpunosti ispratili promene u zahtevima kompanija/korisnika, bez obzira na to da li kompanijama treba samo storidž usluga, umrežavanje, bezbednost ili implementacija aplikacija.

Glavni ili vodeći „public cloud“ dobavljači, kao što su Amazon i Alibaba, shvatili su ove potrebe korisnika veoma ozbiljno i svojim inoviranim poslovnim konceptom počeli su odgovarati na ove potrebe nudeći i usluge „privatnog cloud-a“. Veliki broj drugih kompanija počeo je pratiti ovu inicijativu, pa je i u tom poslovnom domenu došlo do razvoja „multi cloud“ rešenja. Ovakav pristup treba da omogući efekat, da nezavisno od stepena radnog opterećenja cloud infrastrukture, bez obzira na vrstu cloud-a, IT iskustvo korisnika i iskustvo onih koji koriste cloud usluge, mora biti besprekorno, bezbedno i racionalno. Stoga se veliki broj preduzeća i opredelio za racionalnu kombinatoriku radnog opterećenja u javnom, privatnom i hibridnom okruženju, gde je u smislu digitalnog ekonomskog trenda ovo jedna od najznačajnijih tema za 2019. godinu, a verovatno će tako biti i u narednim godinama.

4.4 Blockchain koji se konačno razume

Godine 2018., bila je obeležena 10. godišnjica od objavljivanja „Bitcoin White Paper“ (Bitcoin Bele knjige), čime je Blockchain tehnologija uspostavljena kao tehnološki ekvivalent internetu iz 1998. godine.

Godine 2017., Bitcoin je ušao u mainstream fazu, što bi trebalo da posluži kao podsticaj za rešavanje problema praćenja transfera i transakcija kroz Blockchain tehnologiju. Međutim, činjenica je da se određene tehnologije i brendovi i dalje kreću malo usporenijim tempom nego što su to njihovi tvorci ili analitičari predviđali.

Jedan od ključnih razloga za to, jeste što su mnoge tehnologije, a među njima svakako prednjači Blockchain, zapravo veoma komplikovane za razumeti i primenjivati, dok sa druge strane za nju još uvek nisu propisani ni standardni načini upotrebe, pa se ispostavlja spornim to što je svako želi koristiti na svoj način, čime se dodatno komplikuju već prilično komplikovane okolnosti.

U smislu toga, neke od vodećih kompanija iz domena tehnologije, kao u konkretnom slučaju IBM, na sebe su preuzele obavezu da nastave sa razvojem Blockchain tehnologije, kako bi ona bila u primeni i izvan oblasti kripto valuta.

Ove najave i dešavanja na ovom polju, finansijska industrija veoma pažljivo prati, kao i industrija transporta robe i usluga, uvidevši da im Blockchain tehnologija može puno ponuditi i u slučaju njene masovne primene u ovim oblastima. Iz ovih razloga je sasvim izvesno i jasno da se trendovski potencijal u digitalnoj ekonomiji u 2019. i narednim godinama, može staviti u kontekst Blockchain tehnologije, posebno ako se imaju u vidu neka sručna predviđanja, da će razvoj pojedinih servisa svakako potrajati 2-3 godine, dok ne dođe do trenutka koji će dovesti do ostvarivanja ovih planova.

4.5 Data to Analytics – Machine Learning to Artificial Intelligence (AI) - Analitika podataka, mašinsko učenje i veštačka inteligencija

Vrednost podataka postala je ključni poslovni resurs putem koga kompanije stiču dragocena saznanja na osnovu kojih mogu donositi važne poslovne odluke, a samim tim i kvalitetne odluke u vezi proizvoda, usluga, zaposlenih, strategija, itd.

Sudeći po aktuelnim trendovima, nema naznaka da će u tom smislu biti promena. Ono što je kuriozitet sadašnjeg vremena jeste da određena istraživanja pokazuju da je 90% od svetskog

broja podataka nastalo u protekloj godini, dok je drugi kuriozitet da istraživanja takođe pokazuju da se od svih tih prikupljenih podataka samo 1 procenat se koristi efektivno.

Aktuelni tržišni lideri, kao što su Microsoft Salesforce i dr., svoju lidersku poziciju zasnivaju na konceptu pretvaranja podataka u smislenu poslovnu analitiku, mada i dalje mnoge organizacije ne shvataju pravu snagu i moć podataka i prave razloge za njihovo prikupljanje. U svakom slučaju, došlo je do značajnog poboljšanja na polju obrade podataka koja može povećati stepen mašinskog učenja, tako da trendovi u vezi sa tim sasvim logično ukazuju da će digitalni lideri još više investirati u kreiranje podataka u cilju poboljšanja efekata mašinskog učenja i razvoja veštačke inteligencije.

Može se već sada reći, pa i predvideti, da će rast u ovom domenu najpre biti relativno skroman od 3-4% do 2020. godine, međutim, čak i tako skroman rast proizvešće ogromno povećanje, kako samog broja podataka, tako i načina za njihovu praktičnu i efikasnu upotrebu.

4.6 GDPR (General Data Protection Regulation)

U maju 2018. godine, na snagu je stupila Evropska uredba o opštoj zaštiti podataka (GDPR). Međutim, čak ni skoro godinu dana od tada, bar 1/3 on-line kompanija nije uskladila svoje poslovanje sa ovim važnim propisom.

Iako se radi o uredbi Evropske Unije, kuriozitet je da ona ipak ima prekogranični karakter, pa samim tim i primenu. Ipak, iako je ovo apsolutna činjenica, neke analize govore da u ovom trenutku približno hiljadu američkih web sajtova sa vestima nisu dostupni u Evropi, jer nisu u dovoljnoj meri zainteresovani ni za bezbednost podataka, ni za primenu ove uredbe, što čini se govori i o tome da zapravo nisu zainteresovani ni za svoje klijente i njihovu bezbednost u domenu ličnih podataka.

GDPR uredba predstavlja jedan ozbiljan izazov za sve one koji su skloni poštovanju pravila, obzirom da ih ova uredba obavezuje na značajno veće poštovanje svega što je u vezi sa njihovom interakcijom sa kupcima i klijentima. Kako se sam biznis većinski kreće prema proizvodima i uslugama zasnovanim na podacima, uredba GDPR zapravo i služi kao mehanizam prisile da kompanije prodube svoje odnose sa kupcima i da sve što rade u vezi njih zapravo rade na osnovu njihove saglasnosti i volje. Ipak, postoje i one kompanije koje su u stanju da stvari posmatraju i znatno dalje od samog usaglašavanja sa ovim propisom, pa one ovu uredbu vide kao jasnu

tržišnu šansu da sa svojim korisnicima izgrade suštinsko poverenje, a to je upravo u vreme kada je poverenje između klijenata i kompanija na internetu došlo na prilično nizak nivo.

Uredba GDPR apsolutno nije nastala bez velike nužde za regulisanjem neregulisanog, a to je bilo iz razloga što je pitanje zaštite podataka bilo krajnje neuređeno i puno uzimanja ličnih podataka ljudi „zdravo za gotovo“. Da bi se sa takvom praksom prestalo, bilo je potrebno da GDPR uredba uvede pravilo i obavezu kompanija da obezbede korisnički pristanak o tome kako će prikupljati i koristiti njihove lične podatke i informacije. Takođe, uredba GDPR uređuje i koje vrste ličnih podataka kompanije mogu prikupljati, čuvati i koristiti u Evropskoj Uniji, a preko toga ova uredba reguliše i pitanje iznošenja ličnih podataka građana EU i van Evropske Unije. GDPR uredba uvodi i novo pravilo, odnosno koncept „prava na zaborav“ podataka u evropski pravni sistem, tako da građani Evropske Unije mogu tražiti od kompanija da trajno uklone određeni on-line podatak prikupljen ili obrađivan o njima i njihovim ličnim prilikama. Ukoliko bi došlo do povrede prava građana u domenu ličnih podataka, kompanije imaju ne više od 72 časa da to prijave evropskim regulatornim telima, dok oni koji ne budu postupili u skladu sa pravilima mogu biti suočeni sa kaznama koje se kreću do 4% njihovog godišnjeg prihoda ili 20 miliona eura, u kom slučaju važi pravilo da se za kaznu po ovom osnovu uzima onaj iznos koji je u datom trenutku veći od dva pomenuta.

Interesantno je istraživanje koje je sprovedeno u SAD, a koje je dalo rezultate da najveći stepen zabrinutosti internet korisnika izaziva način na koji kompanije, ali i vlada koriste njihove lične podatke (Statista, 2017). Druga istraživanja pokazuju da 68% potrošača ne veruje kompanijama kada su u pitanju njihovi lični podaci. Navedeno takođe pokazuje i da se ispostavilo da je poverenje uvek ključni faktor kojim se vode korisnici kada biraju određeni brend. Stoga se ispostavilo da su podaci ne samo fundamentalni za digitalni način poslovanja, već istovremeno i najdragocenija stvar koju kupci mogu podeliti sa kompanijom.

U nekim slučajevima, lični podaci predstavljaju mnogo veću vrednost od novca koji je u opticaju između potrošača i kompanije, pa briga potrošača o njihovoj privatnosti stalno raste, iz kog razloga način na koji kompanije tretiraju takve podatke u značajnoj meri definiše i to kako će se oceniti iskustvo potrošača sa određenim brendom ili kompanijom.

Uredba GDPR je učinila i to da kompanije različito reaguju na obaveze nastale u vezi ove uredbe i njenih pravnih zahteva. Tako se dogodilo da su istovremeno mnogobrojne kompanije počele da

traže pravne praznine u ovom propisu, dok druge doslovno i u potpunosti prilagođavaju svoje politike privatnosti ovom propisu, nadajući se da će to biti dovoljno da postupe po novim pravilima i da istovremeno zadovolje zahteve svojih potrošača za poštovanjem njihove privatnosti. Ipak, evidentno je da postoji i treća grupacija kompanija koja stupanje na snagu ove uredbe posmatra potpuno tehnički, tačnije kao priliku da je iskoriste za to da očiste svoje baze podataka.

Najveće „Big Tech“ kompanije, kao što su Facebook, Amazon i Microsoft, objavile su da su se obavezale da ispoštuju sve standarde privatnosti, međutim nije jasno da li je ovo stvarno obavezivanje u duhu samog propisa ili samo puko zadovoljavanje forme i marketing usmeren na potrošače i korisnike. Ovo je presudno, jer od toga kako će ove kompanije postupati u smislu privatnosti korisnika apsolutno zavisi kako će se ponašati i manje tehnološke kompanije u odnosu na ove gigante.

Sve ovo znači da će nastati promena u digitalnim transformativnim trendovima nakon 2019. godine, jer će sada informisani korisnici moći jasno da vide koje kompanije zaista brinu o zaštiti njihovih podataka, ali i koje kompanije ne posluju na takav način.

U svakom smislu, GDPR uredba je pokrenula još jedan globalni trend koji je konačno učinio kompanije koje posluju na internetu odgovornima za to kako se odnose prema privatnosti i ličnim podacima korisnika. Sve navedeno u zbiru znači da će GDPR uredba svojom snagom naterati kompanije da potraže nove i bolje načine da izgrade originalnu vezu sa njihovom potencijalnom publikom, korisnicima i potrošačima, imajući u vidu posledice doskorašnje loše upotrebe, ali i veoma česte zloupotrebe ličnih podataka korisnika zarad kratkoročnih efekata marketinga i prodaje.

4.7 Zakon o zaštiti privatnosti potrošača u Kaliforniji (Carnifornia Consumer Privacy Act)

Opšte je poznato da veliki broj kineskih kompanija prodaje svoje elektronske proizvode i usluge širom sveta, pa samim tim i u SAD. Samim tim, velika količina takvih proizvoda i usluga, pored ostalog, biva plasirana i u američkoj saveznoj državi Kaliforniji, što otvara brojna pitanja iz domena zaštite podataka američkih građana.

Kako bi se ova, prilično neregulisana oblast prava u SAD popunila aktuelnim propisom iz domena zaštite privatnosti potrošača, Kalifornija je kao jedna od najbogatijih i najprogresivnijih

saveznih država u SAD, usvojila jedan od najbimnijih i najširih zakonskih propisa koji se bavi zaštitom privatnosti i bezbednosti podataka. U tom smislu, Kalifornija je na sebe preuzela težak zadatak i učinila je preko potrebni pomak u oblasti privatnosti i bezbednosti podataka, uobličila ga u zakonski propis, nalik na to kako je to neposredno pre toga učinila i EU sa uredbom GDPR.

Ova potpuno nova vrsta zakonskih propisa, bez sumnje će učiniti da kompanije, bilo da su iz SAD-a, ili ostatka sveta, steknu obavezu da ih dosledno primenjuju, ukoliko njihovo poslovanje ima veze sa podacima potrošača u Kaliforniji, bez obzira gde se ti podaci nalazili. Ovakva konstelacija u popunjavanju pravne praznine u domenu ljudskih prava, ispostavila se presudno važnom za sve kompanije koje žele poslovati na Internetu, bez obzira gde se one sedištem nalazile. Uspostavljena je obaveza kompanija da poznaju i razumeju takve propise, kao i da u smislu njihovih ograničenja organizuju svoj način rada i poslovanja i posvete dužnu pažnju ličnim podacima svojih potrošača.

Iako postoje određeni propisi u SAD iz ove oblasti koji su na snazi, više se ne može izbegavati obaveza, ali ni potreba, da kompanije koje posluju na međunarodnom digitalnom tržištu, moraju shvatiti i prihvatiti da je na snagu stupio zakonski pravac u kome će se odvijati njihovo dalje poslovanje. Iako je to tako, još uvek postoji veliki broj kompanija koje nisu stekle svest u vezi ove svoje obaveze, pa je sasvim izvesno da nisu svesne ni svih ostalih uslova poslovanja na pojedinim tržištima. Ti najaktuelniji uslovi zahtevaju od modernih kompanija najpre da shvate, a onda i prihvate potrebu za postojanjem sistema kontrole i bezbednosti ličnih podataka i uopšte privatnosti potrošača.

Kada je u pitanju sam Zakon o zaštiti privatnosti potrošača u Kaliforniji, on je kao takav usvojen u maju 2018. godine, kada je i odobren od strane Guvernera Kalifornije. Međutim, već u septembru 2018. godine je došlo do njegove prve izmene i dopune, a dinamika odvijanja događaja na tržištu, ispostavila je potrebu za još jednom dopunom tog Zakona, koja je sudeći po najavama američkog državnog tužioca već u zakonodavnom procesu.

Zakon o zaštiti privatnosti potrošača u Kaliforniji, kao i uredba GDPR, stupiće na snagu sa određenim odlaganjem u januaru 2020. godine. Razlog za to je što se radi o daleko najvećem i najbimnijem Zakonu o privatnosti koji je donet u istoriji SAD-a, a po rangu je donekle uporediv sa evropskom uredbom GDPR, koja je bezmalo svaku međunarodnu kompaniju osvestila u vezi sa njihovim obavezama da poštuju privatnost potrošača, ukoliko vrše poslovanje na Internetu.

Najkraće rečeno, američka savezna država Kalifornija je, novim Zakonom o privatnosti, svojim građanima zakonski obezbedila izuzetno širok obim prava. Ta prava podrazumevaju da potrošači mogu zahtevati sve postojeće informacije od kompanija koje se bave prikupljanjem podataka o stanovnicima Kalifornije, kao i da kompanije upitaju da li one prikupljaju i obrađuju njihove podatke i da onda shodno svom zakonskom pravu ili potrebi traže izmenu tih podataka, pa i njihovo brisanje iz baza u kojima su se protivno njihovoj volji i znanju našli. Sa druge strane, ovaj Zakon je izričito zabranio kompanijama da diskriminišu potrošače u bilo kom delu u kome njihova prava štiti ovaj zakon, što bi podrazumevalo i obavezu kompanija da potrošačima daju tačne, jasne i blagovremene informacije o tome šta su o njima prikupili, obrađivali i razmenjivali i sa kim.

Ipak, ovaj zakon nije sasvim jasan kada su u pitanju kriterijumi za određivanje toga na koja se sve preduzeća ovaj Zakon odnosi. Ono što je važno istaći, jeste da su u njegovim odredbama jasno prepoznate kompanije koje prikupljaju i trguju ličnim podacima većeg broja potrošača, pa i podacima o domaćinstavima i uređajima, kao i kompanije koje najmanje 50% ili više svojih godišnjih prihoda ostvaruju od prodaje ličnih podataka i informacija o potrošačima.

Iako je ovo prepoznavanje kategorija u jednu ruku dobro, sa druge strane može se primetiti da će ovaj zakon „promašiti“ veliki broj kompanija, upravo iz razloga ovakve postavke kriterijuma. To svakako može izazvati pojavu da će neke kompanije smatrati da se zakon o zaštiti privatnosti potrošača na njih ne odnosi, pa će nastaviti da rade ono što su već radile sa podacima. Međutim, čini se da svakako neće izostati ni varijanta primene zakona u kojoj će mnoge kompanije same shvatiti ili pretpostaviti da se ovaj Zakon odnosi upravo na njih i njihovo poslovanje, pa će svoje poslovanje prilagoditi novonastaloj pravnoj i faktičkoj situaciji. U svakom slučaju, jedno je sigurno, a to je da moć potrošača formalno raste i da će potrošači u periodu koji je pred nama imati veliki uticaj na kompanije koje su obuhvaćene ovim i ovakvim zakonskim propisima, a naročito od trenutka od kada ovaj kalifornijski zakon u celosti stupi na snagu.

Imajući u vidu da kalifornijski zakon ima mnogo sličnosti sa uredbom GDPR, on istovremeno ima i mnoge razlike, iz kog razloga je potpuno jasno da će mnoge kompanije morati da za potrebe razjašnjavanja brojnih nedoumica u vezi njegove primene angažuju specijalizovane advokatske kancelarije kako bi stekle sigurnost u smislu toga koji se propis, kada i u kojim okolnostima primenjuje i koje su njegove zaokružene formalne jurisdikcije.

Pozitivna stvar je što je Zakon o zaštiti privatnosti potrošača u Kaliforniji zapravo postao „okidač“ za prepoznavanje ove pravne praznine na nivou cele federacije SAD, obzirom da od usvajanja ovog zakona počinju najave da će se i američki Kongres ponovo početi baviti problemom zakona o privatnosti, sa ciljem donošenja jednog propisa o privatnosti na federalnom nivou (Federal Act).

Ono što se desilo odmah po ovoj najavi Kongresa, jeste da su se velike tehnološke kompanije kao što je Google momentalno aktivirale na polju lobiranja za svoje interese, obzirom da takve kompanije kao globalni akteri imaju izuzetno veliki uticaj i interes u tome da utiču na sadržaj i strukturisanje takvog novog saveznog zakona o privatnosti u SAD koji će za njih svakako biti obaveziv. Kuriozitet je da je američki Kongres decenijama unazad na veoma upadljiv način pokazivao interes za privatnošću građana, ali je donošenje zakonskog akta iz nekog nejasnog razloga izostalo.

Inertnost Kongresa u tom smislu krajnje je neobična, jer isti nije reagovao ni na niz skandala i kriminalnih slučajeva iz domena zloupotebe podataka, ali je pritisak javnosti, bez obzira na sve izgovore o zauzetosti Kongresa drugim pitanjima, ipak doveo do toga da će Kongres morati da postupi i adekvatno reguliše ovu oblast.

Čini se da je došlo do toga da su u SAD iscrpljeni različiti propisi na nivou saveznih država, iako su ti zakoni na neki način postavili temelje u ovoj oblasti. Međutim, iako su mnoge kompanije oglašene krivima za propuste u zaštiti privatnosti i usled gubitka podataka o potrošačima, jasno je da je ipak došlo novo vreme u kome propisi i pravna uređenost ove oblasti moraju ići dalje.

Činjenica da je nedavno i američki grad San Francisco doneo propis kojim je zabranio primenu „tehnološkog dostignuća“ kao što je softver i tehnologija za automatsko prepoznavanje lica (Automated Facial Recognition), samo zaokružuje potrebu za što hitnijim reagovanjem u smislu zaokruživanja zakonodavnog okvira. Kada je reč o SAD, donošenje ovakvih mestimičnih gradskih odluka najavljeno je i u Oakland-u i Somerville-u, a procenjuje se i da bi ovakav akt San Francisco-a, kao jednog od tehnološki najrazvijenijih delova SAD-a mogao biti još jedan nivo pritiska i putokaz za Kongres i američki savezni nivo odlučivanja. Ipak, pored pravnog razloga, istaknut je i razlog nesavršenosti ovih tehnologija koje su na nekim od mesta testiranja i van SAD-a dale prilično problematične rezultate. Tako je na primer policija Južnog Velsa 2017. godine započela pilot program u oblasti prepoznavanja lica. Cilj ovog programa je bio da među

fudbalskim navijačima automatski prepoznaju i pronadu huligane i potencijalne izgređnike u oblasti javnog reda i mira, usled čega su ovom softveru izložili okupljene na fudbalskim utakmicama i upoređivali njihova lica evidentirana javnim kamerama sa bazom podataka koja sadrži lica od 500.000 ljudi. Rezultati ovog programa bili takvi da je od 2470 ljudi koje je program izdvojio kao „izgređnike“ u samo 173 slučaja lice bilo tačno prepoznato, dok je ostatak prepoznatih lica zapravo bio lažno evidentiran. Samim tim je softver za automatsko prepoznavanje lica neosnovano inkriminisao čak 2297 ljudi (93%). Da bi relativizovali ovu spornu i neuspelu tehnološku inovaciju u radu policije u domenu izlaganja privatnosti građana AI analitici, u zvaničnim izveštajima policije Južnog Velsa navedeno je i da su u devet meseci rada sa ovim softverom od 2000 pozitivnih podudaranja sa bazom podataka ipak uhapsili oko 450 lica.⁴

Ono što je civilizacijski doprinos ranijih propisa o zaštiti privatnosti, jeste da su poredstvom njih potrošači postali mnogo svesniji svoje privatnosti i ujedno znatno obrazovaniji o načinima na koje razne kompanije prikupljaju, obrađuju i upotrebljavaju njihove podatke, pa se čini da su i poslodavac, i zakonodavac, i potrošači postali svesni činjenice da ukoliko se zakonski propisi ne inoviraju, da će mnoge kompanije taj pravni vakuum i situaciju svesno zloupotrebiti za sticanje profita.

Ono što je posebno interesantno, jeste da u SAD na federalnom nivou postoji uporedna procedura nekoliko različitih zakonskih rešenja i predloga u domenu privatnosti. Ti zakonski predlozi su u različitim fazama zakonodavne procedure, a neka od rešenja predloženih u njima veoma su rigorozna prema kompanijama za koje bi se ispostavilo da su odgovorne za kršenje prava potrošača iz domena privatnosti. Predsednik Odbora Kongresa i američki senator, Roger Wicker jasno je izneo stav da: „Kongres mora razviti jedinstveni američki okvir za zaštitu podataka. U tom pravcu je potreban snažan, nacionalni Zakon“.

Koliko je ozbiljno shvaćena ova oblast i njeni trendovi, govori i to da je nedavno čak i Odbor za trgovinu, nauku i transport američkog Senata (čiji je predsednik upravo senator Wicker) najavio da će sazvati raspravu (saslušanje) pod nazivom „Principi politike za federalni okvir za zaštitu podataka u Sjedinjenim Državama“ i u tom smislu na saslušanju ispitati pravce toga šta bi

⁴ <https://www.vecernji.hr/techsci/stop-big-brother-spijuniranju-san-francisco-prvi-zabranio-tehnologiju-prepoznavanja-lica-1319282> - www.vecernji.hr

američki Kongres morao učiniti kako bi rešio problem rizika za potrošače i obezbedio zaštitu privatnosti svim Amerikancima.

Inače, Komitet za trgovinu o kome je reč, nadležan je za Federalnu komisiju za trgovinu, koja je primarna agencija za sprovođenje zaštite privatnosti i informacione bezbednosti u SAD. Senator Wicker je rekao još i da „u doba brzih inovacija u tehnologiji, potrošačima treba transparentnost u načinu na koji se njihovi podaci prikupljaju i koriste“. „Odgovornost i obaveza ovog Odbora jeste da on razvije savezni standard za privatnost, kako bi potrošače zaštitio od gušenja od strane inovacija, ulaganja i konkurencija“.

Dobar deo saslušanja u Senatu usresređen je i na koncept informisanog pristanka, čak i u domenu prikupljanja i korišćenja podataka u politici, imajući u vidu da se ova metoda, odnosno pristup, potpuno oslanja na ideju da ljudi i čitaju i ne čitaju pravila o privatnosti koja se pred njih postavljaju. Ljudi najčešće ne razumeju implikacije prikupljanja i upotrebe njihovih ličnih podataka, iz kog razloga veliki deo zajednice zapravo ima malo koristi od takvog načina obaveštavanja i od takvog vida pristanka potrošača, usled čega se može smatrati da bi to u ilustrativnom smislu ličilo na „oblačenje prozora“.

Senatorica Maria Cantwell je istim povodom rekla da veruje da obaveštenje i pristanak više nisu dovoljni, jer je privatnost previše širok pojam, tj. pojam koji uključuje mnogo elemenata, iz kog razloga se ne bi smeo svesti samo na kontrolu. Primećeno je na Internetu da mnogi njegovi korisnici ne razumeju na šta su zapravo pristali kada kliknu na prozor koji im ispisuje veoma dugačka i složena pravila o privatnosti i sakupljanju podataka.

Profesor Univerziteta Northeastern, Woodrow Hartzog je na saslušanju u Senatu rekao da ovakav model obaveštavanja potrošača i pristanka u najvećoj meri ne funkcioniše. Problem sa postavljenim modelima obaveštavanja i izbora na strani potrošača nastao je tako što je sistem ustrojen u smislu toga da pomogne da kompanije sakriju rizike sa podacima potrošača u svojoj praksi, pri čemu kompanije usmeravaju ka potrošačima manipulativni dizajn, nejasne apstrakcije i prekomerno složene reči i rečenice, dok istovremeno sa druge strane, svakim delom sadržaja prebacuju rizik na drugu stranu takozvanim inženjeringom sistema koji zapravo radi na tome da ubrza proces prenosa prava sa potrošača na kompanije. Sve se to svodi na proizvodnju efekta odricanja potrošača od zaštite prava.

Profesor Hartzog je takođe rekao da je ljudima ponuđen preveliki broj prekidača i dugmića za brisanje i pristup privatnosti. Na pitanja upućena kompanijama u vezi navedenog, rečeno je da je sve što se tiče potrošača definisano u politici privatnosti kompanije, iako tu politiku uglavnom niko od potrošača nije u mogućnosti da pročita, a i ako bi je pročitali, teško da bi je ko razumeo bez pomoći pravnika. Ipak, ako bi kojim slučajem nastala šteta po potrošača iz domena privatnosti, sve što kompanije obećavaju u takvim slučajevima jeste više i bolje kontrole, a kada se povreda ponovi, kompanije se pravdaju dijagnozom da jednostavno nisu dodale dovoljno opcija, nisu poboljšale postavljene menije i potvrđne okvire date potrošačima u „check box“-ovima.

Profesor Hartzog je takođe objasnio, da je ideja kontrole besmislena bez prisustva drugih zaštitnih i informativnih elemenata koji pomažu ljudima da donesu ispravne i informisane odluke. Problem sa razmišljanjem o privatnosti u smislu kontrole, jeste taj što se ona tretira kao da je „Dar od Boga“, a ne suštinsko ljudsko pravo svakog čoveka. Ovakav pristup je iluzoran, jer kontrola ljudima služi da biraju kome će dati autonomiju, a ne prema kome će se od nje odreći.

Privatnost je širok kontekst koji uključuje mnogo različitih elemenata i ne bi se trebao dalje rafinirati do uspostavljanja prave kontrole. Prema profesoru Hartzogu, interes Kongresa mora biti smisljeno, federalno i iskreno zakonodavstvo o privatnosti, jer će u suprotnom svi zakoni koji bi iz suprotnog proizašli bili umanjene koristi i bez značajnog doprinosa, ako bi se izbeglo da se u njihovo donošenje uključe svi važni akteri, počev od praktičara iz oblasti privatnosti, pa sve do specijalizovanih advokata.

Skoriji incidenti iz domena povrede privatnosti koji uključuju Cambridge analytica-u, tj. incident kada je izvršeno neovlašćeno prikupljanje informacija o milionima korisnika Facebook-a, kao i masovna povreda Equifax-a, gde su lični podaci miliona Amerikanaca takođe ukradeni, jasno pokazuju potpuni nedostatak zaštite potrošača u SAD na federalnom nivou.

Tu se mora pomenuti i najnoviji incident koji prenosi Reuters, a u kome je kompanija Capital One izdala saopštenje da su podaci oko 100 miliona građana SAD i 6 miliona kanadana ukradeni u nedavnom hakerskom napadu na baze podataka ove kompanije. Ukradeni podaci sadrže imena, prezimena, adrese, telefonske brojeve i kreditni rejting svih ovih korisnika.

Usled ovakvih rizika, većina tehnoloških kompanija ističe da se slaže da je neophodno donošenje saveznog zakona koji će urediti prikupljanje i korišćenje podataka o potrošačima, upravo kako bi

potrošači imali snažnu kontrolu nad svojim podacima. U tom smislu, važno je omogućiti transparentost u prikupljanju i korišćenju podataka i uporedo sa tim obezbediti snažan mehanizam za sprovođenje zakona putem koga bi se jednostavno mogla utvrditi svaka eventualna odgovornost kompanija.

Međutim, neslaganje velikih tehnoloških giganta svoje obličje pokazuje u detaljima kao što su npr. da li kompanija može krenuti sa prikupljanjem ličnih podataka nakon što korisnik za to da odobrenje (Opt-In), ili treba da zaustavi prikupljanje podataka nakon što se potrošačevo podrazumevano odobrenje opozove (Opt-Out).

Čini se da se velike tehnološke kompanije ipak sa otporom postavljaju prema donošenju ovakvog saveznog američkog propisa, jer na primer Google, kao jedan od najvećih „igrača“ na tržištu, donošenje takvog zakona koji bi potpuno regulisao privatnost podataka potrošača vidi kao potencijalno negativan uticaj na najmanje 50 njegovih aktuelnih proizvoda, usled čega se pritisak za usporavanje legislativne inicijative kanališe kroz pronalaženje kompromisa da se u tom slučaju moraju zadovoljiti i korisnički zahtevi za funkcionalnošću sa jedne, i kontrola privatnosti sa druge strane.

Prema rečima Nithana Sannappa-e, pomoćnika direktora pravnog sektora za proizvode Twitter-a, njihova je zamerka na pristup uredbe GDPR na ovu temu ta što pravo na pristup ličnim podacima prethodno zahteva da kompanije daju korisnicima do znanja koje podatke imaju o njima i koje podatke obrađuju. U tom smislu, on je izneo primer zahteva korisnika kompaniji Netflix da korisniku dostavi istorijat logova gledanja Bandersnatch-a, što je Netflix bio u mogućnosti da ispuni, međutim, on smatra da većina malih kompanija nema resursa na kojima bi izgradila sistem i poslovni proces neophodan za pružanje takve granularne informacije na korisnički zahtev, iz kog razloga Sannappa smatra da regulativa mora pažljivo razmotriti ove prednosti i opterećenja za kompanije, ali i kompromise koji bi morali da postoje između njih.

Prema rečima zvaničnika Microsoft-a, strogi zahtevi Uredbe GDPR nesumnjivo su utrljali put za postupanje drugih zemalja, pa se predviđa da će standardi koji su već operativni u Evropi, zapravo postati operativni i u većem delu sveta. Putem početka primene uredbe GDPR nastao je jedan globalni trend i to tako što je ovom uredbom EU jasno propisano da se podaci evropskih korisnika, odnosno potrošača, mogu preneti isključivo na ona tržišta koja su usklađena sa evropskim standardima, tako da su mnoge zemlje pritisnute ovom odredbom počele donositi

propise koji su usklađeni sa propisima i standardima o privatnosti potrošača EU kako bi mogle poslovati.

Na temeljima ovog trenda, Brazil kao jedna od najvećih južnoameričkih država doneo je svoje zakone, dok Indija i južna Koreja takođe razmatraju predloge takvih i tako usklađenih zakona. Samim tim, može se očekivati da će i SAD nešto slično morati da urade u vezi sa zakonom o privatnosti, obzirom da njihovo propuštanje da to blagovremeno urade daje kao rezultat i propuštanje da zadrže liderske pozicije u ovim oblastima.

4.8 Zakon o Internetu stvari u Kaliforniji (Internet of Things Law)

Krajem septembra 2018. godine, guverner savezne američke države Kalifornije, odobrio je prvi Zakon o informacionoj bezbednosti u SAD, posebno usmeren na pravno uređenje oblasti Interneta stvari (IoT). Ovaj Zakon koji stupa na snagu 1. januara 2020. godine, zahtevaće od proizvođača proizvoda iz domena IoT-a, da proizvode ove vrste opreme „razumnim“ merama bezbednosti.

Ove bezbednosne mere moraju biti usklađene, kako sa prirodom samih uređaja, tako i informacijama koje oni prikupljaju ili sadrže o korisnicima, usled čega te stvari moraju biti dizajnirane na način da pruže zaštitu od neovlašćenog pristupa, uništenja, korišćenja, izmene ili otkrivanja.

Ovaj kalifornijski zakon takođe propisuje da uređaji kojima se može pristupiti spolja, tj. van lokalne mreže, moraju biti opremljeni ili sa jedinstvenom lozinkom ili sa mogućnošću korisnika da kreira svoju sopstvenu lozinku (pristupnu šifru).

Zakon o Internetu stvari odnosi se isključivo na proizvođače IoT uređaja, tako da se isti ne tiče ni distributera, ni maloprodaje, ni potrošača. Za najveći broj kompanija čije je poslovanje zasnovano na prodaji ili korišćenju IoT uređaja, ovaj zakon neće doneti nikakve promene u načinu funkcionisanja i poslovanja.

Ipak, izraz „proizvođači“, koji je upotrebljen u Zakonu, sam po sebi izuzetno je širok i može uticati bar na polovinu svetskih kompanija koje posluju na ovom polju. Ključni pojam u Zakonu definisan je na način da uključuje bilo koju kompaniju koja proizvodi, bilo sama, ili putem treće ugovorne strane, kvalifikovane IoT uređaje koji mogu biti stavljeni na prodaju u Kaliforniji.

Kako u Kaliforniji ne postoji ograničenje za prodaju proizvoda, samim tim bi bilo koji proizvođač mogao bi biti podvrgnut dejstvu ovog Zakona. Usaglašavanje sa ovim Zakonom u nekim slučajevima može biti veoma jednostavno, čak do mere „randomly“ generisane lozinke za svaki pojedinačni uređaj ili obezbeđivanja softverskog alata ili firmvera koji će osigurati kvalitetniju bezbednosnu zaštitu.

Ipak, za neke od proizvođača, posebno onih čiji uređaji prikupljaju ili sadrže osetljive informacije, usklađenost sa ovim propisom može značiti potpunu obnovu proizvoda, čak do mere proizvodnje novih, usled čega se kompanijama preporučuje angažovanje odgovarajućih savetnika za ovu oblast, kako bi obezbedili usaglašenost proizvoda i poslovanja sa ovim propisom i njegovim ograničenjima.

Iako Zakon o zaštiti privatnosti i Zakon o Internet stvarima još uvek nisu stupili na snagu, to ne znači da na njihovom mestu ne funkcionišu drugi međunarodni ili američki propisi sličnog pravnog usmerenja. Primera radi, operateri web sajtova izvan Kalifornije, vrlo verovatno će se morati pridržavati Zakona o zaštiti privatnosti na mreži (California On-line Privacy Protection Act) i formirati svoju web politiku privatnosti kako bi ona sadržala zakonom propisane formulacije u slučaju da poseduju ili upravljaju web sajtovima koji oglašavaju, pružaju usluge ili su jednostavno dostupni stanovnicima Kalifornije.

Ovaj zahtev se mora ispuniti posebno u slučajevima web stranica koje prikupljaju lične podatke potrošača u Kaliforniji, koji uključuju ime i prezime, kućnu ili drugu adresu, adresu elektronske pošte, broj telefona, broj socijalnog osiguranja ili bilo koju drugu ličnu informaciju koja bi omogućila nekom licu da može direktno kontaktirati konkretnog korisnika web sajta, bilo lično ili on-line.

Ovakva bezbednosna politika ima svoje domete čak i u slučajevima kompanija koje se nalaze u udaljenim delovima SAD-a, ako bi njihove web stranice mogle vršiti prikupljanje prethodno pobrojanih ličnih podataka i informacija. Mnoge države, uključujući i samu Kaliforniju, imaju neku vrstu standarda informacione bezbednosti. Ti propisi i standardi su obično koncipirani tako da od preduzetnika zahtevaju (pod uslovom da oni poseduju neku od zakonom predviđenih vrsta ličnih podataka potrošača), da u odnosu na njih uspostave razumne mere bezbednosti, što je vrlo šakaljiva formulacija u slučaju pokretanja spora.

4.9 Kina i Internet stvari

Kineska oblast Shenzhen spada jedan od najrazvijenijih svetskih centara za proizvodnju malih elektronskih potrošačkih proizvoda. U ove proizvode spadaju i proizvodi iz domena Interneta stvari. IoT proizvodi su sada već dostigli nivo masovne proizvodnje, tako da se proizvode u enormnim količinama i masovno implementiraju i integrišu u mrežne sisteme širom sveta.

Pitanje IoT uređaja, kao pitanje budućnosti digitalizacije, otvorilo je mnoga pitanja. Jedno od tih pitanja je i ko je vlasnik intelektualnog vlasničkog prava nad ovakvim proizvodom?

Činjenica je da je razvoj interneta stvari učinio da je na ovo pitanje, ma koliko ono bilo često postavljano, ipak izuzetno teško dobiti konačan odgovor. Konačan odgovor na ovo pitanje najpre zahteva razumevanje procesa razvoja i proizvodnje tehničkih i elektronskih uređaja, imajući u vidu da se on kao takav odvijao u 3 faze između kineskih proizvođača i stranih kupaca.

U prvoj fazi, koja je prema određenim tumačenjima trajala od 1981. - 1995. godine, situacija na ovom polju bila je izuzetno jednostavna. U ovoj prvoj varijanti, kineski proizvođač proizveo bi neki standardni potrošački proizvod koji bi strani kupac kupio u izvornom obliku i eventualno zatražio od kineskog proizvođača da na taj proizvod stavi njegov zaštitni znak, odnosno kupčev logotip.

U takvoj postavci stvari, pitanje intelektualne svojine je bilo potpuno jasno rešeno. To rešenje je bilo takvo da je kineski proizvođač dizajnirao proizvod, a strani kupac je na njega uneo svoj zaštitni znak, odnosno logotip.

U drugoj varijanti, odnosno postavci stvari, radilo bi se o dugogodišnjem proizvodu zastupljenom na tržištu, koji je bio razvijen od strane inostranog kupca. Inostrani kupac bi kineskom proizvođaču doneo gotov proizvod i sa njim ugovorio proizvodnju njegovih kopija, čime bi i u tom slučaju intelektualno vlasništvo nad proizvodom bilo potpuno jasno. Inostrani kupac je posedovao celokupnu intelektualnu svojinu, a kineski ništa.

Ova vrsta odnosa u proizvodnji, donela je čak i jednu vrstu sporne prakse između stranih kupaca i kineskih proizvođača, pa je celokupni proizvodni odnos između dve strane bio dokumentovan samo narudžbenicama, tako da NNN sporazumi o razvoju proizvoda i OEM ugovori bezmalo nisu korišćeni, iz razloga što je smatrano da je vlasništvo nad intelektualnim pravima bilo

nesporno, a cene i uslovi isporuke rešavani su kroz porudžbenice. Ovakav neuređeni odnos često je dovodio do proizvodnje defektnih proizvoda i problema u vezi njima.

U drugoj fazi, koja je trajala od 1995. - 2015. godine, razvijen je novi oblik odnosa između stranih kupaca i kineskih proizvođača. Strani kupci su počeli dolaziti u Kinu bez gotovog proizvoda ili projekta, najčešće samo sa idejom ili predlogom određene vrste proizvoda. Strani kupac bi u takvom slučaju započeo saradnju sa kineskim proizvođačem, kako bi zajedno razvili konkretan proizvod. U nekim slučajevima, kineski proizvođač bi doradio prototip konkretnog proizvoda i komercijalizovao ga, odnosno pripremio ga za masovnu proizvodnju. U toj situaciji, strani kupac bi došao kod kineskog proizvođača sa malo više od samo osnovne ideje, kako bi dve strane zajednički radile na konačnom razvoju proizvoda. Ovakav način proizvodnje predstavlja najviši nivo rizika za strane kompanije, kada je njihovo opredeljenje proizvodnja datog proizvoda u Kini. Strane kompanije su u ovakvim poslovima su najčešće koristile NNN sporazume u fazi fabričkog istraživanja, a kasnije i OEM ugovore za fazu proizvodnje, ali su retko koristile sporazume o razvoju proizvoda radi regulisanja autorskih odnosa dve strane.

Ovo se ispostavilo velikom greškom stranih kompanija, tj. greškom koja je bila uzrok jedne od dve moguće katastrofe za strano preduzeće. Prva moguća katastrofa za strano preduzeće obično nastane kada kineski proizvođač stranoj kompaniji ne naplati ništa za rad na razvoju proizvoda. U tom slučaju kineski proizvođač preuzima inicijativu u smislu proizvoda, cena, plaćanja, količine, kvaliteta i uslova isporuke, usled čega strano preduzeće ne može više ništa učiniti u pravcu svoje zaštite, obzirom da je strana kompanija sačekala da se razvoj proizvoda završi pre nego što se regulišu pitanja intelektualne svojine.

Druga katastrofalna posledica proizilazi iz postupanja stranih kompanija koje ne uzimaju u obzir važna proceduralna pitanja vezana za uspešan razvoj proizvoda. Često se dešava da strane kompanije u poslove sa kineskim proizvođačima ulaze pod pretpostavkom da kineski proizvođači mogu razviti bilo kakav proizvod u kratkim vremenskim rokovima i pod onim uslovima tolerancija koji zadovoljavaju uzuse modernog poslovanja. To najčešće dovodi do posledica da proizvod nikada nije dovršen, ili nikada ne radi ispravno, odnosno da proizvod bude dovršen, ali tek nakon što je njegova tržišna prilika prošla, a troškovi proizvoda i proizvodnje postaju daleko veći od onih koji su bili inicijalno predviđeni za moguće prilike komercijalnog uspeha proizvoda.

Iz navedenog se može zaključiti da je sistem poslovanja i međunarodnih pravno-tehnoloških odnosa izuzetno kompleksan i pun rizika, a nespremnost kompanija da se pravno zaštite onim vrstama ugovora koje su primenjive u Kini, zapravo je fatalan, pa je problem koji je tako nastao i bukvalno nerešiv (Harris Bricken, 2016).

Iz opisanog konteksta proističu razna pitanja, pa i ono ko je u ovakvoj situaciji vlasnik dizajna proizvoda, kalupa i alata, know-how-a i ostalih poslovnih tajni, a onda i šta se sve može dogoditi kada takvi proizvodi uđu u komercijalnu upotrebu, odnosno opticaj, a posebno ako se radi o uređajima iz domena interneta stvari koji nesumnjivo mogu zadirati u privatnost ljudi gde god budu implementirani odnosno instalirani.

U trećoj fazi koja traje od 2015. godine do danas, zapravo smo stigli u eru Interneta stvari. U domenu dizajna, razvoja i proizvodnje elektronskih proizvoda široke potrošnje za IoT tržište, svi napred navedeni nejasni i maksimalno problemski ispunjeni odnosi, sada su i uvećani i produbljeni. Era Interneta stvari je time otvorila ceo niz pitanja.

U doba druge faze, situacija je koliko toliko bila jednostavnija, jer su obično dva poslovna entiteta dizajnirala i proizvodila jedan proizvod. Međutim, era Interneta stvari znatno je usložila situaciju, pa je najveći deo projekata Interneta stvari učinio da je njihov razvojni proces značajno kompleksniji. Tako se razvojni proces usloženog tipa zapravo protekao na više činilaca:

- Koncept proizvoda je najčešće dolazio od strane američkog ili inostranog kupca;
- Spoljni dizajn proizvoda najčešće je zavisio od neke međunarodne dizajnerske firme;
- Interni dizajn i funkcija proizvoda mogu biti u vlasništvu stranog kupca, kineskog proizvođača, provajdera senzora ili drugih komponenti koje su neophodne za povezivanje IoT uređaja sa spoljnom mrežom i digitalnim okruženjem.

Kada je u pitanju dizajn aplikacije IoT proizvoda (što može uključivati i smart telefone), u pitanju je dizajn dva potpuno odvojena softverska seta, jedan softver služi za prosleđivanje komunikacije i nalazi se na samom IoT proizvodu, dok je drugi softver za komunikaciju integrisan u aplikaciji.

Po istom principu kao što je ustrojen kompleksni unutrašnji dizajn fizičkog dela proizvoda, i njegove softverske komponente mogu biti napisane i dizajnirane od više različitih strana, pa to

može biti strani kupac, kineski proizvođač, a veoma često i kompanije za projektovanje, koje su „treća strana“.

Ovde se mora postaviti pitanje situacije koja nije samo hipotetička. To pitanje je situacija kada je sam proizvod dovršen, masovna proizvodnja spremna, a strani kupac za zaokruživanje tržišnog plasiranja proizvoda traži dopunski izvor finansiranja. Problem nastaje tako što će svako ko se bavi finansiranjem, u ovakvoj situaciji, da bi se odlučio da li će da finansira ovakav tržišni projekat ili ne, najpre postaviti pitanje ko je vlasnik konkretnog IoT proizvoda, ko je nosilac intelektualne svojine i sl., pa se često ispostavlja da su ovo pitanja na koja se obično ne može dobiti jasan ili dovoljno jasan odgovor da bi bio dovoljno dobar finansijerima.

Ovakva situacija u kojoj se velika količina IoT proizvoda, kao mrežnih uređaja, opremljenih sensorima, komunikacionom opremom, višestrukim softverskim i komunikacionim rešenjima, a koja nastanu iz ovako spornih proizvodnih odnosa, stvara dalju situaciju u kojoj se možda i može utvrditi ko je proizvođač samog IoT proizvoda ili njegovih segmenata, ali ne i sve ono što je potrebno da bi takav proizvod bio saglasan napred opisanim međunarodnim propisima i standardima. Samim tim, ovo predstavlja izuzetan rizik, kako po samu digitalnu transformaciju poslovanja, tako i po bezbednost kompanija, institucija i fizičkih lica, pa i država, jer ovakav vid disrupcije, koji je nastao iz haotičnih i neuređenih odnosa između dizajnera, proizvođača i hardverskih i softverskih komponentaša, ne deluje ni ohrabrujuće, ni obećavajuće.

Sa druge strane, širina dometa Interneta stvari, tj. interneta u kome je „sve povezano sa svime“ izuzetno je velika. Pretpostavlja se prema nekim stručnim procenama da će u tom povezivanju do 2020. godine biti umreženo više milijardi ovakvih internet stvari, koje će kao takve biti ugrađene u najraznovrsnija poslovna i mrežna rešenja, domove, institucije, infrastrukturu i njene kritične objekte, što u smislu bezbednosnih rizika po osnovu opisanog haotičnog sistema proizvodnih odnosa, ne može dati značajnije optimističnu prognozu.

U svakom slučaju, stiže se utisak da su prethodno obrađena zakonska rešenja koja se sporadično javljaju na globalnom nivou, posebno Kalifornijski zakon o Internetu stvari, ovu situaciju prepoznali i započeli njeno rešavanje, međutim, to je samo početak koji je tek zagrebao po vrhu ledenog brega, obzirom da zakonski propisi poprilično kaskaju za aktuelnim mrežnim i tržišnim događajima vođenih profitom, usled čega je svaki dan kašnjenja zakonodavstava u odnosu na dinamiku digitalizacije poslovanja i tržišta, zapravo pravac koji može otvoriti čak i one

moгуćnosti, koje se već sada mogu naslutiti, a koje će trka za digitalnim profitom svakako želeti da iskoristi.

5. Digitalna ekonomija u Srbiji, prilike i ograničenja

U odnosu na razvijene zemlje, Srbija, kao i ostale države sa područja Zapadnog Balkana, u velikoj meri zaostaje u primeni digitalnih tehnologija, a time i uopšte u digitalizaciji poslovanja. Za širi stepen digitalizacije, pored (nedostajućih) finansijskih sredstava, potrebno je izvršiti niz nekozmetičkih, dakle stvarnih promena u ekonomskom sistemu, kako bi one omogućile podršku i izgradnju novih poslovnih modela baziranih na znanju, inovacijama i naprednim tehnologijama.

Prvi preduslov za takvu ekonomsku transformaciju, jeste da nacionalna ekonomija razvije odgovarajuću infrastrukturu i oslobodi njene potencijale, a svako preduzeće, posebno velika, prihvate inovirane organizacione i poslovne modele bazirane na IKT i shodno tome, unaprede kroz proces obrazovanja i svoju radnu snagu sa neophodnim informacionim veštinama i kompetencijama.

Drugim rečima, nije moguće uspostaviti digitalnu ekonomiju, ako se prethodno ne uspostavi IKT - digitalna infrastruktura i platforme na kojima će se graditi usluge i procesi sa dodatom vrednošću. Izuzetno široka i raznovrsna primena novih tehnologija, ima direktni uticaj na opštu primenu inovacija, ali istovremeno i na povećanje produktivnosti u ostalim sektorima, u čemu ne zaostaje ni efekat poslovne kulture i posvećenosti postavljenim ciljevima promene.

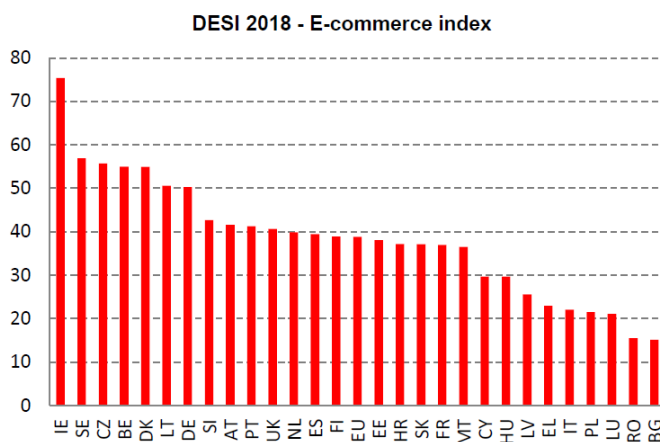
Iskustva pokazuju, da horizontalna primena digitalnih tehnologija u raznim granama i sektorima privrede, formira potpuno nove poslovne mogućnosti, sposobne da menjaju budućnost, kako preduzeća, tako i industrijskih grana kao celine. Ovaj smisao ne zaobilazi ni efekte koje navedeno ima na državu, državnu infrastrukturu, ali i samu digitalizaciju poslovanja na tržištu i njene ciljeve.

Drugi značajan uslov za razvoj digitalne ekonomije u Srbiji jeste znanje. Prema novim analizama, čak za 90% poslova u Republici Srbiji potrebno je osnovno informatičko znanje, a za preostalih 10% specijalističko, odnosno ekspertsko znanje.

Ostvarivanje efekata digitalne ekonomije na taj način je usko povezano ili prepleteno sa pitanjem daljeg razvoja visokog obrazovanja, nauke, a prevashodno univerziteta i fakulteta koji profilišu informacione ili računarske stručnjake.

Prema DESI indeksu (DESIIndex) iz 2018. godine, kojim Eurostat meri stepen digitalizacije zemalja u okruženja: Slovenija zauzima 8. mesto, a Hrvatska 17. mesto među državama članicama EU.

Grafikon br.13 DESI 2018- Indeks digitalne ekonomije po zemljama



Source: European Commission services based on Eurostat data

DESI index ustvari pokazuje koliko su pojedini aspekti digitalnih ekonomija primenjeni u nekoj ekonomiji i društvu, usled čega je ovaj indeks najčešće dobar analitički pokazatelj ekonomske i društvene digitalizacije, a računa se kao ponderisani prosek 5 glavnih DESI kategorija: povezivost, ljudski kapital, korišćenje interneta, integracija digitalnih ekonomija i javne digitalne usluge.

Grafikon br. 14 DESI kategorije

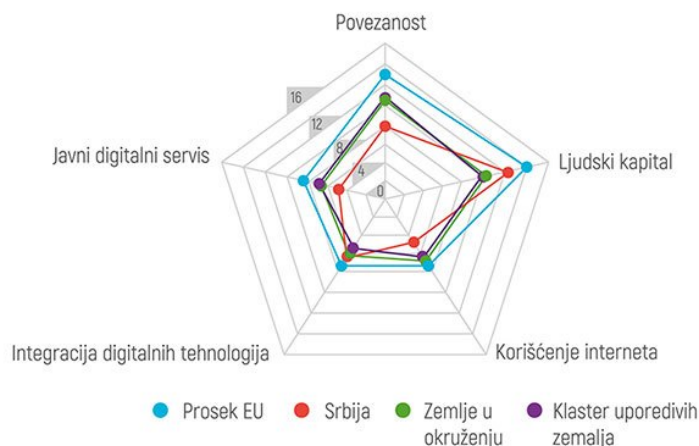


Izvor: Ratel, 2017:19

Prosek DESI indeksa za Evropsku uniju iznosi 50,8 u 2017. godini. U skladu sa DESI metodologijom, Regulatorna agencija za elektronske komunikacije i poštanske usluge Republike

Srbije (RATEL) došla do rezultata da isti indeks za Republiku Srbiju u istoj godini iznosi 35,6, što je daleko ispod evropskog proseka.

Grafikon br.15 Indeks DESI za Srbiju 2017.



Izvor: RATEL, 2017:21

Koliki je stepen digitalizacije u Republici Srbiji, može se sagledati i kroz Indeks mrežne spremnosti, kao pouzdanog indikatora razvoja digitalne ekonomije u nekoj zemlji. Ove podatke objavljuju Svetski ekonomski forum i INSEAD (The Business School of the World), a u publikaciji The Global Competitiveness Report, gde u 2018. godini, Republika Srbija zauzima 65. mesto u odnosu na ukupan broj od 140 posmatranih zemalja.

Indeks pokazuje napredak mrežne spremnosti, kao efikasne platforme za primenu informacionog društva i razvoja digitalne ekonomije i uključuje veći broj indikatora. Osim raspoloživosti i pristupa mreži, indeks obuhvata i sledeće indikatore:

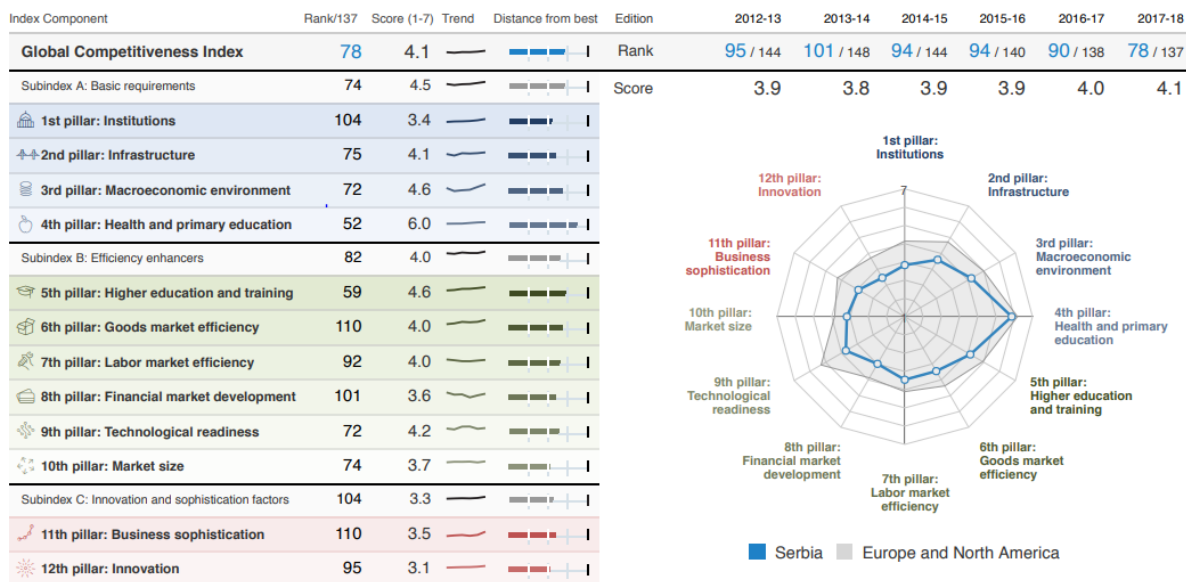
Ukupno okruženje – podindeks okruženja (političko, pravno i inovaciono okruženje);

Sposobnost korišćenja – podindeks spremnosti (infrastruktura, mogućnost pristupa, sposobnosti korišćenja), podindeks primene (individualna primena, primena u kompanijama i vladi);

Uticao na ekonomiju i društvo – podindeks ekonomskog i socijalnog uticaja.

Grafikon br. 16 Prikaz stepena mrežne spremnosti i ostalih pokazatelja Srbije

Performance overview



Izvor: World Economic Forum, Global Competitiveness Report, 2017-18:256

Dublja analiza gore navedenog Izveštaja jasno predočava da se Srbija nalazi u tzv. „novom digitalnom jazu“, usled nedostatka odgovarajućih sposobnosti i kapaciteta da:

- Realizuje adekvatan uticaj primenjene IKT na transformaciju svoje ekonomije i društva; i
- Koristi potencijale IKT u smislu uspostavljenog održivog razvoja i unapređenja kvaliteta poslovanja domaćih preduzeća.

Republika Srbija je, dakle, u ovom trenutku na samom početku ulaska u digitalizaciju privrede i društva, jer je brzina usvajanja i primene novih tehnologija isuviše spora da bi mogla da prati savremene trendove i razvoj na ovom polju.

Razvijene zemlje sa značajnom digitalnom podrškom napreduju daleko brže i imaju mogućnost da otvaraju nove platforme ili unapređuju postojeće, pronalaze (inoviraju) rešenja, stvaraju iskustva i tako kreiraju originalnu i novu digitalnu privrednu strukturu, koja uz digitalizaciju tržišta doprinosi bržem ekonomskom rastu i etabliranju na dinamičnom i konkurentnom tržištu.

Zbog primene spornog modela privatizacije, te propadanja velikih privrednih giganta i sistema, a time i urušavanja privrede u celini, u Republici Srbiji trenutno postoji nedovoljan interes i krajnje su nezadovoljavajući rezultati u razvoju i primeni industrije 4.0 i same digitalne

ekonomije. Po oceni stručnjaka, orijentacija Republike Srbije na industriju 4.0 mogla bi predstavljati motor oporavka srpske privrede. Iz stručne javnosti sve češće dolaze signali i preporuke da nadležni državni organi stvore podsticajni, najpre pravni, a zatim i ekonomski ambijent i specijalizovane fondove za razvoj industrije 4.0 i digitalizacije uopšte, prvenstveno u domenu profitabilnih industrijskih grana.

U procesu pridruživanja Republike Srbije Evropskoj Uniji, posebno treba akceptirati napore i konkretne mere vlade radi smanjivanja digitalnog jaza s jedne, i stvaranja temeljnih pretpostavki za uključivanje u mrežu visoko tehnološki razvijenih zemalja, sa druge strane. U tom pogledu, potrebno je sprovesti sledeći redosled koraka:

- Povećati nivo digitalne transformacije industrije, tj. povećati primenu digitalnih tehnologija;
- Kreirati digitalnu preduzetničku kulturu, tj. unaprediti poziciju i imidž digitalnog preduzetništva i njegovu promociju;
- Privući, razviti i zadržati visoko obrazovane stručnjake;
- Olakšati pristup finansijama i uvećati investicije; i
- Razviti digitalno podržan tržišni ambijent.

Aktuelna reforma ekonomskog sistema zajedno sa reformom državne uprave, otvorila je određene mogućnosti za uvođenje digitalnih tehnologija u različite privredne grane, sektore i kompanije, ali i fiksirala potrebu usvajanja i razrade strategije digitalne tehnologije u Srbiji na osnovu i u skladu sa digitalnom agendom EU i razvojem, postavkama i standardima digitalne industrije i drugih sektora, kao i jedinstvenog digitalnog tržišta u EU.

Prema istraživanju domaćih kompanija „Veza d.o.o.“ i „www.poslovnisoftver.net“ koje je urađeno u periodu februar-mart 2018. godine kroz projekat „PSD Private Sector Development“ na jugu Srbije je urađen analitički presek stanja preduzeća sa aspekta njihove pripremljenosti za digitalno poslovanje i transformaciju. Ovaj projekat sproveden je od strane Razvojne agencije Srbije (RAS) i američke agencije USAID.

Tok istraživanja pratila su sledeća pitanja:

- Dokle se stiglo sa digitalizacijom u kompanijama i upotrebom poslovnih softverskih rešenja?

- Kakav je nivo pripremljenosti kompanija za digitalnu transformaciju?
- Koji su problemi i koje su njihove potrebe?
- Šta je potrebno da se uradi da bi se ubrzala digitalna transformacija tako da kompanije od toga imaju vidljive koristi?

U odnosu na postavljena pitanja, ovde su dati neki od rezultata istraživanja. Istraživanje o upotrebi računara u domaćim kompanijama pokazuje da 100% preduzeća, bez obzira na veličinu, sedište ili delatnost koristi računar u svakodnevnom poslovanju. Uprkos ovom nalazu, procenat zaposlenih koji svakodnevno upotrebljava računar znatno je manji od proseka u zemljama EU.

Procenat izdvajanja za IT kod domaćih kompanija prosečno iznosi 0,5% njihovih prihoda. Ovakvo izdvajanje sredstava za IT nekoliko puta je niže od svetskog proseka koji iznosi 4,0% prihoda kompanija. Ako se pritom uzme u obzir i činjenica da su prosečni prihodi domaćih kompanija daleko niži od prihodnog proseka uporednih svetskih kompanija, to čini da je jaz domaćih kompanija u odnosu na kompanije na svetskom tržištu u apsolutnom iznosu IT budžeta, a možda još i veći.

Delimično je ohrabrujuć podatak da 100% od anketiranih kompanija ima kvalitetnu vezu sa internetom. Sve anketirane kompanije prijavile su pojedinačne IT budžete manje od 5.000 evra na godišnjem nivou, tako da zbirni IT budžet svih anketiranih kompanija iznosi samo oko 50.000 evra na godišnjem nivou. Kako su poslovni prihodi kompanija učesnika u istraživanju procenjena na oko 20 miliona evra, to čini da je udeo njihovog IT budžeta u ukupnim ostvarenim prihodima u proseku manji od 0,25%, što je više nego nedovoljno.

Od svih anketiranih, 6,4% kompanija izjasnilo se da poseduje sopstveni server, što ukazuje i na nizak stepen zastupljenosti LAN mreža i slabu umreženost računara i računarskih resursa u ovim kompanijama. Do nedavno, digitalizacija kompanija sa više od 10 zaposlenih obavezno je podrazumevala primenu LAN mreža, obzirom da je saradnja na 5 i više računara bez postojanja mreže i mrežnih kapaciteta izuzetno teška i neefikasna.

Ista analiza pokazuje i da samo 14,8% kompanija elektronski prodaje robu i usluge drugim preduzećima, dok samo 7,2% kompanija prima porudžbine putem web sajta ili mobilne aplikacije, dok kompanijski B2B portal ima samo 7,4% kompanija.⁵

⁵ <https://poslovnaznanja.co.rs/digitalna-transformacija-poslovanja-u-srbiji-analiza-stanja-i-kako-je-ubrzati/>

Ovakva statistika digitalne transformacije poslovanja, bez obzira što se radi o istraživanju sprovedenom u manje razvijenim krajevima Republike Srbije, poražavajuća je. Upravo ova statistika je plastičan pokazatelj potrebe za sistemskim pristupom digitalnoj transformaciji poslovanja u Republici Srbiji, u kom slučaju nije dovoljno samo angažovanje Privredne komore Srbije i regionalnih i stranih privrednih komora u smislu konsultativnog i trening nivoa, kao što nije dovoljno ni to da se strani donatori bave rešavanjem ovog pitanja tako što će samo ukazivati na ove probleme, trendove i mogućnosti, već je angažovanje države i državnog ekonomsko-ambijentalnog aparata presudan faktor, obzirom da isti treba da omogući takvim kompanijama pristup jeftinim finansijskim izvorima za razvijanje digitalnog razvoja, kako bi se pored voljnog momentuma u kompanijama i konsultantskim nastojanjima na polju podizanja digitalne poslovne svesti, stvorio i ekonomsko-tehnološki inkubacioni ambijent iz koga bi se srpske kompanije mogle uključiti u globalne tokove i trendove, kako bi putem njih mogle steći priliku da iskoriste svoju digitalnu poslovnu šansu.

U svakom slučaju, digitalna transformacija poslovanja vrši se primenom novih digitalnih poslovnih modela, što je kod velikog broja domaćih kompanija nepoznat pojam. Da bi digitalna transformacija bila moguća, mora se razumeti da ona nije samo primena digitalnih tehnologija, već promena modela poslovanja, pa je sve suprotno od toga pojava “lipstick on a pig” fenomena. (Kostić, 2019)

Dok god postoji veliki broj kompanija koje veruju ili prikazuju da uspešno sprovode digitalnu transformaciju poslovanja, a da digitalne tehnologije prikazuju kao zavesu iza koje stoje njihove slabosti, suštinski takve kompanije stoje na ivici svoga doba, usled čega egzistiraju u polju opasnosti da padnu u prošlost. Istine radi, ovaj fenomen nije prisutan samo u Srbiji i kod srpskih kompanija, već takvih slučajeva ima i na zapadu, čak i kada su u pitanju najbolje i najnaprednije kompanije.

