

4 VPLIV DIGITALIZACIJE NA ČLOVEKOVO DOSTOJANSTVO IN SPOŠTOVANJE ZASEBNEGA IN DRUŽINSKEGA ŽIVLJENJA

TEJA ŠTRUKELJ

Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
teja.strukelj@student.um.si

Prispevek se osredotoča na problematiko varstva človekovega dostojanstva ter zasebnega in družinskega življenja v digitalni dobi. Prvi del izhaja iz predpostavke, da je človekovo dostojanstvo pogoj za uresničevanje ostalih temeljnih pravic, v naslednjih delih pa so izpostavljeni določeni primeri, v katerih lahko pride do njihove okrnitve in domnevno tudi kršitve. S tem v mislih sta najprej predstavljeni pravna podlaga in opredelitev pravic, nato pa si sledijo posamezna področja, in sicer zdravstvo, video nadzor in zvočno snemanje, prepoznavna obraza (angl. facial recognition), sledenje lokacije in internet stvari. Končni cilj tega prispevka je osvetliti izbrane temeljne pravice v digitalni dobi ter na tehniko postaviti človekovo dostojanstvo na eni strani in tehnološki razvoj na drugi.

DOI
[https://doi.org/
10.18690/um.pf.4.2023.4](https://doi.org/10.18690/um.pf.4.2023.4)

ISBN
978-961-286-774-4

Ključne besede:
digitalizacija,
človekovo dostojanstvo,
zasebnost,
družinsko življenje,
zdravstvo,
internet stvari



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.pf.4.2023.4](https://doi.org/10.18690/um.pf.4.2023.4)

ISBN
978-961-286-774-4

Keywords:
digitalisation,
human dignity,
privacy,
family life,
healthcare,
internet of things

4 THE INFLUENCE OF DIGITALIZATION ON A PERSON'S DIGNITY AND RESPECT OF PRIVATE AND FAMILY LIFE

TEJA ŠTRUKELJ

University of Maribor, Faculty of Law, Maribor, Slovenia
teja.strukelj@student.um.si

The following article focuses on the issues with safeguarding human dignity, as well as private and family life, in the digital age. The first section suggests that human dignity is a basic requirement for the realization of other fundamental rights, and the subsequent sections highlight specific instances of curtailment and, possible violations of these rights in specific context. Keeping this in mind, the legal foundation and definition of rights are presented first, followed by specific areas such as healthcare, video surveillance and sound recording, facial recognition, location tracking, and the Internet of Things. The goal of this paper is to shed light on fundamental rights in the digital age with the possibility of striking a fair balance between human dignity and technological development.



4.1 Uvod

Antiutopični roman Orwella z naslovom 1984 vsebuje zanimiv in pomenljiv stavek: »Kdor nadzira preteklost, nadzira prihodnost. Kdor nadzira sedanjost, nadzira preteklost«. Tudi če se nam danes zdi, da določen poseg v zasebnost ni nevaren, pa se lahko zgodi, da se bo naše mnenje spremenilo, ko se bomo čez čas soočili s pravimi posledicami. Digitalizacija pomeni uporabo novih digitalnih tehnologij v obstoječem načinu in notranjih procesih poslovanja.¹ Vendar pa je neločljivo povezana z različnimi aspekti našega vsakdana. V svojem delu sem se podrobneje posvetila vplivu digitalizacije na človekovo dostojanstvo, zasebnost in družinsko življenje. Medtem, ko sem se prvih dveh področij lotila bolj s pravnega vidika, pa sem vpliv na družinsko življenje raziskala s psihološkega in sociološkega vidika.

