DIGITALIZACIJA INTEGRISANOG UPRAVLJANJA PANDEMIJSKIM RIZICIMA U SVJETLU ZAŠTITE LJUDSKIH PRAVA I GDPR DIREKTIVE

DIGITIZATION OF THE INTEGRATED PANDEMIC RISK MANAGEMENT IN THE LIGHT OF HUMAN RIGHTS PROTECTION AND THE GDPR DIRECTIVE

Pregledni naučni rad

Dr. sc. Edin Garaplija [*]
Emina Garaplija[*]*, bcc. ecc.*

Sažetak

Globalna pandemija uzrokovane virusom Covid-19 (Korona) je reprezentativni rizik današnjice. Po prvi put u istoriji čovječanstva, sve države Svijeta su jedinstvene u zajedničkom odgovoru ne ovu "modernu pošast", prije svega zbog angažmana Svjetske zdravstvene organizacije (WHO), koja je propisala preporuke mjera odgovora na pandemiju za sve zemlje svoje članice 193 zemlje članice, ali i globalne digitalne razmjene informacija putem mnogobrojnih softvera i društvenih internet mreža. Potreba za opštom digitalizacijom podataka pomoću geografskih informacionih sistema i baza podataka (GIS), otvorio je i druga pitanja, koja se prije svega odnose na zaštitu ljudskih prava i zaštitu ličnih podataka, koji se u interesu javnog zdravlja razmjenjuju među mnogobrojnim korisnicima. Dvije su osnovne upravno-pravne norme na koje se trebamo referisati kod proučavanja ovog fenomena. Prva je Opća deklaracija UN o ljudskim pravima (1948), koja je bila baza za uspostavljanje Evropske Konvencije o zaštiti ljudskih prava i temeljnih sloboda (1950). A druga, Opšta Uredba o zaštiti podataka (GDPR), koja je od 2018. postala obavezujuća za sve države članice EU, ali je i preporuka zemljama kandidatima i potencijalnim kandidatima za članstvo u EU. Ovaj rad daje odgovore i preporuke na zahtjeve za usklađivanje digitalnog upravljanja

[*] *Edin Garaplija, Predsjednik Naučnog savjeta INZA Group, član Naučnoistraživačkog vijeća Asocijacije za upravljanje rizicima AZUR. E-mail: edin.garaplija@inzagroup.eu, edin.garaplija@azur.ba,*

[*] *Emina Garaplija, viši asistent za upravljanje projektima, Asocijacija za upravljanje rizicima u Bosna i Hercegovina. E-mail: emina.garaplija@azur.ba,*

rizičnim podacima, sa univerzalnom obavezom za zaštitu ljudskih prava i zaštitom ličnih podataka od zloupotreba.

Ključne riječi: Pandemija, GIS, ljudska prava, GDPR.

Abstract

The global pandemic, caused by the Covid-19 virus (Corona) is undoubtedly the first representative risk of Today. For the first time in human history, all countries of the World are united in a common response on to this "modern plague", primarily due to the engagement of the World Health Organization (WHO), which prescribed recommendations measures for pandemic response, to all of its 193 member countries, but also due to the global digital exchange of information through numerous software & social internet networks. General digitization of data using geographic information systems & databases (GIS), has opened other issues, primarily related to the protection of human rights & personal data that are exchanged among many stakeholders in the interest of public health. There are two basic administrative & legal norms that we should refer to when research this phenomenon. The first norm is the UN Universal Declaration of Human Rights (1948), which was the basis for establishment of the European Convention for the Protection of Human Rights & Fundamental Freedoms (1950). And the second is the General Data Protection Regulation (GDPR), which became binding on all EU member states, but is also a recommendation to candidate & potential candidate countries for EU membership. This paper provides answers and recommendations to the requirements for harmonization of digital data risk management, with the universal obligation to protect human rights & protect personal data from misuse.

Key words: Pandemic, GIS, Human rights, GDPR.