Prema rečima Bila Gejtsa, vlasnika Microsofta, automatizovanje efikasne poslovne operacije uvećava poslovnu efikasnost kompanije, ali isto tako, automatizacija neefikasne poslovne operacije uvećava poslovnu neefikasnost kompanije.

Stoga, na aktuelnu situaciju i stanje srpske digitalne poslovne transformacije, shodno utvrđenom stanju možemo primeniti i poruku Parouzzi-jevog principa koja glasi: “Ako loše startujemo i nevolje rastu eksponencijalno”

Poglavlje IV: Digitalizacija poslovanja

1. Terminološko i semantičko određenje digitalne transformacije

U semantičkom smislu, digitalna transformacija je prepoznatljiva već više od 15 godina. Sa protokom vremena, digitalnom transformacijom sve se češće objašnjavaju ili opisuju promene koje se nastaju u društvu pod uticajem inovativnih tehnologija i kako se te promene odražavaju na privređivanje kompanija i funkcionisanje javnih servisa.

Uvažavajući da se ovde radi o još uvek nezaokruženom izrazu po značenju, digitalna transformacija se samim tim različito formuliše. Samim tim, može se reći da još uvek ne postoji jedno opšteprihvaćeno ili univerzalno određenje ovog pojma. Najčešće, pod ovim izrazom se podrazumeva apsolutno refokusiran način poslovanja vođen uslovima tržišta koji se bazira na primeni modernih tehnologija i njihovih disruptivnih inovacija. Prema nekim autorima, digitalna transformacija predstavlja „korišćenje novih tehnologija, pri čemu tehnologija nije ključna, već se radi o uvođenju novih digitalnih biznis modela u poslovanje i prilagođavanje svog poslovanja novim digitalnim trendovima“ (Vujević, 2015:59).

U globalnom kontekstu, digitalna transformacija poslovanja najbrže je rastući trend u domenu informacionih tehnologija i poslovanja. Polazeći od toga da ovaj transformativni model nije isključivo tehnološki trend, već središte poslovnih strategija u gotovo svim industrijskim segmentima i tržištima, Westermann i dr. određuju digitalnu transformaciju kao kontinuirani proces kojim se preduzeća prilagođavaju ili pokreću disruptivne promene, kako kod svojih klijenata, tako i na tržištima, iskorišćavajući digitalne veštine za osavremenivanje poslovnih modela, proizvoda i servisa koji bešavno spajaju digitalno, fizičko, poslovno i korisničko iskustvo, istovremeno unapređujući operativnu efikasnost i performanse organizacije (Westerman et. al. 2012).

Velike kompanije kao što su Saga, New Frontier Group, vrlo su rano prepoznali vrednost i mogućnost digitalne transformacije i pod tim terminom podrazumevaju nov način vođenja biznisa usmeren na promenu internih i eksternih strategija kompanije, uz čiju pomoć se upotrebom novih tehnologija obezbeđuje agilniji rad zaposlenih i sadržajniji odnos sa potrošačima (PC Press, 2015).

Mada postoje neznatne razlike, danas digitalnu transformaciju uglavnom pokreće i ubrzava interes kompanije za unapređenje iskustva internih i eksternih korisnika sa unapred jasnim ciljevima - optimizacijom i automatizacijom procesa unaprediti produktivnost i/ili smanjiti troškove poslovanja. Ova dva pokretača utiču na ukupne poslovne prioritete, stavljajući digitalnu transformaciju u središte većine kompanijskih strategija.

Digitalni svet poslovanja poseduje jednu specifičnu performansu koja je do sada nedostajala, a to je da je sve praktično postalo merljivo do poslednjeg detalja. Postepeno ulazimo u eru veće reinovacije, a suština se ogleda u dva osnovna principa. Prvo, potrebno je kontinuirano pratiti potrebe krajnjeg korisnika i u skladu sa tim preoblikovati lanac vrednosti u odnosu na njegov. Drugo, neophodno je konstantno obezbeđivati dodatnu vrednost šireći mrežu saradnika na inovativnim platformama.

U literaturi se navode brojni primeri kako nove tehnologije transformišu ili remete različite industrije, kao npr. autonomna vozila u transportnoj industriji, 3D štampa u proizvodnji, roboti u logistici ili medicini, mrežna ekonomija u turizmu, itd. Drugi ključni pokretači, ili tzv. akceleratori inovacija u savremenom poslovanju, obuhvataju internet stvari (IoT), virtuelnu i proširenu realnost i u poslednje vreme sve više, kognitivno računarstvo.

Među stručnjacima koji neposredno ili uzgredno prate ovu oblast, digitalna transformacija je svojim brzim nastupom, primenom i rezultatima, uveliko promenila, a prema svim prognozama, i nastaviće da menja i redizajnira ukupni poslovni pejzaž, obrazovanje, zabavu, ali i javnu upravu. Tempo promena se rapidno ubrzava, dok se promene permanentno šire u svim pravcima, a disrupcija odvija na organizacionom, društvenom i individualnom nivou.

Prema scenariju digitalne tehnologije, novi poslovni modeli i strategije koje oni generišu, nastaviće i dalje da primarno utiču na većinu poslovnih organizacija, ali i javnih servisa sa sve većim intenzitetom, nezavisno od toga koliko se oni budu tome protivili.

Posledica takvih pristupa jeste da danas nema univerzalne formule digitalne transformacije koja bi bila jedinstvena, ni po svojoj organizacionoj strukturi, ni po načinu poslovanja. Uvođenje digitalne transformacije u kompanije ili preduzeća, mora da uvažava unutrašnje specifičnosti, kao i razvojne strategije i ciljeve koji se nameravaju postići. Na osnovu dosadašnje relativno kratke prakse, u pogledu strukturisanja ili dizajniranja možemo izdvojiti tri stuba digitalne transformacije:

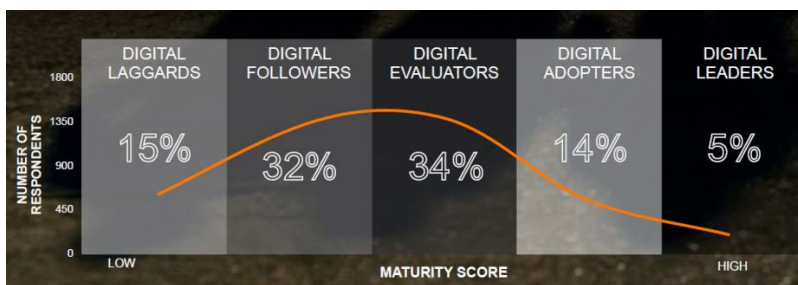
- relevantan sadržaj;
- odgovarajući komunikacioni kanali; i
- podaci o korisnicima.

Rezimirajući napred izneto, proističe da je osnovna karika digitalne transformacije sama informacija, koja obzirom na količinu i protok, čini najvažniji i najtraženiji resurs u modernom poslovnom kontekstu (Čelik, P. 2019:61-81).

Nivo digitalizacije u različitim ekonomijama i sektorima je različit i na tom planu postoje ogromne diskrepance. Najveći broj evropskih kompanija se stoga svrstavaju u dve kategorije – „digitalne istraživače“ i „digitalne igrače“. U najkraćem, kompanije na tržištu priznaju potrebu za transformacijom u digitalno, odnosno one su u ranoj fazi premodelovanja postojećeg (klasičnog) modela u digitalno-poslovni model.

U okvirima šireg konteksta posmatranja, transformacione ideje/inicijative i naponi najčešće se koncentrišu na adaptiranje postojećih poslovno-operativnih procesa, a manje na razvoj konkretnih digitalnih proizvoda ili razvoj novog modela poslovanja (Ibid). Takve kompanije nazivaju se „digitalnim otpornicima“ iz razloga što one nemaju definisanu strategiju digitalne transformacije, a dostupne inicijative su nedovoljno usklađene na strateškom nivou. Nasuprot tome, digitalni transformatori čine one ekonomske subjekte koje isporučuju opipljive digitalne proizvode, usluge i kreirana iskustva, dok su digitalni disruptori veoma nasrtljivi u implementaciji novih digitalnih tehnoloških rešenja i na njima koncipiranih poslovnih modela, bilo da su oni usmereni na obnavljanje, bilo stvaranje novih tržišta. (Dell Technologies, 2016)

Slika br.12 Indeks digitalne transformacije



Izvor: Digital Transformation Index, Dell Technologies, 2016.

Stručnjaci iz domena tehnologije i biznisa, postigli su konsenzus da je danas, imajući u vidu raspon primene i dostupnost, digitalna poslovna transformacija ključ prosperiteta i razvoja svakog poslovnog subjekta, a da je aplikacija centralna okosnica te transformacije.

2. Digitalne mogućnosti, dometi i ograničenja

Ubrzani tehnološki razvoj dovodi do globalne digitalne transformacije društva. Primena savremenih tehnoloških dostignuća, menja gotovo sve sfere ljudskog života, način na koji radi, komunicira, kupuje, provodi slobodno vreme, itd.

Prema Kaufmanu, stručnjaku svetskog ranga za digitalni marketing i profesoru na Lynchburg College School of Business and Economics „digitalnu transformaciju kompanija moraju podržati vlada, akademska zajednica i mediji. Potpuna transformacija kompanija i njihov prelazak na digitalni način rada je neizvestan i kompleksan proces“. Bez obzira na napore koje ulaže, kompanija se ne može sama digitalno transformisati, već u tom smeru mora biti izražen i uticaj okruženja i postojati spoljna stručna edukativna podrška pored primene „best practice“ modela.

Proces tranzicije prema digitalnom je uslov da kompanije prežive pritiske tržišta i konkurencije i obezbede sebi održivu budućnost. U današnjoj, globalizovanoj i interkonektovanoj ekonomiji, imperativi postojanja su integracija, međusobna komunikacija kompanija i njihovih kupaca, međusobna korisnička komunikacija, kao i razvoj strategija i taktika kompanije zasnovanih na stvarnoj vrednosti – poverenju korisnika.

U širem kontekstu, digitalna transformacija predstavlja celovit preobražaj u kome i menadžeri moraju učiti, a ne samo radnici, što podrazumeva i potpuno izmenjen koncept celoživotnog učenja usklađen sa EU okvirom za EU Kompetencije, kako bi na taj način ekonomija i društvo razvili mehanizme za „proizvodnju kompetencija i sposobnosti“, dok je proizvodnja novih stručnih profila kroz obavezno obrazovanje znatno duže i manje fleksibilno.

3. Promene koje generiše digitalna transformacija

Na osnovu istraživačkih nalaza, analiza, kao i vidljivih indikatora koje sa sobom nosi proces primene savremenih tehnologija, proizilazi zaključak da digitalizacija unosi ne samo brojne već i duboke promene, kako u poslovanje, tako i u druge segmente društvenog života. Trend usvajanja strategija digitalne transformacije, u korporativnom segmentu podstiče sve kompanije da se snažnije usmere na unapređenje svog poslovanja.

Digitalizacija kao proces, sprovodi se posredstvom primene digitalnih tehnologija, direktno ili indirektno i po pravilu ostvaruje uticaj na kreiranje vrednosti i konkurentnosti, organizacionog

dizajna (strukture) preduzeća, ljudske resurse, proizvodne procese ili usluge, sistem nagrađivanja i napredovanja i profilisanje strategije razvoja.

Ubrzani prelazak na digitalno poslovanje, poremetiće sve industrije i e-sektore i zahvatiće gotovo celokupan geografski prostor. Digitalizacija menja, pored ostalog, i način povezivanja preduzeća sa kupcima roba i korisnicima usluga uz kreiranje nove vrednosti zajedno sa njima. U digitalnoj eri „za poslovni uspeh je veoma važna dvosmerna komunikacija sa kupcima koja uključuje prikaze proizvoda i usluga koje kupci traže u kontekstu njihovog dinamičkog učešća koje postaje kritično za postizanje poslovnog uspeha“ (Rogers, 2016).

Ključno pitanje za stručnjake i inovatore u ovoj oblasti jeste kakva će biti budućnost ako će svi praktično biti uvek interkonektovani između sebe i umreženi na globalnom planu, odnosno, kako će se digitalni napredak manifestovati na postojeće obrasce i modele poslovanja, rada, kulture i života uopšte?

Pojedine industrije, kao što su osiguranje, bankarstvo, transport, telekomunikacije, energetika, što ne zaobilazi ni javni sektor, digitalizuju se velikom brzinom, ali tempo tog procesa teško može da se postojećim alatima i instrumentima prati sa potrebnom preciznošću.

Digitalnu transformaciju poslovanja prati nov način razmišljanja, pristupa problemima i njihovom rešavanju. S tim u vezi, stručnjaci ocenjuju da ključ uspešne digitalizacije obuhvata: novu strategiju, poboljšanje korisničkog iskustva, digitalni marketing, savremeni CRM sistem, razvoj novog modela upravljanja i poslovanja i inovirani organizacioni dizajn.

Kada se razmatraju svi aspekti ili dimenzije digitalne transformacije, mora se imati u vidu njena sve očiglednija vrednost, kao i to da je ona za poslovanje izuzetno važna. Njeni efekti ogledaju se u povećanju profitabilnosti, rastu i razvoju kompanija u različitim proizvodnim i uslužnim sektorima, što najčešće u praksi može podrazumevati i redefinisane aktuelnih poslovnih modela. Upravo u tome je sadržana i njena osnovna prednost, pa ukoliko su svi elementi obezbeđeni i parametri zastupljeni, ona aktivira i mobilise sve postojeće, ali i potencijalne resurse unutar modernih kompanija, što nije slučaj kod tradicionalnih poslovnih modela u domenu privređivanja.

3.1 Novi model strateškog upravljanja

Novija istraživanja digitalne transformacije, u različitim granama industrije identifikuju više načina ili puteva ka ostvarenju tog cilja, među kojima su dva najvažnija: evolucion i revolucion pristup.

Evolucion pristup primenjuje digitalne mogućnosti kako bi se razvoj ostvario unutar aktuelnog poslovnog modela, odnosno kako bi se kompanija što brže i bolje uključila u korisnički interfejs, obezbedila dijamazon ponude i odgovarajuće sadržaje prilagođene korisnicima. Kompanija tako digitalizuje svoje procese i operacije upravo radi širenja svog poslovnog ekosistema, ali i radi osiguranja boljeg angažovanja zaposlenih i zainteresovanih aktera.

Drugi, revolucionarni pristup, uključuje daleko veće promene. Praktično on iziskuje fundamentalni prelazak na drugačiji poslovni model. Ovakav novi model najčešće donosi i razgranatu strukturu podmodela zajedno sa drastično uvećanim brojem saradnika u tako izgrađenom „poslovnom ekosistemu“.

Posmatrana u tom kontekstu, digitalna transformacija mora se graditi na osnovama koju čine dva elementa: informacija i snaga umrežavanja. Digitalni lideri, ili strateški menadžment, prate taj model i u skladu sa njim kreiraju strateški okvir za budući razvoj kompanije sa odgovarajućom digitalnom orijentacijom.

Prva, i svakako najrelevantnija aktivnost, svodi se na formulisanje i usvajanje nove digitalne strategije, koja, osim što objedinjuje sve digitalne inicijative, uključuje i: pribavljanje svih neophodnih informacija, planiranje, markiranje rizika i šansi, efekte strategije, tj. njene doprinose, kao i aktivnosti vezane za kreiranje podstrategija kao što su: strategija digitalnog marketinga, strategija mobilnog poslovanja, web strategija, strategija CRM-a, odnosno strategija upravljanja odnosima sa kupcima, kao i izradu ostalih pratećih strateških dokumenata kao što su: planovi, programi, elaborati i sl. (Rauser, 2016).

Eksperti i stručni timovi, prilikom kreiranja i sprovođenja digitalne strategije, „moraju evaluirati sve komponente digitalnog ekosistema, sam websajt, sistem upravljanja odnosima sa kupcima, sistem upravljanja resursima preduzeća, kao i online marketinške kampanje“. (Sofronijević, 2017:277)

3.2 Promena poslovanja kompanija/preduzeća i kreiranje novih ekonomskih modela

Generalno uzevši, procesi transformacije poslovanja predstavljaju izuzetno kompleksne inicijative, ideje ili napore koje za cilj imaju unapređenje poslovanja kroz sve funkcije jedne kompanije ili organizacije. Navedeni procesi preispituju i izazivaju fundamentalne promene u načinu na koji se određeni posao obavlja, a integrišu dimenzije strategije, strukture, procesa, tehnologije i ljudi i čime zahtevaju holistički pristup.

Informaciono-komunikacione tehnologije definitivno su potakle rađanje novih naučnih disciplina i redefinisane tradicionalnih. Na ovaj način nastale su nauka o uslugama, nauka o podacima i sl., iz kog razloga se može reći da su informaciono-komunikacione tehnologije zapravo učinile destrukciju i u domenu nauke, ne samo privrede. Destruktivni uticaj IKT-a na modele tradicionalnih ekonomskih sistema zapravo nam je doneo digitalnu ekonomiju. To je dovelo i do drastične promene u domenu proizvodnje zajedno sa pojavom industrije 4.0, a sve to zajedno je uticalo na asortiman dobara i usluga, njihovu globalnu raspodelu, drastično se promenio i sistem ponude i potražnje, a ekonomski sistemi su postali kompleksni i podložni kombinovanju, što je sve zajedno doprinelo jednoj enormnoj složenosti u domenu svih vrsta ekonomskih transakcija.

Tako nastali revolucionarni tehnološki trendovi doveli su do ciklične transformacije i ekonomije i društva, što je pored opšte disrupcije proizvelo eksponencijalni rast i suštinski strukturne promene. Proizvodi i usluge su u svom razvoju kroz inovacije počeli beležiti kvantne skokove zasnovane na tehnološkim inovacijama, redefinisane postojećih i stalno kreiranje novih proizvoda i usluga.

Na temelju ovakvih kretanja nastali su i novi jezički termini sa ciljem da se istim pokuša i jezički ispratiti kretanje globalnih i lokalnih trendova, upravo nastalih usled integracije i interakcije ova dva područja, koja se objedinjuju u jedan jezički izraz – „glokalno“. Tako nastala interakcija tehnologije i društva učinila je ozbiljne pomake i izazove u svim društvenim i ekonomskim segmentima, počev od zdravstvenog aspekta, demografije, do samog kvaliteta života i životnog okruženja. Na ovaj način nastali su novi pojavni oblici održivih razvojnih formi, ali i pojavni oblici novih ekonomskih modela.

3.2.1 Ekonomija deljenja

Ekonomija deljenja (eng. Share Economy), nastala je na logičkom konceptu potrošnje deljenjem, po izvornoj ideji zasnovanoj na racionalnosti u kojoj stvari ne treba posedovati, već ih deliti i razmenjivati, pozajmiti ih umesto kupiti, itd. (Fellander, Ingram, Teigland, 2015).

Ovakav ekonomski rezon zapravo je potaknut razvojem društvenih mreža i novog virtuelnog konstrukta deljenja, gde pripadnici ove društvene zajednice zapravo konstantno dele svoje fotografije, razmenjuju informacije, činjenice o intimi i sl., iz kog razloga je nastao jedan sociološki fenomen da oni koji virtuelno žive na opisani način, ne žive drugačije ni u stvarnom životu.

U savremenoj ekonomiji trendovi su učinili da mašine sve češće zamenjuju ljude u uobičajenim poslovima. Međutim, kada u kontekstu aktuelnog trenutka kažemo mašine, potpuno je jasno da se tu ne misli o gvozdanim mehaničkim napravama i postrojenjima iz vremena ranijih industrijskih revolucija, već su današnje mašine najpre umreženi visoko sofisticirani uređaji koji su u stanju da međusobno komuniciraju.

Džeremi Rifkin izneo je svoje viđenje da će doba koje je pred nama zapravo učiniti da će granični trošak, tj. trošak proizvodnje dodatne jedinice proizvoda, biti sveden na nulu, usled delovanja faktora drastičnog povećanja efektivnosti i produktivnosti, upravo zasnovane na pritisku konkurencije. On smatra da konstantno opadajući troškovi proizvodnje koje je donelo Internet povezivanje „svega sa svime“, kao npr. povezivanje milijardu senzora sa ljudskim domovima, kancelarijskim prostorima, proizvodnim linijama, transportnim sredstvima, aparatima i uređajima, ali i ljudima, doneli su do sada nezabeležene posledice na društvo, obzirom da postoje sredstva komunikacije koja omogućavaju da milioni ljudi nezavisno od lokacije komuniciraju, dele svoja saznanja i znanja i saraduju na stvaranju novih proizvoda i usluga koji se potom pojavljuju na tržištu po relativno niskim troškovima proizvodnje (Rifkin, 2014).

3.2.2 Ekonomija saradnje

Ekonomija saradnje predstavlja ekonomski model zasnovan na tehnologijama koje su u stanju da ljudima omoguće da dele i dobiju, odnosno nabave ono što predstavlja predmet njihove tražnje. Ovaj vid ekonomije ima mnogo toga zajedničkog sa ekonomijom deljenja. Prema doktoru Arunu

Sundararajanu, inače autoru ekonomije saradnje, ovaj vid ekonomije je za relativno kratko vreme pokrenut napred sa veoma niskog nivoa usled tehnološke nerazvijenosti do značajno većeg nivoa sa razvojem interakcija na nivou „consumer 2 consumer“ što je doprinelo tome da se interakcija i razmena sa ljudima može odvijati veoma brzo i na načine putem kojih je moguće uspostaviti poverenje između dva korisnika, što samo po sebi uvećava ekonomiju i ekonomski efekat.

Period sveopšte ekonomske tranzicije konstantno donosi novu inspiraciju za kreiranje novih inovativnih modela i ljudi koji komuniciraju i saraduju širom sveta. Zagovornici ovog ekonomskog modela ističu da bi oni mogli iskoristiti nepopunjene praznine u bruto domaćem proizvodu, međutim jedna od prepreka za to je da regulativa ne prati poslovne tendencije o kojima je ovde reč. Prema Arunu i pristalicama ovog ekonomskog modela, istaknuto je da će vreme ekonomije saradnje tek pokazati svoje potencijale kao jednog novog modela organizovanja ekonomskih aktivnosti.

3.2.3 Zelena ekonomija

Tendencije da se dostigne potpuna proizvodnja energije iz obnovljivih izvora dovela je do nastanka koncepta zelene ekonomije i razvoja tzv. “zelenih poslova“. U smislu obnovljivih izvora energije možemo obuhvatiti sledeće: morsku energiju, vetro energiju, energiju dobijenu iz bio mase, gasnu energiju dobijenu iz deponija, geo i aero termalnu energiju, energiju sunca, energiju dobijenu iz bio gasa i energiju dobijenu iz preradnih postrojenja za otpadne vode.

Zelena ekonomija se temelji na sledećim principima:

- integrisanom pristupu kontroli emisije;
- preventivnom pristupu;
- principima pregovora o uslovima dobijanja dozvola; i
- principima transparentnosti.

3.2.4 Cirkularna ekonomija

Cirkularna ekonomija se odnosi na privredu čiji je cilj ukupna obnovljivost, kako u smislu obnovljivih izvora energije, tako i nasuprot tome, kroz nastojanje eliminacije upotrebe hemikalija i hemijskih sredstava i stvaranja otpora takvom vidu poslovanja.

Ova vrsta ekonomije utemeljena je na sledećim načelima:

Načelu eliminacija otpada: nastajanje otpada moguće je isključivo ako materijali od kojih su sačinjeni određeni proizvodi nisu razgradivi i namenjeni ponovnoj upotrebi, bez obzira da li se radi o tehničkom ili biološkom smislu;

Načelu promovisanja i širenja mogućnosti za iskorišćavanje obnovljivih izvora energije sa ciljem da svi sistemi dostignu nivo stalne upotrebe obnovljivih i održivih energetske izvora;

Načelu podsticajne ljudske aktivnosti u svim segmentima;

Načelu iskorišćenosti resursa radi ostvarivanja nove vrednosti, kako finansijskih, tako i nefinansijskih;

Načelu razmatranja suštine sistema kod koga je od presudne važnosti razumevanje toga kakav je međusobni odnos delova sistema i tih delova sa celinom, gde se elementi sistema cirkularne ekonomije posmatraju u kontekstu zaštite životne sredine i društva kao celine.

Načelu slojevitog posmatranja problema kao načina posmatranja vrednosti materijala sačinjenih u biorazgradivim formama, kako bi se stvorila vrednost koja se zasniva na razlaganju i razgradnji materijala na delove, radi njihove ponovne upotrebe.

3.2.5 Bihejvioralna ekonomija

Ova vrsta ekonomije po svojoj suštini predstavlja kombinovanje ekonomske nauke sa drugim društvenim naukama, ali u domenima koji opisuju i proučavaju ponašanje. Ovaj vid ekonomije skoro isključivo se javlja kada ekonomski analitičari radi poboljšanja deskriptivne vrednosti ekonomske teorije vrše kombinovanje istraživanja i metoda istraživanja iz oblasti ekonomije i drugih društvenih nauka (Weber, 2005:91-108). U tom smislu može se reći da se bihejvioralna ekonomija zapravo bavi uticajem psihologije pojedinca na ukupno ekonomsko odlučivanje, iz kog razloga se u zapadnoj literaturi veoma često za ovu ekonomiju koristi i izraz brain game economy, ekonomija ponašanja ili psihološka ekonomija.

3.2.6 Ekonomija utemeljena na znanju

Osnovni pokretački impuls u aktuelnom ekonomskom okruženju u svetu jesu znanje i nove tehnologije. U takvom ekonomskom okruženju informacije su osnovni resurs za razvoj i stvaranje nove vrednosti. Nesumnjiva je uloga države u domenu ekonomija zasnovanih na znanju, jer država u takvim ekonomijama stimuliše znanje kao resurs, stimuliše njegovo širenje, podstiče nivo i kvalitet ljudskog kapitala i sl.

Stubovi ekonomije zasnovane na znanju prema trouglu znanja obuhvataju:

- obrazovni sistem i suštinsko obrazovanje;
- informacionu, odnosno informatičku infrastrukturu;
- inovacioni sistem zasnovan na istraživanju i tehnologijama; i
- prateće ekonomske podsticaje i institucionalni sistem za praćenje navedenih segmenata.

Pored navedenih pojavnih oblika u domenu ekonomskih modela, pojavljuju se takođe i algoritam ekonomija, aditivna ekonomija zasnovana na 3D printingu i kripto ekonomija, odnosno blockchain ekonomija.

3.3 Poboljšanje korisničkog iskustva

Po svojoj prirodi, kao i načinu primene, digitalizacija menja način povezivanja preduzeća sa klijentima, kupcima i korisnicima usluga, radi kreiranja vrednosti u sadejstvu sa njima. Kompanije koje se oslanjaju na tradicionalni način rada, kontakt i odnose sa kupcima uglavnom uspostavljaju putem marketinških promocija, putem kojih i šalju svoje objave kupcima.

U digitalnoj eri, odnosi i veze sa kupcima uspostavljaju se na potpuno drugačijim osnovima i principima od ranijih. Ipak, najveća korist od digitalnih tehnologija i same digitalizacije ogleda se u povećanoj interakciji kompanije sa konzumentima njenih proizvoda i usluga.

Sa digitalizacijom preduzeća, odnosno kompanija, postiže se bolje korisničko iskustvo. Paralelno sa razvojem tehnologije, menja se svest kupaca, odnosno korisnika, ali i njihove namere, želje i potrebe. U današnjem okruženju, kupac/korisnik nastoji da zadovolji svoje želje na nov i jedinstven način, a to od kompanija iziskuje da njihovi proizvodi/usluge budu prilagođeni interesovanju i zahtevima kupaca.

Kvalitetno korisničko iskustvo je rezultat usklađivanja poslovnih ciljeva kompanije i potreba korisnika. Da bi formulisali i razumeli korisničko iskustvo, kompanije najpre moraju studiozno sagledati šta kupce interesuje, koje su njihove potrebe, i u skladu sa tim, moraju sagledati svoje mogućnosti na planu ispunjenja tih potreba.

U praksi, kompanije u cilju poboljšanja korisničkog iskustva primenjuju najčešće 7 koraka ili aktivnosti i to:

- Intervju sa krajnjim korisnicima, zaposlenima, predstavnicima drugih timova uključenih u razvoj web prezentacija ili aplikacija, radi otkrivanja navika i individualnih želja, potreba korisnika, kako bi na osnovu toga sačinili predlog unapređenja postojećih proizvoda ili pristupili proizvodnji novih.
- Razrada tipičnih grupa korisnika ili tzv. “izrada persona“. Izabrane grupe korisnika služe kao lakmus papir za određivanje prioriteta i odlučivanje o dizajnu i funkcionalnosti proizvoda ili usluga i najviše pomažu pri podizanju svesti o potrebama i zahtevima krajnjih korisnika.
- Heuristička procena je najkraće rečeno metoda analize interfejsa, koju sprovode stručnjaci unutar kompanije, ili putem angažovanih agencija, a prema unapred zadatim preporukama za upotrebljiva poređenja različitih grupa korisnika i njihovih raznovrsnih potreba. Sa razvojem tehnologije i transformacijom navika krajnjih potrošača, proširene su i osnovne smernice, dok su pojedini stručnjaci razvili i sopstvene smernice i metodologije.
- Kognitivna „šetnja“ (walkthrough) je takođe metoda analize poređenja koja služi za testiranje korisnika kroz unapred definisane procese. Ova metoda se često koristi za procenu kritičnih procesa, identifikovanih kroz intervju ili povratne informacije primljenih od korisnika u vezi web stranica. Analiza se sprovodi tako što korisnici odgovaraju na set pitanja tipskog karaktera za svaku pojedinačnu akciju u okviru svakog pojedinačnog procesa.
- Testiranje upotebljivosti je metoda procene korisničkog poređenja ili web stanica, posmatranjem tipičnog korisnika dok koristi poređenje. Time se utvrđuju greške na poređenju, ali i stepen razumevanja i lakoća korišćenja korisničkog poređenja. Testiranje može biti kvantitativnog ili kvalitativnog karaktera. Kvantitativno poređenje sprovodi se u laboratorijama i potreban mu je veći uzorak korisnika, u proseku 10-ak po grupi za testiranje, dok kvalitativno testiranje obuhvata manji uzorak od 3 do 4 korisnika.
- Mapiranje korisničkog putovanja (Customer Journey Mapping) je sveobuhvatni prikaz sleda događaja čiji je centralni subjekt tipični krajnji korisnik. Korisničko putovanje prikazuje pored ostalog i događaje koji su nastali pre ili posle interakcije sa sistemom, a odnosi se i na kontekst uređaja, okruženje, vremenski redosled, lokaciju, lične sklonosti, mentalni model i čitav spektar društvenih varijabli. Obzirom da obuhvata niz radnji na putu od korisničke inicijalne radnje do realizacije, korisnički put se može mapirati za svaku grupu

ili kategoriju korisnika i za svaki način korišćenja. Prilikom mapiranja, mogu se izdvojiti želje korisnika i njihovo realno iskustvo i na taj način utvrditi eventualna mesta za poboljšanja i korekcije.

- Izrada dijagrama toka korišćenja (Process flow) je prikaz interakcije između korisnika i sistema radi obrade i razumevanja svih najvažnijih momenata interakcije. U procesnom smislu obuhvata logička razdvajanja scenarija, te definiše redosled pojedinih akcija. U zavisnosti od konkretnih uloga unutar projektnog zadatka, dijagrami toka izrađuju se u saradnji sa „developerima“ koji će dalje razvijati poslovnu logiku.

Iskustva su pokazala da dobro oblikovano korisničko iskustvo u značajnoj meri poboljšava i optimizuje proizvode i usluge. Krajnji efekat je uspešna simbioza i konvergencija između krajnjih kupaca, proizvođača i davalaca usluga. Na taj način, kupcima se uvećava dostupnost proizvoda i usluga koji im najviše trebaju i za koje su spremni uložiti sredstva, a sa druge strane, proizvođači i davaoci usluga mogu znatno bolje optimizovati svoje radne procese i usmeriti se na projektovanje usluga i proizvoda koje korisnici najviše traže i žele.

Iz tih razloga, sve je više kompanija koje usmeravaju pažnju na bolje pružanje usluga klijentima. Statistički gledano, u 60% slučajeva kupovina se obavi pre kontakta sa prodavcem, jer su kupci putem interneta ili drugih uređaja pretražili asortiman i sadržaj koji im najviše treba.

Kada je u pitanju odnos proizvođača i kupca i dalje je na snazi „pravilo“ – ako su klijenti stvarno zadovoljni tim iskustvom, vremenom će postati lojalni, a to znači da lojalni klijenti kupuju više.

Danas kupci očekuju od brendova da im pruže najveće moguće iskustvo, a to iskustvo ljudi koriste da bi procenili i odredili da li je neki brend vredan njihovog vremena. S tim u vezi, može se slobodno reći da brendovi mogu da iskoriste moć moderne tehnologije i poboljšaju svoju uslugu na osnovu prioriteta svojih klijenata, kako bi im pružili iskustvo koje je na tragu ili prevazilazi njihova očekivanja iz okvira konkretne ciljne grupe.

U stručnoj literaturi, sa manjim ili većim modifikacijama, navodi se 5 načina putem kojih kompanije danas mogu da povećaju angažovanje klijenata i poboljšaju korisničko iskustvo pomoću tehnologije, i to najčešće kao:

- Nadzor ponašanja klijenata i praćenje njihovih napora;
- Promena pravila igre pomoću mašine koja uči;

- Automatizacija za smanjenje vremena čekanja;
- Veštačka inteligencija, četbotovi i samousluga; i
- Poboljšana personalizacija sa poboljšanim podacima.

Dakle, ispunjenje očekivanja kupaca ostaje kritičan element kompetitivne prednosti kompanija. Kombinovanje tzv. mapa potrošačkog puta (Customer Journey map) koje opisuju iskustvo kupca i modela poslovnog procesa, kao i načina ostvarivanja poslovanja i dalje će biti ključno u identifikovanju potreba kupaca i njihovih preferencija, uz individualni pristup i prilagođeno izvršavanje poslovnih procesa.

4. Savremeni sistemi upravljanja odnosima sa kupcima (CRM)

Upravljanje odnosima sa kupcima (Customer Relationship Management - CRM) nema jedinstvenu definiciju. Najsveobuhvatnija definicija bi sudeći po svemu bila da CRM predstavlja metodologiju, strategiju i softver u kombinaciji sa web mogućnostima, koje kompanija koristi kako bi upravljala i organizovala svoje odnose sa kupcima/klijentima/korisnicima/potrošačima.

Prema Tumbasu, CRM predstavlja strategiju koja se primenjuje u cilju sticanja što više saznanja o kupcima, njihovim potrebama i ponašanjima, kako bi se na relaciji kompanija/kupac razvili čvršći međusobni odnosi. Princip upravljanja odnosima sa klijentima koncipiran je radi optimizacije dugoročne relacije klijenata i kompanija radi kontinuiranog stvaranja vrednosti, pored čega je CRM suštinski i poslovna filozofija koja je stalno usmerena na klijenta i njegove potrebe sa jedne strane, i razvijenu organizacionu kulturu kompanije koja služi kao podrška efikasnom marketingu, prodajnim i uslužnim procesima sa druge strane.

Praksa je pokazala, a nauka to potvrđuje, da je savremena tržišna utakmica prepoznala kupca kao njenog glavnog igrača, uvažavajući činjenicu da je moć da odlučuje, bira, pretražuje i upoređuje ponude, rukuje internetom, itd., isključivo u njegovim rukama.

Klijent, odnosno kupac je svoju moć stekao time da vreme u kome on preduzima opisane aktivnosti, kao ni udaljenost od kompanije i proizvoda, njega ne limitiraju da odabere proizvod ili uslugu, proizvođača ili ponuđača, kako bi ostvario neki svoj cilj, zadovoljio neko svoje htenje ili potrebu. Na ovaj način klijenti mogu on-line otvoriti račun u banci, vršiti sve bankarske poslove, birati kanale komunikacije i raditi sve ono što žele ili im je potrebno, kako bi uštedeli vreme i novac. Iz ovog razloga, smatra se da su odnosi sa klijentima u današnje vreme najveća

vrednost, čak po nekim stavovima i nematerijalna imovina kompanije, pa adekvatno upravljanje tim najvrednijim asetom predstavlja fundament postojanja i opstanka svake moderne kompanije.

Da bi kompanije ostale i opstale na tržištu, one moraju da sebe i svoje poslovanje prilagode klijentima, kako bi njihovi proizvodi najbrže pronašli one kojima su namenjeni. Da bi to bilo moguće, kompanije moraju imati strateško opredeljenje koje je okrenuto ka klijentima i njihovim potrebama, a to je moguće ostvariti isključivo u slučaju postojanja i implementacije strategije CRM-a.

Da bi se upravljalo odnosima sa klijentima, odnosno kupcima, kompanija mora poznavati svoje kupce, znati što više o njima, znati koji ih proizvodi i usluge zanimaju, tačnije znati sve ono što mogu saznati, kako bi svoju ponudu strukturisali prema klijentu i njegovim afinitetima, a sve kako bi se učinilo da klijent postane i ostane trajno lojalan kompaniji i njenoj ponudi. Ipak, kao i najveći broj trendova u elektronskom poslovanju, i CRM je nastao na temeljima potrebe svake kompanije da stalno radi na tome da povećava obim poslovanja, profit i poslovnu efikasnost, a za to je CRM presudan kao vid strateškog upravljanja.

Tržište na kome dominira koncept stalnih inovacija, stalnog prodiranja novih proizvoda i usluga i novih konkurenata, a time i snažne konkurencije, učinilo je da je borba za kupca i njegovu naklonost bezmalo uslov i postojanja i opstanka kompanija. U tome se desila i promena u poslovnoj filozofiji koja potiče iz ideje CRM-a, a to je da kompanije nisu više orijentisane prema proizvodu, već prema klijentu, čime je suštinski pomeren fokus poslovanja. Da bi CRM, a time i poslovanje kompanije bilo uspešno, upravljanje odnosima sa klijentima mora biti podržano od cele kompanije, ne samo marketinškog ili nekog drugog pojedinačnog sektora, pa uspeh garantuje isključivo to ako se svi poslovni procesi kompanije suštinski kompatibilizuju sa tim ciljem. Da bi se moglo uticati na aktivnosti klijenta, neophodno je što bolje njihovo poznavanje od strane kompanije, a da bi to bilo moguće, aktivnosti klijenta se intenzivno prate, beleži se sve što oni čine, a kompanija na osnovu analiza tih saznanja stiče spremnost da blagovremeno, još preciznije, pravovremenije deluje, ne samo na aktuelne, već i na buduće potrebe svojih klijenata.

Dakle, kada je u pitanju CRM, u pitanju je kontinuirani proces prilagođavanja svih segmenata poslovanja, poslovne strategije i njihovih podsegmenata klijentima i njihovim potrebama.

CRM nije nastao bez udela poslovne tradicije. Naime, kompanije decenijama unazad prikupljaju podatke o klijentima, njihove lične podatke, lične i porodične prilike, navike i potrebe, kako bi

takve informacije tradicionalno bile upotrebljavane za usavršavanje proizvoda i usluga, kreiranje i promociju novih ili prilagođavanje autonomnih poslovnih modela unapređenju poslovanja, čije je konačno ishodište povećanje profitabilnosti i poboljšanje tržišne pozicije kompanije.

Kada je u pitanju elektronsko poslovanje, nesporno je da ono počiva na informacionim tehnologijama. Međutim, CRM predstavlja vid široke integracije svih dostupnih i primenjenih informacionih tehnologija koje kompanije koriste u svom radu, a to su baze podataka, web sajtovi (prezentacije), kompanijski intranet, kontakt centar kompanije, a iza toga i informacione tehnologije koje se koriste u sektorima za finansije, prodaju, marketing i proizvodnju.

Informacione tehnologije su doprinele da upravljanje odnosima sa kupcima kao poslovna strategija osnaži najvažnije oblasti u funkcionisanju kompanije, sa ciljem maksimizacije njenog poslovnog profita. Radi ilustracije rezultata uspešnog CRM-a, možemo uzeti i jedan hipotetički primer iz domena bankarstva, u kome se na osnovu CRM saznanja stvaraju uslovi za redefinisane pristupa klijentima i njihovom vrednovanju.

Ovaj primer sastoji se iz 4 segmenta:

- Rezultata analize ukupnog potencijala klijenata koji ukazuje na to da 20% klijenata jedne banke proizvodi 150% njene dobiti, dok sa druge strane 40-50% klijenata za 50% umanjuje dobit banke;
- Utvrđenja analize koje kaže da je 10 puta skuplje steći novog klijenta, nego ostvariti i zadržati poslovnu saradnju sa postojećim klijentom;
- Rezultata analize koji govori da prosečan nezadovoljan kupac usluga svoje nezadovoljstvo prenese na još 8-10 drugih ljudi; i
- Utvrđenja da povećanje od 5% klijenata koje je banka uspela zadržati ima potencijal da uveća njen profit između 60 i 100%.

Savremena CRM rešenja najpre predstavljaju poslovnu strategiju kompanije, a zatim i softversko, odnosno informatičko rešenje kompanije da tu strategiju i održi. Samim tim, CRM je do nivoa poslovne sinergije integrisao sve različite vidove upravljanja i samo upravljanje različitim oblastima u okviru kompanije, pa time i poslovnog sistema, kako bi sve to zajedno podrazumevalo sistemsko upravljanje podacima, kupcima i dobavljačima, računovodstvom i finansijama, prodajom i prodajnim mestima, kao i marketingom.

Kao poslovna strategija, CRM služi tome da optimizuje zadovoljstvo klijenata, nivo prihoda i stepen profitabilnosti kompanije. Međutim, razvojni trendovi aktuelnih i budućih rešenja iz domena CRM-a moraju dati održive poslovne odgovore na 5 izuzetno važnih, savremenih pojava. Te pojave su: digitalna transformacija poslovanja, međusoftverske integracije, promene regulatornog okvira na tržištu, promene u domenu marketinga i prodaje, a preko svega i senzibilitet za savremene navike i očekivanja kupaca.

Uloga digitalne forme poslovanja zaokružena je težnjama da nestanu granice između fizičkog i digitalnog, što se apsolutno postiže digitalizacijom svih poslovnih procesa i integracijom savremenih digitalnih tehnologija u njih. U cilju realizacije ove ideje, nastao je veliki broj inovativnih tehnoloških rešenja koja su koncipirana na način da kupcima omoguće da svoje potrebe zadovoljavaju u vreme i na mestima izričito određenih njihovim željama, htenjima i potrebama.

Veliku ulogu u ovom domenu ima i internet stvari koji je omogućio da se veliki broj senzora „tracking“ sistema angažuje za sticanje saznanja o tome kako se kupci ponašaju u trgovini, kakve se informacije dobijaju kroz pametnu naplatu, pametne potrošačke korpe, pametne rafove i police, ali i pametne domove, sve kako bi se stalno analizirali načini koji će omogućiti kupcu da svoju kupovinu i finansijske transakcije vezane za nju, obavi bez gubljenja vremena i bez otežavajućih ili usporavajućih okolnosti.

Korak dalje od Interneta stvari, pojavljuje se i veštačka inteligencija kao glavni resurs za kreiranje CRM-a druge generacije, koji će biti u stanju da uoči, uči i razume baze podataka u kojima su sadržane sve interakcije ljudi sa mašinama i kompanijama, kako bi se putem tog delovanja pronašli novi poslovni odgovori i kako bi sistemski CRM poslovni fokus kompanije usmerio na najvažnije stvari. Kombinacija veštačke inteligencije i mašinskog učenja na putu je da stvori sistem učenja iz podataka o korisnicima i da na osnovu tih učenja unapredi rezultate poslovanja. U navedenom se ne može zaobići ni koncept Big Data koji omogućava rešavanje poslovnih problema na temelju preuzimanja, upravljanja i obrade velike količine podataka.

Kada je u pitanju digitalna strategija kompanije, ona je po svojoj suštini veoma opsežan pojam koji samim tim obuhvata širok dijapazon aspekata primene digitalnih tehnologija u kompaniji. Ta primena se kreće od najosnovnijih stvari, kao što su digitalni informacioni displeji (terminali) na mestima prodaje, pa sve do primene uređaja za virtuelnu realnost i proširenu stvarnost.

Digitalni trend koji je izazvao međusoftversku integraciju, zapravo je potakao integrisanje CRM-a i ERP-a (Enterprise Resource Planning) u cilju značajnog pojednostavljenja poslovnih procesa sa ciljem povećanja produktivnosti kompanije. Ova međusoftverska integracija funkcioniše na principima, ne samo razmene podataka između dva sistema, već njihovog povezivanja i usklađivanja u kompleksnu i usklađenu, tj. celovitu bazu podataka. Putem primene ovog rešenja, zaposlenima je omogućena momentalna dostupnost svih postojećih podataka, odnosno dostupnost svih podataka o koricnicima u realnom vremenskom intervalu. Ovom međusoftverskom integracijom rešen je i problem dvostrukog unošenja podataka u obe baze pojedinačno, usled čega se svaki podatak ili izmena učinjena u ERP sistemu, istovremeno integriše i pojavljuje u sistemu CRM, kao i suprotno. Ovim pristupom bitno su optimizovani i troškovi koje kompanije imaju u vidu radne snage, bilo u domenu održavanja IT-a, ili u domenu obuke zaposlenih, jer svi zaposleni zapravo istovremeno obavljaju svoje poslove u objedinjenoj platformi CRM/ERP.

Ovakva integracija poslova u okviru kompanije, dalje se integriše sa e-commerce rešenjima, što donosi novi kvalitet poslovanja, jer povećava tačnost porudžbina i njihovu brzinu. Na ovaj način postignuta je sinhronizovana kontrola podataka o proizvodima i uslugama, ali i o njihovim cenama i pratećim značajnim obeležjima, koja su dalje ukrštena sa podacima o aktuelnim i potencijalnim klijentima, što čini osnov za kreiranje jasne strategije rada sektora za marketing i prodaju kompanije.

Razvoj i implementacija digitalnih strategija je osim razvojne komponente i komponente racionalizacije poslovanja, dovela i do pritiska na kompanije koje funkcionišu u domenu elektronskog poslovanja na Internetu, da se povinuju izmenama i tendencijama u inoviranju zakonskih propisa i ostale pravne regulative, koja, usled sveprisutnog digitalnog pritiska, teži da uredi pitanje prava potrošača na zaštitu ličnih podataka, bilo da je u pitanju njihova prekomerna ili nesvrshodna upotreba ili zloupotreba u marketinške svrhe.

U tom segmentu prednjači evropska opšta uredba o zaštiti ličnih podataka koja predviđa veoma ozbiljne sankcije u slučaju narušavanja privatnosti građana EU na neki od opisanih načina. Novina koja je nastupila sa ovom uredbom jeste da ova uredba zabranjuje upotrebu podataka o ličnosti potrošača bez njihovog znanja i u suštini promovise institut informisanog pristanka o radnjama i htenjima kompanije u vezi sa njima. Druga novina u domenu zaštite prava potrošača, zapravo je njihovo pravo da zahtevaju brisanje svojih ličnih podataka iz svih baza podataka u

koje su dospeli bez prethodne saglasnosti, što samim tim uključuje i sam CRM, dok su sa druge strane kompanije u obavezi da obezbede sigurne skladišne kapacitete za ove podatke, kako istima niko ko nije ovlašćen, ne bi mogao pristupiti.

Uredba GDPR je od svog stupanja na snagu u maju 2018. godine uveliko doprinela u menjanju do tada uobičajene poslovne prakse zasipanja potrošača neželjenim elektronskim komercijalnim porukama koje nisu samo bile ograničene na e-mail, sms i telefonske pozive, usled čega su kompanije koje primenjuju savremeno CRM rešenje u svoje poslovanje uvele brigu za podatke kupaca, iz čega se može izvesti paralela da uspešno i pouzdano rešenje iz domena CRM ne može više biti takvo, ako ne omogući i doslovnu primenu GDPR uredbe.

Sve napred navedeno dovelo je do toga da su kompanije morale pronaći novi pristup u domenu marketinga i prodaje. Taj novi pristup podrazumeva dublje sagledavanje u prodaji i marketingu koje se u stručnim krugovima naziva i Omnichannel.

Omnichannel koncept danas preovlađuje, imajući u vidu da je on strateški usmeren na potrebe kupaca, a kao takav on eliminiše granice između različitih kanala marketinga i prodaje, čime stvara integraciju sa centralnom pozicijom na kojoj je kupac i sekundarnom na kojoj je brend.

Kako su u ovom konceptu svi kanali marketinga i prodaje apsolutno sinhronizovani, kupci ih mogu koristiti sve istovremeno, ili se lako prebacivati sa jednog na drugi. Da bi pronašli određeni proizvod ili uslugu, kupcima je dostupno mnoštvo kanala kao što su društvene mreže, pretraživači i sl., a prodaja kao ishod poslovanja može se obavljati istovremeno i u on-line i u off-line modu, odnosno kanalu, bilo preko postojeće fizički prisutne prodavnice, bilo preko internet prezentacije, društvene mreže ili sličnog kanala.

Slika.br.13 Prikaz Omnichannel marketing koncepta



Izvor: https://www.singlegrain.com/wp-content/uploads/2019/03/SG-Omnichannel-Marketing_Using-the-Content-Sprout-to-Overcome-Info-Overload.jpg

Sve ovo omogućio je i zaokruženi koncept u domenu načina plaćanja koje se može odvijati u fizičkom novcu ili putem platnih kartica, elektronskog ili m-bankinga, što u kontinuitetu omogućava i različite vrste načina isporuke dobara i usluga. Dalji razvoj ovih koncepata proizveo je nastajanje novih poslovnih modela u elektronskoj trgovini i poslovanju, pa se integracija dogodila i u opsegu „starih“ modela elektronskog poslovanja (B2B i B2C), koja je proizvela integrisani poslovni model B2B2B2C (Business-to-Business-to-Business-To-Consumer) što su zapravo e-prodavnice čiji je glavni zadatak promovisanje proizvoda i pronalaženje kupaca, ali bez kontakta ovih prodavnica sa robom koja je u prodaji.

Ovakav način poslovanja zapravo u nekom smislu predstavlja delimični outsourcing prodajne i marketing funkcije preduzeća, međutim CRM sistem i dalje beleži i analizira sve podatke o prodaji i kupcima koji su nastali na ovaj način. Sve navedeno, u smislu zaokružene poslovne evolucije, dovelo je i do evolucije kod samih kupaca, tačnije došlo je do nastanka nove generacije kupaca. Tako, generacije kupaca rođene u osamdesetim i devedesetim godinama prošlog veka i kupci rođeni od sredine devedesetih godina prošlog veka na ovamo, veoma često imaju potpuno različite navike i potrebe, usled čega se moraju različito tržišno tretirati i segmentirati. Razlog za to je sasvim jednostavan, a to je što novije generacije potrošača svoje afinitete artikulišu kroz dublju povezanost sa brendovima putem raznih uređaja i mreža, čime su oni u svakom trenutku u mogućnosti da prate personalizovana iskustva drugih potrošača u domenu kupovine koja je od njihovog interesa, te u slučaju prijemčivog saznanja stečenog na ovaj način, oni robu žele nabaviti što brže i što lakše i posredstvom svojih pametnih telefona i drugih mobilnih uređaja, čime onda oni preuzimaju ulogu onih koji dalje „šeruju“ svoje iskustvo u vezi kupovine i kupljene robe ili usluge, najpre putem društvenih medija na kojima su prisutni.

Digitalno doba i komunikacije i česta nepromišljenost i nepažljivost kupaca, učinili su da je on-line poslovanje i on-line postojanje nepresušni izvor digitalnih tragova potrošača. U tom prostoru leži najveći potencijal savremenog CRM sistema koji je projektovan da te tragove zabeleži, obradi i analizira primenom holističkog pristupa, kroz tzv. “360 Customer View“, čime ovaj sistem sabira sve važne podatke o jednoj osobi na jednu web lokaciju. Tako prikupljeni podaci proističu iz svih vrsta kontakata i komunikacije uspešnih marketinških kampanja, prodajnih prilika, istorijata kupovina i svega sl., što bi moglo da se ukrsti kroz domen odnosa kompanija sa kupcima i domen upravljanja tim odnosima.

Slika br. 14 Model CRM – 360° View



Izvor: Wikipedia

Ovo je uvek zato, jer planiran i ambiciozan rast kompanije može garantovati samo kontrolisano okruženje u kome se pažljivo i holistički upravlja svim prodajnim procesima, a u kojima se neguje zadovoljstvo klijenata i kontekst njihovih očekivanja, ali i poznavanje njihovih navika i prilika radi efikasnog pružanja „aftersales“ podrške, koja jedina može obezbediti dugoročnu i tesnu saradnju i održavanje poverenja sa klijentima.

Da bi sve opisano bilo funkcionalno kao sistem, potrebno je da bude objedinjeno u savremeno CRM rešenje, međutim, savremeno CRM rešenje ne rešava sve probleme kompanije, jer CRM sisteme imaju i svi važni konkurenti, a takvi konkurenti takođe potpuno svesno koriste sve potencijale omnichannel virtuelnog sveta. U tom svetu na liderskim pozicijama opstaju samo najposposobniji i oni koji predano rade i prepoznaju potrebe kupaca i trendove u njihovoj evoluciji i evoluciji komunikacionih kanala, odnosno oni koji se trendovski kreću napred kroz kupce i njihove afinitete i pritom razumeju da su kupci promenljiva i često „Trend Driven“ kategorija.

Ovde se ne sme zanemariti ni sistem u kome životni ciklus klijenata nije statičan, kao ni relacije klijenata sa povezanim licima, iz kog razloga kompanija koja želi opstati i stalno rasti na tržištu, mora veoma pažljivo rukovati marketing kampanjama i njihovim rezultatima, jer samo to garantuje da će ponuda koja se iznosi pred klijente uvek biti prilagođena, ne samo klijentima kao opštoj kategoriji, već i segmentima u kojima se oni dele prema potrebama, interesovanjima i sl.

5. Prednosti i vrednosti koje stvara digitalno poslovanje

U stručnim krugovima i diskursu, sve češće se govori o tzv. digitalnom rascepu, tj. digitalnom jazu i digitalnom usponu. Primena najsavremenije IK tehnologije, tj. digitalizacija u najširem smislu, bilo da se primenjuje u državnoj upravi ili ekonomiji, kako pokazuju rezultati, dovodi do povećanja produktivnosti i konkurentnosti. U uslovima rastuće globalizovane ekonomije i konkurentskih pritisaka koje ona donosi, navedeni elementi ne dovode samo do povećanja društvenog proizvoda i blagostanja nacije, već daju prikaz shavatanja imperativa zadržavanja priključka u odnosu na zemlje digitalne lidere (Čelik, P.2019:61-81).

Prednosti primene IK tehnologija su „ogromne i brojne:

- Brža i učestalija pojava inoviranih usluga i proizvoda višeg nivoa kvaliteta i sa nižom cenom;
- Efikasnije upravljanje poslovnim i partnerskim procesima radi stvaranja vrednosnih lanaca;
- Proširivanje tržišta i lakše sprovođenje vertikalne i horizontalne integracije preduzeća;
- Smanjenje svih troškova elektronskih transakcija i brži povraćaj sredstava uloženi u e-poslovanje;
- Povećanju brzine, efikasnosti i ekonomičnosti rada;
- Nove poslovne mogućnosti bez obzira na lokaciju sedišta kompanije;
- Dvadesetčetvorčasovno radno vreme, 365 dana u godini;
- Povećanje zadovoljstva kupaca i korisnika usluga;
- Velika prilagodljivost i brzina odgovora na zahteve kupaca;
- Ogromne uštede u vremenu i opipljivim resursima; i
- Povećanje ekonomičnosti, produktivnosti i rentabilnosti poslovanja“ (Miletić et. al., 2014:977).

Sveprisutnost inovativnih tehnologija čini motor daljih inovacija za budućnost digitalne ekonomije, najpre tako što podržava savremene vizije budućnosti, kako u domenu sektora energetike, tako i saobraćaja, zdravstva, i sl., kao i transformacije drugih sektora kreativne industrije, proizvodnje, uključujući i sektor finansijskih usluga (Čelik, P.2019:61-81).

Kompanije koje su se opredelile za sopstvenu stratešku opciju primene savremenih digitalnih tehnologija u cilju podizanja nivoa konkurentne prednosti, ostvaruju uvećan nivo profita i više

su okrenute ka korisničkim potrebama, što za rezultat ima i osnaživanje tržišne pozicije i stvaranje poslovnog prestiža.

6. Uticaj digitalizacije na ekonomske efekte - rast produktivnosti i tržište rada i zapošljavanje

Masovna primena digitalnih tehnologija poslednje generacije, unela je suštinske promene i u poslovno okruženje i svakodnevni život ljudi. O efektima i posledicama ovakve disruptivne evolucije, u javnom diskursu i nauci, često se javljaju suprotstavljeni stavovi, počev od onih zasnovanih na potpunom optimizmu u smislu budućih trendova, pa sve do onih koji ističu krajnje problematične strane i razloge za zabrinutost.

Poslovne operacije i svakodnevne aktivnosti ljudi, bezmalo u celosti počivaju na digitalnim tehnologijama. Domen ovih digitalnih tehnologija veoma je širok i počinje od uobičajenih baza podataka i mobilnih servisa, pa preko društvenih mreža, cloud computing-a, big data i sl., pa vodi do interneta stvari, veštačke inteligencije, proširene realnosti, blockchain tehnologije i robotike i dalje do autonomnih vozila, dronova, pametnih kućnih uređaja, itd. Činjenica je, dakle, da digitalizacija predstavlja proces do sada neviđene širine i masovnosti.

Može se reći da su sve sfere života i poslovanja dobile prefiks „e“, bez koga nema ni opstanka kompanije na tržištu, ali ni savremenih formi funkcionisanja čoveka. Automatizacija i integrisani informacioni sistemi za podršku upravljanja postali su sveprisutni, robotizacija velikom brzinom preuzima sve poslove u kojima se obavljaju repetitivne funkcije, menjajući ljude na njima.

Onaj ko se upustio blagovremeno u digitalizaciju, može očekivati efekte poslovanja u smislu uvećane ekonomičnosti i bržeg razvoja proizvoda i usluga. Ovakav trend, kakav forsira „ekonomija mašina“, svakako ima svojih posledica, kako na aktuelnost zanimanja ljudi, tako i ukidanja velikog broja radnih mesta usled automatizacije i robotizovanja proizvodnje i poslovanja uopšte.

Digitalizacija je svoje domete pokazala i u domenu stalnog razvoja i inoviranja servisa za upravljanje gradovima, servisa iz domena komunalnih poslova i usluga pokrivenih projektima pametnih gradova. Digitalizacija poslovanja je svoju primenu pronašla i u optimizaciji javnog saobraćaja, racionalizaciji potrošnje električne energije i vode, pa čak i u domenu evolucije praćenja dešavanja u domenu ekologije.

Ni obrazovanje „nije umaklo“ procesu digitalizacije. Ovim pitanjima bavio se i Svetski ekonomski forum, pa je u izveštaju sa ovog foruma ukazano na puni disruptivni kapacitet ovog tehnološkog razvoja, gde je izneta jedna od krajnje uznemirujućih istina. „Današnji osnovci baviće se zanimanjima koja sada ne postoje, a većinu profesija zameniće mašine i veštačka inteligencija“ (WEF, 2016).

Iako naša država reaguje relativno sporo na ove tendencije, Vlada Republike Srbije je saopštila da će od septembra 2018. godine u svim osnovnim školama u Republici Srbiji biti započeto sa nastavom informatike, jer škole više ne mogu pružiti adekvatno obrazovanje bez nabavke savremene informaciono-komunikacione opreme, tehnologije i infrastrukture.

Svakodnevni život ljudi je povezan i skoro potpuno zavisian od velikog broja digitalnih servisa i uređaja preko kojih se životne potrebe ljudi svakodnevno realizuju. Da bi ljudi efikasno komunicirali sa državnom administracijom, na raspolaganje im je stavljena cela serija servisa sa prefiksom „e“, a to su e-obrazovanje, e-trgovina, e-bankarstvo, e-zdravstvo, e-uprava, itd.

Iako ovi servisi zapravo postoje, javljaju se razlike u njihovoj primeni, u zavisnosti od nivoa razvijenosti određenih sredina u kojima se shvata da se ovde radi o tendencijama koje su neizbežne. Veliki proizvođači aparata i uređaja, godinama unazad proizvode pametne kućne aparate koji se povezuju sa smart phone aplikacijama, a putem kojih uz upotrebu internet infrastrukture, komuniciraju sa svojim vlasnicima i pružaju im obaveštenja o tome šta se događa u njihovim domovima, bilo prijavljujući ili najavljujući početak ili kraj aktivnosti koje su njihovi vlasnici prethodno isprogramirali.

Već 2020. godine, prema nekim najavama, biće delimično ili u značajnijoj meri uvedena 5G mobilna mreža, koja treba da zaokruži (eko)sistem interneta stvari u kome će se posredstvom senzora konačno umrežiti preko 20 milijardi uređaja sa preko 200 miliona „smart“ kućnih aparata. Ljudska domaćinstva se postepeno robotizuju i opremaju smart i high-tech uređajima, što najavljuje promenu, kako u sadržaju života i rada, tako i njegovu dinamiku. Naučno-tehnološki progres definitivno utiče na intelektualni i psihofizički razvoj ljudi. Sve ovo govori da je digitalna transformacija, a samim tim i revolucija, nepovratno promenila i privatni i poslovni aspekt života čoveka.

Ispostavilo se da digitalizaciju poslovanja i njene trendove nedovoljnom brzinom prati zakonska regulativa. Inovacija kao resurs je postala svima dostupna, tako da su današnje poslovne barijere

izuzetno niske, zahvaljujući digitalnoj ekonomiji i internetu kao platformi. Jedinствен je momenat u istoriji da su velika preduzeća iz perioda industrijskog vremena u situaciji da budu ugrožena od strane novih, malih i inovativnih firmi, koje se progresivnim digitalnim idejama i poslovnim inovacijama probijaju na tržištu i zauzimaju svoja mesta. Jedan od razloga za to je i taj, što je put od proizvođača robe ili usluge do njenog kupca bitno skraćen, obzirom da je poslovne akcije i transakcije moguće izvesti trenutno.

Sve navedeno izazvalo je potrebe, ne samo u poslovnoj zajednici, već i u naučnoj i političkoj, a posebno u svetu rada i zapošljavanja i to ne samo u manjem broju nerazvijenih zemalja, već naprotiv i u Evropi i Americi. Digitalna transformacija poslovanja u nekim oblastima pravi disruptivni haos, dok istovremeno u drugim oblastima dovodi do stabilizacije poslovanja.

Novonastala situacija je u javnom diskursu uzrokovala debatu, usled široke tržišne penetracije Ubera na tržište putničkog saobraćaja. Prema određenim poslovnim i naučnim krugovima, ono što je na tržištu učinio Uber predstavlja potpunu liberalizaciju u domenu usluga i proširenje dometa konkurencije i šire, i dalje, i dublje, što je daleko prevazišlo čak i najhrabrija predviđanja predlagača Bolkestein direktive.

Po nekim mišljenjima, ono što je Uber kao digitalna platforma učinio, nazire u neku ruku mogući kraj socijalnog modela zastupljenog u Evropi, obzirom da je Uber model koji je zapravo zaobišao radno zakonodavstvo i propise koji uređuju radno vreme. Raspored radnog vremena je obesmišljen, kao i postojanje kancelarije kao mesta rada. Nema više postupaka za otpuštanje radnika i njihovo zapošljavanje, itd.

Postoji i druga forma mišljenja o navedenom, a to je da je pojava digitalne ekonomije vesnik novih poslovnih mogućnosti, kako u domenu usluga kroz olakšanu pojavu saradničkih projekata u kojima je upotrebnа vrednost sredstava značajnija od vlasništva, tako i u domenu industrije u kojoj će proizvodne linije sve izraženije inteligencije stalno umanjivati vrednost radnika i njihov doprinos, a što će suštinski proizvesti potpuno novi vid saradnje između ljudi i mašina.

Ovakav kontekst stvari iznedrio je nekoliko pitanja na koja je veoma teško dati konkretan odgovor. Kada je u pitanju tržište rada, digitalizacija poslovanja otvorila je sledeća pitanja:

- Da li digitalna ekonomija gasi više poslova nego što ih stvara?
- Postoji li bilo kakav pouzdan način predviđanja njenog krajnjeg ishoda?

Kada je u pitanju status radnika, digitalizacija je otvorila sledeća pitanja:

- Hoćemo li svi postati samozaposleni?
- Da li je ovo kraj rada za zaradu kakav poznajemo ili početak inoviranih fleksibilnih oblika zapošljavanja koji su prilagođeni željama i potrebama samih radnika?

Kada su u pitanju uslovi rada, digitalizacija je otvorila sledeća pitanja:

- Da li će i dalje biti moguće sprovesti propise iz domena rada kojima se ograničava radno vreme, zaštita i bezbednost na radu i kolektivna zaštita radničkih prava?
- Hoće li radna mesta kakva poznajemo i dalje postojati?

Kada je u pitanju područje osposobljavanja radnika, digitalizacija je otvorila sledeća pitanja:

- Da li ćemo svi morati da postanemo informatički inženjeri?
- Koje će sve vidove osposobljavanja radnika zahtevati digitalna industrijska revolucija?
- Da li će se pojaviti nove podele u domenu kategorizacije radnika?