4.2 Vpliv digitalizacije na človekovo dostojanstvo in zasebnost

4.2.1 Pravna podlaga in opredelitev pojmov

4.2.1.1 Človekovo dostojanstvo

Listina Evropske unije o temeljnih pravicah človekovo dostojanstvo opredeljuje v samem začetku akta in sicer v 1. členu, ki pravi da je človekovo dostojanstvo nedotakljivo in ga je treba spoštovati in varovati.² Prav tako varstvo človekove osebnosti varuje tudi Ustava Republike Slovenije (v nadaljevanju Ustava), ki v 34. členu zagotavlja pravico do osebnega dostojanstva in varnosti.³

Človekovo dostojanstvo je neločljivo povezano z vsemi ostalimi človekovimi pravicami, tako primarnimi kot tudi sekundarnim, lahko bi rekli, da se brez spoštovanja človekovega dostojanstva ostale pravice sploh ne morejo uresničevati v vseh razsežnostih. To se kaže tudi v tem, da se je SEU večkrat opredelilo do tega. To je storilo tudi v zadevi C-377/98, v kateri je Kraljevina Nizozemska predložila

¹Štempihar, A.: Kaj je zares digitalno poslovanje?, IIBA Slovenija, april 2017, <https://slovenia.iiba.org/sites/slovenia/files/IIBA_mesecniki/mesecniki_clanki/Mesecnik_IIBA_april_2017-Clanek_%20Kaj_zares_je_digitalno_poslovanje_AS.pdf> (20.4.2020).

²Listina unije o temeljnih pravicah, UL EU C 303 z dne 14.12.2007, str. 1-16.

³Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a).

predlog za razglasitev ničnosti Direktive o pravnem varstvu biotehnoških izumov.⁴⁵ V 70. paragrafu sodbe je poudarjeno, da mora Sodišče pri nadzoru skladnosti aktov institucij s splošnimi načeli prava Unije nadzorovati spoštovanje temeljne pravice človekovega dostojanstva in osebne celovitosti. Nadalje je v 71. paragrafu pojasnjeno, da spoštovanje človekovega dostojanstva, ki je zagotovljeno v prej omenjeni direktivi, prepoveduje, da bi bilo človeško telo na različnih stopnjah svojega nastajanja in razvoja lahko izum, ki bi ga bilo mogoče patentirati. Kot primer lahko vzamemo človekovo dostojanstvo v kazenskem ali pravnem postopku. Organ pregona oziroma organ, ki vodi postopek, mora zagotoviti varstvo vseh oseb, ki so v postopek vključene, na način, da mora zagotoviti varstvo njihovih podatkov in skrbeti za primerno obravnavo, ne glede na obtožbe, ki osebo bremenijo. Prav tako je s človekovim dostojanstvom povezano izvrševanje na primer socialnih pravic. Oseba, ki ostane brez dohodka je upravičena do socialne pomoči s strani države, ki bi morala biti namenjena izključno takrat, ko je cilj zavarovanje človekovega dostojanstva ene osebe ali več oseb. Tudi na primer oskrba v zdravstvu se s pojmom dostojanstva neločljivo povezuje. Paliativna oskrba je mogoče trenutno še najbolj aktualna in pereča tema. Pogosto pa se s pojmom dostojanstva srečamo tudi v postopkih izvršbe, ki je ena izmed bolj kočljivih pravnih situacij in je poseg v dostojanstvo tako rekoč neizogiben, vprašanje je le to, da je poseg sorazmeren.

Človekovo dostojanstvo je po besedah Etelke Korpič Horvat temeljna vrednota vsake demokratične državne in družbene ureditve.⁶ Države so do pojma človekovega dostojanstva razvile različne pristope. Na najvišjo raven ga povzdigne nemška zvezna ustava, ki v 1. členu navaja, da je človekovo dostojanstvo nedotakljivo ter da je njegovo spoštovanje in varstvo obveznost celotne državne oblasti.⁷ Za primerjavo slovenska Ustava v prvih členih ureja državno ureditev, človekove pravice pa se pričnejo od 14. člena dalje. Ustavno sodišče je v zadevi *Titova cesta* štelo, da poseg v človekovo dostojanstvo ni le poseg v človekovo pravico in temeljno svoboščino, temveč da je kot posebno ustavnopravno načelo "načelo spoštovanja človekovega dostojanstva neposredno utemeljeno že v 1. členu Ustave,

⁴ Zadeva C-377/98, *Kraljevina Nizozemska proti Parlamentu in Svetu*, ECLI:EU:C:2001:523.

⁵ Direktiva Evropskega parlamenta in Sveta 98/44/ES z dne 6. julija 1998, o pravnem varstvu biotehnoških izumov, Uradni list Evropske unije, L 213, 30.7.1998, str. 13–21.