1. UVOD

Svjetska zdravstvena kriza uzrokovana pojavom smrtonosnog virusa COVID-19 koja je pogodilo cjelokupno čovječanstvo, pokazala je sve slabosti dosadašnjeg pristupa zaštiti života i zdravlja ljudi, njihove imovine i životne sredine. Zdravstvo se pokazalo kao jedna od najranjivijih društvenih

infrastruktura, kojoj su hitno potrebni efikasniji i inovativniji pristupi u upravljanju podacima i rješavanju kriza. Prema zvaničnim podacima Svjetske zdravstvene organizacije (World Health Organisation – WHO), pandemija je počela u Kini krajem 2019. godine, gdje je do sada djelimično poznati i vakcinama kontrolisani virus „SARS“, koji je u obliku „svinjske“ i „ptičije“ gripe ranijih desetljeća pogađao veliki broj zemalja, mutirao u do sada nepoznati oblik, sa višestruko težim i smrtonosnijim posljedicama po živote i zdravlje ljudi. Zahvaljujući tome što je Kina u poslednjem desetljeću postala svjetski trgovinski epicentar, koji je pomoću zračnih i prekookeanskih logističkih lanaca povezan sa svim dijelovima Svijeta, ali i opštoj nepoznanici vrste, karakteristika i jačine virusa, ova „pošast“ se munjevito proširila po Evropi i Sjevernoj Americi, da bi se nešto kasnije slučajevi zaraze pojavili i na ostalim kontinentima. Svjetska zdravstvena organizacija je na proljeće 2020. proglasila globalnu svjetsku pandemiju uzrokovanu virusom Covid-19. Prema podacima WHO, objavljenim na njihovom zvaničnom web portalu, na dan 29. oktobra 2021.godine, nešto više od godinu i pol dana nakon potvrđenih prvih slučajeva pozitivnih na ovaj virus, Svijet je brojao preko 245 miliona zaraženih, skoro 5 miliona smrtnih slučajeva i preko 6.8 milijardi primljenih doza vakcina protiv Covida 19. Poprilično mlaka i neuvjerljiva prvobitna reakcija WHO, čiji su najveći finansijeri SAD i Kina, doprinijela je početnoj zbunjenosti na globalnom nivou, u pogledu primjene integrisanih mjera zaštite i spašavanja. Brzina širenja virusa koja je iznenađujuće pogodila sve zemlje Svijeta, pokazala je nepripremljenost šire društvene zajednice koja se suočila sa ovim najznačajnijim milenijumskim iskušenjem. Pred svjetsku naučnu i stručnu javnost, nametnula su se brojna pitanja u cilju identifikacije, analize i vrednovanja rezultata do kojih se došlo i dolazilo u proteklim godinama, kada je u pitanju način, sredstva, principi i taktike upravljanja rizicima. Teorijska načela su se sukobila sa praktičnim. Scenariji rizika koji su razvijani u procjenama ugroženosti pojedinačno za najrazvijenije zemlje Svijeta i njihovo društveno-političko uređenje, pokazali su se neefikasnim u pogledu procjene i primjene mjera preventivne zaštite, a posebno brzog odgovora na vanredne situacije i novonastalu pandemijsku krizu. Nacionalne procjene i planovi, koji su predvidjeli ovakve vrste rizika, su se ograničili na svoje teritorije, zanemarujući i zaboravljajući lance nabavki i transporta koji u uslovima globalne pandemije postaju prioritetna vitalna kritična infrastruktura (KI). Kritična infrastruktura ne smije ni pod koju cijenu biti prekinuta, jer mnoge zemlje Svijeta, pa i one najrazvijenije, nisu u mogućnosti da samostalno

opstaju kada je u pitanju proizvodnja hrane, opreme i lijekova za zaštitu i zdravlje stanovništva. Svjetska pandemija je pokrenula globalni mehanizam kriznog upravljanja, koji je podrazumijevao centralizaciju i mapiranje prikupljenih podataka vezanih za broj oboljelih, smrtnost a kasnije i vakcinaciju, te izdavanje globalnih zdravstvenih uputstava i procedura za prevenciju i postupanje u borbi protiv „korona virusa“. Međutim, prema mišljenju autora ovog teksta, bar u prvim mjesecima odgovora na ove izazove ovaj „mehanizam je zaškripao u svojoj implementaciji i njegovi zupčanici su se poprilično sporo pokrenuli, te je postalo evidentno da ih pod hitno treba podmazati novim pristupima u rješavanju ove i sličnih kriza koje nas očekuju u skoroj budućnosti.“ Ako se uzme podatak da su u bazama podataka širom planete pohranjene lične informacije miliona ili čak milijardi stanovnika, koje su izložene svakodnevnim prijetnjama od unutrašnjih i vanjskih zloupotreba, onda možemo zaključiti da će posljedice ove krize zahvatiti ne samo zdravstvene i ekonomske aspekte pojedinca, već i njihova temeljna ljudska prava i slobode.