Da bi se mogli makar i okvirno kontekstualno dati odgovori na postavljena pitanja, potrebno je razumeti šta se to dogodilo na tržištu samo nekoliko godina ranije. Naime, 2014. godine, nastala je start-up kompanija Uber. Ova kompanija je za veoma kratko vreme preplavila evropsko tržište prevoza putnika i to posredstvom internet aplikacije za povezivanje putnika i prevoznika. Za samo nekoliko meseci, ovaj poslovni koncept prikazan je kao tehnološki napredak i predstavljen kao simbol američkog poslovnog razvoja, oličen kao Uber. Tržište je bilo „šokirano“ činjenicom da jednostavna mobilna aplikacija putem par algoritama može učiniti da svako može postati taksi prevoznik i to bez ikakvog prethodnog osposobljavanja, bez obaveze plaćanja poreza i doprinosa iz domena obaveznog socijalnog osiguranja i bez drugih regulatornih ograničenja iz oblasti osiguranja, liceniranja, tehničke ispravnosti vozila i sl. To je dovelo do toga da se samozvani „Uber taksisti“ bukvalno kad god to požele mogu nelojalno takmičiti na tržištu sa tradicionalnim taksi kompanijama i pojedincima.

Na ovaj način je celokupni postojeći i decenijama pažljivo regulisani poredak bio srušen jednim krajnje jednostavnim američkim start-up konceptom, koji pritom nema nijedno jedino vozilo registrovano na svoje ime.

Ovaj fenomen se u praksi počeo nazivati i „Uberizacija ekonomije“. Kompanije su od nastanka ovog fenomena razvile specifičan strah da će postati Uberizovane. Od taksista do TV mreža, od

filmskih radnika do restorana i banaka, način na koji fizička lica i kompanije posluju svakodnevno se menja tolikom brzinom da veliki broj kompanija jedva drži korak sa promenama.

Nastanak uberizacije direktna je posledica razvoja interneta i brzih mreža, koncepta Big Data i spajanja posredstvom internet platforme velike količine komercijalnih, ličnih i geografskih podataka i eksplozije potpuno novih oblika mobilnih uređaja koji korisnicima i potrošačima, ali i pružaocima usluga i radnicima omogućavaju pristup brzom mobilnom internetu uvek i svuda.

Poređenja radi, današnji smart phone od nekoliko stotina američkih dolara ima performanse super računara iz 1975. godine, čija je cena bila oko 5 miliona američkih dolara (McKinsey Global Institute, 2013), iz kog razloga se može razumeti kako je došlo do uberizacije tržišta posredstvom mobilnih uređaja.

Navedeni tehnološki trendovi su za samo nekoliko godina, zahvaljujući mrežama, obrisali sve granice i udaljenosti između entiteta, stvarajući tako novu „sirovinu“ - podatke, koje platformne kompanije i start up-ovi mogu direktno i bez posrednika upotrebljavati u poslovne svrhe. Na ovaj način obrisane su i preostale granice između kuće, radnog mesta, ali i mesta na kome se odmara.

Svi uslovi za obavljanje profesionalne aktivnosti su ovim pretransformisani, a ove promene direktno utiču na industriju, intelektualni i fizički rad, radnike i zaposlene u kompanijama, kao i one koji su samozaposleni.

Potpredsednica francuskog nacionalnog saveta za digitalizaciju, Kristin Balag, u avgustu 2015. godine, dala je izjavu za Le Monde i iznela jedno veoma interesantno zapažanje, a to je da svaki čovek koji poseduje mobilni telefon može stvarati i nuditi usluge, odnosno postati „digitalni“ proizvođač (Le Mond, 23.08.2015.).

Digitalizacija je, dakle, stvorila preduslove da svako ko želi uvećati svoje prihode ili zaradu, to može učiniti na ovaj način. Sa druge strane, promenjena je i paradigma vlasništva, jer je uobičajeni format do sada bio takav da se radi o isključivo privatnom vlasništvu nad stanovima, automobilima, kućama, alatima i sl. Ova imovina obično nije bila stalno korišćena i imala je veliki prazan hod u domenu upotrebe, usled čega ovakva imovina za njenog vlasnika više ne predstavlja samo „mrtvi“ kapital koji proizvodi trošak, već kapital koji može biti suprotno od toga upotrebljen da na veliki broj načina doprinese ostvarivanju prihoda.

Ova konceptualizacija otvorila je izuzetno veliki broj pitanja o celokupnom postojećem socijalno-ekonomskom modelu, obzirom da je nagla transformacija u digitalno dovela i do promene statusne paradigme o čoveku kao radniku, o platformi kao poslodavcu, o mestu stvaranja profita, a time i o tome kome se duguju porezi i doprinosi, kako definisati moderni monopol i konkurenciju, šta u tom smislu činiti sa dugo prisutnim i temeljno uređenim socijalnim modelima, te kako možemo posmatrati korišćenje zemlje kao resursa, kako se moramo odnositi prema razvoju, ličnim i kolektivnim pravima, odgovornostima, i sl.

Činjenica je da se „posledice“ digitalne revolucije moraju posmatrati iz svih vizura, jer pored ostalog on-line rad i zapošljavanje koje funkcioniše preko virtuelnih kanala, može proizvesti različite situacije, kao npr. da ljudi koji su zaposleni na slabo plaćenim poslovima, nakon završetka rada kod tih poslodavaca, mogu npr. da ponude svoje preostalo vreme i lično prevozno sredstvo Uberu i ostvare dodatnu zaradu.

Pored toga, nije nemoguća ni situacija iz domena globalnog poslovanja da direktor neke kompanije angažuje svog poslovnog sekretara u zemlji trećeg sveta kako bi mu on „online“ organizovao dnevne aktivnosti i pazio na preuzete obaveze. Tada se otvaraju sva ova prethodno pobrojana pitanja koja je proizveo tzv. “trojac“ sastavljen od pametnog telefona, interneta i big data/AI.

Ovo je bio jedan objektivni prikaz digitalne situacije i bez ulaženja u ostale aspekte disruptivnih tehnologija, kao što su nano tehnologije, napredni materijali, 3D štampa i sl., o kojima je prethodno bilo reči u ovom radu.

Razvoj novih ekonomskih modela, o kojima je takođe bilo reči, temelj su jedne nove ekonomije zasnovane na prethodno pomenutom „trojcu“, međutim, kolika je prava veličina te ekonomije u smislu materijalnih efekata, to najčešće nije zabeleženo u statističkim podacima, a razlog za to je što je digitalna ekonomija 21. veka, tj. ekonomija koja je zasnovana na disruptivnim tehnologijama, veoma različita i od razvoja i primene tehnologija koje su u ranijim periodima suštinski uticale na tržište rada i zapošljavanja.

Priroda fenomena „digitalne robe“ izuzetno je otežala evaluaciju ukupnog efekta digitalne ekonomije na BDP. Iz tog razloga su nastali pravi problemi u praćenju i proceni celokupne vrednosti transakcija nastalih na tehnologiji, kao i stvarni i ukupni učinci ovog digitalnog

fenomena. Svako pliće ili površnije sagledavanje ovih trendova i fenomena ne može doprineti punom razumevanju i sagledavanju ovog problemskog sklopa.

Za razliku od svih ostalih revolucija, tehnologija koja se danas poslovno usvoji, veoma brzo biva integrisana u sve segmente kapitala kompanije, bilo da je u pitanju fizički, intelektualni ili ljudski, usled čega dolazi do stvaranja više vrednosti uz manje ulaganje. Ovakva konstelacija svojim punim disruptivnim potencijalom do iščeznuća istiskuje uobičajene poslovne principe, načine obavljanja poslova i maltene sve ranije primenjivane organizacione pristupe.

Ovakav scenario slaže se i sa principom „destruktivne kreacije“ Jozef-a Schumpeter-a, koja po principu govori da se ovde ne radi o prilagođavanju novim radnim principima i praksama, već o potpunom raskidu sa prethodnim poslovnim modelom, kako bi bilo moguće okrenuti kormilo ka novom poslovnom konceptu u svim njegovim segmentima.

Postalo je više nego jasno da je tehnologija temelj poslovanja organizacije, a da su tehnološke inovacije, u konkretnom slučaju - digitalne, pogon svakog budućeg rasta.

Svedoci smo toga, da se pred našim očima odvija tranzicija, od društva koje je pokretala energija, ka društvu koje je utemeljeno na podacima pohranjenim u informacionim tehnologijama, a koji su zamenili energiju kao pokretačku snagu društva. Ipak, neke dublje stručne analize i posmatranja kažu, da sam Internet kao globalna mreža na koju se povezuju sve stvari i svi uređaji, zapravo uveliko uvećava potrošnju električne energije, a samim tim i broj energetskih izvora iz kojih ta električna energija potiče, što čini da i internet predstavlja uzrok globalnog zagađenja životne sredine. Kako je Internet suštinski pogonjen energijom, pitanje je u kojoj meri se napred izneto stanovište o tome da je nova tehnologija manje opasna po životnu sredinu zapravo promenilo (Gesi, 2012:87).

Digitalna revolucija je obećala tehnološku inteligenciju koja će se ogledati u inteligentnim fabrikama, inteligentnoj organizaciji rada, inteligentnom upravljanju i sl. Sa druge strane, obećanje se proteže na inteligentne gradove, prodavnice, sisteme za proizvodnju energije, a onda i inteligentnu putnu i drugu infrastrukturu i sl. Veliko je pitanje šta se može desiti sa radnom snagom, bilo da je ona fizička ili kancelarijska i u kom domenu će sve to uticati na sektor pružanja usluga. Postavljeno je stoga realno pitanje da li će se radni potencijal radne snage čoveka zapravo svesti na izvršavanje poslovnih zadataka o kojima odlučuju mašine putem algoritama ili će i dalje ostati nekog prostora za vanmašinsku kreativnost čoveka?

Kraj ekonomije zasnovane na vlasništvu nad infrastrukturom kao izvorom vrednosti, učinio je da novi početak bude ekonomija u kojoj vlasnik podataka jeste onaj koji kreira i upravlja vrednošću. Oni koji ovo nisu shvatili, našli su se u prostoru „digitalne opasnosti“ ili još gore na meti „uberizacije“.

Poslovne strategije više nisu strategije, ako nisu koncipirane tako da su u potpunosti pažljivo ukrštene sa stalno širećim digitalnim strategijama, koje su opet pod stalnim pritiskom mrežnih, mobilnih, socijalnih, globalnih i drugih inovacija.

Kompanije su se našle u situaciji, u kojoj, da bi odgovorili na tzv. “stalni tehnološki zemljotres“, moraju ili angažovati, ili proizvoditi menadžere za oblasti primene i kontrole novih digitalnih tehnologija. Ovi menadžeri se usmeravaju, da pored ostalog, isprate raspon razvoja digitalnih strategija, kako bi sa pozicije oficira za vezu između različitih sektora kompanije mogli da sprovedu promene u čitavoj organizaciji. U takvom timu nameću se i nove vrste menadžera i eksperata, pored ostalog, tu su „data miner“, „data analyst“, kao i tzv. “data manager“-i, ali ne samo oni. Ovakva organizaciona struktura služi da kompaniji obezbedi stalno i neometano cirkulisanje poslovnih informacija. Predmetna organizaciona koncepcija zapravo čini da kompanije stoje na informacionim platformama za koje se može reći da su postale pametne fabrike 21. veka (Bauernhansl, 2016).

Tabela br.1. Poslovi u digitalnoj ekonomiji

Poslovi kojima pretil najveći rizik od automatizacije/digitalizacije	Poslovi najmanjeg rizika od automatizacije/digitalizacije	Novi poslovi
Kancelarijski posao i administrativni zadaci Prodaja i trgovina Promet, logistika Prerađivačka industrija Građevinarstvo Finansijske usluge Usluge - prevodenje, poresko savetovanje	Obrazovanje, umetnost i mediji Pravne usluge Upravljanje ljudskim resursima Poslovanje Neki aspekti finansijskih usluga Pružanje zdravstvenih usluga Kompjuterski stručnjaci, inženjeri i naučnici Usluge - socijalni rad, frizer, nega lepote	„Vrh lestvice“ Analitičari podataka, rudari podataka, arhitekta podataka Programeri i radnici za razvoj aplikacija Stručnjaci za umrežavanje, veštačku inteligenciju, itd. Dizajneri i proizvođači novih inteligentnih mašina, robota i 3D printera Stručnjaci za digitalni marketing i e-trgovinu „Dno lestvice“ Digitalni roboti „Golijati“, radnici na nosu i filtriranju podataka i ostali „mehanički Turci“ koji rade na digitalnim platformama Uberovi vozači, povremeni poslovi (popravke, kućne popravke, briga o kućnim ljubimcima, itd) u „kolaborativnoj“ ekonomiji

Izvor: Christophe Degryse (ETUI 2016) na temelju podataka Freya i Osbornea, Forda, Valsamisa, Irani, Heada, Babineta

Prema izveštaju Svetskog ekonomskog foruma (WEF), već do 2020. godine biće ukinuto više od 7 miliona radnih mesta, a otvoriće se novih 2 miliona u 15 vodećih razvijenih zemalja, kao i u zemljama u razvoju (WEForum, 2016:13).

Ovakvo predviđanje jasno ukazuje da će vreme pred nama doneti potrebu za radikalnim restrukturiranjem tržišta rada i zapošljavanja i pojave ogromnog broja tehnoloških viškova u raznim segmentima tržišta rada. Samim tim neminovne su i prateće neizvesne društvene promene posledice. Da li će se tako stvoriti klasa beskorisnih ljudi koji nisu u stanju da se adaptiraju na visoko evolutivnu tehnološku šok terapiju, ostaje da se vidi. Svakako, postojaće veliki broj ljudi koji neće uspeti da se prilagode tome da se njihov život odvija u svetu hiperprodukcije, umreženosti i virtuelnosti.

Takođe, očekuje se tendencija u jačanju trendova u domenu privremenih i povremenih poslova zasnovanih na „freelance“ konceptu, gde će radnici živeti u jednoj državi, raditi u drugoj ili više njih, a zaradu ostvarivati u digitalnim valutama i putem digitalnih novčanika, čime će se neminovno otvoriti sva ona formalno-pravna i socijalna pitanja o kojima je već bilo reči.

Ovaj način neminovno će dovesti do ubrzavanja kada je u pitanju nastanak novih poslova i zanimanja, dok će sa druge strane, izuzetno brzo zastarevati veliki broj zanimanja, pa će mnoga znanja dobiti epitet „obsolete“ (zastareo). Iako postoji intenzivni razvoj brojnih novih poslovnih područja, sasvim je jasno da ona neće biti u stanju da proizvedu stotine miliona novih radnih mesta. Prema Bonciu, analiza studije Banke Engleske iz 2015. godine zaključuje da će u predstojećih 10-20 godina sa tržišta nestati oko 80 miliona poslova samo u SAD, dok će istovremeno u Velikoj Britaniji nestati oko 15 miliona poslova.

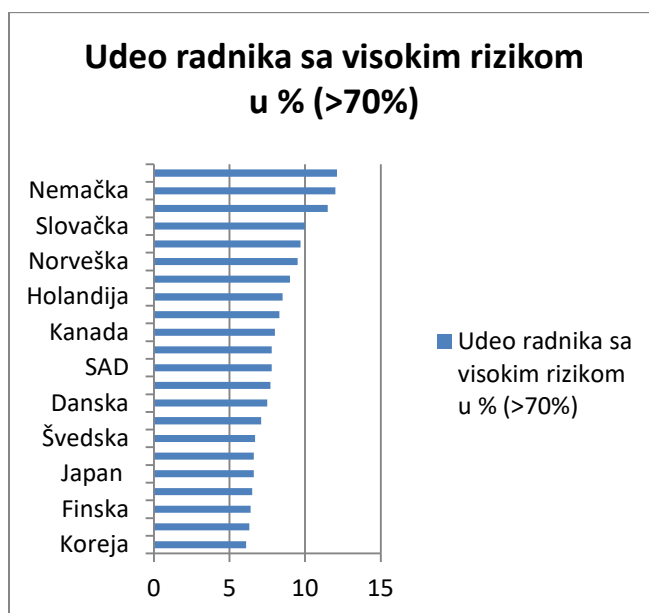
Ono što zabrinjava u ovoj studiji jeste što ove cifre zapravo predstavljaju 50% aktivne radne snage u obe ove razvijene države, iz čega se može razumeti razorni disruptivni potencijal svih ovih promena. Slična predviđanja daje i Svetski ekonomski forum, prema kome će 2020. godine u 15 najrazvijenijih država i zemalja u razvoju nestati ukupno 1,9 milijardi poslova, dok od tog broja barem 5 miliona zbog veštačke inteligencije, robotike, itd.

Izveštaj UNCTAD-a iz 2017. godine, ukazuje da će nerazvijene i srednje razvijene države biti umereno izložene uticaju automatizacije poslovanja, upravo zbog nižih troškova rada i radne snage i nedovoljne dostupnosti primenjenih tehnologija, tj. usled niskog nivoa industrijskog razvoja.

Povećana automatizacija u poslednje vreme pokreće mogućnost kontra trenda u proizvodnom smislu, pa se očekuje masovno preseljavanje proizvodnih delatnosti iz nisko razvijenih u visoko razvijene zemlje, usled čega nastaje opasnost da se na ovaj način približno 2/3 radnih mesta u nerazvijenim zemljama može izgubiti.

Primetan je trend da i visoko razvijene zemlje i zemlje visoke konkurentnosti usled masovne primene robota beleže ili povećanja ili male padove u zapošljavanju u segmentu proizvodnje.

Grafikon br. 17 Udeo radnika pod visokim rizikom od automatizacije u OECD zemljama (%)



Izvor: Arntz, M., T. Gregory and U. Zierahn (2016), „The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis“, OECD Social, Employment and Migration Working Papers, No. 189, OECD Publishing, Paris

Prethodni grafikon prikazuje angažman radnika pod visokim rizikom od implementacije procesa automatizacije, a koji iznosi više od 70%. Istraživači nalazi pokazuju da je najveća stopa rizika evidentirana u Nemačkoj i Austriji, gde je udeo tako zaposlenih 12%, dok je najmanji rizik prema ovim nalazima u Estoniji i Koreji i iznosi 6%. Prema mišljenju autora studije, razlika u stopi rizika od 6% između pomenutih zemalja može biti determinisana drugačijom poslovnom organizacijom, prethodnim tehnološkim investicijama, a može se objasniti i strukturom obrazovanja zaposlenih radnika.

U nastavku, ova analiza potkrepljuje i opšteprihvaćenu pretpostavku manjeg rizika automatizacije kod visokoobrazovanih zaposlenih i zaposlenih koji ostvaruju veći dohodak, dok

najveći rizik od automatizacije preti niskokvalifikovanoj radnoj snazi i radnoj snazi sa nižim ličnim dohotkom. Sve u svemu, kada je uticaj digitalizacije i automatizacije na tržište rada i zapošljavanja u pitanju, mišljenja su i dalje podeljena, pa ni literatura usled toga ne nudi konsenzus po ovom pitanju.

Kako svi podaci govore, nesumnjivo je da digitalizacija donosi rast produktivnosti, dok kod zaposlenosti u tom smislu nije uspostavljen konsenzus. Određena predviđanja idu do toga da povećanje opšteg nivoa digitalizacije za 10% može trajno uvećati stopu rasta GDP-a do 1%.

Ovakvo je i predviđanje Privredne komore Srbije za zemlje zapadnog Balkana. Prema predsedniku PKS Marku Čadežu, istraživanja pokazuju da su mala i srednja preduzeća koja su izabrala internet kanal kao put do svojih potrošača, već u naredne 3 godine od implementiranja ovog koncepta zabeležila rast prodaje za gotovo 25%, za razliku od onih kompanija koje nisu koristile ovaj kanal za plasman svojih roba i usluga.

Poglavlje V: Strateško povezivanje poslovanja i informaciono-digitalnih tehnologija

Vek koji je za nama doneo je intenzivni tehnološki i ekonomski razvoj. Ovakav razvoj događaja u tom periodu, u stručnim krugovima je nametao postavljanje pitanja „Zašto kompanije postoje?“ Među onima koje je ovo pitanje posebno zaintrigiralo, bio je i dobitnik Nobelove nagrade iz oblasti ekonomije, Ronald Koase.

Postavljanje ovakvih pitanja u okvirima razvoja ekonomske teorije i misli ima svoju jasnu ulogu, jer se na tim osnovama javljaju razne inicijative, počev od onih koje na idejnom nivou pokreću i donose promene, pa do onih u okviru kojih se pojavljuje intenzivna primena novih informacionih i srodnih tehnologija. U tom smislu, može se izvesti i jasan odgovor na prethodno postavljeno pitanje, imajući u vidu da isti jasno diferencira stav da kompanije ne postoje radi kontrolisanja troškova poslovanja, već da bi u smislu svoje poslovne misije stvarale novu vrednost, tj. dodatnu vrednost za svoje kupce, vlasnike i akcionare. Ovakav stav izneo je i Peter Drucker, otac posleratne, odnosno moderne teorije upravljanja, koji takođe na ovom stanovištu objašnjava izneto pitanje (Drucker, 1999).

Razvoj ekonomske teorije je postepeno iznedrio i suštinski kompletirao postavljenu tezu o razlozima postojanja kompanija, pa su se prethodni stavovi, koji su svakako tačni, dalje izdiferencirali i ka tome da je suština poslovanja kompanije zapravo zadovoljavanje potreba njenih korisnika usluga i kupaca, što dalje dovodi do neophodnosti razumevanja tih potreba. Ovakav kontekst kreira kompanijsko iskustvo, koje je resurs koji omogućava stvaranje tih novih vrednosti u lancu.

Vrednost koju na tržištu stvaraju kompanije, nije vrednost koja nastaje samo za kompaniju, već je to ono što kompanija stvara za svoje kupce, shodno pravilu zakona konkurentnosti, a što mora biti takvo da i kupcima i potrošačima donosi veću vrednost od uloženog iznosa. Ta vrednost, kao vrednost oportunitetnog troška za potrošača, i u subjektivnom, i u objektivnom smislu mora biti veća, ili treba biti veća od one vrednosti koju ti kupci ili potrošači za isti iznos, odnosno ulaganje mogu ostvariti u odnosu na konkurentske ponude.

Pored toga, ne smeju se zaboraviti ni paradoksi koje navedeni koncept stvara, ako se ima u vidu da isti princip stvaranja vrednosti za kompaniju, istovremeno očekuju i njeni vlasnici i akcionari, obzirom da je to i njihov razlog ulaganja u kompaniju. Očekivanje vlasnika i akcionara kompanije je da se vrednost koju proizvodi kompanija putem njihovog investicionog ulaganja

(za proizvodnju proizvoda i usluga namenjenih potrošačima) mora takođe stalno uvećavati, a time i njihova neto dobit u odnosu na ova ulaganja.

U tom smislu, postojanje i egzistiranje kompanija na tržištu, kao i uloga kakvu pritom ima menadžment kompanije, nikome ne ostavlja lak zadatak, upravo usled ove suštinske konfrontacije koncepata, obzirom da se uvek mora ponuditi više i više novih vrednosti po sve nižoj i nižoj ceni za kupce, uz istovremeno neprekidno zahtevanje sticanja sve veće dobiti za kompaniju, vlasnike i akcionare.

Imajući u vidu da se ovde radi o imperativima koji drže spregu između poslovanja, dobiti i konkurentnosti na tržištu, sa ciljem pomirenja ovih suprotstavljenosti, morao je nastati čitav niz temeljnih promena i u samom poslovanju kao generalnoj kategoriji. Usled navedenog, kompanije su počele da shvataju da su se našle na turbulentnim ekonomskim i tržišnim prostorima, pa ako žele opstati, one se moraju prilagoditi i poslovati u tim turbulentnim tržišnim uslovima, jer više nema mesta tome da se kompanije oslanjaju na tradicionalne modalitete, bilo u smislu samog poslovanja, bilo u smislu stvaranja novih vrednosti.

Kako bi kompanije mogle postići ono što od njih tržište i uslovi postojanja zahtevaju, one se moraju okrenuti i ići u susret raznim izazovima, kao što su stalno rastuća dinamika tržišta i konstantni tehnološki razvoj i napredak, gde će kompanije, prateći međusobno zavisnu tržišnu dinamiku i tehnološki napredak, u svoj rast i razvoj stalno uključivati primenjiva savremena dostignuća zbog stalno rastuće potrebe unapređenja postojećih modela poslovanja. Kompanije bi u tom smislu, na osnovu dubokih analiza, morale zaključiti da li postojeći modeli poslovanja mogu ili ne mogu odgovoriti dinamici tržišta, kao bi se opredelile za odgovarajuće metode istraživanja i razvoja, radi stvaranja novih poslovnih modela, a čija je suština prilagođena prilikama tržišnog okruženja i njegove dinamike. Usled ovih turbulencija, savremeno poslovno okruženje postaje izloženo uticaju nebrojenih činilaca koji zadiru u sve sfere poslovanja, društva i okruženja kao celine.

Radi opstanka na tržištu, česte i neočekivane promene prilika, pred kompanije postavljaju nove izazove koji zahtevaju njihovu spremnost da brzo, i sve brže odgovaraju na izazove, probleme i prilike koje kreira dinamično, čak turbulentno konkurentsko okruženje. Bez obzira na to, i kompanijama koje drže korak sa promenama i tržištem, budućnost donosi ubrzanje, neizvesnosti i dinamiku konkurentskog okruženja za uspešnost budućeg poslovanja, imajući u vidu da

stvaranje novih vrednosti u budućnosti, skoro bez izuzetka podrazumeva upotrebu raznih digitalnih tehnologija u kombinaciji sa svim drugim poslovnim resursima.

Usled toga, kompanije se distanciraju od svojih tradicionalnih i generičkih poslovnih aktivnosti i modela i okreću inovativnim konceptima, disruptivnim inovacijama i tehnologijama koje su u stanju odgovoriti potrebama i željama kupaca i potrošača. Ovakvi iznuđeni izbori vrše se uz povećanje obima i kvaliteta usluga koje se pružaju krajnjim korisnicima, ali i uz neizvesnosti koje takav iskorak donosi.

Iz navedenog se jasno može utvrditi potreba za strateškim usmerenjem poslovanja kompanije, koje kao takvo ne može izostaviti segment strateškog planiranja i razvoja informacionih sistema, a u sklopu toga i svih pratećih aktivnosti koje kompanije prevode na prostor digitalne transformacije poslovanja.

Kako intenzivna primena digitalnih tehnologija i naprednih informacionih sistema, kao podrške kompanijskom poslovanju mogu doneti i trenutne i strateške koristi i doprineti pozicioniranju u odnosu na konkurenciju, ovi resursi moraju biti stavljeni u funkciju neposredne podrške i ostvarivanja ovako strateški postavljenih ciljeva poslovanja.

Imajući u vidu da digitalna tehnologija i savremeni informacioni sistemi direktno utiču na konkurentnost poslovanja, u tome se mogu izdvojiti parametri iz kojih proističe njihov suštinski uticaj na ukupnu operativnu poslovnu efikasnost. To dovodi do toga da takva strategija poslovanja počiva na principu niskih i kontrolisanih troškova, što samo po sebi ima evolutivni karakter, koji, kao takav, u slučaju uspostavljanja određenih okolnosti u kompaniji i na tržištu, postaje pokretač stalne poslovne inovativnosti i promena. Time se vrši ili uspostavlja jasna strategija tržišnog razlikovanja kompanija i njihovog stalnog diferenciranja u smislu i forme i sadržaja poslovanja i poslovne aktivnosti.

1. Sinergija informacionih tehnologija i poslovanja

Područje informacionih sistema i informacionih tehnologija, suštinski predstavlja nezahvalnu oblast za obradu, a sa druge strane izuzetno potrebnu, čak i neizbežnu za izučavanje. Glavni razlog za to je činjenica da skoro da ne postoji grana savremene naučne discipline koja je toliko propulzivna, da je njen razvoj, razmera, inovativna sposobnost, terminološko područje pa i tema delatnosti, kao i kontekst daljeg razvoja, bezmalo sveukupno neodrediv.

Često se iz ovih razloga dešava da informatičko neznanje, nerazumevanje i neupućenost dovode do toga da se informatika kao oblast posmatra striktno iz tehničke vizure i time kao pozadina svih delatnosti i poslovnih procesa kompanije. Posmatranje ove propulzivne oblasti na takav način, kao segmenta bez bitnijih uticaja u savremenom poslovanju, često dovodi do toga da se i među samim stručnjacima iz pojedinih oblasti pojavljuju razlike u posmatranju ovog fenomena, tj. da li bi informatika trebalo da bude isključivo usmerena na opise pojedinih alata, tehnologija, softvera i slično, ili nešto što suštinski prožima svaki vid savremenog poslovanja i čini njegovu apsolutnu potporu.

Posledično, razvile su se oblasti kao što su primenjena informatika i informatika u poslovanju, te kasnije i drugi segmenti koji najavljuju nastajanje i intenziviranje dubljeg razumevanja informatike kao nosioca digitalne transformacije poslovanja. Ovo logičko-kontekstualno povezivanje dalo je prostora za razumevanje sveukupnog strateškog prožimanja poslovanja i informaciono-digitalnih tehnologija, koje već daje efekte, upravo kroz proces sinergije informacionih tehnologija i opšteg poslovanja radi ostvarivanja svrhe egzistiranja kompanije kao tržišnog entiteta i ekonomskog subjekta od velikog značaja za društvenu i socijalnu dobrobit.

1.1 Prednosti i očekivanja

Činjenica je da informacione tehnologije kao sredstvo digitalnog razvoja poslovanja daju jasna očekivanja u smislu prednosti kod svih onih koji su zakoračili u na njima zasnovane procese poslovne transformacije i shodne implementacije, ali i razvoja pratećih informacionih sistema, kao krvotoka i nervnog sistema takve poslovne transformacije.

Dosledna primena informatike u poslovanju podrazumeva stalno praćenje promena, kako informatike kao struke, tako i multidisciplinarnih pristupa. Imajući u vidu da je jedino tako moguće odgovoriti na potrebu da se sistematično izuče, razjasne i približe svi ovi sadržaji kao deo šireg konteksta sagledavanja, moguće je razumeti da nema digitalne ekonomije bez podrške informacionih sistema koji joj daju kontekstualno okruženje.

Kao što ne postoje dva ista i jednaka čoveka, tako ne postoje ni dva potpuno jednaka, odnosno istovetna informaciona sistema, niti dva potpuno ista načina i sistema njihove primene. Ovakav zaključak proističe iz toga što se najveći izvor dodatne vrednosti u okviru digitalne ekonomije suštinski krije u inventivnom osmišljavanju i uspostavljanju suptilnih formi poslovne funkcije ovih sistema, ali takođe i suptilnih zaštitnih mehanizama i mera koji su autorski proizvod

jedinstvene ljudske pameti, a ne plod rutinske primene tehnologije algoritma, koja bi i sama po sebi organizovana u određenu infrastrukturu tako funkcionisala. Na ovaj način postaje jasno zašto određena tehnologija, čak i kada je povezana u istovetnu arhitekturnu infrastrukturu, svoj kvalitet ili nekvalitet pokazuje tek kroz ukupni kvalitet organizacionih i drugih resursnih mera, kao temelja poslovne osnove. Ta osnova samim tim mora biti potpuno specifična i za određeno poslovno okruženje projektovana, kao i sve ostale relevantne poslovne politike.

Čak iako bi određene informacione tehnologije i njihova struktura i arhitektura bile preslikane na neko drugo, veoma slično poslovno okruženje, one ne bi davale iste poslovno-tehničke rezultate, a samim tim ni jednak nivo bezbednosti. Iz toga može izvući zaključak da ne postoje dva jednaka informaciona sistema, ni po implementiranom nivou zaštite.

Istovremeno, ovaj kontekst dovodi do zaključka, da niti postoje, niti su postojali, pa samim tim ni u budućnosti neće postojati potpuno sigurni informacioni sistemi, iz kog razloga na ovaj izazov mogu odgovoriti isključivo multidisciplinarni pristupi i kompleksni načini holističkog modela upravljanja bezbednošću, jer će samo sistemi, uspostavljeni na ovim postulatima biti sposobni da stvaraju i iskoriste ukupnu sinergiju postojećih tehničko-tehnoloških, organizaciono-upravljačkih, fizičkih, društvenih i sličnih oblika zahteva i kontrola, a koji samo tako i pod tim uslovima mogu činiti, s jedne strane ekonomski opravdan, a sa druge strane, poslovno efikasan sistem zaštitnih mera u kontekstu digitalne transformacije poslovanja i njenih pratećih bezbednosnih implikacija.

2. Uticaj informacionih sistema na proizvodnu efikasnost poslovanja

Uticaj informacionih sistema na proizvodnu efikasnost uvek podrazumeva vizionarske koncepte i scenarije poslovne primene digitalnih tehnologija, usled čega samo sveobuhvatno posmatranje ovog resursa može uočiti nove horizonte i uspostaviti jasnije razumevanje digitalnog ekonomskog okruženja u kome svakodnevno živimo i radimo.

Savremeno poslovno okruženje podrazumeva i savremeno tehnološko okruženje, bez koga više nije moguće ni zamisliti, a kamoli razvijati poslovnu ili privatnu svakodnevicu. Bez obzira na postojeći nivo tehnološkog razvoja, u svakom poslovnom segmentu predstoji sveobuhvatna i intenzivna primena potpuno novih digitalnih i transformativnih tehnologija, koje će kao takve, nepovratno transformisati i naše životne i poslovne navike, sa jedne strane učiniti život i

poslovanje lakšim, bržim i efikasnijim, a sa druge strane pojedinca i privredu izložiti sve novijim i sve brojnijim sajber rizicima.

Na ovaj način nastao je veliki pritisak novih tehnologija na poslovanje, a samim tim i pritisak kompanija i pojedinaca koji te tehnologije razvijaju na celokupno okruženje, pa se u tom pravcu konstantno razvijaju razni scenariji primene takvih tehnologija. Međutim, ove inspirativne, čak i vizionarske poduhvate, treba sagledati i kroz kritičku prizmu i prostor njihove bezbednosti, te izlaganja svih modela rada i upravljanja sve inovativnijim rizicima od sajber kriminala, koji uz svaku dozu benefita, digitalizacije života i poslovanja, zahtevaju osmišljavanje i implementiranje raznovrsnih inovativnih metoda za rano otkrivanje i sprečavanje prevara i rizika koje masovne informacione tehnologije iz talasa u talas donose u sajber okruženje i sajber prostor.

Iz opisanog konteksta se vidi da ne postoji samo jedna strana ove medalje, već svako „zašto“ ima svoje „zato“, kao što i svaki „input“ ima svoj „output“ i time i oportunitetni trošak.

Širi kontekst i primeri iz prakse, kao i svi inovativni pristupi, uvek podrazumevaju metodički koncept koji inovativno poslovno okruženje i digitalnu transformaciju poslovanja mora držati u zoni najvišeg stepena operativne efikasnosti u poslovanju i kod korisnika tehnologija konstantno poboljšavati kompetencije u ovom području, jer operativna efikasnost poslovanja, koja donosi veći obim, promet i prihod, uvek podrazumeva i potrebu za većim stepenom digitalne i sajber bezbednosti, koji opet ne sme ni u kom slučaju iskazati ni manjak sposobnosti, ni manjak kompetencija u bilo kojoj sferi multidisciplinarnog pogleda na benefite i rizike digitalnog koncepta poslovanja.

U tom smislu, vođenje poslova u uslovima digitalne ekonomije i disruptivne transformacije kroz korišćenje savremenih informacionih i digitalnih tehnologija, jeste zapravo budućnost koja je već počela, pa će njeni postulati i uticaji na operativnu poslovnu efikasnost stajati u direktnoj međuzavisnosti sa oblastima sajber bezbednosti, opšte bezbednosti, kontrole i revizije informacionih sistema itd., imajući u vidu da se ovde ne radi o trendovskom kapacitetu, već o nečemu što je i sada, i ovde sa tendencijom da tu i ostane.

3. Informacioni sistemi kao generator inovativnosti u poslovanju

U savremenom poslovnom dobu, ispostavila se činjenica da je digitalna tehnologija, globalno posmatrano, jedan integralni deo savremenih informacionih sistema. Digitalna tehnologija kao

takva, u domenu svoje funkcije, čini onaj deo savremenog poslovnog informacionog sistema koji se koristi radi automatizacije poslovnih procesa i njihovog ubrzanja, a što za svoje ciljano ishodište ima umanjenje ukupnih troškova poslovanja. Iz toga se može razumeti da ovako postavljeni savremeni informacioni sistemi po svojoj ekonomskoj vokaciji, čine temelje implementiranih delova strategije niskih troškova u poslovanju kompanije. Ovakve postavke se mogu bliže prikazati i kroz svakodnevne primere poslovanja sa kojima potrošači i korisnici usluga imaju kontinuiranu interakciju.

U tom smislu treba istaći i neke pojedinačne primere koji potvrđuju pomenuta pravila.

Na primer, trošak pojedinačne transakcije koja se ostvaruje posredstvom e-bankinga za banku predstavlja 100 puta manji trošak, nego ako bi se takva transakcija izvršila na tradicionalni način, tj. putem šaltera i šalterskog službenika. Isto tako, trošak rezervacije mesta kod vazduhoplovne kompanije, koja se vrši u on-line postupku putem interneta bar je 7 puta jeftinija, nego ukoliko bi se rezervacija vršila na klasičan način.

Primer koji označava fascinantnost primene strategije niskih troškova kompanije i njenu efikasnost i efektivnost, mogao bi nam dati prikaz efekata u ovoj oblasti kakav ima informacioni sistem logističke kompanije Fedex, koji je u stanju da na dnevnom nivou obradi više od 100.000.000 elektronskih transakcija. Ukoliko bi se ovakva i ovako obimna aktivnost vršila na tradicionalan način i isključivo u formi papira, odnosno samo putem ljudskog rada i komunikacije, jasno je da najpre ovo ne bi bilo moguće, dok bi sa druge strane postignuti nivo aktivnosti bio znatno, čak drastično skuplji.

Činjenica je da su ovakvi informacioni sistemi i digitalne tehnologije kroz svoje sinergetsko delovanje u poslovanju iznedrile brojne sisteme koje danas koriste i vazduhoplovne kompanije, a koje posredstvom ovih i ovakvih sistema mogu izvršiti na desetine miliona promena cena mesečno, raditi sa stotinama hiljada pozicija kupaca, razmenjivati na hiljade poslovnih poruka u sekundi, obrađivati na hiljade transakcija u sekundi i sve to uz vreme odziva u manje od dve sekunde, bez obzira na deo sveta iz koga se transakcija potencira.

Iz ovih primera se vidi, da savremeni informacioni sistemi i digitalne tehnologije čine okosnicu modernog globalnog poslovanja, pa je postalo nemoguće i zamisliti odvijanje masovnih poslovnih procesa bez stalne podrške ovih sistema, jer ovakvi sistemi predstavljaju i temeljnu i ključnu infrastrukturu modernog poslovanja. Ova infrastruktura omogućava brzo, tačno i

pouzdana obavljanje širokog spektra transakcija, a time i efikasno implementiranje svih poslovnih strategija kompanija, bez obzira na sektor.

Činjenica da se putem savremenih informacionih sistema danas odvijaju skoro sve važne poslovne transakcije i aktivnosti, a da informacioni sistemi pohranjuju, evidentiraju i obrađuju sve rezultate rada. Analitički kapaciteti ovih sistema daju mogućnosti onima koji donose odluke da imaju stalni nadzor u sprovođenju svake poslovne aktivnosti i mogućnost da posredstvom analitike utiču na kvalitet i efikasnost sprovođenja svih poslovnih aktivnosti i strategije.

Digitalne tehnologije i savremeni informacioni sistemi bez sumnje predstavljaju interaktivnog činioca svake razvojne strategije i svih inovativnih poslovnih modela, a uz sve to i jednog od nosilaca svih nastojanja diferencijacije i uspostavljanja posebnosti poslovnog modela kompanije na tržištu. Takve inovacije daju podsticajni karakter sve radikalnijim poslovnim promenama, koje usled konstantnog inoviranja poslovnih modela, iznova nameću sve novija i efikasnija pravila u odvijanju poslovnih procesa, a koja kao takva, za veoma kratko vreme bivaju nametnuta kao novi poslovni standard.

Primeri takvih inovativnih poslovnih modela vidljivi su svuda oko nas, te u tom kontekstu treba najpre pomenuti kompanije kao što su Amazon, Google, YouTube, Uber i sl.

Ovakve tehnologije čine najbolje primere disruptivnih inovacija zasnovanih na primeni digitalnih tehnologija u savremenim informacionim sistemima, usled kojih se u celosti menjaju, ne samo poslovni modeli u svim industrijskim granama, već i očekivanja i ponašanja kupaca i korisnika usluga koje su ovako nastale. I u ovom segmentu, primeri se mogu pronaći svuda oko nas.

Tako, vazduhoplovna industrija već duži niz godina funkcioniše „on-line“ i putem interneta vrši prijave za let, „on-line“ prodaje elektronske prevozne karte, pruža „on-line“ usluge mobilnog „check-in“-a, itd. Avioni kompanije Boeing snabdeveni su informacionim sistemima zasnovanim na Google glas tehnologiji, čiji je osnovni zadatak brzo lociranje kvarova.

Sa druge strane, vazduhoplovna kompanija United Airlines omogućava svojim korisnicima i korisnicima Apple uređaja da već na samom ulasku u avion mogu preuzeti na svoje uređaje sav postojeći zabavni sadržaj kako bi ga mogli koristiti tokom leta. Ovakav trend razvoja će sasvim sigurno dovesti do toga da fiksni i mobilni uređaji za zabavu ugrađeni u avione postanu zastareli i nepotrebni.

Maloprodaja širom sveta, već duže vreme poseduje mogućnost praćenja proizvoda putem RFID tehnologije⁶ i drugih srodnih tehnologija za označavanje proizvoda, usled čega ove tehnologije imaju efekta na praćenje svih poslovnih procesa, počev od same prodaje, do upravljanja zalihama tih proizvoda. Iz navedenih razloga, ove tehnologije postale su standard kod najvećih poslovnih lanaca koji se bave maloprodajom.

Walmart, koji je inače jedan od najvećih svetskih maloprodajnih lanaca, elektronski je označio veliki broj maloprodajnih artikala u svojoj mreži, a sve kako bi primenom tehnologije mogao u svako doba izvršiti analizu poslovanja i izvršiti instant popis robe na zalihama kao i popis prodate robe, dok koncept „Future stores“ omogućava kupovinu i prodaju bez blagajni i prodavaca, što ujedno predstavlja i najnoviji retail biznis koncept.

Interesantno je pomenuti da se razvoj digitalnih maloprodajnih tehnologija ne završava samo na ovome. Kompanija Tesco, jedan od vodećih britanskih maloprodajnih lanaca, izuzetno je posvećena intenzivnoj primeni savremenih informacionih sistema zasnovanih na digitalnim tehnologijama, kako bi konstantno inovirali svoj „retail“ poslovni model.⁷ U njihovom konceptu svi proizvodi su označeni RFID tehnologijom, a ova tehnologija je u stalnom kontaktu sa pametnim softverom kome se proizvodi neprekidno javljaju i razmenjuju podatke o tome gde se tačno nalaze. Sistem automatskih promena i nivelisanja cena sprovodi se automatizovano kroz informacioni sistem za digitalne cene. Ovaj informacioni sistem je u stanju da izvrši promenu u nivelisanju cena za više miliona artikala za samo nekoliko sekundi usled stalne analize ponude i potražnje za njima.

Sistem digitalnih kamera u maloprodajnim objektima uspostavljen je i organizovan radi konstantnog praćenja količina artikala, pa ovaj sistem ustrojen da prati i to da li je došlo do nestašice nekog od artikala, a ukoliko je do toga došlo, inteligentni softver za kontrolu zaliha robe odmah angažuje zaposlene da obnove ovu zalihu. Ovaj softver je takođe opremljen mogućnošću praćenja, ne samo količine, već i svežine zaliha, o čemu takođe automatski upozorava zaposlene u lancu odgovornosti.

⁶ RFID (engl. Radio Frequency Identification Device) predstavlja računarski čip koji radio frekvencijom može u svoju okolinu periodično (npr. na svakih 30 sekundi) slati podatke koji su na njemu pohranjeni. To mogu biti razni podaci o proizvodu koji je opremljen takvim čipom, poput matičnih podataka, stanja zaliha, roka trajanja robe, itd.

⁷ Video link: Retail Innovation trends compilation https://www.youtube.com/watch?v=mxAKS07_rpo i In-Store IT-induced innovations in TESCO <https://www.youtube.com/watch?v=noa4SmYhjTA>

Ova tehnologija je dovela i do još jednog inovativnog servisa, gde kupac preko terminala, kao interaktivne prodavnice, može kupiti određenu robu „online“ i preuzeti je na destinaciji na koju se uputio preko povezane avio kompanije, pa će sistem obezbediti preuzimanje robe ili namirnica na mestu destinacije, a ne mestu trgovine.

Tendencija je u poslednje vreme da se maloprodajni lanci širom sveta intenzivno interesuju, investiraju i pripremaju za primene još novijih i modernijih tehnologija zasnovanih na veštačkoj inteligenciji i proširenoj stvarnosti, a koje se već sada konceptualno integrišu u poslovne modele ovih kompanija.

U oblasti finansijskih usluga došlo je do izuzetno brzog razvoja sistema za mobilna plaćanja, pa danas nije nikakva novina da se finansijske transakcije i plaćanja vrše putem mobilnih telefona. U tom smislu treba izdvojiti već ustaljene usluge plaćanja parkinga putem mobilnog telefona, kao uobičajenu stvar. Na ovim osnovama su razvijene usluge m-parking i usluge m-plaćanja.

U smislu prepoznavanja sadržaja dokumenata i formulara, razvijene su i usluge kao što je Photo-Pay. Ova usluga je osmišljena tako da nakon fotografisanja određenog formulara, softver pristupa automatskom popunjavanju naloga za plaćanje i do kraja sprovodi automatizovanu proceduru. Razvojem ovih tehnologija i na njima zasnovanih usluga, obim finansijskih plaćanja učinjenih na ovaj i slične načine, nekoliko godina unazad uveliko prevazilazi hiljadu milijardi američkih dolara, iz čega je moguće uočiti njihov ukupni poslovni potencijal.

Da bi ovakve usluge bile moguće, razvijene su i usluge transfera mobilnog novca.

Interesantno je primetiti da je još 2013. godine u vodećem svetskom ekonomskom časopisu Economist objavljen tekst u kome se Kenija predstavlja kao vodeća zemlja u razvoju i implementaciji usluga sa mobilnim novcem. Kada je u pitanju ova usluga, najpre se misli na mPesa uslugu, koja svojim korisnicima omogućava da sve bankarske poslove obavljaju van banke i putem pametnih telefona preko kojih telekomunikacione kompanije omogućavaju jednostavan, brz i jeftin transfer novca u sve krajeve sveta.

Interesantno je napomenuti da je ovakva usluga, odnosno servis, uspostavljen usled velikih radnih migracija u Africi, gde veliki broj ljudi iz ruralnih krajeva odlazi na rad u velike afričke gradove, usled čega im je ovakav servis neophodan kako bi novac koji zarade u velikim

gradovima mogli transferisati svojim porodicama u ruralnim krajevima, ili vršiti sve ostale vrste transakcija i prenosa novca bez obzira gde se nalazili.

Ovakvi trendovi nisu ostali bez efekta ni u severnoj Evropi, tj. u skandinavskim zemljama. U ovim zemljama je sistem bezgotovinskog plaćanja već dugi niz godina uobičajeni standard, pa iz ovih razloga skandinavske zemlje razmatraju i implementaciju ideje i formalnog ukidanja gotovinskog plaćanja, imajući u vidu da je već neko vreme preko 95% svih transakcija zapravo izvršeno bezgotovinskim putem, jer se transakcije uglavnom vrše putem elektronskih i mobilnih sredstava plaćanja, iz kog razloga je, na primer, u Danskoj od početka 2016. godine, u skladu sa ovim tendencijama, donet čak i zakon da trgovci nemaju obavezu da primaju gotovinu kao sredstvo plaćanja prilikom prodaje roba i usluga.

Ovakve digitalne i elektronske tendencije dovele su i do decentralizovanih digitalnih valuta, odnosno, valuta koje nisu pod kontrolom monetarnih vlasti, odnosno nisu u vlasti centralnih banaka država. Uspostavljanje ovakvog digitalnog decentralizovanog, u suštini paralelnog valutnog sistema, predstavlja suštinsku digitalno-finansijsku revoluciju, kako u smislu vrednovanja valuta, tako i u smislu načina plaćanja, iz kog razloga se ove digitalne valute sve više koriste i kao sredstvo trgovine i prikazivanja finansijskih izveštaja.

Od digitalnih valuta, najviše se izdvojio Bitcoin, koji je, imajući u vidu mogućnost i anonimnih transakcija, postao najčešće transakciono sredstvo i u legalnoj, i nelegalnoj trgovini. Uprvo radi transparentnosti u finansijskim i drugim poslovnim transakcijama, osmišljena je i implementirana Blockchain tehnologija, koja tek donekle daje rezultate u praćenju transakcija.

Potrebno je razmisliti i o mogućnosti koja može proisteći iz ovakve konstelacije stvari, a to je da digitalna transformacija poslovanja suštinski vodi ka tome da svet može ostati bez optičaja fizičkog novca, a da će šuma digitalnih valuta u nekom trenutku možda dovesti do toga da će se izdiferencirati samo jedna digitalna valuta koju će koristiti ceo svet.

Najzastupljenije digitalne valute u ovom trenutku su Bitcoin, Ethereum, Monero, Litecoin, Zcash, Decred, Namecoin, DASH, Ripple, LBRY i za ove valute širom sveta postoji čak i veliki broj menjačnica i bankomata na kojima se ove digitalne valute mogu konvertovati u zvanične valute država i njihovih centralnih monetarnih vlasti.

Digitalna transformacija poslovanja u svakom smislu izuzetno utiče na trendove u savremenim plaćanjima. Takve trendove su bez sumnje prepoznale brojne tehnološke kompanije i u tom smislu razvile ponudu sopstvenih proizvoda i tehnologiju za vršenje usluga digitalnog platnog prometa. U tom smislu su u ovom tržišnom segmentu započela veoma ozbiljna konkurentska nastojanja pa kompanije poput PayPal, Stripe, Square, ApplePay, GoogleWallet, SamsungPay, itd. iskazuju tendenciju da prošire i nametnu sopstvene tehnologije i rešenja i da kroz njih probaju osigurati da njihova rešenja postanu opšteprihvaćena i svuda implementirana.

Na ovom tržištu se konstantno pojavljuju brojni novi „igrači“ koji pokušavaju „progurati“ na tržište svoje inovativne digitalne platforme za prenos novca, plaćanje i mikrofinansiranje, čime se broj digitalnih proizvoda i usluga drastično i inovativno uvećava na ovom polju.

Istovremeno, pojavljuju se i servisi digitalnih interaktivnih kreditnih kartica koje objedinjuju sve fizičke kartice i sve do sada standardne načine plaćanja kako bi se dodatno osnažilo plaćanje prenosnim uređajima sa kojih će se moći čitati finansijske informacije i vršiti transakcije. U ovoj oblasti izuzetno je angažovan Mastercard koji stupa u strateška partnerstva sa kompanijama koje nude usluge digitalnih platformi, pa je trend razvoja ovih tehnologija takav, da se kreće ka masovnoj upotrebi biometrijskih autorizacija plaćanja, čak i na bazi selfi-ja, do koje ideje se došlo prepoznavanjem sve većih mogućnosti i konektivnosti pametnih telefona i uređaja koji su već izvesno vreme u stanju da vrše skeniranje i autorizovanje putem jedinstvenih biometrijskih karakteristika korisnika ovih uređaja.

Ovakvi tehnološko-razvojni potencijali nesumnjivo donose jedan „tehnološki nedogled“ koji proizvodi brojne distruptivne inovacije, kao uopšte, tako i u oblasti finansija, pa iz njih nastaju nove mogućnosti pozajmljivanja i kreditiranja, sve do mikrofinansiranja, iz čega je proizašla nova ekonomska kategorija nazvana „ekonomija deljenja“ čiji je tipičan primer Lending Club (Mandelbaum, 2015).

U oblasti proizvodnje automobila i oblasti javnog prevoza, takođe je došlo do izuzetno visokog stepena kooperacije, a posebno između proizvođača vozila i tehnoloških i telekomunikacionih kompanija koje u ovoj oblasti predstavljaju vodeće faktore razvoja tehnologije. Ovakva kooperacija dovela je do zajedničkog projektovanja proizvoda i usluga sa proizvođačima automobila, pa se pametne tehnologije više ne ugrađuju samo na nivou automobila kao sistema, već se razvijaju tehnologije, ne samo za vozila, već i za njegove elemente (na primer tehnologije

kompatibilne sa ostalim naprednim sistemima u javnom transportu). Ovakve tehnologije podrazumevaju i pametnu javnu infrastrukturu, kako bi svi ovi činioци proizveli sinergetsko okruženje u kome će vozila biti, ne samo prevozno sredstvo, već i deo sistema pametne infrastrukture koja će moći ostvarivati međusobnu komunikaciju i interakciju, a sve sa ciljem da se saobraćaj može odvijati u većem obimu, efikasnije i sigurnije i uz proizvodnju velike količine podataka koji će služiti za naprednu analitiku i donošenje budućih odluka i razvojnih strategija, kako na nivou vlada, tako i kompanija pružaoca ovih inteligentnih usluga.

Domete u segmentu ove tehnologije prikazuju kompanije Google, Volvo i Tesla, a njima se polako pridružuju i proizvođači automobila kakvi su Audi i dr., imajući u vidu da niko od velikih igrača ne želi da ispadne iz tržišne trke na ovom polju. U okviru testiranja ovih i ovakvih tehnologija, za sada je najbolje rezultate postigao „Google Car“ koji je uspeo preći preko 500 miliona kilometara bez bilo kakvog saobraćajnog akcidenta.

Sa druge strane, kompanija Volvo, kao tradicionalno inovativna kompanija u automobilskoj industriji, namerava proizvesti automobil u koji će biti implementirana pametna tehnologija koja treba da omogući da u Volvo automobilima više niko ne pogine, a da su takva očekivanja kompanije zasnovana na softveru koji je koncipiran tako da posredstvom njega automobil „odbija“ da se sudari.

Kompanija Tesla takođe radi na ovakvim projektima, međutim, sa manje uspeha, imajući u vidu da je njihov automobil doveo do jednog fatalnog ishoda sa ljudskom žrtvom, tako što je softver pametnog automobila imao propust koji je doveo do sudara automobila sa kamionom.

Kupci skupocenih Audi modela u okviru „dodatne opreme“ imaju na raspolaganju aplikaciju za samostalno parkiranje vozila, kao i softver za komunikaciju sa umreženim javnim garažama, onda i pametnu tehnologiju radi inteligentnog određivanja brzine kretanja vozila, kako bi vozilo maksimalno iskoristilo zeleni talas svetlosne saobraćajne signalizacije, čime, po mišljenju konstruktora, ove tehnologije smanjuju gužve, štede gorivo i saobraćaj čine sigurnijim.

Samo iz ovih primera je moguće uvideti da je broj inovacija u ovoj oblasti izuzetno veliki i svakodnevan pa bi ga bilo jako teško u većem obimu obuhvatiti i obraditi.⁸ Pametne tehnologije i

⁸ Video Linkovi: Audi launches traffic light recognition system i Audi self parking system
http://www.youtube.com/watch?v=a6zrRukr6WO&feature=player_embedded
<http://www.youtube.com/watch?v=AciORQ2CXFs>

njihovi kreatori u oblasti saobraćaja ponudili su nova rešenja koja negiraju potrebu da svako bude vlasnik vozila. Ova ideja se bazira na tome da je u ljudskoj prirodi da čovek teži vlasništvu nad što boljim i skupljim vozilom, a da onda takvo vozilo najveći deo vremena provodi u garaži ili na parkingu, usled čega svako takvo vozilo gubi na vrednosti u „upotrebnom praznom hodu“, pa su na tom konceptu razvijene cele digitalne platforme za deljenje i prevoz, koje, sudeći po tendencijama izuzetno dobijaju na značaju.

Novi algoritmi za korišćenje automobila i optimizaciju njihovog korišćenja bazirani na aplikaciji, stalno će očitavati naše lokacije i u odnosu na njih interaktivno predlagati upotrebu najbližeg slobodnog automobila. Na sadašnjem nivou tehnološke razvijenosti ove platforme, potreban je vozač koji deljeni automobil dovozi do korisnika, međutim, tendencija razvoja ovih tehnologija bazira se na tome da će u budućnosti autonomni samovozeći automobili to moći raditi sami.

Primena ovih tehnologija podrazumeva da je na ovaj način cena koštanja automobila zapravo samo cena usluge njegovog korišćenja, a koja je određena prema vremenu korišćenja i pređenoj kilometraži, iz kog razloga prestaje potreba za troškovima kupovine i amortizacije automobila, troškova registracije, osiguranja, održavanja, goriva, troška gubitka vrednosti usled starenja vozila, itd., što daje jednu potpuno novu koncepciju i pogled koji preispituje potrebu vlasništva nad istim. U tom smislu, shodno potrebama korisnika, moguće je angažovati različite vrste automobila, pa i u smislu veličine i luksuzne opremljenosti, upravo kakav bi prema potrebi korisnika bio potreban za određenu priliku ili odlazak na željenu destinaciju.

Ako bi se postojeća digitalna transformacija i digitalna budućnost posmatrale kroz prizmu aktuelnih digitalnih i tehnoloških tendencija, čini se da je krajnje nezahvalno predviđati u kom pravcu će se razvijati čak i kompanije kao što su Google, Apple i sl., jer sa ovog stanovišta ne može biti izvesno ni to da li će ove kompanije ostati u postojećem tržišnom segmentu ili će možda postati proizvođači automobila, finansijske institucije ili razviti neke sasvim druge poslovne modele prema zahtevima tržišta i potrošača. Razlog za ovakvo posmatranje budućnosti je nesumnjivo taj što savremene digitalne tehnologije i informacioni sistemi iznova kreiraju nove poslovne procese i poslovna ishodišta, dok istovremeno nepovratno menjaju strukturu svih do sada poznatih poslovnih delatnosti.

Iako je sve to tako, mora se primetiti i jedan paradoks, a to je da se korisnici ovih i ovakvih tehnoloških sredstava, aplikacija i platformi izuzetno brzo navikavaju, ne samo na nove

tehnologije, već i savremene informacione inovacije, prihvatajući da čak one „preko noći“ postaju standardi u pružanju usluga i organizaciji pojedinih poslovnih procesa, što opet sa druge strane primorava konkurentske kompanije na tržištu, čak i kada nisu preterano za to zainteresovane, da moraju ulagati u ovakve inovacije i na njima zasnivaju dalji opstanak na tržištu.

Iz do sada iznetog više nego jasno proističe da skoro da ne postoji proizvod ili usluga iz digitalne sfere, koji nisu implementirani u sve veći broj proizvoda i usluga, usled čega to dalje te proizvode i usluge stalno digitalno inovira, čineći ih ne samo interaktivnim, već i kontaktibilnim. Digitalne tehnologije i savremeni informacioni sistemi temeljno utiču na disruptivne inovacije, pa te inovacije konstantno forsiraju kreiranje sve novijih poslovnih modela, a sve na način da se njima nepovratno menjaju sve strukture, bezmalo svih postojećih delatnosti.

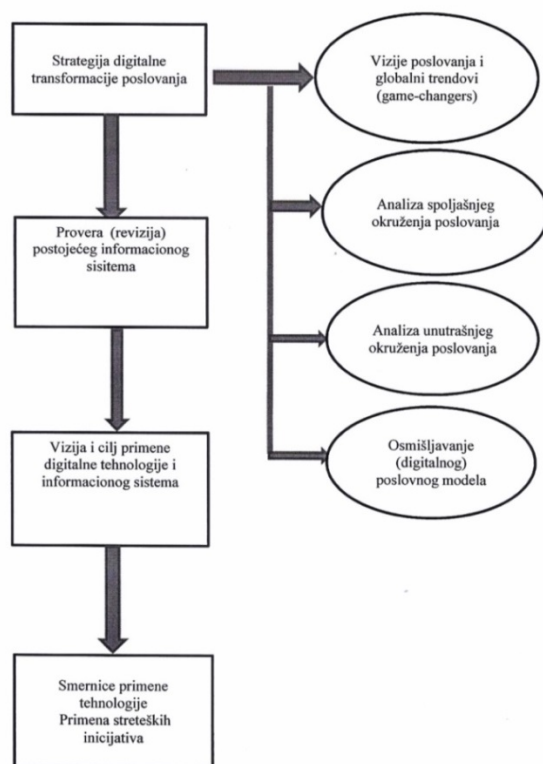
Tendencije ovih tehnologija su takve da radikalno poboljšavaju poslovne performanse kompanija, usled čega one utiču na smanjenje ukupnih poslovnih troškova, dok protok informacija od i ka potrošaču, u slučaju implementiranih inovacija putem informisanog kupca, u potpunosti oblikuje tako nastalu konkurentsku prednost kompanije na tržištu.

Sve napred izneto, i u tehnološkom i poslovno konceptualnom smislu nepovratno utiče na sve generičke osnove poslovanja, kao i postavljene razvojne strategije. Da bi se na polju sve veće i inovativnije konkurencije razvijala i održavala određena konkurentska prednost, tada se prema definiciji mora tržišno egzistirati kroz stalno razlikovanje na tržištu, a to se postiže putem konstantnog refokusiranja poslovanja koje je pogonjeno digitalnim transformativnim procesima i neprekidnim akcijama konkurencije na tom polju.

4. Strategija primene digitalnih tehnologija u poslovanju

Digitalna tehnologija primenjena i implementirana u poslovanju posledično izaziva potrebu za stalnim refokusiranjem strateških planova njene primene, usled čega se u poslovanju kompanije pojavljuje ne samo opšta strategija poslovanja, već i njen digitalni model, tj. digitalna strategija poslovanja. Ovakva strategija poslovanja svoju suštinu pronalazi u konstantnom osmišljavanju novih poslovnih aktivnosti, kako bi one u lancu omogućavale stalni razvoj informacionih sistema utemeljenih na digitalnim tehnologijama, a kako bi sve zajedno činilo potporu za ostvarenje, kako kratkoročnih, tako i dugoročnih poslovnih ciljeva.

Za ostvarenje ovih ciljeva, kao potrebe, izdiferencirale su se stalna i efikasna podrška digitalnih tehnologija u postojećem, odnosno aktivnom poslovnom modelu, korišćenje digitalnih tehnologija kao osnove za promenu postojećih poslovnih procesa i stvaranje inoviranih (disruptivnih) poslovnih modela, koji su zasnovani na intenzivnoj primeni digitalnih tehnologija u smislu temelja stalne poslovne inventivnosti.



Slika br. 15 Koraci i faze postupka dizajniranja i primene strategije digitalne poslovne transformacije

Iz prethodne šeme jasno se vidi, da se po pravilu strateško planiranje i digitalna transformacija poslovanja u velikoj meri oslanjaju na prethodno uspostavljene metode strateškog planiranja razvoja postojećih informacionih sistema kao fundamenta. Na tom primeru se vidi da kvalitetni i postavljeni koncepti modernog poslovanja mogu bez većih teškoća biti prilagođeni uslovima moderne digitalne tehnologije i svim zahtevima primene takvih tehnologija.

Ipak, da bi ostvarivanje ovih ciljeva bilo moguće u modernom poslovanju, potrebno je postojanje adekvatne arhitekture i infrastrukture. Takav pristup strateškom planiranju informacionih sistema, kao pozadini svih poslovnih procesa, jeste jedan opsežan, multidisciplinarni i suštinski sveobuhvatan skup aktivnosti, koje kao takve služe da se usklade postavljeni ciljevi poslovnog i

informacionog sistema, a sve kako bi se postavio adekvatan temelj za nadogradnju kroz planiranje digitalne poslovne infrastrukture čiji je razlog postojanja da omogući ostvarivanje postavljenih poslovnih ciljeva (Lederer, Salmela, 1996:237-253).

4.1 Faze izrade strateškog plana primene digitalnih tehnologija

Da bi digitalna poslovna promena bila utemeljena i održiva, ona mora biti zasnovana na konkretnim fazama i jasnim koracima koji su definisani kroz primenu određenih metoda, kako bi se poslovni plan podvrgao nadogradnji kroz primenu digitalnih tehnologija. Takvi koraci su globalne vizije i analize poslovanja. U ovom koraku sprovodi se analiza „Game change“-ra, ispituju se globalni tehnološki, poslovni i ostali interdisciplinarni trendovi i sve to zajedno procenjuje na način da pruži jasan odgovor na to kakav će biti njihov uticaj na dalje poslovanje kompanija. Nakon toga, potrebno je izvršiti temeljnu analizu konkurentske industrije i ukupnog poslovnog okruženja, imajući u vidu globalne domete interneta, pa nakon toga pristupiti izradi strateške analize koja podrazumeva generičke strategije konkurentske prednosti, tj. pet snaga konkurentske prednosti, odnosno, Pestle analize. U okviru ovog segmenta moraju se sagledati politički, ekonomski, socio-kulturološki i tehnološki faktori, kako pravni, tako i oni koji se tiču životne sredine.

