Revija za kriminalistiko in kriminologijo / Ljubljana 72 / 2021 / 1, 36–50

Družbeno nadzorstvo v času covida-19[1]

Aleš Završnik[1], Pika Šarf[2]

Pandemija virusa SARS-CoV-2, ki povzroča covid-19, je pospešila že prej močno prisotno obdelavo podatkov o posameznikih in na njih temelječe družbeno nadzorstvo. Hkrati z eno največjih zdravstvenih kriz sodobnega sveta smo danes priča najstrožjemu omejevanju mobilnosti z namenom preprečevanja socialnih stikov, ki je sicer uveljavljena metoda preprečevanja širjenja nalezljivih bolezni, še nikoli pa se ni pojavila v takem obsegu. Globalno »izredno stanje« je neločljivo povezano s tveganji za erozijo človekovih pravic in temeljnih svoboščin. V boju proti nevidnemu sovražniku so države pripravljene sprejemati dvomljivo učinkovite visokotehnološke rešitve, na primer brezpilotne letalnike, termalne kamere, tehnologijo obrazne prepoznave in različne aplikacije za sledenje stikom ali nadzor omejevanja gibanja, ki posegajo v posameznikovo zasebno sfero. Utemeljene so na že znani premisi, da se bo moral vsak izmed nas odpovedati delčku svojih pravic za zaščito zdravja ali celo obstanka skupnosti kot celote. Dihotomija med preprečevanjem širjenja smrtonosnega virusa na eni strani in (domnevno nujnimi) omejitvami pravic posameznikov na drugi je le navidezna: najrazličnejše digitalne rešitve velikokrat že na ravni tehnologije ne morejo doseči rezultatov, ki jih obljubljajo, ali pa predlagana tehnologija ni toliko bolj učinkovita od manj invazivnih ukrepov, da bi pretehtala večji poseg v temeljne pravice.

Ključne besede: covid-19, družbeni nadzor, digitalne tehnologije, sledenje stikom, aplikacija

UDK: 343.9:616-036.21

1 Uvod

Množično zbiranje podatkov v digitalizirani družbi, ki ga je omogočila tehnologija za shranjevanje velikih količin podatkov, in razvoj podatkovnega rudarjenja in podatkovne analitike sta bila v polnem razmahu že pred trenutno zdravstveno krizo (Šarf, 2018; Završnik, 2017). Zaradi povečanja števila uporabnikov spleta, predvsem pa zaradi naraščanja števila tehnoloških naprav, ki jih nosimo s seboj ali se prek njih povezujemo na splet ali internet stvari, rast količine zbranih podatkov že dolgo ni več linearna, temveč eksponentna, in naj bi se vsaki dve leti podvojila (Holmes, 2017).

Pandemija covida-19 je temu trendu množičnega zbiranja in obdelovanja podatkov dala nov zagon. Priča smo največjim globalnim motnjam mobilnosti v moderni dobi: žariščnim točkam (angl. *hot spots*), ki so zaprte za vhode in izhode, zaprtim državnim mejam, »družbenemu distanciranju«[4], začasnemu zapiranju prostorov za delo ter zapiranju izobraževalnih ustanov, restavracij in turističnih kapacitet in rekreacijskih centrov. Vse te omejitve gibanja se nanašajo na vzpostavitev in vzdrževanje fizične distance in ločitev ljudi v fizičnem prostoru. Pri omejevanju mobilnosti prebivalstva med pandemijo so države uporabile tri pravne ukrepe: 1) odreditve karantene za zdrave posameznike, ko so se vrnili z okuženega območja; 2) samoizolacije za posameznike, ki so potrjeno okuženi, in 3) nov *sui generis* ukrep »*stay-at-home*«. Slednji je pravno nejasen in ga je v svoji dosledni različici uveljavila le manjšina evropskih držav (npr. Španija in ne Slovenija spomladi 2020), po vsebini pa je zelo podoben hišnemu priporu.[5]

Vzdrževanje fizične razdalje zahteva izravnalne procese povečane digitalizacije – več komunikacije in dejavnosti se seli na splet. Ukrepi za zajezitev širjenja koronavirusa so

[1] Prispevek je nastal v okviru raziskovalnega dela na raziskovalnem programu Družbeno nadzorstvo, kazenskopravni sistem, nasilje in preprečevanje viktimizacij v kontekstu visoko tehnološke družbe (P5-0221), ki ga financira Javna agencija za raziskovalno dejavnost Republike Slovenije (ARRS), in ciljnega raziskovalnega programa Človekove pravice in regulacija umetne inteligence, vredne zaupanja (V5-1930), ki ga poleg ARRS financirajo Ministrstvo za pravosodje, Ministrstvo za zunanje zadeve, Ministrstvo za javno upravo in Ministrstvo za Ministrstvo za izobraževanje, znanost in šport.

[2] Dr. Aleš Završnik, redni profesor za kriminologijo, Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, Slovenija. E-pošta: ales.zavrsnik@pf.uni-lj.si

[3] Pika Šarf, mlada raziskovalka, Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, Slovenija. E-pošta: pika.sarf@pf.uni-lj.si

[4] Pojem »družbeno distanciranje« (angl. *social distancing*) je izjemno neposrečen, saj naj bi bilo glavni cilj pri preprečevanju prenašanja okužb ravno fizično in ne družbeno distanciranje: le prvo preprečuje okužbe, drugo pa je mogoče ohranjati tudi na daljavo po spletu ipd.

[5] Ukrep »stay-at-home« je po vsebini podoben kazenskopravnemu omejevalnemu ukrepu hišnega pripora, kot je prikazal Gorkič (2020): 1) glede na namen, 2) glede na »zavezanca«, 3) glede na učinke, 4) glede na nadzor in 5) glede na sankcije.

povzročili selitev celega spektra dejavnosti (od najbolj vsakdanjih do profesionalnih) v spletno okolje: videokonference in opravljanje dela od doma z uporabo oddaljenega dostopa do delodajalčevih strežnikov (VPN),[6] spletne učilnice in izobraževanje na daljavo z uporabo spletnih platform in storitev, nakupovanje prek spletnih trgovin, vzdrževanje socialnih stikov s pomočjo najrazličnejših aplikacij in spletnih omrežij itd. Neizogibna posledica tega dodatnega premika iz fizičnega sveta na internet je generiranje še večje količine podatkov, ki razkrivajo podrobnosti o našem vsakdanjem zasebnem, polzasebnem življenju in javnem udejstvovanju.

Družbeni podatkovni nadzor se zaradi obsežnih načrtno izvajanih motenj mobilnosti v času epidemije intenzivira in spreminja. Intenzivira se, ker ukrepi za preprečevanje širjenja vsakršne epidemije temeljijo na obvladovanju mobilnosti posameznika, da epidemija ne preraste v pandemijo[7] in ta v endemijo[8], to pa omogoča nadzor nad podatki. Spreminja se nadzor s selitvijo družbenih osebnih dejavnosti v digitalna spletna okolja, kjer ponudniki spletnih tehnologij pridobivajo vedno več nadzora in uvida (vednosti), medtem ko drugim brez dostopa do sledi digitalnih dejavnosti prebivalstva nadzorstvena moč usiha. Za razliko od preteklih pandemij v moderni dobi (HIV, SARS, MERS, ebola, zika) je pandemijo koronavirusa, ki povzroča covid-19, zaznamovala večja stopnja podatkovnega nadzorstva. Deloma je to mogoče pripisati rasti digitalizacije na svetovni ravni[9] (več podatkov nudi več vzvodov moči) in naraščajoči veri v moč digitalnih tehnologij oziroma vzponu tehnološkega solucionizma (Morozov, 2013).

Podatki kot »nova nafta« v času pandemije tako pritekajo iz najrazličnejših por naših raztreščenih življenj na zasebno-javne in službeno-prostočasne prostore in trenutke. Iz teh podatkov, ki so stranski produkt ali »digitalni izpušni plin« (angl. *digital exhaust*), nastaja nova ekonomija 4.0. Iz podatkov, ki naj ne gredo v nič, temveč v svojevrsten »digitalni kompost«, naj bi pridobili kar največ uvidov tudi v širjenje virusa med ljudmi.

Za razumevanje razširjanja virusa pa je treba razumeti ljudi: analiza gibanja ljudi ni cilj sam po sebi, cilj je identificirati in razumeti stike med ljudmi, razumeti družbene mreže. To razumevanje se lahko uporabi za razumevanje virusa in njegovega potovanja po populaciji, uporablja pa se lahko tudi za druge poljubno izbrane (»dobre« ali »slabe«) kontingentne politične cilje. In to je mesto, kjer v razumevanje epidemiološke situacije vstopajo (ne)formalni agenti družbenega nadzora in pravna regulacija.

Učinek epidemiologije je tudi, da so se subjekti podatkovnega nadzora razpršili. Pandemijo so nekatera velika podatkovna podjetja »kapitalizirala« kot zmagovalci, na primer Google in Apple, ki obvladujeta trg operacijskih sistemov mobilne telefonije, oglaševalska industrija (angl. *adtech*) z več podatki o uporabnikih, in prodajne spletne platforme, na primer Amazon, Alibaba. Podatkovni nadzor zaradi povečane uporabe digitalnih storitev so okrepili ponudniki podporne »infrastrukture«, na primer telekomunikacijski operaterji. Drugi so poraženci, na primer ponudniki turističnih zmogljivosti (npr. booking.com ali Airbnb).

S korporacijskimi subjekti nadzora so v različno intenzivnih spregah (glede na čas in prostor) državni organi (obveščevalni, varnostni in zdravstveni), ki sodelujejo pri uporabi podatkovne »nove nafte«. Priča smo premreženju spreg v nadzorstveno-industrijskem kompleksu (Ball in Snider, 2013) in državljani smo pred nemogočo izbiro: ali je primerneje zaupati tehnološkima velikanoma Applu in Googlu (npr. ki sta za vsak svoj operacijski sistem pripravila aplikacijski vmesnik (angl. *application programming interface*, API), ki je podlaga za razvoj decentraliziranih aplikacij za sledenje stikov prek mobilnih naprav) ali državam (npr. Franciji in Madžarski, ki razvijata lastni centralizirani aplikaciji). V obeh primerih je aplikacija nameščena prostovoljno.

Razraščanje digitalnega družbenega nadzora v različne smeri predstavlja izzive v spremembah v delovanju akterjev formalnega in neformalnega družbenega nadzora: 1) horizontalen nadzor (angl. *lateral surveillance*) se izvaja s programi medsebojne kontrole prebivalstva kot oblike ovajanja ne-

---

[6] Raziskava Skupnega raziskovalnega središča (JRC) Evropske komisije je pokazala, da se je odstotek zaposlenih, ki so pred epidemijo vsaj občasno delali od doma, od leta 2009 vseskozi počasi povečeval in je lani obsegal 15 % vseh zaposlenih. V času pandemije je ta odstotek naglo narasel na 25 %, po nekaterih podatkih pa celo 40 % zaposlenih. Slovenija je bila sicer poleg Estonije, Portugalske in nordijskih držav identificirana kot država z največjim deležem delavcev, ki so že pred pandemijo covida-19 delali od doma (European Commission, 2020b).

[7] Pandemijo definiramo kot epidemijo, ki se pojavi na svetovni ravni ali skozi večje geografsko območje, preči državne meje in tipično prizadene veliko število ljudi (Svetovna zdravstvena organizacija [WHO], 2011).

