ANALIZA PRAKSI PRIKUPLJANJA I OBRADE PODATAKA ZA VRIJEME COVID PANDEMIJE - SLUČAJ HRVATSKE

Politiscope, veljača 2021.

UVOD

Uspješno upravljanje pandemijom Corona virusa podrazumijeva uspostavu novih praksi prikupljanja osjetljivih podataka građana s ciljem očuvanja javnog zdravlja. Nažalost, ključna tijela javne vlasti koja upravljaju pandemijom u Hrvatskoj pokazuju kontinuirani nemar prema temeljnim pravima građana provodeći i promovirajući nezakonite i štetne prakse prikupljanja i obrade podataka.

Pandemija prijeti uvođenjem novih nezakonitih oblika digitalnog nadzora koji ne poštuju privatnost, krše ljudska prava i predstavljaju ugrozu temeljnih demokratskih načela. Autoritarne države uspostavile su **sustav potpunog digitalnog nadzora** kao suvremeni oblik kontrole populacije. No, pandemija Corone poslužila je kao izgovor za uvođenje nezakonitih praksi nadzora u usidrenim i defektnim demokracijama, nudeći lažnu dilemu izbora između privatnosti i javnog zdravlja. Dok su neke države članice privatnost prepoznale kao ključan problem epidemiološkog digitalnog nadzora građana, Vlada RH je u nizu primjera pokazala iznimno zabrinjavajući odnos prema osobnim podacima svojih građana i zaštiti njihove privatnosti. Iako je ograničenje temeljnog ljudskog prava na zaštitu podataka u vrijeme pandemije moguće, ono mora biti utemeljeno u zakonu, proporcionalno te je potrebno propisati adekvatne mjere zaštite takvih podataka. Umjesto da propisane obrade budu utemeljene u zakonu i štite prava građana, u Hrvatskoj imamo pravi pravni košmar, u kojem javna tijela izdaju proizvoljne i nestručne upute za prikupljanje podataka dok se obveznici zakona nalaze u pravnoj nesigurnosti.

U fokusu analize su tijela javne vlasti koja oblikuju epidemiološka prikupljanja podataka građana o njihovim kontaktima: Stožer za civilnu zaštitu, Hrvatski zavod za javno zdravstvo (dalje u tekstu: HZJZ), Agencija za zaštitu osobnih podataka, Vlada RH. Praćenje rada Stožera, AZOP-a i Vlade je nužno u odnosu na činjenicu da su prakse epidemiološkog prikupljanja podataka određene uputama i mjerama koje izdaju Stožer i Zavod te općim epidemiološkim pristupom i digitalnim rješenjima za praćenje, koje su u nadležnosti Vlade.

Izvještavanjem o radu ovih ključnih tijela, utemeljenom na analizi, želimo dokinuti nezakonite pandemijske prakse prikupljanja podataka te izgraditi principe dobrog upravljanja i transparentnosti među institucionalnim akterima koji oblikuju javnu politiku privatnosti. Analiza je namijenjena institucionalnim akterima zaduženima za oblikovanje javne politike privatnosti, samostalnim i neovisnim institucijama koje štite ljudska prava građana, organizacijama civilnog društva te građanima i široj javnosti.

U nastavku je izložena analiza najrelevantnijih i najproblematičnijih slučajeva obrade i prikupljanja podataka s ciljem zaštite javnog zdravlja u Hrvatskoj: i) neustavne izmjene Zakona o elektroničkim komunikacijama, ii) nelegitimni i nezakoniti pravni okvir za

pandemijsku obradu podataka, iii) digitalni asistent Andrija objavljen bez Politike privatnosti, iv) nezakonite upute Stožera frizerskim i kozmetičkim salonima, v) nelegitimna obrada podataka učenika u školama, vi) slučaj Beroš-Badrić, vii) dostava pogrešnih rezultata testiranja.

Za shvaćanje šireg političkog konteksta u kojem AZOP djeluje, potrebno je uzeti u obzir da se radi o instituciji koja nije samostalna i neovisna od Vlade, iako se službeno radi o neovisnom nadzornom tijelu. Naime, osim što štiti ugrozu temeljnih prava građana od strane privatnih tvrtki, AZOP ujedno provodi i nadzor nad radom svih tijela javne vlasti, ako ista prikupljaju i obrađuju osobne podatke građana. Istovremeno, na čelnom mjestu AZOP-a se nalazi osoba koja **ne ispunjava minimalne zakonom propisane uvjete** te se nalazi u **trajnom sukobu interesa** jer je prethodno preuzimanju pozicije ravnatelja AZOP-a bio član HDZ-a i državni dužnosnik u Ministarstvu graditeljstva. Detaljnije informacije su dostupne u **Analizi rada Agencije za zaštitu osobnih podataka**.