Činjenica je da politički faktori ne mogu biti izučavani bez proučavanja pravnih i zakonodavnih faktora, imajući u vidu da oni suštinski, kroz poslovni ambijent, utiču na rad organizacije. Ovde se akcenat posebno stavlja na delove zakonodavnog okvira koji daju mogućnost povlašćenog poslovanja, onda prihvatljivost propisa o zaštiti životne sredine, poreska politika, zakon o zapošljavanju, generalna politika vlade, njen kurs i opredeljenost, opšti zakonski propisi i drugi pravno specifični delovi zakonskog okvira, koji su deo targetiranog poslovnog i tržišnog podneblja.

Kada su u pitanju ekonomski faktori, oni veoma često igraju presudnu ulogu za poslovanje kompanije. Stoga ova analiza mora dati odgovore na pitanja kao što su: „da li se radi o zemlji u tranziciji i koji je pravac te tranzicije?“, „da li je tržište zasićeno konkurentskim proizvodima i uslugama, itd.“ Ovi faktori u mnogome utiču na formiranje i implementaciju strategije određenog preduzeća na određenom tržištu.

U delu u kome se proučavaju ekonomski faktori, analiziraju se i segmenti kao što je inflacija, zaposlenost, raspoloživ prihod, poslovni ciklus, raspoloživost i utrošak energije, kao i ostali

faktori koji su specifični za konkretnu zemlju ili region, na osnovu čega se dobija jasan odgovor na sve dileme po pitanju statusa i modela sprovođenja tranzicije i njenih rezultata i posledica.

Kada su u pitanju socio-kulturološki faktori, tu se mora voditi računa o tome da nije svaki proizvod adekvatan za svako tržište, niti je strategija penetracije ista za svako tržište. Razlog za to je taj što ljudi iz različitih podneblja imaju različite navike, želje, osećanja i nade, a ti faktori kao subektivni elementi ličnosti veoma utiču na želju za kupovinom određenih proizvoda. U okviru izučavanja socio-kulturoloških faktora, obavezno se u obzir uzimaju faktori kao što su: demografska struktura stanovništva, raspodela prihoda, socijalna pokretljivost, promene načina života, nivo i način potrošnje, obrazovni nivoi na tržištu, a uz to i običaji, verovanja, strahovi i ubeđenja koja postoje na određenom podneblju.

U delu koji se tiče tehnoloških faktora, sagledavanje je veoma kompleksno iz razloga što je uticaj tehnologije na rad kompanije izuzetan. Tehnološko ubrzanje čiji smo svedoci, čini period zastarevanja dobijenih informacija i primenjenih tehnologija izuzetno kratkim, tako da taj period traje od 6 meseci do godinu dana. Stoga je izučavanje i analiziranje tehnoloških faktora na određenom podneblju od izuzetne, a najčešće i presudne važnosti.

U okviru analize ovih faktora, posebno se analiziraju i faktori kao što su novi pronalasci i inovacije, brzina transfera tehnologija, nivoi zastarevanja tehnologija, internet i razvijenost internet infrastrukture i ukupne informacione tehnologije.

U okviru pravnog segmenta analiziraju se pravni faktori koji uključuju propise koji mogu biti od značaja i uticaja na poslovanje. U tom smislu vrše se sagledavanja propisa o zaštiti potrošača, diskriminaciji, zapošljavanju, antimonopolske pravne regulative, propisi kojima se štite autorska prava i podaci o ličnosti, itd.

U domenu zaštite životne sredine analiziraju se faktori sa ekološkim implikacijama, kao što su klima, zagađenost, pitanja pristupu sirovinama, itd.

Kada je u pitanju analiza unutrašnjeg poslovnog okruženja, u okviru ovih analiza najčešće se koriste SWOT analiza, analiza lanca vrednosti i strateška rešetka.

Nakon toga, sledi osmišljavanje digitalnog poslovnog modela koji bi mogao da odgovori na potencijalne penetracije novih tržišnih konkurenata, dostupnost adekvatnih dobavljača i cenovne elastičnosti kod nabavki, kupce, njihovu kupovnu moć, navike i osetljivost na cenovne

fluktuacije, ali i njihovu sklonost ka zamenama proizvoda i usluga drugim proizvodima uz razjašnjenje iz kojih sve razloga.

Digitalni model poslovanja je onaj poslovni model koji mora dati odgovore na sva ova pitanja, ne samo u analitičkom smislu već i u konkurentskom smislu na tržištu.

Nakon osmišljavanja digitalnog poslovnog modela, nesumnjivo je potrebna temeljna analiza funkcionisanja postojećeg informacionog sistema, a u tom smislu i analiza neophodnosti upotrebe novijih i naprednijih digitalnih tehnologija u postojećem digitalnom okruženju i sistemu privređivanja. Moraju se takođe izdiferencirati i vizije i ciljevi postojećeg informacionog sistema koji su u stanju da podrže digitalni poslovni model, ali uz primenu metoda jasnog pozicioniranja uloge i značaja takvog informacionog sistema u novom modelu poslovanja. Uporedo sa tim, moraju nastati i smernice razvoja informacionog sistema, a sledstveno tome, operativno sprovođenje plana digitalne promene poslovanja uz implementaciju merila uspešnosti, definisanja metoda praćenja sprovođenja i nadzora nad implementacijom, te vrednosti koje se tako stvaraju i prioriteta u sprovođenju ovih aktivnosti.

Ključni partneri Ko su naši ključni partneri? Ko su naši ključni dobavljači? Koji su to ključni resursi potrebni od naših partnera? Koje ključne aktivnosti naši partneri sprovode?	Ključne aktivnosti Koje su to ključne aktivnosti koje su neophodne za ostvarivanje dodate vrednosti? Za naše kanale distribucije? Odnose sa klijentima? Tok prihoda?	Dodata vrednost Koje su to vrednosti koje mi pružamo klijentima? Koje probleme naših klijenata mi pokušavamo da rešimo? Koje vrste proizvoda i usluga nudimo određenom segmentu tržišta? Koje potrebe potrošača mi zadovoljavamo? Koji nam je minimalno održiv proizvod?	Odnosi sa potrošačima Kako privlačimo, zadržavamo i uvećavamo broj naših potrošača? Kakve smo odnose sa potrošačima uspostavili? Kako smo se integrisali sa celim biznis modelom? Koliko nas oni koštaju?	Segmenti potrošača Za koga stvaramo vrednost? Ko su naši najvažniji klijenti? Kakvi su arhetipovi naših klijenata?
	Ključni resursi Koje ključne resurse zahtevaju naše vrednosti? Naši kanali distribucije? Odnosi sa potrošačima? Tok prihoda?		Kanali prodaje Kroz koje kanale prodaje možemo dopreti do ciljanih segmenata potrošača? Kako naše kompanije sada dolaze do njih? Koji su najefektniji? Koji su najisplativiji? Kako ih integrišemo sa rutinom potrošača?	
Struktura troškova Koji su to najvažniji troškovi u našem biznis modelu? Koji su ključni resursi najskuplji? Koje su ključne aktivnosti najskuplje?		Tok prihoda Koliku vrednost su naši potrošači spremni da plate? Koliku vrednost sada plaćaju? Kakav je model prihoda? Koje su cenovne taktike?		

Tabela br. 2 Biznis model Canvas - metoda za analizu biznis modela

4.2 Tehnologija izrade strateškog plana

Izrada strateškog plana informacionih sistema predstavlja poslovni proces koji je u celini koncipiran da podupre ciljani poslovni model. Proces strateškog planiranja informacionih sistema određuje strategiju informacionih sistema, njegovu ulogu u poslovnom sistemu, ciljeve njegovog korišćenja i poželjnu arhitekturu koja je u stanju da odgovori postavljenom poslovnom zahtevu.

Jasno je stoga, da je strateško planiranje informacionih sistema multidisciplinarni skup isprepletanih aktivnosti kojima se usklađuju ciljevi poslovnog informacionog sistema i planira informaciona infrastruktura koja omogućava ostvarivanje svih ciljeva poslovanja (Lederer, Salmela, 1996:237-253).

Iz tih razloga, logički i algoritamski principi definišu hijerarhiju koraka radi postizanja ovih ciljeva, pa se iz strategije poslovanja određuje i definiše informaciona strategija poslovanja, tj. strategija informacionih sistema iz koje se onda izdvajaju pojedinačne strategije njegovih sastavnih delova.

Strategija poslovanja	Sistem poslovanja	Informacioni sistem
↓		
Strategija informacionog sistema		Strategija
↓		Organizacija
Tehnologija (IT) - Ljudi - Procesi IS		Procesi i procedure
↓		Infrastruktura
Metrike	Ciljevi	Aplikacije
↓	Željeni učinak	Projekti
Poslovna vrednost informatike	Strategije	Budžet
		Metrike

Tabela br. 3 Izvođenje informatičke strategije iz strategije poslovanja

Sprovođenje strategije poslovanja, po svom značaju, iziskuje aktivno učešće najvišeg menadžmenta kompanije, glavnog informacionog menadžera (eng. CIO - Chief Information Officer), ali i menadžera ostalih važnih poslovnih funkcija prema postavljenoj hijerarhiji upravljanja organizacijom.

Kompanije često pribegavaju pravilima projektnog organizovanja, pa u svom radu često formiraju posebna organizaciona tela i odbore. U praksi se ti odbori nazivaju odborima za upravljanje poslovnom informatikom ili kako se često na engleskom govornom području ova tela nazivaju „IT Steering Committee“. Ova specijalizovana tela imaju zadatak da nadziru sprovođenje strateškog informacionog plana kompanije. U ovakvim konstelacijama, najčešće Odbor za upravljanje poslovnom informatikom čini posebnu savetodavnu i organizacionu celinu koja je ustrojena kao nezavisna od sektora i informatičkog odeljenja, usled čega je neposredno odgovorna menadžmentu kompanije.

Zadatak ovakvog odbora nije jednostavan, imajući u vidu da on mora voditi računa o tzv. „konektovanju“ informatike i poslovanja i time njihovog usklađivanja u kompaniji, shodno poslovnim prioritetima i ciljevima. Konačan ishod ovakvog procesa je izgradnja i konstantno inoviranje i poboljšavanje poslovnih informacionih sistema, obzirom da oni čine faktor koji omogućava ostvarenje zacrtanih poslovnih ciljeva, a u sklopu toga održanje ili poboljšanje konkurentske pozicije uz stvaranje novih poslovnih vrednosti.

Da bi to bilo moguće, potrebna je izrada detaljne analize rada informatike i informacionih sistema, formulisanje ciljeva i smernica budućeg informacionog sistema i plan za implementaciju inovacija koji podrazumeva metodologiju sprovođenja i preporuke za isto.

Delovi poslovnog plana	Određuju →	Delove IS strateškog plana
Misija, vizija, ciljevi poslovanja, vrednosti i prioriteti	Smernice ↓	Određuju viziju, misiju i ciljeve IS, učinak i strategije
Struktura delatnosti, obeležja tržišta, finansiranje	Industrijska analiza ↓	Određuju zahteve koji se postavljaju pred buduće IS, konkurentsku prednost i IS
SWOT – snage, slabosti, prilike i pretnje poslovanju	Situaciona analiza ↓	Sposobnost izvršavanja IT projekata, određuju potencijalne IT projekte, SWOT analiza IS
Činioci uspeha, metrike poslovnih procesa	Metrike uspešnosti ↓	Određuju metrike uspešnosti IS
Ciljevi i strategije	Planovi ↓	Određuju ključne IT projekte i postavljaju prioritete
Finansiranje	Finansijski modeli	IT budžet, politika IT ulaganja, ciljevi IT projekata

Tabela 4 Delovi poslovnog plana određuju delove strateškog plana informatike

5. Oblikovanje digitalnog poslovnog modela

Digitalni poslovni model sam po sebi predstavlja sistem prilagođavanja načina i modela poslovanja uslovima digitalne ekonomske transformacije, tj. digitalne ekonomije, radi čega taj

model nastupa sa ciljem pronalaženja održivih izvora prihoda i stvaranja dodate vrednosti putem novog poslovnog modela, tj. modela koji intenzivno koristi digitalnu i informacionu tehnologiju.

Suštinski gledano, digitalizacija poslovnih modela čini veoma kompleksan skup aktivnosti kojima se utvrđuju utrživi izvori prihoda, načini učestvovanja partnera u poslovnim aktivnostima, rešavaju moguće poslovne kontroverze, pa koncept poslovnih modela zapravo čini most između upotrebe savremenih tehnoloških dostignuća, najpre elektronske poslovne infrastrukture, a onda i stvaranja adekvatne ekonomske vrednosti za sve učesnike ekonomskih transakcija. Stoga, poslovni model predstavlja koncept prema kome kompanija u sadejstvu sa svojim poslovnim partnerima intenzivno koristi digitalne tehnologije radi stvaranja nove vrednosti bilo na elektronskom ili tradicionalnim fizičkim tržištima.

Pojava i razvoj elektronskog tržišta koje nije prostorno ograničeno, zahteva stalnu analizu globalnih trendova unutrašnjeg i spoljnog poslovnog okruženja, pa proces strateškog planiranja zapravo čini nastavak osmišljavanja inoviranog poslovnog modela. Kako se ovde radi o digitalnoj promeni poslovanja, u tim okvirima je potrebno osmisliti i održiv digitalni poslovni model, tj. poslovni model koji pojačano koristi digitalnu tehnologiju putem koje želi doći do ostvarenja postavljenih poslovnih ciljeva.

Poslovni model, stoga, mora dati nedvosmislene odgovore na pitanja koje i kakve vrednosti kompanija isporučuje svojim kupcima, koje tržišne prilike pokušava iskoristiti, koje usluge i proizvode nudi korisnicima, te koju strategiju sledi u digitalnom konkurentskom i poslovnom okruženju. Osmišljavanje poslovnog modela, pored ostalog služi i tome, da se putem njega preispitaju sposobnosti i potencijali koje kompanija poseduje i planira iskoristiti da bi unapred određeni poslovni koncept sprovela u delo. U najkraćem, poslovni model određuje ono što kompanija čini za svoje korisnike i kupce, ali i način na koji to radi i kako kompenzuje ono što nudi kupcima i korisnicima.

Ipak, u današnje vreme uspostavljena su određena pravila i zakonitosti koje olakšavaju osmišljavanje poslovnih modela, pa su u tom cilju nastali brojni predlozi koji preduzetnicima i menadžerima, ako ne samo olakšavaju, oni i strukturisu takav složeni proces. U tom smislu, treba

izdvojiti „Biznis model Canvas“ koji predstavlja poligon za skiciranje najvažnijih obeležja poslovnog modela (videti tabelu br.2).⁹

Skiciranje digitalnog poslovnog modela podrazumeva obavezu menadžmenta da odgovori na konkretna poslovna pitanja, među kojima se izdvajaju sledeća:

1. Ko su naši poslovni partneri, ko su naši dobavljači, koji su poslovni resursi koje poseduju naši partneri i dobavljači suštinski važni za naš poslovni model, koje ključne aktivnosti sprovode naši partneri, itd.?
2. Koje i kakve vrednosti isporučujemo svojim korisnicima; koje njihove potrebe i probleme mi stvarno rešavamo; koje usluge i proizvode naša ponuda obuhvata u odnosu na naše kupce i korisnike?
3. Koje su aktivnosti potrebne da kupcima isporučimo vrednosti; koji su i kakvi naši distributivni kanali, kakvi su odnosi sa klijentima i koji su održivi izvori prihoda?
4. Koji su nam ključni resursi potrebni da bi kupcima i korisnicima mogli isporučiti očekivane vrednosti; koji su naši distributivni kanali, odnosi sa klijentima i naši održivi izvori prihoda?
5. Kako dolazimo do naših kupaca, kako ih i čime zadržavamo i kako im omogućavamo da se razvijaju sa nama, koje i kakve vrste odnosa sa kupcima u ovom trenutku imamo, kako su naši kupci povezani sa ostalim delovima poslovnih modela i koliko nas oni zapravo koštaju?
6. Kojim se klijentima mi zapravo obraćamo; ko su naši najvažniji kupci i korisnici, koji su njihovi preferirani načini ponašanja i trošenja?
7. Koje poslovne kanale tj. kanale komunikacije, distribucije i prodaje naši korisnici očekuju; koje i kakve digitalne platforme poslovanja oni od nas očekuju i žele koristiti; koje poslovne kanale koriste naši konkurenti; koji su poslovni kanali najuspešniji, a koji troškovno najefikasniji; koje kanale poslovanja možemo upotrebiti u svom poslovnom modelu?
8. Kakva je troškovna struktura u našem poslovnom modelu; koji resursi su najskuplji; koje aktivnosti su najskuplje; koji su kanali poslovanja skupi?
9. Koja je naša struktura prihoda; od čega zarađujemo novac; u kojoj meri su naši prihodi održivi; od čega zavise naši stalni prihodi; koju vrednost korisnici zaista žele da plate i

⁹ The business model canvas, Business Model Alchemist, <http://businessmodelalchemist.com/>

koliko; šta tačno korisnici plaćaju kada koriste naš poslovni model i imamo li različite cenovne taktike?

6. Analitički kontekst funkcionisanja informacione infrastrukture postojećeg poslovnog modela

Strateško planiranje informacionog sistema je od izuzetne važnosti kao osnova za sprovođenje temeljne revizije informacionog sistema i njegovih funkcionalnih komponenti. Revizija informacionih sistema predstavlja i složen i metodološki temeljan postupak, kako provere funkcionisanja informacionog sistema, tako i analize njegovog rada u odnosu na projektovane potrebe poslovanja. Revizijom informacionih sistema se bave revizori informacionog sistema, ali oni ne vrše provere da li je postojeći informacioni sistem „dovoljno svež i savremen“, već samo kako postojeći informacioni sistem i njegovi sastavni delovi vrše svoje poslovne funkcije i održavaju poslovanje.

U tom smislu, cilj revizije informacionih sistema je zapravo detaljna analiza stanja postojeće poslovne informacione infrastrukture, a u sklopu toga uočavanje mogućih odstupanja i problema na osnovu kojih se mogu dati preporuke menadžmentu kompanije za poboljšanjem oslabljenih funkcija. Samim tim, to je metodološki utemeljen postupak, obzirom da se u njenoj primeni najčešće koriste svetski priznati standardi i okviri, kao što je npr. CobiT.¹⁰

Imajući u vidu potrebu digitalizacije poslovanja kompanije, revizori informacionih sistema moraju odstupiti od svih uobičajenih rutina koje podrazumevaju sprovođenje isključivo tehnoloških revizija, pa se umesto toga moraju usmeriti prema strateškim revizijama informacionog sistema, jer će upravo one biti te koje će menadžmentu kompanije dati ključne preporuke za uspešno zaokruživanje digitalizacije poslovanja. Ove preporuke bi trebale podrazumevati i aktuelne tehnološke trendove, fleksibilnu i skalabilnu infrastrukturu, hibridne računarske oblake, naprednu analitiku podataka, višefunkcionalni i energični pristup softverskom razvoju, saradnju sa start-up-ovima, intenzivnu eksternalizaciju kao metod stvaranja digitalne platforme poslovanja, itd.

U smislu navedenog, ova faza strateškog planiranja informacionih sistema treba da rezultira detaljnom i sveobuhvatnom analizom postojećeg stanja u ovom sistemu uz dokumentovanje

¹⁰ CobiT- Control Objectives for Information and Related Technologies je dobra praksa stvorena od strane međunarodne profesionalne asocijacije ISACA za menadžment informacione tehnologije (IT) i IT upravljanje

njegovog stanja prema CobiT odrednicama, procenom potencijala preduzeća za digitalnu promenu u poslovanju i preporukama sa smernicama i scenarijima za sprovođenju ovakvih inovacija u delo.

6.1 Ciljevi i smernice primene digitalnih tehnologija

Na temelju sprovedenih analiza postojećeg informacionog sistema, određuju se i ciljevi procesa strateškog planiranja informacionog sistema. Ulazne varijable, odnosno inputi u taj proces su sledeći: analiza poslovanja, industrija poslovnih i tržišnih potreba, kao i preispitivanje poslovnih procesa i budućih smernica poslovanja radi izrade procene u kojoj meri samo poslovanje utiče na postojeće informacione sisteme i obratno. Samim tim, u ovoj fazi se sprovodi revizija informacionih sistema sa jasnim akcentom na strateške komponente i pravila korporativnog upravljanja informatičkom funkcijom u preduzeću.

U konačnom zbiru, ova transformativna faza se završava određivanjem kratkoročnih planova koji se mogu momentalno sprovesti uz određivanje ciljeva rada informatike koji pretpostavlja misiju, viziju, ali i ključne ciljeve i strategije. Da bi se izvršila detaljna analiza informatike i informacionog sistema u kompaniji, najpre se mora izvršiti detaljna analiza informacionih trendova, proučavanje prakse konkurencije i na kraju vršenje temeljne unutrašnje i spoljašnje revizije informacionih sistema.

U sklopu ove revizije, detaljno i dubinski se analiziraju informacione potrebe kompanije, poslovne aplikacije, informaciona ugrožavanja, podaci, hardver, organizacija rada informatičke funkcije i sl. Pored toga, vrši se i popis stanja u svim područjima rada informatičke poslovne funkcije u preduzeću i u tom smislu inventura poslovnih aplikacija kroz složeni pristup koji podrazumeva razvojno okruženje, platforme, operativne sisteme, vlasništvo, održavanje, aplikacioni portfolio, korisnike, tehnologiju, arhitekturu, planove, performanse, uticaj na poslovne procese, troškove, robusnost, nivo fleksibilnosti aplikacija, procenu povezivosti aplikacija, baze podataka, itd.

Kao nadogradnja na sve navedeno, vrši se i inventura hardvera, računarske mreže i mrežne opreme, kao i ocena ukupnih performansi i njihovog rada. Vrši se inventura stanja podataka, načina rada informatike i svih informatičkih procesa, uključujući i inventuru svih informatičkih projekata, analiza informatičkog budžeta i metrika uspešnosti informacionog sistema. Primenom ovih inventura informatike kao poslovne funkcije, stvaraju se neophodni preduslovi da se iz

postojećih poslovnih ciljeva, prema zahtevima poslovanja mogu odrediti ciljevi, ovlašćenja i poželjna arhitektura budućeg informacionog sistema, tj. misija, vizija, ciljevi i strategija rada informatičke funkcije preduzeća.

7. Razrada strategije, sistem etabliranja i pozicioniranje uloge digitalnih tehnologija u poslovanju

Strateški plan informatike, ili digitalna strategija kompanije, predstavlja važan formalni poslovni dokument kojim se shodno strategiji i ciljevima poslovanja određuju prioritete upotrebe informacionih sistema utemeljenih na digitalnim poslovnim tehnologijama, njihovoj optimalnoj hijerarhijskoj poziciji, prioritetima ulaganja u informacione projekte, ali i poslovne rizike koji proizilaze iz njihovog intenzivnog korišćenja i primene.

Može se zaključiti da kompanije koje nisu uspostavile strateški plan informatike, objektivno ne vode sistemsku brigu o ovim odlučnim poslovnim pitanjima, iz čega se može razumeti da ovakve kompanije ni nemaju jasan odgovor na pitanje zašto zapravo troše novac na informatiku, kao ni čemu im informatika i informacioni sistemi uopšte služe. Iz ovog se dalje može razumeti da takve kompanije informatiku i informacione sisteme zasnovane na digitalnim tehnologijama ne smatraju podjednako važnom poslovnom funkcijom.

U ovakvim poslovnim okolnostima i poimanju stvari, novac uložen u informacione sisteme i informatiku se zaista može tretirati kao trošak, obzirom da ta investicija ne podržava ciljeve poslovanja. Stoga, pri određivanju poželjne uloge poslovne informatike, menadžmentu kompanije od prilične pomoći može biti McFarlanov model Strateške rešetke (McFarlan, McKenney, Pyburn, 1983).

Iako je ovaj model nastao pre više od 30 godina, njegova logika i dalje čini referentni model za određivanje adekvatnosti položaja informacionog sistema u organizacionoj strukturi kompanije. Prema tom modelu, strateška pozicija informatike čini funkciju dve varijable i to: strateške važnosti postojećih i strateške važnosti budućih informacionih sistema, pa u zavisnosti od nivoa važnosti tih varijabli možemo razlikovati 4 tipa organizacije poslovanja (Panian, 2001:41-43): podržavajuću, fabričku, pretvaračku i stratešku.

Dvadesetak godina nakon nastanka izvornog modela strateške rešetke, McFarlan je sa svojim saradnicima doradio ovaj model i prilagodio ga novonastalim okolnostima. Neizbežna je stoga

potreba i da se primeti postojanost i inovativnost izvornog modela koji je uprkos nepredvidivom razvoju informatike i njene poslovne primene, uspeo predvideti ključne trendove i poslužiti svrši svoga nastanka. Ta svrha je pomoć menadžmentu u tome da definiše i utvrdi optimalnu ulogu informatike u poslovanju. Tako se taj rad, zajedno sa kasnijim Nolanovim radovima (Nolan, 1977:114-124), može smatrati teorijskim počecima informatičkog menadžmenta, tj. poslovne informatike, odnosno, početkom intenzivne primene poslovne informatike.

McFarlan i Nolan su izvršili doradu modela strateške rešetke (eng. Strategic Grid), prema kome se mogu razlikovati dve osnovne strategije informacionog sistema, a time i dve osnovne uloge poslovne informatike:

- Reaktivna (obrambena, defanzivna) strategija, i
- Proaktivna (napadačka, ofanzivna) strategija.

Tabela br. 5 Defanzivna i ofanzivna strategija

DEFANZIVNA INFORMATIKA	OFANZIVNA INFORMATIKA
<p>Operativna podrška poslovanju (factory mode)</p> <p>Ako sistem prestane da funkcioniše na minut ili više, istovremeno počinje dolaziti do poslovnih gubitaka;</p> <p>Produžetak vremena odziva sistema na više od 1 sekunde ima ozbiljnih posledica na rad njegovih spoljnih i unutrašnjih korisnika;</p> <p>Mnoge ključne poslovne aktivnosti odvijaju se u realnom vremenu, tj. „on-line“;</p> <p>Suštinu rada na sistemu čini njegovo održavanje;</p> <p>Radovi na sistemu omogućavaju neznatnu stratešku prednost ili dramatične finasijske uštede.</p>	<p>Strateška podrška poslovanju (strategic mode)</p> <p>Ako sistem prestane funkcionisati minut ili više, dolazi do trenutnih poslovnih gubitaka;</p> <p>Produžetak vremena odziva sistema na više od 1 sekunde ima ozbiljnih implikacija na rad njegovih spoljnih i unutrašnjih korisnika;</p> <p>Novi sistemi obećavaju velike promene u smislu poslovnih procesa i usluga;</p> <p>Novi sistemi obećavaju značajno smanjenje troškova;</p> <p>Novi sistemi će omogućiti troškovnu i procesnu prednost, tj. prednost u domenu pruženih usluga u odnosu na konkurenciju.</p>
<p>Podrška poslovanju (support mode)</p> <p>Čak i uz učestale prekide funkcionisanja sistema do 12č, nema ozbiljnijih posledica po poslovanje;</p> <p>Prihvatljivi odziv korisničkih transakcija u stvarnom vremenu može trajati i do 5 sekundi;</p> <p>Interni sistemi su gotovo nevidljivi kupcima i dobavljačima. Potreba za ekstranet funkcijom je stoga mala;</p> <p>Preduzeće se može vratiti na ručne radne procedure kod 80% transakcija u poslovanju;</p> <p>Suštinu rada na sistemu čini njegovo održavanje.</p>	<p>Podrška preokretu u poslovanju (Turnaround model)</p> <p>Novi sistemi obećavaju velike promene u domenu poslovnih procesa i usluga;</p> <p>Novi sistemi obećavaju značajno smanjenje troškova;</p> <p>Novi sistemi će omogućiti troškovnu i procesnu prednost tj. prednost domenu pruženih usluga u odnosu na konkurenciju;</p> <p>IT čini više od 50% kapitalnih ulaganja;</p> <p>IT učestvuje sa više od 15% ukupnih troškova poslovanja.</p>

Odbrambena tj. reaktivna ili defanzivna informatika se u engleskoj terminologiji najčešće naziva i „*Defensive IT*“. Njena polazna ideja je da je početni zadatak informacionih sistema u poslovanju da učine troškovno efikasnu, sigurnu i pouzdanu tehnološku osnovu za odvijanje procesa poslovanja i pratećih transakcija. Po tom modelu je korišćenje pouzdanih i uvek dostupnih informacionih usluga važnije od razvijanja inovativnih rešenja kojima se može uticati na strategiju poslovanja.

Čest je primer da kompanije koje su adekvatnom primenom inovativnih poslovnih informacionih sistema ostvarile konkurentsku prednost, da ovu strategiju primenjuju radi održavanja ovako stečene prednosti. Primena ove strategije podrazumeva da nadzorni organi i uprava kompanije zahtevaju garanciju da je postojeća informaciona infrastruktura sigurna i zaštićena od raznih rizika, kao i da su troškovi njene upotrebe pod kontrolom. Ovo je zato što se tu radi o strateškoj primeni informatike u poslovanju, usled čega bi i najmanji incident, otežano funkcionisanje ili prekid rada informacionog sistema, kompaniji mogao pričiniti velike gubitke i izložiti je ogromnim rizicima.

Usled ovakvih izazova, nastala je praksa da odbor za upravljanje informatičkom funkcijom u kompaniji konstantno vodi brigu i o uspešnosti i reviziji informacionih sistema. Iz tog razloga su pored glavnog informacionog menadžera (CIO) i menadžera uprave kompanije zaduženog za informatiku, članovi ovog odbora istovremeno i izvršni menadžeri ključnih poslovnih funkcija, dok se njihovim radom upravlja na korporativnom nivou.

Sa druge strane, proaktivna tj. napadačka ili ofanzivna informatika (engl. „*Offensive IT*“), odnosno strategija, podrazumeva da poslovni informacioni sistemi imaju funkciju da pored nužne podrške redovnom odvijanju poslovanja budu korišćeni i u svrhu promene poslovne strategije, ali pre svega kao sredstvo za postizanje konkurentskih prednosti. Stoga i ofanzivna, i proaktivna uloga poslovnih informacionih sistema nastaje kada su strateški razlozi za njihovo korišćenje na istom nivou, ili čak važniji od kriterijuma pouzdanosti i dostupnosti.

To znači da ofanzivna uloga poslovnih informacionih sistema čini da se oni primenjuju kao oslonac i inovacije poslovanja i njegove radikalne transformacije. Takve aktivnosti su sa jedne strane veoma bitne, ambiciozne i rizične, ali sa druge strane i potencijalno veoma isplative.

Kompanije primenjuju ovu strategiju kada žele poboljšati svoju konkurentsku i tržišnu poziciju i žele ugroziti ili „napasti“ lidera na tržištu. Najčešći način ovog „napada“ jeste korišćenje

inovativne tehnologije u kombinaciji sa poslovnim informacionim sistemima koji daju efekat operativne efikasnosti i znatno nižih troškova poslovanja, što radikalno menja način odvijanja poslovnih procesa usled postignute sinergije. Ova, po svojoj suštini veoma složena strategija, veoma često ima dvojni karakter koji podrazumeva da kompanija mora vršiti ulaganja u perfektno i mehanički tačno funkcionisanje postojećih sistema infrastrukture i istovremeno neprekidno razvijati kompletno nove inovativne sisteme koji će voditi ka dostizanju ili održavanju konkurentske pozicije.

Imajući u vidu da se poslovni informacioni sistemi koriste i u strateške svrhe, pored nadzora nad njihovim funkcionisanjem, uloga odbora za upravljanje informatičkom funkcijom u kompaniji je i savetodavna, obzirom da odbor upućuje i predloge strateških inicijativa radi davanja doprinosa ostvarivanju ciljane konkurentske prednosti.

Kompanije koje koriste ovakvu ofanzivnu strategiju poslovnih informacionih sistema, obično uspostavljaju i druga savetodavna i nadzorna tela na korporativnom nivou za upravljanje informatikom, pa se ta tela najčešće nazivaju odborima za upravljanje projektima ili odborima za stratešku primenu informatike (eng. „*IT Governance Committee*“), a sve kako bi se ovim turbulentnim područjem što efikasnije upravljalo.

7.1 Podrška poslovanju

Osnovni cilj poslovnih informacionih sistema je da oni pruže operativnu i tehnološku podršku poslovanju. Kompaniji je iz ovog razloga potrebna pouzdana, sigurna i uvek dostupna informatička podrška, jer ako je poslovanje kompanije suštinski bazirano na stabilnosti i efikasnosti primenjenih informacionih tehnologija, u tom slučaju bi čak i vrlo kratak prekid u funkcionisanju informacionih sistema ili pojedinih njegovih delova ili servisa, jednoznačno bio i prestanak odvijanja kritičnih poslovnih procesa, što samo po sebi poslovanje izlaže ogromnom riziku i troškovima, a što opet može izazvati i nepopravljivu poslovnu štetu.

Stoga, uz ključne pokazatelje uspešnosti poslovanja, procenjuje se i uspešnost menadžmenta, i to na osnovu nivoa dostupnosti informacionih sistema u poslovanju, gde se kao jedno od merila uzima i strateški cilj poslovanja koji može biti postavljen na nivou da 99,994% vremena informacioni sistem mora biti i dostupan i besprekorno funkcionalan, usled čega je zadatak informacionog menadžmenta da ovaj zahtev ispuni, kako na troškovno efikasan, tako i na poslovno delotvoran način.

Iako je poslovno-informacioni-sistem najpre uspostavljen kao važno sredstvo povezivanja unutrašnjih procesa poslovanja i integrator celokupnog poslovanja, njegove granice se protežu i van toga, sve do kupaca, dobavljača i poslovnih partnera. Ovo znači da se poslovnim informacionim sistemom mogu služiti i drugi ovlašćeni korisnici izvan postojeće organizacije, što pored rizika donosi i velike uštede, te čini temelj i eksterno operativne efikasnosti kompanije.

Usled toga, kompanija i njen menadžment teško mogu zamisliti efikasno poslovanje bez stalne podrške poslovnih informacionih sistema, iz kog razloga je informatika stalno zastupljena tema na sastancima odgovorne kompanijske uprave i operativnog menadžerskog tima. U ovom kontekstu se intenzivno koristi internet tehnologija, pa je većina poslovnih procesa kompanije „on-line“. Ovo takođe znači da se u kompaniji veoma ozbiljno i intenzivno sprovodi koncept elektronskog poslovanja.

Iz ovih razloga, poslovanje kompanije je izuzetno zavisno od informatičke podrške, pa ukoliko dođe do toga da informacioni sistem i informacioni servisi ne podrže aktivnosti korisnika, to za posledicu može imati ozbiljne poteškoće i štete za kompaniju. Stoga, poslovanje u ovim okolnostima zahteva krajnje pouzdanu, izuzetno sigurnu i uvek dostupnu informatiku i informatičku infrastrukturu, a ona kao takva mora biti „zrela“, a ne pomodarska, jer pouzdano poslovanje zahteva proverena rešenja i tehnologiju, a ne eksperimente sa tehnološkim novotarijama kojih danas ima i previše. Stoga su kritični informacioni i poslovni procesi, kontrola informacione infrastrukture, kontinuitet poslovanja, plan oporavka nakon prekida rada sistema, kontrola zrelosti sistema i kontrola nivoa ulaganja u informatiku.

U smislu iznetog, radi upravljanja kontrolom kvaliteta poslovanja, nužno je konstantno pratiti performanse rada sistema i periodično sprovoditi revizije njegove uspešnosti. Ovo zato, jer je primena informacionih sistema zapravo temelj operativne efikasnosti kompanije, tj. temelj koji omogućava značajne finansijske uštede, s tim što uz to PIS (Poslovni informacioni sistem) nije izvor poslovne diferencijacije, niti strateške prednosti kompanije.

7.2 Proaktivna strategija

Kompanije najčešće koriste proaktivnu strategiju poslovnih informacionih sistema u vreme kada pokreću velike informatičke projekte i druge velike projekte u smislu promene poslovanja, što podrazumeva radikalnu promenu poslovnih procesa, opsežne poslovne inovacije i sl.

To je znak da se te kompanije u najvećem broju slučajeva nalaze u procesu radikalne i sveobuhvatne transformacije poslovanja, pa se informatika u njima koristi kao sredstvo i poluga ove transformacije sa ciljem da se postigne strateška konkurentska prednost kompanije na tržištu.

Najčešća obeležja ove strategije jesu velika i ciljana ulaganja u informatiku, što usled nepredvidivog razvoja digitalnih sredstava može činiti priličan rizik, dok sa druge strane u određenom periodu i potencijalno održivu konkurentsku prednost na tržištu. Zato u slučaju primene ove strategije postoji više izražena potreba za inovativnom, nego za pouzdanom informatikom. Ovo ne znači da kompanija ne vodi računa o pouzdanosti i dostupnosti postojećih informacionih sistema, već da kompanija u relativno kratkom roku želi postojeći informacioni sistem zameniti novijim, tj. inovativnijim u smislu efikasnosti informatičkog rešenja.

Novi informacioni sistemi stoga moraju obezbediti drastična unapređenja poslovnih procesa i usluga, veliku uštedu u smislu troškova, ali i potencijalno vodeću poziciju na tržištu. Usled toga, ova strategija je veoma rizična, pa kompanije koje prve uspeju implementirati neko novo tehnološko rešenje, obično neko vreme uspevaju održati svoju kompetitivnu prednost, iako je ta konkurentska prednost nastala samo na temelju skupog inovativnog rešenja kratkoga daha, obzirom da ih tržišni imitatori veoma brzo uspevaju kopirati i preuzeti.

Kako ove kompanije intenzivno troše finansijska sredstva na informatiku sa nadom da će tako postići značajne strateške pomake u odnosu na konkurenciju, time im je poslovanje i izloženije riziku, usled čega pametne kompanije relativno kratko vreme sebe podvrgavaju ovoj strategiji. To rizično vremensko razdoblje, najčešće se odnosi na vreme implementacije novog informatičkog projekta, nakon čega menadžment kompanije pribegava tome da potraži neku novu poželjnu strategiju primene informacionih sistema, odnosno informatike u poslovanju. U tom razdoblju je manja potreba za pouzdanim i neprekidnim sistemom, jer su postojeći sistemi dovoljno jednostavni da se u slučaju neželjenih događaja mogu pokriti i manuelnim „back up“ procedurama. Stoga su za ovu strategiju primene poslovnih informacionih sistema nužni i kritični stalna kontrola i nadzor uprave i nadzornih tela kompanije, a to se najpre odnosi na upravljanje rizicima i kontrolu doslednosti sprovođenja informatičkih projekata.

7.3 Predlog strateškog plana informacionog sistema kao podrške poslovnom procesu

Problemi u razvoju informacione strategije kompanije, najčešće se odnose na nezainteresovanost menadžmenta, loš imidž informatičke funkcije u kompaniji, nedostatak vremena za definisanje

ili sprovođenje strategije i slabo sprovođenje strategije u slučaju da ona postoji. Ključni činioci uspeha informatičke, odnosno informacione strategije, najčešće su uključenost i predanost najvišeg menadžmenta kompanije, dobra analiza poslovanja (i to ne samo tehnologije i informatike) i samim tim i dobar informatički menadžment, gde se posebno ističe CIO koji predstavlja lice koje pored tehničkih performansi razume i onu mnogo važniju, tj. poslovnu stranu informatike i sposoban je da primenom svojih poslovnih znanja i veština ova pitanja razjasni i najvišim nivoima menadžmenta i izazove njihovo interesovanje i naklonost.

Poglavlje VI: Upravljanje rizicima u digitalnom poslovanju

Intenzivna primena informacione i digitalne tehnologije, kompanijama sa jedne strane donosi mnoge poslovne koristi, ali ih sa druge strane istovremeno izlaže i potpuno novim rizicima i neželjenim posledicama.

Informatički, tj. informacioni ili sajber rizici predstavljaju one rizike koji nastaju usled intenzivne primene informacionih tehnologija pri obavljanju poslovnih aktivnosti. Stoga se može reći da je u današnje vreme evidentno da su ovim vrstama rizika zapravo izloženi svi poslovni subjekti, a posebno oni čije je poslovanje zasnovano na korišćenju savremene digitalne tehnologije radi ostvarivanja poslovnih ciljeva.

Informatički rizici, odnosno rizici primene informacionih sistema i tehnologija, nikako se ne smeju smatrati samo tehnološkim rizicima, obzirom da bi to minimiziranje činilo da ovi rizici nisu od velike važnosti za uspešnost poslovanja. Suprotno tome, ukoliko bi menadžment kompanije napravio procene koje su pogrešne u tom smislu, to bi kompaniju moglo izložiti velikom riziku i direktnoj finansijskoj šteti, kako u direktnom, tako i u indirektnom smislu.

1. Pojam i sadržaj informatičkog rizika

Rizik predstavlja opasnost ili verovatnoću da će određeni izvor pretnje u određenim okolnostima iskoristiti ranjivost sistema, čime se može pričiniti bitna šteta na imovini organizacije. Informatički rizici su, stoga, vrsta poslovnih rizika koji proizilaze iz intenzivne upotrebe informacionih sistema i digitalne tehnologije kao podrške odvijanju i unapređenju poslovnih procesa i uopšte poslovanja. Ovi rizici odnose se na opasnosti i pretnje od toga da intenzivna primena informacionih sistema može biti uzrok neželjene ili neočekivane posledice i bitne finansijske i druge štete unutar kompanije, ali i njenog neposrednog i šireg okruženja. Ta šteta se može sagledati u materijalnom i finansijskom smislu, a može biti direktna i indirektna.

Informacioni rizici mogu biti predstavljeni funkcijom koja čini međusobno delovanje varijabli poput imovine organizacije, bilo da je ona materijalna ili nematerijalna, bilo da se ona iskazuje kroz incidente, neželjene događaje ili ranjivosti, kao što su slabost sistema koja bi se mogla sagledati kroz nivo efikasnosti primenjenih kontrola čiji je cilj sprečavanje pojava neželjenih događaja.

Ipak, pravilo sugerše da, što je kompanija integrisala više efikasnih kontrola za sprečavanje nastanka ili efekta neželjenih događaja, za toliko se smanjuje i verovatnoća da će kompanija biti izložena informatičkim rizicima, tj. povećava se verovatnoća da se rizici neće dogoditi, ili će kompanija biti izložena informatičkim rizicima nižeg stepena intenziteta. Ako rizici i nastupe, njihov učinak će biti bitno slabiji, radi delovanja efikasnih proaktivnih informatičkih kontrola. Upravo iz ovih razloga, od izuzetne je važnosti stalno proveravanje i testiranje efikasnosti informatičkih kontrola, kako bi se bolje, efikasnije i spremnije moglo upravljati informatičkim rizicima.

Informacioni rizici su u suštini rizici poslovanja u vezi sa strateškom primenom, operativnim korišćenjem, vlasništvom, upravljanjem, primenom i uticajem digitalne i informacione tehnologije na poslovanje. Ovi rizici se baziraju na događajima koji mogu imati negativan uticaj na poslovanje, tj. poslovni koncept u kome je primenjena poslovna informatika, a pre svega informacioni sistemi utemeljeni na informacionoj infrastrukturi i digitalnim tehnologijama. U uslovima digitalne ekonomije i sve masovnije primene digitalnih tehnoloških rešenja, svi informatički rizici, ujedno su i cyber rizici. Iako cyber rizici spadaju u podskup informacionih rizika, potrebno je istaći da oni predstavljaju rizike primene digitalne tehnologije u cilju osmišljavanja, sprovođenja, nadzora i upravljanja nad digitalnim poslovnim modelima (Čelik, P.2019:61-81).

U smislu toga, informacioni, tj. informatički rizici imaju dve sledeće važne karakteristike: uvek su prisutni i imaju dvostruku narav.

Može se stoga reći, da su informatički rizici, rizici stalne prisutnosti, pa je kontrolisanje tih rizika kroz mehanizme korporativnog upravljanja informatikom, ozbiljan izazov na putu postignuća strateških ciljeva poslovanja.

Kako informatički rizici imaju i dvostruku narav, ona se ogleda u sledećem:

- dobro vođene informacione inicijative kreiraju novu vrednost, nove poslovne prilike i održivu konkurentsku poziciju, odnosno prednost;
- loše vođene informacione inicijative destruktivno utiču na poslovanje kao celinu, ne stvaraju novu vrednost, urušavaju preostale poslovne resurse, proizvode poslovne gubitke i izazivaju ogorčenje kod zaposlenih, a time samo štetu i probleme.

Najvažniji činioci upravljanja informatičkim rizicima odnose se na učestalost određene pojave i težinu takve pojave izražene na poslovanje, čime informatički i cyber rizici proizilaze iz delovanja pretnji.

2. Osnovne vrste i obeležja rizika

Pretnje se obično dele, uzevši u obzir mesto njihovog nastanka, na unutrašnje, kao što su interna prevara, neovlašćeni pristup informacijama iznutra, krađa resursa informacionih sistema, greške pri unosu podataka u aplikacije, nesvesno odavanje poverljivih informacija i spoljne pretnje, kao što su hakerski napadi, zlonamerni računarski kod, socijalni, odnosno društveni inženjering, epidemije i pandemije bolesti, elementarne nepogode, itd.

Identifikovane pretnje je uvek potrebno staviti u kontekst resursa informacionog sistema i njegove ranjivosti, obzirom da bi ih pojedine pretnje mogle instrumentalizovati i na taj način izazvati poslovnu štetu.

Neki od primera ranjivosti mogli bi biti predočeni kroz nepostojanje zaštite od malicioznog koda, neprimerena, odnosno loša konfiguracija vatrenog zida (Firewall-a), nekontrolisan pristup poslovnim aplikacijama kroz zaobilaženje potvrđivanja korisničkog identiteta, kao i slučajevi u kojima zaposleni imaju nizak nivo svesti o bezbednosti informacionog sistema, nepostojanje ili neupotrebljavanje sistema za neprekidno napajanje električnom energijom, itd.

2.1. Strateški rizici

Poznavanjem ranjivosti, pretnji i njihovih štetnih efekata na poslovanje, rizici informacionih sistema se mogu proceniti kroz dva njihova temeljna svojstva:

- verovatnoću da će pretnje iskoristiti ranjivost informacionog sistema;
- nivo štetnog efekta koji može nastati u slučaju da pretnja zloupotrebi postojeću ranjivost.

Obzirom na specifična područja na koja se fokusiraju, razlikuju se sledeće vrste informatičkih rizika:

- strateški (korporativni) informatički rizici;
- rizici sprovođenja informatičkih programa i projekata;
- rizici sprovođenja poslovnih procesa (operativni ili transakcioni), informatički rizici;

- infrastrukturni informatički rizici.

Strateški, odnosno, korporativni informatički rizici, predstavljaju rizike neusklađenosti opšteg poslovanja i informatike, odnosno čine sve rizike koji imaju obeležja pretnje strateškim poslovnim interesima, bilo u smislu donošenja pogrešnih odluka, ili pak njihovog nedonošenja. Ovi informacioni rizici su na najvišem nivou upravljanja, usled čega oni kompaniji mogu pre svega doneti i finansijsku štetu i nenadoknadle gubitke. Navedeni rizici se često odnose i na propuštene prilike za korišćenje digitalne informacione tehnologije, koja je mogla doprineti povećanju poslovne efikasnosti ili novim strateškim inicijativama (oportunitetni trošak).

Ovde se, dakle radi o svim informatičkim rizicima koji su utemeljeni na propustima rada menadžmenta, a usled kojih kompanija nije spremna da postane, a time ni da ostane konkurentna i da kao takva prati trendove digitalne ekonomije i istoimene transformacije.

Primeri strateških informatičkih rizika su sledeći:

- rizik pogrešne informatičke strategije i rizik nastao usled njenog nedonošenja;
- rizik nastao usled nekompetentnosti menadžmenta u oblasti digitalne transformacije poslovanja;
- rizik nastao usled nespremnosti kompanije na promenu, posebno nespremnosti kompanije na disrupciju u poslovnom modelu;
- rizik nastao usled nespremnosti kompanije da transformiše svoje poslovanje u digitalno;
- rizik nastao usled neprimerene organizacione kulture u uslovima digitalne ekonomije;
- rizik nastao usled nepredvidive tržišne utakmice;
- rizik nastao usled promena u okruženju i tehnologijama;
- rizik nastao usled otežanog rada;
- rizik nastao usled tehnološke i infrastrukturne nespremnosti kompanije u domenu promene ili aktuelizovanja poslovnih modela;
- rizik nastao usled nekompetentnosti menadžmenta da vodi kompaniju u turbulentnim digitalnim ekonomskim uslovima;

- rizik nastao usled nedostatka znanja i kompetencija menadžmenta u domenu korporativnog upravljanja informatikom;
- rizik nastao usled toga da menadžment ne razume ulogu i značaj informatike u savremenom poslovnom okruženju, odnosno u savremenom poslovanju;
- rizik nastao usled implementacije informacionih sistema u slučaju spajanja i preuzimanja kompanija na tržištu;
- rizik nastao usled propadanja informacionih projekata ili drugih kapitalnih investicija;
- rizik nastao usled pogrešnih ulaganja u informatičku funkciju preduzeća;
- rizik nastao usled nepoštovanja zakonskih propisa i obaveza kompanije iz domena informatike, itd.

2.2. Rizici sprovođenja informacionih programa i projekata

Rizici sprovođenja informatičkih programa i projekata, po svojoj suštini predstavljaju rizike ulaganja u informatiku. Samim tim, to su rizici koji proističu iz verovatnoće da ulaganje u informatiku neće biti ispravno vođeno, čime uključuje rizike i da implementiranja tih ulaganja kroz informatičke projekte i programe neće biti efikasno, a to znači da neće doprineti stvaranju nove vrednosti odnosno ispunjenju postavljenog cilja.

Rizici sprovođenja poslovnih procesa, tj. operativni, transakcioni i informatički rizici jesu svi rizici koji se tiču primene informacione tehnologije u redovnom sprovođenju poslovnih procesa. U ovu kategoriju možemo ubrojati sve operativne informatičke rizike na koje se treba kritički osvrnuti, sve u cilju da bi se procesi iz domena poslovanja mogli odvijati na način koji je provereno bezbedan i pouzdan.

Tipični primeri ove vrste informatičkih rizika su:

- Bezbednosni informatički rizici, rizik fizičke i logičke bezbednosti sistema;
- Rizici neprekidnosti poslovanja;
- Rizici sprovođenja informatičkih usluga.

2.3. Rizici sprovođenja poslovnih procesa

Rizik sprovođenja poslovnih transakcija, najpre podrazumeva odgovore na pitanja da li su transakcije tačne, potpune, celovite, da li je ustrojena efikasna podela dužnosti, kontrola i ovlašćenja u radu.

U tom smislu nastaju sledeći rizici:

- Rizik nastao usled ometanja sprovođenja ili prekida poslovnih transakcija;
- Rizik nastao usled zamene softvera, tj. rizik usled pogrešne primene softvera;
- Rizik nastao usled neovlašćenog pristupa podacima i aplikacijama, odnosno rizik usled njihove izmene prilikom prenosa;
- Rizik nastao usled povrede integriteta tj. celovitosti podataka, tačnosti aplikacija, pouzdanosti i dostupnosti sistema i servisa;
- Rizik nastao usled neovlašćenog ubacivanja podataka u sistem, odnosno rizici usled pogrešnog unosa zbog nedostataka u pristupnim kontrolama informacionom sistemu;
- Rizik nastao usled nedostupnosti informacionog sistema;
- Rizik nastao usled oporavka informacionog sistema nakon neželjenog događaja;
- Rizik nastao usled gubitka pristupa podacima, rizik nečitljivosti, odnosno neupotrebljivosti dostupnih podataka nakon prekida ili drugog neželjenog događaja, itd.

2.4. Infrastrukturni informatički rizici

Informatički infrastrukturni rizici predstavljaju rizike rada informacione infrastrukture i opreme. Ovi rizici podrazumevaju i sve ostale rizike koji se odnose na redovno, odnosno uobičajeno funkcionisanje informacione infrastrukture. Informatički infrastrukturni rizici se odnose i na dostupnost i funkcionalnost računarske mreže, infrastrukturne podrške baze podataka, komunikacione infrastrukture, servisa elektronske pošte i svih ostalih informacionih servisa koje kompanija pruža u okvirima svog poslovanja.

Kao što je to nažalost prilično često, primera lošeg upravljanja različitim vrstama informatičkih rizika i dalje ima puno. Neretko se dešava i to da kompanije čije poslovanje zapravo leži na primenjenim informacionim tehnologijama i dalje nemaju adekvatno razvijen sistem

korporativnog upravljanja strateškim informacionim rizicima. Ovo zapravo znači da menadžment kompanije uopšte nije imao kompetencije iz oblasti upravljanja informatikom, niti je kod menadžmenta postojala svest o uticajima informacionog sistema na poslovanje, usled čega su se prema informatičkim projektima kompanije odnosili sa nepažnjom, što je proizvelo da je projekat zamene i dorade transakcionog sistema ili dugo, ili predugo čekao na dozvolu.

Često se događa i da rizicima sprovođenja poslovnih transakcija zapravo niko ni ne upravlja, pa samim tim nije nastao ni plan kontinuiteta poslovanja u slučaju neželjenog događaja. Prethodna situacija govori i da se nisu radile ni revizije funkcionisanja informacionog sistema u cilju pronalaženja grešaka i sprečavanja nastanka poslovnih problema. Svi ovi činoci bezrezervno utiču na to da takva kompanija u potpunosti nespremno dočeka probleme i rizike vezane za funkcionisanje informacionog sistema. Menadžment kompanije očigledno nije bio svestan problema i rizika za poslovanje, što bez razlike ima za posledicu da kompanija doživi poslovnu katastrofu sa ogromnom direktnim i indirektnim materijalnim i nematerijalnim štetama, pa i štetom od gubitka ugleda od kojeg se ovakve kompanije najčešće nikada ne oporave.

U aktuelnom tržišnom ambijentu gde ordinira žestoka konkurentska arena, ovakve kompanije, bez obzira na njihov inicijalni tržišni i finansijski potencijal, najčešće dožive tržišnu i poslovnu diskreditaciju, usled čega bivaju prodane nekoj drugoj kompaniji iz istog poslovnog segmenta po minimalnoj ceni i pod jako lošim uslovima. Drugi scenario je da kompanija koja je sebi dozvolila loše upravljanje informacionim rizicima jednostavno prestane da postoji kao pravni entitet, a sa tim prestaje da živi i njena ideja i uloga namenjena tržištu.

Iz ovih razloga je potrebno objasniti rizik kontinuiteta poslovanja i oporavka od neželjenog događaja u smislu njegovog izvornog pojmovnog značenja. Naime, upravljanje kontinuitetom poslovanja (Business Continuity), kao poslovni proces, čini ceo skup aktivnosti, pravila i procedura, prema kojima se preventivno deluje u okvirima kompanije u cilju sprečavanja pojava neželjenih i štetnih događaja u poslovanju. Pored toga, upravljanje kontinuitetom poslovanja podrazumeva i skup reaktivnih mera koje se primenjuju prema matrici postupanja u slučaju njihovog nastanka. Ovim procesom se suštinski angažuju različiti poslovni resursi, od ljudskih do materijalnih, kako bi se uspostavila neprekidnost poslovnog procesa, a time redukovao i poslovni rizik koji proizilazi iz iznenadnih prekida ključnih poslovnih funkcija ili procesa, ali i njihovog otežanog funkcionisanja.

Osnovna svrha i cilj upravljanja neprekidnošću poslovanja jeste da omogući siguran kontinuitet poslovanja ukoliko dođe do neočekivanog ili nepredviđenog događaja, otežanog rada ili ispada informacionog sistema kompanije. Drugi značajan deo ovog procesa, jeste da on omogući efikasan i brz oporavak i najbrže moguće reuspostavljanje poslovanja nakon štetnog događaja - Disaster Recovery (Spremić, 2007:310) .

Osim reaktivnih mera koje kanališu postupanje u slučaju nastanka iznenadnog štetnog događaja, ključni smisao procesa upravljanja neprekidnošću poslovanja, jeste da se putem njega ustroje odgovarajuće preventivne mere kojima će se sprečiti nastanak ili smanjiti verovatnoća fatalnog poslovnog ishoda.

Rizik prekida poslovnog kontinuiteta spada u izuzetno važne poslovne rizike u domenu upravljanja, a to su rizici kojima su izložene bezmalo sve kompanije koje koriste informacione tehnologije i sisteme za odvijanje ključnih poslovnih procesa. Obaveza najviših organa upravljanja u kompaniji je da ustroje jasne mehanizme upravljanja kontinuitetom poslovanja, da utvrde potencijalne štete i neželjene događaje koji bi mogli biti uzrok prekida poslovnih procesa, ili uzrok njihovog otežanog odvijanja. Njihova obaveza je takođe da u tom smislu odrede i konkretne protivmere za opisani slučaj i to kroz kontrolne i organizacione mere definisane kroz korporativna pravila, čime bi se smanjio ili ublažio uticaj nepovoljnih događaja na poslovanje i ukupnu poslovnu funkciju.

Okruženje digitalne ekonomije i poslovanja podrazumeva i stalnu i intenzivnu primenu digitalnih tehnologija u svakodnevnom sprovođenju poslovnih transakcija. Intenzivna primena digitalnih tehnologija u današnje vreme donosi brojne benefite u poslovanju, međutim, ako se njima ne upravlja adekvatno, mogu nastati brojni bezbednosni problemi i incidenti koji će kao takvi bitno ili u celosti ugroziti poslovanje i stvoriti štetu.

U današnje vreme se još uvek može sresti paradoks u kome se još uvek javljaju poslovni entiteti u kojima se informacioni deo poslovne funkcije bez ikakvog opravdanja percipira odvojenom funkcijom od poslovanja uopšte, a u tom smislu neki idu do toga da se informatika u poslovanju posmatra samostalnim kontrolnim okruženjem. Stoga, pitanje upravljanja informacionim rizicima nije samo tehnološki problem, ali ni problem koji treba samostalno rešavati isključivo ona organizaciona jedinica kompanije koja je zadužena za informatiku, već se ovde radi o

poslovnom problemu koji se mora što hitnije prepoznati na korporativnom nivou kako bi se njime efikasno upravljalo sa što manjim posledicama.

Sve napred izneto ukazuje na apsolutnu nužnost za ustrojavanje modela korporativnog upravljanja informacionim rizicima, kako bi on obuhvatio, pored ljudi i infrastrukturu, podatke, ali i poslovne politike i procese.

3. Plan upravljanja informatičkim rizicima

Upravljanje informatičkim rizicima predstavlja osetljiv i sistematičan analitički proces, kojim organizacija otkriva (pronalazi), prepoznaje (identifikuje), umanjuje (redukuje) i nadzire (kontroluje) potencijalne rizike i gubitke kojima je izložena (Panian, Spremic, 2007).

Osnovni cilj ovog procesa je da otkrije i identifikuje slabosti u organizaciji i sistemu, da proceni nivo opasnosti kojem su izloženi resursi poslovanja i ponudi racionalan, izvodljiv i troškovno efikasan način smanjivanja njihovog intenziteta. Ovakav proces omogućava organizacijama da utvrde veličinu, tj. ozbiljnosti težine i razmera, kao i učinaka potencijalnih gubitaka i time verovatnoće da će se takav gubitak eventualno i dogoditi. Uz to, taj proces podrazumeva i protivmere koje mogu delovati na smanjenje verovatnoće ili obima gubitka, usled čega je osnovni zadatak procesa upravljanja rizikom taj da se sistemskim metodama i merama održava poželjni nivo bezbednosti poslovanja, odnosno održava prihvatljiv nivo širokog dijapazona mogućih rizika, kojima je poslovanje, kao kontinuirani radni proces, izloženo.

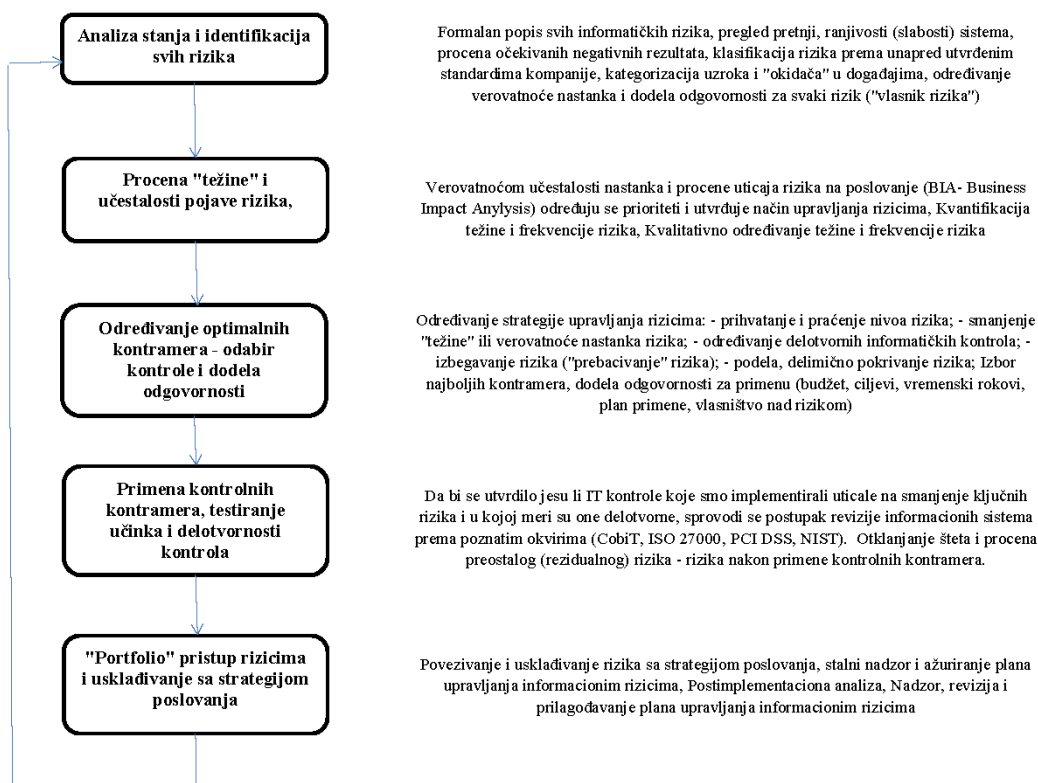
Prihvatljiv nivo rizika je rizik intenziteta koji je još uvek na nivou da ne ugrožava odvijanje važnih poslovnih funkcija i procesa, odnosno, još uvek ne ugrožava ostvarenje uspostavljenih poslovnih ciljeva kompanije. Važno je stoga napomenuti, da u okolnostima savremenog poslovanja koje je u celosti povezano sa informacionim sistemima, najčešće ne možemo postaviti čvrstu granicu među organizacijama, usled čega se pitanja informatičkih rizika protežu i na dobavljače, poslovne partnere, kupce, itd.

Istovetno je važan i obratni smer ranjivosti, obzirom da je npr. ranjivost informacionog sistema dobavljača u potpuno povezanom digitalnom poslovnom okruženju apsolutni izvor rizika, koji kao takav može izložiti i informacioni sistem matične kompanije. Samim tim, podizanje svesti i nivoa znanja o sistemskom praćenju informacionih rizika, presudan je segment u gotovo svim

organizacijama koje na bilo koji način u svom radu i poslovanju koriste poslovne informacione sisteme.

Plan upravljanja informacionim rizicima predstavlja sistemski proces koji sadrži sledeće korake:

- utvrđivanje odnosno, identifikovanje svih informacionih rizika;
- određivanje nivoa, odnosno intenziteta informacionih rizika kroz procenu njihove težine na poslovanje i imovinu kompanije, te učestalost njihovog pojavljivanja;
- određivanje optimalnih protivmera u odnosu na utvrđene rizike kroz postavljanje informacionih kontrola;
- dodela odgovornosti i sprovođenje informatičkih kontrola uz adekvatno dokumentovanje situacije;
- stalni nadzor, revizija plana upravljanja informacionim rizicima i usklađivanje sa strategijom poslovanja.



Slika br.16 Faze i koraci u upravljanju informatičkim rizicima

3.1 Identifikacija i klasifikacija rizika

Identifikacija i klasifikacija upravljanja informacionim rizicima predstavlja početni, a veoma često i najteži deo izrade plana upravljanja ovim rizicima. Ovakva aktivnost, ne odnosi se samo na formalni popis svih informatičkih rizika, već i na pregled pretnji, slabosti sistema, očekivanih negativnih efekata, klasifikaciju prema unapred utvrđenim organizacionim pravilima, kategorizaciju uzroka i okidača događaja, određivanje verovatnoće nastanka i dodelu odgovornosti za rizik.

Osnovni cilj identifikovanja svih informatičkih rizika jeste procena njihovog uticaja na poslovanje i klasifikaciju, kako prema nivou kritičnosti, tako i verovatnoći nastanka, odnosno učestalosti pojavljivanja rizika. Stoga, većina tih rizika spada među poslovne, odnosno upravljačke rizike, koji „pogađaju“ različite hijerarhijske nivoe u poslovanju organizacije. Da bi se adekvatno, tj. kvalitetno upravljalo rizicima, moraju se razviti mehanizmi stalnog praćenja poslovne izloženosti raznim vrstama rizika i njihovih ključnih pokazatelja.

U tom slučaju, ako bi se nekim poslovnim rizicima, ili rizicima nižeg prioriteta i nivoa kritičnosti, neprimereno upravljalo, oni veoma brzo mogu prevazići postavljene hijerarhijske stepenice i izazvati ogromne štete i gubitke. Proces određivanja informatičkih rizika uvek započinje sa definisanjem njihovog delokruga, odnosno granica i delova informacionog sistema.