[8] Endemijo definiramo kot pandemijo, ki je »ušla izpod nadzora«, kar pomeni, da je ni več mogoče točno geografsko locirati in zajeziti. Za tipičen primer pretekle pandemije velja endemična razširitev virusa HIV (Brenza, 2020).

[9] Po podatkih Statističnega urada Republike Slovenije (SURS) v Sloveniji raste tako raba interneta kot tudi (pametnih) mobilnih naprav. Leta 2019 je internet redno uporabljalo 83 % ljudi (SURS, 2019), leta 2015 pa 10 % manj (73 % prebivalstva) (SURS, 2015). Že od leta 2008 imamo v Sloveniji več mobilnih telefonov kot prebivalcev – leta 2019 je bilo teh že petino več (119-odstotna stopnja penetracije mobilne telefonije). Povečala se je tudi količina prenesenih mobilnih podatkov, do spleta pa prek mobilnih telefonov dostopa 73 % prebivalstva (SURS, 2020).

zakonitega združevanja ljudi, ki kršijo odloke o maksimalnem številu skupin ljudi, v Rimu tako na primer deluje aplikacija za anonimno prijavo nedovoljenega združevanja ljudi (Zajc, 2020); 2) nadzor od spodaj navzgor (angl. *sous-veillance*), primer je predlog »protikorupcijske aplikacije« kot oblike nadzora državljanov nad državnimi funkcionarji (Kovačič, 2020b), in 3) javno-zasebni oziroma participativni nadzor, v katerem prebivalci skupaj z oblastmi izvršujejo nadzor. Na primer v mestu Cuneo na severozahodu Italije lahko krajani v mrežo kamer, ki jih je postavila policija, vključijo svoje zasebne kamere, da bi tako mreža prekrila večino ulic (Zajc, 2020).

Članek sledi lijakasti strukturi: najprej prikaže spremembe družbenega nadzora, pri čemer je poudarek na novih digitalnih tehnologijah »odrešitve« in digitalnem nadzoru, uporabljenem po svetu za vzpostavitev ali nadziranje fizične distance. Nato prikaže različne tehnologije za sledenje, njihove prednosti in pomanjkljivosti, v osrednjem delu pa se osredotoči na tri vrste izzivov digitalnega nadzora prek aplikacij za sledenje stikov oziroma beleženje bližine med posamezniki (angl. *contact tracing*, *proximity tracing*): tehnološke, pravne in etične izzive tovrstnega sledenja ljudi oziroma njihovih stikov ali njihove fizične razdalje.

2 Intenziviranje digitalnega nadzorovanja po svetu

Tehnološki entuziasti proučujejo različne načine, kako prepoznati okuženost posameznika brez telesnega stika »na daljavo« iz biometričnih značilnosti posameznika. Iskanje glasovnih biomarkerjev covida-19 se na primer nanaša na analizo govora, ki naj prepozna okužbo z virusom, kar je oblika profiliranja posameznika – cilj je razumeti, kako posameznikov govor ustreza predhodno oblikovanim profilom »okuženega« govorca. Analize se nanašajo tudi na različne druge zvoke in glasove, ki jih (hote ali nehote) spuščajo telesa, na primer analizo kašlja: ideja je te glasove prestreči z nameščanjem mikrofonov v predmete vsakodnevne rabe za identifikacijo različnih bolezni in motenj. V ta namen je v Izraelu ministrstvo, pristojno za obrambo, skupaj z zagonskim podjetjem Vocalis Health ljudi pozvalo k donaciji posnetkov svojih glasov (Anthes, 2020), da bi identificirali poseben »glasovni odtis« obolelih za covidom-19 (npr. težko dihanje med govorom), do katerega bi prišli z metodo strojnega učenja, ki bi razpoznala razlike v govoru med zdravimi in bolnimi posamezniki.

Primer glasovnih biomarkerjev odstira ideologijo tehnološkega solucionizma: »nismo še na cilju, potrebnih je več podatkov«; »tehnologija je zgolj pomagalo«, »nihče si ne domišlja, da bi odločala tehnologija sama«. Vendarle iz raziskav na drugih področjih avtomatizacije vemo, da tehnološka orodja obdaja avra objektivnosti (v nasprotju s človeškim odločevalcem, ki se praviloma moti ter ga spremljajo številne zavestne in nezavedne hibe pri sprejemanju odločitev), hevristika predsodka avtomatizacije (angl. *automation bias*), zamenjave korelacij z vzročnimi zvezami (Završnik, 2019).

Tehnologija za uveljavljanje karantene v indijski zvezni državi Karnataka je aplikacija, ki od posameznika, ki mu je odrejena karantena, zahteva, da naloži sebek (angl. *selfie*) v vladni portal vsakih 30 minut, kar dokazuje spoštovanje samoizolacije (Gilbert, 2020). Na Kitajskem so v uporabi številne tehnologije (Mozur, Zhong in Krolik, 2020): 1) merjenje temperature na daljavo (SenseTime, 2020), 2) sistemi za prepoznavo obrazov na vhodih stavb (identifikacija obraza, pokritega z masko, merjenje telesne temperature s takojšnjo primerjavo z identifikacijskimi dokumenti), 3) sledenje z brezpilotniki, 4) podatkovni nadzor prek dveh podjetij z največ podatki (Alibaba in Tencet prek mega aplikacije WeChat) itd. Pa vendar je Kitajska v prvem spomladanskem valu pandemije kombinirala tehnologijo s strogim režimom zapiranja (npr. stanovanja, zapečatena za celomesečna obdobja), zaprtjem meja in okrepljenim ročnim sledenjem stikov. Podpora javnemu zdravstvenemu sistemu je bila močna, le malo je bilo prepuščenega posameznikovi izbiri ali odgovornosti, bolni so bili takoj odstranjeni in nameščeni v državnih klinikah (Hessler, 2020). Veliko vlogo so imeli tudi dotlej že pozabljeni sosedski odbori, ki so opravljali oblike neformalnega nadzora nad izvajanimi ukrepi.

Azijski model soočanja s pandemijo koronavirusa je pokazal nove razsežnosti kombinacije tehnologije s človeškimi sledilci stikov. V Singapurju je predsednik vlade kot glavni razlog za uspeh navajal tradicionalno detektivsko delo, ki je bilo ključno za uspešno zajezitev širjenja virusa (intervjuji z okuženimi in izsledite oseb, ki so bile v stiku z okuženimi osebami), vodja njihove aplikacije TraceTogether pa je javno izrazil dvom o njeni učinkovitosti (npr. aplikacijo si je namestil vsak šesti prebivalec) (Dayaram, 2020). Poleg detektivskega dela je Singapur kril stroške celotne zdravniške oskrbe in testov, ki so bili izjemno razširjeni in lahko dostopni, osebam z odrejeno samoizolacijo pa zagotovil denarno nadomestilo. Južna Koreja je postavila najmanj ovir pri uporabi najrazličnejših podatkov (Schmitt, 2020): lokacijske podatke za sledenje pacientov so zbirali telekomunikacijski operaterji in izdajatelji kreditnih kartic.

V Evropi oblike tehnološko okrepljenega nadzora niso bile izjemno drugačne, čeprav je bilo največ prizadevanj za izgradnjo aplikacij za sledenje stikom. Predvsem je razvoj tehnoloških rešitev v evropskem prostoru potekal z mislijo na varstvo temeljnih pravic posameznikov. Medtem ko azijskim državam z drugačnim kulturnim, sistemskim in pravnim ozadjem množični nadzor ni tuj, bi ekstenzivno zbiranje osebnih podatkov

nasprotovalo uveljavljenim standardom varstva pravic, predvsem pravice do zasebnosti in varstva osebnih podatkov, kot ga poznamo v državah evropskega pravnega prostora. V Italiji so tako na primer kljub načeloma drugačnemu pravnemu redu v primerjavi z azijskim modelom v uporabi brezpilotni letalniki, ki nagovarjajo mimoidoče in jim s termokamerami samodejno merijo telesno temperaturo, in tehnologija prepoznavanja obrazov. Ta zaznava domnevno sumljive vedenjske vzorce (npr. posedanje dlje časa na določenem območju), išče izginule predmete, šteje ljudi, prepoznava hitrost in smer njihove hoje, razločuje ljudi glede na barvo njihove polti. V Lombardiji so krajevne oblasti v sodelovanju z mobilnimi operaterji sledile premikom prebivalcev prek GPS njihovih pametnih telefonov, sistem pa lahko sledi 85 % celotne populacije (Zajc, 2020).

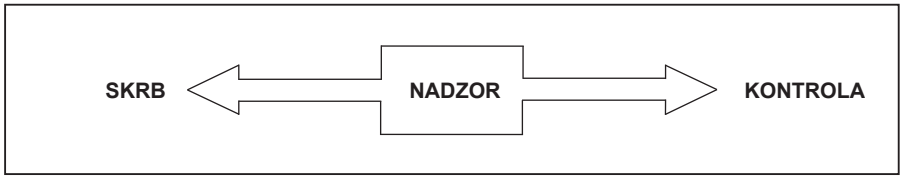
»Naravni« trend pri razvoju aplikacij za sledenje stikom oziroma fizične bližine ljudi, ki so bile najprej razvite in vodene na nacionalni ravni, je, da postajajo interoperabilne. V jesenskem valu pandemije v letu 2020 je Evropska komisija vzpostavila interoperabilnostno shemo (angl. *interoperability gateway*) (European Commission, 2020a) oziroma storitev, ki bo povezala nacionalne aplikacije po Evropi, k shemi pa so pristopile najprej le tri države (brez možnosti povezave aplikacij centraliziranega tipa, kot ga razvijata Francija in Madžarska) (Bicheno, 2020).

Kreativnost tehnologov, ki se čutijo poklicane za reševanje številnih (tudi povsem družbenih) problemov, kaže, kako težko je ločiti ambicije (kaj bi lahko storili?) od nujnosti (kaj moramo storiti?) in kako sploh razumeti problematične oblike nadzora. Namreč, razlika je med nadzorom, katerega cilj je na anonimiziran način razumeti človeške družbene mreže na eni strani, ter družbenim mreženjem, ki razkriva osebne podatke, povečuje ranljivosti že tako ranljivih skupin in povečuje nesorazmerje družbene moči na drugi. Razlikovanje med nujnim zdravstvenim nadzorom (skrb za drugega) in policijskim nadzorom (kontrola drugega), med policijsko uro in epidemiološko uro je nemogoče *in abstracto* določiti, podobno kot razlikovanje nadzora na delovnem mestu, ki zasleduje cilj zagotavljanja zdravja in varnosti pri delu od nadzorovanja delavcev (npr. z vidika učinkovitosti, kontrole stikov z zunanjim svetom). V srčiki te razlike odstirajo samo naravo družbenega nadzorovanja: konkreten družbeni nadzor je mogoče postaviti na premico med skrbjo (za nekoga) in kontrolo (nad nekom) (slika 1).

Konkretne oblike tehnološko okrepljenega družbenega nadzora po svetu kažejo tudi težavo časovne omejenosti. Vsaj teroristični napadi 9/11 kažejo, kako se je tehnološki nadzor razvil, razširil in ostal: večmilijonski program množičnega (neosredotočenega) nadzora na telefonsko infrastrukturo, ki je pregledoval meta podatke milijonov posamičnih telefonskih številk, je po podatkih *New York Timesa* vodil le do dveh izvirnih preiskav (Dibble, 2020).