IZMJENE ZAKONA O ELEKTRONIČKIM KOMUNIKACIJAMA

Vlada RH je u ožujku 2020. predložila **nacrt izmjena Zakona o elektroničkim komunikacijama**, prema kojem bi ministri, u izvanrednim okolnostima, imali ovlast izdavanja zahtjeva telekomunikacijskim operaterima za obradom podataka o geolokaciji mobilnih uređaja građana. Budući da nacrt izmjena, kao ni predloženi amandmani, nisu sadržavali dovoljna jamstva zaštite privatnosti, sigurnosti i ustavnih prava građana i građanki RH, Politiscope je zastupnicima Hrvatskog sabora dostavio **prijedloge amandmana**.

Predloženi amandmani osigurali bi da svako zadiranje u potencijalno veoma osjetljivu kategoriju podataka može biti isključivo privremeno, proporcionalno, nužno za ostvarenje svrhe te transparentno. Naši prijedlozi uključuju ograničenje obrade podataka o lokaciji na temelju jednog zahtjeva ministra na najdulje 30 dana (izdavanjem novih zahtjeva ministar bi imao mogućnost produljiti period obrade podataka ako se za to ukaže potreba). U slučaju obrade podataka o lokaciji svih građana na određenom geografskom području, uvedena je obveza poopćivanja podataka o lokaciji na razinu gradske četvrti ili lokalne jedinice. Naposljetku, predložena je izričita zabranu izrade profila ispitanika na temelju obrade prikupljenih podataka o lokaciji.

Amandmani udruge Politiscope su ujedno uključivali korisne elemente prijedloga Pučke pravobraniteljice i Kluba zastupnika Socijal-demokratske partije: obveza definiranja skupine ispitanika i vremenskog perioda obrade podataka, obveza obavještavanja ispitanika o obradi podataka, obveza uništavanja prikupljenih podataka u roku od 30 dana u slučaju nepokretanja odgovarajućeg postupka, izričito navođenje tijela nadležnog za poslove civilne zaštite kao jedinog nadležnog za obradu podataka te obvezu obavještavanja nadležnih tijela o poduzetim radnjama.

Glasna **kritika stručne javnosti, aktivističkih organizacija koje se bave zaštitom ljudskih prava** i **privatnosti** te ujedinjene oporbe, povećali su političke troškove provedbe ovakvog modela nadzora građana te je Vlada odustala od guranja predloženih izmjena zakona. Čini se da je dodatan razlog za odustanak od izmjena prevladavajuće mišljenje stručne javnosti o potrebi **usvajanja izmjena dvotrećinskom većinom**, što bi podrazumijevalo suradnju s oporbom. Zaustavljanjem ovih izmjena, spriječen je razvoj novog oblika digitalnog nadzora građana putem njihovih mobilnih uređaja, za kojeg možemo pretpostaviti da bi ostao u pogonu i nakon završetka pandemije.

Nakon odustajanja od praćenja geolokacije građana, Vlada RH se prihvatila razvoja manje invazivnog digitalnog rješenja, u skladu s globalno popularnim konceptom o aplikaciji za "praćenje kontakata" potencijalno zaraženih osoba – digitalnom rješenju kojim su brojne države pokušale spriječiti širenje korona virusa. U srpnju 2020., Ministarstvo zdravstva, HZJZ te tvrtka APIS **predstavili su mobilnu aplikaciju Stop COVID-19**, koja služi upozoravanju građana o osobnoj izloženosti epidemiološki rizičnom kontaktu. Aplikacija je temeljena na Google/Apple sustavu "Obavijesti o izloženosti„ (*Exposure Notification*) koji funkcionira tako da mobiteli putem Bluetooth tehnologije razmjenjuju **nasumične ključeve**. Spomenuti sustav globalno je najkorišteniji za ovaj tip aplikacije, ponajprije zbog činjenice da su upravo navedeni tehnološki giganti vlasnici najvećih *smartphone* platformi. Unatoč inzistiranju na zaštiti privatnosti korisnika od samog početka razvoja, nakon izlaska aplikacija ispostavilo se kako ipak postoje određeni propusti koji se tiču prikupljanja metapodataka o korištenju, što je problem posebice izražen u Android verzijama. Vjerujemo da su vijesti s problemima u sferi zaštite podataka, zajedno s tehničkim poteškoćama hrvatske verzije, doprinijeli **iznimno slabim brojkama** korištenja aplikacije.

Iako su vidljivi pomaci u promišljanju o privatnosti korisnika, pogotovo u odnosu na niz prethodnih invazivnih ideja i rješenja poput digitalnog asistenta Andrije, ni Stop COVID-19 aplikacija nije u potpunosti razvijena prema "privacy by design" načelu. Riječ je o načelu koje je Uredba pretvorila u pravnu obvezu, a koje podrazumijeva da je u svakoj fazi razvoja i dizajna bilo kojeg digitalnog rješenja, privatnost korisnika postavljena kao temeljni stup njegove funkcionalnosti. Rješenje napravljeno sukladno "privacy by design" načelu ne može sadržavati softverske komponente trećih strana koje su poznati kršitelji privatnosti, poput servisa Google Analyticsa, što je slučaj sa hrvatskom verzijom Android aplikacije. Također, tehnološki

kapacitirano i samostalno nadzorno tijelo za zaštitu podataka trebalo bi biti u stanju prepoznati manjkavosti aplikacije koja obrađuje osjetljive podatke građana te dati jasne preporuke za korekcije istih. AZOP je dao zeleno svijetlo korištenju aplikacije, bez jasne argumentacije o aspektu zaštite osobnih podataka i popratnih preporuka kako da se isprave manjkavosti u tom pogledu. Dodatne i detaljnije informacije o aplikaciji su dostupne u Pravnoj i tehničkoj analiza Stop COVID-19 aplikacije.