Potreba za opštom digitalizacijom podataka pomoću geografskih informacionih sistema i baza podataka (GIS), otvorio je i druga pitanja, koja se prije svega odnose na zaštitu ljudskih prava i zaštitu ličnih podataka, koji se u interesu javnog zdravlja razmjenjuju među mnogobrojnim korisnicima. Dvije su osnovne upravno-pravne norme na koje se trebamo referisati kod proučavanja ovog fenomena. Prva norma je Opća deklaracija UN o ljudskim pravima (1948), koja je bila baza za uspostavljanje Evropske Konvencije o zaštiti ljudskih prava i temeljnih sloboda (1950). A druga je Opšta Uredba o zaštiti podataka (GDPR), koja je od 2018. postala obavezujuća za sve države članice EU, ali je i preporuka zemljama kandidatima i potencijalnim kandidatima za članstvo u EU. Ovaj rad daje odgovore i preporuke na zahtjeve za usklađivanje digitalnog upravljanja rizičnim podacima, sa univerzalnom obavezom za zaštitu ljudskih prava i zaštitom ličnih podataka od zloupotreba.

Slika 1: grafički prikaz WHO zvaničnih informacija u GIS bazi

2. MEĐUNARODNE NORME ZA MAPIRANJE PODATAKA U GIS-U

Uspostava digitalnog modela integrisanog upravljanja rizicima, prati slijed globalnih trendova i procesa za provedbu efikasnijih strateških i operativnih politika u sistemima nacionalne sigurnosti. Ovakvim modelom ne samo da zadovoljavamo visoke međunarodne standarde u oblasti sigurnosnih politika, već preventivno unapređujemo postojeće sisteme zaštite. Za uspješnu uspostavu digitalnog modela, potrebno je najprije razumjeti terminološke pojmove jednog ovako složenog procesa, te sistematski izanalizirati uzroke, posljedice i preventivno-operativne mjere zaštite. Sam digitalni model nam daje odgovore na raznovrsna pitanja i dileme oko izbora najefikasnijeg pravca uspostave integrisanog sistema zaštite savremenih društava. Evropskim smjernicama za procjenjivanje rizika se zahtijeva digitalizacija podataka, odnosno mapiranje procjena rizika u geo-referentnim sistemima i bazama podataka (GIS). Mapiranje obuhvata mape rizika, mape uticaja na stanovništvo, ekonomiju i kritičnu infrastrukturu, te mape kapaciteta odgovora, uključujući javni, privatni i NVO sektor. Glavni izazovi za budućnost razvijanja procjenjivanja rizika i mapiranje su:

- digitalizacija geografskih informacija (vektorski podaci, prostorna rezolucija, GLS-podaci);
- uključivanje više događaja i uticaja (npr. uključujući uticaj na ekosisteme ili manje događaje, odnosno događaje koji su ispod nivoa

praga baza podataka koje se odnose na globalne katastrofe koje se trenutno koriste);

- poboljšane i standardizovane definicije i terminologija za ekonomske gubitke i/ili troškove oštećenja (npr. uključujući i troškove obnove), ugroženih ljudi, itd;
- više podataka dostupnih javnosti; validacija podataka koji se odnose na konkretnu i ocjena kvaliteta/kontrola kvaliteta u cjelini; usklađivanje metodologije, podataka i modela podataka.