3 Rabe digitalne tehnologije za sledenje

Komu ali čemu aplikacije za sledenje sledijo? Pojem sledenja se je v kontekstu uporabe aplikacij za sledenje zaradi implikacije, da gre za množični nadzor prebivalstva, začel spreminjati. Evfemistični nadomestki služijo pravnemu rahljanju dosedanjih pravnih omejitev pri izvajanju nadzora. Sledenje prebivalstvu naj ne bi bil cilj oblasti: sledi se virusu, medosebnim »kontaktom« (angl. *contact tracing*) ali še manj od tega, sledi se le »bližini« (angl. *proximity tracing*). Z vidika varovanja posameznikove zasebnosti tako prihaja do luščenja tega, kaj naj štejemo za varovanje zasebne sfere posameznika, ker naj se z izvajanjem sledenja »kontaktom« osebe ne bi sledilo osebi »kot taki«. To implicitno temelji na predpostavki, da stiki niso del posameznikove pravno varovane zasebne sfere. Analogno, v kontekstu kazenskega pregona, bi to pomenilo, da policija ne potrebuje preiskovalnega naloga sodišča za sledenje, če jo zanima »zgolj« sledenje stikom, ne pa tudi sledenje »osebi sami«, oziroma še toliko manj, če je osredotočena le na sledenje predmetom (npr. prepovedanim drogam). Očitno bi moralo biti, da je tako luščenje plasti zasebnosti in reducira-



Slika 1: Pojem nadzora (vir: lasten)[10]

[10] Nadzor se giblje med "negativno" kontrolo in "pozitivno" skrbjo. Ni "črno-bel", temveč je nekje na premici med obema skrajnostima. Npr. v primeru nadzora na delovnem mestu, vodstvo lahko nadzoruje zaposlene v skrbi za njihovo zdravje oz. to celo mora početi v skladu z delovno pravno zakonodajo. Vendar se ta legitimen nadzor (angl. surveillance) premakne od "pozitivne" skrbi (angl. care) v "negativno" kontrolo (angl. control) (npr. če vodstvo prebira e-pošto podrejenim).

nje osebe na nekaj, kar ne obsega tudi njenih osebnih stikov in komunikacije, problematično: varovanje posameznikove zasebnosti obsega pojmovno tudi njene stike, ti odnosi so del tega, kar tvori posameznikovo osebnost in kar ščiti pravica do zasebnosti. Komunikacijska zasebnost je, kot je že odločilo na primer Evropsko sodišče za človekove pravice (ESČP) v zadevi Malone proti Združenem kraljestvu[11] (Malone v. the United Kingdom, 8691/79), sestavni del pravice do zasebnosti. Osebni odnosi z drugimi so tisto, kar tvori bistvo posameznika (človek je odnosno bitje), razkrivanje osebnih stikov z drugimi ljudmi zato pomeni poseg v posameznikovo zasebnost.[12]

V prizadevanjih za uveljavitev omejitev mobilnosti v najmanjši možni meri in razumevanje prenosa okužb so se podatki o rabi mobilnih telefonov pokazali kot možni vektor približevanja razumevanju prenosa virusnih okužb. Načini sledenja mobilnim telefonom, ki so jih države razvile v boju zoper koronavirus, so bili do zdaj izjemno različni, ker so temeljili na različnih vrstah podatkov in ker so se podatki analizirali na različne načine (centralizirano proti decentralizirano): 1) bazne postaje mobilne telefonije pokrivajo velik del ozemlja, a imajo nizko stopnjo lokacijske natančnosti; 2) tehnologija GPS je v telefonih sicer bolj natančna (še vedno pa lahko locira napravo le do pet metrov natančno), a ne deluje v notranjih prostorih; 3) desetletje stara raba tehnologij Bluetooth in WiFi[13], ki se je že uporabljala za lokacijski marketing v trgovinskem sektorju, se je zdela primerna.

Tehnologija Bluetooth, brezžična tehnologija za povezovanje različnih digitalnih elektronskih naprav na razdaljah do 400 metrov, se je pri tem pokazala kot tista, ki naj iz stikov med napravami omogoči sklepanje na stike med ljudmi. Čeprav je bila tehnologija bolj obrobnega pomena v tehnološkem svetu, ustvarjena za popolnoma druge cilje (kjer pogosto ni delovala zadovoljivo niti za svoj primarni namen),[14] je bila ideja privlačna. Kot meni Anderson (2020), so vlade in tehnologi hitro zapadli v napako v silogističnem sklepanju: 1) Nekaj moramo narediti. Aplikacije so nekaj. 2) Torej, moramo jih razviti in uporabiti. Tehnologi so tako predlagali tehnično rešitev za nekaj, kar je primarno družbeni problem, oblasti pa so zaigrale »teater zdravja« kot dokaz, da nekaj vendarle počno.

Ideja o napravah, ki same izračunavajo bližino po vnaprej nastavljenih parametrih, na primer kakšen stik naprav naj šteje za epidemiološko relevanten (npr. če gre za stik naprav v trajanju več kot X minut in na razdalji naprav manj kot Y metrov, kar določi epidemiološka stroka glede na poznavanje načina prenašanja virusa po zraku), je privlačna. Zlasti ker obstajajo načini izračunavanja stikov na način, da podatki ne bi bili preneseni k državnim organom (npr. zdravstvenim oblastem ali represivnim organom), če pa bo prenos podatkov (tehnološko) nujen, bo kriptiran.[15]

Na svetu obstaja že več kot 80 aplikacij, ki se razlikujejo po številnih vidikih,[16] glede na cilje pa jih lahko razdelimo na: 1) aplikacije za nadzor upoštevanja karantene (angl. *quarantine compliance* oz. *quarantine enforcement*); 2) za nadzor simptomov ter 3) za beleženje fizične bližine in sledenje stikom (angl. *proximity tracing; contact tracing*).

Pri prvih aplikacijah za nadzor upoštevanja karantene gre za *osredotočen nadzor* znanih okuženih oseb. To je bistveno za presojo njihove legitimnosti in Evropsko sodišče za človekove pravice je te vrste nadzora že presojalo. Omejitve svobode gibanja so dovoljene, kot je odločilo v nosilnem primeru o omejitvah pravic v karanteni (Enhorn v. Sweden, 56529/00). Sodišče je sicer v tem primeru ugotovilo kršitev pravice, ker je ukrep karantene trajal kar sedem let in Švedska ni dokazala, da blažji ukrepi niso bili mogoči. Odločilo pa je tudi, da gre pri tovrstnem omejevanju za poseg v zasebnost, ki pa mora biti: *zakonit*, *nujen, sorazmeren* in časovno omejen – *začasen*.

---

[11] Podobno je tudi Ustavno sodišče Republike Slovenije, sklicujoč se na sodbo ESČP Malone proti Združenemu kraljestvu, odločilo, da so kot sestavni del telefonskih komunikacij zaščiteni tudi podatki o klicanih telefonskih številkah: »Podatke, ki so razvidni iz izpisa telefonskega spomina, je treba glede na njihovo naravo obravnavati kot sestavni del komunikacijske zasebnosti. Zato pomenita pridobitev podatkov o zadnjih opravljenih in zadnjih neodgovorjenih klicih ter vpogled v vsebino sporočila SMS vpogled v vsebino in okoliščine komunikacije ter s tem poseg v pravico iz prvega odstavka 37. člena Ustave.« (Up-106/05). Če so to podatki o klicanih številkah, tudi če zveza ni bila vzpostavljena, to pomeni, da so zaščiteni podatki tudi o »stikih« in »bližini« pri sledenju stikom in merjenju »bližine«.

[12] Vprašanje, ali je poseg upravičen, je od tega ločeno vprašanje, ki zahteva tehtanje različnih pravic. Na tem mestu je ključna ugotovitev, da gre za poseg (v pravico do zasebnosti).

[13] WiFi je brezžična tehnologija, ki omogoča, da se lahko naprava poveže v računalniško omrežje, za svoje delovanje proizvaja naslov MAC (Media Access Control), ki je edinstveno določilo, ki jo je proizvajalec dodelil omrežni strojni opremi. Naslova MAC po navadi ni mogoče spreminjati, zato se je uporabljal za vohunjenje. Vendar pa je zaradi množičnega nadzora, ki ga je razkril E. Snowden, industrija začela uporabljati naključne naslove MAC v svojih napravah, da bi se izognili sledenju in spremljanju države. Vendar pa to spreminjanje ni brez cene: MAC je mogoče zlonamerno spremeniti in s tem vplivati na varnost omrežja (t. i. MAC spoofing).

[14] Izumitelja Bluetootha, inženirja pri švedskem Ericssonu, Jaap Haartsen in Sven Mattisson, sta izrazila dvom o njeni natančnosti.

[15] Vendar je anonimnost sledenja s tehnologijo Bluetooth vprašljiva. Na to kažejo analize trga lokacijskega marketinga, ki deluje prek nameščenih svetilnikov Bluetooth (angl. *Bluetooth beacons*), saj je več raziskav dokazalo možnost deanonimizacije in razkrivanja lokacijskih podatkov uporabnikov. Bluetooth je lahko vektor možnega napada in razkrivanja lokacijskih podatkov (Curtis, 2015).

[16] Pregleden prikaz ponuja »*Covid Tracing Tracker*«, ki ga je vzpostavil MIT.

Oblike nadzora nad upoštevanjem karantene se danes že izvajajo tudi z »elektronskimi zapestnicami« (angl. *electronic monitoring* – EM), kar so v številnih kazenskopravnih sistemih poznali do zdaj zgolj kot obliko kazenske sankcije, kot obliko predčasnega odpusta s prestajanja kazni zapora ali kot obliko varščine (omejevalni ukrep).[17] Na primer elektronski nadzor z biometričnimi tehnologijami izvajajo v Liechtensteinu z elektronskimi zapestnicami (Pascu, 2020). Prav tako je v Južni Koreji načrtovana uvedba sledilnih zapestnic, ker so ugotovili, da ljudje telefone puščajo doma in vseeno kršijo karanteno. Tehnologija omogoča tudi določanje dodatnih storitev, kot je vzpostavitev navidezne geografske meje, ustvarjene na zemljevidu znotraj aplikacije (angl. *geofencing*), tako da aplikacija spremlja lokacijo posameznika in pri prečkanju navidezne meje sproži nadaljnje ukrepe (npr. ob odhodu več kot X metrov od doma oseba prejme opozorilni klic).