⁶ Korpič-Horvat, E.: Razvoj socialne varnosti in varovanje človekovega dostojanstva v odločitvah Ustavnega sodišča Republike Slovenije, Podjetje in delo, št. 6-7, 2018, str. 1325.

⁷ Nemška zvezna ustava, Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 28. Juni 2022 (BGBl. I S. 968) geändert worden ist.

ki Slovenijo opredeljuje kot demokratično republiko".⁸ Prav tako je Ustavno sodišče v tej zadevi navedlo: "Po vsebini gre pri človekovem dostojanstvu za predpostavko, da ima vsak človek enako in absolutno notranjo vrednost, ki mu pripada prav zato, ker je človek. Spoštovanje človekovega dostojanstva zato pomeni varstvo osebne vrednosti posameznika pred neupravičenimi posegi in zahtevami države in družbe."

4.2.1.2 Izzivi digitalizacije za varstvo zasebnosti

Listina EU o temeljnih pravicah spoštovanje zasebnega življenja omenja v 7. členu, preko katerega podeljuje pravico do spoštovanja zasebnega in družinskega življenja, stanovanja ter komunikacij posameznika. Seveda pa je z zasebnostjo povezano tudi varstvo osebnih podatkov, ki je v Listini varovano v 8. členu, ki posamezniku podeljuje pravico do varstva osebnih podatkov, ki se nanj nanašajo. Evropska konvencija o človekovih pravicah (v nadaljevanju EKČP),⁹ v 8. členu prav tako nudi varstvo pravice do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja. Drugi odstavek istega člena pa navaja, da se tudi javna oblast ne sme vmešavati v izvrševanje te pravice, razen, 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. To pa je lahko že predmet razprave. Razmerje med Listino EU o temeljnih pravicah in EKČP je opredeljeno v 3. odstavku Listine EU o temeljnih pravicah, ki pravi, da sta, v primerih ko listina vsebuje pravice, ki ustrezajo pravicam, zagotovljenim z Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin, vsebina in obseg teh pravic enaka, kot vsebina in obseg pravic, ki ju določa navedena konvencija. Konvencija na evropski ravni namreč predstavlja osnovo, minimum pravic. Prav tako navaja, da s to določbo ne preprečuje širšega varstva po pravu Unije. Varstvo zasebnosti in varstvo osebnih podatkov v 35. in 38. nudi tudi Ustava.

Zasebnost je v digitalizaciji tako rekoč nemogoče pričakovati.¹⁰ Kazalniki za to so predvsem razkritja, ki vsake toliko časa javnost opozorijo na vdor v zasebnost s

⁸ Zadeva »Titova cesta«, Ustavno sodišče RS, Sodba U-I-109/10 z dne 26. septembra 2011.

⁹ Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Uradni list RS – Mednarodne pogodbe, št. 7/94).

¹⁰Newman Forbes, D.: What Is Privacy In The Age Of Digital Transformation?