NELEGITIMNA I NEZAKONITA PANDEMIJSKA PRAKSA PRIKUPLJANJA I OBRADE PODATAKA

U slučaju pandemije, prikupljanje i obrada podataka o kontaktima su opravdani svrhom zaštite javnog zdravlja. No, recital 45. Opće uredbe o zaštiti podataka (dalje u tekstu: Uredba) jasno ističe kako je u ovakvim slučajevima potrebno stvoriti zakonski okvir koji regulira prikupljanje i obradu podataka te između ostalog propisuje: svrhu i opseg prikupljanja podataka, načine zaštite, rok čuvanja, subjekte kojima se osobni podaci mogu otkriti, razdoblja pohrane i mjere za osiguravanje zakonite i poštene obrade.

Isto tako, obrada zdravstvenih i drugih osjetljivih podataka građana je dopustiva jedino ako je utemeljena u zakonu te se provodi u svrhu zdravstvene zaštite, sprečavanja ili kontrole zaraznih bolesti. Naime, recital 52. Uredbe predviđa mogućnost odstupanja od zabrane obrade posebnih kategorija osobnih podataka (poput zdravstvenih), ako je to predviđeno pravom države članice te je obrada podataka u javnom interesu.
Tijekom 2020. godine pokrenute su dvije izmjene Zakona o zaštiti pučanstva od zaraznih bolesti, no iste nisu predviđale uređenje zakonskog okvira za pandemijsku obradu podataka s ciljem zaštite javnog zdravlja. Samim time, sve upute izdane od strane HZJZ-a javnim ustanovama i poslovnim subjektima, a vezane uz prikupljanje osobnih podataka korisnika njihovih usluga su – nelegalne i nelegitimne. Naime, prikupljanje osobnih podataka građana bez privole s ciljem zaštite javnog zdravlja predstavlja ograničenje temeljnih prava te je isto potrebno urediti zasebnim zakonskim propisom, što je obveza definirana recitalima 45. i 52. Uredbe.

Udruga Politiscope dostavila je svim klubovima zastupnika Hrvatskog sabora amandmane na Zakon o zaštiti pučanstva od zaraznih bolesti, koji bi takvu obradu podataka učinili zakonitom. Predloženim amandmanima omogućuje se obrada posebnih kategorija osobnih podataka od strane pravnih i fizičkih osoba koje obavljaju gospodarske djelatnosti, a u svrhu sprečavanja i suzbijanja zaraznih bolesti, odlukom ministra na prijedlog Hrvatskog zavoda za

javno zdravstvo, u suradnji s nacionalnim nadzornim tijelom za zaštitu podataka. Izmjenama se definira obveza navođenja osnovnih stavki o obradi podataka u sadržaju odluke kojim se naređuje obrada, s ciljem zaštite osobnih podataka, ali i drugih temeljnih prava građana. Definiranjem minimalnog opsega sadržaja odluke kojom se naređuje prikupljanje i obrada, dodatno se osigurava zaštita osobnih podataka i drugih temeljnih prava građana.

Naposljetku, predloženim izmjenama se uvodi obveza uključivanja Agencije za zaštitu osobnih podataka u donošenje odluka kojima se naređuje prikupljanje i obrada osjetljivih podataka građana s ciljem sprečavanja širenja zaraznih bolesti. Na taj način se želi izmijeniti dosadašnja praksa retroaktivnog očitovanja AZOP-a o izrečenim mjerama prikupljanja i obrade podataka te se potiče rano i proaktivno uključenje nadzornog tijela, sukladno njegovim osnovnim zadaćama definiranih člankom 57. Uredbe, a s ciljem zaštite prava i sloboda pojedinaca u pogledu obrade podataka.

Umjesto razvoja kvalitetnog zakonskog okvira koji jasno uređuje ključna pitanja prikupljanja i obrade podataka nužnih za očuvanje javnog zdravlja, Vlada RH odlučila je pandemijom upravljati putem nedovoljno jasnih te pravno upitnih preporuka i uputa HZJZ-a. Na taj način su uspostavljene nezakonite i štetne prakse pandemijskog prikupljanja i obrade podataka, stvorena je pravna nesigurnost i potpuni košmar koji je doveo do besmislenih administrativnih opterećenja voditelja obrade podataka te nepotrebnih rizika financijskih kazni za poslovne subjekte. U nastavku analize izložit ćemo kaotične situacije nastale izdavanjem preporuka za prikupljanje osobnih podataka od klijenata salona te učenika u školama.