Druga oblika nadzora z uporabo aplikacij je *neosredotočen nadzor celotnega prebivalstva* kot skupka potencialno okuženih posameznikov. Presoja legitimnosti je pri uporabi teh aplikacij odvisna od več dejavnikov, zlasti od vrste podatkov, ki se obdelujejo, mesta obdelovanja, kdo ima dostop do podatkov itd. V Južni Koreji in Izraelu na primer aplikacije za sledenje uporabljajo lokacijske podatke pametnih telefonov, podobno kot na Norveškem, kjer je organ za varstvo osebnih podatkov začasno prepovedal nadaljnjo uporabo aplikacije za sledenje koronavirusu (Chadwick, 2020). Ta je temeljila na lokacijskih podatkih GPS in tehnologiji Bluetooth, ampak je nesorazmerno posegala v varstvo osebnih podatkov zaradi kontinuiranega beleženja lokacijskih podatkov in informacij o osebnih stikih uporabnikov.[18]

Presoja množičnega nadzora z aplikacijami za beleženje stikov je odvisna od številnih parametrov delovanja aplikacije. S tehnološkega vidika je pomemben razvoj protokola DP-3T (angl. *decentralized privacy-preserving proximity tracing*) ter zakulisnega boja med centraliziranimi in decentraliziranimi aplikacijami za sledenje. Za delovanje DP-3T ne potrebuje lokacijskih podatkov, pač pa tehnologijo Bluetooth, stiki so psevdonimizirani prek kod (uporabnik ne ve, kdaj ali kje je bil v stiku z okuženo osebo), v centralni strežnik aplikacija pošilja naključne kode, ki se spreminjajo vsakih 15 minut, brez centralne zbirke, ki bi lahko identificirala ljudi, številke (kode) drugih naprav v stiku pa so shranjene le lokalno na uporabnikovi napravi – ker se preračunavanje odvije lokalno, je ta aplikacija decentralizirana (Troncoso et al., 2020).

Kljub tehnološko dovršeni in obetavni rešitvi DP-3T, ki jo je oblikovalo več kot deset evropskih univerz, je to le sestavni del aplikacije za sledenje.[19] Protokol in njegovo idejo sta prevzela tudi Google in Apple (Nellis in Dave, 2020), ki sta na lastnih operacijskih sistemih pripravila aplikacijski vmesnik (API) za razvijalce aplikacij. Ker je protokol zgolj osnova za izdelavo aplikacije, je nujen, ne pa tudi zadosten pogoj za primerno varstvo pravic posameznika pri uporabi aplikacij za sledenje. Tudi DP-3T je mogoče zlorabiti, na primer, če države uporabijo aplikacijo (zasnovano na njegovi osnovi) kot obvezno prepustnico s kazalcem tveganja, na primer za omogočanje dostopa do delovnega mesta ali pri življenjsko nujnih opravilih.

V nadaljevanju analiziramo pravne in tehnološke izzive ter nato pokažemo pogoje, ki lahko vodijo k oceni, ali je konkretno sledenje etično legitimno.

4 Pravni in tehnološki vidiki družbenega nadzora v dobi covida-19: študija primera aplikacij za sledenje stikom okuženih s covidom-19

4.1 Pravni vidiki

Aplikacije za sledenje stikom okuženih s covidom-19 predstavljajo grožnjo pravici do zasebnosti in varstva osebnih podatkov. Pravici do zasebnosti in varstva osebnih podatkov, kot ju določajo mednarodni, regionalni in nacionalni pravni akti, sicer nista absolutni pravici in se lahko pod določenimi pogoji omejita. Pandemija covida-19 gotovo predstavlja izredno situacijo, ki od držav zahteva ukrepanje z namenom varovanja zdravja prebivalstva ter lahko vključuje tudi posege v pravno varovane pravice in svoboščine, vendar pa so tudi v izrednih razmerah države dolžne izpolnjevati predpisane materialne in postopkovne pogoje, pod katerimi so take omejitve dopustne. Mednarodni pakt o državljanskih in političnih pravicah (1992) v 4. členu in Evropska konvencija o človekovih pravicah (1994) v 15. členu tako izrecno predvidevata možnost razveljavitve (derogacije) nekaterih pravic v obsegu, ki ga izredno stanje zahteva. Do vključno septembra 2020 je zaradi razglasitve pandemije covida-19 to možnost uporabilo deset držav pogodbenic Evropske konvencije o človekovih pravicah, to so Latvija, Romunija, Armenija, Moldavija,

[17] Elektronski nadzor so že pred dvema desetletjema sprejele Velika Britanija, Švedska, Nizozemska, Belgija, Francija, Portugalska, Nemčija in Švica (Meyer, Haverkamp in Lévy, 2002).

[18] Izredno problematične rabe, ki popolnoma nasprotujejo evropskemu režimu prava varstva osebnih podatkov in zasebnosti, se pojavljajo v ZDA: uslužbenci zdravstvenega sistema tam pridobivajo velike količine lokacijskih podatkov od zelo ohlapno reguliranih spletnih oglaševalcev, razprave pa potekajo z Googlom.

[19] Druga evropska pobuda za izgradnjo protokola za korona aplikacije je PEPP-PT (*Pan-European Privacy-Preserving Proximity Tracing*), ki pa se je izkazala za problematično zaradi centraliziranega shranjevanja podatkov.

Estonija, Gruzija, Albanija, Severna Makedonija, Srbija in San Marino, ki pa so konvencijske pravice derogirale v različnem obsegu (Zghibarta, 2020). V sodobni zgodovini ni mogoče najti krize, ki bi pripeljala do primerljivega števila derogacij temeljnih človekovih pravic na globalni ravni (Scheinin, 2020). Izčrpen odgovor na vprašanje, ali je derogacija določenih človekovih pravic v primeru pandemije ne samo utemeljena, temveč tudi pravilna odločitev, presega obseg pričujočega članka. Greene (2020) na primer zagovarja pozitiven učinek derogacije s tem, da zanjo zahtevani pogoji pravzaprav omejujejo moč in samovoljo držav v izrednih situacijah ter pripomorejo k učinkovitemu varstvu človekovih pravic (Neuman, 2016). Njeni nasprotniki na drugi strani opozarjajo na možnost zlorabe razglasitve izrednih razmer in posledične razveljavitve človekovih pravic v politične namene, na primer za zatiranje nasprotnikov vladajočega režima ali odpravo temeljnih demokratičnih procesov in kavtel. Scheinin (2020) za omejevanje zlorab predlaga dosledno spoštovanje načela normalnosti (angl. *principle of normalcy*), v skladu s katerim tudi v kriznih situacijah, na primer ob povečani grožnji zaradi terorizma ali pandemije nalezljive bolezni, obveljajo vsi običajno vzpostavljeni temeljni demokratični postopki, pooblastila državnim organom ter uveljavljene temeljne pravice in svoboščine, ki se lahko omejijo ob doslednem spoštovanju načela nujnosti in proporcionalnosti.

Omejitve človekovih pravic so mogoče tudi brez tega najbolj skrajnega ukrepa, medtem ko absolutnih pravic, na primer pravice do življenja in prepovedi mučenja, tudi derogacija ne more odpraviti ali omejiti. Evropska konvencija o človekovih pravicah tako v 8. členu, ki v prvem odstavku določa pravico posameznika do zasebnega in družinskega življenja, v drugem odstavku ureja dopustne posege v to pravico, ki se lahko omeji, če je to »določeno z zakonom in nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi« (Evropska konvencija o človekovih pravicah, 1994). Podobne pogoje za omejevanje pravic določa tudi prvi odstavek 52. člena Listine Evropske unije o temeljnih pravicah (2012): »Kakršnokoli omejevanje uresničevanja pravic in svoboščin, ki jih priznava ta listina, mora biti predpisano z zakonom in spoštovati bistveno vsebino teh pravic in svoboščin. Ob upoštevanju načela sorazmernosti so omejitve dovoljene samo, če so potrebne in če dejansko ustrezajo ciljem splošnega interesa, ki jih priznava Unija, ali če so potrebne zaradi zaščite pravic in svoboščin drugih.«

Omejitev pravice do varstva osebnih podatkov je v sekundarni zakonodaji EU konkretizirana v 23. členu Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov), ki predstavlja mehanizem za vzpostavitev ravnovesja med pravico do varstva osebnih podatkov na eni strani in drugimi legitimnimi interesi države na drugi (Kuner, Bygrave, Docksey in Drechsler, 2020). Razlogi, ki lahko terjajo omejevanje pravic posameznika, v 23. členu Splošne uredbe o varstvu podatkov niso omejeni na ravnanje držav kot posledico razglašenih izrednih razmer, temveč so določeni taksativno, a hkrati izredno široko in vključujejo tudi zagotavljanje javnega zdravja (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). Omejitev mora biti določena v zakonu, ne sme posegati v bistvo pravice do varstva osebnih podatkov ter mora biti nujno in sorazmerno sredstvo za doseganje vsaj enega izmed navedenih ciljev. Pri presoji, ali sta izpolnjena pogoja nujnosti in sorazmernosti, se upošteva časovni in družbeni okvir uvedenih ukrepov, ki v nobenem primeru ne morejo biti absolutne in trajne.[20] To je potrdil tudi Evropski odbor za varstvo podatkov v kontekstu boja proti pandemiji covida-19 (European Data Protection Board [EDPB], 2020a). Velika večina držav članic EU se kljub grožnji pandemije ni odločila za tako drastičen ukrep. Edina država, ki je to možnost izkoristila, je Madžarska, ki je na podlagi vladne uredbe 179/2020 z dne 4. 5. 2020 v času razglašenih izrednih razmer glede vseh osebnih podatkov, ki se obdelujejo z namenom odkrivanja, razumevanja in preprečevanja širjenja koronavirusa, suspendirala uresničevanje pravic iz 15. do 22. člena Splošne uredbe o varstvu podatkov (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). Odločitev madžarske vlade je bila deležna ostre kritike EDPB (2020a), zakonitost vseh ukrepov v času pandemije pa je pod drobnogled vzela tudi Evropska komisija (Makszimov, 2020). EDPB je ob tem izpostavil, da obstoj pandemije ali katerega koli drugega izrednega stanja še ne more samo po sebi utemeljevati omejevanja pravic posameznikov, na katere se podatki nanašajo. Evropski regulatorni okvir varstva osebnih podatkov je kljub visoko

[20] Drugačno stališče zastopa Tina Kraigher Mišič v Komentarju Splošne uredbe o varstvu podatkov (Pirc Musar et al., 2020), ki navaja, da so omejitve izjemoma lahko absolutne in trajne. Vsaj glede absolutnosti že sama Splošna uredba o varstvu podatkov tega ne dopušča, saj morajo vsakršne omejitve spoštovati bistvo pravice do varstva osebnih podatkov, nadalje pa morajo zakonodajni ukrepi, ki predvidevajo omejitev pravice, vsebovati vsaj vse zahteve, ki so navedene v drugem odstavku 23. člena (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016).

postavljenim zahtevam glede varstva pravic posameznikov in dolžnosti upravljavcev dovolj fleksibilen, da omogoča učinkovito odzivanje na (zdravstvene) krize (EDBP, 2020a).