strani korporacij. Takšen primer je bil razkrit lansko leto in sicer s strani virtualnega asistenta Amazon Alexa, ki naj bi ves čas poslušal in snemal pogovore uporabnikov, tudi ko ti asistenta sploh niso potrebovali in uporabljali.¹¹ Večina uporabnik se ne zaveda, da Amazon hrani kopijo vsega, kar je naprava poslušala in posnela. Prav tako pa ni nič manj sporno delovanje aplikacije Siri v Applovih aparaturah in pa Googlevega asistenta, saj delujeta po istem principu. Vsi upravljalci navedenih aplikacij pomirjajo, da naprava zvok snema le, če je poklicana po imenu, vendar pa se je novinar Geoffrey Fowler podrobneje posvetil raziskovanju arhiva posnetkov svoje Alexa naprave in ugotovil, da zajema tako ukaze namenjene napravi kot tudi pogovore zasebne in občutljive narave, ki so izgleda nekako sprožili »wake work« naprave. Po zagotovitvi Amazona naj bi se primeri, ko pride do tega, zmanjševali. Glavni namen snemanja pa naj bi bil ta, da se lahko delovanje naprave posodablja in izboljšuje. V kolikor bi uporabnik mikrofon izklopil, bi napravi vzel glavni namen delovanja. Do velike dileme pa bi prišlo v primeru, da bi naprava posnela na primer zelo občutljivo vsebino zasebnega pogovora in ga v zmoti posredovala drugim uporabnikom. To pa niti ni le teorija, temveč obstaja že resnični primer.¹² Družina iz Portlanda je prejela nepričakovan klic, da naj izključi vse Alexa naprave v svojem domu, saj so postali žrtve hekerjev. Vse se je začelo na način, da je ena izmed naprav Alexa posnetke posredovala brez soglasja družine. Amazon se je na kritike odzval z odgovorom, da je določen pogovor moral vsebovati besedo podobno besedi Alexa, ki je napravo prebudila, nadalje pa je naprava še »pridobila« smiselna navodila, komu naj posnetek posreduje. Vendar naj bi bile podobne situacije izjemno redke, prav tako pa naj bi bilo vsem uporabnikom omogočeno dostopati do arhiva posnetkov, kar pomeni, da bi lahko neustrezne vsebine tudi zbrisali. Apple pa na primer posnetkov pogovorov iz aplikacije Siri ne shranjuje individualizirano, temveč naj bi bila baza skupna in anonimna. Tudi Google je do nedavnega posnel prav vse zvoke, ki jih je zaznal njegov asistent, kar je spremenil šele pred nedavnim. Geoffrey Fowler se je v članku sarkastično pošalil, da bi vsem podatkom, ki jih je o sebi izbrskal v Alexinem arhivu, zavidala celo tajna policija. Na koncu se avtor zave, da Amazon ne

<<https://www.forbes.com/sites/danielnewman/2019/05/02/what-is-privacy-in-the-age-of-digital-transformation/#8050c9c628ed>>, (4.5.2020).

¹¹ Alexa has been eavesdropping on you this whole time, Geoffrey Fowler, The Washington Post, <<https://www.washingtonpost.com/technology/2019/05/06/alex-a-has-been-eavesdropping-you-this-whole-time/>> (4.5.2020).

¹² An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says, Hamza Shaban, The Washington Post, <<https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-family-s-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/?noredirect=on>> (4.5.2020).

pridobiva zgolj informacij s snemanjem, temveč kar celotno sliko vsakdana. Oprema doma je namreč že digitalizirana do te mere, da lahko upravljalec sistema brez težav razpozna lastnosti in značilnosti uporabnika. Potrebno se je zavedati, da Amazon sodeluje tudi z ostalimi napravami in aparati v našem domu, pod pretvezo zagotavljanja najboljše možne uporabniške izkušnje. To pomeni, da pridobi podatke o tem, koliko se je naše stanovanje ogrevalo, kakšno glasbo smo poslušali, koliko svetlobe smo uporabljali tekom dneva, koliko časa smo bili budni, koliko hrane smo konzumirali in s katerimi osebami smo komunicirali.

Zatem, ko so luč sveta ugledala razkritja žvižgačev, kot je npr. Snowden, je Evropski parlament sprejel resolucijo, v kateri je Agencijo EU za temeljne pravice (v nadaljevanju FRA) pozval, naj pripravi raziskavo o varstvu temeljnih pravic v okviru opravljanja nadzora. Leta 2015 je bilo s strani agencije objavljeno poročilo,¹³ ki pa po mnenju piscev II. dela poročila, ki je bilo pripravljeno leta 2018 že ni več dosledno spremembam, ki so se vmes dogodile.¹⁴ Zaradi pogostih terorističnih napadov, migracijskih pritiskov in vedno več kibernetских groženj je namreč več držav članic EU sprejelo zakonodajo za okrepitev zbiranja obveščevalnih podatkov. S tem je nemalo članic razširilo uporabo nacionalnih zakonov, da bi lahko obveščevalnim in varnostnim organom omogočile boljši nadzor in pregled nad možnimi zlorabami in grožnjami državnemu sistemu.