Geografski informativni sistem (GIS), je okvir za prikupljanje, upravljanje i analizu podataka. Ukorijenjen u nauci o geografiji, GIS integrira mnoge vrste podataka. Analizira prostornu lokaciju i organizira slojeve informacija u vizualizacije pomoću mapa i 3D scena. Pomoću ove jedinstvene mogućnosti GIS otkriva dublji uvid u podatke, poput obrazaca, odnosa i situacija, pomažući korisnicima da donose pametnije odluke. GIS predstavlja osnovni alat za mapiranje rizika, na globalnom svjetskom nivou, koji je nastao 60-tih godina, za potrebe višeslojnog upravljanja prostornim podacima i njihovim pridruženim osobinama (atributima). Ovaj inovacioni odgovor za kolektovanje, upravljanje i vrednovanje podataka, u svojim fazama razvoja naišao je pored informaciono-tehničkih i na izazove zaštite i funkcionalnog upravljanja podacima o rizicima, uticajima i kapacitetima snaga. Ovaj alat nam daju i mogućnosti vizualizacije putem preciznog mapiranja georeferentnih podataka. Pomoću njih generišemo nivo transparentnosti informacije o ranom upozorenju na rizike, te omogućavamo funkcionalan pregled angažovanosti svih zainteresovanih učesnika u sistemu zaštite i spašavanja. Integracija akcija procjenjivanja i mapiranja rizika, doprinosi donošenju preciznijih, odlučnijih i efikasnijih odluka o prioritetima postupanja, te se pristupa najtežim rizicima sa odgovarajućim mjerama prevencije i pripravnosti. U generalnom smislu GIS predstavlja računalni sistem sposoban za integrisanje, spremanje, uređivanje, analiziranje i prikazivanje geografskih informacija. U specifičnom smislu, GIS predstavlja "pametne karte", koje svojim korisnicima dopuštaju stvaranje interaktivnih upitnika (istraživanja koja stvara korisnik), analiziranje prostornih informacija i uređivanje podataka, preciziranih u prostoru (Garaplija, 2018).

Uspostava georeferentnih baza podataka, podrazumijevamo uspostavljanje sistema identifikacije, analize i vrednovanja podataka, usklađenog sa INSPIRE direktivom za digitalizaciju podataka i EUROSTAT

klasifikacijom i kategorizacijom. Mapiraju se uticaji rizika na ljude, imovinu i životnu sredinu, te podataka o kapacitetima integrisanih službi i mjera zaštite. Pri kolektovanju podataka treba slijediti Evropske smjernice za procjenjivanje rizika od katastrofa izazvanih klimatskim promjenama ili ljudskim nemarom i namjerom, kojima se preporučuju slijedeće mape:

(1) Mape koje prikazuju očekivani prostorni raspored glavnih opasnosti. Različite opasnosti i intenziteti treba da budu predstavljeni u odvojenim podlogama (eng. „layer).
(2) Mape uticaja koje pokazuju prostornu distribuciju svih relevantnih elemenata koji treba da budu zaštićeni (škole, bolnice, javna dobra, mjesta masovnih okupljanja, infrastruktura, prirodno zaštićena područja i sl.)
(3) Mape kapaciteta, koje daju skupine podataka o brojnosti i materijalnim resursima snaga za suprotstavljanje izazovima i posljedicama od katastrofa.

Procjene nacionalnih rizika trebaju sadržavati zahtjeve zakonodavstva EU o uporedivosti i interoperabilnosti podataka. U skladu sa INSPIRE direktivom*, forme podataka predstavljaju osnovu Pravilnika o implementaciji koji definiše niz tehničkih aranžmana za interoperabilnost i harmonizaciju setova prostornih podataka u vezi sa temama navedenim u Aneksu II i III Direktive INSPIRE. Pravilnik o implementaciji usvojen u velikom broju specifičnih oblasti (meta-podaci, specifikacije podataka, mrežni servisi, objavljivanje podataka i usluga i praćenje i izvještavanje) pomoći će da se osigura da prostorne infrastrukture podataka koji se razvijaju u državama članicama doprinesu poboljšanju upotrebljivosti nacionalnih podataka potrebnih za procjenu rizika. Evidentni su međunarodni napori da se razviju globalni uporedivi informacioni sistemi razvijeni na međunarodnom nivou, kao što su GIS platforme za praćenje rizika od katastrofa, ili CRED* platforma razvijena od strane reosiguravajućih društava (Europe RE, Munich Re, Swiss Re). Velika količina mapiranih informacija predstavljaju osjetljive službene ali i lične podatke, koje treba pravilno zaštiti od mogućih zloupotreba i pristupati

---

* *INSPIRE direktiva je definisala infrastrukturu važnih informacija u Evropi, https://inspire.ec.europa.eu/about-inspire/563#*

* *CRED (Center for research epideiology of disasters) – istraživački centar uspostavljen od Evropa RE*

sa posebnim senzibilitetom kako se ne bi ugrozile osnovne ljudske slobode i prava.