PREPORUKE ZA RAD SALONA: HZJZ I OBRTNIČKA KOMORA

U svibnju 2020., vlasnici salona u kojima postoji izraženi fizički kontakt (frizerski, kozmetički, tattoo i slični saloni), našli su se u iznimno zbunjujućoj i financijski rizičnoj situaciji – nakon što je Hrvatski zavod za javno zdravstvo izdao **preporuku o prikupljanju podataka** klijenata.

Kako je istaknuto u prethodnom poglavlju analize, takva preporuka je nezakonita prije svega zbog nepostojanja nacionalnog zakonskog okvira koji uređuje prakse prikupljanja podataka građana s ciljem zaštite javnog zdravlja, sukladno recitalu 45. Uredbe. Osim toga, nedostajao je čitav set informacija neophodnih da saloni ovom obradom ne bi kršili niz obveza Uredbe: nije razjašnjen pravni temelj takve obrade, nisu preporučene tehničke ni organizacijske upute za zaštitu podataka, a salonima nije ukazano da trebaju promijeniti svoje Politike privatnosti.

Način objave uputa o prikupljanju podataka za salone, koji ne uključuje detaljne informacije o zaštiti podataka, zajedno s pasivnošću AZOP-a, doprinijeli su tome da se uspostavi nelegitimna i nezakonita praksa obrade podataka. Potvrda za ovaj zaključak je došla u obliku obrasca za prikupljanje podataka klijenata kojeg je **Hrvatska obrtnička komora dostavila svim salonima**, vjerojatno s idejom da će pomoći salonima. HOK je obrascem demonstrirao potpuno nepoznavanje načela i obveza Uredbe i obrte potaknuo prema njenom kršenju te ih tako nepotrebno izložio riziku visokih novčanih kazni. U obrascu se pogrešno navodila pravna osnova za prikupljanje podataka (privola), prikupljala se prekomjerna količinu podataka (uključujući osjetljive podatke) te se povećavao rizik gubitka ili otuđenja podataka (nepotrebno se kreiraju fizički dokumenti koji sadrže osjetljive informacije klijenata). AZOP je **mišljenje s jasnijim uputama** izdao tek nakon što je obrazac Obrtničke komore izazvao veliki interes, ali i negodovanje javnosti. Agencija je istaknula kako ne postoji zakonita osnova za obradu podataka u navedenom obrascu, već samo onih podataka navedenih u mjerama HZJZ (broj mobitela korisnika usluga, ime i prezime te vrijeme dolaska i odlaska iz salona).

Osim uspostavljanjem jasnog zakonskog okvira sukladnog recitalu 45. Uredbe, ova kaotična situacija mogla se izbjeći i da je AZOP, umjesto reaktivno, za promjenu djelovao proaktivno te se uključio u proces izrade preporuka HZJZ-a ili barem reagirao nakon što su one izdane. Budući da očigledno ne uživa ugled samostalne i neovisne institucije, AZOP je u potpunosti izignoriran prilikom izrade svih uputa HZJZ-a, a nadzorno tijelo potvrdilo je taj dojam izostankom ili tromom reakcijom na uspostavu nezakonitih i štetnih praksi prikupljanja podataka.

PRIKUPLJANJE I OBRADA PODATAKA U ŠKOLAMA

Krajem travnja 2020., HZJZ je u svojim **preporukama o povratku učenika u školske klupe** naložio školama da od roditelja traže potpisivanje izjave koje potvrđuju da djeca nemaju simptome Covid-19, da ne postoji sumnja da su zaraženi koronom, da se radi o djetetu s oba zaposlena roditelja te da ne postoji druga mogućnost njegovog zbrinjavanja. Još se jednom pokazalo kako Vlada očigledno nema kapacitete za osmisliti kvalitetan zakonski okvir za prikupljanje podataka u okolnostima pandemije, pa odgovornost za to prebacuje na sama javna tijela. U potpunosti je neprimjereno uređivati prikupljanje najosjetljivijih podataka građana kroz preporuke i upute, a posebice kada se prikupljaju podaci maloljetnih osoba.

Ključni pravni problem je kršenje osnovnih načela Uredbe: nije uopće jasno koja je svrha obrade podataka, još je manje jasan pravni temelj takve obrade, a škole i vrtići nisu dobili sve potrebne upute. Stoga roditeljima nisu mogli pružiti adekvatne informacije o obradi (koliko dugo se podaci njihove djece zadržavaju, kako se čuvaju, tko im ima pristup, koja prava imaju prilikom obrade zdravstvenih podataka njihove djece). Istovremeno, škole i vrtići nisu dobili uputu kako provesti tehničke i organizacijske mjere zaštite zdravstvenih podataka, koje Uredba tretira kao posebno osjetljive. Osim toga, izjava uopće nema ikakvu pravnu težinu, odnosno roditelj ne snosi posljedice ako ju ne potpiše ili ako da netočne podatke. Stoga ostaje nejasno što se uopće htjelo postići uvođenjem te izjave.