Zdaj, ko imamo dobro predstavo, kaj pojmi človekovo dostojanstvo, varstvo zasebnosti in varstvo osebnih podatkov pomenijo, jih lahko povežemo tudi z neizbežno digitalizacijo. Porajajo se mi predvsem vprašanja povezana z varstvom osebnih podatkov na področju zdravstva, preko aplikacij za diagnosticiranje in elektronskih baz podatkov o zdravstvenem stanju posameznikov. Prav tako bi bila smiselna razprava o tem, kako korporacije pridobivajo podatke o obnašanju in navadah posameznikov, ki so nadalje podlaga za prilagojene ponudbe in pa povečanje povpraševanja po njihovih storitvah. Nekaj besed bom posvetila sledenju lokacije in pa snemanju govora preko mobilne naprave. V zadnjih letih se vse bolj sprašujemo, kaj za našo prihodnost pomeni ti. tehnologija prepoznave obraza »face

¹³ Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v EU – Del I: Pravni okviri držav članic, Agencija FRA, 2015, <<https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELLAR:35149923-8c2c-11e5-b8b7-01aa75ed71a1&from=FR>> (4.5.2020).

¹⁴ Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v Evropski uniji – Del II, Agencija FRA, 2018, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_sl.pdf> (4.5.2020).

recognition technology«. Vsi naštetih problemi vzbujajo nastanek nemalo teorij zarot, zato je raziskovanje teh tem zelo zanimivo.

Do pomembnosti varovanja temeljnih svoboščin se opredeljuje tudi Bela knjiga o umetni inteligenci, ki jo je pripravila Evropska komisija: *»Glede na velik vpliv umetne inteligence na našo družbo in potrebo po vzpostavitvi zaupanja je nujno, da evropska umetna inteligenca temelji na naših vrednotah in temeljnih pravicah, kot sta človekovo dostojanstvo in varstvo zasebnosti.«*¹⁵

Zaskrbljujoče podatke izkazujejo tudi raziskave Sveta Evrope, ki opozarjajo na vpliv razvoja algoritmov in tehnologije, na temeljne človekove pravice, ki jih zagotavlja EKČP.¹⁶ Predvsem je ogroženo zasebno in družinsko življenje, v povezavi z osebni podatki. Na prvi pogled piškotki niso nevarni, vendar ravno ti pripomorejo k profiliranju uporabnika in polnjenju baze o uporabniku.¹⁷ Moj pomislek na tem mestu je, da se uporabniki ne zavedamo, da ima lahko na primer vsakdanje odklepanje zaslona mobilnega telefona s prstnim odtisom v prihodnosti potencialno negativne učinke. »Pravica do pozabe" iz 17. člena GDPR na koncu ne bo imela pravega učinka, saj se uporabniki niti ne zavedamo, koliko podatkov smo v svet že prostovoljno posredovali in jih ne bomo nikoli več mogli vzeti nazaj. Mogoče posamezni podatek o nas še ne predstavlja tako velike grožnje, vendar bo sistem kaj kmalu, če tega seveda še ne počne, zmožen povezati na prvi pogled nepovezane vsebine. Mislim, da je dovolj že vpogled v elektronsko pošto ali pa v datoteke, ki jih ima posameznik shranjene v oblaku. Seveda pa bo kot glavni cilj zbiranja podatkov vedno izpostavljena nacionalna varnost, vsi pa vemo, da je lahko profiliranje zelo pomemben dejavnik tudi v iskanju načinov, kako na pravi način pristopiti k volilcem. V kolikor bo v bazi podatek o tem, da je oseba bolj konservativno usmerjena, se ji bodo v skladu s tem prikazovale vsebine, ki se bodo dopadle njenemu političnemu mišljenju. To se v praksi že udejanja in ni zgolj znanstvena fantastika v prihajajočih letih. Med drugim smo bili temu priča v teku zadnjih predsedniških volitev v

¹⁵ Evropska komisija, BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final.

¹⁶ ALGORITHMS AND HUMAN RIGHTS, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, Svet Evrope 2018, <<https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>> (2.6.2020).

¹⁷ Angleško »cookies«.