U ovom koraku je od presudne važnosti prikupljanje što veće količine podataka o informacionom sistemu čije bi rizike korišćenja trebalo definisati, tj. odrediti. U smislu toga, potrebno je rutinski prikupiti podatke o hardveru, softveru, podacima, mreži, povezanosti delova sistema, zaposlenima koji koriste i održavaju sistem, misiji, viziji sistema, strateškoj važnosti sistema za organizaciju i korisnicima sistema, kao i dodatne podatke o tome koje funkcije i nivoe funkcionalnosti sistem mora omogućiti u svako doba, kakva je bezbednosna arhitektura sistema, kakav je protok informacija, kakav je način obrade podataka, kakve su menadžerske kontrole, kakve su manuelne i automatizovane kontrole, kakva je logička i fizička bezbednost, itd., tj. prikupiti precizne podatke o celokupnom informatičkom okruženju.

Tehnike kojima se stručnjaci, najčešće revizori informacionog sistema u ovom pravcu služe, jesu ankete, upitnici, razgovori sa ključnim korisnicima sistema i menadžmentom, pregled dokumentacije i stručno opažanje anomalija u radu informacionog sistema.

3.2 Procena težine rizika

Nakon sticanja dobrog uvida u način rada sistema, njegove granice i zahteve koji su pred njega postavljeni, potrebno je odrediti ključne varijable funkcije rizika, kao što su imovina, pretnje i ranjivost. Imovina je sve ono što kompanija poseduje i što za nju ima poslovnu vrednost. Imovina informacionog sistema predstavlja poslovnu vrednost njegovih sastavnih delova, a može biti materijalna i nematerijalna. Za neke od njih, kao na primer hardver, lako je odrediti i upotrebnu i poslovnu vrednost, dok je za ovu drugu, neopipljivu, odnosno nematerijalnu imovinu, kao što su softver ili podaci, teže proceniti stvarnu vrednost, a samim tim i potencijalni gubitak ili posledicu nastalu po osnovu njih.

Pretnja se definiše kao mogućnost ili namera nekog lica da preduzme određene radnje koje nisu u skladu sa ciljevima organizacije. Izvori pretnji u tom smislu mogu biti:

- Prirodni, koji podrazumevaju prirodne katastrofe, zemljotrese, poplave i sl.;
- Ljudske greške, odnosno činioci unutar poslovne organizacije, čije pretnje nastaju namernim ili slučajnim greškama koje učine ljudi, najčešće nezadovoljni zaposleni u organizaciji. Tipični primeri navedenog su neovlašćena upotreba resursa poslovnih informacionih sistema, ali i zaraza sistema računarskim virusima ili slučajno brisanje važnih podataka;
- slučajni događaji ili nenamerna aktivnost, predstavljaju situaciju u kojoj su bez namere pokrenuti događaji koji mogu prouzrokovati slabost sistema. Ovakva situacija može biti proizvedena putem bilo koje nehotične aktivnosti korisnika, kojom je na primer došlo do brisanja važnih podataka, promene u svojstvima sistema, greške u radu sistema, upada u sistem bez namere činjenja štete, nepridržavanje preuzetih obaveza, itd. Iako se ovde radi o nenamernim, slučajnim ili nehotičnim greškama, one mogu u velikoj meri ugroziti rad sistema i izložiti ga riziku. U ovu kategoriju rizika, spadaju i moguće prirodne katastrofe kao što su požari, poplave, oluje i sl., na koje nemamo previše uticaja, ali možemo bar donekle predvideti njihove domete i štete i preduzeti odgovarajuće, odnosno neophodne preventivne mere koje će sprečiti moguće posledice;
- namerno pričinjenu štetu ili ugrožavanje rada informacionog sistema čine namerni napadi na imovinu sistema, napadi računarskim virusima sa ciljem pričinjenja direktne štete ili

ometanja rada, napadi sa ciljem neovlašćenog upada u sistem i pričinjenje štete u smislu promene podataka, promene programskog koda, itd.;

- činioci iz okruženja poslovne organizacije, kao što su nestanak struje, terorizam, poslovna konkurencija, špijuni, kriminalci, računarski hakeri i sl.

Nakon što je organizacija postala svesna svih pretnji i potencijalnih neželjenih događaja koji mogu ugroziti neometan rad njenog sistema, nužno je odrediti slabosti, odnosno ranjivosti sistema. Ranjivost je svaka moguća slabost bilo kog dela imovine, odnosno poslovne organizacije ili slabost neke njene zaštitne mere. Ranjivost predstavlja relativnu meru kojom se procenjuje nivo efikasnosti kontrola unutar pojedinih delova informacionog sistema. Stoga, kada je u pitanju ranjivost, ona se odnosi na nedostatak ili oslabljenost sistema i njegovih ključnih delova (procedure i bezbednosnih politika, dizajna, algoritma, ključnih aplikacija), ili internih kontrola koje namernim ili nenamernim delovanjem mogu prouzrokovati bezbednosni incident ili povredu bezbednosne politike.

Tipični primeri slabosti, odnosno ranjivosti informacionog sistema mogu biti loše logičke i fizičke kontrole, neprimerena ili neefikasna poslovna praksa, loše koncipirani poslovni ugovori, itd. Samim tim, što su automatske ili manuelne implementirane kontrole efikasnije, to je nivo ranjivosti sistema niži. U tom slučaju kontrole koje su ugrađene u informacioni sistem sprečavaju da se neka pretnja uopšte i dogodi, ili ako se ona ipak dogodi, da njen uticaj na poslovanje bude minimiziran.

Postupanjem na opisani način, direktno se smanjuje verovatnoća, a time i mogućnost nastanka pretnji, a usled toga i njihov negativan učinak na imovinu organizacije i njenih podsistema. Sa druge strane, primena mehanizama kontrole zahteva određena finansijska sredstva, usled čega je neophodno pre donošenja takvih odluka sprovesti i odgovarajuću procenu nivoa ugroženosti i utvrditi njihovu potencijalnu finansijsku vrednost, odnosno težinu.

Informacioni rizici, u skladu sa navedenim, predstavljaju verovatnoću nastanka nekog neželjenog događaja, u suštini pretnje, koja u datim okolnostima može izazvati štetu, zastoj ili umanjenu intenzitet rada informacionog sistema ili pak štetu u odnosu na informacije koje su u sistemu pohranjene.

Primer takvog neželjenog događaja, odnosno pretnje koja predstavlja informacioni rizik, može biti napad računarskim virusima. Ovakva pretnja u realnim okolnostima neprekidno postoji i kao takva se može ostvariti u svakom trenutku. Ipak, ako je neka kompanija primenila odgovarajuće kontrolne protivmere, pa na primer koristi uvek ažurne verzije antivirusnog softvera sa važećom licencom i ima definisane odgovarajuće organizacione procedure, tj. pravilnike o antivirusnoj zaštiti, tada je ranjivost sistema na nižem procenjenom nivou, nego kada bi to bilo tako da se te protivmere ne sprovode, ili da nisu efikasne. U tom smislu, čak i kada pretnja realno postoji, njen negativan učinak na imovinu sistema, na primer podatke u njemu, neće biti toliko izražena, pa samim tim ovoj kombinaciji imovine, pretnje i ranjivosti, koja čini rizik napada kompjuterskim virusom, donekle možemo pripisati niži nivo.

Uticaj koji takav neželjeni događaj može imati na poslovanje organizacije, meri se veličinom i obimom štete koja može nastati, radi čega je veoma važno odrediti, kako težinu, tako i učestalost pojavljivanja informatičkih rizika. Da bi došlo do utvrđenja verovatnoće pojave ovakvog neželjenog događaja, potrebno je sistemski analizirati sve pretnje koje proizilaze iz korišćenja informacionih sistema i informacione tehnologije (ukupni rizik), a onda iste dovesti u vezu sa potencijalnim ranjivostima (slabostima sistema) i odrediti u kojoj meri se taj rizik može tolerisati, pa u odnosu na sve to zajedno opredeliti kontrole kojima će se takve slabosti ublažiti ili svesti na prihvatljivi nivo.

Procena intenziteta informacionih rizika, po pravilu se obavlja primenom kvantitativnih i kvalitativnih mera, tzv. metrikama. Cilj upotrebe kvantitativnih metrika jeste procena mogućih direktnih finasijskih gubitaka nastalih kroz delovanje određenog informatičkog rizika. Pri tome, radi se o subjektivnoj proceni koja može u manjoj ili većoj meri biti realna i objektivna, odnosno u manjoj ili većoj meri utemeljena na realnim događajima, pretnjama, ranjivostima i potencijalnim posledicama.

U svakom slučaju, procena nivoa informatičkih rizika je vrlo složen i zahtevan zadatak, tj. zadatak koji najčešće obavlja radna grupa sastavljena od analitičara rizika koji funkcionišu uz podršku izvršnog segmenta menadžmenta. Stoga je prilično korisna poslovna praksa upravo ona koja određuje mehanizme i pravila kojima se sprovode takve procene, kao npr. metodologija upravljanja rizicima, pravilnik za procenu nivoa rizika i sl., pa se u te aktivnosti radi njihove ukupne efikasnosti moraju obavezno uključiti i stručni saradnici i zaposleni.

Tabela br.7 Primer procene nivoa informacionih rizika i utvrđivanja strategije odgovora na rizike

Verovatnoća nastanka neželjenog događaja (ranjivost sistema)					
Uticao – nivo „ozbiljnosti“ neželjenog događaja	A Vrlo moguća	B Moguća	C Povremena	D Retko moguća	E Gotovo nemoguća
I (visoka)					
II					
III					
IV (niska)					

	Rizik 1	Neprihvatljiv, kritičan, vrlo moguć i zahteva trenutnu reakciju top menadžmenta
	Rizik 2	Neprihvatljiv, zahteva korektivnu akciju i uključivanje višeg sloja menadžmenta
	Rizik 3	Prihvatljiv uz praćenje i izveštavanje menadžmenta
	Rizik 4	Prihvatljiv, bez potrebe uključivanja menadžmenta - rešiv na postojećem nivou upravljanja

Kvantitativne metode informacionih rizika, najčešće se odnose na utvrđivanje brojčanih vrednosti koje odgovaraju obeležjima rizika i najčešće se temelje na proceni vrednosti direktne i indirektno štete koja može nastati, ukoliko bi došlo do neželjenog događaja. Tipičan primer kvalitativnih mera može biti kritičan, visok, srednji i nizak nivo rizika. Na primer, ako je informatički rizik procenjen na kritičan nivo, to znači da je neželjeni događaj vrlo verovatan, a to dalje implicira da je ranjivost sistema prilično velika, obzirom da ne postoje kontrolne mere koje bi sprečile njegov nastanak ili razmere štete.

Samim tim, ovakav informacioni, tj. informatički rizik može izuzetno negativno uticati na poslovanje, iz čega može proizaći veliki direktan finansijski gubitak. U ovakvom slučaju bi temeljnim organizacionim merama trebalo propisati obavezu upravljanja ovim rizicima od strane najvišeg menadžmenta kompanije. Tako, nakon utvrđivanja izvora pretnji, sledi procena verovatnoće nastanka i samim tim izračunavanje ozbiljnosti neželjenih događaja, koje kao takvo sadrži što je više moguće precizniju estimaciju potencijalnog gubitka u slučaju nastanka neželjenog događaja. Iza toga sledi razrada scenarija informatičkih rizika kako je to prikazano prethodnom tablicom, usled čega se određuju prioriteta i utvrđuje način upravljanja rizicima.

3.3. Određivanje protivmera i scenariji upravljanja rizicima

Tipični scenariji upravljanja informacionim rizicima, tj. strategije odgovora su:

Prihvatanje rizika - jeste slučaj kada je organizacija upoznata sa intenzitetom rizika, iz kog razloga ga stalno nadzire i u skladu sa propisanim korporativnim pravilima konstantno procenjuje njegov uticaj na poslovne procese i poslovanje. Kada prema propisanim korporativnim pravilima nivo uticaja rizika na poslovanje postane neprihvatljiv, preduzimaju se propisane mere za smanjenje rizika.

Smanjivanje intenziteta rizika - je slučaj kada organizacija preduzima odgovarajuće aktivnosti kojima smanjuje uticaj rizika na poslovanje. Tada organizacija smanjuje ozbiljnost rizika i verovatnoću njegovog nastanka, čime se zapravo smanjuje ranjivost sistema. U oba slučaja od suštinskog značaja je implementiranje usmerene kontrole, kako bi se time intenzitet pretećeg rizika smanjio.

Izbegavanje rizika – je slučaj kada u skladu sa korporativnim pravilima organizacija delimično ili u potpunosti izbegava potencijalni rizik.

Podela rizika – je slučaj kada organizacija preusmerava, odnosno vrši transfer rizika na neku drugu stranu, pa na primer u odnosu na rizik kupuje polisu osiguranja i upravljanje rizika vrši tako što pod komercijalnim uslovima iznajmljuje usluge druge specijalizovane kompanije. Sledeći čest primer je kada kompanija stvara partnerstva sa drugim kompanijama, u kom slučaju tako regulišu upravljanje kontinuitetom poslovanja.

U zavisnosti od rezultata procene uticaja rizika na poslovnu funkciju, analiziraju se različiti scenariji upravljanja ovim rizicima. Na primer, ako postoji rizik koji je velike verovatnoće, jer efikasne kontrole ne postoje, to može potencijalno kritično uticati na poslovanje, pa taj scenario zahteva promptnu reakciju najviših nivoa menadžmenta kroz strategiju smanjenja intenziteta rizika, dok u slučaju poznatog rizika koji je već identifikovan i već se prati njegov uticaj na poslovanje, nikakva dodatna akcija nije potrebna, osim jasne korporativne procedure kojom je određeno ko je neposredno odgovoran za stalno praćenje pokazatelja ovog rizika i izveštavanje o njima viših nivoa menadžmenta, što bi samo po sebi predstavljalo strategiju prihvatanja rizika i stalnog praćenja njegovog nivoa.

Opšte IT kontrole	Kontrole putem aplikacija
Korporativne kontrole	Preventivne kontrole
Upravljačke kontrole	Detektivne kontrole
Operativne kontrole	Korektivne kontrole

Tabela br. 8 Podela informatičkih kontrola

Scenariji upravljanja rizicima u najvećoj meri se odnose na određivanje odgovarajućih vrsta informatičkih kontrola, tzv. manuelnih, poluautomatskih ili potpuno automatskih kontrola informacionih sistema. Podela kontrola se može definisati i u smislu objekta kontrole, pa se ona može podeliti na opšte, IT i aplikacione kontrole koje se po načinu delovanja mogu podeliti na preventivne, detektivne i korektivne, a onda u odnosu na hijerarhijsku poziciju na koju se odnose, na korporativne, upravljačke i operativne kontrole.

Informatičke kontrole su veoma važna tema u području upravljanja informacionim rizicima. Menadžment kompanije u saradnji sa menadžmentom informacionih sistema, direktno je odgovoran za oblikovanje, sprovođenje i ocenu efikasnosti sistema internih kontrola informacionih sistema, dok je zadatak korporativnog nivoa upravljanja da odredi pravila igre i poželjnu, tj. obaveznu praksu postupanja. U svetskim razmerama već izvesno vreme postoje koordinisane inicijative koje su usmerene ka standardizaciji okvira internih kontrola, pri čemu se može zaključiti da efikasna kontrola poslovanja ni u kom smislu nije moguća bez efikasnog sistema internih kontrola informacionog sistema, kao što su ISO 27000, CobiT, ITIL, itd.

3.4 Omeđivanje odgovornosti i provera sprovođenja kontrole

Nakon sprovedene analize rada informacionih sistema, uticaja informacionih rizika na poslovanje, utvrđivanja upravljačkih scenarija, dodele kontrola i određivanja strategija odgovora, sledi celokupan pregled aktivnosti upravljanja informacionim rizicima.

U narednoj tabeli prikazan je primer pregleda rezultata plana upravljanja informacionim rizicima i oblika izveštavanja koji je primeren različitim nivoima upravljanja.

Rizik	Uzrok/Opis rizika	Uticaj-ozbiljnost rizika	Verovatnoća rizika	Potencijalni gubitak	Strategija odgovora	Kontrola	Odgov. lice
Prekid rada sistema	Spoljni uticaj ili usled grešaka u aplikacijama i opremi	Gubitak podataka usled kritičnog prekida u poslovanju	12 – 17%	500.000 RSD	Hitna akcija radi smanjenja intenziteta rizičnog događaja i njegovih posledica	-CobiT DS4 -ITIL BCM -ISO 27001	XYZ

Tabela br. 9 Hipotetički primer pregleda rezultata plana upravljanja informacionim rizicima

3.5. Stalni nadzor i revizija plana

U slučajevima poslovnih okruženja u kojima informacioni sistemi integrišu poslovne funkcije i procese, oni istovremeno predstavljaju i osnovu modela poslovanja. Time su se stvorili neophodni infrastrukturni i organizacioni preduslovi za stratešku primenu informatike u poslovanju. Savremene digitalne informacione tehnologije se sve više ugrađuju u postojeće proizvode, usled čega stvaraju nove potrebe i odgovarajuće usluge, a time nepovratno menjaju poslovne procese i delatnosti, dok upotreba i efikasno upravljanje informacionim sistemima, čiji su digitalne tehnologije sastavni deo, ostaju ključna pitanja funkcionisanja i razvoja kompanije.

Usled ovih poslovno-tehnoloških okolnosti, nije novina plaćanje parkinga ili pregled dostupnosti najbližih parking mesta posredstvom mobilnog telefona. Više nije neočekivano ni to da se pokretanjem mobilne aplikacije koja uz određene prostorne, tehnološke i infrastrukturne pretpostavke može omogućiti da vaš automobil sam pronade parking mesto u posebno opremljenoj garaži i javi vlasniku gde je parkiran, ako mu zatreba. Šef smene u nekom od velikih supermarketa može šetati među policama i zahvaljujući RFID tehnologiji, na ekranu ručnog terminala bežičnim putem pregledati karakteristike proizvoda koji se na njima nalaze, što bi uključivalo stanje zaliha, rok trajanja i sl. za sve pojedinačne proizvode.

Sva ova i brojna druga obeležja savremenih poslovnih procesa, ne bi bila moguća bez veoma efikasne i mehanički tačne primene informacionih sistema u poslovanju, pa to sve zajedno čini obeležja primene informacionih sistema kao strateškog partnera u poslovanju. Samim tim radi se o poslovnoj funkciji čija efikasna i intenzivna primena može doprineti digitalnoj transformaciji i kroz nju poboljšati rezultate poslovanja. Poboljšani rezultati poslovanja ogledaju se kroz niže troškove, diferencijaciju, rast, povezivanje kompanija sa okruženjem, bolju konkurentsku poziciju, inovaciju modela poslovanja, stratešku promenu procesa poslovanja, kreiranje digitalnih platformi poslovanja, nepovratnu promenu organizacione strukture u pojedinim industrijama, itd.

U takvoj konstelaciji, informatika zauzima sve istaknutije mesto u organizacionoj strukturi kompanije, dok istovremeno funkcija menadžera informatike (CIO) pripada najvišem nivou menadžmenta, imajući u vidu da se digitalno ekonomsko okruženje u stvaranju nove ili dodatne poslovne vrednosti najviše oslanja na informaciono-digitalne tehnologije.

Interaktivni sinergetski potencijal i „narav“ digitalne tehnologije, da bi se kreirala nova ili dodatna vrednost, zahteva da informacioni sistemi, pored unutrašnjih formalnih i neformalnih, koriste i brojne spoljašnje izvore resursa oslonjene na digitalne tehnologije, najčešće u vidu senzora, interneta stvari, društvenih mreža, računarstva u oblacima, itd.

Upravo radi široke mogućnosti interakcije sa okolinom, kao i radi mogućnosti integracije sa ostalim odvojeno razvijanim tehnologijama, informacione i komunikacione tehnologije, a posebno novije digitalne tehnologije možemo smatrati pokretačima digitalne ekonomije i pokretačima sve ubrzanijeg razvoja informacionih sistema, preko kojih se u digitalnoj ekonomiji sprovode poslovne transakcije. Ipak, ovo apsolutno ne znači da se pri upravljanju IT-em više ne možemo oslanjati samo na unutrašnje činioce. Koncept savremenog korporativnog upravljanja informatikom počiva na dva nivoa i to: strateškom i operativnom.

Kada je u pitanju strateški, odnosno korporativni nivo IT upravljanja, on je usmeren na spoljašnje okruženje, strateško promišljanje i vizije digitalnih platformi poslovanja, kojima će se pokriti interes svih zainteresovanih strana.

Kada je u pitanju operativni, mahom tehnološki nivo IT menadžmenta, on se odnosi na unutrašnje poslovno okruženje, administriranje, tj. upravljanje poslovanjem uz pronalaženje najboljih tehnoloških i administrativnih rešenja u smislu toga kako da se određeni inovativni poslovni model sprovede u delo.

Korporativno upravljanje informatikom predstavlja skup pravila, metoda i mehanizama kojima se strateški povezuje poslovanje i informatika i na taj način omogućava njena intenzivna primena, koja kao takva treba da rezultira većom poslovnom vrednošću i samim tim poboljšanim rezultatima poslovanja. Bez obzira na različitost pojmova koji se upotrebljavaju u ovoj oblasti, po njihovoj prirodi možemo zaključiti da se tu radi o kontinuiranom pristupu osmišljavanja i sprovođenja inovativnih poslovnih modela koji funkcionišu uz intenzivnu podršku digitalne tehnologije i savremenih informacionih sistema. Na taj način se strateški povezuju samo poslovanje kompanije i mogućnosti koje donosi primena digitalnih tehnologija, sa ciljem kreiranja nove poslovne vrednosti i prilagođavanja poslovanja kompanije svim parametrima uspostavljene digitalne ekonomije. Sledstveno tome, korporativno upravljanje poslovno-informatičkom funkcijom čini set mehanizama, strateških inicijativa i kontrolnih procedura

kojima se obezbeđuje da se informatički potencijali upotrebljavaju u svrhu kreiranja nove, odnosno uvećane poslovne efikasnosti i vrednosti.

Koncept korporativnog upravljanja informatičkom funkcijom organizacije, bazira se na dva suštinska načela i to: načela upravljanja informatičkim rizicima (do kojih neminovno dolazi usled potrebe za upotrebom digitalne i informacione tehnologije) i načela stvaranja nove poslovne vrednosti kroz digitalizaciju poslovanja.

Prvo načelo, odnosno korporativno upravljanje informacionim rizicima, sastoji se od upravljačkih mehanizama koji smanjuju efekat pretnji, te se istim vrši implementacija kontrola kojima se upravlja nivoom bezbednosnih rizika, ali i greškama koje se ogledaju kroz neuspešne IT projekte.

Drugo načelo, tj. korporativno upravljanje vrednostima stvorenim od strane informatike u poslovanju, zapravo se odnosi na modele pomoću kojih se pokušava stvoriti što je moguće više nove vrednosti za poslovanje, kako za IT ulaganja, tako i upotrebe informatičkih resursa poslovanja.

Najvažniji ciljevi korporativnog upravljanja informatičkom funkcijom preduzeća stoga su:

- Stvaranje veće vrednosti i koristi za poslovanje, kroz ulaganja u digitalne i informacione tehnologije;
- bolje shvatanje i upravljanje rizicima primene digitalnih i informacionih tehnologija;
- bolje upravljanje svim informatičkim resursima kao što su infrastruktura, procesi, podaci i posebno ljudi, kako bi se strateški planovi digitalizacije poslovne funkcije i primene informacionih tehnologija mogli sprovesti u delo;
- podrška digitalizaciji poslovanja.

U ovom kontekstu treba napomenuti da postoji veliki broj primera iz prakse koji potvrđuju činjenicu da mnogi izvršni menadžeri i dalje nemaju dovoljno znanja, pa samim tim ni kompetencije u području veoma osetljivog korporativnog upravljanja informatikom. Nedavno istraživanje (PricewaterhouseCoopers, 2014) sprovedeno na uzorku od 863 izvršna menadžera, potvrdilo je napred iznetu tezu. Zaključak je da ovi menadžeri, iako smatraju da se najveći izazovi u savremenom vođenju poslovanja odnose na primenu digitalnih tehnologija i cyber

rizika, samo 49% njih je bilo uključeno u razvoj strategije informatike, dok je većina potpuno iskreno priznala da oni nemaju dovoljno kompetencija u ovom području.

S tim u vezi, ako informacione sisteme koristimo kao stratešku poslovnu funkciju, neophodan preduslov njihove efikasne upotrebe svakako će biti sprovođenje mehanizama korporativnog upravljanja informatičkom funkcijom i redovne provere njihovog kvaliteta, odnosno revizije informacionog sistema.

Revizijom informacionih sistema proverava se funkcionalnost, efikasnost i uspešnost njihove primene u poslovanju, a sve kako bi rizike primene informacionih sistema održavali na željenom, odnosno prihvatljivom nivou. Obzirom na rastuću složenost informacionih sistema, posebno radi međusobnog prožimanja digitalne i informacione tehnologije sa poslovnim procesima, njihova sve izraženija strateška uloga u poslovanju kroz automatizam odvijanja brojnih poslovnih procesa putem informacionih sistema, ali i ponude sasvim novih inovativnih informacionih usluga, učinila je neophodnim da informacioni sistemi moraju biti obuhvaćeni sistemskim organizacionim merama kontrole, kao i sistemima nadzora i provere kvaliteta.

4. Ranjivost informacionih sistema

Kvalitet informacionih sistema predstavlja relativnu kategoriju kojom se meri odstupanje njegove realne funkcije u odnosu na idealnu (Panian, 2001). To je odstupanje, odnosno zaostajanje realne funkcije sistema za idealnom funkcijom, pa je takav sistem kvalitetniji i obratno.

Informacioni sistemi se sastoje od niza međuzavisnih delova (hardware, software, dataware, lifeware, netware i orgware) koji koordinisano deluju u skladu sa postavljenim poslovnim zahtevima. Iz ovih razloga je merenje kvaliteta informacionih sistema veoma složen i zahtevan postupak u sklopu koga je potrebno utvrditi idealnu funkciju sistema i pregledati, a naravno i proveriti (revidirati) njegov trenutni nivo uspešnosti. Da bi se proverila uspešnost informacionih sistema, neophodno je dobro poznavati i proveravati uspešnost njegovih sastavnih delova i komplementarnost njihovih međudelovanja.

Osnovni činioci kvaliteta informacionih sistema su:

- Infrastrukturalna podrška i pripadajući software, tj. uređaji koji podržavaju rad informacionih sistema, računarska oprema i komunikaciona infrastruktura, zajedno sa sistemskim aplikativnim i komunikacionim softverom, koji kao takav omogućava njihov rad;
- transakcioni i ostali podaci, kao i dostupnost, celovitost i sigurnost podataka;
- metode i načini unosa i arhiviranja svih vrsta podataka;
- korišćenje, uticaj na poslovanje i funkcionalnost informacionih sistema;
- efikasnost podrške poslovnim transakcijama, delotvornost, podrška poslovanju, itd.;
- zadovoljstvo korisnika kroz jednostavnost korišćenja usled zrelosti informacionog sistema i podrške sprovođenju poslovnih transakcija.

Činioci kvaliteta informacionog sistema deluju koordinisano u skladu sa zahtevima poslovanja, a u skladu su sa komponentama informacionog sistema. Zakon minimuma kvaliteta informacionih sistema određuje da je kvalitet informacionog sistema jednak proizvodu nivoa kvaliteta svake njegove pojedinačne komponente, u smislu čega se isti svodi na kvalitet njegove najslabije karike u lancu. Ovo znači da se upravljanje nivoom kvaliteta informacionog sistema ostvaruje ravnomernim ulaganjem u razvoj svih njegovih delova, a ne prekomernim ulaganjem samo u pojedine komponente, što bi otvorilo prostor novoj ranjivosti informacionog sistema.

Revizija informacionog sistema je stoga analitička komponenta korporativnog upravljanja informatikom pomoću koje se proverava učinak informatike na poslovanje i sprovodi sveobuhvatna provera njegovog rada. Kroz merenje učinka informatike na poslovne procese može se proceniti i njihova ranjivost, usled čega se merenje učinka može odnositi i na sledeće parametre:

- Broj incidenata u određenom vremenskom razdoblju;
- broj aktivnih incidenata;
- prosečno vreme rešavanja incidenata;
- odnos broja i karakteristika incidenata otkrivenih sistemom nadzora u odnosu na ukupan broj incidenata;
- broj sprovedenih redovnih promena u realizaciji proizvodnje koje su prouzrokovale incident;

- broj vanrednih promena u realizaciji proizvodnje koje su prouzrokovale incident;
- broj promena na realizaciji proizvodnje koje nisu prijavljene kroz službenu proceduru;
- broj nastalih problema i ukupni broj incidenata koji su ih prouzrokovali;
- odnos identifikovanih i rešenih problema u određenom vremenskom razdoblju;
- broj problema čiji je uzrok nepoznat;
- odnos zahteva koji nisu preuzeti u rad, odnosno rešeni u predviđenom vremenskom roku u odnosu na celokupni broj zahteva.

Kvalitet informacionih sistema predstavlja relativnu kategoriju kojom se meri odstupanje njegove realne funkcije u odnosu na idealnu, dok je idealna funkcija informacionog sistema zadata zahtevima koje je prema tom sistemu odredilo poslovanje, a to se najčešće čini strateškim planom informacionih sistema (Panian, 2001).

Strateški plan informatike stoga mora biti usklađen sa strateškim planom poslovanja, usled čega poslovanje određuje koje to ciljeve i zadatke informatička funkcija mora ispuniti kako bi bila korisna i time strateška poslovna funkcija, a koja pritom mora odgovoriti na rizike, pretnje i ranjivosti.

5. Postupak optimizacije rizika

Poslednja decenija usled izloženosti pritisku informacionih inovacija i na njima zasnovanih poslovnih procesa, doprinela je da se čak i uobičajeni poslovni procesi usled informatičke izloženosti učine visokorizičnima, a istovremeno i potencijalno efikasnijim i višestruko isplativijim.

S tim u vezi, poslednja decenija bitno je promenila i samu narav rizika, pa se u tome i sveukupna percepcija informacionih rizika takođe u velikoj meri promenila. Dijapazon ovih rizika počeo se kretati od uobičajene prevencije izolovanih neželjenih događaja, koji kao takvi nemaju bitnijeg uticaja na poslovanje, a o kojima se u smislu uobičajene prakse pažnja posvećivala od strane menadžera određenih po funkciji, pa sve do današnjih tj. modernih rizika koji su usled sveopšte tehnološke prisutnosti došli do direktnog uticaja na ključne poslovne procese.

U tom smislu, nastala je neophodnost da se osmisle i implementiraju integrisani modeli korporativnog upravljanja ovim rizicima. Primeri za to su brojni i svi ukazuju na veoma ozbiljne

uticaje ovih rizika na poslovanje. U tom smislu može se pomenuti i primer kompanije Cisco, koja je svetski lider u oblasti IT-a i umrežavanja, kojoj, ako bi se dogodilo da njen informacioni sistem postane nedostupan čak i na samo jedan dan, menadžment i korporativna nadzorna tela ove kompanije, pretpostavljaju da bi kompanija u takvom slučaju imala izgubljen prihod od oko 70 miliona američkih dolara (Nolan, McFarlan, 2005).

Ovaj vid štete predstavlja samo direktnu štetu, međutim, postoji i indirektna šteta, koja bi pored ostalog proizvela gubitke u smislu pada vrednosti akcija na tržištu u tom periodu, čime bi se ovaj rizik prelio na daleko veći ukupni gubitak, koji bi, obzirom na vrednost kompanije i njenih deonica, mogao dostići čak i vrednosti u iznosima koji se mere milijardama američkih dolara.

Slična je situacija i ako bi došlo do prekida odvijanja informatičkih poslovnih procesa i u drugim industrijama, gde na primer, za samo jedan sat prekida poslovanja u brokerskoj, odnosno finansijskoj industriji, ukoliko bi do njega došlo, šteta na globalnom nivou može iznositi oko 6,5 miliona dolara, čime je jasno da visokorizičnost ovih izuzetno profitabilnih vidova poslovanja, zahteva i adekvatne odgovore.

Navedeno je dovelo i do potrebe pažljivog upravljanja ulaganjima u dostupne digitalne tehnologije i informatičke projekte, i to posebno u najuspešnijim kompanijama, shodno napred iznetim primerima. Praksa upravljanja informatikom i njenim izazovima poprilično se razlikuje od kompanije do kompanije, a rezultati istraživanja „potvrđuju da razloge slabog uticaja ulaganja u informatiku na produktivnost poslovanja treba tražiti i u često nedefinisanoj ulozi informatike u poslovanju“ (Spremic, Hlupic, 2007:4).

Nažalost, i dalje postoje kompanije u kojima ne postoji niko odgovoran za donošenje odluka vezanih za informatiku, pa i one kompanije u kojima i danas menadžment nije u stanju da opiše sam proces upravljanja informatikom, kao ni ulogu ni važnost ovog važnog segmenta na poslovanje u celini. Na ovom primeru se može razumeti da loša praksa upravljanja informatikom ima veliki uticaj na to da je poslovanje takvih kompanija podložno ogromnim rizicima, mogućoj direktnoj i indirektnoj finansijskoj šteti, a time i konkurentskom položaju tih kompanija na tržištu. Princip pokretanja reaktivnih mehanizama, umesto negovanja proaktivnih, zapravo predstavlja sistem bavljenja posledicama umesto uzrocima, što čini i u neku ruku objašnjenje da li su i koje kompanije u stanju vršiti uloge u domenu optimizacije rizika, imajući u vidu da

optimizacija rizika direktno zavisi od fenomena prepoznavanja rizika i identifikovanja njegovih specifičnosti u odnosu na implementirani model poslovanja.

Svođenje optimizacije rizika na ulaganje u hardver ili neki softver neće rešiti sve one organizacione probleme u kompaniji koji su nastali posredstvom informatičkih rizika, jer na taj način postaje više nego jasno da tehnološki trendovi na tržištu diktiraju primenu informatike u poslovanju, a ne samo poslovne potrebe, kako se to često smatra. Ovo zato, jer informatika ne predstavlja organizacioni „čarobni štapić“, kako to često loši menadžeri smatraju, usled čega ovakvo shvatanje poslovne informatike i njenih rizika u veoma kratkom roku dolazi na naplatu, bilo u vidu neisplativog informatičkog ulaganja, ili čak propalog informacionog projekta koji nije bio u stanju da odgovori na zahteve tržišta, potrebe kompanije i pretnje konkurencije.

„Najčešći razlozi neuspeha informatičkih projekata, tj. ulaganja u informatiku, jesu organizacione, a ne tehničke prirode i odnose se na:

- Nedovoljnu podršku od strane menadžmenta i nedovoljno dobro poznavanje poslovne strane informatike;
- nedostatak resursa;
- izostanak uključenja u projekat odgovarajućih korisnika;
- unutrašnji otpori informatičkom projektu i organizacionim promenama koje oni donose;
- loša analiza organizacije i poslovnih procesa;
- neusklađenost projekta sa poslovnim planovima;
- nejasna odgovornost za sprovođenje projekta;
- loš odabir informatičkih alata.
- loše predstavljanje rezultata“ (Spremic, 2002:309), što sve zajedno predstavlja elemente na osnovu kojih se može sagledati postupak optimizacije rizika.

6. Savremene pretnje i modaliteti ugrožavanja digitalnog poslovanja

Poslovni sistemi modernog doba, koji egzistiraju na tržištu, najčešće su izloženi širokom dijapazonu, bilo realnih, bilo potencijalnih rizika i pretnji, koji kao takvi imaju direktnog i indirektnog negativnog uticaja, kako na poslovanje, tako i uspešnost kompanije na tržištu.

Savremeni svet, političko, ekonomsko i digitalno poslovno okruženje, često izlažu kompanije učestalim društvenim promenama, neizvesnoj pravnoj i ekonomskoj situaciji, ograničenom

izboru kvalifikovane i profesionalne radne snage itd., što sve zajedno proizvodi čitav spektar bezbednosnih rizika i pretnji po sistem digitalnog poslovanja, usled čega ovi faktori, pored cyber kriminala, zahtevaju pridavanje adekvatnog značaja i pažnje.

Korporativna bezbednost, a time i sam koncept industrijske bezbednosti, prevazišli su u značajnoj meri svoje teoretske osnove, imajući u vidu da se kompanije bez obzira na njihovu delatnost i stepen prisutnosti na tržištu, bilo tradicionalnom ili digitalnom, dovode u situaciju da budu izložene raznim vidovima pretnji, pa se tu može navesti, pored ostalih i: industrijska špijunaža, sabotaza, konkurentske pretnje, pretnje finansijskim prevarama, itd., kako u tradicionalnom smislu, tako i u digitalnom poslovnom prostoru. U tom pravcu, u digitalnom poslovnom vokabularu, cyber pretnje imaju različita obličja i vidove i sledstveno stalnom inovativnom elementu ugrožavanja, sledeće popularne nazive: napredne uporne pretnje, reciklirane cyber pretnje, savremene cyber pretnje, insajderske pretnje, itd.

U smislu navedenog, ove pretnje već duže vreme ne predstavljaju apstraktne „digitalne momente“ već naprotiv, sasvim opipljive i egzaktne, obzirom da podjednako ugrožavaju, kako samo poslovanje i poslovnu infrastrukturu, tako i bezbednost predmeta zaštite, imajući u vidu da ove pretnje imaju i unutrašnji i spoljašnji karakter, odnosno da su pretnje po digitalno poslovanje i internog i eksternog tipa. U tom smislu, potrebno je prilikom sagledavanja digitalnog aspekta urediti i segment bezbednosne kulture učesnika u digitalnom poslovanju, kao i potrebu adekvatnosti menadžmenta koji će se ovim pitanjem baviti na sistematičan način, bilo po principima primene sopstvenih resursa, bilo po principu outsource-inga.

Savremeno poslovno okruženje dovelo je do preplitanja tradicionalne ekonomije i ekonomije novog doba, tj. digitalne ekonomije. Ovakav kontekst poslovanja doveo je do stvaranja novih poslovnih sadržaja, uvećao je vrednost proizvoda i usluga, doveo je do nastajanja roba, proizvoda i usluga kakve pre ove tehnološke revolucije nisu postojale, usled čega je postalo veoma teško da sa ove distance današnje trendove digitalnog poslovanja stavimo u kontekst neke ranije poslovne ili proizvođačke prakse.

Neki od razloga za ovakvo shvatanje, krajnje su objektivni. Primer za to može biti sada već uobičajeno korišćenje „sharing“ servisa, koji daju mogućnost skladištenja, transporta i sinhronizacije digitalnih podataka korisnika i postojećih dokumenata koji se nalaze na internetu.

Ovakvi trendovi su doveli do disruptivnih uticaja na tradicionalne poslovne modele koji su takođe nametnuli i inovirana poslovna pravila.

Na primer, muzička industrija je decenijama funkcionisala po principima prodaje nosača zvuka, počev od potpuno analognih, do potpuno digitalnih. Međutim, dalja evolucija razvoja digitalnog formata u potpunosti je razbila uobičajene sisteme proizvodnje, distribucije i prodaje zvučnih nosača, formatima izvedenim u domenu digitalne konverzije, koji su takvi da se mogu deliti mimo klasične distributivne šeme, čime su ti formati u potpunosti promenili uvreženi poslovni rezon i nametnuli nova pravila, kako u domenu same naplate korišćenih sadržaja, tako i domenu zaštite autorskih prava u vezi sa ovako distribuiranim sadržajima, a što samo po sebi direktno utiče na potrebu prilagođavanja radi opstanka muzičke industrije kakvu smo do tada poznavali.

Međutim, domet digitalne ekonomije nije se zadržao samo na tome, obzirom da postoje i primeri određene vrste simbioze digitalnog poslovnog modela i određenih tradicionalnih poslova, što je nesumljivo doprinelo rastu u ovom ekonomskom segmentu iz domena pružanja usluga.

Kako je novi ekonomski koncept po dubini skrojen na temeljima analize i razumevanja korisničkih potreba, može se reći da je najznačajniju revoluciju, ili bar blizu toga, donela eksponencijalno rastuća Uber usluga, koja je donela nezamislive novine u domenu povezivanja fizičkog taksi prevoza i internet aplikacije kojima sinergetski spajaju korisnike koji imaju automobil sa onima kojima je potreban prevoz. Ovakav digitalni model poslovanja po tumačenju tradicionalnih taksi prevoznika, a kao digitalna poslovna platforma, predstavlja ozbiljnu pretnju, iz kog razloga se ovakvo digitalno disruptivno poslovno dešavanje može razumeti i destruktivno i konstruktivno u odnosu na dosadašnji klasični ekonomski model.

Digitalna ekonomija zasnovana je na uporednom razvoju informacione i telekomunikacione tehnologije koje zajedno čine „infrastrukturu“ koja svom silinom svog razvoja transformiše tradicionalne načine svakodnevne komunikacije i poslovanja. Brojne digitalne platforme omogućile su organizovanje velikog broja društvenih mreža, a time i veliku ponudu raznorodnih mobilnih aplikacija, koje su sa sobom donele i razvoj „cloud“ tehnologije i servisa, neslućeni razvoj unapređenih vidova virtuelne realnosti, čime se bezmalo razbio dosadašnji socijalni i sociološki model interakcije i komuniciranja i stvorila tzv. nova društvena interakcija.

Sve ovo zajedno, pored uobičajenih vidova disrupcije, dovelo je do razvoja raznih vidova cyber pretnji od kojih ćemo kasnije obraditi nekoliko najozbiljnijih.

Moderni cyber kriminal, kao fenomen, ne samo da prati, već često i prevazilazi domete i prostore identifikacije i zaštite poslovnih informacionih sistema i infrastrukture. U periodu u kome je došlo do ekstenzivnog razvoja poslovne informatike, mreža i digitalnog poslovanja, cyber kriminal bio je uzrok koji je izazvao opsežna razaranja, kako u velikim, tako i malim i srednjim preduzećima širom sveta, maltene bez razlike. Načini kojima se cyber kriminalci služe, veoma su inventivni i stalno evoluiraju na načine koji su veoma sofisticirani, a do mera u kojima svaki, čak i najmanji bezbednosni propust ili previd može biti poslovno fatalan.

Savremena literatura konstatuje evoluciju hakerskog ekosistema koji je proizveo brojne alate za otkrivanje ranjivosti u poslovnim informacionim sistemima i maskiranje malvera u cilju onemogućavanja njihovog otkrivanja. Sistem cyber napada više nije takav da je neposredno uzročno-posledično vezan, već isti ima razvijene i unapred određene inteligentne konotacije u kojima je napad po najlogičnijem algoritmu, postupno i dobro isplaniranim radnjama i nastoji da sakrije maliciozni „malware kod“ unutar dokumenata koji su u opticaju, bilo na web sajtovima, serverima ili mrežama, kako bi u određenom trenutku, napadači bili u mogućnosti da takve dokumente, koji veoma često sadrže i „exploite“ starije generacije, prevedu u sasvim nove i do tada nepoznate pretnje.

Najčešće, cyber kriminalci bivaju fokusirani na krađu podataka, sabotazu poslovanja i njegovog kontinuiteta, a veoma često nastupaju i samo sa ciljem ugrožavanja ugleda napadnute kompanije i njenih resursa. Kada je u pitanju krađa podataka, u takvom slučaju meta su isključivo poverljivi podaci i veoma osetljive informacije napadnutog poslovnog entiteta i sistema.

Cyber kriminalci nakon uspešne infiltracije u poslovni informacioni sistem i mrežu, uvek pokušavaju izvesti eksfiltraciju svih dostupnih poverljivih korporativnih podataka, ali ne samo njih, već i ličnih i finansijskih podataka, medicinskih statusa, intelektualne svojine i sl. koji se mogu zloupotrebiti na tržištu ili inače. Ako se uzme u obzir činjenica da je pejzaž koji je meta napada izuzetno razuđen, kao i da je taj prostor često ukotvljen između velikog broja interno i eksterno povezanih mreža i mobilnih uređaja povezanih na njih, a onda i velikog broja cloud servisa i internet prostora kao celine, teško je i pomisliti da ovakve povrede neće nastaviti da se događaju uprkos svim nastojanjima onih čiji je cilj da to spreče.

Nastanak novih pretnji za sobom povlači potrebu novih inovativnih vidova zaštite, tako da već duže vreme zaštita bazirana samo na antivirusnim programima nije dovoljna, već ona može biti

samo deo aktivnog sistema zaštite. U tom smislu, proaktivni pristup zaštite preventivnim delovanjima u kombinaciji sa ostalim sredstvima zaštite, mogu predstavljati odgovarajući, odnosno u dovoljnoj meri efikasan sistem zaštite.

U poslednje vreme se kao vidovi ugrožavanja pojavljuju i „Zero-Day attacks“ (ZDA) i „Advanced Persistent Threat“ (APT).

6.1 Zero-Day napadi

Da bi moglo doći do „Zero-Day“ napada, potrebno je najpre razumeti šta su Zero-Day ranjivosti. Zero-Day ranjivosti predstavljaju softverski nedostaci koji postoje u sistemu, ali su još uvek neotkriveni, tj. nepoznati. Takvi softverski nedostaci usled svoje neotkrivenosti ostaju bezbednosno nepokriveni jer za njih nije napravljena bezbednosna (softverska) „zakrpa“, odnosno softverska popravka.

Ova vrsta ranjivosti predstavlja softverski prostor putem koga može doći do kompromitacije operativnog sistema, baza podataka, aplikacije, platforme ili sličnog softverskog dobra. Problem ranjivosti ovih sistema jeste taj što one ostaju nepoznate i proizvođaču softvera, sve dok se ne dogodi slučaj u kome takvo kompromitovanje bude primećeno, nakon čega otklanjanje ranjivosti traje onoliko vremena koliko je vendoru određenog softvera potrebno da proizvede, objavi i nakon toga izdistribuiraju zakrpu za konkretnu softversku komponentu putem koje je došlo do bezbednosne softverske kompromitacije.

Da se radi o veoma ozbiljnim pretnjama, govori i činjenica da postoje Zero-Day napadi koji se neprimetno izvršavaju u dužem vremenskom periodu u tzv. „low-profile“ modu, koji često ostaje neprimetan sve dok se iz određenog sistema ne izvuku ciljane i vredne informacije i podaci.

Jedan od najpoznatijih primera ove vrste napada, jeste slučaj u kome su hakeri od kompanije Sony putem Spear-Phishing tehnike, a posredstvom e-mail attachment-a uspešno instalirali zlonamerni kod putem koga je došlo do kompromitacije osetljivih podataka, ugovora i sl. što je proizvelo globalnu aferu. Specifičnost Zero-Day napada je ta da oni nemaju potpis, pa ih to čini podobnim da prilično lako budu provučeni kroz antivirusne zaštite, sisteme za sprečavanje hakerskih napada i druge analitičke tehnologije, čime se omogućava odvijanje maliciozne radnje i aktivnosti u dužem vremenskom periodu, pre nego što ona bude otkrivena.

6.2 Reciklirane cyber pretnje

Činjenica je da u poslednje vreme „Malware“ kao vrsta malicioznog koda čini jedan od najvećih digitalnih bezbednosnih izazova iz razloga što se njihovo delovanje može maskirati modifikovanjem poznatog malicioznog koda ili njegovom enkripcijom, što čini da poznati i prepoznatljivi malware postaje nepoznat i neprepoznatljiv, čime njegov tvorac, najčešće haker, stiče prednost nad sistemom zaštite. Ovakav vid promene zastarelog ili prevaziđenog malicioznog koda radi stvaranja nove pretnje predstavlja proizvodnju reciklirane cyber pretnje.

6.3 Napredne uporne pretnje

Napredne uporne pretnje, za razliku od Zero-Day pretnji koje su proizvod hakera ili hakerskih grupacija, najčešće bivaju implementirane od strane država koje imaju za to finansijskih i tehničkih mogućnosti i koje ovaj vid delovanja smatraju legitimnim sredstvom za ostvarenje nacionalnih ciljeva i interesa putem ciljanih akcija u sajber prostoru.

Ove pretnje podrazumevaju složene modele programiranja, ali i upornost i doslednost u sprovođenju napadnih tehnika, kao i postupnost u fazama napada, usled čega su ove pretnje izuzetno teške za otkrivanje, a iste mogu delovati od nekoliko nedelja pa do više godina. Njihov princip predstavlja „step-by-step“ tehniku, kao seriju malih događaja, koji ako se ne sagledavaju kao celina, a što je vrlo teško usled njihove prirode, izgledaju sasvim bezazleno. Tako, kada ove pretnje, odnosno koraci budu otkriveni, tada se može govoriti samo o posledicama takvog napada, a ne o mogućnostima zaštite.

Iz ovog razloga napredne uporne pretnje predstavljaju pretnje od izuzetne opasnosti za svaku organizaciju. Prethodno smo pomenuli primer kompanije Sony koja je velika globalna organizacija, međutim, kada je u pitanju ovaj vid pretnji, on nije usmeren samo na velike kompanije, već naprotiv, žrtve ovog vida ugrožavanja bile su i male i srednje kompanije, čiji značaj, bez obzira na veličinu čini baza informacija, podataka i dokumenata kojima elektronski raspolazu. Zapravo svako ko poseduje podatke, informacije i dokumenta koji mogu biti opasni u pogrešnim rukama, moraju biti svesni ovog vida pretnji, kao i činjenice i potrebe da ih razumeju, te da čine sve napore radi efikasne prevencije, jer ako to ne uspe, nastaće strahovite posledice.

Usled opasnosti i štetnosti ovakvih pretnji, pristupilo se pokušajima da se izračuna vrednost štete po kompromitovanom zapisu, pa se došlo do rezultata da je „prosečna cena povrede podataka po

osnovu naprednih upornih pretnji, oko 154 dolara po zapisu, dok je prema Ponemon istraživanju, uzimajući u obzir i velike i male incidente, ukupna cena jedne ovakve povrede, porasla za 23% tj. na 79 miliona USD u 2015.godini“ (Ponemon, 2015:1).

Izračunato je da ovakvi događaji proizvode dugoročnu štetu po brend i ugled kompanije. Utvrđeno je da vrednost brenda usled direktne štete radi kršenja bezbednosti u proseku doživi pad vrednosti od 21%. Ovo dalje povlači teško vraćanje poverenja korisnika kompaniji koja nije bila u stanju da zaštiti čak ni svoje sopstvene informacije ni podatke.

Da bi se odgovorilo na opisane pretnje i prevenirale njihove posledice, nastala je potreba da se proizvede inteligentna tehnologija koja može ispratiti sve cyber izazove i da blagovremeno otkrije i blokira napredne pretnje. U tom smislu razvijena je „sandbox“ tehnologija, koja bezbedno vrši kontrolu sumnjivih fajlova u određenom virtuelnom okruženju, tako da se oni, ako bi i bili aktivirani, onemogućavaju da izvrše svoj maliciozni zadatak jer su u tom virtuelnom prostoru bezopasni.

Sandbox tehnologija ima zadatak da presretne izvršni fajl malicioznog koda i da ga aktivira u virtuelnom okruženju, tzv. emulatoru i tamo izvrši dubinsku analizu koju nije moguće da izvrše antivirus i firewall. Na ovaj način se u bezbednom virtuelnom okruženju testira kako se izvršni softver malicioznog koda ponaša, s tim da je istom onemogućeno da pristupi bilo kom sistemu ili mreži van kontrolisanog okruženja, čime se sprečava da maliciozni softver ostvari svoju ulogu, a to je da ošteti određenu mrežu ili digitalnu infrastrukturu ili nedozvoljeno pribavi štićene informacije. Na ovaj način postiže se da su brzina i preciznost detekcije napada zapravo veći od bilo kog uobičajenog modela zaštite, čime je ovaj sistem zasnovan na preventivno-proaktivnom modelu, što je u suštini najbolja i najefikasnija tehnologija u detektovanju i neutralizovanju nepoznatih, naprednih, a time i upornih pretnji.

Poglavlje VII: Dizajniranje i kontekstura informacione bezbednosti u digitalnom poslovanju

Sve veća učestalost napada na informacionu infrastrukturu i sisteme, kako kompanija, tako i institucija čiji rad podrazumeva smeštanje poverljivih sadržaja, kao što su personalni podaci korisnika, korisnička imena i lozinke, poverljivi dokumenti i sl., iziskuju suštinsko uređenje pravila koja bi trebala dovesti do zaštite materijalnih i intelektualno-svojinskih vrednosti takvih organizacija. Kako je činjenica da sajber napade nije moguće sa sigurnošću predvideti, a često ni sprečiti, to ne umanjuje potrebu preduzimanja svih mera predostrožnosti, kako bi se eventualna šteta koju bi cyber napad prouzrokovao redukovala na najmanju moguću meru (Čelik, P.2019:61-81).

Činjenica je da je najčešći motiv cyber napada sticanje protivpravne finansijske koristi, međutim, činjenica je takođe i da je u značajnom broju slučajeva ovih napada, nastala finansijska šteta bila daleko manja od štete koja je sistemu naneta otkrivanjem poverljivih informacija koje su u njemu pohranjene. Ovakav činjenični korpus iziskuje suštinsko redizajniranje i definisanje prefinjene informatičke konteksture i prepoznavanje suštine informacione bezbednosti u digitalnom poslovanju.

Da bi to bilo moguće, potrebno je sprovesti definisanje skupa bezbednosnih pravila koja imaju moć objedinjavanja celokupnog područnog konteksta svih elemenata ranjivih na određene vrste napada, pa ta pravila nazivamo sigurnosnom politikom. Cilj sigurnosne politike je da uredi dizajn i konteksturu svih pravila ponašanja i odgovornosti korisnika određenog informacionog sistema, sa ciljem minimiziranja potencijalnih posledica i šteta koje mogu nastati, kako namernim, tako i nenamernim radnjama i delovanjima (Ibid).

Visok stepen zaštite informacionog sistema može se podrazumevati u onim kontekstima u kojima određena organizacija ima definisanu i primenjenu bezbednosnu politiku, pa ta bezbednosna politika kao pristup ima ulogu razvijanja svesti kod zaposlenih o značaju informacione bezbednosti i bezbednosne kulture, kao i stalne edukacije o njima, ali istovremeno i o svim mogućim rizicima i posledicama bezbednosnih incidenata (Ibid).

1. Određenje pojma i sadržaja informacione bezbednosti

Pojam informacione bezbednosti prvi put je upotrebljen u Sjedinjenim Američkim Državama na temeljima teorije informacionog ratovanja - eng. Information Warfare.

Prema Danielu Wulf-u, 60-ih godina 20. veka nastao je i termin komunikacione bezbednosti - eng. „COMSEC - Communication Security“. Sa značajnijom pojavom računara šireg opsega primene, 70-ih godina 20. veka, nastala je i terminološka jedinica kompjuterska bezbednost – eng. „COMPUSEC - Computer Security“. Do kraja 80-ih godina 20. veka, usled ekspanzije personalnog računarstva, COMSEC i COMPUSEC objedinjeni su u jedinstvenu terminološku jedinicu Informaciona bezbednost – eng. „INFOSEC - Information Security“, čime je konačno učinjen pokušaj da se integrišu neke ranije potpuno odvojene discipline, kao na primer bezbednost osoblja, kompjuterska, odnosno računarska bezbednost i komunikaciona i operativna bezbednost (Wolf, 2003).

Temelj na kome je zasnovan INFOSEC, već tada je bio usmeren na onemogućavanje neautorizovanog pristupa informacionim sistemima i njihovim resursima. Istovremeno je došlo i do razmatranja bazičnih bezbednosnih postavki u vidu poverljivosti, integriteta i raspoloživosti informacija.

Dalji intenzivni razvoj računarstva doveo je do nastanka mreža i umrežavanja i time pojava mreža kao što su LAN i WAN i time Interneta, što rezultira proširenjem liste informacionih svojstava sa bezbednosnim zahtevima, a to su pre svega autentičnost i neporecivost sadržaja.

Prema aktuelnim shvatanjima pojma kakav je nacionalna bezbednost, informatička bezbednost predstavlja jednu od osnovnih komponenti nacionalne bezbednosti, što ovu problematiku čini trajnom i krajnje aktuelnom (Sinkovski, 2005:31-81).

Prema odredbama Zakona o informacionoj bezbednosti Republike Srbije, član 2, stav 1 tačka 3, „informaciona bezbednost predstavlja skup mera koje omogućavaju da podaci kojima se rukuje putem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost tih podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica“

2. Tri stuba bezbednosti

Da bi mogli definisati šta je predmet zaštite bezbednosne politike, potrebno je da se bezbednosnom politikom obezbede 3 svojstva informacija koje sadrži određeni sistem. Ta svojstva informacija čine poverljivost, integritet i dostupnost. Ova svojstva zaštićena su troslojnim bezbednosnim nivoima, koji su: bezbednost organizacija, lična bezbednost i fizička bezbednost. U cilju zadovoljenja propisanih bezbednosnih standarda za informacione sisteme, informacione sisteme delimo na 3 glavna dela:

- Računarsku opremu;
- Programe; i
- Komunikaciju.

Mehanizmi zaštite i sprečavanja ugrožavanja bezbednosti informacionog sistema podeljeni su na 3 osnovna nivoa. Kao prvi i najvažniji nivo, imamo fizičku bezbednost, koja kao takva, obuhvata bezbednost računarske opreme i u njoj pohranjenih podataka. Kao drugi nivo, utvrđena je lična sigurnost, odnosno zaštita, kako korisnika, tako i poverljivih podataka o njemu, i na kraju, bezbednost informacija koja predstavlja ishodište interakcije ova dva nivoa.

2.1 Poverljivost

Poverljivost čini mehanizam zaštite informacija čiji je zadatak sprečavanje njihovog otkrivanja od strane neovlašćenih lica ili sistema (Čelik, P.2019:61-81). Ukoliko se dogodi da se zaštićenim, odnosno poverljivim informacijama i sadržajima ne rukuje na pravilan i propisan način, može doći do narušavanja njihove tajnosti, a time i otkrivanja ovih informacija nepozvanim licima, bilo da je to učinjeno usmenim, pisanim, odnosno štampanim putem, kopiranjem, slanjem elektronskom poštom, i sl.

U tom smislu, najčešćim pretnjama poverljivosti informacija smatraju se:

Napadači - koji eksploatacijom sigurnosnih propusta pokušavaju otkriti i pribaviti zaštićene informacije, bez obzira na to da li je to radi sopstvene koristi ili radi šireg konteksta zloupotrebe tih informacija putem njihovog objavljivanja na internetu;

Lažno predstavljanje - radi sticanja mogućnosti neovlašćenog pristupa poverljivim informacijama u informacionim sistemima, najčešće zloupotrebom pristupne šifre drugog korisnika;

Neovlašćena aktivnost - kada legalni korisnik informacionog sistema pohranjene podatke menja, briše, kopira i sl., suprotno pravilima i svojim ovlašćenjima;

Kopiranje podataka na nezaštićene lokacije - kada se ugrožavanje poverljivosti podataka vrši njihovim kopiranjem na sisteme sa nedovoljnim nivoom zaštite u odnosu na inicijalni informacioni sistem;

Zlonamerni programi - u pitanju su maliciozni programi putem kojih je moguće ostvariti neovlašćen pristup informacionom sistemu u kome su pohranjeni poverljivi podaci, a sve radi njihovog neovlašćenog otuđenja (Ibid).

2.2 Integritet

Prilikom rukovanja podacima, izuzetnu važnosti čini očuvanje njihovog integriteta. To se najčešće postiže na način što je korisnik informacionog sistema onemogućen u tome da vrši izmene podataka bez posebnog odobrenja, usled čega bi integritet podataka predstavljao da su podaci o kojima je reč, potpuni, ispravni i jednoznačni, tj. u skladu sa svojim izvorom.

Važan segment sistema zaštite podataka jeste i minimiziranje verovatnoće, bilo namernog, ili nenamernog slučaja povrede integriteta podataka. Ovako se osigurava puna tačnost i apsolutna ispravnost podataka uskladištenih u velikim informacionim sistemima, što se postiže nekom od vrsta autentifikacije korisnika kroz utvrđenje njegovog identiteta, pa se u te svrhe najčešće koriste jednokratno dodeljene lozinke, pametne identifikacione kartice, biometrijski čitači i sl.

Nakon eliminisanja mogućnosti namernih izmena poverljivih podataka, veoma je važno održati oprez koji će u najvećoj meri garantovati da se neće dogoditi ni slučajne izmene u domenu ovih podataka. Ovaj efekat može se postići organizovanjem strogo poverljivog i profesionalnog okruženja koje treba predstavljati garant da neće doći ni do namernih, ni nenamernih izmena šticećenih podataka.

2.3 Dostupnost

Svrha postojanja informacionog sistema jeste da su informacije koje su pohranjene u njemu uvek i u svakom trenutku dostupne njegovim korisnicima u nekompromitovanom obliku. Da bi to bilo moguće, neophodno je u svakom trenutku osigurati rad takvog sistema i u punom formatu vršiti njegovo održavanje u domenu unosa i obrade podataka, kao i sistema za zaštitu kanala komunikacije i pristupne infrastrukture za do pohranjenim informacija (Čelik, P.2019:61-81).

Najčešći Najčešći razlog nedostupnosti informacija jesu DoS (Denial of Service) napadi, odnosno napadi koji dovode do prestanka mogućnosti obrade podataka od strane angažovanog servera. Kada je u pitanju ova vrsta napada, pod njih se podrazumeva svaka vrsta sajber napada na server u cilju onemogućavanja njegovog rada sa ovlašćenim licima i korisnicima. Mehanizam ovih napada je takav, da napadač organizuje veliki broj računara ili IoT stvari organizovanih u Bot Net mreže i istovremeno šalje veliki broj zahteva, sve do mere koju ovaj sistem usled tehničkih ograničenja više ne može podneti, čime se proizvede posledica da informacioni sistem prestane da prima i obrađuje sve dalje zahteve, čime se ovlašćenim licima i korisnicima onemogućava dalji pristup podacima i mogućnost rada.

Da bi se jedan DoS napad sproveo, neophodno je da napadač najpre primenom sofisticiranih metoda pronađe određene bezbednosne propuste u računarima i sistemima i da njihovom eksploatacijom uspostavi kontakt sa njima i nad njima preuzme kontrolu. Nakon toga, napadač na teret tih propusta i preuzete kontrole nad ovim računarima i sistemima, ustanovljava Bot Net mrežu i usmerava sve njihove resurse u formi enormnog saobraćaja na server koji napada. Posle određenog vremena i usled enormnog broja zahteva i prekomernog saobraćaja napadnuti server više nije u mogućnosti obraditi pristigle zahteve od Bot Net mreže, usled čega napadnuti server počinje da odbija sve novopristigle zahteve, kako od spolja, tako i od ovlašćenih korisnika unutar sistema.

Ipak, potrebno je napomenuti da do gubitka mogućnosti obrade podataka u informacionom sistemu ne dolazi isključivo iz prethodno opisanog razloga, već se to može dogoditi i radi posledica prirodnih katastrofa i zlonamernih aktivnosti ljudi na informacioni sistem. Iz ovih razloga, prirodne katastrofe (zemljotresi, požari, poplave..) mogu biti koren prestanka predviđenog rada informacionog sistema, dok sa druge strane ljudski zahvati, bili oni nenamerni ili namerni, mogu izazvati jednako ozbiljnu štetu i posledice, kao i pomenute prirodne katastrofe (Čelik, P.2019:61-81).

U slučajevima kakav je naveden, preduzimaju se mere bezbednosti koje treba da osiguraju stalnu dostupnost podataka i resursa informacionog sistema. Pre svega, ovde treba pomenuti fizičke mere bezbednosti koje moraju obezbediti fizičko-tehničko sprečavanje neovlašćenog pristupa informacionom sistemu i svim njegovim delovima, kao i ostalim sistemima koji bi mogli dovesti, do bilo koje neplanirane ili nedopuštene promene u poslovnom okruženju (Ibid).

Uporedo sa navedenim, preduzimaju se i druge tehničke mere, kao pristup čiji je zadatak da osiguraju ispravnost i funkcionisanje, kako informacionog sistema, tako i svih njegovih delova. Najčešće, taj efekat se postiže tzv. mirroring-om, koji obezbeđuje da se istovremeno sadržaj hard diskova višestruko iskopira u formi „bekapa“, i ukoliko bi došlo do kvara na jednom od aktivnih hard diskova, naredni disk sa identičnim sadržajem preuzeće njegovu funkciju i obezbediti efekat visoke redundantnosti informacionog sistema.

Pored navedenih hardverskih, preduzimaju se i odgovarajuće softverske tehničke mere kojima se vrši konstantno testiranje ispravnosti rada angažovanih programa uz obaveznu redovnu izradu bezbednosnih kopija, na način adekvatan čak i za slučaj u kome bi došlo do prekida u napajanju sistema električnom energijom.

Da bi se ustrojili odgovarajući bezbednosni standardi, neophodno je uspostaviti i odgovarajuće bezbednosne politike u okvirima postojeće organizacije, kojima bi se doslovno primenili takođe odgovarajući standardi iz domena bezbednosti informacionog sistema. Ovakav način rada obezbeđuje upravljanje bezbednosnom politikom prema utvrđenim standardima, čime se najpre obezbeđuju svi aspekti zaštite informacionog sistema, a u sklopu toga i potvrđeni kvalitet primenjenih mera bezbednosti.