Ako državno tijelo namjerava naložiti obradu osjetljivih osobnih podataka građana, trebalo bi to učiniti u suradnji s Agencijom za zaštitu osobnih podataka, tijelom koje je u Hrvatskoj zaduženo za provedbu Uredbe. Izostanak ovoga je doveo do situacije u kojoj svaka škola i vrtić izrađuje svoju izjavu te su neke čak tražile i podatke dodatne onima navedenima u Uputi HZJZ-a. Udruga Politiscope je dobila na uvid neke od tih izjava i one su, sasvim očekivano, imale raznih manjkavosti. Osim prekomjerne obrade, nekim izjavama se od roditelja tražila privola, koja istovremeno nije bila dobrovoljna. Obrascima se stvarao lažan osjećaj postojanja pravne obveze davanja podataka, a jasno je da ravnatelji istovremeno nisu znali što bi točno trebali raditi s tim podacima, niti kako i koliko dugo ih čuvati. Nakon snažne kritike **stručne** i **zainteresirane** javnosti te samih roditelja, HZJZ je u sljedećim preporukama za škole i vrtiće odustao od ideje potpisivanja ovakvih izjava.

AZOP uopće nije reagirao na sporne izjave, no oglasio se u studenom 2020. **mišljenjem** o prikupljanju podataka u zagrebačkim školama koje je zatražio Nastavni zavod za javno zdravstvo „Dr. Andrija Štampar“, s ciljem sigurnijeg odvijanja nastave, a sukladno preporukama HZJZ-a. Agencija navodi kako je pravna osnova za takvu obradu javni interes, a sukladno Zakonu o odgoju i obrazovanju u osnovnoj i srednjoj školi te Zakonu o zaštiti pučanstva od zaraznih bolesti. Navedeni zakoni sadrže odredbe koje bi se mogle smatrati

nacionalnim propisom u smislu recitala 52. Uredbe, no istovremeno, niti jedan od navedenih zakona ne sadrži ni približno sve obvezne elemente definirane recitalom 45. Uredbe, što čini oslanjanje na javni interes kao pravnu osnovu za obradu podataka pravno neodrživim.

U ovom slučaju ponovno se ističu dva ključna elementa koja se protežu kroz čitav period pandemijske obrade podataka u Hrvatskoj. Prvi, nepostojanje kvalitetnog zakonskog okvira koji regulira obradu u kriznim situacijama sukladno recitalima 45. i 52. Uredbe. Drugi, kontinuirana pasivnost AZOP-a kao nadzornog tijela za zaštitu podataka. U ovom slučaju, AZOP se uopće nije javno oglasio o tome smatra li sporne izjave zakonitima, niti je obrazovnim ustanovama na bilo koji način pomogao u provedbi mjera HZJZ.

NASTAVA NA DALJINU

Tijekom prvog vala pandemije Korona virusa u Hrvatskoj, u razdoblju od ožujka do lipnja 2020. godine, sve škole u Hrvatskoj u potpunosti su prešle na model održavanja nastave na daljinu. Takav model podrazumijevao je i korištenje softverskih alata za održavanje nastave putem interneta, kako za gledanje snimljenih video lekcija, tako i za video-konferencijsku komunikaciju učenika s nastavnicima.

Ministarstvo znanosti i obrazovanja, nadležne agencije i ustanove pokazale su potpunu nebrigu o zaštiti osobnih podataka i privatnosti učenika u procesu prelaska na model nastave na daljinu. Posebno zabrinjava da se u niti jednom dokumentu o nastavi na daljinu izdanom od strane Ministarstva obrazovanja i CARNET-a, privatnost ne uzima kao relevantna značajka prilikom korištenja različitih softverskih alata u svrhu provođenja nastave. Plastičan primjer nedostatka svijesti o privatnosti unutar hrvatskog obrazovnog sustava je web stranica www.skolazazivot.hr, polazišna točka svakom učeniku za informacije i pristup sadržajima online nastave. Naime, stranica sadrži čak četiri trackera (tehnologije za praćenje) koji se bez davanja privole postavljaju na uređaj svakog posjetitelja te podatke o ponašanju učenika na stranici dijele s Facebookom, Googleom te tvrtkom ShareThis.

Politiscope je proveo analizu najčešće korištenih aplikacija iz perspektive zaštite privatnosti učenika, s ciljem davanja jasnih preporuka. Škole koriste alate IT divova poput Googlea i Microsofta, koji su uronjeni u niz skandala povezanih s privatnosti. Na taj način podaci učenika postaju dio nezakonitog i netransparentnog sustava stvorenog primarno za programirani sustav aukcija u svrhu prikaza reklama. Politiscope stoga preporuča da se Google Classrom i Microsoft Teams u potpunosti izbjegavaju u provedbi nastave na daljinu. Udruga daje snažnu preporuku za korištenje rješenja otvorenog koda koja ujedno omogućuju postavljanje alata na vlastite servere. Na ovaj način se ostvaruje potpuna kontrola privatnosti učenika dok se u školama stvara kultura zaštite privatnosti učenika. Takvi servisi su BigBlueButton za nastavu na daljinu te Jitsi Meet za manje video konferencijske razgovore.