Združenih državah Amerike.¹⁸ Vendar pa za predložitev naših podatkov nismo vedno krivi sami, saj lahko te predloži 3. oseba z ali brez našega dovoljenja. S tem vprašanjem se je ukvarjalo Sodišče EU v zadevi C-131/12.¹⁹ Tožnik v tej zadevi je želel, da novičarski časnik in pa Google brskalnik ugodita njegovi prošnji, da se ob vpisu njegovega imena v iskalnik kot prvi zadetki ne prikazujejo več novice o tem, da je bil udeležen v postopku izvršbe. Sodišče se je ukvarjalo z vprašanjem, če podjetje Google, kot upravljalec brskalnika dejansko upravlja z osebnimi podatki tožnika, glede na dejstvo da so njegovi podatki objavljeni v člankih, neodvisnih od Googla. Sodišče EU je v 33. točki sodbe podalo razlago, da *»družba, ki upravlja iskalnik, določa namene in sredstva te dejavnosti, tako da jo je treba šteti za „upravljavca“ te obdelave.* Kot upravljalec osebnih podatkov pa je nosilec brskalnika dolžan ugoditi pravici osebe do izbrisa podatkov (črtanja novic iz prvih zadetkov v iskalniku), ne glede na to, da bo na primer vsebina na internetu še vedno obstajala (bo objavljena zakonito ali ne). Vendar pa bi bila pravica osebe omejena, v kolikor bi se izkazalo, da je poseg v njene temeljne pravice upravičen zaradi prevladujočega interesa javnosti (dostop do javnih informacij). Tipičen primer so informacije javnega značaja.

4.2.2 Digitalizacija na področju zdravstva

Po definiciji Svetovne zdravstvene organizacije iz leta 1948 je zdravje: *»stanje popolnega telesnega (fizičnega), duševnega (mentalnega) in socialnega blagostanja/ugodja in ne zgolj stanje odsotnosti bolezni ali betežnosti/nemoči.«* Lahko se strinjamo, da je zdravje ena izmed najbolj pomembnih vrednot človeka, ki je povezana tudi z ohranjanjem človekovega dostojanstva. Tudi zdravstveni sistem se v digitalni dobi razvija in s sabo prinaša mnoge spremembe tako pri obravnavi pacientov kot skladiščenju vseh podatkov o pacientih. V zadnjem času se govori o elektronskih napotnicah, elektronskih receptih, elektronskih zdravstvenih kartotekah in tudi o aplikacijah, ki so namenjene diagnosticiranju zdravstvenih težav uporabnika.

¹⁸ Cadwalladr C., Graham-Harrison, E.: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 2018, <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>> (1.6.2020).

¹⁹ Zadeva C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu*, ECLI:EU:C:2014:317.

Informacijski pooblaščenec na svoji spletni strani pojasnjuje, kakšno mora biti varstvo zdravstvenih podatkov oseb.²⁰ Vsi, ki imajo opravka z zdravstvenimi podatki (zdravstvene ustanove in zavodi, idr.), morajo v skladu z zakonodajo učinkovito urediti in zagotoviti varnost zdravstvenih kartonov posameznikov, izdanih receptov, evidence bolnikov in drugih podatkov. Vendar pa se kot glavni problem varnosti ne zdijo dejstva, da se na primer zdravstveni kartoni nahajajo na mizi in so tako dostopni mimoidočim, temveč grožnja, da nekdo vdre v informacijsko bazo in tako pridobi kočljive podatke o osebi, ki se zdravi ali se je zdravila v preteklosti. Načini obdelovanja in vnašanja podatkov v elektronske zdravstvene kartoteke (v nadaljevanju EZK), se med zdravstvenimi ustanovami zelo razlikujejo. Raziskovalna skupina na Tehnološkem inštitute Massachusetts (MIT), si želi v svet EZK uvesti inovativno rabo blockchain tehnologije. To se ne bi zgodilo na klasičen način veriženja blokov, temveč z uporabo ti. "pointers-ov", ki so kot neke hiperpovezave. In kako bi to delovalo? Zdravnik po obravnavi pacienta podatke vnese v aplikacijo, minimalen kos podatkov v anonimizirani obliki pa gre na blockchain unikatnim identifikatorjem pacienta. Torej se na blockchain prenese zgolj povezava do internih podatkov, ki jih upravlja zdravnik. Če pacient zamenja zdravnika, bo novi zdravnik lahko preko unikatnega identifikatorja v verigi blokov dostopal do podatkov, ki jih je vnašal prejšnji zdravnik. To bo pomenilo večjo doslednost pri zdravstveni oskrbi in pa onemogočilo šume v komunikaciji ter odpravilo težave, ki so bile povezane s pridobivanjem zdravstvenih kartotek v fizični obliki.²¹ V fazi zaključevanja pisanja (junij 2020), se že kažejo rezultati uporabe aplikacija za diagnosticiranje korona virusa. Predvsem je razvidno to, da sta se v pripravo aplikacij hitro vključili korporaciji Apple in Google, kar je skrb vzbujajoče predvsem z vidika varstva osebnih podatkov, ki so zaradi posegov prej omenjenih akterjev že nemalokrat bili izpostavljeni in ogroženi. Najprej je britanska vlada namreč imela vizijo razvoja neodvisne aplikacije, ki bi podatke uporabnikov o širjenju virusa zbirala preko bluetooth povezave. Podatki bi se shranjevali centralizirano, kar bi pomenilo večjo varnost podatkov, vendar pa se je rok za pripravo te aplikacije znova in znova podaljševal, zato je britanska vlada v aprilu sporočila, da se bosta v pripravo aplikacije vključila giganta Google in Apple.²²