3. LJUDSKA PRAVA I PRIMJENA GDPR DIREKTIVE ZA ZAŠTITU LIČNIH PODATAKA

Ovim radom se želimo osvrnuti na potencijalno kršenje ljudskih prava i zaštitu podataka koje građani pohranjuju u zdravstvenim bazama podataka, nipošto ne ulazeći u rasprave o potencijalnom narušavanju ljudskih prava u procesu vakcinacije stanovništva od virusa COVID 19, koja se provodi širom Svijeta u skladu sa preporukama Svjetske zdravstvene organizacije. Ipak, u cilju suzbijanja epidemije, od njenog samog početka pa do neke završne faze imunizacije stanovništva, evidentno je da različite ustanove i organizacije svakodnevno kolektuju lične podatke o milionima, pa i milijardama stanovnika širom Svijeta. Da li se svi učesnici u ovome procesu pridržavaju obaveza zaštite ličnih podataka i temeljnih ljudskih sloboda, da li su preuzeti lični podatci pravilno pohranjeni u bazama podataka i da li su sigurni od zlonamjernih „cyber napada, pitanja su koje sve više zaokupljaju stručnjake širom planete.

Zaštita osobnih podataka i poštovanje privatnoga života spadaju u temeljna evropska prava i slobode (Selimić, 2018). Evropski parlament oduvijek se zalaže za uspostavu ravnoteže između jačanja sigurnosti i zaštite ljudskih prava, uključujući zaštitu podataka i privatnosti. U maju 2018. na snagu su stupili novi evropski propisi o zaštiti podataka, kojima se jačaju prava građana i pojednostavljuju pravila za poduzeća u digitalnom dobu. Evropska unija jamči dosljednu primjenu temeljnog prava na zaštitu podataka, ugrađenog u Povelju EU-a o temeljnim pravima. Također, zauzima i čvršće stajalište o zaštiti osobnih podataka u svim svojim politikama, uključujući provedbu zakona i sprečavanje zločina, te u međunarodnim odnosima, što je posebno važno u globalnom društvu u kojem se tehnološke promjene odvijaju velikom brzinom. Prije nego što je Ugovor iz Lisabona stupio na snagu, zakonodavstvo o zaštiti podataka u području slobode, sigurnosti i pravde bilo je podijeljeno između prvoga stupa (zaštita podataka za privatne i komercijalne potrebe uz primjenu postupka Zajednice) i trećega stupa (zaštita podataka za potrebe provedbe zakona na međuvladinoj razini), zbog čega su se postupci odlučivanja u ta dva područja odvijali prema različitim pravilima. Ugovorom iz Lisabona ukinut je ustroj po stupovima i stvorena čvršća osnova za razvoj

jasnijeg i efikasnijeg sistema zaštite podataka. Istovremeno je Parlament, kao novi suzakonodavac, stekao nove ovlasti. Članom 16. Ugovora o funkcioniranju Europske unije omogućuje se da pri provedbi aktivnosti na koje se primjenjuje pravo Unije, Parlament i Vijeće određuju propise o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije, te u državama članicama. Nakon programa iz Tamperea (iz septembra 1999.) i Haškog programa (iz studenog 2004.), Europsko je vijeće u prosincu 2009. odobrilo višegodišnji program u području slobode, sigurnosti i pravde za razdoblje od 2010. do 2014., poznat kao „Stockholmski program". U svojim je zaključcima iz jula 2014. Europsko vijeće definiralo strateške smjernice za predstojeće godine, koje se odnose na zakonodavno i operativno planiranje u području slobode, sigurnosti i pravde, u skladu s člankom 68. UFEU-a. Jedan od glavnih ciljeva je bolja zaštita osobnih podataka u Evropskoj uniji.