Za odgovor na vprašanje, ali so aplikacije za sledenje okuženim s covidom-19 in nekatere druge aplikacije, ki so jih razvile države v boju s koronavirusom, skladne s tem okvirom, je ključno, katere podatke obdelujejo in ali ti spadajo v kategorijo (občutljivih) osebnih podatkov v skladu z definicijo Splošne uredbe o varstvu podatkov. Kljub opozorilom, da je za ohranitev visoke stopnje varstva osebnih podatkov in za zaščito zasebnosti posameznikov nujno, da aplikacije, uporabljene v boju proti koronavirusu, zbirajo le anonimizirane podatke, na eni strani, ter obljubam razvijalcev tehnoloških rešitev, da bo zasebnost uporabnikov glavno vodilo razvoja, na drugi, pa aplikacije, ki so trenutno v uporabi v Evropski uniji, kažejo drugačno sliko. Ocena učinka nemške aplikacije Corona-Warn-App, na kateri temelji tudi slovenska aplikacija #OstaniZdrav, navaja ne le, da aplikacija obdeluje osebne podatke, temveč da obdeluje posebne kategorije osebnih podatkov (Bock et al., 2020), tj. občutljive osebne podatke, ki so v skladu s Splošno uredbo o varstvu podatkov deležni posebne zaščite. To potrjujejo tudi poročila več nadzorstvenih organov za varstvo osebnih podatkov, na primer francoskega Commission Nationale de l›Informatique et des Libertés (CNIL, 2020) in slovenskega Informacijskega pooblaščenca (2020). Aplikacije za sledenje stikom okuženih s covidom-19 se razlikujejo v obsegu kategorij podatkov, ki jih obdelujejo, vendar pa velika večina vendarle obdeluje osebne podatke, ki so kvečjemu psevdonimizirani.[21] Ti se pogosto zamenjujejo za anonimizirane podatke (EDPB, 2020b), vendar pa je z vidika prava varstva osebnih podatkov med njima ključna razlika: psevdonimiziranih podatkov samih po sebi ni mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, je pa to mogoče storiti z uporabo dodatnih informacij, zato imajo še vedno naravo osebnih podatkov. Anonimiziranih podatkov za razliko od osebnih podatkov ni mogoče povezati z določenim ali določljivim posameznikom, tj. posameznikom, ki ga je mogoče določiti neposredno ali posredno. Iz uvodne opombe 26 dodatno izhaja, da anonimizirani niso samo podatki, ki jih v nobenem primeru ne bi bilo mogoče povezati z določenim ali določljivim posameznikom, ampak so to tudi podatki, ki onemogočajo identifikacijo »*z uporabo vseh sredstev, za katera se razumno pričakuje, da jih bo upravljavec ali druga oseba uporabila za neposredno ali posredno identifikacijo posameznika*« (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). Anonimizacija mora onemogočiti povratno identifikacijo posameznika, na katerega se podatki nanašajo, ne le upravljavcu, temveč tudi vsem ostalim (Article 29 Data Protection Working Party, 2014). Odgovor na vprašanje, ali gre za anonimiziran podatek ali osebni podatek, se lahko spreminja v času (Article 29 Data Protection Working Party, 2014) – zaradi povečanja računalniške zmogljivosti in napredka različnih tehnik umetne inteligence je mogoče pričakovati, da bo vsaj nekatere podatke, ki danes veljajo za anonimizirane, in zato trajno ločene od posameznikov, na katere se nanašajo, v prihodnosti mogoče spet povezati z njimi in jim vrniti naravo osebnih podatkov (Bradford, Aboy in Liddell, 2020). To stopnjo anonimnosti je dejansko izredno težko doseči (EDPB, 2020b; Article 29 Data Protection Working Party, 2014).

Nadalje se postavlja vprašanje, ali katero izmed kategorij podatkov, ki jih obdelujejo aplikacije za sledenje stikom, uvrščamo med posebne vrste osebnih podatkov, obdelava katerih je zaradi njihove posebej občutljive narave dovoljena le pod strogo določenimi pogoji. Splošna uredba o varstvu podatkov v 9. členu nudi posebno zaščito podatkom, ki razkrivajo informacije o preteklem, sedanjem ali prihodnjem telesnem ali duševnem zdravstvenem stanju posameznika, vključno s podatki o njegovih boleznih ali tveganjih za nastanek bolezni. Vsaj koda, ki jo posameznik dobi od pooblaščenega zdravstvenega osebja v primeru pozitivnega testa na covid-19 in mu omogoča vnos okužbe v aplikacijo, je občutljiv osebni podatek (Bock et al., 2020). Obdelava te vrste osebnih podatkov je prepovedana, razen če velja ena od izjem iz drugega odstavka 9. člena Splošne uredbe o varstvu podatkov. Med drugim je skladno z drugim odstavkom obdelava dovoljena, če posameznik, na katerega se podatki nanašajo, vanjo veljavno privoli ali pa je taka obdelava potrebna zaradi bistvenega javnega interesa, če je sorazmerna z zasledovanim ciljem, ne posega v bistvo pravice do varstva osebnih podatkov ter so hkrati zagotovljeni ukrepi za zaščito temeljnih pravic in interesov posameznika, na katerega se občutljivi podatki nanašajo (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016).

Obdelava osebnih podatkov mora, zato da je zakonita, temeljiti na eni izmed pravnih podlag iz 6. člena Splošne uredbe o varstvu podatkov. Tako kot v primeru obdelave ob-

[21] Psevdonimizacija je v Splošni uredbi o varstvu podatkov opredeljena kot »obdelava osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku« (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016).

čutljivih osebnih podatkov je tudi obdelava ostalih podatkov med drugim zakonita, če posameznik, na katerega se podatki nanašajo, vanjo privoli ali če obdelavo narekuje izpolnjevanje naloge v (bistvenem) javnem interesu (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). Vprašanje pravne podlage je ločeno od vprašanja prostovoljnosti uporabe aplikacij za sledenje stikom okuženim s covidom-19. Čeprav so vsaj v državah Evropske unije aplikacije prostovoljne, je po mnenju Evropskega odbora za varstvo podatkov v primeru, ko gre za obdelavo osebnih podatkov, ki jo opravlja javni organ in je hkrati v javnem interesu, najprimernejša pravna podlaga obdelave iz člena 6(1)(e) Splošne uredbe o varstvu podatkov (»*obdelava je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu*«), ki naj ima prednost pred obdelavo na podlagi privolitve (EDPB, 2020b). Pravna podlaga je v tem primeru lahko določena bodisi v nacionalnem pravnem redu države članice ali pravnem redu EU, obdelava pa mora biti sorazmerna glede na legitimni interes, ki ga zasleduje (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). V nasprotju s priporočilom EDPB pravno podlago obdelave podatkov velike večine evropskih aplikacij za sledenje stikov predstavlja privolitev in to, čeprav predstavlja opravljanje nalog v javnem interesu ne le primerno, ampak tudi ustreznejšo pravno podlago za zakonitost obdelave podatkov teh aplikacij. Večina evropskih aplikacij za sledenje stikom temelji na programskemu vmesniku, ki sta ga razvila Google in Apple, ki v pogojih uporabe dovoljujeta le uporabo njune tehnološke rešitve za potrebe organov javnega zdravja. Upravljavci osebnih podatkov bodo v teh primerih nujno javni organi, sledenje stikom pa pomeni obdelavo podatkov v javnem interesu.

Vse aplikacije, ki obdelujejo osebne podatke na podlagi privolitve posameznika, morajo zadostiti strogim pogojem, ki jih glede veljavnosti soglasja postavlja Splošna uredba o varstvu podatkov: privolitev mora biti prostovoljna, specifična, ozaveščena in nedvoumna (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). Za prostovoljno privolitev se šteje, če ima posameznik možnost dejanske in proste izbire ter lahko privolitev zavrne ali prekliče brez škode. Pogojevanje uresničevanja določenih temeljnih svoboščin, na primer prostega gibanja ali prehoda meje, z naložitvijo aplikacije temu nasprotuje, zato tako soglasje ne izpolnjuje pogoja prostovoljnosti, kot tako pa ne šteje kot veljavna privolitev v skladu s pogoji Splošne uredbe o varstvu podatkov.

Splošni pravni akt, ki predstavlja pravno podlago za obdelavo osebnih podatkov v javnem interesu, bi moral tudi natančno predpisati namen zbiranja, shranjevanja in posredovanja zbranih podatkov, ter prepovedati kakršno koli nadaljnjo obdelavo, predvsem z namenom preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj. V nasprotnem primeru bi se lahko spremenil namen podatkovne zbirke (angl. *function creep*), ki se primarno ne bi več uporabljala za preprečevanje širjenja nalezljive bolezni, temveč bi lahko postala preiskovalno orodje v rokah represivnih organov (Kitchin, 2020). Google in Facebook sta sicer državam, ki želijo uporabiti njun vmesnik, to možnost omejila, ter jim v pogojih uporabe izrecno prepovedala kakršno koli uporabo zbranih podatkov v druge namene, vključno s preprečevanjem, odkrivanjem in preiskovanjem kaznivih dejanj in nadzorom omejevanja gibanja.

Vendar pa je za dosledno upoštevanje načela omejitve namena odgovoren upravljavec, ki mora biti tudi jasno in natančno določen. Zagotoviti mora, da so osebni podatki zbrani za določene, izrecne in zakonite namene (specifikacija namena, angl. *purpose specification*) ter se nadalje ne obdelujejo na način, ki ni združljiv s temi nameni (združljiva uporaba, angl. *compatible use*) (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). Obseg kategorij podatkov, ki se zbirajo, mora biti natančno opredeljen in v skladu z načelom najmanjšega obsega podatkov omejen le na tiste podatke, ki jih je treba zbirati, zato da se doseže legitimen cilj, ki je v javnem interesu. Aplikacije, ki delujejo na podlagi tehnologije Bluetooth, tako na primer zbirajo tudi podatek o IP naslovu uporabnika, kar je nujno za njihovo delovanje (Bock et al., 2020), zato zbiranje tega podatka ni prekomeren poseg v pravico do varstva osebnih podatkov. Prav tako te aplikacije na telefonih, ki uporabljajo informacijski sistem Android, za delovanje zahtevajo dostop do lokacijskih podatkov, čeprav jih ne zbirajo. Obdelava tovrstnih podatkov bi kršila načelo najmanjšega obsega podatkov, ker take aplikacije oddaljenost dveh posameznikov ocenjujejo na podlagi signala Bluetooth, ne pa njune lokacije, zato zbiranje te vrste podatkov presega obseg, potreben za dosego legitimnega cilja. Skladno s prvim odstavkom 25. člena Splošne uredbe o varstvu podatkov (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016) je minimizacija obsega zbranih podatkov ena izmed možnih oblik uresničevanja načel vgrajenega in privzetega (angl. *privacy by design* in *privacy by default*) varstva osebnih podatkov, saj ti narekujeta, da upravljavec s tehnološkimi in organizacijskimi ukrepi zagotavlja spoštovanje načel varstva osebnih podatkov

(Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). V primeru aplikacij za sledenje stikom okuženih s COVID-19 se poleg že omenjene omejitve zbiranja podatkov le na nujno potrebne kategorije lahko uresničuje še s psevdonimizacijo podatkov (EDPB, 2020b), decentralizirano hrambo podatkov (Rosello in Dewitte, 2020) ter avtomatiziranim izbrisom podatkov po preteku določenega obdobja hrambe, ki mora biti utemeljeno na dejanskih, objektivnih merilih medicinske stroke in omejeno na obdobje, nujno potrebno za to, da se uresničuje legitimni cilj preprečevanja širjenja nalezljive bolezni covid-19. Povprečna inkubacijska doba bolezni covid-19 je pet dni, 97,5 % vseh okuženih pa razvije bolezenske znake v 11 dnevih po okužbi (Lauer et al., 2020). Simptomi se redko pojavijo po 14 dneh po okužbi, zato Svetovna zdravstvena organizacija svetuje, naj se okuženim odredi 14-dnevna karantena. Aplikacije, ki predvidevajo tak časovni okvir hrambe podatkov, torej temeljijo na objektivnih merilih medicinske stroke, in ta ni pretiran.