Dvije aplikacije dobile su nešto blažu ocjenu, no nisu preporučene za korištenje jer prepoznate manjkavosti pretežu nad prednostima alata – Loomen i Zoom. Detaljnije informacije o privatnosti u učenju na daljinu i provedenoj analizi aplikacija, dostupne su u **Analizi aplikacija za učenje na daljinu iz perspektive zaštite privatnosti djece**.

DIGITALNI ASISTENT ANDRIJA

Vladin digitalni asistent Andrija, **predstavljen u travnju 2020.**, krši preporuke Europske Komisije, osnovne obveze i temeljna načela Uredbe. Pritom, Vlada je kao jedini način pristupa servisu odabrala Whatsapp - platformu konzorcija Facebook, posljednjih nekoliko godina obilježenog nizom skandala povezanih sa zaštitom osobnih podataka.

Preporuke Europske komisije za razvoj digitalnih rješenja u borbi protiv COVID-19 pandemije su prekršene jer u razvoj nije uključeno nacionalno nadzorno tijelo za zaštitu podataka (AZOP). Osim očigledne činjenice da Vlada i prateća tijela nisu ni spomenula involviranost nadzornog tijela za zaštitu podataka, dodatan dokaz je i kršenje najosnovnijih obveza Uredbe. Asistent je puna tri dana bio u pogonu bez objavljene Politike privatnosti, čime je prekršeno načelo transparentnosti, budući da su korisnicima uskraćene osnovne informacije o obradi podataka (tko je voditelj obrade podataka, prosljeđuju li se podaci trećim stranama, kako kontaktirati službenika za zaštitu podataka, u koju svrhu se njihovi podaci prikupljaju, itd.).

Naknadna objava Politike privatnosti prepune manjkavosti, osim diletantizma, otkriva kako privatnost očigledno nije bila jedno od načela razvoja asistenta, budući da ni naknadnom objavom nije prestalo kršenje načela zakonitosti obrade podataka i načelo smanjenja obrade podataka. Servis ističe da ne prikuplja podatke koji bi omogućili identifikaciju, što je u potpunosti netočno, jer prikuplja brojeve mobilnih uređaja ispitanika. Budući da nema pravne osnove za takvu obradu, Digitalni asistent Andrija tako krši načelo zakonitosti obrade podataka, kao i načelo smanjenja količine podataka. Nadalje, nisu dovoljno detaljno opisane tehničke i organizacijske zaštite osjetljivih podataka niti je jasno imaju li privatne tvrtke koje su radile na razvoju servisa pristup osjetljivim podacima građana.

Izrazito je problematičan odabir Whatsappa kao platforme za prikupljanje osjetljivih podataka. U vrijeme pisanja ove analize, iščekuje se **odluka irskog nadzornog tijela u slučaju protiv Whatsappa** zbog prijavljene netransparentnosti i neadekvatnog informiranja korisnika o dijeljenju osobnih podataka s trećim stranama. Whatsapp je sastavni dio digitalnog imperija u vlasništvu Marka Zuckerberga, čiji zaposlenici pred predstavničkim tijelima država diljem svijeta odgovaraju na pitanja izabranih predstavnika naroda, o brojnim skandalima vezanim uz zaštitu osobnih podataka, *hakiranje* izbornog procesa, porast govora mržnje i širenje lažnih

vijesti. Whatsapp je stoga neprihvatljiva platforma za razvoj bilo kakvih digitalnih rješenja u vlasništvu države.

Slučaj digitalnog asistenta Andrije jedan je od najboljih pokazatelja Vladinog odnosa prema obradi osjetljivih osobnih podataka građana. Rješenje je prilikom izlaska kršilo praktički sva najosnovnija načela Uredbe, a uz to i osnovnu preporuku Europske komisije o uključivanju nadzornog tijela za zaštitu podataka u proces razvoja pandemijskih digitalnih rješenja. S druge strane, činjenica da AZOP nije našao shodnim reagirati na ovako problematičan digitalni servis ne ukazuje samo na pasivnost, već i na ovisnost te podređeni odnos institucije prema Vladi RH.

SLUČAJ BEROŠ - BADRIĆ

U kolovozu 2020., Ministar zdravstva Vili Beroš se fotografirao kršeći propisane preporuke Hrvatskog zavoda za javno zdravstvo, **u društvu s pjevačicom Ninom Badrić**, koja je pak bila u prethodnom kontaktu s osobom kojoj je dijagnosticiran Covid-19. Opravdavajući svoje neodgovorno ponašanje, Beroš je u **razgovoru za televiziju N1** izjavio kako je kontaktirao Nastavni zavod za javno zdravstvo, gdje mu je kolegica otkrila kako niti jedan pojedinac s tog događaja nije COVID pozitivan, a pjevačica Badrić nije zabilježena ni kao kontakt pozitivne osobe.