Kada su u pitanju merodavne institucije za ustanovljavanje ovakvih standarda u području zaštite informacionih sistema, tu se najpre mora pomenuti ISO (International Organization for Standardization) i IEC (International Electrotechnical Commission).

Standardi Međunarodne organizacije za standardizaciju i Međunarodne elektrotehničke komisije iz ISO/IEC 27000 serije, kompanijama, odnosno organizacijama pružaju neophodne standardizovane smernice za konstruisanje, primenu i promenu informacionih sistema, kao i primenjenih procesa rada unutar predmetne organizacije.

U ovom smislu za područje bezbednosti informacionih sistema, najčešće se primenjuju dva međunarodna standarda i to:

- ISO/IEC 27001 i
- ISO/IEC 27002 (pre 2007. godine poznat kao ISO/IEC 17799:2005)

Pri izradi bezbednosne politike organizacije, preporučuje se primena oba navedena standarda.

3. Bezbednost Cloud-a

U periodu koji je za nama, naročito kada je u pitanju poslednja decenija, bezbednost poslovnih podataka predstavlja ključni element postojanja kompanija. Upored sa tim, i element zaštite od pretnji i rizika po ovaj segment poslovanja, iziskuje delovanje brojnih resursa neophodnih za ostvarivanje ove zaštite (Čelik, P. 2019:61-81).

Iako praksa nalaže ove poslovno-bezbednosne vrednosti, veliki broj kompanija i dalje nije razvio poslovno-bezbednosnu svest u ovoj oblasti. Ovakva konstelacija u organizaciji, čak ni kada su u pitanju najveći poslovni sistemi, ne obezbeđuje adekvatne uslove da organizacija drži korak, kako sa agresivnim konkurentskim okruženjem, tako ni sa rizičnim okruženjem koje se nad organizacijom nadvija iz cyber prostora u obliku cyber kriminala.

Jedan od načina da se ovaj problem efikasno reši, jeste računarstvo u oblaku kao koncept koji je u stanju da omogući potpunu brigu o informacionim resursima kompanije, a uporedo sa tim, ponudi i adekvatnu bezbednost podataka. S tim u vezi, računarstvo u oblaku, tj. Cloud computing, predstavlja revolucionarni pomak u domenu primenjive poslovne informatike.

Već izvesno vreme, određeni tehnološki krugovi Cloud tehnologiju najčešće predstavljaju tehnologijom štednje. Ipak, zabrinutost kompanija klijenata za službene tajne i sigurnost sopstvenih podataka i dokumenata čini da se mnoge od tih kompanija drže po strani i posluju uzdržano usled nedostatka referenci Cloud provajdera. Ovo dalje čini da čak i kompanije koje bi se možda i odlučile na prelazak na ovu vrstu poslovne strategije i tehnologije i dalje nisu spremne na takav radikalni poslovni potez, jer bi takav potez po njima podrazumevao da poslovne podatke iz svog poseda presele na tuđe servere i infrastrukturu, što je po njihovoj oceni apsolutno van kontrolisanog okruženja.

Mnoge poslovne organizacije, kada je u pitanju Cloud tehnologija, iz navedenih razloga prihvataju veću cenu poslovanja kako bi zadržali autonomiju nad podacima i tehnologijom koju koriste, tj. kako ne bi došle u poziciju da se izlože rizicima koji nastaju sa curenjem podataka, tj. narušavanjem poverljivosti, a što bi bez sumnje moglo voditi ka gubljenju poverenja klijenata i drugih finansijskih posledica povezanih sa tim, o čemu je već ranije bilo reči (Čelik, P. 2019:61-81).

Sa druge strane, postoje i globalne organizacije čija poslovna politika i bezbednosna pravila ne dopuštaju čuvanje poslovnih podataka na informacionim sistemima koji su u tuđem vlasništvu. Takve kompanije su iz navedenih razloga napravile sopstveni poslovni kompromis i time zadovoljili svoje potrebe (i racionalne i bezbednosne), uspostavljajući određenu vrstu privatnog Cloud-a, koji kao takav nesumnjivo ima svojih prednosti.

Ipak, kada je reč o malim i srednjim preduzećima, samim tim i biznisima u razvoju koji nemaju poslovni potencijal velikih organizacija, može se reći da je za njih računarstvo u oblaku, tj. Cloud computing, idealno poslovno rešenje, koje zadovoljava ne samo njihove poslovne potrebe, već i bezbednosne (Ibid).

Činjenica je da Cloud provajder ne može biti bilo ko, obzirom da kompanija koja se želi baviti pružanjem Cloud usluga, ipak mora zadovoljiti, pored strogih tehničkih kriterijuma, naročito i one iz domena bezbednosti. Samim tim, donošenje poslovne odluke o prelasku na Cloud tehnologiju i servise, predstavlja poslovni zaiokret ka principima outsource-inga, zapravo suštinske eksteralizacije određenih poslovnih funkcija i procesa.

Eksteralizacija poslovnih funkcija i procesa, odnosno njihovo poveravanje spoljnim saradnicima i partnerima, uvek mora podrazumevati primenu strogih i poslovnih i bezbednosnih standarda kompanije, a te uslove, odnosno standarde eksterni provajder uslova mora zadovoljiti ili u toj meri, ili u meri koja prevazilazi očekivanja klijenta.

Kada određena kompanija sve svoje poslovne aktivnosti zasniva na sopstvenoj IT infrastrukturi, ona izlaže sebe troškovima vezanim za osnovne poslovne funkcije, ali i eksternim rizicima i pretnjama, a time i mogućim cyber napadima koji suštinski mogu biti svakodnevnici. Samim tim, rizici za poslovanje ne obuhvataju samo eksternost, obzirom da je praksa dokazala da se štete i gubici često po svom nastanku baziraju i na osnovama internih rizika, bilo da su oni slučajni ili namerni. Iz ovih razloga, sve kompanije ovog nivoa moraju primenjivati efikasne bezbednosne mere i ka unutra i ka spolja.

Sve navedeno navodi kompanije da one moraju primenjivati što efikasnija antivirusna i firewall rešenja, čak i u sloju aplikacije, a ta efikasna rešenja imaju svoju cenu i znatno opterećuju poslovanje zbog visoke cene kvalitetnih softvera i opreme proverenih i referentnih proizvođača.

Samim tim, trošak na ovom polju konstantno raste, počev od segmenta kupovine i održavanja softverskih i hardverskih proizvoda, a nakon toga i troškova licenci i aftermarket podrške, a iza toga i troškova koji se pojavljuju u vidu obuke i organizovanja potrebnih izvršilaca koji će biti nadležni i odgovorni za uspostavljanje i održavanje uspostavljenog sistema na način koji obezbeđuje maksimalnu sigurnost podataka i infrastrukture.

Sa druge strane, Cloud computing, kao kompleksni višeslojni servis omogućava kompaniji da kompletnu brigu u oblasti poslovne informatike, uključujući i njenu bezbednost, prepusti izabranom Cloud provajderu i njegovom profesionalnom osoblju, kako bi na taj način kompanija svoj „problem“ eksteralizovala, funkcionišući dalje na tržištu bez briga vezanih za investiranje u ovoj oblasti poslovanja.

Ipak, ovaj način poslovne racionalizacije ne podrazumeva sam po sebi i prelazak odgovornosti za štete i posledice po korisnike kompanije na cloud provajdere u slučaju narušavanja bezbednosti podataka, iz razloga što korisnike ne zanimaju pozadinski potencijali i poslovni izbori kompanije sa kojom saraduju ili od nje kupuju proizvode i usluge, već samo, jedino i isključivo potpuna bezbednost njihovih podataka i ono što kao dodatu vrednost dobijaju za svoj uloženi novac.

Samim tim, odgovornost pružalaca usluga na Cloud tržištu konstantno raste, pa Cloud provajderi moraju, obzirom da je to njihova osnovna delatnost, da nivo bezbednosti svog poslovanja i usluga koje pružaju podižu i drže na najvišem nivou, radi čega su pojedini stručnjaci skloni da kažu da su podaci kod Cloud provajdera često daleko bezbedniji nego u slučaju kada bi se nalazili na informatičkoj infrastrukturi same kompanije. Stručnjaci to objašnjavaju time što je taj poslovni segment nekoj kompaniji sekundarna poslovna aktivnost, a Cloud provajderu primarna i jedina i nemaju prostora za greške.

Jedan od parametara koji korisnicima Cloud usluga, kao i potencijalnim korisnicima pruža određenu meru bezbednosti, jeste da kompanija koja želi postati Cloud provider mora da ispuni međunarodne standarde u ovoj oblasti, kao što je na primer, međunarodni standard ISO 27001. Takođe, između Cloud korisnika i Cloud providera obavezno se potpisuje i Ugovor o čuvanju poverljivih podataka, koji između ostalog i pravno štiti korisnika i njegovu privatnost. Važno je istaći da Cloud provajder nema pravo da bez odobrenja vlasnika podataka istima pristupa ili sa njima manipuliše.

Treba naglasiti da je pretežno dominantan stav stručnjaka u poslednje vreme, da Cloud tehnologija kao poslovni kontekst u oblasti pružanja IT servisa više nije deo pitanja da li će, već samo kada će tradicionalni IT gurnuti u prošlost, jer će tržište i pritisak konkurencije na tom polju učiniti svoje.

Savremene poslovne tendencije već izvesno vreme podrazumevaju da su kanali komunikacije kompanija veoma često zasnovani na bežičnim i mobilnim mrežama, što često podrazumeva da se prilikom komuniciranja i razmene podataka i dokumenata od mesta inicijalnog zahteva do odredišta najčešće koristi tuđa IK infrastruktura. To je najveći broj kompanija navelo da uspostave obavezu razvijanja sistema upravljanja bezbednošću informacija, sa ciljem da se protok i manipulacija informacijama obave jednostavno, brzo i efikasno, tj. na način koji uliva tržišno poverenje, kako među poslovnim partnerima, tako i među korisnicima na tržištu (Čelik, P., 2019:61-81).

U ovakvim tržišnim odnosima i uslovima, neophodno je organizovati proaktivan pristup bezbednosti, tj. pristup pravovremene identifikacije rizika radi obezbeđivanja bezbednog i sigurnog elektronskog poslovanja, negovanja dobre poslovne prakse, dostupnost informacija u zaštićenom i bezbednom okruženju, efektivniji i efikasniji rad informacionih sistema, negovanje i produbljenje poverenja kompanije sa njenim klijentima i partnerima, poboljšanje tržišnog kredibiliteta i ugleda kompanije, efikasnije korišćenje informatičkih resursa neophodnih za čuvanje i razmenu podataka, istovremeno jasno uređivanje funkcije i obaveza učesnika u poslovnim procesima, kako bi sve to zajedno, kao proaktivni poslovno-bezbednosni pristup, uredilo preduslove za ostvarenje suštinski određive kompetitivne prednosti kompanije (Čelik, P., 2019., str. 75).

Bezbednost i zaštita informacija suštinski predstavlja i zaštitu bezbednosti i kompanijskog Know-How. Samim tim, upravljanje rizicima na nivou definisanom kroz međunarodno priznate standarde i uz uvažavanje principa dobrog upravljanja, u velikoj meri umanjuje mogućnosti i verovatnoću nastanka nepredviđenih poslovno-bezbednosnih situacija. Ovakva poslovna organizacija, tj. organizacija koja posluje na ovim principima, nesumnjivo ima sve potrebne preduslove da ostvari konkurentsku prednost na tržištu.

4. Strateški, institucionalni i regulatorni okvir informacione bezbednosti u Evropskoj Uniji: rešenja, iskustva i pouke

U protekle dve decenije, pojava Interneta, a još više od toga, cyber prostora, izvršila je uticaj neviđenih razmera na sve segmente društva i sve društvene zajednice. Svakodnevni život, temeljna ljudska prava, društvena i ekonomska kretanja, preko noći su počela da zavise od informacionih i komunikacionih tehnologija. Tako nastali cyber ambijent omogućava društveno uključivanje u cyber prostor svih zajednica, i to tako što je cyber prostor srušio sve do tada uspostavljene barijere između država, zajednica i građana, uspostavivši tako široku interakciju za razmenu ideja i informacija na globalnom nivou.

Nastali cyber prostor kao tekovina dostignutog razvoja, morao je rešiti problem koji je nastao u prostoru između fizičkog i virtuelnog sveta, a u smislu toga da je postalo neophodno da se prava i obaveze i dostignuti nivo bezbednosti iz fizičkog sveta moraju prelići i na cyber prostor kako bi se na taj način obezbedila vladavina prava i zaštita prava i interesa svih, pa i u domenu cyber prostora i ambijenta.

Cyber prostor mora biti zaštićen od incidenata, zlonamernih aktivnosti i zloupotreba, pa vlade država u tom smislu, imaju značajnu ulogu kako bi obezbedile slobodan i bezbedan cyber prostor i „cyber protok“.

Činjenica da je cyber prostor virtuelan, ne sme značiti da u njemu može biti dozvoljeno kršenje svih onih prava i sloboda zajemčenih u fizičkom svetu. Stiče se utisak da u široj javnosti postoje shvatanja da inkriminisana dela izvršena u virtuelnom okruženju imaju manju težinu u odnosu na ista dela izvršena u fizičkom svetu i okruženju.

Da bi takvo uređenje bilo moguće, Evropska Unija je, shvatajući značaj i dimenzije ove problematike usmerila svoja nastojanja da pravno uredi cyber prostor, punim angažovanjem na izradi strategija cyber bezbednosti, kako bi uredila prioritete i aktivnosti svog delovanja na ovom složenom polju.

Stručnjaci koji su se bavili ovom problematikom, shvatili su da Evropska Unija mora dostići određeni nivo otpornosti na cyber rizike i pretnje, kao i da taj proces može biti uspešan samo kroz učešće velikog broja društvenih činilaca iz domena javnog i privatnog sektora. Uzevši u obzir da je Evropska Unija po svojoj strukturi izuzetno složena i na nadnacionalnom i

subnacionalnom nivou, shvaćena je potreba za usvajanjem odgovarajućih regulativa i na nivou Unije i država članica, kao i da je potrebno opredeliti koji će zajednički organ biti nadležan za ukupnu informacionu bezbednost, kako bi se u tom smislu uspostavili i nacionalni timovi za prevenciju i reagovanje na cyber incidente - CERT (Computer Emergency Response Team).

Kako je informaciona i komunikaciona tehnologija postala kičma ekonomskog rasta, takođe je postala i kritični resurs na kome svi ekonomski sektori počivaju. Ove tehnologije čine da ekonomije funkcionišu i rastu u ključnim sektorima kao što su finansije, zdravstvo, energetika i transport, dok su istovremeno mnogi poslovni modeli utemeljeni na neprekidnoj dostupnosti interneta i neometanog funkcionisanja informacionog sistema.

Ipak, i pored nastojanja EU da na svim nivoima uredi ovo polje, nije dovoljno da se na ovom prostoru angažuje samo država, već je neophodno i motivisanje privatnog sektora da bude što spremniji na izazove predstojećeg tehnološkog razvoja, a da bi to angažovanje bilo uspešno, neophodno je da svi uvećaju svoja ulaganja na polju informacione bezbednosti.

Međutim, svest u privatnom sektoru ne figurira na ovom nivou, obzirom da značajan deo privatnog IKT sektora, ulaganja na polju bezbednosti smatra teretom, a ne investiranjem, što čini potrebnim da se na ovom polju ulože dodatni napor kako bi se to dovelo u ravan sa postojećom tržišnom logikom.

Da bi ovakvi mehanizmi bili efikasni na polju prevencije i zaštite, stručnjaci su shvatili da se promene na ovom polju ne smeju dešavati segmentalno i razučeno, već da države članice Evropske Unije moraju imati mehanizam putem koga će moći da razmenjuju podatke i informacije o svim evidentiranim opasnostima, krizama i incidentima u IKT sistemima i da je u tom smislu od izuzetne važnosti da nadležne službe država održavaju simulacione vežbe situacija nastalih iz cyber incidenata, kako bi se na njima razmenjivala iskustva i podizala svest i država članica i činilaca privatnog sektora.

Na ovaj način se može postići efekat širenja potrebnih informacija o cyber pretnjama radi pravovremenog preduzimanja zaštitnih mera. Iz tog razloga strategija cyber bezbednosti Evropske Unije najpre definiše nadležne organe koji pre svih treba da daju doprinos ispunjenju ovih pomenutih prioriteta i ciljeva. Tu se najpre navodi Evropska agencija za bezbednost mreža i podataka (ENISA), čija je obaveza objavljivanje izveštaja o cyber incidentima, kao i organizacija

radionica za podsticanje unapređenja javno-privatnih partnerstava. Pored ENISA-e, među takvim organima, identifikovani su i Europol i Eurojust.

Uz navedene institucije, potrebno je pomenuti i nadležne organe za zaštitu podataka, koji ovu ulogu vrše u svom delokrugu. Radi realizacije opisanih ciljeva, Europol je nekoliko godina ranije, osnovao Evropski centar za cyber kriminal (European Cyber Center - EC3).

Evropski parlament je sredinom 2016. godine doneo odluku o proširenju ingerencija Europol-a i to tako što će ova evropska policijska agencija ubuduće moći da ima pristup javnim i tajnim bazama podataka radi vođenja krivičnih istraga.

Prema izmenjenoj i dopunjenoj uredbi koja je usvojena od strane Evropskog parlamenta i Veća Evrope, Europol dobija, pored proširenja postojećih zadataka i nadležnosti i potpuno nove zadatke, (Evropski parlament, 2016), u sklopu njih i da:

- prikuplja, skladišti, obrađuje, analizira i razmenjuje informacije, uključujući i kriminalističke obaveštajne podatke,
- bez odlaganja obaveštava države članice o svim važnim informacijama,
- vrši koordinaciju, organizaciju i sprovođenje istražnih i operativnih radnji,
- učestvuje u zajedničkim istražnim timovima i predlaže njihovo osnivanje,
- pruža informacije i analitičku podršku državama članicama u vezi sa važnim međunarodnim događajima,
- priprema procenu opasnosti, strateški i operativnih analiza i izveštaja o opštem stanju bezbednosti,
- vrši podelu i unapređenje stručnog znanja o metodama sprečavanja kriminala, istražnim postupcima, tehničkim i forenzičkim istragama i dr. (Pejanović, Komarčević, Čelik, 2017)

U opisanoj konstelaciji, cyber kriminal je vrsta kriminala koja beleži konstantan rast. Iako ne postoje pouzdani podaci usled čestog neevidentiranja i neprijavlivanja cyber prekršaja i krivičnih dela, procenjuje se da najmanje milion ljudi na dnevnom nivou bude izloženo nekoj vrsti cyber kriminala ili incidenta. Problem cyber kriminala ne može biti problem jedne države ili jednog fizičkog prostora, imajući u vidu da cyber prostor ne vidi granice na način kako su one ustrojene u fizičkom svetu, pa je samim tim globalna povezanost „svih i svega“, učinila da ova vrsta kriminala i u smislu žrtve i učinioca nema premca u dosadašnjem poimanju.

Da bi došlo do smanjenja obima cyber kriminala, pravni okviri moraju biti ustrojani na način koji omogućava efikasnost njihovog sprovođenja u kažnjavanju ovakvih krivičnih dela, iako i tu suštinski postoji ograničenost primenjivih propisa na nivoima konkretnih ustavno-pravnih poredaka, koji za razliku od cyber kriminala, vrlo teško rešavaju pitanje prekograničnog i jurisdikcionog.

U tom smislu, Evropska Unija je postupno pojačavala regulatorni okvir informacione bezbednosti, uvažavajući do tada prikupljena iskustva, pouke i rešenja. U tom smislu, Savet Evrope doneo je Konvenciju o visokotehnološkom kriminalu, usled zabrinutosti zbog rizika da se računarske mreže i elektronske informacije „mogu koristiti za izvršenje krivičnih dela i da dokazi koji se odnose na takva dela mogu biti sačuvani i preneseni preko takvih mreža“ (Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, Sl. glasnik RS 19/2009).

Ovom Konvencijom, države članice Saveta Evrope i druge države potpisnice ove Konvencije, potaknute su na neophodno postupanje „radi sprečavanja radnji usmerenih protiv poverljivosti, celovitosti i dostupnosti računarskih sistema, mreža i računarskih podataka, kao i zloupotebe tih sistema, mreža i podataka, za obezbeđivanje krivično-pravnog sankcionisanja, ponašanja opisanih u ovoj Konvenciji i usvajanja mera dovoljnih za delotvornu borbu protiv ovih krivičnih dela, tako što će se na unutrašnjem i međunarodnom nivou, olakšati otkrivanje, istraga i gonjenje ovih krivičnih dela, što će obezbediti uslove za brzu i pouzdanu međunarodnu saradnju“ (Ibid). Radi ujednačavanja prakse na nivou potpisnica Konvencije, došlo je do definisanja termina i njihovog međunarodnog unificiranja, na način kako je to opisano u čl. 1 Konvencije.

Važan deo opšteg regulatornog okvira u smislu opisanog predstavlja i Direktiva Evropske Unije o napadima na informacione sisteme, objavljena u Službenom glasniku EU, L218/8 dana 14.08.2013. godine, sa punim nazivom Direktiva 2013/40/EU Evropskog Parlamenta i Saveta od 12.08.2013. godine, o napadima na informacione sisteme i zamenu Okvirne Odluke Saveta br. 2005/222/JHA.

Da bi pomenuti regulatorni okvir i nastojanja bili efikasni i IKT sistemi razvili otpornost, ta problematika mora biti sagledana i u okvirima odbrambenih i nacionalnih bezbednosnih interesa i u smislu uspostavljanja i aktiviranja resursa i kapaciteta efikasne cyber odbrane, gde ovakvi kapaciteti moraju biti skoncentrisani na otkrivanje, reagovanje i oporavak od sofisticiranih cyber napada i pretnji.

Stoga je važnost razvoja komplementarnog sistema odbrane od presudnog značaja. Masovna proizvodnja hardvera i softvera i njihovih komponenti u nekim segmentima dovela je do problema sa kvalitetom i pouzdanošću, što je u pojedinim slučajevima imalo negativan efekat na zaštitu i bezbednost privatnih i poslovnih podataka.

U tom smislu, sagledana je razuđenost Evropske Unije i na teritorijalnom i na institucionalnom nivou, kao i na nivou harmonizacije svih postojećih segmenata, usled čega se došlo do zaključka koji zapravo sugerše i pomenuta strategija, a koja konstatuje da se postavljeni cilj može ostvariti isključivo putem jedinstvenog tržišta koje će garantovati bezbedne elektronske proizvode, posebno u domenu informacionih i komunikacionih tehnologija.

Kako bi se to postiglo, predložena je Direktiva o bezbednosti mreža i informacija, tzv. NIS Directiva (European Commission, COM, 2013), sa ciljem da se uspostavi obaveza svih tržišnih subjekata da preduzmu mere kojima će osigurati bezbednost sopstvenih IKT sistema kroz nabavku IKT proizvoda koji će ispunjavati postavljene bezbednosne uslove. Na ovom nivou pokrenuta je inicijativa kod javnih i privatnih subjekata sa ciljem identifikacije dobre bezbednosne prakse radi kreiranja preduslova za identifikovanje bezbednih IKT rešenja čija će se primena preporučivati.

Ključni aspekt naslonjen je na potrebu za što boljim upravljanjem rizicima i usvajanju, kako bezbednosnih standarda, tako i odgovarajućih principa sertifikacije. U iznetom kontekstu regulisanja tržišnih i bezbednosnih pravila, kao i regulative, Evropska Komisija je pred ENISA-u postavila zadatak da se angažuje na razvijanju tehničkih smernica i preporuka koje će dovesti do usvajanja neophodnih standarda i dobrih praksi u domenu bezbednosti u informaciono-komunikacionim i tele-komunikacionim sistemima. U ovom segmentu Komisija je prepoznala i razloge za dalji razvoj standarda bezbednosti i u domenu Cloud computing-a, sa posebnim osvrtom na zaštitu podataka.

5.1. Evropska strategija i politika informacione bezbednosti

Prema jednoj od opšteuvreženih definicija, informaciona bezbednost je aspekt bezbednosti koji se odnosi na sve bezbednosne rizike vezane za upotrebu informacionih tehnologija, uključujući i bezbednost podataka, uređaja, informacionih sistema, mreža, organizacija i pojedinaca.

Intenzivan razvoj informacionih i digitalnih tehnologija kao takav, donosi nesumnjive koristi i prednosti za društvo koje ih primenjuje, međutim, cena tog razvoja podrazumeva da sa njim dolaze i novi bezbednosni izazovi i rizici.

Strategija informacione bezbednosti Evropske Unije (Cybersecurity Strategy of the European Union) visokotehnološki kriminal definiše kao vrstu kriminala koja je u najvećem porastu, gde na dnevnom nivou najmanje milion ljudi, uključujući i decu, bude žrtva napada.

Sve češći napadi hakera na informacione sisteme, u mogućnosti su da značajno ili potpuno ugroze poslovanje, kako preduzeća, tako i funkcionisanje državne uprave, javnih servisa, sistema nacionalne bezbednosti, dok su pojedinci, u najvećoj meri deca, usled svoje nepripremljenosti u sve većoj meri izloženi rizicima od ucena, prevara i zlostavljanja putem Interneta.

Činjenica je da je na opštem planu upotreba IKT u porastu u svim segmentima (države, privrede i građana), a na tom trendu se zasniva i sve veći broj poslova i aktivnosti. Državni organi i institucije sve se više oslanjaju na resurse informacionog sistema, a radi lakšeg i efikasnijeg obavljanja poverenih nadležnosti. Istim putem, krenula je elektronska uprava koja na temeljima potencijala informacionih tehnologija, konstantno inovira domen usluga koje pruža.

Nema razlike ni u domenu kritične infrastrukture i delatnosti objekata od opšteg interesa. Na tom polju razvijeno je elektronsko zdravstvo i evidencija. Konstantan je rast i primenjenih aplikativnih softvera, kao i povezivanje i integrisanje baza podataka. Stoga su napadi na informacione sisteme stekli potencijal da značajno ugroze ukupno funkcionisanje države, za šta postoji veći broj primera, a težina posledica je direktno zavisna po obuhvatu i umreženosti sistema državne uprave. Primera radi, 2007. godine, Estonija je preživela izuzetno ozbiljan cyber napad na državne i IKT sisteme i na IKT sisteme finansijskih institucija što je dovelo do blokade i platnog prometa i sistema e-uprave, koji je još tada u ovoj državi bio veoma razvijen.

Da ovo nije samo primer usamljenog, već i veoma ozbiljnog slučaja, praksa prepoznaje i svetski poznati incident vezan za računarski virus „Stuxnet“ koji je infiltriran u informacioni sistem nuklearnih postrojenja u Iranu. Ovaj virus je zapravo ciljano napao određene delove infrastrukture iranskog nuklearnog programa, tzv. centrifuge putem hakovanja parametara njihovih kontrolera i interfejsa, čime je umalo izazvana katastrofa ozbiljnih razmera sa nuklearnom konotacijom.

Početakom 2016. godine desio se i hakerski napad na Centralnu banku Bangladeša, kojom prilikom je usled krađe ključeva svih sistema, došlo do izdavanja većeg broja naloga za prenos novčanih sredstava sa računa banke Federalnih rezervi u Njujorku u iznosu od 81 milion dolara.

Na talasima informaciono-komunikacionih tehnologija, pored ovih, nastale su i mnoge druge pretnje koje su usmerene na ugrožavanje nacionalne bezbednosti, a koje prema odredbama međunarodnog prava spadaju u oblik neoružane agresije, koja je postala ne tako retka u sistemu napetih međunarodnih odnosa.

Sudeći po ovim saznanjima, može se bez sumnje razumeti da je stepen razvijenosti država proporcijalan broju elektronskih servisa i usluga koje oni pružaju, a što onda izaziva korelaciju sa nivoom i stepenom rizika kojima su bile, ili će biti izložene ukoliko strateški ne pristupe rešavanju pitanja svoje cyber bezbednosti.

Da bi cyber bezbednost bila na visokom nivou, na visokom nivou mora biti i sistem zaštite informacija koje su u opticaju u digitalnim i komunikacionim sistemima i krugovima. Da bi to bilo moguće, Evropska Unija se okrenula razvoju jedinstvenog digitalnog tržišta, što sa jedne strane predstavlja informaciono bezbednosni projekat, a sa druge strane ulaganje za koje se iznosi pretpostavka da bi moglo uvećati bruto društveni proizvod EU za približno 500 milijardi evra na godišnjem nivou.

Razvoj povezanih tehnologija koje uključuju elektronska i beskontaktna plaćanja, cloud computing i machine-to-machine komunikacija, predstavlja tehnologije kojima će građani morati da ukažu poverenje. Međutim, praksa je pokazala, a to potvrđuje i istraživanje Eurobarometra iz 2012. godine, da skoro 1/3 Evropljana nisu bili sigurni da će biti sposobni da koriste internet za bankarstvo i kupovinu. Sa druge strane, ogromna većina građana Evrope ističe da izbegavaju on-line otkrivanje svojih ličnih podataka i informacija, upravo iz razloga bezbednosti. Ovakav stav se pravda statistikom Evropske Unije da je više od 1 u 10 korisnika Interneta već bio žrtva on-line prevare.

Može se reći da je moderno doba poslednje generacije stvorilo digitalni svet, kao svet koji donosi izuzetne koristi, ali i svet koji je izuzetno ranjiv. Incidenti u domenu cyber bezbednosti, bez obzira da li su se dogodili namerno ili slučajno, rastu do alarmantnih razmera imajući u vidu da mogu izazvati disrupciju čak i kod onih životno važnih servisa koje smo usled civilizacijskih

dometa počeli uzimati zdravo za gotovo, a to su: vodosnabdevanje, zdravstvo, snabdevanje električnom energijom i u krajnjoj meri mobilni servisi.

Ovakva dešavanja predstavljaju opasnost zato što njihovo poreklo može uključivati razne pozadine, počev od čisto kriminalnih, preko politički motivisanih, pa do terorističkih ili državno sponzorisanih napada, ali i potpuno prirodnih katastrofa izazvanih nenamernim greškama.

Jedan od problema zašto se ekonomija Evropske Unije suočava sa cyber kriminalom jesu i aktivnosti koje su usmerene i protiv njenog privatnog sektora i individualnih građana.

Porast primene računara i računarskih komunikacija povećava uzorak ranjivih i njihov dijapazon, a time cyber kriminalci bivaju motivisani da iznova sofisticiraju metode za neopaženu infiltraciju u IKT sisteme kako bi iz njih izvukli ključne informacije radi neposredne zloupotrebe ili zaključavanja podataka radi ucene otkupom. Ovi okviri doveli su do narastanja i ekonomske špijunaže i maliciozne aktivnosti sponzorisanih od strane pojedinih država u cyber prostoru, što je samo po sebi proizvelo još jednu kategoriju pretnji, kako samoj Evropskoj Uniji, tako i vladama država članica, ali i njihovim kompanijama i građanima.

Ovakav splet događaja pretili da ugrozi ključne tekovine Evropske Unije u domenu privatnosti i ljudskih prava, imajući u vidu sve veću dostupnost tehnologija za nadgledanje i kontrolu građana. U tom smislu Evropska Unija ističe svoje zalaganje da promoviše on-line slobodu, kao i da osigura poštovanje temeljnih ljudskih prava u on-line okruženju.

Bezgranični i višeslojni internet projekat postao je jedan od najsnažnijih instrumenata globalnog razvoja koji se najčešće odvija bez vladinog nadzora i uređenja. Stoga je Evropska Unija krenula putem da svoje osnovne vrednosti primeni na isti način i u digitalnom i u fizičkom svetu, kako bi zakoni i ostala regulativa bili primenljivi u svim oblastima svakodnevnog života, što uključuje i cyber domen.

Ovakve tendencije zasnovane su na načelima fundamentalnih ljudskih prava i njihovih temeljnih vrednosti. Evropska Unija vidi reciprocitet u tome da ljudska prava pojedinaca ne mogu biti obezbeđena u novom dobu, bez toga da se obezbedi sigurno mrežno okruženje i bezbedni informacioni sistemi.

S tim u vezi, svako deljenje informacija za svrhe cyber bezbednosti na individualnom planu iz tog razloga mora biti u skladu sa evropskim propisom o zaštiti ličnih podataka, u kom smislu moraju uvek i u svakom slučaju biti uzeti u obzir lična prava na ovom polju.

Shodno navedenom, Evropska vizija prezentirana u Strategiji cyber bezbednosti Evropske Unije, artikulisana je u 5 strateških prioriteta, kako bi mogao biti pružen odgovor na napred iznete izazove. Ti izazovi su sledeći:

- Dostizanje cyber otpornosti, tj. drastično smanjenje cyber kriminala;
- razvijanje politike cyber odbrane;
- sposobnosti vezane za zajedničku bezbednost i odbrambenu politiku;
- razvijanje tehnoloških i industrijskih resursa za cyber bezbednost;
- uspostavljanje koherentne međunarodne politike za cyber prostor za Evropsku uniju i promovisanje ključnih evropskih vrednosti (Nedeljković, S. 2015:144).

Činjenica je da se cyber incidenti ne zaustavljaju na granicama ako se te granice nalaze u okvirima svepovezane digitalne ekonomije i društva. Stoga, svi činioци, počev od NIS nadležnih vlasti, preko CERT-ova i primene zakona u industriji, imaju obavezu da zajedničkim zalaganjem, kako na nacionalnom, tako i na nivou cele Unije, rade zajedno da ojačaju domet cyber bezbednosti. Razrada uloga i nadležnosti faktora u ovom poslu, ključni je izazov u Evropskoj Uniji, međutim kompleksnost pitanja i diversifikovani okvir učesnika, jasno govore da centralizovani evropski nadzor na to ne može adekvatno odgovoriti. Stoga su nacionalne vlade država članica najbolje pozicionirane da organizuju sistem prevencije, ali i odgovora na cyber incidente i napade u saradnji sa privatnim i javnim sektorom. Svakako, priroda rizika bez granica često će zahtevati odgovor koji će uključivati i nadnacionalni nivo, tj. nivo Unije.

Uporedo sa razgranatom mrežom na nacionalnom nivou država članica, kao i na nivou Evropske Unije, postoji i nivo sa velikim brojem učesnika koji se bave pitanjima cyber bezbednosti. Tu se najpre misli na ENISA-u, Europol - EC3 i EDA (European Defence Agency), odnosno Evropsku odbrambenu agenciju, imajući u vidu da one operišu na velikom broju polja, bilo samostalno ili zajednički, na kom nivou analiziraju trendove procene rizika, vrše obuke i dele iskustva o najboljim praksama.

Kada je u pitanju agencija EDA, u njoj je ustanovljen Cyber Defence Project Team ili Projekt tim za cyber odbranu koji ima sve potrebne potencijale i resurse da bude upotrebljen kao vektor za kordinaciju akcija na polju cyber odbrane.

Programski odbor Europol - EC3, povezaće se pored ostalih, sa Eurojust-om, Cepol-om, a države članice putem EU Cybercrime Task Force¹¹ sa EU jedinicama za borbu protiv cyberkriminala, kao i jedinicama država članica EU, onda ENISA-om i Evropskom Komisijom kako bi pružili šansu za razmenu njihovih ekspertskih saznanja, a sve to kako bi svi zajedno obezbedili da EC3 svoje akcije u borbi protiv cyber kriminala sprovede na partnerskom nivou i uz poštovanje prava, obaveza i nadležnosti svih ostalih učesnika u ovoj složenoj strukturi.

U međunarodno-pravnom smislu, Evropska komisija i njen visoki predstavnik zajedno sa državama članicama koordiniraju međunarodne akcije na polju cyber bezbednosti. Evropska komisija, visoki predstavnik i države članice, uredili su principe angažovanja kojima će se putem politike dijaloga i u saradnji sa međunarodnim partnerima i organizacijama, kao što su Savet Evrope, OECD, OSCE, NATO i UN rešavati ova pitanja.

4.2. Evropski odgovor na slučaj cyber krize velikih razmera

Cyber krize velikih razmera definitivno su u stanju da utiču na vlade država članica Evropske Unije, ali i na poslovne entitete i pojedince. Kao rezultat strategije i posebno predložene Direktive za mreže i informacione sisteme (NIS), prevencija, detekcija i odgovori na cyber incidente moraju se popraviti, a da bi to bilo moguće, učesnici u ovim poslovima na nivou Unije moraju dosledno i blagovremeno razmenjivati informacije o svim većim cyber incidentima i napadima. U tom smislu, mehanizmi odgovora na cyber incidente i napade razlikovaće se u zavisnosti od prirode veličine i prekograničnosti posledica konkretnog incidenta.

Ukoliko se desi da incident ima ozbiljne posledice po kontinuitet poslovanja, NIS Direktiva predviđa aktivaciju nacionalnih ili NIS planova za saradnju na nivou Unije, sve u zavisnosti od dometa i prekogranične prirode predmetnog incidenta. U tom slučaju mreža NIS nadležnih vlasti biće aktivirana za potrebe razmene informacija i podrške. Ovakav pristup treba da omogući, kako očuvanje, tako i reuspostavljanje narušenih mrežnih potencijala ili servisa.

¹¹ Jedinica za specijalne operacije protiv cyber kriminala, sastavljena od šefova EU Cybercrime Units

Ukoliko incident po svojoj prirodi u pozadinskom smislu ima kriminal, Europol - EC3 mora biti obavešten kako bi zajedno sa vlastima pogođenih zemalja inicirali istragu, obezbedili dokaze, identifikovali izvršioce i na kraju obezbedili da oni budu krivično gonjeni i osuđeni.

Ukoliko bi incident po svojoj prirodi bio iz domena cyber špijunaže ili državno sponzorisani incident radi napada sa posledicama po nacionalnu bezbednost, vlasti za nacionalnu bezbednost i odbranu bi u tom slučaju u proces uključile sve ostale relevantne nadležne organe i institucije, kako bi oni bili obavešteni da su pod napadom i kako bi se mogli braniti i zaštititi. Mehanizmi ranog upozoravanja bi u tom slučaju bili aktivirani, a ako je potrebno i procedure kriznog upravljanja. U svakom slučaju, ukoliko bi cyber napad, odnosno incident izazvao posledice većih razmera, stvorili bi se uslovi da država članica pokrene klauzulu Evropske solidarnosti prema čl. 222 Sporazuma o funkcionisanju Evropske Unije.

Ukoliko bi incident bio takav da kompromituje lične podatke građana, nacionalne vlasti za zaštitu podataka, odnosno Nacionalne regulatorne vlasti bi se morale uključiti u skladu sa Direktivom 2002/58/EC.

Na kraju, upravljanje cyber incidentima i napadima biće potpomognuto mrežom za podršku međunarodnih partnera Unije, što samo po sebi može uključivati i tehničko ublažavanje posledica, krivičnu istragu ili aktivaciju mehanizama za odgovor putem kriznog upravljanja.

4.3. CSIRT - Mreža nacionalnih timova za odgovor na sajber incidente

Aktuelni cyber trendovi su svojim kontinuiranim delovanjem pokrenuli raznovrsne procese u cilju podizanja spremnosti EU kao celine, ali i država članica da se odrede prema cyber pretnjama. Međutim, pravi realni i održivi pomak na ovom planu učinjen je tek izradom NIS Direktive koja je zapravo najadekvatniji korak ka uvođenju jedinstvene i ujednačene cyber regulative na prostorima cele Evropske Unije. Na tom polju EU već određeno vreme sprovodi intenzivne radnje, kako bi pravno regulisala veoma važno pitanje, kao što je zaštita ličnih podataka, ali i bezbednost informacionih sistema. Kako bi mogao biti dat adekvatan odgovor, doneta je NIS Direktiva koja je uredila načine postupanja država članica u odnosu na pretnje iz cyber prostora, načine upravljanja rizicima koji prete iz cyber okruženja i uređenje i uspostavljanje formalno-pravnog okvira u kome će ova pitanja biti kompletno uređena.

Uporedo sa navedenim, Evropska Unija je donela i Uredbu GDPR o kojoj je već bilo reči, a kojom je zaokružila mere i sankcije u ovoj oblasti, odnosno pravila koja kompanije moraju obavezno primenjivati u smislu zaštite ličnih podataka korisnika na Internet-u, a na način koji nije omeđen granicama. GDPR uredba od trenutka njenog stupanja na snagu sredinom 2018. godine, automatski je integrisana u zakonske propise svake države članice. Ona služi ne samo da uredi ovu oblast, nego i da određene smernice na koji način bi države članice morale urediti svoj preostali pravni okvir.

Reformisano zakonodavstvo o zaštiti podataka pruža brojne mehanizme za neometan prenos podataka u međunarodnim okvirima. Osnovna svrha tih pravila i mehanizama jeste da osigura da lični podaci građana Evrope budu zaštićeni u svakom trenutku njihovog prekograničnog prenosa. Radi rešavanja ovog problema, u posebnom dokumentu Evropske Komisije je predstavljen sveobuhvatan i pojednostavljen EU okvir za razmenu i zaštitu ličnih podataka namenjen globalnom okruženju (Pejanović, Komarčević, Čelik, 2017).

Proces donošenja ove Uredbe nije bio nimalo lak ni jednostavan. EK je još 2013. godine predložila da se krene sa izradom Direktive, kako bi se na taj način obezbedio visok nivo, kako mrežne, tako i informacione bezbednosti na nivou cele Unije. GDPR uredba je dala dobre osnove za donošenje NIS Direktive koja je usvojena u julu 2016. godine pred Evropskim parlamentom, nakon čega je ista stupila na snagu i krenula sa primenom. Međutim, stupanje na snagu Uredbe GDPR je moralo biti odloženo do sredine 2018. godine radi prilagođavanja svih aktera njenim standardima.

Uporedo sa navedenim, Evropska Unija je razvijala i svoju cyber strategiju kao krovni dokument visokog nivoa koji ima za cilj da uredi okvir za ostvarivanje ciljeva, ali opredeljuje i uloge i odgovornosti nadležnih tela i drugih činilaca.

Da bi primena ovih dokumenata bila obezbeđena, NIS Direktiva je pred države članice postavila zahtev da one uspostave jedan ili više CSIRT timova (Computer Security Incident Response Team) kao službe čiji je osnovni zadatak promptna reakcija na incidente u domenu bezbednosti informacione infrastrukture i sistema.

CSIRT služba radi svoje efikasnosti počiva na angažovanju iskusnih eksperata iz domena informacionih tehnologija. Njihova uloga je rešavanje bezbednosnih rizika i incidenata. Ovi timovi organizovani su tako da obezbeđuju visok nivo i stalnu dostupnost svojih usluga, njihovo

funkcionisanje obezbeđuje se na lokacijama koje su provereno bezbedne, a opremljeni su najmodernijim sistemima za upravljanje postavljenim zahtevima. S tim u vezi, države članice su u obavezi da angažuju dovoljno stručnih službenih lica u cilju osiguranja dostupnosti korisnicima u svakom trenutku, a što se opet obezbeđuje korišćenjem redundantne infrastrukture koja garantuje u najvećoj mogućoj meri kontinuitet u radu.

Kako se sigurnosni incidenti mogu dogoditi bilo kada, napadi na informacione sisteme često se događaju van radnog vremena, jer se tako entitetima koji su predmet napada izazivaju najveća šteta i posledice. CSIRT kao sistem predstavlja produženi način zaštite od neželjenih i nepredviđenih događaja i istovremeno i najspremniji sistem za brzo i proaktivno reagovanje na pretnje u trenutku koji je što bliži njihovom nastanku. CSIRT kao sistem u takvoj situaciji pruža odgovarajuća sredstva za prosleđivanje izveštaja o ovim incidentima svim nadležnim telima i drugim korisnicima njihovih usluga, imajući u vidu da je širenje ovako nastalih informacija uvaženo kao važan resurs za adekvatnu cyber odbranu. Samim tim, CSIRT je uspostavio mehanizme koji funkcionišu 24 časa, 7 dana u nedelji, 365 dana godišnje.

Opšte usluge CSIRT sistema čine sledeće: utvrđivanje kriminalnih aktivnosti „belih kragini“, oporavak podataka, praćenje zloupotreba interneta i na internetu, praćenje krađa vlasničkih informacija, prikupljanje dokaza o incidentima, rukovanje, odnosno, upravljanje incidentima, računarska forenzika, odgovor na cyber incidente 24/7, oporavak od katastrofe, testiranje dubine i efekata izvršene penetracije u sistem, te obezbeđivanje sistema za rešenja prilikom otkrivanja upada u sistem i sl.

Osim proaktivnih modela delovanja, sistem CSIRT pruža i reaktivne usluge iz domena istrage za potrebe poslovnih entiteta koje su neophodne nakon neželjenih događaja, odnosno incidenata koji su se desili u oblasti cyber bezbednosti. U tom delu, CSIRT je specijalizovan da pruža sledeće usluge:

- Utvrdi da li je određeni neželjeni događaj ili bezbednosni incident potrebno tretirati kao predmet specijalizovane istrage;
- Sprovodi odgovarajuće istrage o tome šta je glavni uzrok, izvor i priroda bezbednosnog incidenta, kao i da izvrši stručnu procenu nivoa nastalih posledica i šteta uz davanje stručnih preporuka za efektivniji odgovor na nastalu krizu;

- U slučaju da se radi o cyber krivičnom delu, koordinira aktivnosti neophodne radi očuvanja dokaza, vrši ispitivanje oštećenih i sl.;
- Upravlja sistemom za obaveštavanje i razmenu informacija u domenu sistema korisnika;
- Upravo sa tim priprema odgovarajuće izveštaje o nalazima istrage, uzrocima neželjenog događaja, naučenim lekcijama i stečenom znanju, kao i preporučenim merama za buduće delovanje koje je neophodno kao predlozi i preporuke menadžmentu.

Po svemu sudeći, cilj sistema, odnosno mreže CSIRT je organizovanje efikasnog bezbednosnog upravljanja problemima i krizama koji su zasnovani na proaktivnim pristupima bezbednosnim propustima i incidentima, te efikasna reakcija na sve izazove informacione bezbednosti.

U sklopu navedenog, cilj CSIRT sistema, odnosno mreže, služi i tome da institucionalizuje i centralizuje sistem izveštavanja o incidentima, koordinira sistemskim odgovorom na bezbednosni incident koji može imati negativan uticaj na veliki broj informacionih sistema, pruži direktnu podršku i tehničku pomoć klijentima, promovise bezbednosne računarske politike unutar organizacije (i u odnosu na korisnike), podstiče proizvođače da budu proaktivni u odgovorima na probleme i prigovore vezane za njihove proizvode i institucionalizuju povezivanje sa pravnim i kriminalističkim istražnim organima.

Tokom samog incidenta, CSIRT može vršiti praćenje revizijskih logova informacionog sistema, kao i da izveštava o svim neuobičajenim ili suspektim aktivnostima. Takođe, CSIRT izveštava o bilo kakvim neuobičajenim događajima u kritičnim sistemima i vrši informisanje najvažnijih članova mreže o operativnim procedurama, štiti dokaze o predmetnom incidentu prema smernicama za korisnike i uputstvima stručnog tima, vrši procenjivanje nastale štete na sistemima i podacima, obavlja izveštavanja nadležnih državnih organa na nacionalnom i lokalnom nivou, pomaže u utvrđivanju opsega izvršenog upada u sistem i identifikovanja pristupne tačke sistemu (ranjive tačke) i izvoru upada, sve kako bi na tome izradio preporuke za eliminisanje sporne tačke pristupa putem koje je izvršen upad u sistem i njegova kompromitacija.

Pored ostalog, CSIRT može vršiti kategorizaciju bezbednosnih incidenata, utvrditi da li predmetni incident determiniše potrebu za daljom istragom, da sprovede istragu, dodaje neophodne nove članove za potrebu istrage, aktivno prati i pruža zaštitu mreži od dejstva računarskih virusa, održava baze podataka i održava podatke o incidentima i priprema izveštaje i

daje preporuke menadžmentu. U smislu iznetog, CSIRT-ova uloga je i u domenu pomoći kod upravljanja timovima za reagovanje na incidente unutar organizacije i to tako što pomaže u definisanju standarda, prakse, usluga i alata.

Ovakav pristup i organizacija protiv cyber kriza i incidenata, predstavlja jasan i smislen odgovor na činjenicu da institucije i kompanije u Evropi nisu dovoljno zaštićene od cyber napada, a posebno jer su cyber napadi suštinski takvi da su jeftini i da se uvek odvijaju pod velom tajne, usled čega ih je lako demantovati, što samo po sebi povećava rizik po informacije i sisteme, obzirom da je upravo iz ovih razloga cyber napad kao vrsta elektronskog kriminala jednako atraktivna forma i pojedincima i teroristima, ali i državnim agencijama i vladama.

U smislu toga, preduzimanje odgovarajućih tehničkih i organizacionih mera za upravljanje rizicima koji prete mrežnim i informacionim sistemima na kojima počiva svakodnevno poslovanje, zahteva implementiranje svih mogućih mera kojima će se sprečiti ili svesti na najmanju moguću meru efekti svakog incidenta, kako bi se na taj način obezbedio i kontinuitet poslovanja i usluga koje kompanije i njihovi informacioni sistemi pružaju na tržištu.

Opisani proaktivni pristup predstavlja odgovor ne samo na incidente, već i na to što se veliki broj incidenata često i ne prijavljuje, shodno čemu je jasno da CSIRT mreža predstavlja jedan adekvatan i dobro osmišljen, ali i krajnje realan odgovor na cyber krize i incidente i malih i velikih razmera, tj. sistem koji nudi u praksi razne potvrđene mehanizme za upravljanje cyber krizama i prevencijom visokotehnološkog kriminala.

Za visokotehnološki kriminal je odavno postalo jasno da se protiv njega ne može boriti i delovati samostalno, već uvek i isključivo sistemski, mrežno i umreženo, a posebno jer su izvršioци cyber kriminalnih dela najčešće u jednoj državi, oštećeni u drugoj, dok računarska ili infrastruktura putem koje je izvršeno određeno kriminalno delo u nekoj trećoj zemlji ili u više zemalja istovremeno, iz kog razloga uska saradnja različitih nadležnih službi mora biti na opisani način uređena i primenjena krajnje proaktivno, tj. do mere koja ne deluje deduktivno na dostignuti nivo ljudskih prava u EU, odnosno na nivo ljudskih prava koja se garantuju.

5. Koordinisani odgovor na prekogranične cyber incidente/krize

Upotreba informaciono-komunikacionih tehnologija proizvela je, usled promene poslovnih koncepata i njihovog stalnog inoviranja, u najvećem broju slučajeva i određen stepen zavisnosti

od njihovog adekvatnog funkcionisanja. Svi moderni ekonomski sektori usled dinamičnih informatičkih trendova, učinili su da preduzeće i građani postanu trajno i međusobno povezani i suštinski međuzavisni, ne samo lokalno, već i prekogranično, što je verovatno više nego ikada ranije u istoriji.

Upravo zbog toga, nastala je opasnost od cyber incidenata, ako se ima u vidu da oni predstavljaju faktor koji ima uticaj kako na pojedinačne države, tako i cele unije država, kao što je npr. Evropska Unija u kojoj postoji jasna međuzavisnost između obima i stepena informatičkog razvoja, primene informacionih tehnologija i sistema, kao i rizika koje to nosi, a koji bi usled cyber incidenta širih razmera mogao prouzrokovati ozbiljne poremećaje, kako na tržištu jedne države, tako i na svim povezanim tržištima, a posebno jedinstvenom digitalnom nadnacionalnom tržištu kakvo je evropsko.

Cyber kriza može nastati na slučajevima cyber incidenata koji su učinili uticaj na veći broj sektora i aktivnosti, usled čega su postali preobimni da bi ih jedna država samostalno mogla rešiti. Kako se dešavaju krize koje utiču na dve ili više država, a na koje takav incident ima dalekosežne tehničke, ekonomske i političke efekte, jasno je da je tako pogođenim državama potrebna podrška, koordinacija i odgovor kakav se može pružiti isključivo na političkom nivou cele Evropske Unije.

U takvom slučaju, prednost unije država jeste mogući združeni odgovor koji sadrži i kibernetičke i nekibernetičke mere za ublažavanje nastalih posledica. Cyber incidenti predstavljaju vrstu incidenata koje nije moguće predvideti, iz kog razloga su i reagovanja na njih uvek međuzavisna o obimu i dinamici, o sredstvima koja su primenjena, kao i činjenici zavisnoj od geografskog područja iz koga incidenti i krize dolaze, pa samim tim i od toga da li se posledice tih incidenata pojavljuju u jednoj ili više zemalja.

Efikasni odgovori na cyber incidente i krize, posebno one velikih razmera koji se dešavaju na nivou cele Evropske Unije zahtevaju brzu i efikasnu multidisciplinarnu saradnju svih činilaca i aktiviranje svih kapaciteta Unije kako bi se uspostavila puna sposobnost aktiviranja mehanizama i dobro uvežbanih postupaka, saradnje i razmene podataka i to sve po principu koji jasno uređuje odgovornosti i uloge aktera, kako na nivou država članica, tako i na nivou cele Unije kao sistema povezanih država.

U cilju reagovanja na ovakve izazove, pristupilo se razvoju temeljnih mehanizama saradnje u domenu cyber incidenata u Evropi koji će kao takvi pojačati ukupnu prekograničnu saradnju, a kako bi putem nje bila obezbeđena puna pripravnost u odnosu na cyber incidente i reaktivne mehanizme odgovora.

6. Da li je iko bezbedan?

Opisani izazovi digitalnog poslovanja zasnovanog na informacionim i komunikacionim tehnologijama, očigledno predstavljaju prostor u kome bezbednost počiva na tankoj liniji između dve krajnosti. Brojni primeri pokazuju da nisu bezbedni ni veliki, ni mali, ni kompanije, ni organizacije. Da je to zaista tako, govori i najnoviji primer hakovanja američke NASA, odnosno njene laboratorije za mlazni pogon, gde je jeftinim računarom od svega 25 dolara došlo do ugrožavanja najznačajnijih segmenata IT mreže ove svemirske agencije.

Napad hakera na NASA odigrao se u aprilu 2018. godine kada je neovlašćeno otuđeno oko 500 mb zaštićenih podataka i informacija iz jednog od glavnih NASA sistema zaduženog za misije. Slučaj je učinio da se njime „pozabavi“ i Kancelarija generalnog inspektora NASA, Odseka za reviziju koji je objavio opsežan izveštaj o krajnje lošoj bezbednosnoj politici i stanju u ovom odeljenju NASA, ali ne samo u njemu.

Ono što se dogodilo u NASA prikaz je napred pomenute tanke linije između bezbednosti i rizika, a konkretan primer ukazuje na to da je do ugrožavanja informacionog sistema NASA došlo usled propusta u vezi sa načinom na koji je laboratorija NASA za mlazni pogon (JPL) upravljala svojom informacionom infrastrukturom i uređajima. Ispostavilo se da ova NASA laboratorija nije vršila nadzor nad svojom mrežom i bazom podataka „ITSDB“ koja služi za praćenje toga koji su uređaji i oprema povezani sa unutrašnjom mrežom.

Propustom sistemskih administratora NASA došlo je do propusta u ažuranju inventara uređaja koji su povezani na sistem, te je utvrđeno da je jedan od sistemskih administratora čak propuštao da bude ažuran u tome da redovno vrši „inventar“ i unosi nove uređaje u „ITSDB“ i bezbednosno ih tretira. Tako se dogodilo da je na mrežu NASA neautorizovano priključen maleni Raspberry Pi računar koji je nakon tog neovlašćenog priključenja iskorišćen kao vektor preko koga je haker pristupio JPL mreži i izvukao dragocene podatke.



Slika br. 17 Raspberry Pi - Single board computer

Na ovaj način se dogodilo da jedan jeftin i skoro banalan uređaj, neautorizovano priključen na mrežnu infrastrukturu izuzetne važnosti, potkopa čak i sisteme koji služe za slanje robota u svemir.

Šta je zapravo Raspberry Pi? Raspberry Pi je maleni računar koji se sastoji od jedne elektronske ploče veličine kreditne kartice, koji je projektovan za potrebe učenja osnova informatike u školama u zemljama u razvoju.

Kada je u pitanju to kakvi su podaci nestali u ovakvom Raspberry Pi hakerskom napadu na američku svemirsku agenciju, pored ostalog treba navesti da su u pitanju osetljivi lični podaci nekoliko hiljada službenika NASA. Ovi podaci pored ostalog sadrže i brojeve njihovog socijalnog osiguranja kao najosetljiviji lični podatak.

Kako je ovaj napad otkriven tek u oktobru 2018. godine, podaci o ovom incidentu bili su donekle skrivani, sve dok vest o incidentu nije procurila u javnost, a to se dogodilo nakon što su zaposleni u NASA dobili interno obaveštenje o izvršenom cyber napadu. Najveća šteta je što je ovakav događaj izuzetno negativno uticao na ugled i kredibilitet NASA, koja je do tada bila respektabilna institucija svetskog ranga. Na ovakav pad kredibiliteta američke svemirske agencije posebno je uticala činjenica da su u ovom hakerskom napadu iz NASA izvučeni podaci za period od čak 12 godina, tačnije od jula 2006. do oktobra 2018. godine.

Na opisani način izvučena je baza podataka ljudskih resursa NASA u delu njihove civilne službe, koja obuhvata, kako one koji su u ovoj agenciji dobili posao, tako i one koji su napustili ovu agenciju u tom periodu, pa sve do onih koji su interno premeštani u NASA na različite pozicije u tom periodu.

Ovaj zastrašujući primer u kome je sve ono negativno u cyber bezbednosti prikazano kroz jednu od tehnološki najnaprednijih organizacija na svetu, prikazao je da čak i takve institucije i

organizacije često nisu u stanju da se nose sa pitanjem sopstvene cyber bezbednosti, što svima ostalima jasno govori da više ne postoji niko ko ne može postati žrtva cyber napada i cyber kriminala, pa je nepreduzimanje onih dostupnih i propisanih mera proaktivne zaštite u konkretnom slučaju, bilo da se radi o tehničkom nivou ili nivou ljudskih resursa, apsolutno na granici razuma.

Kompanije koje nisu u stanju da shvate i prihvate obavezu da je za njihov rast, opstanak i bezbednost neophodno stalno raditi sa zaposlenima i proveravati ih, kako u delu toga da li se pridržavaju preporuka za korišćenja bezbednih lozinki, tako i kada je u pitanju otvaranje iz nepažnje ili radoznalosti nepoznatih linkova ili fajlova koji su prilozi spornih e-mail poruka, očigledno biraju da ih vreme „obriše“ sa tržišta.

Da napred opisano nije usamljeni incident kada je u pitanju ova svemirska agencija, govori još jedan primer velikog tzv. “Data Breach“-a, iz 2016. godine, kada je na sličan način iz ove agencije izvučeno 276 GB krajnje osetljivih podataka i informacija, koji su se kretali od logova vezanih za letove, do najličnijih podataka više hiljada zaposlenih u NASA.

Prikaz osetljivosti digitalnog poslovanja, kakav je dat kroz primer rada i funkcionisanja NASA, zapravo leži na kumulativu, pa čak i sinergiji nebezbednog ponašanja zaposlenih, od najnižih, pa sve do najviših nivoa hijerarhijske lestvice, dok je sa druge strane u tehničkom smislu celokupni rizik nastao putem zloupotrebe jeftine igračke koja je u NASA mreži prikazala sve karakteristike ranjive internet stvari, čime je na krajnje očigledan način došlo do pokaznog primera ogromne ranjivosti visoko rafiniranih sistema putem segmenta u njihovom lancu bezbednosti.

Činjenica je da ovaj primer pokazuje određeni splet okolnosti i kada je u pitanju nebezbedno ponašanje zaposlenih, u kome je neko od zaposlenih neovlašćeno uneo i priključio na mrežu sporni Raspberry Pi uređaj, koji nakon priključenja nije od strane sistem administratora popisan i bezbednosno obrađen, pa je haker, upravo na ranjivosti ovog neovlašćeno unetog uređaja u objekte i mrežu NASA, a koji je potom neovlašćeno priključen na njen mrežni sistem, izveo celokupni hakerski napad i zaobišao bezbednosne protokole. Ovaj napad i celokupna situacija u vezi njega može nam dati jasan indikator da ovakav splet događaja kojim je ozbiljno kompromitovana NASA možda i nije bio slučajan.

Prema izveštaju „Cyber Management and Oversight at the Jet Propulsion Laboratory“ od 18. juna 2019. godine, koji je sačinjen od strane NASA Kancelarije glavnog inspektora (Kancelarije

za reviziju), otkriveni su još neki važni detalji o „Data Breach“ incidentu koji se dogodio u NASA.

Iz ovog izveštaja, sačinjenog na čak 49 strana, proizilazi da su hakeri pored napred iznetog izvukli čak 23 fajla, od čega su 2 sadržala informacije o propisima o međunarodnom prometu oružja u vezi sa laboratorijom za naučnu misiju na Marsu (Cyber Management and Oversight at the Jet Propulsion Laboratory, 2019). Problem sa podacima koji su ovde i ovako „procureli“ u stvari pokazuje da je NASA JPL odeljenje, zapravo odeljenje zaduženo za rad na planetarnoj robotizovanoj svemirskoj letelici, kao što je „Curiosity Rover“ i različitim satelitima koji orbitiraju oko planeta u sunčevom sistemu.

Pored toga, ovo odeljenje upravlja i sa NASA Deep Space Network (Mreža dubokog svemira), što je zapravo svetska mreža povezanih satelitskih tanjira koji se koriste za slanje i prijem informacija sa NASA svemirskih letelica koje se nalaze u aktivnim misijama, što čini razmeru ovih incidenta još jasnijom.

Istražitelji ovog slučaja su rekli da je i pored navedenog neovlašćenog pristupanja mreži, laboratorija JPL-a i 28. aprila 2018. godine doživela hakerski napad, kada je haker pristupio njihovoj IT mreži, usled čega je nakon otkrivanja ove intruzije još nekoliko drugih postrojenja NASA moralo biti isključeno sa mreže iz straha da će napadači, obzirom na njihova saznanja o unutrašnjoj arhitekturi i konfiguraciji sistema NASA, verovatno biti u stanju da „provale“ i u preostale delove ovog mrežnog sistema.

Ova vrsta napada klasifikovana je kao „Napredna uporna pretnja“, imajući u vidu da je napad trajao približno godinu dana bez toga da je bio naslućen ili detektovan. Iz ovog razloga proširena je i istraga o ovom slučaju.

Jedan od temeljnih propusta NASA JPL mreže bio je i taj da ona nije bila interno podeljena na više manjih segmenata, iako je to osnovna bezbednosna praksa, koja, ako se dosledno primenjuje hakerima značajno otežava situaciju da i kada „provale“ u sistem, kroz njega ne mogu sa lakoćom da se kreću, kompromituju podatke i proizvode posledice.

Još jedna od ključnih zamerki istražitelja Glavnog inspektorata NASA bila je i to što je na ovom slučaju otkriveno i da IT osoblje NASA JPL sa značajnim vremenskim zaostatkom prilazi

rešavanju bilo kog bezbednosnog problema, što je možda jedan od ključnih razloga zašto je napad neprimećeno trajao približno godinu dana.

Sa druge strane, utvrđeno je da administratori IT JPL-a, čak i kada bi utvrdili postojanje potencijalne ili aktuelne pretnje za IT sistem posredstvom neke od njegovih ranjivosti, taj problem nisu u pojedinim slučajevima rešavali i duže od 180 dana.

Da ovaj incident nema samo konotaciju odnosa između hakera i NASA, govori i primer da je u decembru 2018. godine američko Ministarstvo pravde optužilo 2 kineska državljanina radi hakovanja NASA, Cloud provider-a i američke Mornarice (Indictment, 18 CRIM 891, 17.12.2018).

Prema ovoj optužnici, ova 2 hakera bili su članovi elitne kineske hakerske jedinice poznatije kao „APT 10“, za koju se pretpostavlja da iza nje stoji kineska vlada. Na ove hakere je stavljena sumnja da su pored JPL-a napali i NASA Goddard svemirski centar, međutim američko Ministarstvo pravde nije dalo bliže podatke o ovim intruzijama.

Potvrđeno je i da je u decembru 2018. godine NASA obelodanila još jedan incident ove vrste, a to je incident odvojen od onog koji se desio u aprilu 2018. godine, usled čega se radi o incidentu koji je zapravo otkriven u oktobru 2018. godine, kada su od NASA ponovo ukradeni podaci o zaposlenima.

Sudeći po ovim primerima koji potiču iz jedne od najrazvijenijih svetskih zemalja, tj. zemlje koja prednjači u domenu digitalnih i komunikacionih poslovnih platformi i rešenja, primer nebezbednosti jedne od njenih najrespektabilnijih institucija mora otvoriti pitanje o tome koliko je digitalna transformacija poslovanja zaista donela, a koliko odnela kroz svoje bezbednosne implikacije, kao i da li smo bezbedni ako znamo i imamo u vidu da se digitalna transformacija poslovanja i njeni granulati koriste kao vektor, ne samo u domenu uobičajenog cyber kriminala, nego i međudržavnog cyber ratovanja u kome je očigledno moguća meta svaka organizacija, a ne samo kompanije, finansijske institucije, i sl.

Poglavlje VIII: Rezultati istraživanja

Razvoj savremenih IKT tehnologija, globalizacija i prateće internacionalizovanje poslovanja, neminovno su doveli do zaoštavanja konkurentskih odnosa na tržištu, koji za sobom povlače i neminovnost turbulentnog okruženja i organizacije koja mora pružiti adekvatan odgovor na to, a taj odgovor je ponudila digitalizacija poslovanja.