Ker so aplikacije za sledenje stikom namenjene pomoči pri preprečevanju širjenja covida-19, ni dovolj le omejevanje obdobja hrambe podatkov, ki jih obdelujejo, temveč njihovega delovanja v celoti. Pravna podlaga za njihovo vzpostavitev mora vsebovati klavzulo o časovni omejenosti ukrepa (angl. *sunset clause*), ki natančno opredeljuje, do kdaj bo aplikacija delovala (EDPB, 2020b). Če tega časovnega okvira ni mogoče določiti vnaprej, bi moral biti vzpostavljen sistem rednega periodičnega preverjanja izpolnjenosti pogojev za tak ukrep.

Dodatno grožnjo zasebnosti predstavlja nepooblaščen dostop do osebnih podatkov. Čeprav popolne varnosti v spletnem okolju ni, je upravljavec podatkov dolžan z organizacijskimi in tehničnimi ukrepi zagotavljati raven varnosti, ki ustreza naravi, obsegu in namenu obdelave, tveganju in resnosti potencialnih vplivov na pravice in svoboščine posameznikov, stopnji tehnološkega razvoja ter stroškom, povezanim z zagotavljanjem te stopnje varnosti (Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES, 2016). Aplikacije za sledenje stikov obdelujejo občutljive osebne podatke velikega števila ljudi: v Nemčiji si je aplikacijo naložilo 19 milijonov uporabnikov, 1,7 milijona v Švici, v Sloveniji pa je mobilno aplikacijo do današnjega dne (19. 10. 2020) preneslo okoli 165 tisoč uporabnikov (Ministrstvo za javno upravo Republike Slovenije, 2020). Celo v Franciji, ki ima izredno majhen delež uporabnikov in posledično zanemarljivo število izdanih opozoril o tveganih stikih, to pomeni obdelavo podatkov dveh milijonov prebivalcev. Ker gre hkrati za posebej občutljive podatke o zdravstvenem stanju posameznikov, na katerega se veže uresničevanje celotnega spektra pravic posameznika, predvsem pravice do svobode gibanja, dela in izobraževanja, bi imelo lahko razkritje teh podatkov resne posledice za njihovo uresničevanje, zato se zahteva najvišja stopnja varnosti obdelave. Šifriranje in decentralizacija delno poskrbita za zagotavljanje varnosti, vendar pa glede na velika tveganja, povezana z obdelavo občutljivih podatkov velikega števila uporabnikov, ne bosta zadoščala za izpolnjevanje standardov v skladu s Splošno uredbo o varstvu podatkov, predvidene ukrepe pa bodo morali upravljavci tudi redno preverjati in dopolnjevati v skladu z razvojem tehnologije in pojavom novih groženj.

4.2 Tehnološki vidiki

Še preden se začnemo spraševati o varnosti tehnološke rešitve, je treba odgovoriti na vprašanje, ali ta sploh lahko omogoči uresničitev cilja, ki ga skuša doseči država pri njeni uvedbi, saj v nasprotnem primeru poseg v pravice in svoboščine ne bo legitimen. Anderson (2020) in Schneier (2020) opozarjata, da glavna težava aplikacij za sledenje stikom okuženih s covidom-19 niso tveganja za zasebnost in varstvo osebnih podatkov posameznikov, pač pa samo dejstvo, da nimajo nikakršne uporabne vrednosti in ne morejo doseči cilja, ki ga (domnevno) zasledujejo. Aplikacije kot odziv na širjenje pandemije so paradigmatičen primer ideologije tehnološkega solucionizma (Morozov, 2013), ki temelji na predpostavki, da je z uporabo prave računalniške kode mogoče reševati zapletena in večplastna družbena vprašanja. Tako poenostavljeno razumevanje tehnologije in nekritična vera v njene sposobnosti pogosto vodita v sprejemanje pravno in etično dvomljivih visokotehnoloških rešitev. Do tega prihaja, čeprav njihova učinkovitost sploh ni raziskana ter lahko hkrati globoko posegajo v pravice posameznika in ustroj demokratične družbe.

Niti tehnologija Bluetooth niti GPS nista bila razvita z namenom spremljanja stikov posameznikov in sta pri izvrševanju te funkcije dokaj nenatančni. Delovanje tehnologije GPS je močno odvisno od ovir v okolici, ki vplivajo na komunikacijo med mobilno napravo in satelitom, zato slabše delujejo v notranjih prostorih in v bližini visokih zgradb. Tudi v idealnem okolju brez tovrstnih ovir lahko tehnologija GPS določi lokacijo posameznika le na pet metrov, natančnost pa se močno poslabša v urbanem okolju (7–13 m). Aplikacije, ki temeljijo na tehnologiji Bluetooth, ne pridobijo podatka o lokaciji posameznika, temveč ocenjujejo stopnje ogroženosti na podlagi podatkov o oddaljenosti mobilnih naprav in času trajanja stika. Mobilne naprave za določanje razdalje med napravami uporabljajo t. i. *received signal strength indication*, ki – poenostavljeno povedano – na podlagi moči signala Bluetooth oceni oddaljenost druge naprave. Razdalja in ča-

sovno trajanje kot parametra, ki opredeljujeta tvegan stik, se določita v skladu z dognanji epidemiološke stroke, vendar pa nista enaka epidemiološkemu stiku in rezultat vsakokratnega stika naprav ne bo nujno tudi prenos virusa SARS-CoV-2. Informacija o oddaljenosti med dvema posameznikoma oziroma njunima mobilnima napravama je natančnejša od tehnologije GPS in manj odvisna od motenj v okolici, vendar pa vseeno ne more zaznati tehničnih pregrad med napravama (osebama), na primer pleksi stekla med prodajalcem in kupcem v trgovskem središču ali karoserije vozil, ki stojita drug ob drugem pred rdečo lučjo semaforiziranega križišča. Prav tako niso upoštevane druge okoliščine stika, na primer, ali je do njega prišlo na prostem ali v zaprtem prostoru, kje sta uporabnika imela mobilne naprave ter ali sta se pogovarjala in kako glasno sta govorila (Burgess, 2020). Taki in njim podobni življenjski primeri bodo ustvarili množico napačnih rezultatov, tako pozitivnih kot negativnih, od katerih je odvisna učinkovitost aplikacij za sledenje stikov. Do lažno pozitivnih rezultatov (angl. *false positives*) pride v primeru, ko aplikacija posameznika obvesti o potencialno nevarnem stiku, vendar do njega dejansko ni prišlo. Razlogi, ki lahko povzročijo napačne pozitivne rezultate, so različni. Predvsem bo do njih prihajalo zaradi že opisane premajhne natančnosti tehnološke rešitve, na kateri temeljijo. Prav tako bodo posledica neupoštevanja vseh okoliščin domnevnega prenosa, na primer fizičnih preprek med osebama, ki naj bi bili v stiku, ali nošenja zaščitne opreme, ki ne preprečuje možnosti okužbe, jo pa znatno zmanjšuje. Ne nazadnje aplikacija ne upošteva dejstva, da se virus ne prenese v vsakem primeru tveganega stika, temveč le v določenem deležu. V primeru opozorila o tveganem stiku morajo biti zato uporabnikom dana jasna navodila o nadaljnjem ravnanju, predvsem pa mora javni zdravstveni sistem vsem omogočiti pravočasno testiranje, na podlagi katerega bodo ob potrjeni okužbi dejansko napoteni v izolacijo in s tem preprečili nadaljnji prenos bolezni. Sama aplikacija brez ustrezno izobraženega prebivalstva, ki nima dostopa do brezplačnega testiranja, ne more prispevati k uresničevanju zastavljenega cilja.

V primeru napačnih negativnih rezultatov (angl. *false negatives*) uporabnik o tveganem stiku ni obveščen, čeprav je do okužbe s koronavirusom prišlo. K temu bodo enako kot v primeru napačnih pozitivnih rezultatov prispevale tehnične pomanjkljivosti tehnologije Bluetooth, še bolj pa nezadostno število uporabnikov aplikacije, ki bi omogočili, da bi ta lahko delovala učinkovito in zanesljivo. Delež državljanov, ki si je aplikacijo naložilo, je med evropskimi državami različen: največji je na Finskem in Irskem, kjer presega tretjino prebivalstva posamezne države, v Nemčiji se delež giblje okoli 20 %, v Italiji okoli 10 %, najmanjši pa je odstotek v Franciji (4 %). Nobena izmed evropskih držav se ni še niti približala 60-odstotnemu deležu prebivalstva, ki naj bi aplikacijo uporabljalo, da bi bila zanesljivo učinkovita glede na modele Univerze v Oxfordu (University of Oxford, 2020), ki pa poudarjajo, da bi tudi manjši odstotek uporabnikov aplikacije vendarle pripomogel k zajezitvi širjenja pandemije. Ob tem je treba upoštevati tudi dejstvo, da del prebivalstva – pogosto celo najranljivejši del, ki je zaradi svoje starosti ali gmotnega položaja nadpovprečno izpostavljen okužbi – sploh nima možnosti, da bi si aplikacijo naložilo, saj delujejo samo na določenih pametnih telefonih.[22]

Družbene posledice lažnih rezultatov so dvojne. Lažni pozitivni rezultati zmanjšujejo zaupanje prebivalstva v njihovo učinkovitost in lahko v skrajnem primeru pripeljejo do popolnega zavračanja njene uporabe. Postavlja se vprašanje, ali bodo posamezniki, ki bodo obveščeni o več tveganih stikih, do prenosa okužbe pa ne bo prišlo, pozneje sploh še pozorni na tovrstna obvestila, ali pa bo njihova pozornost padala z vsakim dodatnim napačnim pozitivnim rezultatom do takrat, ko bodo aplikacijo v celoti prenehali uporabljati. Po drugi strani napačni negativni testi v ljudeh vzbujajo občutek lažne varnosti, zaradi katere lahko okuženi posameznik kljub morda slabemu počutju nadaljuje vsakdanje življenje in se ne samoizolira, ker zmotno misli, da tveganju okužbe ni bil izpostavljen.

5 Sklepno: Etika kot prešitje prava in tehnologije

Digitalno sledenje stikom sproža poleg vprašanja varstva osebnih podatkov in zasebnosti tudi dvome glede spoštovanja načela enakosti in prepovedi diskriminacije. Dostop do tehnologije (npr. pametnih telefonov ustrezne kakovosti) lahko vodi do neenakega položaja skupin prebivalstva, ki niso dovolj tehnično vešče ali premožne (npr. strošek nakupa opreme, prenosa podatkov). Koga torej posebej ciljati oziroma čigavim stikom slediti? Odgovor je, ali vsem ali pa predvsem najbolj ranljivim skupinam glede na starost in poklic, ki so nesorazmerno bolj izpostavljeni: ali imajo ti pametne telefone (brezdomci, starejši v DSO, obsojenci na prestajanju kazni zapora)?