Ministar je tako priznao da, kada god to poželi, jednim običnim telefonskim pozivom može dobiti pristup osjetljivim osobnim podacima građana. Iz perspektive Uredbe, važno je jasno istaknuti kako svrha obrade zdravstvenih podataka o osobama zaraženima virusom te njihovim kontaktima zasigurno nije telefonska provjera Ministara jesu li određeni pojedinci zaraženi ili ne, s ciljem umanjivanja političke štete načinjene vlastitim neodgovornim ponašanjem. Shodno navedenom, situacija u kojoj Ministar telefonskim pozivom od Nastavnog zavoda za javno zdravstvo dobiva takve podatke, kršenje je osnovnih načela Uredbe - načela ograničavanja svrhe; načela zakonitosti, poštenosti i transparentnosti; načela cjelovitosti te povjerljivosti.

U odgovoru na **upite portala Index** o cijeloj situaciji, AZOP je dao niz teško razumljivih birokratskih odgovora te na kraju stao u obranu ministra. U nekoherentnom odgovoru AZOP-a nije ponuđena jasna argumentacija niti objašnjenje za takav stav: "slijedom njegovih nadležnosti i ovlaštenja kao i zadaća, a imajući u vidu i definirano Odlukom Vlade Republike Hrvatske o izradi digitalne platforme i uspostavi interoperabilnosti u svrhu praćenja i suzbijanja zaraznih bolesti, iz iskazanog nije razvidno da bi se radilo o kršenju Opće uredbe o zaštiti podataka odnosno Zakona o provedbi Opće uredbe o zaštiti podataka."

Činjenica da nacionalno nadzorno tijelo za zaštitu podataka smatra kako navedeni postupak

nije problematičan je skandalozna i samo dodatno potvrđuje javnu percepciju nesamostalnosti tijela, koja je dodatno osnažena imenovanjem Zdravka Vukića, bivšeg člana HDZ-a te bivšeg državnog dužnosnika u Ministarstvu graditeljstva, na poziciju ravnatelja AZOP-a.

GRAD ZAGREB I ANTIGENSKI TESTOVI: KRIVI NALAZI, SLANJE REZULTATA NA KRIVE ADRESE

U prosincu 2020. **mediji su izvijestili** o mladoj Zagrepčanki koja je dobila pozitivan rezultat brzog antigenskog testa na Covid-19, prije nego je uopće otišla na testiranje. Pročelnik grada Zagreba za zdravstvo u **razgovoru za medije** je potvrdio kako je Ured za zdravstvo imao problema sa slanjem niza nalaza. Pročelnik je priznao da se, osim slanja krivih nalaza testova, događalo i slanje rezultata na krive adrese.

Kod netočnog obavještavanja o pozitivnom testu, riječ je o višestrukom kršenju načela točnosti definiranog Uredbom, dok je ova situacija školski primjer za važnost tog načela. Naime, zaprimanje netočnog nalaza antigenskog COVID-19 testa može imati opipljive posljedice na život pojedinca te potencijalno rezultirati ponašanjem kojim se ugrožava zdravlja svih drugih pojedinaca koji s tom osobom dođu u kontakt.

Kod slanja nalaza sa osjetljivim osobnim podacima krivim osobama, riječ o ozbiljnoj povredi osobnih podataka ispitanika. U ovakvom slučaju, rizik za ispitanike je nedvojbeno dovoljno visok da voditelj obrade (grad Zagreb) ima obvezu obavještavanja AZOP-a i ispitanika čiji su podaci izloženi.

Udruga Politiscope je uputila zahtjeve za pravom na pristup informacijama u kojima se od **Grada Zagreba traži informacija** je li izvijestio AZOP o učinjenim propustima te se od **AZOP-a traži informacija** jesu li tražili očitovanje po službenoj dužnosti.

Ovo je tek jedan, u nizu primjera nedostatne pažnje koje javna tijela posvećuju zaštiti podataka građana, čiji glavni uzrok možemo pronaći u odredbama Zakona o provedbi Uredbe koje isključuju mogućnost dodjele upravne novčane kazne javnim tijelima. Ukoliko je zbog kršenja Uredbe nastala bilo kakva materijalna ili nematerijalna šteta, građani imaju pravo na pokretanje sudskog postupka za naknadu štete.