U ovim okvirima, digitalizacija poslovanja neminovno je zahtevala razvijanje poslovnih procesa u vidu strateškog planiranja, detaljnu analizu sveukupnog organizacionog okruženja, kako na nivou internog, tako i eksternog, definisanje organizacionih vrednosti i upravljanja prema ciljevima i na sve to formiranje vizije poslovne strategije koja će omogućiti ostvarivanje ovih ciljeva uz najmanju prisutnost bezbednosnih implikacija koje donosi digitalna transformacija poslovanja. Da bi se došlo do konkurentskih prednosti na tržištu, često se poslovanje izlaže pionirskim poduhvatima u oblasti informatike koje se u pojedinim slučajevima ispostavi rizičnim i takvim da sa druge strane kompanijama donosi tržišnu ranjivost, uporedo sa prednostima.

1. Prikaz rezultata istraživanja

U periodu kojim se bavi ovaj rad, u praksi je bilo više primera u kojima su pogrešne procene menadžmenta dovele do eskalacije ozbiljnih posledica. Te posledice su dalje poslovanje kompanije izložile informatičkim rizicima. Evo i nekih primera:

Rizik promašenih ulaganja u informatiku – prema istraživanju koje je sproveo časopis CFO (CFO Research Services, 2005) u 2005. godini, samo 40% finansijskih direktora je smatralo da informatička ulaganja daju očekivane rezultate;

Rizik neuspešnog sprovođenja informacionih projekata – samo 30% informacionih projekata može se smatrati uspešnim. Prema Gartnerovom istraživanju (Gartner, 2002) koje je sprovedeno na uzorku najboljih američkih kompanija, utvrđeno je da je 20% informatičkih troškova potpuno nepotrebno učinjeno usled čega je došlo do nepotrebnog rasipanja sredstava;

Rizik prekida ili otežanog funkcionisanja informacionog sistema, kao uzrok prekida odvijanja poslovnih procesa – prema istraživanjima DRI (Disaster Recovery Instituta), utvrđen je kuriozitet da čak 93% kompanija koje iznenadno dožive prekid poslovanja, a ne poseduju plan za reuspostavljanje njegovog kontinuiteta, najčešće prestanu poslovati na tržištu u roku od 5 godina od tog događaja. Čak polovina kompanija koje obustave kritične funkcije u poslovanju na više

od 10 dana nikada se ne regenerišu. Za kompanije iz liste Fortuna 500 vreme zastoja poslovanja po minuti kompanije u proseku košta 96.000 USD (Kenneth, Fulmer, 2005:7).

Rizik bezbednosti informacionog sistema – prema istraživanjima koja su sprovedi ISACA (2012.) i Ernst&Joung (2011.), troškovi informatičkog kriminala procenjeni su na milijardu američkih dolara godišnje, dok je prosečan trošak prekida rada informacionog sistema bio oko 5.000 dolara po minuti, dok je ukupan trošak povezan sa zloupotrebama podataka porastao na 7,2 miliona dolara, odnosno 204 dolara po incidentu u odnosu na 138 dolara koliko je to bilo u 2005. godini.

Činjenica je da u skoro svim industrijama primena digitalne i informacione tehnologije može imati veoma pozitivan učinak na poslovanje. Radi toga je nastao trend da svi poslovni subjekti, bez razlike i izgovora ulažu u informatiku. Ipak svaka, pa i ova medalja, ima svoje naličje, pa tako konstantni pritisak za stalnom primenom novih digitalnih i informacionih tehnologija u poslovanju donosi i sve brojnije rizike kojima veliki broj menadžera nije dorastao, jer oni veoma često ne razumeju prirodu tih rizika i samim tim njima loše upravljaju.

Brojni su primeri i pogrešnog i lošeg vođenja informatičke funkcije preduzeća, kao što su brojni i primeri da je usled toga došlo do velikog broja direktnih i indirektnih poslovnih gubitaka i šteta u poslovanju.

U nastavku će biti dato nekoliko primera koji su prikazali glavna obeležja informacionih rizika, najpre u razdoblju koje je bilo do intenzivne digitalizacije poslovanja (2010. godine), a onda i do danas, kako u svetu, tako i kod nas, obzirom na rastuću složenost informacionih sistema i njihovu neizbežnu poslovnu primenu, usled čega se bez ustručavanja može zaključiti da će u budućnosti razmere takvih problema i njihovih posledica biti daleko izraženije, kako uostalom i govore ovi primeri.

Tabela br. 9 Primeri informatičkih incidenata

NEKI OD POZNATIH BEZBEDNOSNIH INCIDENATA		
Godina	Organizacija	Opis incidenta
2007	TJX Companies	Zbog nezaštićene bežične mreže ukradeni su podaci 94 miliona kreditnih i debitnih kartica
2007	HM Revenue &	Izgubljena 2 diska sa ličnim podacima 25 miliona porodica u

	Customs	Velikoj Britaniji
2007	HSBC Bank	Kazna od 3,2 miliona funti radi gubitka podataka životnog osiguranja za 180.000 klijenata. Uzrok ovog incidenta je izgubljeni disk u pošti, a na kome podaci nisu bili kriptovani.
2008	Bank of New York Mellon	Ukradene trake sa podacima iz serverske sobe. Nosači podataka su sadržali lične podatke 12,5 miliona klijenata.
2009	Heartland Payment System	Izugbljeno oko 130 miliona podataka usled zaraze informacionog sistema malicioznim kodom
2011	Sony Playstation Network	Ukradeno oko 24 miliona ličnih podataka, podataka o transakcijama i sl. korisnika mreže Sony Playstation. Gubitak po osnovu ovog slučaja se procenjuje na 171 milion dolara.
2014	Agencija za privatizaciju Republike Srbije	Tekstualna baza sa ličnim podacima preko 5.190.396 građana i više od 4000 finansijskih dokumenata iz evidencije nosilaca prava na besplatne akcije Republike Srbije bila je dostupna na internetu usled velikih sigurnosnih propusta u informacionom sistemu. Radi se o podacima – koji sadrže ime, prezime, srednje ime, JMBG i status u evidenciji prava građana na besplatne akcije. Prema nalazima Share fondacije, propust se desio na nivou administratora platforme, a ne administratora servera ili hosting providera. Za ovaj slučaj niko nije ni disciplinski, ni prekršajno, ni krivično odgovarao uprkos prijavama Poverenika za zaštitu ličnih podataka.
2019	Facebook	Podaci o više od 540 miliona korisnika Facebook-a mesecima su bili javno vidljivi putem Amazonovih servera
2019	Instagram	Izloženi su podaci o 49 miliona korisnika Instagrama. Radi se o podacima sa profila korisnika ove mreže u vidu privatnih telefonskih brojeva, e-mail adresa i sl.

2020	Novi Sad	Kriptomalver "Pwndlocker" ransomware napad izvršen je na sve javne službe grada Novog Sada. Povodom ovog incidenta gradonačelnik Novog Sada za medije je izneo "Bez svega smo ostali. Nije mogla da se radi objedinjena naplata, nisu mogle da se izdaju građevinske dozvole, prestao je da radi sistem video nadzora i sve je stalo. Ugasili su sve ono što smo radili kroz digitalizaciju i kroz informacione tehnologije". Ovom prilikom je prema grubim procenama pričinjena ogromna materijalna šteta čiji se negativni efekti još uvek procenjuju. Rezultate toga da li su i u kojoj meri kompromitovani lični i zaštićeni podaci građana doneće rezultati analiza koje su u toku, a koje će biti poznate nakon potpunog reuspostavljanja napadnutog složenog informacionog sistema.
------	----------	--

Priroda informatičkih rizika se u novije vreme prilično menja, iz kog razloga se posledice grešaka današnjih informacionih sistema sve više naslanjaju na rizike iz sajber domena i kao takvi imaju sledeća globalna obeležja (ISACA, 2015):

- Ukupne štete od krađe u američkim bankama su oko 100 miliona USD godišnje, dok se oko 600 miliona USD potroši na sprečavanje tih događaja. U Italiji su na primer u 2006. godini troškovi štete od krađe u bankama iznosili su oko 65 miliona USD, dok je 649 miliona USD utrošeno na sprečavanje krađa;
- Trošak po osnovu cyber kriminala iznosi oko 1000 milijardi USD, što čini od 0,2 do 0,4% svetskog GDP-a, odnosno 7% GDP-a SAD-a;
- Trošak zaštitnih mera od cyber kriminala iznosi 67 milijardi USD, dok štete iznose oko 200 milijardi USD. Čak 97% cyber napada bi se moglo izbeći da su kompanije uspostavile efikasne sisteme zaštite;
- 95% kompromitovanih resursa sadržavalo je poverljive podatke;
- Kada je u pitanju šteta od krađe podataka, procenjeno je da jedna krađa podataka košta oko 5,5 miliona dolara. Razlozi krađe - 58% čine „haktivisti“, dok 39% prouzrokuje nemar zaposlenih, a preostala 3% odnosi se na ostale uzroke;
- Svakodnevno se isporuči oko 100 milijardi spam poruka;

- Većina ljudi bi svoju lozinku otkrila u zamenu za čokoladu;
- Informatičke greške u kritičkoj nacionalnoj infrastrukturi mogu prouzrokovati velike katastrofe. Primer za to je računarski virus „Stuxnet“ kojim su napadnuta nuklearna postrojenja u Iranu;
- Sve su češće hakerske pljačke bankomata, dok je DARPA uspešno hakovala automobil i nad njim preuzela kontrolu;
- SAD su cyber prostor proglasile 5. vojnom zonom pored kopna, mora, vazduha i svemira.
- Cyber kriminal se na nivou pojedinca manifestuje na sve češće krađe podataka, ugrožavanja privatnosti i gubitka digitalnog identiteta, dok je kibernetičko (cyber) ratovanje postalo svakodnevice.

Bezbednosni incidenti imaju sve veći uticaj na poslovanje. Iako se mnogi od ovih incidenata ne prijavljuju ili bivaju zataškani, istraživanje iz 2004. godine je pokazalo da su kompanije koje su iskusile bezbednosne informatičke incidente u proseku izgubile 2,1% svoje vrednosti, uz prosečan gubitak od preko 1,6 milijardi po incidentu (Cavusoglu, Mishra, Raghunathan, 2004:69-104).

Preko 60% finansijskih institucija doživelo je napad u oblasti cyber bezbednosti (Piccoli, Pigni, 2016:345).

Propusti i greške u informacionoj bezbednosti, a time i privatnosti, mogu imati krajnje negativne posledice na organizacije, obzirom da su uzrok direktne finansijske i ostale štete kroz prekid rada, nemogućnost sprovođenja poslovnih procesa, krađa podataka i sl., ali isto tako i indirektno negativne efekte na pravne obaveze u oblasti regulatornih propusta i kazni, a onda i kroz gubitak ugleda i kroz često nepovratno narušavanje imidža i poverenja kod korisnika.

Iz ovih razloga digitalno ekonomsko okruženje zahteva stalnu i intenzivnu primenu digitalnih tehnologija u sprovođenju poslovnih transakcija. Takvo okruženje doprinosi brojnim koristima u poslovanju, ali ako se digitalnim tehnologijama ne upravlja adekvatno, ova medalja može imati i drugu stranu, najčešće u vidu bezbednosnih incidenata koji direktno ugrožavaju poslovanje i stvaraju brojne štete.

U julu 2015. godine, hakeri Kris Valasek i Čarli Miler su daljinskim putem hakovali putnički automobil „Jeep Cherokee“ dok se kretao autoputem. Ranjivosti i bezbednosni propusti u

informacionom i „Entertainment sistemu“ koji je sastavni deo svakog današnjeg automobila, ovim hakerima su omogućili da sa razdaljine od preko petnaest kilometara preuzmu upravljanje nad ovim vozilom i svim njegovim ključnim funkcijama. To je bio prvi poznati primer da su hakeri, doslovno iz svojih fotelja, preuzeli kontrolu nad putničkim vozilom i prouzrokovali kompaniji koja je proizvela to vozilo ogromne štete i probleme, koje su pored ostalog podrazumevale i servisni opoziv 1.400.000 vozila, otklanjanje ovih bezbednosnih propusta, nadoknadu štete, izmenu regulatornih i industrijskih pravila, itd.

Broj i opseg bezbednosnih incidenata, uprkos svim naporima da se oni sprečavaju, ipak stalno raste. Istraživanja pokazuju da je 2009. godine otkriveno oko 3,4 miliona bezbednosnih incidenata. U 2014. godini ovaj broj je porastao na 43 miliona. Koliki je stvarni broj neotkrivenih bezbednosnih incidenata ostaje nepoznato.

Imajući u vidu stalni i krajnje progresivni napredak digitalne ekonomije, sasvim je sigurno da u budućnosti možemo očekivati još veće razmere bezbednosnih incidenata, usled čega već sada možemo izneti tvrdnju da ovi incidenti nisu samo informatički problem koji spada u tehničke, poslovne i pozadinske rizike, već da se zapravo radi o strateškim poslovnim rizicima koji bukvalno „preko noći“ mogu promeniti sve, uključujući i konkurentsku poziciju kompanija i gradova, što potvrđuje i nedavni ransomver napad izvršen na informatičku infrastrukturu grada Novog Sada koji je ovu infrastrukturu i sve njene funkcije potpuno paralisao.

Prema Allianz barometru rizika za 2019. godinu, pored zastoja u poslovanju, vodeći rizik za kompanije su sajber incidenti. Statistički gledano, čak 37% ispitanika smatra da su sajber incidenti glavni globalni poslovni rizici, jednako kao i zastoji u poslovanju. Gubici po osnovu sajber kriminala, prema ovom istraživanju, drastično i konstantno rastu i već iznose oko 600 milijardi dolara godišnje, što čini značajan rast u odnosu na 445 milijardi dolara koliko je to bilo tokom 2014. godine. (Allianz Risk Barometer 2019, str.9.)

Tabela br. 10: Pet najvećih rizika za mala preduzeća sa trendovima kretanja (<250 mil EUR godišnjeg prihoda)

Br.		%	2018	Trend
1.	Cyber incidenti (npr.cyber kriminal, IT promašaji/zastarelost, povrede podataka, kazne i prekršaji)	32%	2 (30%)	↑
2.	Promene u zakonodavstvu i regulativi (npr. Trgovinski i tarifni rat, ekonomske sankcije, protekcionizam, Begzit, dezintegracija Euro zone)	30 %	5 (22%)	↑

3.	Prirodne katastrofe (npr. Oluje, poplave, zemljotresi)	27 %	3 (28%)	=
4.	Razvoj tržišta (npr. Volatilnost, intenzivna konkurencija/nov ulaz na tržišta, merdžeri i akvizicije, fluktuacija tržišta)	27 %	4 (27%)	=
5.	Poslovna interupcija (uključujući i disrupciju lanca snabdevanja)	26 %	1 (33%)	↓

Izvor: Allianz Risk Barometer 2019, str. 22

Vezano za prethodnu analizu, treba istaći veliku zabrinutost malih i srednjih preduzeća vezano za sajber napade i zloupotrebu podataka, imajući u vidu da ova vrsta preduzeća nema jaku i sposobnu organizaciju da na takav izazov odgovori adekvatno, za razliku od toga kako to mogu i rade velike kompanije. Ovakvu situaciju potvrđuje i Volker Muench, Global Practice Leader, Utilities & Services, IT Communication, AGCS i ističe da su mnoga mala i srednja preduzeća u proteklom periodu imala probleme sa zaštitom podataka, ali ih nisu uvek prijavljivali nadležnima zbog straha od gubitka stečenog tržišnog poverenja i reputacije, a time i mogućeg gubitka ugovora sa klijentima. Iz dostupnih podataka u sprovedenom istraživanju može se utvrditi jasna veza između sajber poslovanja i gubitka tržišne reputacije, posebno u ovom segmentu privrede.

Kompanije sa visokim stepenom digitalizovanog poslovanja moraju, s obzirom na rastuće rizike, planirati veliki broj scenarija, a to znači i utvrđivanja uzročnika koji remete poslovanje, jer su u današnjem umreženom društvu upravo u tom pogledu najranjivije, što jasno potvrđuje i globalna situacija izazvana pandemijom SARS-CoV-2 virusom koja je desetkovala tržišta i velikih i malih država i kompanija i maltene sve grane industrije, a gde se konačni ishod iz ove perspektive ne može još uvek statistički i naučno ni sagledati, niti je to u ovom trenutku zahvalno prognozirati.

Rizici koji remete poslovanje, odnosno disruptivni rizici, mogu biti fizički, kao što su prirodne katastrofe, ratovi i sl., ali i virtuelni sa fizičkim posledicama u vidu prekida funkcionisanja informatičkih sistema, koji opet mogu biti zlonamerni ili slučajni.

Tabela br. 11 Uzroci prekida poslovanja koji najčešće izazivaju strah kod kompanija

Cyber incidenti	Požari, eksplozije	Prirodne katastrofe	Prekid kod dobavljača i poslovnih procesa	Kvar mašina
50%	40%	38%	28%	28%

Izvor: Allianz Risk Barometer 2019, str. 10

Prekidi poslovanja i gubici izazvani na taj način postaju sve veći i sve kompleksniji, imajući u vidu da se lanci snabdevanja sve više oslanjaju na veći broj manjih snabdevača, posebno kada je u pitanju industrijski sektor (automobilski, elektronski i farmaceutski). Čak bi i događaj kakav je

požar u nekoj od ovih industrija mogao dovesti do ozbiljnih gubitaka usled nedostatka ugradnih delova, kaže Volker Muench, Global Practice Leader, Utilities & Services, IT Communication, AGCS.

U proteklom periodu smo mogli videti ozbiljne gubitke u sektoru osiguranja od ovakvih događaja koji prevazilaze 1 bilion € (\$1.1mlrd). Sa samo jednim požarom cela fabrika može nestati, a sa tim staje i celokupna proizvodnja, usled čega se gubici u lancu snabdevanja uzročno generišu. Čak i kvar na mašinama u proizvodnji može imati sličan efekat, a da ne govorimo o biohazardima globalnog tipa, kakav imamo od kraja 2019. godine i koji ima tendenciju da po različitim procenama traje i dalje od sredine 2020. godine.

2. Diskusija rezultata istraživanja

Prilikom razmatranja ranjivosti digitalnog poslovanja mora se imati u vidu okolnost da rizici u poslovanju mogu proizilaziti iz vlastitog poslovanja, ali i iz poslovanja dobavljača, kupaca ili isporučilaca informatičkih usluga i resursa, ali i globalnih biohazarda. Iz tih razloga, menadžment kompanije ima obavezu da kontinuirano prati i analizira situaciju u sajber i opštem okruženju i shodno svojim potrebama i mogućnostima (pr)ocenjuje nivo kompanijske ugroženosti, a zatim i nivo potrebnih finansijskih i drugih ulaganja radi razvoja i unapređenja preventivnih programa i profilisanja zaštitno-operativnih odgovora. Savremeni pristupi i rešenja u domenu upravljanja rizikom, analitički alati, odgovarajuće metodologije, procedure i inovativna partnerstva, mogu značajno doprineti boljem razumevanju, ublažavanju i amortizovanju posledica savremenih sajber incidenata i kriza, te redukovanju tako nastalih gubitaka.

Praksa je u više navrata potvrdila da su sajber rizici i rizici zastoja u poslovanju međusobno povezani i uslovljeni i da između njih postoji visok nivo korelacije, budući da napadi ucenjivačkim softverom (Ransomware) ili slučajni prekidi informacionih sistema, često dovode do poremećaja poslovanja ili pružanja usluga, čime nastaju veliki finansijski troškovi čija amplituda u širokom rasponu varira između kompanija i sektora u zavisnosti od njihovog stepena digitalizacije i spremnosti da adekvatno reaguju na izloženosti ranjivostima (Čelik, P. 2019:61-68).

U radu su, stoga, opsežno analizirani brojni parametri i faktori od uticaja na poslovanje i njegovu bezbednost. Analiza je obuhvatala lokalno i međunarodno pravno okruženje i interakciju, pravnu

i poslovnu prekograničnost i njihovu interakciju, tehnološko okruženje, određene demografske parametre i druge činioce koji egzistiraju pod dejstvom ovih faktora. Neki od njih su sagledani kroz prizmu poslovnih prilika, uz istovremeno stavljanje u korelaciju sa mogućim pretnjama po organizaciju, koje bi mogle nastati po ovim osnovima.

Polazišta poslovnog i tržišnog uspeha kompanija jasno ukazuju na potrebu da poslovne organizacije radi tržišnog opstanka i konkurentske prednosti, moraju koristiti sve prilike u domenu poslovnog okruženja, ali vodeći pritom računa da uporedo sa tim moraju činiti sve kako bi minimizirali sve tako nastale rizike i pretnje po svoju konkurentnost i opstanak, a kako bi pravilnim izborima i prihvatljivim rizicima obezbedili svoj razvoj i time tržišni rast u svojoj poslovnoj oblasti. Tako se ispostavilo da konkurentska prednost počiva na poslovnom kvalitetu zasnovanom na jasnoj poslovnoj distinkciji konkretne poslovne organizacije na tržištu, a koja, kao takva, prateći korisnička iskustva svojim načinom poslovanja utiče na spremnost korisnika da se opredele ili da nastave saradnju sa ovom kompanijom ili organizacijom ili da se inicijalno opredele za njene proizvode ili usluge u odnosu na konkurente.

Analiza digitalne transformacije poslovanja, da bi bila objektivna, mora biti sagledana kroz različite segmente poslovanja, počev od preduzeća i organizacija kao poslovnih entiteta, koji mogu biti mikro, mali, srednji i veliki, a onda i javnog i uslužnog sektora koji pokrivaju ostatak celine. Zajedničko za sve ove poslovne segmente jeste umrežavanje. Ono je fiksno, širokopojasno, Wi-Fi, mobilno, 2G, 3G, 4G, 5G.

Istraživanje ne bi moglo biti potpuno ukoliko se na osnovu njega ne bi mogle dati određene kvantitativne projekcije, koje bi u tom smislu obuhvatale broj i rast internet korisnika uređaja i njihovih veza, moderne mrežne performanse i nove poslovno-tržišne zahteve koji su zasnovani na aplikacijama. Kvalitativni segment ovih procena i analiza, pruža se u 4 strateška područja i to: aplikacije, bezbednost kao segment koji je sveprožimajući, infrastrukturna transformacija i pružanje podrške zaposlenima i timovima da na sve promene i inovacije adekvatno odgovore, uprkos stepenu njihove disrupcije.

Kada je u pitanju globalna projekcija pristupa internetu, može se predvideti da će do 2023. godine približno 2/3 svetskog stanovništva imati pristup internetu. Uporedno, do 2023. godine, svet kakav poznajemo imaće do 5,3 milijarde korisnika interneta, za razliku od 3,9 milijardi koliko je to bilo u 2018. godini, kada je to procentualno učešće obuhvatalo tek nešto preko

polovine svetskog stanovništva. Razvojni trendovi u ovoj oblasti su očekivani, imajući u vidu globalna kretanja, međutim, ono što prevazilazi ovakva očekivanja za isti vremenski period jeste rast broja uređaja spojenih na mreže, koji bi do 2023. godine mogao dostići brojeve koji će biti čak do 3 puta veći od broja svetske populacije. Suštinski, to bi značilo da će svet do 2023. godine imati približno 3,6 umreženih uređaja po glavi stanovnika, za razliku od 2018. godine kada je to bilo oko 2,4. U apsolutnim brojkama, do 2023. godine može se očekivati nešto preko 29 milijardi umreženih uređaja, što je više nego značajan pomak u odnosu na nešto preko 18 milijardi uređaja koliko je to bilo 2018. godine.

Ono što još jasnije prikazuje sliku ovog trenda razvoja jeste projekcija da će polovina od svih globalno povezanih uređaja i uspostavljenih veza zapravo biti u segmentu M2M, odnosno da će od 2018. do 2023. godine udeo ovih veza porasti sa 33 na 50%. Sistem veza M2M koji je drugim rečima IoT, jasno ukazuje da će najveći deo ovog razvojnog trenda biti zapravo u domenu internet povezanih uređaja u domaćinstvu, a da ovaj trend neće izostaviti ni automobilsku industriju u kojoj takođe raste ova vrsta primene.

Kada su u pitanju 5G tehnologija i uređaji, može se pretpostaviti da će do 2023. godine, u svim segmentima mobilnih uređaja, negde oko 10% biti vezano za 5G, što znači da će aktuelne tehnologije i uređaji ostati dominantni, a kao što je očekivano, najveći deo tog segmenta će biti pokriven pametnim telefonima. Ovakve projekcije nisu ostvarive ukoliko ovaj tehnološki razvoj ne bude podržan rastom brzine fiksne širokopojasne mreže, za koju se takođe u ovom periodu očekuje udvostručavanje i dostizanje brzina do 110 Mbps. Samim tim doći će do velikog ubrzanja mobilnih mrežnih veza, a onda i rast koji će doneti primena 5G tehnologije, putem koje ove brzine mogu dostići i do 575 Mbps.

Trendovi rasta brzine prenosa kakvi su prethodno dati, jasno ukazuju i na trendove koji će dovesti do porasta preuzimanja mobilnih aplikacija, a taj rast će najviše biti izražen u domenu društvenih medija, igara i naravno poslovnih aplikacija. Samim tim, ovakvi trendovi rasta i razvoja u sferi digitalnog takođe donose i svoje statistike sa dosta visokim procentima i u pratećim negativnim pojavama. Naime, u periodu koji je za nama na globalnom nivou zabeležen je rast od 776 % kada su u pitanju sajber napadi od godine do godine, recimo između 2018. i 2019., pa je i samim tim za očekivati da će se ukupan broj DDoS napada bar udvostručiti i u periodu između 2018. i 2023. godine i kretaće se u rasponu od 7,9 do 15,4 miliona napada.

Ovakav razvojni trend svake godine najpre donosi, a onda i tržišno usvaja veliki broj novih uređaja i tehnologija čije se procesne i tehnološke karakteristike konstantno uvećavaju primenom veštačke inteligencije. Samim tim, primetan je drastičan tržišni rast M2M aplikacija i njihove primene koja se kreće od segmenta pametnih brojlara, video i zdravstvenog nadzora, transporta, praćenja pošiljki i sl., pa ovi segmenti usled njihove otvorenosti za ove tehnologije enormno utiču i doprinose rastu i broja uređaja i njihovih uspostavljenih veza. Samim tim, može se slobodno pristupiti projekciji da će ovo biti najbrže rastuća kategorija veza do 2023. godine.

Kada su u pitanju M2M aplikacije, one zbog svojih svojstava i tržišnog uticaja, doprinose da u mnogim industrijama dođe, kako do ubrzavanja rasta, tako i do primene interneta stvari. Ako se tome doda i primena interneta stvari u domaćinstvima, može se zaključiti da je IoT postao pretežni sistem putem koga se podaci, stvari, procesi i ljudi, povezuju međusobno i na internet.

Ovakav trend razvoja neposredno utiče i na povezane aplikacije u domaćinstvu, posebno u domenu kućne automatizacije (pametnog domaćinstva), onda obezbeđenja domaćinstva i pratećih sistema video nadzora, povezanosti bele tehnike na nivou domaćinstva sa inovativnim aplikacijama koje prate njihov rad i sl., što će činiti značajan udeo u ukupnom broju ostvarenih M2M konekcija.

Usled navedenog, očekuje se rast povezanih aplikacija u automobilskoj industriji, njihova primena u upravljanju voznim parkovima, enterntejnment sistemima u vozilu, povezivanja na internet, servisne dijagnostike vozila, navigacione tehnike, itd. Ovakvi trendovi pokazuju da će postepeno doći do težišnog pomeranja prometa klasičnih korisničkih uređaja, kao što su pametni telefoni, tv aparati i slično, ka M2M konekcijama usled povećane upotrebe inovativnih aplikacija.

Tehnološka kretanja i trendovi kakvi su prikazani, dovode do promena i u domenu korisničkih očekivanja, obzirom da se tehnologija već sada percipira svemogućom i sveobuhvatnom, usled čega korisnici očekuju od svojih provajdera da njihovo internet iskustvo, a samim tim i očekivanje njima učini mrežu i uvek i svuda dostupnom, ali istovremeno i sigurnom, kao i da njihova lična i poslovno-profesionalna imovina uvek i svuda bude bezbedna. Međutim, kretanja u proteklim godinama ukazuju da se radi o razdoblju koje je donelo ozbiljne bezbednosne pretnje i rizike, značajna kršenja bezbednosti podataka i u javnosti široku raspravu o tome. Analize ovakvih dešavanja pokazale su korelaciju sa nivoom finansijski utvrdive štete u poslovnom

smislu, kao i štete nastale po brendove kao posledice kršenja bezbednosti podataka, usled čega se izdiferenciralo da se konačno sajber bezbednost tretira kao poslovni rizik cele kompanije, a ne samo IT sektora, kako je to do nedavno bilo. Jedan od zaključaka u odnosu na nalaze rada sa sigurnošću može biti da je digitalno tehnološki napredak jedan od glavnih pokretača ekonomskog rasta sa jedne, i istovremeno razlog koji je doveo do veće pojave sajber napada i kriminala sa druge strane.

Razlog za ove nalaze jeste taj što su ključni trendovi, kao što su elektronska trgovina, mobilna plaćanja, Cloud tehnologija, analitika Big Data, IoT, veštačka inteligencija, mašinsko učenje i sve veći broj društvenih medija, značajno povećali stepen sajber opasnosti kako za korisnike ovih servisa, tako i za kompanije. Složenost interakcije pobrojanih segmenata donosi za rezultat da priroda pretnji nastalih na tom polju postaje sve raznolikija.

U novembru 2019. godine došlo je do 1272 povrede iz domena bezbednosti podataka sa bezmalo 163 miliona zapisa koji su otkriveni u ovom segmentu. Interesantno je da je najveći broj kršenja bio iz domena bankarstva i zdravstva i da su u tim segmentima nastala najveća kršenja u oblasti osetljivih evidencija, te da prosečni troškovi po izgubljenom ili ukradenom zapisu konstantno rastu sudeći prema izveštajima IBM-ovog Instituta za bezbednost i Ponemona za 2018. godinu. Razvoj Cloud tehnologije i sama digitalna transformacija bitno su doprineli povećanju ukupnih troškova nastalih po osnovu povrede u oblasti podataka.

Važno je u sklopu ovih trendova navesti i aplikacije nove generacije čiji se poslovni zadatak izdiferencirao u domenu stvaranja novih poslovnih modela. Veštačka inteligencija, mašinsko učenje i brojne povezane aplikacije, masovni su korisnici digitalne transformacije koja je u toku, pa bazirano na tome kreiraju nove poslovne modele i utiče na razne industrijske grane i sektore.

Jedan od izuzetnih primera aplikacije sledeće generacije jeste prediktivna analitika, čiji je zadatak da primenom naprednih analitičkih tehnika upotrebi već postojeće podatke, kvalitetno ih i brzo analizira i na osnovu njih vrši predviđanja predstojećih događaja. Samim tim, prediktivna analitika našla je svrhu u preoblikovanju načina poslovanja kompanija, usled čega je postala primenjiva i kod mnogih industrijskih IoT rešenja, imajući u vidu da može koristiti podatke dobijene iz senzora IoT uređaja i na osnovu njih predvideti vreme otkaza opreme, opštih

vremenskih obrazaca, potrebe za rotacijom useva u poljoprivredi i predviđanja prinosa određenih kultura i puno toga sličnog u raznim industrijama.

Jedan od rezultata ove tehnologije i prikaza njene revolucionarnosti može se sagledati kroz automobilsku industriju i stvaranje autonomnih vozila, dok sa druge strane primena nije izostala ni u industriji finansijskih usluga gde se ova vrsta analitike veoma dobro pokazala u domenu kreiranja novih načina za upravljanje portfoliom. Samim tim, možemo zaključiti da postoje promenljive tehnologije koje proizvode stalno evoluirajuće poslovne modele. Primer mobilnih aplikacija nema samo pasivnu ulogu, već njihov koncipirani uticaj može imati i ulogu da sugestivno potakne potrebe budućih potrošača ili malih i srednjih preduzeća, iniciranjem određenog pravca koji bi se postupno mogao pretvoriti u njihovu potrebu. Ovakav pristup može imati i određeni manipulativni kontekst putem koga mogu nastati i brojne zloupotrebe.

Na temelju ovih rešenja može se primetiti da gotovo u svim poslovnim sektorima postoji uvećana potražnja, kako za novim, tako i za poboljšanim aplikacijama čija je uloga povećanje produktivnosti radne snage i/ili poboljšanje konkretnih korisničkih iskustava. Ovi trendovi koji su očito interaktivni i vertikalno i horizontalno, IT sektore mnogih kompanija stavljaju pred izazove da moraju konstantno transformisati informacionu infrastrukturu kako bi je održavali prilagođenom novim i sve novijim tehnologijama. Internet stvari, veštačka inteligencija, mašinsko učenje i poslovna analitika uporno menjaju način na koji programeri moraju graditi pametne aplikacije, a sve kako bi time uprkos stalnoj evoluciji aplikacija i tehnologija, konstantno pojednostavljivali poslovne transakcije i pružali nove poslovne mogućnosti. Samim tim, danas je postalo moguće iskoristiti široki raspon usluga koje pružaju servisi Cloud tehnologije na osnovima kojih je moguće izgraditi inteligentne poslovne platforme, koje za korisnika neprimetno povezuju aplikacije, integrišu IoT rešenja i omogućavaju prilagodljivost velikih baza podataka za njihovu lakšu, bržu i sveobuhvatniju analizu. Ovaj kontekst time omogućava da se sve poslovne, trgovinske i korisničko-potrošačke aplikacije, uvek i iznova mogu prilagoditi putem odgovarajuće infrastrukture i pravih partnera, kao i dizajniranjem neke nove arhitekture i sopstvenog poslovnog rešenja.

Kretanja o kakvim je reč, pred IT menadžere i mrežne menadžere stavlja veoma težak zadatak, a to je održavanje i redukovanje troškova mrežnih operacija. Sve se češće događa da enormno brz rast broja i količine podataka, ali i broja i vrsta uređaja, značajno premašuje mogućnosti IT

timova u kompanijama. Usled čestog nerazumevanja ovih procesa, menadžment strukture kompanija nalažu mrežnim menadžerima manuelni pristup u rešavanju ovih problema, koji objektivno u datim okolnostima nije u stanju odgovoriti ovim izazovima, pa to najčešće rezultira sporošću reagovanja i nastanku operativnih troškova koji postaju čak 2 do 3 puta veći od troškova same mreže. Ovakva poslovna zamka ili nepažnja, rešiva je samo pojačanom IT automatizacijom kojom se upravlja i centralno i daljinski, što se ispostavilo ključnim poslovnim rešenjem koje omogućava držanje koraka u postojećem digitalnom okruženju i njegovim bezbednosnim implikacijama. U tom domenu već sada imamo određene dokazane inovacije na polju softverski definisanog umrežavanja, inteligentna poboljšanja mrežnih krajeva i objedinjena pravila i kontrole domena koji pomažu organizaciji u dostizanju veće efikasnosti, postojanosti i kvaliteta usluga. Samim tim softverski upravljane mreže pružaju opciju prilagođavanja svim ciljanim mogućnostima i kreiranje fleksibilne i programabilne infrastrukture za inoviranje poslovnih potreba kompanije, čineći tako njenu mrežu značajno prilagodljivijom dinamičkim zahtevima poslovanja i informacionog prometa i okruženja.

3. Preporuke za dalja istraživanja

Istraživanje kojim se bavila ova disertacija, obuhvatilo je širok dijapazon oblasti i promena u njima, kojima se stručni krugovi već duži niz godina bave, a koje, usled stalnih, inovativnih i ukrštajućih promena iz domena tehnologije i njene poslovne primene, moderna nauka sa teškoćama prati. Razlog za ovakvo tumačenje je diskrepanca između principa na kojima je baziran rapidni digitalni uspon, u kome tržište najčešće „preko noći“ diktira nove trendove i tehnološki razvoj i na taj način jednostavno ne ostavlja vremena nauci da se ona konsoliduje u okvirima granica svog interesovanja i da blagovremeno pruži pun naučni izraz i kumulativno tumačenje takvih pojava. Iz ovog razloga se uzročno-posledično može konstatovati da tu leži bitan segment preporuke ovog rada za dalja istraživanja i naučna usklađivanja.

U narednom delu rada, bazirano na ovim principima, data su opsežna sumirana velikog broja zapažanja, analiza iznetih stavova, najvažnijih istraživačkih nalaza, uključujući i analizu širokog spektra dostupnih istraživanja, uključujući i pretežne stavove, referentne pojave i trendove i zapravo jedan širi kontekst sagledavanja hipotetički postavljene tematike.

U radu su primenom svih predviđenih istraživačkih metoda u potpunosti dokazane, kako glavna, tako i sve pomoćne postavljene hipoteze i ujedno date višestruke preporuke za dalja istraživanja

sa odgovarajućim smernicama, imajući u vidu teorijsku zasnovanost problema istraživanja, kao i istraživačku elaboraciju svih relevantnih pitanja vezanih za digitalnu transformaciju, digitalnu ekonomiju, ranjivost digitalnih entiteta, ranjivost digitalnog poslovanja, a posebno aktuelne i potencijalne bezbednosne pretnje i rizike koji donose disruptivne tehnologije i inovacije.

U navedenim okvirima sajber ili kibernetička sigurnost morala bi biti glavni prioritet svima koji koriste internet, bilo za poslovne ili lične potrebe. Šaroliki digitalni krajolik sve je zahtevniji kao izazov u oblasti zaštite imovine, kako pojedinaca, tako i kompanija, ali i javne uprave. Upravo iz tih razloga, za sigurnost uređaja, zaposlenih i konekcija, infrastrukture i podataka, moraju biti zadužena pronicljiva i skalabilna rešenja po potrebi, a u slučaju ozbiljnijih izazova potrebno je imati i odgovarajuće poslovne partnere čija će saradnja, profesionalnost i iskustva biti od značaja u ranom prepoznavanju i što bržem otklanjanju posledica nastalih štetnim događajima.

Prema referentnoj studiji menadžera za informacionu bezbednost kompanije Cisco za 2019. godinu, dva od prvih tri bezbednosna pitanja odnose se na bezbednost elektronske pošte. Ono što ova studija primećuje jeste da bez obzira na to da li se ulaže u zaštitu putem prelaska na Microsoft Office 365 i nivo bezbednosti koji kompanija Microsoft u tom domenu pruža ili se pribegava alternativnim rešenjima koja nude opsežniju proveru identiteta poruka, činjenica je da elektronska pošta i dalje ostaje vektor sajber pretnje broj 1. Ovaj izveštaj takođe primećuje da su dva od prvih 10 napada i dalje insajderske pretnje i da bezbednost prvo mora biti sagledana u smislu pretnji iznutra, a onda u istoj meri i od pretnji spolja, što će reći, da se u ovom domenu već duže vreme ništa značajno ne menja.

Današnja bezbednosna pitanja jasno naglašavaju potrebu za boljom multifaktorskom proverom autentičnosti, usled čega bezbednosna politika kompanije mora uspostaviti pravi odnos između zaštite podataka i jednostavnosti upotrebe. Samim tim, efikasan pristup sajber bezbednosti treba da omogući pristup svim pravim licima, ali i da istovremeno ne ometa ovlašćene korisnike po osnovu nespretnih radnji na autentifikaciji određenih korisnika. U širem kontekstu, ne može se zaobići ni spremnost kompanija da odgovore zahtevima propisa o zaštiti ličnih podataka. Tu se nameće pitanje koliko su kompanije u ovom trenutku usklađene sa Opštom uredbom o zaštiti ličnih podataka EU (GDPR). Prema Cisco-voj studiji za 2019. godinu, tek 59% globalnih preduzeća potvrdilo je da u ovom trenutku ispunjavaju sve ili većinu zahteva GDPR. Sledećih

29% kompanija iznelo je da će za primenu GDPR biti spremni u roku od godinu dana, a za 9% kompanija za usklađivanje biće potrebno više od godinu dana.

Ono što je interesantno za primetiti, iako je GDPR inicijalno koncipiran da se primenjuje na kompanije u Evropskoj Uniji, odnosno na obradu ličnih podataka prikupljenim o pojedincima koji su građani EU, ipak je samo 3% ispitanika u globalnom istraživanju iznelo da ne veruje da se GDPR odnosi, tj. primenjuje na njihovu organizaciju. Samim tim, iz ovog podatka može se zaključiti da globalizacija nije samo poslovni kontekst, već i pravni, i da je ona učinila da i sami propisi mogu imati, ne samo prekograničnu, već i globalnu primenu na poslovanje. Može se iz konteksta navedenog takođe razumeti da je GDPR učinio da mnoge kompanije usmere deo svojih ulaganja u obuku zaposlenih i njihovo usavršavanje u domenu zaštite podataka, te stalno praćenje razvoja propisa iz ove dinamične oblasti. Kažnjivost prestupa u oblasti ličnih podataka, pored pravne, ima i svoju finansijsku i tržišnu konotaciju putem narušavanja imidža kompanija, iz kog razloga je privatnost podataka postala jedno od stalnih pitanja na nivou organa upravljanja mnogih organizacija, a takav razvoj i osvešćivanje kompanija potakli su upravo kupci koji su postali svesni svojih prava, jer oni prvo obezbede da najpre njihovi dobavljači i poslovni partneri adekvatno odgovore na pitanja iz oblasti privatnosti i bezbednosti, pa tek od adekvatnosti tog odgovora i prikazane ozbiljnosti zavisi da li će uopšte raditi nešto zajedno.

Svi zaposleni u organizaciji, a posebno oni čiji je posao bezbednost, moraju imati veliko znanje o tome kako reagovati na incident. Međutim, Cisco-vo istraživanje ne potvrđuje ovu hipotezu. Prema nalazima ove kompanije, na osnovu sprovedene ankete, ispostavilo se da 75% ispitanika zapravo zna šta i kako mora činiti nakon nastupanja bezbednosnog incidenta. Ovim putem došlo se do zaključka da se ovde radi o jednoj ozbiljnoj ranjivosti na koju odgovor mora dati brza, efikasna i kvalitetna obuka svih zaposlenih. Obuka o kojoj je reč služi za postizanje poslovne „okretnosti“, koja mora biti jedan od glavnih prioriteta kompanija i organizacija svih veličina, a ona se može osnažiti upućivanjem globalne radne snage na rad i funkcionisanje sa pravim alatima. Samim tim, automatizacija, mobilnost i saradnja, ključne su preporuke za upravljanje, kako složenom informatikom, tako i svim novim očekivanjima i zahtevima kupaca i korisnika. Posledično, produktivnost radne snage više ne predstavlja primarni problem modernih kompanija.

Izrada plana reakcije na incident, ukoliko se ne posmatra suštinski, može se percipirati, kako zastrašujućim, tako i nerešivim zadatkom. Međutim, postoje načini i pristupi u kojima se celokupni proces treba razbiti na segmente kojima se u datim okolnostima može adekvatno i bezbedno rukovati.

Sofisticirani napadi, poput naprednih uporednih pretnji, najčešće su usmereni na one kompanije u kojima se nalaze velike vrednosti, kao na primer banke, kompanije koje rade sa kreditnim karticama, velike trgovačke organizacije, zdravstvene ustanove i sistemi, hotelski lanci i slično, upravo iz razloga što su u njima pohranjene ogromne količine podataka o kreditnim karticama i drugim osetljivim ličnim i profitabilnim podacima. Ono što je karakteristično i zajedničko za sve njih, jeste da nijedna kompanija, bez obzira na to koja je njena veličina ili u kom industrijskom segmentu posluje, čak i kada ima izuzetnu zaštitu od spoljašnjih napada, nije zaštićena od napada insajdera ili nasumičnih zlonamernih softvera, krađe identiteta, ransomvera ili napada koji su uzrok uskraćivanja usluga.

Način na koji kompanija reaguje u ovakvim situacijama, u najvećem broju slučajeva znači razliku između sprečavanja određenog incidenta i brzog vraćanja kompanije u poslovne tokove na uobičajeni način, ili naspram toga pretrpeti enormnu štetu koja na ugledu kompanije, koja pritom može trajati godinama.

Prema podacima Ponemon instituta koji proističu iz izveštaja o kršenju bezbednosti podataka za 2019. godinu, prosečna cena incidenta na globalnom nivou iznosi oko 3,9 miliona dolara, dok za američka preduzeća prosečna cena incidenta iznosi približno 8,2 miliona dolara. Procenjeno je da uspostavljanje tima za reagovanje na incidente smanjuje troškove ovakvih događaja za čak 360.000 dolara, što jasno opredeljuje potrebu za uspostavljanjem ovog mehanizma i proaktivne zaštitne funkcije.

Jedan od najkarakterističnijih rezultata iz ovog Ponemonovog izveštaja najslikovitije prikazuje dubinu i kompoziciju ove problematike, a to je da je prosečno vreme koje je potrebno za identifikaciju kršenja iz domena bezbednosti podataka čak 197 dana, dok je prosečno vreme koje je neophodno za zaustavljanje ovakvog incidenta, nakon što je utvrđeno da je do njega došlo, oko 69 dana. Ovakav nalaz donosi zastrašujuću vest, a to je da se u velikom broju slučajeva napadači u ovim sistemima neotkriveni nalaze više od 6 meseci, pa ovo predstavlja jasan pravac za dalja istraživanja.

Kvantitativni prikazi metodologija i prognoza koji se nalaze i pretežno prikazuju u radu, dolaze iz različitih analitičkih izvora, počev od prognoza stanovništva Ujedinjenih nacija, a onda i pouzdanih analitičara kao što su IDC, Gartner, ABI Research, Ponemon, Cisco i dr.

Doprinos ovog rada temelji se na pregledu i analizi savremene domaće i referentne strane literature, istraživačkih nalaza, studija i analitike globalnih trendova i događaja, kao i odgovora na njih, uz opsežno razmatranje autora o preporukama za buduća istraživanja.

ZAKLJUČNA RAZMATRANJA

Postavljena istraživačka ideja i konceptualni okvir ovog istraživanja, kroz iznete nalaze, dobili su svoje ključne odrednice i sve potrebne fundamentalne elemente. Sprovedeni istraživački proces, kroz tematsku razradu, adekvatno je definisao, kako najvažnije segmente metodološkog okvira, tako i bitne istraživačke nalaze, putem kojih je izvršena analiza širokog spektra raznih istraživanja, važećih i praktično uvreženih stavova, kao i kredibilnih dostupnih rezultata.

Ovakav princip primenjen u naučnom radu, izdiferencirao je skladnost odnosa između definisanog problema, predmetnog okvira, ciljeva i postavljenih hipoteza istraživanja.

Kompleksnost teme koja svakodnevno pronalazi nove puteve za tehnološko-bezbednosnu granulaciju, teško je uhvatljiva, iz kog razloga je ona zahtevala posebnu veštinu, širok pristupni spektar, sistematičnost u povezivanju standarda, pojava i trendova, kako bi došlo do punog kapaciteta sagledavanja postavljene tematike.

Digitalna poslovna transformacija, u svom naličju uobličava brojne bezbednosne implikacije. Što je veća izraženost informaciono-komunikacionog progresu, proporcionalno dolazi do značajnijeg stepena usložnjavanja i bezbednosnih tendencija i faktora. Ključni razlog za to je što digitalnu transformaciju ne čini samo primena novih tehnologija u poslovnim procesima, već je u pitanju jedna sveobuhvatna disruptivna transformacija svih postojećih modela privređivanja, uključujući i one koji se tiču načina komunikacije i interkonektovanja svakog modernog privrednog društva sa njegovim dobavljačima, kupcima i javnom administracijom (Čelik, P.2019:61-81).

Ovakav model razaranja tradicionalnog poslovnog koncepta, ne samo da zahteva, već i podrazumeva novi sistem uspostavljanja vrednosti, kreiranje novih poslovno-komunikacionih kanala i lanaca, a u skladu sa tim i sprovođenje promena u oblastima marketinga, menadžmenta,

zapošljavanja i radnih odnosa, ali i tržišnog pristupa i interpersonalnih odnosa, kako unutar svake kompanije, tako i u svim relacijama kompanije sa njenim okruženjem i događajima.

Ovakav ekonomsko/poslovno/tehnički model „pogurao“ je promene u svim pravcima. Kako su te promene usmerene suštinski ka korisniku, objektivno je da je na tim osnovama došlo do promene u korisničkim očekivanjima, pa su tako nastala nova dinamična i poslovna iskustva, kojima kompanije, pritisnute konkurencijom, ubrzano personalizuju svoje proizvode i usluge i sve poslovne inovacije vrše u skladu sa zahtevima i preferencijama svojih kupaca i poslovnog okruženja.

Primena disruptivnih tehnoloških modela na tek donekle kontrolisani način, od izuzetnog je uticaja na ekonomske i opšte društvene procese, odnose i socijalna dešavanja. Samim tim, brzina nastajanja promena u korisničkom ponašanju radi sticanja novih tržišnih znanja i iskustava, dovodi do ubrzane evolucije korisničkih očekivanja i načina interakcije sa kompanijama. Ovakva kontekstura i dozvoljava da se može reći da digitalizacija poslovanja, a time i digitalizacija kao širi pojam, ne deluje ni samo regionalno, ali ni samo lokalno, jer disruptivne inovacije, čak i kada su osmišljene lokalno, mogu „preko noći“ pogoditi globalnu ekonomiju tzv. disruptivnim fenomenom koji se naziva „uberizacija“ (Ibid).

Samim tim, skoro svakodnevno, „nad glavom“ ekonomije nadvija se mač stalne inovativne transformacije ekonomskih sektora. Promene se dešavaju na svim poljima, počev od poljoprivrede, pa sve do infrastrukture, a one disrupuju čak i tradicionalne industrije poput proizvodnje i transporta (Ibid).

Iznalaženje odgovora na pitanje u kom pravcu će se dalje odvijati tehnološki razvoj, koje tehnologije će izmeniti način proizvodnje, kakve će biti komunikacije i uopšte ponašanje ljudi u budućnosti i kakvi će trendovi u tehnološkom smislu dominirati u globalnom, regionalnom ili lokalnom okruženju, iziskuje multidisciplinarnu projekciju primenjenih rešenja utemeljenu na korisničkim iskustvima, te brojnim istraživačkim i naučnim naporima koji su usmereni na rešavanje konkretnih društvenih, privrednih, životnih i drugih pitanja i problematika koje u aktuelnom vremenskom okviru opterećuju gotovo sve države, nezavisno od njihovog kreativnog i tehnološkog statusa.

U ranijoj fazi, disruptivne tehnologije dolazile su u talasima. Međutim, za veoma kratko vreme svet digitalnih trendova pokazuje i svoju drugu stranu. Četvrta industrijska revolucija, tj.

industrija 4.0, ima skoro nesagledivu dubinu i širinu. U tom pravcu imamo svakodnevno aktuelizovanje pretnji i rizika iz oblasti digitalnog poslovanja koje zahtevaju često, krajnje zahtevno i prilično obimno usaglašavanje postavljenih strateških agendi, a sa time i promenu u dizajnu operativnih zaštitnih mehanizama, i to više ne samo u sferi digitalne ekonomije, već i u sferi države i njenog administrativnog aparata.

Razvijajući se na taj način, digitalna transformacija poslovanja je izvršila sveobuhvatan pritisak na svest svih njenih činilaca i aktera. Digitalna transformacija je promenila ideale, ponašanje i paradigme, redefinisala fokus i načine privređivanja, stvarajući još uvek nedovršeni i time nezaokruženi tržišno-poslovni model. Disruptivne tehnologije zasnovane na stalnim inovacijama, kada se posmatraju kao deo kompleksnog globalnog poslovno-tehnološkog okruženja, ispostavile su se svojevrsnom pretnjom digitalnom poslovanju kao modelu, jer stalno izviruće i neograničene mogućnosti tehnologije obrnuto proporcionalno daju i neograničene mogućnosti tehnološki zasnovanih zloupotreba ranjivih strana digitalno/tehnološkog/poslovnog modela, što samo po sebi čini izvor stalne pretnje izazivanjem disbalansa na relaciji razvoja tehničko-tehnoloških inovacija i njihove primene sa jedne strane i pratećih zaštitnih mehanizama i bezbednosnih izazova sa druge strane (Čelik, P.2019:61-81).

Rezimiranje ovakve globalizirane situacije kristalno jasno ispoljava zaključak da transformacija poslovanja u digitalno, u vreme u kome živimo, više nije stvar izbora. Ako neko želi da postoji i opstane, da se tržišno pozicionira na turbulentnom digitalizovanom konkurentskom tržištu, onda on mora da zna da je digitalna poslovna transformacija imperativ tog postojanja. Kompanije koje nisu ovo shvatile ili koje nisu prihvatile ovu realnost, doživeće umesto „uberizacije“, tzv. „kodakovanje“, tj. nestaće sa tržišta kao Kodak (Ibid).

Digitalno tržišno poslovanje koje više ne poznaje geografske i teritorijalne odrednice uobičajene za svet kakav poznajemo, satkalo je cyber prostor nesagledive širine i dubine u kome je svako od svakog udaljen samo jednim „klik“-om. Digitalizovani prostor u kome svi koji imaju internet vezu i pametni uređaj mogu postati digitalni ponuđači i proizvođači, daje jednu široko iznijansiranu lepezu poslovne disrupcije i prateće neizvesnosti koja je na svakom koraku moguća.

Činjenica je da su kompanije lideri shvatili ovaj izazov, kao što je činjenica i da su te kompanije u tom pravcu i inovirale načine komuniciranja sa svojim partnerima, uspostavila je nove modele

saradnje sa potrošačima i javnom upravom, redizajnirajući tako ključne poslovne procese, a što je sa sobom donelo potrebu i sasvim novih modela organizovanja (Čelik, P. 2019. str.78).

Pritisak transformativne moći digitalnog poslovnog modela zahteva potpuno nove načine upravljanja, kako horizontalno, tako i vertikalno, a sve kako bi se time osvojio neophodan prostor za unapređenje poslovne efikasnosti. Tako postignuta poslovna efikasnost podrazumeva istovremeno smanjenje, kako troškova poslovanja, tako i maksimizaciju i racionalizaciju upotrebe postojećih i resursa dostupnih u budućnosti(Ibid).

Ipak, prethodno nabrojane prednosti i perspektive digitalne transformacije, pored prednosti, donose i teško sagledive pretnje i rizike. Prikupljena i analizirana tržišna iskustva bez sumnje pokazuju da kompanije, čak i kada su spremne i digitalno obazrive, u velikom broju slučajeva nisu u stanju da isprate tempo razvoja svih modernih tehnologija, što ih izlaže i znanim i neznanim rizicima, dok sa druge strane ni same države nisu u ništa boljoj situaciji na ovom polju, jer ni one ne uspevaju da pravovremeno i adekvatno, kako institucionalno, tako ni regulatornim okvirom odgovore i obuhvate sve nastale promene i inovacije i urede okvir za sankcionisanje u slučajevima zloupotreba.

Da bi se to utvrdilo, u ovoj disertaciji je primenjen istraživački princip komplementarnosti različitih izvora i metoda prikupljanja, te obrade i analize podataka usled nedovoljne teorijske izgrađenosti predmetne tematike, čime je autor uslovljen na eksplorativnu prirodu radi zadovoljavanja istraživačkih zahteva. Takva konstelacija je zapravo glavni razlog radi koga je u radu primenjen deskriptivni sistem istraživanja.

Primenjeni sistem istraživanja je u celosti dokazao postavljeni hipotetički okvir i svojom celovitošću dao, kako materijalne, tako i sadržajne osnove uz preporuke za buduća istraživanja, čime je naučni doprinos ovog rada zagarantovan i jedinstven.

Napredak u daljem razvoju digitalnih tehnologija primenjenih u poslovanju, bilo za proizvodnju ili za pružanje usluga, suštinski je zasnovan, a može se reći i zavistan, kako od informacija, tako i umreženih informacionih sistema čija je osnovna uloga da nastale i prikupljene informacije obrade, izanaliziraju i kompaniji daju nova saznanja za prilagođavanje ili inoviranje postojeće poslovne strategije, upravo na osnovu ovakvog „informacionog blaga“. Na ovaj način postiže se ekspanzija razvoja i kvalitativnost upravljanja kroz izradu aplikacija za podršku ovim segmentima.

Sudeći po nalazima istraživanja, države, ekonomije, kompanije, sektori, službe, servisi i sl., na tržištu mogu opstati, steći ili zadržati kompetitivnost, samo ukoliko njihov poslovni model stoji na ovim osnovama. Da je to nesporna činjenica, najbolje ilustruju napori Evropske Unije i njenih država članica da uhvate izgubljeni korak sa digitalnim trendovima i tokovima njihovih konkurenata.

Kao i u svakom drugom segmentu i u Evropskoj Uniji su pojedine države članice veoma rano, takoreći na vreme prepoznale potrebu za promene u pravcu digitalne transformacije, čime su ovakve inovacije počele da se uvode najpre u ključne privredne sektore, a onda i u druge proverene modele i društvene segmente.

Ono što je specifično za Evropsku Uniju, jeste da je ona shvatila i potrebu definisanja i usvajanja potpuno novog regulatornog okvira, zajedno sa paketom podsticajnih mera, kao sistema mera pažljivo strukturisanih za iskorišćavanje svih pogodnosti i potencijala zaokruženog i unificiranog jedinstvenog evropskog digitalnog tržišta.

Evropski model digitalne poslovne transformacije jasno je stavio akcenat na inovativnost kao motor razvoja, a time i što spremnije dočekivanje nadolazećih disruptivnih tehnologija i talasa.

Ovako ustrojeno „novo digitalno doba“, pred istraživače i stručnjake je postavilo potrebu da oni moraju razmišljati i kao inovatori i kao preduzetnici, bez obzira koliko to konfliktno zvučalo, jer svaka nova ideja i rešenje moraju biti blagovremeno prepoznati, imajući u vidu da će oni, bilo delimično, bilo u potpunosti promeniti ili zameniti prethodnu tehnologiju i primenjeno rešenje (Čelik, P.2019:61-81).

Jedan od osnovnih motiva za ovakav pristup, predstavlja i razvoj IoT tehnologije, odnosno tehnologije Interneta stvari, imajući u vidu da je tendencija razvoja ove tehnologije usmerena na povezivanje iste sa skoro svim ostalim naprednim tehnologijama, a pre svega nastupajućom 5G mrežom. Ova mreža biće temelj preko koga će ići povezivanje velikog broja senzora na veoma malom prostoru. Ovi senzori biće generatori proizvodnje velike količine podataka čija će upotrebljivost zavisiti od njihovog razumevanja i izvlačenja iz njih adekvatnog nivoa znanja, koje opet leži na potrebi da IoT tehnologija bude što efikasnija, a da sa druge strane ne ugrozi poslovnu i informacionu bezbednost.

Ova tehnologija će po prvi put pružiti mogućnost robotizaciji da postane komplementarna sa veštačkom inteligencijom. Razvoj veštačke inteligencije ukršten je sa velikim brojem oblasti, počev od poboljšanje mreže senzora, pa preko nano tehnologije i automatike, čime se veštačka inteligencija evidentira u različitim poslovnim oblastima i društvenim segmentima.

Četvrta industrijska revolucija posredstvom veštačke inteligencije povezuje dva do sada potpuno odvojena i rastuća digitalna područja, a to su robotika i elektronsko poslovanje. Ova integracija proizvodi jednu homogenu celinu čije je ciljano ishodište pametna fabrika. Oslonac ovog razvoja je kibernetičko-fizički sistem (Cyber-Physical-System CPS) čiji je funkcionalni oslonac internet sistem Cloud tehnologije.

Kibernetičko-fizički sistem je drugim rečima IoT ekosistem, koji kao takav, pored ostalog sadrži mrežu sastavljenu od pametnih satova, pametnih zgrada, „smart“ rešenja za pametne automobile, pametne gradove, pametnu poljoprivredu, medicinu, saobraćaj, ekologiju, pametnu oblast zaštite i spasavanja, itd.

Već duže vreme ne predstavlja retkost ni razvijanje koncepta pametnog grada na temeljima projekata pametne ekonomije, pametne javne uprave, pametnog saobraćaja, pametnog stanovništva, pametne okoline, pametnog življenja, itd. Iznalaženje potpunog odgovora na pitanje koji je dalji pravac tehnološkog razvoja, koje tehnologije će izmeniti i zaokružiti način proizvodnje, kakvi će biti trendovi ponašanja i komunikacije ljudi u budućnosti, pa i kakvi će biti budući trendovi na lokalnom, regionalnom i globalnom nivou, sasvim izvesno predstavljaće preporuku ovog rada za dalje istraživanje.

Aktuelni momentum, dostupna saznanja iz prakse i za sada oskudna literatura, još uvek nemaju sveobuhvatnu kompetentnost da bi dali konačnu projekciju sinergetskog efekta inovativnih digitalnih rešenja baziranih na korisničkim iskustvima, radi čega će dalji istraživački i naučni napori, ipak morati biti usmereni na rešavanje brojnih društvenih, privrednih, egzistencijalnih i drugih pratećih pitanja i problema koji danas nemilosrdno opterećuju sve zemlje, nevezano za njihov geografski položaj i razvojni i tehnološki status ili kapacitet (Čelik, P.2019:61-81).

Odgovor na pitanje zašto je sve to tako, ipak je donekle jednostavan. Digitalna privredna transformacija je svojom dinamikom naprosto obrisala sve do tada uspostavljene granice koje su egzistirale između tradicionalne (materijalne) i savremene digitalne ekonomije. Time je došlo do suštinskog razdvajanja resursno zasnovane ekonomije od ekonomije znanja ili savremeno

rečeno, ekonomije zasnovane na bitovima i bajtovima, tj. ekonomije čiju dodatnu vrednost generišu inovativne tehnologije, informacije i podaci putem njihove sveobuhvatne analize i znanja stečenih na tim osnovama.

Ipak, dosadašnji razvoj digitalne ekonomije isprofilisao je neke svoje ključne komponente. U te komponente spadaju vlada, pravna regulativa, širok dijapazon politika, internet, www, telekomunikaciona industrija, provajderi digitalnih usluga, elektronsko poslovanje i elektronska trgovina, tehnološki generisane informacije, sistemi za kreiranje i upravljanje znanjem, prava iz domena intelektualne svojine, ljudski kapital i njegova primenjiva znanja, stalno istraživanje i razvoj i na tome nastale nove tehnologije i rešenja (Čelik, P.2019:61-81).

Na globalnom planu takođe nema razlike, posebno ako se uzme u obzir činjenica da se transformacija poslovanja u digitalno, kao i stalna transformacija digitalnog poslovanja u zavisnosti od dostignutog nivoa razvoja, baziraju na samom središtu gotovo svih industrijskih segmenata i tržišta. Delokrug primene i opšta dostupnost digitalnog transformativnog fenomena ključ je digitalne transformacije, a time i ključ razvoja i opstanka svake tržišno orijentisane organizacije, dok je aplikacija okosnica transformacije izvršene u tom pravcu.

Ipak, ovo posmatranje ima i svoj širi kontekst. Digitalna transformacija ne predstavlja samo navedeno, već jedan celovit transformativni momentum u kome ne moraju učiti i unapređivati se samo radnici, već i menadžeri, imajući u vidu da ni oni više nisu izuzeti iz koncepta celoživotnog učenja i stručno/saznajne nadgradnje. Nesposobne da se odazovu ovome, vreme će eliminisati sa tržišta.

Elementi kao što su informacija i snaga umrežavanja, model su za strateški okvir razvoja digitalnih lidera, a tu digitalnu orijentaciju i njene ciljeve mora ostvariti sistem od strateškog menadžmenta naniže. Ovim fenomenima počinju da se bave neke nove naučne discipline, a nastala je potreba i za redefinisanjem tradicionalnih.

Činjenica da je ova disertacija dotakla širi kontekst koji je već prepoznat u stručnim krugovima, te koncept u kome je nastao jedan digitalni rascep koji nije po strani ostavio ni nauku, pa je tako nastali digitalni uspon pokazao da nema vremena da sačeka naučni izraz i tumačenje, što bitno usmerava preporuke ovog rada za dalje istraživanje.

Prefiks „e“ je učinio da ni poslovne strategije, a samim tim ni strategije razvoja nauke nisu više strategije, ako njihova koncepcija nema usklađenost sa stalno širećim digitalnim strategijama, tj. svim onim strategijama koje bitišu pod konstantnim pritiskom, kako mrežnih, tako i mobilnih, ali i socijalnih, globalnih i svih ostalih inovacija.

Humano-tehnološki biodiverzitet i primena nano, bio, kvantnih i drugih tehnologija, ipak je izdiferencirao stav, da kao što ne postoje dva jednaka čoveka, tako ne postoje ni dva jednaka, iako fizički istovetna informaciona sistema, što samim tim ne daje ni potpuno dva istovetna načina i sistema njihove primene ili upravljanja. Suptilne forme inventivnog osmišljavanja poslovnih funkcija i rešenje takvog sistema zahteva i suptilne, rafinisane forme zaštitnih mehanizama, a samim tim i mera koje su autorski proizvod jedinstvenog dometa ljudske pameti i inteligencije, a ne plod rutinske primene tehnologije digitalnih algoritama.

Ovo naučno saznanje jasno razvejava i daje odgovor na pitanje zašto određene tehnologije, čak i kada su povezane u istovetnu arhitekturnu infrastrukturu, svoj kvalitet ili nekvalitet pokazuju tek kada budu implementirane u ukupni kvalitativni sistem organizacionih i drugih mera kao temelja poslovne osnove i funkcije. Odgovor na to pitanje je to što je inovativnost važna, a tu je ljudski kapital i dalje nezamenjiv da projektuje rad resursa za konkretno poslovno okruženje i ambijent. Samim tim, preslikavanje određenih informacionih tehnologija, pa i njihove strukture i arhitekture na neko drugo slično poslovno okruženje, ne daju iste poslovne ni bezbednosne rezultate. Iz tog razloga širi kontekst navodi na zaključak da ne postoje dva jednaka informaciona sistema ni po poslovnom efektu, ni po implementiranom nivou zaštite, a samim tim ni po funkcionalnosti.