Poleg dostopa do tehnologije je pomembno, da so jasno izraženi dvomi o sami tehnični učinkovitosti digitalnega sledenja: ali je zmožno »prevesti« stike med napravami v epidemiološko relevantne stike med ljudmi? Poleg tehnoloških dvomov so jasno izraženi tudi pravni in družbeni dvomi. Na primer

[22] Čeprav lahko za boleznijo covid-19 zbolijo vsi, imajo starejše osebe s kroničnimi obolenji pogosteje težji potek bolezni, ki se lahko konča tudi s smrtjo. Hkrati je v skupini prebivalstva, starejših od 65 let, uporaba pametnih telefonov najmanjša. Medtem ko pametne telefone uporablja več kot 90 % prebivalstva v starostni skupini med 16 in 44 let, pa je ta delež v skupini 65–74 let le še 40 % (SURS, 2020).

Svet Evrope je jasno ugotovil, da ni dokazov, da digitalno sledenje pomaga pri boju s pandemijo covida-19 (in obratno, da ni dokazov, da ne pomaga), in zato (brez jasno ugotovljene učinkovitosti) ni vredno družbenega in pravnega tveganja, ki ga tako sledenje prinaša (Council of Europe, 2020).

Podatki o naloženih aplikacijah na telefone so le en člen v verigi obveščanja. Dokazano je, da je ta delež izjemno pomemben: matematični izračun pokaže (Wai Yee, 2020), da če 20 % prebivalcev uporabi aplikacijo, obstaja le 4-odstotna verjetnost, da bo uporabnik z aplikacijo prišel v stik z drugim aktivnim uporabnikom aplikacije. Nadalje, v primeru okužbe uporabnika aplikacije je nujno njegovo aktivno ravnanje: v Sloveniji mora uporabnik aplikacije, za katerega je bila ugotovljena okužba in je pridobil kodo TeleTAN od Nacionalnega inštituta za javno zdravje, v roku treh ur od prejema kodo vnesti v aplikacijo lastne naprave, česar pa pravno ni dolžan storiti. V Veliki Britaniji so rezultati študije pokazali izjemno majhno pripravljenost uporabnikov aplikacije sodelovati, tj. ukrepati v skladu z opozorili. Študija z več kot 30 tisoč prebivalci je pokazala, da je le 18 % ljudi upoštevalo samoizolacijo, čeprav so jim tako svetovali epidemiologi v sistemu ročnega sledenja stikov in jim hkrati še pojasnili razloge za tak ukrep. Delež takih uporabnikov, ki ne bi sledili priporočilu samoizolacije, bi bil pri avtomatizirani obliki svetovanja iz aplikacije, ko ta ugotovi potencialni tvegan stik (sicer na neznanem kraju ob neznanem času), občutno manjši.

Zaupanje uporabnikov v digitalno sledenje je majhno po vsej Evropi, večinoma zaradi skrbi za varstvo osebnih podatkov in možnosti zlorab, tj. da bodo podatki uporabljeni izključno za namen, za katerega so bili zbrani, da bo do podatkov dostopalo izključno zdravstveno osebje in da bodo podatki ostali anonimizirani. Zaupanje je majhno tudi zaradi nezaupanja v zanesljivost tehnologije Bluetooth. Ta ni bila ustvarjena za ta namen, lahko sproža lažne alarme (napačne pozitivne in negativne zadetke). Študija, ki je primerjala nemško, italijansko in švicarsko aplikacijo, je pokazala, da je tehnologija tako nezanesljiva, kot da bi bila naključna, in da bližina naprav ni pomembna (Leith in Farrell, 2020).

Sistem digitalnega sledenja stikov lahko vpliva na stigmatizacijo in namerno izpostavljanje ranljivih skupin, na primer poglabljanje družbene distance do romske skupnosti, ki naj ne bi skrbela za enako stopnje higiene rok, ali ljudi azijskega porekla, ker koronavirus izvira iz Vuhana, kar lahko vodi do iskanja »grešnih kozlov«.

Fizično distanciranje je v deprivilegiranih skupnostih razumljeno kot ideja privilegirancev. Revščina ne omogoča enake mere vzdrževanja fizične distance, vsi družbeni sloji in načini življenja ne omogočajo v enaki meri vzpostavljanja fizične distance ali ukrepov *stay-at-home*. Stiske so zato izredno različne zaradi popolnoma objektivnih pogojev življenja. V Singapurju so na primer žarišča bolezni covid-19 domovi migrantskih delavcev, ki živijo v prenatrpanih prostorih, v Sloveniji pa domovi za starejše občane, v katerih oskrbovanci nimajo ustreznih pogojev za gibanje, dostopa do svežega zraka. Biti sam ali na varni razdalji je zato privilegij.

Aplikacije, ki dopuščajo samostojne vnose uporabnikov ali ki ne vsebujejo dovolj varnih povezav ali šifriranja, so lahko tarče zlorab in manipulacij. To je izjemno pomembno v družbenem kontekstu poplave lažnih novic in političnih manipulacij. Na primer, aplikacija brez zadostne varnosti omogoča politične manipulacije (npr. način, kako zmanjšati volilno udeležbo z ustvarjanjem panike pred boleznijo v izbranem volilnem okraju), gospodarsko onemogočanje (npr. z lažnim poročanjem o žariščih v konkurenčnem podjetju), lahko postane orožje državljanske nepokorščine ali tujih obveščevalnih služb, ki bi se vmešale v notranje zadeve s sejanjem panike v posameznih predelih države z lažnim alarmiranjem (Soltani, Calo in Bergstrom, 2020). Zaradi morebitnih varnostnih ranljivosti, ki jih lahko vsebujejo aplikacije (in jih kot socio-tehnični sistemi zelo pogosto vsebujejo),[23] jih je mogoče uporabiti kot sredstva za tovrstne napade.

Nevarnost ne pomeni avtomatično, da ni mogoče oblikovati sistema, ki bi bil dovolj (!) dober in sorazmerno učinkovit. Zahteve za etično uporabo aplikacij za digitalno sledenje so:

— pilotna vpeljava (npr. Švica je s pilotno študijo preizkušala delovanje aplikacije);
— nadzor delovanja aplikacije v obliki inkluzivnega in transparentnega svetovalnega odbora, ki vključuje predstavnike javnosti;
— razgrnitev etičnih načel, ki so podlaga za delovanja aplikacije, pojasnitev njenih stroškov in koristi uporabnikom;
— zagotovitev enakega dostopa do aplikacije in enake obravnave ob okužbi;
— uporaba transparentnega algoritma za preračunavanja zadetkov, dostopnega za pregled (angl. *auditing*);
— obdobne evalvacije in raziskovanje intervencij za boljšo obveščenost upravljavcev aplikacije;
— nadzor (angl. *oversight*) in učinkovita pravna sredstva, povezana z rabo aplikacije;
— delitev izkušenj in znanj pri implementaciji z drugimi državami, zlasti tistimi z nizkimi dohodki;

[23] Nemška aplikacija Corona Warn je imela napake v kriptografski implementaciji in je omogočala razkritje, ali je neka oseba okužena z virusom ali ne. Napake v nemški aplikaciji so bile odpravljene avgusta 2020, slovenska aplikacija pa tega popravka nima, saj je kodo nemške aplikacije prevzela že pred implementacijo navedenega popravka (Kovačič, 2020a).

— svobodna uporaba za uporabnike;

— vodenje režima v skladu s tremi načeli: enakost obravnave, poštenost in zmanjševanje trpljenja.

Literatura

1. Anderson, R. (12. 4. 2020). Contact tracing in the real world. *Light Blue Touchpaper.* Pridobljeno na https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/
2. Anthes, E. (2020). Alexa, do I have COVID-19? *Nature, 586*(7827), 22–25.
3. Article 29 Data Protection Working Party. (2014). *Opinion 05/2014 on Anonymisation Techniques.* Pridobljeno na https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf
4. Ball, K. in Snider, L. (ur.) (2013). *The surveillance-industrial complex. A political economy of surveillance.* London: Routledge.
5. Bicheno, S. (20. 10. 2020). EU interoperability gateway for contact tracing apps goes live. *Informa tech.* Pridobljeno na https://telecoms.com/507003/eu-interoperability-gateway-for-contact-tracing-apps-goes-live/
6. Bock, K., Kühne, C. R., Mühlhoff, R., Ost, M. R., Pohle, R. in Rehak, R. (29. 4. 2020). Data protection impact assessment for the Corona App. *Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung*. Pridobljeno na https://www.fiff.de/dsfa-corona-file-en/at_download/file
7. Bradford, L. R., Aboy, M. in Liddell, K. (2020). COVID-19 contact tracing apps: A stress test for privacy, the GDPR and data protection regimes. *Journal of Law and the Biosciences, 7*(1). Pridobljeno na https://doi.org/10.1093/jlb/lsaa034
8. Brenza, A. (14. 5. 2020). What is an endemic virus? WHO warns COVID-19 ‹May never go away›. *Explore Health.* Pridobljeno na https://www.health.com/condition/infectious-diseases/coronavirus/what-is-an-endemic-virus
9. Burgess, M. (14. 10. 2020). Bluetooth bugs are making contact tracing apps spit out tons of errors. *Wired UK.* Pridobljeno na https://www.wired.co.uk/article/contact-tracing-app-notification-bluetooth
10. Chadwick, L. (15. 6. 2020). Norway data protection authority temporarily bans use of coronavirus tracking app. *Euronews.* Pridobljeno na https://www.euronews.com/2020/06/15/norway-data-protection-authority-temporarily-bans-use-of-coronavirus-tracking-app
11. Commission Nationale de l'Informatique et des Libertés (CNIL). (2020). *Publication of the CNIL's opinion on the „StopCovid" mobile application project.* Pridobljeno na https://www.cnil.fr/en/publication-cnils-opinion-stopcovid-mobile-application-project
12. Council of Europe. (2020). *Joint Statement on Digital Contact Tracing by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe.* Pridobljeno na https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7.
13. Curtis, J. (6. 9. 2015). How to get a Facebook beacon for your local business. *Business 2 Community.* Pridobljeno na https://www.business2community.com/facebook/how-to-get-a-facebook-beacon-for-your-local-business-01318868
14. Dayaram, S. (16. 4. 2020). Singapore had the coronavirus under control. Now it›s locking down the country. *CNET.* Pridobljeno na https://www.cnet.com/google-amp/news/singapore-had-the-coronavirus-under-control-now-it-is-locking-down-the-country/?__twitter_impression=true
15. Dibble, M. (27. 2. 2020). NSA spent $100M on phone surveillance program that prompted two unique FBI leads. *Washington Examiner.* Pridobljeno na https://www.washingtonexaminer.com/news/nsa-spent-100m-on-phone-surveillance-program-that-prompted-two-unique-fbi-leads
16. Enhorn v. Sweden, 56529/00, European Court of Human Rights. (2005). Pridobljeno na https://www.globalhealthrights.org/wp-content/uploads/2014/04/Enhorn-v.-Sweden.pdf
17. European Commission. (2020a). *Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps.* Pridobljeno na https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043
18. European Commission. (2020b). *Science for policy briefs. Telework in the EU before and after COVID-19: where we were, where we head to.* Pridobljeno na https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf
19. European Data Protection Board. (EDPB). (2020a). *Thirtieth Plenary session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR.* Pridobljeno na https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en
20. European Data Protection Board. (EDPB). (2020b). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.* Pridobljeno na https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf
21. Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP). (1994). *Uradni list RS* (7/94).
22. Gilbert, D. (9. 4. 2020) These 30 regimes are using coronavirus to repress their citizens. *Vice News.* Pridobljeno na https://www.vice.com/en_us/article/dygbxk/these-30-regimes-are-using-coronavirus-to-repress-their-citizens
23. Gorkič, P. (30. 4. 2020). Predavanje v okviru srečanj »Imeti svoj glas« na Pravni fakulteti Univerze v Ljubljani [ZOOM].
24. Greene, A. (1. 4. 2020). States should declare a State of Emergency using Article 15 ECHR to confront the Coronavirus Pandemic. *Strasbourg Observers Blog.* Pridobljeno na https://strasbourgobservers.com/2020/04/01/states-should-declare-a-state-of-emergency-using-article-15-echr-to-confront-the-coronavirus-pandemic/
25. Hessler, P. (17. 8. 2020). How China controlled the coronavirus. *The New Yorker.* Pridobljeno na https://www.newyorker.com/magazine/2020/08/17/how-china-controlled-the-coronavirus
26. Holmes, D. E. (2017). *Big Data: A very short introduction.* Oxford: Oxford University Press.
27. Informacijski pooblaščenec. (2020). *Predlog Zakona o interventnih ukrepih za pripravo na drugi val COVID-19 – EVA 2020-2611-0033 – MNENJE.* Pridobljeno na https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/2020/DZ_Zakon_o_interventnih_ukrepih_za_pripravo_na_drugi_val__COVID-19_2020-2611-0033_Burnik.pdf
28. Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity.* Pridobljeno na https://doi.org/10.1080/13562576.2020.1770587
29. Kovačič, M. (21. 8. 2020a). OstaniZdrav – Slovenska aplikacija za sledenje stikom. *Telefoncek.si.* pridobljeno na https://telefoncek.si/2020/08/21/ostanizdrav-slovenska-aplikacija-za-sledenje-stikom/