Poveljom Evropske unije o temeljnim pravima, poštovanje privatnoga života i zaštita osobnih podataka, navedeni su u članovima 7. i 8. kao usko povezana, ali zasebna temeljna prava. Ako gledamo automatizaciju obrade osobnih podataka, Konvencija za zaštitu osoba Vijeća Evrope broj 108, od 28. siječnja 1981., bila je prvi pravno obvezujući međunarodni instrument donesen u području zaštite podataka. Njena je svrha svakoj fizičkoj osobi osigurati poštovanje prava i temeljnih sloboda, a osobito pravo na privatnost u pogledu automatizovane obrade osobnih podataka koji se na nju odnose. Protokolom o izmjeni te konvencije nastojalo se proširiti njeno područje primjene, povećati nivo zaštite podataka i poboljšati efikasnost. Konvencijom za zaštitu ljudskih prava i temeljnih sloboda od 4. novembra 1950. Člankom 8., se uspostavlja pravo svake osobe na poštovanje njenog privatnog i obiteljskog života, doma i dopisivanja. Direktivom EU broj: 2016/680 Europskog parlamenta i Vijeća Evrope, detaljnije je definisana zaštita pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija i o slobodnom kretanju takvih podataka. Direktivom se štiti temeljno pravo građana na zaštitu podataka svaki put kada tijela kaznenog progona koriste osobne podatke. Njome se osigurava primjerena zaštita osobnih podataka žrtava, svjedoka i osumnjičenih za kaznena djela te olakšava prekogranična suradnja u borbi protiv kriminala i terorizma. A Direktivom 2002/58/EZ Europskog parlamenta i Vijeća Evrope. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o

privatnosti i elektroničkim komunikacijama) se postavlja osjetljivo pitanje zadržavanja podataka, o čemu je Sud EU-a u više navrata raspravljao i donio niz presuda, a posljednji put 2020., kada je izjavio da se opće i neselektivno zadržavanje podataka o prometu i lokaciji protivi pravu EU-a.

Evropski nadzornik za zaštitu podataka neovisno je nadzorno tijelo koje jamči da institucije i tijela EU-a poštuju svoje obveze u vezi sa zaštitom podataka. Glavne zadaće evropskog nadzornika za zaštitu podataka su nadzor, savjetovanje i suradnja. Evropski odbor za zaštitu podataka, nekadašnja Radna skupina iz članka 29., ima status tijela EU-a i pravnu osobnost te vlastito tajništvo. Okuplja nacionalna nadzorna tijela iz Unije, Ured europskog nadzornika za zaštitu podataka i Komisiju. Evropski odbor za zaštitu podataka ima široke ovlasti odlučivanja u sporovima između nacionalnih nadzornih tijela te davanja savjeta i smjernica o ključnim konceptima iz Opće uredbe o zaštiti podataka i Direktive o zaštiti podataka u području izvršavanja zakonodavstva. Parlament je zaštitu privatnosti postavio kao politički prioritet i tako odigrao ključnu ulogu u oblikovanju zakonodavstva EU-a u području zaštite osobnih podataka. Također u okviru redovnog zakonodavnog postupka ravnopravno s Vijećem radi na reformi zaštite podataka. Rad na posljednjem važnom elementu, novoj uredbi o privatnosti i elektroničkim komunikacijama, završio je 2017. te sada s nestrpljenjem očekuje da Vijeće dovrši svoj dio posla i da započnu međuinstitucionalni pregovori. Parlament pomno nadzire međunarodne sporazume o prijenosu podataka i brine se da se njegov glas po tom pitanju čuje, Parlament je sada fokusiran na nadzor provedbe zakonodavstva EU-a o zaštiti podataka, na aspekte zaštite podataka u području umjetne inteligencije i Akta o digitalnim uslugama te na druge buduće prijedloge Komisije koji bi mogli utjecati na zaštitu podataka.