PREPORUKE

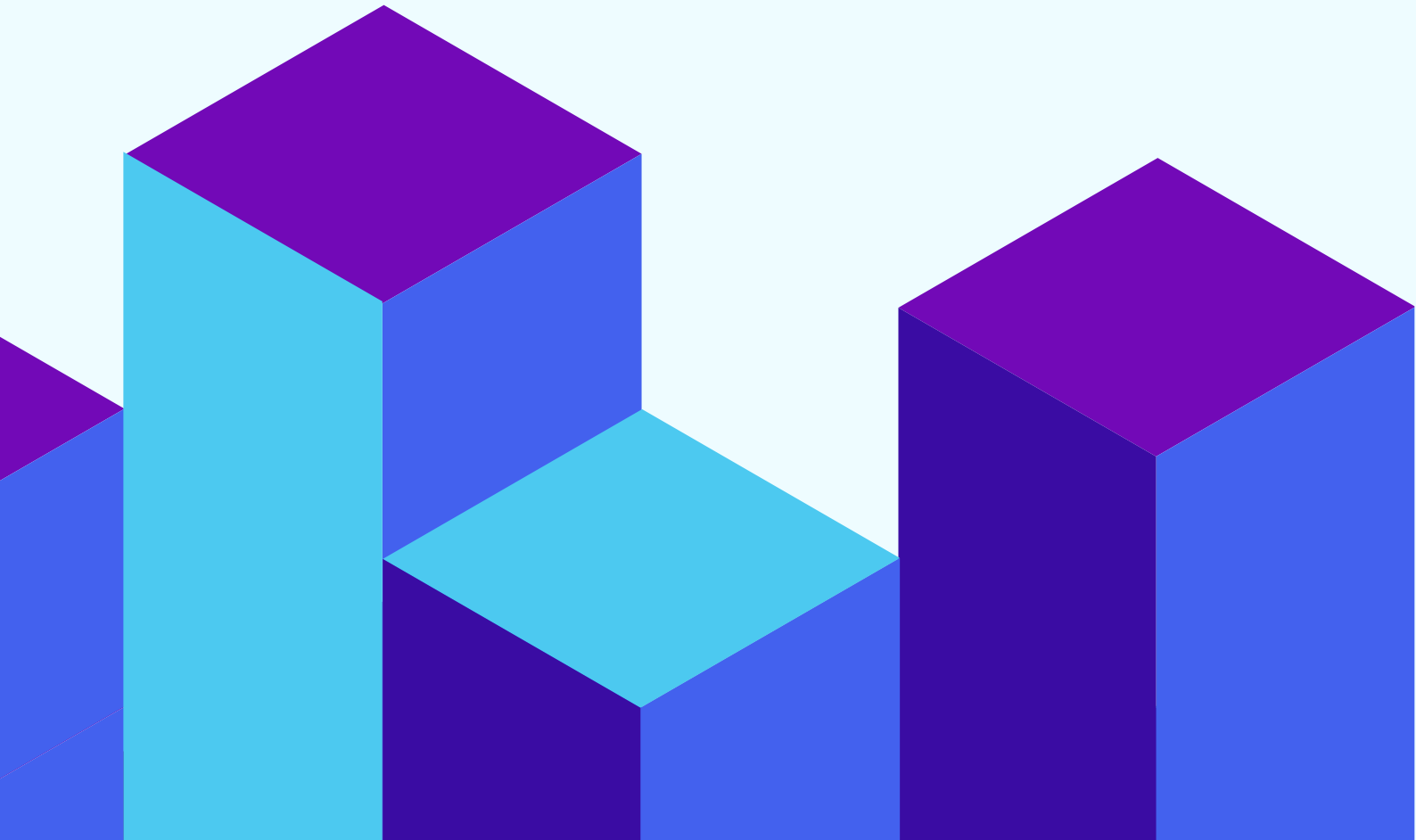
- izmjene Zakona o zaštiti pučanstva od zaraznih bolesti u skladu s recitalom 52. Uredbe, na način da definira zakonsku osnovu za odstupanje od zabrane obrade posebnih kategorija podataka u svrhu sprečavanja ili kontrole zaraznih bolesti

- izmjene Zakona o zaštiti pučanstva od zaraznih bolesti (ili drugih nacionalnih propisa, poput Zakona o odgoju i obrazovanju u osnovnoj i srednjoj školi ili Zakona o zaštiti na radu) u skladu s recitalom 45. Uredbe, na način da zakonski okvir sadrži sve nužne elemente propisane recitalom

- izmjene Zakona o provedbi Opće uredbe o zaštiti podataka, na način da se ukine isključenje primjene upravnih novčanih kazni na tijela javne vlasti

- neophodna proaktivnija uloga Agencije za zaštitu osobnih podataka, uz proširenje tehnoloških kapaciteta tijela i provedbu novog postupka imenovanja ravnatelja neovisne nadzorne institucije

- obvezna primjena „privacy by design“ načela, procesa dizajna i razvoja digitalnih rješenja u kojima je privatnost korisnika temeljno pravilo razvoja rješenja te najosnovniji stup funkcionalnosti - pogotovo kada izradu takvog rješenja naručuju sama tijela javne vlasti



Projekt "Privatnost u doba Corone" je podržan s 4.973 € financijske podrške Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova.

Kreiranje ove analize omogućeno je financijskom podrškom Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova. Sadržaj ove analize isključiva je odgovornost udruge Politiscope i ne odražava nužno stavove država donatorica i Upravitelja Fonda.