30. Kovačič, M. (14. 7. 2020b). Predlog za uvedbo protikorupcijske aplikacije. *Telefoncek.si.* Pridobljeno na https://telefoncek.si/2020/07/14/predlog-za-uvedbo-protikorupcijske-aplikacije/
31. Kuner, C., Bygrave, L. A., Docksey, C. in Drechsler, L. (ur.) (2020). *The EU General Data Protection Regulation (GDPR): A commentary.* New York: Oxford University Press.
32. Lauer, S. A., Grantz, K. H., Bi, Q., Jones, F. K., Zheng, Q., Meredith, H. R. et al. (2020). The incubation period of coronavirus disease 2019 (COVID-19) from publicly reported confirmed cases: Estimation and application. *Annals of internal medicine*, *172*(9), 577–582.
33. Leith, D. J. in Farrell, S. (2020). Measurement-based evaluation of Google/Apple Exposure Notification API for proximity detection in a light-rail tram. *PLOS ONE, 15*(9). Pridobljeno na https://doi.org/10.1371/journal.pone.0239943
34. Listina Evropske unije o temeljnih pravicah. (2012). *Uradni list Evropske unije,* (C 326/391).
35. Makszimov, V. (14. 5. 2020). Jourová: Commission looking at Hungary's emergency changes to labour code and GDPR. *Euractiv.* Pridobljeno na https://www.euractiv.com/section/justice-home-affairs/news/jourova-commission-looking-at-hungarys-emergency-changes-to-labour-code-and-gdpr/
36. Malone v. the United Kingdom, 8691/79, European Court of Human Rights. (1984). Pridobljeno na http://hudoc.echr.coe.int/rus?i=001-57533
37. Mednarodni pakt o državljanskih in političnih pravicah (MPDPP). (1992). *Uradni list RS* (35/92).
38. Meyer, M., Haverkamp, R. in Lévy, R. (ur.). (2002). *Will electronic monitoring have a future in Europe?* Freiburg: Max Planck Institute.
39. Ministrstvo za javno upravo Republike Slovenije. (2020). *Mobilna aplikacija #OstaniZdrav.* Pridobljeno na https://www.gov.si/teme/koronavirus-sars-cov-2/mobilna-aplikacija-ostanizdrav/
40. Morozov, E. (2013). *To save everything, click here: The Folly of technological solutionism public affairs.* New York: PublicAffairs.
41. Mozur, P., Zhong, R. in Krolik, A. (1. 3. 2020). In coronavirus fight, China gives citizens a color code, with red flags. *New York Times.* Pridobljeno na https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
42. Nellis, S. in Dave, P. (10. 4. 2020). Apple, Google to create contact tracing technology to fight coronavirus spread. *Reuters.* Pridobljeno na https://www.reuters.com/article/ul-health-coronavirus-apple-alphabet/apple-google-to-create-contact-tracing-technology-to-fight-coronavirus-spread-idUSKCN21S1UF
43. Neuman, G. (2016). Constrained derogation in positive human rights regimes. V E. Criddle (ur.), *Human rights in emergencies* (str. 15–31). Cambridge: Cambridge University Press.
44. Pascu, L. (16. 4. 2020). Liechtenstein to provide citizens with biometric bracelets to contain coronavirus. *BiometricUpdate.com.* Pridobljeno na https://www.biometricupdate.com/202004/liechtenstein-to-provide-citizens-with-biometric-bracelets-to-contain-coronavirus
45. Pirc Musar, N., Lemut Strle, R., Remic, M., Drev, M., Kraigher Mišič, K., Poljšak, A. et al. (2020). *Komentar Splošne uredbe o varstvu podatkov.* Ljubljana: Uradni list Republike Slovenije.
46. Rossello, S. in Dewitte, P. (25. 5. 2020). Anonymization by decentralization? The case of COVID-19 contact tracing apps. *European Law blog.* Pridobljeno na https://europeanlawblog.eu/2020/05/25/anonymization-by-decentralization-the-case-of-covid-19-contact-tracing-apps/
47. Scheinin, M. (6. 4. 2020). COVID-19 symposium: To derogate or not to derogate? *OpinioJuris.* Pridobljeno na http://opiniojuris.org/2020/04/06/covid-19-symposium-to-derogate-or-not-to-derogate/
48. Schmitt, C. (28. 4. 2020). Global perspectives on data collection, contact tracing, and COVID-19. *Medium.* Pridobljeno na https://medium.com/berkman-klein-center/global-perspectives-on-data-collection-contact-tracing-and-covid-19-8fbbcfdff25f
49. Schneier, B. (1. 5. 2020). Me on COVID-19 contact tracing apps. *Schneier on Security.* Pridobljeno na https://www.schneier.com/blog/archives/2020/05/me_on_covad-19_.html
50. SenseTime. (2020). *SenseTime enables Singaporean SMEs to safely resume operations with contactless AI thermal screening solution.* Pridobljeno na https://www.sensetime.com/me-en/news-detail/54299?categoryId=21072
51. Soltani, A., Calo, R. in Bergstrom, C. (27. 4. 2020). Contact-tracing apps are not a solution to the COVID-19 crisis. *Brookings: Tech stream.* Pridobljeno na https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/
52. Statistični urad Republike Slovenije (SURS). (2015). *V zahodni Sloveniji je imelo v prvem četrtletju 2015 dostop do interneta 83 % gospodinjstev, v vzhodni pa 73 %.* Pridobljeno na https://www.stat.si/StatWeb/News/Index/5509
53. Statistični urad Republike Slovenije (SURS). (2019). *Razvitost slovenske digitalne družbe: nameni uporabe interneta in s tem povezane težave.* Pridobljeno na https://www.stat.si/StatWeb/News/Index/8423
54. Statistični urad Republike Slovenije (SURS). (2020). *Nove mobilne tehnologije – nove navade, nove pasti?* Pridobljeno na https://www.stat.si/StatWeb/News/Index/8626
55. Šarf, P. (2018). Veliko podatkovje, podatkovna analitika in umetna inteligenca: ali je Splošna uredba o varstvu podatkov res prilagojena izzivom digitalne dobe? *Pravna praksa, 37*(18), II–VII.
56. Troncoso, C., Payer, M., Hubaux, J. P., Salathe, M., Larus, J., Bugnion, E. et al. (2020). Decentralized privacy-preserving proximity tracing. *GitHub.* Pridobljeno na https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf
57. University of Oxford. (2020). *Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown.* Pridobljeno na https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown
58. Up-106/05, Ustavno sodišče Republike Slovenije (2008). Pridobljeno na http://www.us-rs.si/documents/bf/0c/up-106-052.pdf
59. Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov). (2016). *Uradni list Evropske unije,* (L 119/1).
60. Wai Yee, Y. (1. 5. 2020). Coronavirus: More need to use contact tracing app for it to be effective. *The Straits Times.* Pridobljeno na https://www.straitstimes.com/singapore/more-need-to-use-contact-tracing-app-for-it-to-be-effective
61. World Health Organization (WHO). (2011). *The classical definition of a pandemic is not elusive.* Pridobljeno na https://www.who.int/bulletin/volumes/89/7/11-088815/en/
62. Zajc, I. (3. 10. 2020). Varovanje po italijansko: droni, tehnologija prepoznavanja obrazov in »participativni videonadzor«. *MMC RTV Slovenija.* Pridobljeno na https://www.rtvslo.si/svet/evropa/varovanje-po-italijansko-droni-tehnologija-prepoznavanja-obrazov-in-participativni-videonadzor/537844

63. Završnik, A. (2017). Algoritmično nadzorstvo: veliko podatkovje, algoritmi in družbeni nadzor. *Revija za kriminalistiko in kriminologijo, 68*(2), 135–149.
64. Završnik, A. (2019). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*. Pridobljeno na https://doi.org/10.1177/1477370819876762
65. Zghibarta, P. (11. 4. 2020). The whos, the whats, and the whys of the derogations from the ECHR amid COVID-19. *EJIL: Talk!*. Pridobljeno na https://www.ejiltalk.org/the-whos-the-whats-and-the-whys-of-the-derogations-from-the-echr-amid-covid-19/.

Social Surveillance in the Time of COVID-19

Aleš Završnik, Ph.D., Professor of Criminology, Institute of Criminology at the Faculty of Law Ljubljana, Slovenia.
E-mail: ales.zavrsnik@pf.uni-lj.si

Pika Šarf, M.A., Young Researcher, Institute of Criminology at the Faculty of Law Ljubljana, Slovenia. E-mail: pika.sarf@pf.uni-lj.si

The pandemic of the SARS-CoV-2 virus, which causes COVID-19 disease, has increased the already pervasive processing of personal data and social surveillance, which is based on it. Along with one of the biggest health crises in the modern world, we are witnessing the severest restriction of mobility in order to prevent social contacts, which is an established method of preventing the spread of infectious diseases but has never occurred on such a scale. The global "state of emergency" is inextricably linked with the risk of erosion of human rights and fundamental freedoms. In the fight against the invisible enemy, states are willing to adopt dubiously effective high-tech solutions, such as drones, thermal cameras, facial recognition technology, and various contact tracking or movement restriction applications that encroach on an individual's private sphere. They are based on the already known premise that each of us will have to give up a piece of our rights to protect the health or even the community's survival as a whole. The dichotomy between preventing the spread of the deadly virus on the one hand and (supposedly urgent) limitations on individual rights on the other is only fictional: a wide variety of digital solutions often fail to achieve the promised results even at the level of imposed technology, or the proposed technology is not as effective as to outweigh greater limitations on fundamental rights in comparison with less invasive measures.

Keywords: COVID-19, social surveillance, digital technologies, contact tracing, application

UDC: 343.9:616-036.21