General Data Protection Regulative (GDPR) je opšta Uredba EU 2016/679 EC o zaštiti ličnih podataka. Uredba se bavi harmonizacijom zaštite ličnih podataka na nivou EU, te definiše veći stepen kontrole za lica čiji se podaci obrađuju i unapređuje upravljanje savremenim rizicima iz ove oblasti. Sistemi KI spadaju među najveće rukovaoce (operatere) podataka o ličnosti i u postupku usklađivanja sa obavezama utvrđenih Uredbom treba da izvrši punu analizu svog postojećeg regulatornog i infrastrukturnog okvira sa zaštitom ličnih podataka. Također, primjenom Uredbe pruža se prilika za ispravke eventualnih ranijih nedostatka u postojećim procesima, te se od organizacija očekuje podizanje opšte svijesti o standardima zaštite ličnih podataka, a posebno imajući u vidu zaprijećene stroge sankcije za slučaj

neusklađenosti. Uredba daje definiciju područja primjene, ujednačavanja propisa u jedinstveni mehanizam, odgovornost i transparentnost, pravne osnove za dobrovoljnost davanja ličnih podataka, službenike za zaštitu ličnih podataka, pseudonomizaciju (zaštitu imena i prezimena), povredu zaštite ličnih podataka, kaznenu politiku, pravo pristupa i pravo na zaborav, prenos podataka, integrisanu zaštitu i evidenciju o aktivnostima obrade podataka.

Sa aspekta vanjske i unutrašnje zaštite podataka, najvažnija poglavlja su definisanje rada službenika za zaštitu ličnih podataka i integrirana zaštita podataka, kojima se daju precizne smjernice za izradu procedura i primjenu određenih mjera zaštite tajnosti podataka. Ako se osnovne djelatnosti voditelja obrade sastoje od postupaka obrade, koji zbog svoje prirode, obima ili svrhe iziskuju redovno i sistemsko praćenje ispitanika u velikoj mjeri, odnosno ako aktivnosti obrade uključuju opsežnu obradu posebnih kategorija podataka, potrebno je imenovati stručnu osobu sa znanjima u području zaštite podataka koja će pomoći voditelju ili izvršitelju obrade, te nadzirati usklađenost s mjerama iz GDPR-a. Od službenika za zaštitu podataka očekuje se stručnost u upravljanju IT procesima, sigurnosti podataka (uključujući odgovor na "cyber napade") i ostalim kritičnim pitanjima koja se tiču pohrane i obrade ličnih i osjetljivih podataka. Potrebni nivo znanja širi je od samog razumijevanja zakonskih propisa. Više podataka o pojedinostima i funkciji službenika za zaštitu podataka dati su u dokumentu "Smjernice o službenicima za zaštitu podataka", izdatom od strane Radne skupine za zaštitu podataka. Mjere tehničke i integrirane zaštite podataka propisuju primjenu zaštitnih mjera u sam postupak razvoja procedura, proizvoda i usluga. Treba od početka primijeniti visoki nivo mjera za zaštitu privatnosti, a voditelj obrade mora osigurati da tehničke i proceduralne mjere budu adekvatne i u skladu sa propisima za vrijeme cjelokupnog trajanja postupaka obrade. Voditelji obrade trebaju primijeniti mehanizme kojima bi se spriječila obrada osobnih podataka, osim ako je to potrebno za svaku od određenih svrha.

Zaštita podataka dobijenih u procesu integrisane zaštite predstavlja veoma važan preventivno-operativni segment koji se izvodi u tri faze: pripremnoj, operativnoj i arhivnoj. Ovaj proces počinje planiranjem sistema zaštite podataka, izradom procjene i plana IT zaštite shodno smjernicama i međunarodnim standardima. Od izuzetne je važnosti pravilno odabrati adekvatne alate za prikupljanje, obradu i arhiviranje podataka, koji svojim akreditovanim i licenciranim softverima garantuju maksimalnu zaštitu osjetljivih i ličnih podataka. Današnje GIS vektorske baze većinom u svom

kodu imaju napredni enkripcijski standard, Advanced Encryption Standard (AES), vodeni žig („watermark“), te hologramsku i biometrijsku zaštitu svojim pristupima. Zaštita vektorskih mapa podrazumjeva šifriranje podataka vektorskih mapa, kontrolu pristupa korisnika i identificiranje operatera, odnosno vlasnika, u cilju sprečavanja šteta, napada ili ilegalnih distribucija, koje se mogu dogoditi u proces integracije niza geografskih informacija. Istraživači su dali rješenja zaštite putem „vodenog žiga“ za zaštitu autorskih prava i metode napredne enkripcije (šifriranja) usmjerenih na različite domene unutar samog sistema, vodeći računa o međunarodnom upravno-pravnom naslijeđu, Uredbi GDPR i standardu ISO 27000.