Ova praktično-naučna činjenica, govori nam i dovodi nas do zaključka da ne postoje, da nisu postojale, pa ni da u doglednoj budućnosti neće postojati potpuno sigurni informacioni sistemi.

Ovaj izazov zahteva „case by case“ odgovor zasnovan na multidisciplinarnom pristupu i kompleksnim holističkim modelima upravljanja, jer samo ovakvi sistemi imaju transformativnu moć da stvaraju prilike koje će iskoristiti celokupnu sinergiju svih postojećih i dostupnih tehničko-tehnoloških, organizaciono upravljačkih, fizičkih, društvenih i sličnih vrsta zahteva i kontrola.

Utvrđenja pokazuju da se samo tako i pod tim uslovima mogu uspostaviti ekonomski opravdani i poslovno efikasni sistemi zaštitnih proaktivnih mera u kontekstu digitalne poslovne transformacije i naravno svih njenih pratećih bezbednosnih implikacija.

Osnovni cilj poslovnih informacionih sistema jeste da oni pruže operativnu i tehnološku, a time i stratešku podršku poslovanju. Kompanije se u tom pravcu mogu osloniti samo na pouzdanu i uvek dostupnu informatičku podršku adekvatno primenjenih informacionih tehnologija. U suprotnom, čak i veoma kratak prekid funkcionisanja poslovnih informacionih sistema, pa čak i pojedinih njegovih delova ili servisa, značio bi tzv. “digitalnu komu“, koja implicira prestanak odvijanja kritičnih poslovnih procesa, van tehnološkog vegetiranja sistema. Ukoliko bi se dogodio ovakav vid „poslovanja“ on bi nesumnjivo bio prikaz poslovanja izloženog ogromnom riziku i troškovima, a najčešće i nepopravljivoj poslovnoj šteti, kako u materijalnom, tako i nematerijalnom smislu.

Stoga, greške i propusti u informacionoj bezbednosti nesumnjivo se dotiču ugrožavanja privatnosti. Ovakvi scenariji mogu imati krajnje negativne posledice po poslovanje organizacije, jer prekid rada istovremeno znači i nemogućnost sprovođenja poslovnih procesa, a ovu situaciju prati krađa podataka, tj. ugrožavanje privatnosti, što će nesumnjivo imati i direktno i indirektno negativne efekte na poslovanje, a pored takve vrste materijalne i nematerijalne štete, istovremeno će nastati i pravne posledice u domenu učinjenih regulatornih propusta i kazni, a to sve zajedno implicira sinergetski negativan učinak, kako na gubitak ugleda, tako i nepovratno narušavanje imidža i anuliranje poverenja korisnika na tržištu.

Bezbednosni incidenti kao druga strana medalje naprednog digitalnog poslovanja, nesumnjivo stvaraju brojne štete.

Krajnje progresivni napredak digitalne ekonomije i transformacije, bez sumnje vodi u neizvesnu budućnost, tj. budućnost čiji će plodovi pored ostalog biti još veće razmere bezbednosnih incidenata. Stoga, iz rezultata ovih istraživanja možemo definisati pitanja i zauzeti stav da bezbednosni incidenti nisu samo informatički problem, da bezbednosni incidenti nisu samo tehnički, poslovni i pozadinski rizici, već da se radi o strateškim poslovnim rizicima koji mogu preko noći u poslovnom smislu promeniti sve, uključujući i tržišnu i konkurentsku poziciju kompanije.

Rizik po jednoj od definicija predstavlja opasnost, odnosno verovatnoću da će određeni izvor pretnje u određenim okolnostima iskoristiti ranjivost sistema, a time se može pričiniti ozbiljna šteta na intelektualnoj i fizičkoj imovini organizacije. Iz tog razloga se ovde može izneti stav da su informatički rizici, zapravo rizici stalne perfidne prisutnosti, usled čega je kontrolisanje takve vrste rizika kroz mehanizme korporativnog upravljanja informatičkom funkcijom, izazov bez presedana na putu do postignuća strateških poslovnih ciljeva u kojima fokus čini zadovoljni korisnik-potrošač.

Noviji vidovi pretnji zahtevaju inovativne vidove zaštite, a ti vidovi zaštite moraju biti kompleksni. Samim tim, nezamenjiv je i proaktivni pristup zaštite tj. zaštite kompleksnim proaktivnim delovanjem, a taj sistem je nemoćan ukoliko nije delotvorno ukombinovan sa ostalim sredstvima zaštite. Napadi na informacione sisteme i informacionu infrastrukturu, bilo kompanija ili institucija, beleže stalni rast i učestalost. Meta napada nisu same institucije i kompanije, već njihove digitalne vrednosti koje podrazumevaju posedovanje poverljivih sadržaja, ličnih podataka korisnika, korisničkih imena i lozinki, zaštićenih dokumenata, itd., pa i sadržaja zaštićenih intelektualnom svojinom, pa je sve to dovelo do potrebe za utvrđenjem pravila koja bi bila u stanju pružiti zaštitu materijalnim i intelektualno-svojinskim vrednostima takvih organizacija.

Obzirom da cyber napade nije moguće predvideti sa sigurnošću, a najčešće ih nije moguće ni sprečiti, u tom smislu jedino što daje donekle efikasnu perspektivu jesu proaktivne, predostrožne mere koje povećavaju stepen bezbednosti u onim segmentima koji mogu biti od interesa cyber kriminala, kako bi se na tom temelju štetna verovatnoća svela na najmanju moguću meru, tj. minimum.

Nije sporno da je najčešći motiv cyber napada protivpravna imovinska korist, međutim, često je neposredna finansijska šteta u slučaju cyber napada mnogostruko manja od one koja je određenom sistemu ili organizaciji pričinjena eksponiranjem u njemu pohranjenih poverljivih informacija, naročito kada je reč o korisnicima.

Ustanovljavanje odgovarajućih bezbednosnih pravila koja imaju apsorpcionu moć da obuhvate celokupni područni kontekst segmenata podložnih raznim vrstama cyber napada, zapravo čine bezbednosnu politiku. Cilj ove politike je da uredi, kako dizajn tako i konteksturu svih pravila ponašanja i tako definiše suštinske odgovornosti u odnosu na konkretni informacioni sistem,

zajedno sa područjem njegove primene. Rezultat toga mora biti minimiziranje šteta i posledica bilo nenamernog, bilo namernog delovanja i radnji.

Da bi cyber bezbednost bila na visokom nivou, na istom nivou mora biti i sistem zaštite informacija koje su u opticaju u digitalnim i komunikacionim sistemima i krugovima.

Na osnovu nalaza ovog rada, može se zaključiti da je moderno doba poslednje generacije stvorilo digitalno transformisani svet, koji sa jedne strane donosi izuzetne koristi, dok je istovremeno sa druge strane izuzetno ranjiv.

Incidenti u domenu cyber bezbednosti, bez obzira na pozadinu njihovih dešavanja, mogu izazvati disrupciju, ne samo kod klasičnih poslovnih servisa, već i onih koji su usled civilizacijskih dometa počeli da se uzimaju zdravo za gotovo. Kada se to kaže, najčešće se misli na snabdevanje električnom energijom, vodosnabdevanje, zdravstvo i sl., obzirom da se njima u smislu poimanja i rangiranja po važnosti za korisnike u velikoj meri približavaju mobilni i digitalni servisi.

Dijapazon ugrožavanja u sferi digitalnog može imati razne pozadine. One se kreću od čisto kriminalnih, pa preko politički motivisanih, a onda i terorističkih i državno sponzorisanih. Međutim, u tu klasifikaciju moraju se ubrojati i prirodne katastrofe, ali i katastrofe izazvane nenamernim ljudskim greškama i biohazardima. U svakom slučaju, kvalitet svake preduzete mere ceni se kroz kontinuitet poslovanja i usluga koje kompanije, organizacije, društva, vlade i države putem svojih informacionih sistema pružaju na tržištu.

Može se reći da je celokupna kontekstura digitalnog, a time i prekograničnog poslovnog sistema, zapravo globalna i iz lokalne i iz globalne vizure. U tom kontekstu nastao je i termin „glokalno“, što bi po definiciji bilo „proces modifikacije globalnih uticaja u lokalnim kontekstima“. Na ovaj način je britanski sociolog Robertson još devedesetih godina prošlog veka definisao ovaj fenomen, što je u naučnom smislu potaklo da se dublje proanalizira neposredni uticaj interneta. Internet je učinio spajanje, ne samo termina, nego i odrednica globalno i lokalno, na koji način je došlo do sagledavanja globalnog uticaja ova dva pojma, kao i njihovog pratećeg fenomena koji ima svoje zagovornike i protivnike, a usmeren je ka kulturološkom ujednačavanju.

Digitalne platforme su zaista svet pretvorile u globalno selo, umrežile sve tačke, probile ekonomske barijere koje su postojale na granicama država i istovremeno smanjile troškove međunarodnih interaktivnih i transakcionih tokova. Tako su nastale potpuno nove zajednice

korisnika, a time i potpuno nova tržišta i na globalnom i na lokalnom nivou, tzv. „glokalna tržišta“.

Kompanije su tako dobile ogromne baze podataka kupaca i potencijalnih kupaca, ali i mogućnost da primene efikasne načine da do tih kupaca dođu, bez obzira na to gde se oni nalaze. Na ovaj način, kroz digitalnu transformaciju poslovanja, nastala su mala preduzeća koja posluju širom sveta. Ove takozvane „mikro multinacionalne kompanije“ da bi uspele u svojim globalnim nastojanjima, poslužile su se prisutnošću i dostupnošću digitalnih platformi kao što su Facebook, Aliexpress, Alibaba, Amazon, Ebay, itd., kako bi se putem njihovih globalnih potencijala direktno povezale sa kupcima i dobavljačima u svim zemljama sveta. Ovo je učinilo paradoks da ne samo mala preduzeća, već i najobičniji preduzetnici svoje aktivnosti mogu vršiti „glokalno“.

Zapravo, ni za koga više prekogranične aktivnosti nisu prepreka. Desio se još jedan paradoks da u globalizaciji učestvuju i pojedinci na isti način kao što to čine mala preduzeća i preduzetnici. Oni preko digitalnih platformi uče, nude svoje usluge, pronalaze poslove, pronalaze prostor da plasiraju svoje talente i grade svoje sopstvene profile, organizuju društvene mreže i krugove. Po prvi put u istoriji, tokovi podataka čine veći efekat od globalne trgovine robom.

Iako digitalni poslovni model pruža mnoge mogućnosti, globalni tokovi uglavnom su skoncentrisani na uzak krug vodećih zemalja. Ipak i dalje se dešava da se ekonomske praznine između vodećih zemalja i ostatka sveta zapravo sporo zatvaraju.

Takođe se desilo da je prethodni period učinio da su mnoge kompanije razvijajući prekogranične poslove, u klasičnom smislu postale izuzetno organizaciono složene, a samim tim često i manje efikasne. Digitalni model poslovanja kao vid transformacije, zapravo je i ovim konglomeratima ponudio mehanizme za poslovno pojednostavljenje, a time i sužavanje organizacionog modela, koji bi, kao znatno racionalniji, postao i sposobniji da odgovori na globalna kretanja. Tako su mnoge kompanije u sudaru sa digitalizacijom i globalizacijom došle u situaciju da moraju preispitati svoju ukupnu konkurentsku poziciju, svoju imovinu, proizvode i u skladu sa tim, ukupnu organizacionu strukturu.

Digitalna transformacija poslovanja je donela i to, da ne samo kompanije, već i države ne mogu sebi dozvoliti da budu isključene iz globalnih tokova, jer u tom slučaju mogu propustiti da iskoriste jednu od temeljnih vrednosti globalizacije koja se oslikava kroz idejna kretanja, kretanja i imputa i talenata, koji kao motor pokreću stalne inovacije i uvećanje produktivnosti.

Tako nastala digitalna globalizacija uvećava broj dostupnih izbora, usled čega u veoma kratkom vremenskom periodu dolazi do niza disruptivnih pomaka u kojima su lanci vrednosti meta u stalnom pokretu, kao što su to i nove centralne ekonomske aktivnosti.

Industrija 4.0 kao koncept nudi opštu prilagodljivost, međutim, čini se da potrošači ipak žele više.

U određenim krugovima pojavljuju se teze o masovnoj personalizaciji proizvoda koja je zapravo moguća samo u slučaju suštinskog povratka čoveka u proizvodnju. Prema nekim stidljivim najavama, ovakav vid industrije mogao bi biti čak nazvan „Industrija 5.0“.

Ovakav industrijski koncept osnažuje ljude kreatore da bolje shvate osnovne ljudske potrebe i nastojanja da nabave proizvod putem koga se mogu izraziti, a ta vrsta proizvoda jeste ona za koju su kupci i korisnici spremni da plate veću, tzv. „premijum cenu“.

U toj koncepciji proizvodnje, ljudsko učešće je neprikosnoveno. U ovom smislu i pravcu, uveliko se razvijaju tzv. kolaborativni roboti, tzv. „koboti“, koji su koncipirani na način da kompanijama omoguće širok spektar personalizovanih proizvoda kakve zapravo traže današnji potrošači. „Koboti“ su zapravo rešenje koje treba da unese ljudski dodir u masovnu proizvodnju.

Uključivanje ljudskih bića u središte industrijske proizvodnje potpomognuto alatima kao što su koboti, omogućava da industrija u nastajanju, tj. „Industrija 5.0“ nije samo tu da potrošačima pruži proizvode koje oni žele sada, već da sa druge strane radnicima pruži poslove koji su mnogo inventivniji i smisleniji od onih koji su radnicima bili u ponudi duže od jednog veka. Ono što se o digitalnoj ekonomiji i transformaciji može sa sigurnošću reći, jeste da se ona širi izuzetno snažno i krajnje neravnomerno i uvek prema izvorima profita.

Promene utiču na svakoga, bilo da ih je on pokrenuo ili im se našao na putu.

Druga činjenica koju ne smemo izostaviti jeste, da je u toku raspodela novonastalog „digitalnog kolača“ i da su se u tom segmentu kao lider najpre nametnule SAD. Međutim, digitalni svet i doba uveli su nove „tigrove“ i „lavove“ u ovu arenu i to upravo one koji nisu mnogo zainteresovani da razumeju želju SAD-a da po svaku cenu zadrži svoju dosadašnju poziciju i produbi razliku koju je postupno decenijama stvarala u odnosu na druge. Činjenica da se tržištu već dogodila „uberizacija“ jasno govori da SAD još uvek donekle idu korak ispred Evropske

Unije, međutim, da li se to može reći za i kinesku konkurenciju i još neke azijske ekonomije, to je već diskutabilno i može biti preporuka za dalja istraživanja.

U ovakvoj konstelaciji, bezbednost je postala, ne samo u kompanijama, već i kod korisnika, visokorangirani prioritet. Digitalni komfor korisnika odavno ima svoju cenu u domenu izloženosti cyber pretnjama, jer ove pretnje, kako bi neki stručni krugovi definisali, ipak u smislu razvojnog nivoa za nijansu imaju brži razvoj nego što tržište zaštitnih proizvoda može odgovoriti. Ispostaviće se da digitalna transformacija poslovanja leži na poverenju korisnika koje je u jednom trenutku jako kao tvrđava, a već u sledećem može biti pretvoreno u prah.

Može se stoga zaključiti da digitalno poslovanje i transformacija počivaju na digitalnom poverenju. Digitalno poverenje počiva na digitalnom ugledu, a sve to zajedno na prerogativu nazvanom digitalna bezbednost, odnosno digitalna otpornost, koja tek može garantovati profit.

Sumiranjem svega iznetog, digitalna poslovna transformacija je u sudaru sa digitalnom bezbednošću otvorila, pored svih poslovnih izazova i potrebe država da lokalno uređuju globalna i prekogranična pitanja koja je digitalni poslovni model stvorio. U tom smislu, ispostavilo se da je informacija roba najveće vrednosti i da je informacija jedina vrsta robe koja svojom eksploatacijom ne gubi na vrednosti. Iz tog razloga vrednost informacije kao robe naročito raste i stvara stalnu dodatnu vrednost kroz njeno novo korišćenje, a naročito ako je pritom bezbedna i zaštićena od onih kojima ne bi smela biti dostupna.

Tendencije uvođenja lokalnih pravnih propisa sa globalnom primenom, kakav je slučaj sa uredbom Evropske Unije, GDPR, kao i pored ostalog i Zakona o bezbednosti podataka američke savezne države Kalifornija, ili kalifornijski Zakon o internetu stvari, zapravo predstavljaju stvaranje do sada nezamislivog pravnog okvira u kome lokalni pravni propisi definišu tržišne modele poslovanja, ne samo regionalno, već i interkontinentalno. U središtu ove bezbednosne konstelacije jeste korisnik (potrošač) i njegov podatak kao „novo zlato“ koje mora uživati „glokalnu“ zaštitu.

Iz svega iznetog možemo zaključiti da su u ovoj disertaciji u potpunosti dokazane, kako glavna, tako i sve pomoćne postavljene hipoteze i ujedno date višestruke preporuke za dalja istraživanja sa odgovarajućim smernicama.

Korišćena literatura:

Bibliografski izvori:

1. *10 Major Application Areas of Drone*, Geospatial World, April 6th 2018
2. *2015 Cost of Data Breach Study: Global Analysis*, (2015). Ponemon Institute, Research Report, pp.1
3. *5G Wireless Mobile Technology*, (2019). Electronics Notes
4. *A strategy for smart, sustainable and inclusive growth*, (2010, March 3). Communication from the Commission, COM 2020, Brussels
5. Ablon L., Libicki M., Golay A., (2014). *Markets for Cybercrime Tools and Stolen Data*, Sponsored by Juniper Networks.
6. *Akcioni plan za sprovođenje prioriteta iz "eSEE Agenda+ za razvoj informacionog društva u Jugoistočnoj Evropi za period 2007-2012. godine"*, "Službeni glasnik RS", 29/09
7. Alex R. M., Aayad Al H., Khalil Al R., (2010). *Cyber Crimes: Threats and Protection*, International Conference on Networking and Information Technology.
8. *Annual World Robotics Report*, (2018). International Federation of Robotics, presented at Press Conference in World Robot Summit in Tokyo
9. Argote, L. (2013). *Organizational Learning: Creating, Retaining and Transferring Knowledge*. New York: Springer Science + Business Media.
10. Ar-Raqib, A; Roche, E. M; (2009). *Virtual Worlds Real Terrorism*, Ardworf Publications, Den Haag.
11. Assange, J., (2014). *When Google Met WikiLeaks*, OR Books, New York – London.
12. Athey, S., (2018). *Reshaping Markets to Solve Poverty and Inequality*, Stanford Business, 10.10.2018.
13. Avižienis A., Laprie J. C., Randell B., Landwehr C.(2004). "Basic Concepts and Taxonomy of Dependable and Secure Computing", *Transactions On Dependable And Secure Computing*, Vol.1, No.1, January-March
14. Bartlett J., (2015). *The Dark Net: Inside the Digital Underworld*, Melville House, New York/London.

15. Berman S. J, (2012). Digital transformation: Opportunities to create new business models. *Strategy & Leadership*, 40 (2), pp 16-24.
16. Bharadwaj A, El Sawy O. A, Pavlou P. A, & Venka-traman N. V, (2013). Digital business strategy: toward a next generation of insights, *MIS Quarterly*, 37(2), pp. 471-482.
17. Bigo, D. et al.(2013). National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law, European Parliament, Brussels, pp. 14–15,
18. Bishop, J; (2015). Psychological and Social Implications Surrounding Internet and Gaming Addiction, IGI Global, Hershey.
19. Blum, W; (2014). America’s Deadliest Export: Democracy: The Truth About U.S. Foreign Policy and Everything Else, Zed Books, London/New York.
20. Bossler, A; (2015). Metadata Analytics, Law, and Future of the Internet, in: *The Future Internet*, Springer, Cham.
21. Boyd&Crawford, *Six Provocations for Big Data*, (2011). Oxford Internet Institute, A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, September 21, 2011.
22. Branković, S., (2017). *Veštačka inteligencija i društvo*, Filozofski fakultet, Niš, Srpska politička misao, broj 2/2017.god, Institut za političke studije, Beograd, 24. vol. 56. str. 13-32
23. Brynjolfsson, E., Mitchell, T., Rock, D.,(2018). What Can Machines Learn, and What Does It Mean for Occupations and the Economy?, *AEA Papers and Proceedings*, 108, OI:10.1257/pandp.20181019, 43-47
24. Bubanja, V.M., (2015), *Zašto je Srbiji potrebna digitalno podržana razvojna strategija*, *Ekonomski vidici*, XX, Br. 2-3: str. 153-166
25. Budimir, M., (2010). Utjecaj posljedica globalizacije i razvitka informacijsko-komunikacijskih tehnologija na novi svjetski poredak, “Praktični menadžment”, Vol. I, broj 1.
26. Buhr, D., (2015). *Social Innovation Policy for Industry 4.0*, Division for Social and Economic Policies, Friedrich-Ebert-Stiftung Publisher, pp.6

27. Burwell, F., (2018). Making America first in the digital economy: The case for engaging Europe.
28. Cavusoglu, H., Mishra, B., Raghunathan, S. (2004, Fall). The effect of Internet security breach announcements on market value: Capital market reaction for breached firms and Internet security developers, *International journal of Electronic Commerce*, 9(1), 69-104.
29. Centre for European Studies, Brussels.
30. CFO Research Services (2005): Risk Denial from the Top?, CFO Publishing Corp. i PriceWaterhouseCoopers.
31. Charney, C., (2009). Rethinking the Cyber Threat: A Framework and Path Forward, Microsoft.
32. Chiesa, R., Ducci, S, Chiappi, S. (2004). Hacker Profiling Project,
33. Ciancaglini, V., Balduzzi M., Goncharov M., McArdle R., (2013). *Deep web and Cybercrime*, A Trend Micro Research Paper.
34. Coase, R, The nature of the firm, *Economica*, Number 4, pp. 386-405, 1937. i Coase, R, *The Firm, the Market and the Law*, University of Chicago Press, Chicago, IL, 1998.
35. Coase, R. (1937). The nature of the firm, *Economica*, Number 4, pp. 386-405.
36. Coase, R. (1998). *The Firm, the Market and the Law*, University of Chicago Press, Chicago, IL
37. Cobb, S., (2014). Four basic and effective defensive measures against cybercrime, Tech Brief, ESET Business Solutions.
38. Coderre, D., (2009). *Internal Audit, efficiency through automation*, John Wiley&Sons Inc.New Jersey, USA, 2009.
39. Coxall, M., (2015). *Civil Disobedience: A Practical Guide*.
40. Čelik, P., (2019). *Institucionalne mere za povećanje sajber sigurnosti poslovanja u Evropskoj Uniji*, *Ekonomске teme*, Niš, Vol. 57 (3), str. 351-364
41. Čelik, P., (2019). *Bezbednosne implikacije digitalnog poslovanja*, *Ekonomija- teorija i praksa*, godina XII, broj 4, str. 61-81
42. Ćuzović, Đ., Sokolović-Mladenović, S., (2014). *Globalizacija digitalne ekonomije*, *Međunarodna naučna konferencija Univerziteta Singidunum Sinteza 2014.*, str.144
43. *Cyber Threats to National Security*, (2011). Symposium Five: Keeping the Nation's Industrial Base Safe From Cyber Threats, 2011 CACI International Inc.

44. D'Souza, C., & Williams, D. (2017). The Digital Economy. Bank Of Canada Review, 5.
45. Da Rosa I, & de Almeida J, (2017). Digital Transformation in the Public Sector: Electronic Procurement in Portugal, In Digital Governance and E-Government Principles Applied to Public Procurement (pp. 99-125), IGI Global.
46. Damnjanović, D., (2016)., Primena Internet of Things (IoT) rešenja u upravljanju održavanjem u proizvodnji, Atom Bits d.o.o., str.117
47. Dandoulaki, M; Halkia, M; (2013). Social Media (Web 2.0) and Crisis Information: Case Study Gaza 2008-09, in: Examining the Concepts, Issues, and Implications of Internet Trolling, IGI Global, Hershey.
48. *Data snapshot: AI Chatbots and Intelligent Assistants in the Workplace*, Spiceworks Study, 2018.
49. Davis C., Schiller M. and Wheeler K., IT revizije Savez računovođa i revizora Srbije, 2008.
50. Digital Transformation Index, (2016)., Dell Technologies EMC
51. *Digitalna transformacija gospodarstva 2016 - 2020*. - Inicijativa za ubrzanje digitalne transformacije i za suradnju po 5-Helix inovacijskom modelu, Infodom grupa, pp.1
52. Đoković G., Pavićević, S., Čelik P. (2014). Razvoj preduzetništva, tranzicija i ljudski resursi, Glasnik za društvene nauke, Alfa univerzitet, godina V, br.5, Beograd
53. Đoković G., Čelik P., (2016). „Informacione tehnologije kao ključni faktor ekonomskog i tehnološkog razvoja preduzetništva“, Druga međunarodna naučno-stručna i biznis konferencija LIMEN 2016, Zbornik radova „Liderstvo i menadžment – integrisane politike istraživanja i inovacija“
54. Đoković G., Čelik P., Milunović M., (2016). „Informatički izazovi preduzetništva podstaknuti novim ekonomskim tendencijama“, Međunarodna naučno-stručna konferencija MBS HR 2016, Beograd
55. Drajić, D., (2017)., Uvod u IoT, Izdavačka misao, 2018., str.13
56. Drucker, P. (1999). Management Challenges for the 21st Century, HarperBusiness, New York.
57. Dunn, C. M; (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, Routledge, New York.

58. Đurđević, D; Stevanović, M. (2015). Izazovi nacionalnoj bezbednosti u kiberprostoru društvenih mreža: studija slučaja „Navalni“, Zbornik, Forenzička revizija, Beograd.
59. Economy Discussions, 2015
60. Ekonomski efekti tranzicije i restrukturiranja privrede Srbije u funkciji evropskih integracija
61. Electronics and Information (J-6), International Co., Taiwan, ROC cDCGS for Communications, Ministry of National Defense, Taiwan, ROC Received 1 October 2003; received in revised form 11 March 2004; accepted 20 March 2004
62. Eloff J., Eloff M., Information Security Management – A New Paradigm
63. Ernst & Young (2011). *Into the cloud, out for of the fog*, Global Information Security Survey 2011, Ernst & Young, USA.
64. Fellander, A., Ingram, C., Teigland, R., Sharing Economy- Embracing Change with Caution, Entreprenorskapsforum, 2015.
65. Fitzgerald M, Kruschwitz N, Bonnet D, & Welch M, (2014). Embracing digital technology: A new strategic imperative. MIT Sloan Management review, 55(2), 1.
66. Fulmer, K. L., (2005). Business Continuity Planning -A Step-by-Step Guide with Planning Forms, Third Edition, The Rothstein Catalog On Disaster Recovery, Brookfield, Connecticut, pp. 7
67. G. Milovanović, P. Veselinovic, (2009). Globalizacija i tranzicija, Ekonomski fakultet, Kragujevac.
68. Galbraith, J. (2012). The evolution of enterprise organization designs. Journal of Organization Design, 1(2), 1-13.
69. Gardiner M., The Critical Incident Response Maturity Journey, White Paper, EMC, 2013
70. Gartner Top 10 Strategic Technology Trends for 2019, Gartner Report
71. Gartner, (2002), "The Elusive Business Value of IT", August 2002.
72. *GeSI SMARTer 2020*, The Role of ICT in Driving a Sustainable Future, Global e-Sustainability Initiative aisbl and The Boston Consulting Group, Inc. pp.87
73. Global Competitiveness Report 2018, World Economic Forum
74. Great Britain Parliament, (2013). House of Commons: Home Affairs Committee, Undercover Policing: Interim Report, Thirteenth Report of Session 2012-13, The Stationary Office, London.

75. Groznik, A., Kovačić, A., Spremić, M., (2003). Do IT Investments Have a Real Business Value?, *Applied Informatics*, No.4, 2003, pp.180-189.
76. Grupa autora (koordinator: J. Bajec,), (2010). Postkrizni model ekonomskog rasta i razvoja Srbije 2011-2020., USAID-SEGA projekat, Beograd.
77. Harris Bricken, International Law Firm, 2016.
78. Harshak A, Schmaus B, & Dimitrova D, (2013). Building a digital culture: How to meet the challenge of multichannel digitization. Booz & Company, Strategy&, pwc, 1, 1-15.
79. Hermann, M., Pentek, T., Otto, B., (2015). Design Principles for Industrie 4.0 Scenarios: A Literature Review. 10.13140/RG.2.2.29269.22248.
80. Hern, A. (2016). Blockchain: The answer to Life, universe or everything,
81. Hopia, H; (2015). Dawn of the Drones: Europe's Security Response to the Cyber Age, Wilfried Martens
82. *How 3D Printers Work*, (2014). US Department of Energy, pp.1
83. Hu, Q., Kapucu, N. (2016). Information Communication Technology Utilization for Effective Emergency Management Networks. *Public Management Review*, 18(3), 323-348.
84. Husain, Z., Dayan, M., Di Benedetto, C.A. (2016). The impact of networking on competitiveness via organizational learning, employee innovativeness, and innovation process: A mediation model. *Journal of Engineering and Technology Management*, (In Press).
85. Industry 4.0 Challenges and solutions for the digital transformation and use of exponential technologies, (2015). Deloitte, pp.6-7
86. *Intelligent technology: As digital applications encroach on various aspects of daily life, the impact on the economy will help us live smarter and better*, *Finance And Development*, 53(3), 6-9.
87. Internet ogledalo, (2019), DATA, str.22
88. *IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers*, (2019), Business Insider, The Internet of things
89. ISACA (2012). Extracting Value from Information Chaos: Why Good Governance Makes Good Sense, CobiT 5, ISACA, Rolling Meadows, Illinois, USA.

90. ISACA (2015). Global Cyber Security Status Report, ISACA, Rolling Meadows, Illinois, USA.
91. ISO/DIS 31000
92. ITGI (2003). Board Briefing on IT Governance, 2nd ed., IT Governance Institute, Rolling Meadows, SAD.
93. ITGI (2007). CobiT 4.1 - Framework, Control Objectives, Management Guidelines and Maturity Models, IT Governance Institute, Rolling Meadows, SAD.
94. Jovković S., Čelik P., (2017). „Dometi i ograničenja digitalizacije pravosuđa u Republici Srbiji“ - „Benefits and Limitations of Digitization of the Judiciary in Serbia“, XIV Međunarodni naučni skup, “Pravnički dani - prof. dr Slavko Carić“, Novi Sad, ISBN 978-86-6019-076-7 (M31)
95. Kagermann H., Wahlster W., Helbig, J., (2013), Recommendations for implementing the strategic initiative INDUSTRY 4.0, Final report of the Industry 4.0 Working Group, pp.6-7
96. Kagermann, H., Osterle, H., & Jordan, J. M. (2011). IT-driven business models: Global case studies in transformation, Hoboken, Nj.
97. Kane G. C, Palmer D, Phillips A. N, Kiron D, & Buckley N., (2015). Strategy, not technology, drives digital transformation. MIT Sloan Management Review and Deloitte University Press, 14.
98. Kaplan B, Truex D. P, Wastell D, Wood-Harper A, T. & DeGross, J, (2010). Information Systems Research: Relevant Theory and Informed Practice, Springer.
99. Kokles, M., Romanová, A., Hamranová, A. (2015). Information Systems in the Post-Transition Period in Enterprises in Slovakia. Journal of Global Information Technology Management, 18(2), 110-126.
100. Komarčević M., Čelik P., (2018). „Uticaj disruptivnih tehnologija na zaštitu ličnih podataka i privatnosti u digitalnom prostoru“, X Međunarodna naučna konferencija: „Sloboda i bezbednost u relanom i sajber prostoru“ (M33)
101. Komarčević M., Dimić M., Čelik P., (2017). Challenges and impacts of the digital transformation of society in the social sphere in: SEER, Journal for Labour and Social Affairs in Eastern Europe, seite 31-48, jahrgang 20 ISSN print: 1435-2869, ISSN online: 1435-2869, doi: 10.5771/1435-2869-2017-1-31; (M31)

102. Komisija Evropskih zajednica, COM 2003 (2003). Izveštaj Komisije Vijeću o spremnosti BiH za pregovore o Sporazumu o stabilizaciji i pridruživanju EU, Brisel.
103. *Komunikacija Komisije europskom Parlamentu, Vijeću Europskom gospodarskom i socijalnom Odboru i Odboru Regija, Digitalizacija europske industrije- Iskorištavanje svih prednosti jedinstvenog digitalnog tržišta*, Evropska Komisija, COM 2016, 180 final, 2
104. Kotlica, S., Stanojević, N., (2017). *Technology, innovation and competitiveness in the globalized economy*, Visoka škola akademskih studija „Dositej“ Beograd
105. Kozlovski N., A Paradigm Shift in Online Policing – Designing Accountable Policing
106. Krsmanović, B., (2013). Izazovi digitalne ekonomije, VIII Međunarodni Simpozijum i korporativnom upravljanju, Banja Vrućica
107. Krsmanović, B., (2014). *Koncept digitalne ekonomije*, Novi Ekonomist br.15, 4-10
108. Krsmanović, B., Polić, St., *Informacione tehnologije u računovodstvu I reviziji*, Bijeljina, 2008.
109. Ernst & Young (2006.) *Achieving Success in a Globalized World Is Your Way Secure?*, 2006 Global Information Security Survey.
110. International Organization for Standardization (ISO), *Code of Practice for Information Security Management, ISO/IEC 17799*, Switzerland, 2005.
111. Kuntsman, A; Stein, Rebecca, (2015). *Digital Militarism: Israel's Occupation in the Social Media Age*, Stanford University Press, Stanford.
112. Kwo-Jean Farna, Shu-Kuo Lina, Andrew Ren-Wei Funga, *A study on information security management system evaluation assets, threat and vulnerability*, Institute of Information Management, National Chiao-Tung University, 1001 Ta Hsueh Road, Hsinchu 300, Taiwan, ROC b Internet Security Solutions
113. Lajović, D., Vulić, V., (2010). *Tehnologije i inovacije*, Ekonomski fakultet Podgorica, str. 34
114. Laprie J.C. (1995). *Dependability - Its Attributes, Impairments and Means, Predictably Dependable Computing Systems*, B. Randell et al., eds., pp. 3-24.
115. Lazarević G., *Uticaji IT informacionog društva na društveno-ekonomski razvoj*, Izvorni naučni članak, UDK:681.518:330.34, JEL:D83, F63, 2012.

116. Lederer A.L., Salmela H., (1996). Toward a Theory of Strategic Information Systems Planning, journal of Strategic Information Systems, Volume 5, Number 3, pp. 237-253, 1996.
117. Lederer A.L., Salmela H., Toward a Theory of Strategic Information Systems Planning, journal of Strategic Information Systems, Volume 5, Number 3, pp. 237-253, 1996.
118. Lee, K.F. (2018)., AI Superpowers: China, Silicon Valley, and the New World Order 1st Edition, Houghton Mifflin Harcourt; 1 edition, September 25, 2018
119. Lee, N; (2014). Facebook Nation: Total Information Awareness, Springer, New York.
120. Leković, V., (2017). *Institucionalne promene kao determinanta privrednog razvoja Republike Srbije*, Ekonomski fakultet, Univerzitet u Kragujevcu
121. Lepore, J., (2014). *The Disruption Machine*, The New Yorker, June 16th
122. Liang, T.P., You, J.J., Liu, C.C. (2010). A resource-based perspective on information technology and firm performance: a meta analysis. *Industrial Management & Data Systems*, 110(8), 1138-1158.
123. Limbu, Y.B., Jayachandran, C., Babin, B.J. (2014). Does information and communication technology improve job satisfaction? The moderating role of sales technology orientation. *Industrial Marketing Management*, 43, 1236-1245.
124. Mahoney, M., (1998). The History of Computing in the History of Technology, Program in History of Science Princeton University, Princeton, Nj (*Annals of the History of Computing* 10, 113-125)
125. Mandelbaum, R. (2015). How Lending Club is shaping the future of small-business Loans <http://www.inc.com/magazine/201505/robb-mandelbaum/Lending-club-money-on-demand.html>
126. Mandelbaum, R. (2015): How Lending Club is shaping the future of small-business Loans <http://www.inc.com/magazine/201505/robb-mandelbaum/Lending-club-money-on-demand.html>
127. Marković, D., Nedić, D.N., (2016). Mogućnosti primene IoT tehnologije u stočarstvu i veterini, DOI: 10.7251/VETJ1601059MUDK 631.12.017.1/.3:681.513.2B., str.58
128. Maroofi, F., Rastad, S.A., Amjadi, M. (2015). Examining the Role of Information and Communication Technology to Improve Job Satisfaction. *Journal of Applied Sciences*, 15, 752-762.

129. Matijašević, M., (2018). *Sigurnosni zahtjevi i izazovi u 5G pokretnim mrežama*, Završni rad, Osijek,
130. Matt C, Hess T, & Benlian A, Digital transformation strategies. *Business&Information Systems Engineering*, 57(5), 339-343, 2015.
131. Mauher, M., (2016). 1869
132. Mayurakshi R., Parthasarathy R., (2007). *GTAG 7 - Global Technology Audit Guide: Information Technology Outsourcing*, The Institute of Internal Auditors.
133. McFarlan. F. W., McKenney, j. L., Pyburn, Ph. j., (1983). *The Information Archipelago - Plotting a Course*, Harvard Business Review, jan-Feb 1983.
134. McKinsey Global Institute Report, 2013
135. McKinsey Global Institute Report, 2016
136. McKinsey Quarterly Report, April 2017, McKinsey Global Institute, No.2
137. Mell, P., Grance, T., (2011). *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, US Department of Commerce, Special Publication,pp.2
138. Meyer, D. (2016). *Why Adidas is turning to robots in Germany and US*.
139. Michael K. Bergman, (2000). *The Deep Web: Surfacing Hidden Value*, White paper.
140. Mijalković, S. (2014). „Sex-Espionage“ as a Method of Intelligence and Security Agencies, *Bezbednost*, br. 1, str. 5–22, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd.
141. Mijalković, S; (2015). *Trash Intelligence kao metod obaveštajno-bezbednosnog rada*, *Bezbednost*, br. 1, str. 5–18, Ministarstvo unutrašnjih poslova Republike Srbije, Beograd.
142. Miletić, Lj., Ničić, M., Ćurčić, R., (2014). *Uticaj informacionih tehnologija na lanac vrednosti i podizanje konkurentnosti preduzeća*, Međunarodna konferencija Univerziteta Union, Sinteza 2014, 977
143. Milovanović, G., i Veselinović, P. (2009). *Globalizacija i tranzicija*. Kragujevac: Ekonomski fakultet Univerziteta u Kragujevcu,17-23
144. Minghetti, M. (2014) *Collaborative Intelligence: Towards the Social Organization*, Cambridge Scholars, Newcastle.

145. Mitchell, J.I., Gagné, M., Beaudry, A., Dyer, L. (2012). The role of perceived organizational support, distributive justice and motivation in reactions to new information technology. *Computers in Human Behavior*, 28(2), 729-738.
146. Mitić, S., Duđak, Lj., Savić - Šikoparija, T. (2014). Primena informacione tehnologije kao podrška organizacionom učenju, 12. Međunarodna naučno-stručna konferencija, Doba znanja, 26-27. septembar 2014., Sremski Karlovci, Srbija.
147. Müller, V. & Bostrom, N. (2016). Future progress in artificial intelligence: A survey of expert opinion In *Fundamental Issues of Artificial Intelligence*, Berlin: Springer pp. 553-571.
148. Musa, A., (2006). *E-Uprava i problem digitalne podijele aktivnosti usmjerene na poboljšanje pristupa Internetu u EU i Republici Hrvatskoj*, Zagreb.
149. Mutula, S. (2010). *Digital Economies: SMEs and E-Readiness Business Science Reference*, New York, pp.17
150. Najdanović M. i Rajković S., (2012). *Internet i elektronsko poslovanje*, Poslovno komuniciranje, Departman za Multimedijalne tehnologije, Univerzitet u Nišu.
151. Navimipour, N.J., Soltani, Z. (2016). The impact of cost, technology acceptance and employees' satisfaction on the effectiveness of the electronic customer relationship management systems. *Computers in Human Behavior*, 55, 1052–1066.
152. Navimipour, N.J., Zareie, B. (2015). A model for assessing the impact of e-learning systems on employees' satisfaction, *Computers in Human Behavior*, 53, 475-485.
153. Nedeljković, S. (2015). Evropska strategija bezbednosti Sajber pretnje- Značaj za Srbiju, *Vojno delo* 3/2015, Ministarstvo unutrašnjih poslova R. Srbije, str.144.
154. Nolan, R. and McFarlan, F.W., (2005). *Information Technology and Board of Directors*, Harvard Business Review, October, 2005.
155. OECD (2004). *Principles of Corporate Governance: 2004 edition*.
156. Oettinger, G., (2016). *Industrija 4.0 i budućnost*, PC Press
157. Omand, D. (2015) *Understanding Digital Intelligence: A British View*, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, IGI Global, Hershey, pp. 113–115.

158. Page, S. (2016). 12.1 Business Process Management. In Power of Business Process Improvement - 10 Simple Steps to Increase Effectiveness, Efficiency, and Adaptability (2nd Edition) AMACOM – Book Division of American Management Association.
159. *Pametne fabrike budućnosti, Internet stvari za automatizaciju*, Industrija br. 54, (2015), str. 16
160. Panian, Ž, Spremić, M. (2007). Korporativno upravljanje i revizija informacijskih sustava, Zgombić i partneri, Zagreb.
161. Panian, Z., (2001): Kontrola i revizija informacijskih sustava, Sinergija, Zagreb, str. 41-43.
162. Pejanović Lj., Komarčević M., Čelik P. (2017). *Centralizacija i militarizacija područja bezbednosti u Evropskoj Uniji*, Crisis Management Days, 10th International Scientific Conference, Velika Gorica
163. Petkovic, Z., (2018). English as a CyberLanguage, X Međunarodna naučna konferencija: „Sloboda i bezbednost u relanom i sajber prostoru“, Beograd
164. Peppet, S., R., (2014). *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, Texas Law Review, Vol. 93:85
165. Perić, E., (2017). Industrija 4.0, Hrvatska gospodarska komora, Zagreb, str. 5
166. Phillips, W. (2015). This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream Culture, MIT Press, Cambridge/London.
167. Piccinini E, Hanelt A, Gregory R, & Kolbe L., (2015). Transforming Industrial Business: The Impact of Digital Transformation on Automotive Organizations, Thirty Sixth International Conference on Information Systems, Fort Worth.
168. Piccoli, G., Pigni, F. (2016). Information Systems for Managers, edition 3.0, Prospect Press, pp. 345, USA.
169. Popesku M., (2016). *Četvrta industrijska revolucija I budućnost istraživanja tržišta: Podaci kao nova nafta*
170. Porter, M., (1985). Competitive Advantage, The Free Press, New York.
171. Powell, W.W., (1990). Neither Market nor Hierarchy: Network Forms of Organization, Research in Organizational Behavior, 12, pp. 295-336.

172. Prahalad, C.K., Hamel G. (1990). The Core Competence of the Corporation, Harvard Business Review, May - June 1990, pp. 79-91.
173. Pregled tržišta telekomunikacija i poštanskih usluga u Republici Srbiji u 2017. godini, Regulatorna agencija za elektronske komunikacije i poštanske usluge - RATEL
174. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, SWD (2013) 31 final, SWD (2013) 32 final, European Commission, COM (2013) 48 final, 2013/0027(COD) Brussels, 2013.
175. Rahman, A., Hamid, A., Zakir, U., Chin, (2017). Emerging Technologies with Disruptive Effects: A Review, Perentis eJournal, 7, 111-128.
176. Raičević V., Glomazić R., Matijašević, J., (2012). *Upravljanje projektima kroz IT komunikacije*, Zbornik radova sa I Međunarodnog naučnog skupa „Moć komunikacije 2012“ - održane 1-2. juna 2012. god. u Beogradu; Panevropski Univerzitet „Apeiron“, Banja Luka; str. 206-217
177. Raičević, V., Matijašević, J., Ignjatijević S., (2012). Ekonomski efekti i pravni aspekti elektronskog novca i elektronskog plaćanja, Economy and Market Communication Review (Emc Review), Fakultet poslovne ekonomije, Panevropski Univerzitet Apeiron, God./Vol. II, Br./No. I, Banja Luka, str. 105-118
178. Rauser, A., (2016). Digital Strategy: A Guide to Digital Business Transformation. CreateSpace Independent Publishing Platform
179. Reagle, J., (2015) Reading the Comments: Likers, Haters, and Manipulators at the Bottom of the Web, MIT Press, Cambridge, London.
180. Rifkin J., (2014). Društvo u kojem je granični trošak jednak nuli, New York Times
181. Rights for Superior Results, (2004). Harvards Business School Press.
182. Robinson, M. (2016). How Americans thinks world will look like in 2036.
183. Rogers D.L, (2016). The Digital Transformation Playbook: Rethink Your Business for the Digital Age, Columbia University Press
184. Roztocky, N., Weistroffer, H. R. (2011). Information technology success factors and models in developing and emerging economies, Information Technology for Development, 17(3), 163 –167.

185. Roztocky, N., Weistroffer, H. R. (2015). Information and communications technology in developing, emerging and transition economies: An assessment of research, *Information Technology for Development*, 21(3), 330-364.
186. Saga, (2016). PC PRESS br.219
187. Schultz, F., Utz, S., Göritz, A. (2011). Is the medium the message? Perceptions of and reactions to crisis communication via twitter, blogs and traditional media, *Public Relations Review*, 37(1), 20-27.
188. Schwab, K., (2016). The Fourth Industrial Revolution, World Economic Forum, pp.7-8
189. Sehlin, D., Truedsson, M. (2018). *A Conceptual Cooperative Model Designed for Business Processes, Digitalisation and Innovation*, Master thesis | Industrial Engineering and Management Spring term, Linköping University
190. *SewBot Is Revolutionizing the Clothing Manufacturing Industry*, Device Plus, February 19, 2018.
191. Shorer-Zeltser, M; Ben-Israel, G. M., (2016) Developing Discourse and Tools for Alternative Content to Prevent Terror, in: *National Security and Counterintelligence in the Era of Cyber Espionage*, IGI Global, Hershey, pp. 102–122.
192. Simulation, Volume 1, Issue 6, pp. 17-25
193. Sinkovski S., (2005). Informaciona bezbednost – komponenta nacionalne bezbednosti, *Vojno delo*, 2/2005, str. 31-81
194. Smokvina, R. (2016). Industrie 4.0.-primena interneta stvari u industriji, *Open Infotrend*, Vol. 5, No.202, p. 30-34
195. Snow, C.C., Miles, R.E., Coleman, H.j., (1992). Managing the 21st Century Network Organization, *Organizational Dynamics*, 21 (1), Winter 1992, pp. 5-20.
196. Socher, R., (2018). Interview with Chief Scientist at Salesforce: Dr. Richard Socher, December 27th 2018
197. Sofronijević A, Milićević V, & Ilić B. (2014). Smart City as Framework for Creating Competitive Advantages in International Business Management, *Management*, 71, 5-15.
198. Sofronijević, A., Milićević, V., Ilić, B., (2017). Strategijski pristup digitalnoj transformaciji poslovanja, *Tehnika –menadžment*, 67, 2
199. Soja, P., Cunha, P.R. (2015). ICT in Transition Economies: Narrowing the Research Gap to Developed Countries, *Information Technology for Development*, 21(3), 323-329.

200. Soleša, D., Černetič M., Gerlič I., (2007). New Media in Education, Selected topics, University of Novi Sad - Faculty of Education in Sombor, Faculty for Organizational Sciences in Kranj and University of Maribor - Faculty of Education Maribor, pg. 218.
201. Solesa, D., Juričić, V., Raisman, M. (2014). Web 2.0 as a potential for development of young people, Technical Gazette 21(6), 1403-1409.
202. Solesa, D., Mateljan, V., Juricic, V. (2012). Developing curriculum for the “Information technology” study programme, Technics Technologies Education Management, 7(4), 1561- 1567.
203. Solesa, D., Solesa-Grijak, Đ. & Kojic, N. (2014). New Teaching Methods Applied In Computer Science Teaching. Proceedings of the IADIS International Conference Interfaces and Human Computer Interaction. Lisbon, Portugal, pp. 69-75.
204. Spremić M., Metode provedbe revizije informacijskih sustava (2007)., UDK 007:65.012.16
205. Spremić, M. (2005.) Procjena razine pouzdanosti internih kontrola informacijskog sustava s pomoću CobiT metodologije, Revizija, računovodstvo i financije, br. 12/2005, str. 126-134.
206. Spremić, M., Strugar, I., (2002.) Strategic Information System Planning in Croatia: Organizational and Managerial Challenges, International Journal of Accounting Information Systems, Vol. 3, Num. 3, pp. 183-200.
207. Spremić, M. (2005.) Managing IT risks by implementing information system audit function, Proceedings of the 3rd International Workshop in Wireless Security Technologies, Westminster University, London, 04-05.04.2005, pp. 58-64.
208. Spremić, M. (2012). Measuring IT Governance Performance: A Research Study on CobiT- Based Regulation Framework Usage, International journal of Mathematics and Computers
209. Spremić, M., (2002). Barriers to Effective Management of Information Technology Projects in Croatia, Proceedings of Abstracts of the 2nd SENET Conference on Project Management, Cavtat, 2002, pp. 309-317.
210. Spremić, M., Hlupić, V., (2007). E-Commerce in Croatia, Information Technology for Development, Vol. 13, Num.4., pp.391-409

211. Sria, V., Spremic, M., (2000.): Informacijskom tehnologijom do poslovnog uspjeha, Sinergija.
212. Stigter, E.,J., (2019) Microsoft's new quantum computing lab in Delft opens its doors to a world of possibilities, Microsoft, 21.02.2019.
213. Stojanović D., Digitalna ekonomija i transformacija poslovnih procesa – izazovi i rizici, UDK: 339:004.738.5 Datum prijema rada: 09.02.2017. Datum korekcije rada: 27.02.2017. Datum prihvatanja rada: 13.03.2017. Ekonomija teorija i praksa, str.86
214. Symons, C., (2005). IT Governance Framework: Structures, Processes and Framework, Forrester Research, Inc.
215. Tapscott, D., Ticoll, D., Lowy, A., Digital Capital: Harnessing the Power of Business Webs, Harvard Business School Press, Boston, 2000, str. 7.
216. Tasoglu, S., & Demirci, U. (2013). Bioprinting for stem cell research. Trends in biotechnology, 31(1), 10–19. doi:10.1016/j.tibtech.2012.10.005
217. The “Smart Factory” of the Fourth Industrial Revolution: An Interview with Fraunhofer's Thomas Bauernhansl, (2016). TOP500 News Team, May 30
218. The business model canvas, Business Model Alchemist, <http://businessmodelalchemist.com/>
219. The Digital Economy and Society Index (DESI) for 2018, European Commission
220. Urošević, V. (2009). Nigerijska prevara u Republici Srbiji, Bezbednost, Br. 3/2009, godina LI, Beograd
221. Varian, H. (2016). Intelligent Technology, Finance and Development, vol. 53, pp.7
222. Vidas Bubanja, M., Bubanja, I., (2017). The Challenge of Going Digital, Journal of engineering management and competitiveness (jemc), vol. 7, no. 2, 126-136,
223. Violino, What is Big Data Analytics, Everything you need to know, InfoWorld, January 2018
224. Visualizing the Social Media Universe in 2018, WEF, august 17th, 2018
225. Vujović, Internet ogledalo 2015, pp.59
226. Vujović; B., Digitalna disrupcija i kako se odbraniti, Internet ogledalo, 2017, pp. 62
227. Wallace, P., (2015). The Psychology of the Internet, Cambridge University Press, Cambridge.
228. Wavestone Global Survey on Deep Tech Investments, (2017). 24-25

229. Weber, R., Behavioral economics, (2005.), The handbook of economic sociology, pp.91-108
230. Weill, P., Ross, J.W. (2004). IT Governance: How Top Performers Manage IT Decision.
231. Westerman G, & Bonnet D., (2015). Revamping your business through digital transformation. MIT Sloan Management Review, 56(3), 10.
232. Westerman G, Bonnet D, & McAfee, A., (2014). Leading digital: Turning technology into business transformation. Harvard Business Press.
233. Westerman, G., Tannou, M., Bonnet, D., Ferraris, P., & McAfee, A. (2012). The Digital Advantage: How Digital Leaders Outperform their Peers in Every Industry, MIT Center for Digital Business and Capgemini Consulting
234. What matters in the boardroom – director and investors views on trends shaping governance and the board of the future (2014). PricewaterhouseCoopers
235. Wisniewski, J., (2016). WikiLeaks and Whistleblowing: Privacy and Consent in an Age of Digital Surveillance, in: Ethics and the Future of Spying: Technology, National Security and Technology, National Security and Intelligence Collection, Routledge, New York/London.
236. Wohlers Associates Report, 2019, ISBN 978-0-9913332-5-7
237. Wolf, D. (2003). Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development, National Security Agency US, July 22, 2003
238. Wong, W. P., Tseng, M.-L., & Tan, K. H. (2014). A business process management capabilities perspective on organisation performance. Total Quality Management & Business Excellence, 25(5-6), 602-617.
239. World Economic Forum (2016). Digital Transformation of Industries: Digital Enterprise, World Economic Forum White Paper
240. Wright, K. B., Abendschein, B., Wombacher, K., O'Connor, M., Hoffman, M., Dempsey, M., Shelton, A. (2014). Work-related communication technology use outside of regular work hours and work life conflict: The influence of communication technologies on perceived work life conflict, burnout, job satisfaction, and turnover intentions, Management Communication Quarterly, 28(4), 507-530.

241. Xinwen Fu, Zhen Ling, Wei Yu, Junzhou Luo, (2010). Cyber Crime Scene Investigations (C2SI) through Cloud Computing, 2010 IEEE 30th International Conference on Distributed Computing Systems Workshops.
242. Yeu-Pong, L., Po-Lun, H., Using the vulnerability information of computer systems to improve the network security, Department of Computer Science and Information Engineering, Chung Cheng Institute of Technology, National Defense University, Tauyuan 33509, Taiwan, ROC, Received 20 September 2006; received in revised form 7 March 2007; accepted 8 March 2007
243. Zakon o informacionoj bezbednosti, „Sl.glasnik RS“, 6/2016i 94/2017
244. Zakon o potvrđivanju konvencije o visokotehnološkom kriminalu, "Sl. glasnik RS - Međunarodni ugovori", br. 19/2009

Elektronski izvori:

<http://www.seecult.org/vest/sajber-nebezbednost>

<https://www.propia.se/files/Examensarbeten/rapport.pdf>

<https://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education>

<https://scindeks-clanci.ceon.rs/data/pdf/2217-5458/2017/2217-54581701080S.pdf>

<http://oneal.research.ucf.edu/entrepreneurship.html>

http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

<https://www.automatika.rs/vesti/iot/baidu-i-xiaomi-rade-na-zajednickom-razvoju-tehnologija-kao-sto-su-iot-i-vestacka-inteligencija.html>

<http://www.erazvoj.com/index-mi-gradimo-poslovne-veze.html>

<http://www.ekfak.kg.ac.rs/images/Nir/InstitucionalnePromene/InstitucionalnePromene2017.pdf>

<http://www.ekof.bg.ac.rs/wp-content/uploads/2015/09/Ek-Ideje-i-Praksa-25.pdf>

http://www.iteo.rs.ba/sites/default/files/ITeO_2015_zbornik.pdf

<https://scindeks-clanci.ceon.rs/data/pdf/2334-9638/2017/2334-96381702126V.pdf>

<https://www.iserbia.rs/biznis-i-edukacija/cetvrta-industrijska-revolucija-4716>

https://www.academia.edu/38697343/Technology_innovation_and_competitiveness_in_the_globalized_economy_in_Serbian

<http://www.ekfak.kg.ac.rs/images/Nir/ProjekatFakulteta/Zbornik2019->

<Ekonomski%20efekti%20tranzicije%20i%20restrukturiranja%20privrede%20Srbije%20u%20funkciji%20Oevropskih%20integracija.pdf>

http://www.infodom.hr/UserDocsImages/Inicijativa_Digitalna%20transformacija%20gospodarstva%202016_2020.pdf

http://darhiv.ffzg.unizg.hr/id/eprint/5064/1/KocijanK_BigData.pdf

<https://www.bizlife.rs/lifestyle/afterhour/koliko-novca-ce-biti-utroseno-na-internet-stvari-u-narednih-pet-godina/>

<https://www.businessinsider.fr/intelligence/the-internet-of-things-2019-how-the-iot-continues-to-transform-business-homes-and-cities-through-next-generation-digital-solutions-510>

<https://pcpress.rs/Business-IT/PCPress-Business-and-IT.pdf>

<https://samoobrazovanje.rs/sta-je-internet-of-things-internet-inteligentnih-uredjaja/>

<https://repozitorij.etfos.hr/islandora/object/etfos:2040/preview>

https://raf.edu.rs/docs/Diplomski_radovi/Miroslav-Djuricic_Evolucija-Profila-Korisnika-Veba.pdf

<https://future.internetsociety.org/2019/wp-content/uploads/sites/2/2019/04/InternetSociety-GlobalInternetReport-ConsolidationintheInternetEconomy.pdf>

https://www.norips.org/uploads/1/4/6/3/14634014/prezentacija_biljana_simic.pdf

http://www.sattelevizija.com/vesti/jedna_vest/racunarstvo_u_oblacima_cloud_computing_17127144458

<file:///C:/Users/Petar/Downloads/MR%20-%20Tehnologija%20Cloud%20computing-a.pdf>

<file:///C:/Users/Petar/Downloads/7-16-PB.pdf>

https://www.blic.rs/vesti/svet/roboti-ce-do-2030-izbrisati-20-miliona-radnih-mesta/d10xhkr?utm_source=blic_kat_it_sidebar&utm_medium=sidebar_najnovije_info

https://www.b92.net/biz/vesti/svet.php?yyyy=2019&mm=06&dd=22&nav_id=1557682

http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2017-3/69-2017-3-00-Ceo_broj_VD.pdf

http://www.iteo.rs.ba/sites/default/files/ITeO_Zbornik_radova_2017.pdf

<https://srbodroid.com/nezvanicno/moj-stav/nosiva-tehnologija-i-grupno-finansiranje-iliti-wearables-crowdfunding/>

<file:///C:/Users/Petar/Downloads/489-Article%20Text-1077-1-10-20171023.pdf>

<http://www.ftn.uns.ac.rs/n2144512288/disertacija>

<https://www.datalab.rs/elektronsko-poslovanje-kako-sta-gde/>

<https://www.hgk.hr/documents/hgk-industrija-4058d8c59722f1e.pdf>

<http://old.bos.rs/materijali/aspekti.pdf>

<https://www.iserbia.rs/biznis-i-edukacija/cetvrta-industrijska-revolucija-4716>

<http://mbs.edu.rs/wp-content/uploads/2016/07/US-Preduzetnistvo-i-menadzment-malih-i-srednjih-preduzeca.pdf>

[https://www.google.com/search?num=15&as_qdr=all&q=/+Izvor:+Deloitte+\(2015\)+Industry+4.0&tbm=isch&source=univ&sa=X&ved=2ahUKEwji6Y7QuZDjAhVisosKHYIuAGAQsAR6BAgMEAE](https://www.google.com/search?num=15&as_qdr=all&q=/+Izvor:+Deloitte+(2015)+Industry+4.0&tbm=isch&source=univ&sa=X&ved=2ahUKEwji6Y7QuZDjAhVisosKHYIuAGAQsAR6BAgMEAE)

<https://www.ictbusiness.info/kolumne/sto-nam-donosi-digitalna-transformacija>

<https://pcpress.rs/industrija-4-0-i-buducnost/>

<https://naslovi.net/search.php?q=tehnologija+internet+tehnologije&start=401>

<http://www.indmanager.edu.rs/site1/images/037rs/pdf/Zbornik%20radova%20TuP2017.pdf>

<https://samoobrazovanje.rs/cetvrta-industrijska-revolucija-sta-to-znaci-i-kako-da-se-postavimo/>

<https://elab.fon.bg.ac.rs/udzbenik-internet-inteligentnih-uredaja/pametni-gradovi/>

<file:///C:/Users/Petar/Downloads/US%20-%20Upravljanje%20prodajom%20-%202018.pdf>

<https://proprium.hr/pametni-gradovi/>

<https://www.istokpavlovic.com/blog/konacno-jednostavno-objasnjenje-sta-je-blockchain-bitcoin-majnovanje-i-kriptovalute/>

<https://www.securitysee.com/2018/06/industrija-4-0-dolazak-na-srpsko-trziste/>

<http://www.nspm.rs/hronika/rts-pad-nekadasnjeg-japanskog-giganta-%E2%80%93-u-tosibinim-fabrikama-se-sad-uzgaja-salata-i-spanac.html?alphabet=l>

<http://er-singidunum.blogspot.com/2014/03/sajber-fizicki-sistemi-svet-inovacija.html>

<https://vesti.mas.bg.ac.rs/?p=9100&lang=lat>

<https://www.industrija.rs/uploads/pdf/broj54/files/assets/common/downloads/publication.pdf>

<http://www.noviekonomist.info/pdf/ekonomist%2015%20-%20final.pdf>

<https://www.vreme.com/cms/view.php?id=1370434>

<https://www.vreme.com/cms/view.php?id=1370434&print=yes>

<http://www.projektura.org/blog/2015/03/digitalna-ekonomija-nesto-poznato-na-pomalo-drugaciji-nacin-hr/>

file:///C:/Users/Petar/Downloads/Zloupotreba%20IT%20u%20svrhe%20korupcije_SER_BIH_MN.pdf

https://masmi.rs/wp-content/uploads/2016/11/E-business-vesti_MASMI.pdf

<http://www.fefa.edu.rs/ekonomija-kako-opstati-u-svetu-digitalizacije/381112600080/>

http://www.deb.org.rs/wp-content/uploads/2015/05/Ekonomski-vidici-2-3_2015.pdf

https://www.ratel.rs/upload/documents/Pregled_trzista/RATEL%20-%20Pregled%20trzista%20u%202015.pdf

<https://www.insead.edu/news/2018-gtci-talent-diversity-competitiveness-fuel-future-of-work>

<http://www.eraozvoj.com/index-mi-gradimo-poslovne-veze.html>

https://www.google.com/search?num=15&as_qdr=all&q=U+tom+pogledu,+utvr%20%91en+je+i+redosled+koraka:+Povecati+stopu+digitalne+transformacije+industrije-+tj.&spell=1&sa=X&ved=0ahUKEwio57eG6pDjAhXV8qYKHSerAfUQBQgwKAA

<https://positive.rs/resursi/bits-koncept/digitalna-transformacija/>

<http://wwwold.saga.rs/proizvodi-resenja/digitaltransformation.html>

<https://www.webizrada.com/blog/digitalna-transformacija-poslovanja>

https://www.researchgate.net/profile/Dusan_Regodic/publication/321474270_Sinergija_arhitekture_organizacije_i_upravljanja_poslovnim_procesima_Synergy_of_architecture_architecture_and_business_process_management/links/5a22a7d7aca2727dd87c86e3/Sinergija-arhitekture-organizacije-i-upravljanja-poslovnim-procesima-Synergy-of-architecture-architecture-and-business-process-management.pdf

<http://www.ftn.kg.ac.rs/konferencije/rppo13/Monografije/IKT%20U%20MENADZMENTU.pdf>

<http://www.tfzr.uns.ac.rs/Content/files/0/DOKTORSKA%20DISERTACIJA%20Milena%20Cvjetkovic.pdf>

http://www.dgt.uns.ac.rs/download/us_interna_kontrola_revizija.pdf

http://www.odbrana.mod.gov.rs/odbrana-stari/vojni_casopisi/arhiva/VD_2017-7/69-2017-7-00-Ceo_broj_VD.pdf

http://ecesm.net/sites/default/files/DEV_1.1_ME.pdf

<http://nardus.mpn.gov.rs/bitstream/handle/123456789/3064/Disertacija.pdf?sequence=1&isAllowed=y>

http://www.fbim.meste.org/fbim_srpski/FBIM_Najava_clanaka_srp.html

<https://www.osce.org/sr/serbia/272206?download=true>

<http://blog.erazvoj.com/?p=35410>

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=11&ved=2ahUKEwjgsv7i8aDjAhUhxKYKHbjcANYQFjAKegQIDRAC&url=https%3A%2F%2Fsingipedia.singidunum.ac.rs%2Fpreuzmi%2F41381-primena-crm-a-i-unapredjenje-elektronskog-bankarstva-u-cilju-povecanja-zadovoljstva-klijenata-banca-intesa%2F1460&usg=AOvVaw3LjeQ1Kbp7vgjygxtxMOY0>

<http://www.youtube.com/watch?v=AciORQ2CXFs>

<http://edukacija.rs/poslovne-vestine/marketing/pest-analiza>

http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

<https://dustinstout.com/social-media-statistics/>

<https://www.weforum.org/agenda/2018/08/visualizing-the-social-media-universe-in-2018>

<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>