4. ZAKLJUČCI

U različitim nacionalnim, regionalnim i inter-regionalnim zdravstvenim bazama podataka širom planete pohranjene su lične informacije miliona ili čak milijardi stanovnika, koje su izložene svakodnevnim prijetnjama od unutrašnjih i vanjskih zloupotreba. Sukladno tome možemo zaključiti da će posljedice globalnih kriza zahvatiti ne samo zdravstvene i ekonomske aspekte pojedinca, već i njihova temeljna ljudska prava i slobode.

Razvoj Geo-Informacionih Sistema (GIS) i potreba za digitalizacijom podataka koji se u interesu javnog zdravlja razmjenjuju među mnogobrojnim korisnicima, otvara brojna pitanja koja se prije svega odnose na zaštitu ljudskih prava i zaštitu ličnih podataka pojedinca. Dvije su osnovne upravno-pravne norme na koje se trebamo referisati kod proučavanja ovog fenomena i traženja odgovora na brojna pitanja. Prva je Opća deklaracija UN o ljudskim pravima (1948), koja je bila baza za uspostavljanje Evropske Konvencije o zaštiti ljudskih prava i temeljnih sloboda (1950). A druga je Opšta Uredba o zaštiti podataka (GDPR), koja je od 2018. postala obavezujuća za sve države članice EU, ali je i preporuka zemljama kandidatima i potencijalnim kandidatima za članstvo u EU.

Preventivno rješenje za uočene probleme je šire uključenje akademske zajednice i referentnih stručnih organizacija za razvoj GIS baza i zaštitu ličnih podataka. Najefikasniji odgovor na rizike zloupotrebe podataka je interoperabilna sinergija svih dionika iz integriranog sistema prikupljanja, korištenja i zaštite ličnih podataka. Ovaj proces treba sagledavati u okviru javno privatnog partnerstva i formiranja Quadriplex (četverostrukog) lanca sastavljenog od karika akademske zajednice, javne uprave, privatne inicijative

i nevladinog sektora. Kao generalni zaključak ovog rada, možemo se referirati na mišljenje Mihailović, Garaplija, (2022) u kome ističu da je „S3 platforma moćan mehanizam za stvaranje snažne koordinacije između naučnoistraživačke zajednice i industrijskih struktura. Kao takav, služi kao svojevrsna referentna tačka za inovacione aktivnosti u smislu njihovog usmjeravanja ka identifikovanim potrebama privrede.

LITERATURA

1. Garaplija, E., Karisik, A., 2022. S3 - Smart Strategy Specialisation - case study "INZA GROUP".
2. Mihailovic, A., Garaplija, E., 2022. The S3 platform as a digital transition accelerator in EU enlargement countries“
3. Opća deklaracija UN o ljudskim pravima (1948)
4. Evropske Konvencije o zaštiti ljudskih prava i temeljnih sloboda (1950)
5. Opšta Uredba o zaštiti podataka (GDPR), (2018)
6. CRED (Center for research epideiology of disasters) – istraživački centar Evropa RE
7. Direktiva 2002/58/EZ Europskog parlamenta i Vijeća Evrope. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)
8. General Data Protection Regulative (GDPR), opšta Uredba EU 2016/679 EC o zaštiti ličnih podataka
9. Direktiva EU broj: 2016/680 Europskog parlamenta i Vijeća Evrope, o zaštiti pojedinca u vezi sa obradom osobnih podataka od strane nadležnih tijela
10. Selimić, M., 2018. Pravo na dobru upravo kao osnovno pravo prema povelji Evropske unije o temeljnim pravima. Anali, Pravni fakultet Zenica
11. INSPIRE direktiva je definisala infrastrukturu važnih informacija u Evropi, https://inspire.ec.europa.eu/about-inspire/563#