²⁰ Zdravstveni podatki, Informacijski pooblaščenec, <<https://www.ip-rs.si/varstvo-osebni-podatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/zdravstveni-podatki>> (19.4.2020).

²¹ Tehnologija, ki stoji za kriptovalutami, bi lahko reševala življenja, <<http://m.racunalniskem-novice.com/index.php?id=tehnologija-ki-stoji-za-kriptovalutami-bi-lahko-resevala-zivljenja.html>> (19.4.2020).

²² Rory Cellan-Jones: Coronavirus: What went wrong with the UK's contact tracing app?, BBC, 20.6.2020, <https://www.bbc.com/news/technology-53114251?at_custom4=8D4889AE-B307-11EA-A6BA-

Zanimiv primer na področju zavarovalništva in tehnologije prihaja iz ZDA. Gospod, ki je imel težave s smrčanjem in posledično dihanjem med spanjem, je uporabljal napravo CPAP (aparatus za vzdrževanje stalnega pritiska v dihalnih poteh). Po tem, ko je napravo nekaj časa uporabljal, je želel s strani zavarovalnice pridobiti sofinanciranje za nov aparat. Takrat pa ga je ta obvestila, da podatki kažejo, da je stari aparat nepravilno uporabljal in mu navedla podatke za posamezni dni/noči, ko aparata ni uporabljal ustrezno oz. celo noč. Zavarovalnica je s pridobivanjem podatkov o spanju tako lahko zavarovancu odklonila sofinanciranje nadgradnje.²³ Mar to pomeni, da bi lahko bila v prihodnosti zdravstvena premija izračunana tudi na podlagi tega, kako dober je naš spanec?

4.2.3 Video nadzor in zvočno snemanje

V trenutni situaciji, ko virus COVID-19 predstavlja resno grožnjo in je poponoma spremenil naš vsakdan, so posebej do izraza prišle tudi aplikacije za diagnosticiranje virusa. Potencialne pasti tovrstnih aplikacij so razdelane že v več člankih.²⁴ Potekata dve aktivni raziskavi (Cambridge University in Carnegie Mellon University) za pripravo aplikacije, ki bi lahko povedala, ali je uporabnik okužen z virusom ali ne. To bi bilo izvedljivo s pomočjo umetne inteligence, ki bi na podlagi posnetkov zdravih oseb in bolnih oseb prepoznala kašelj in dihanje, ki sta značilna za virus covid-19. Projekt s cambriške univerze se imenuje Covid-19 Sounds, uporabnik pa mora dihati in kašljati v mikrofonski, hkrati pa mora navesti nekaj splošnih podatkov o sebi (spol, starost, pozitiven test na virus). Projekt deluje prek spletne strani in ne preko standardne mobilne aplikacije. Skupina na drugi univerzi pa izdeluje Covid Voice Detector. Pri omenjenem pa mora uporabnik kašljati in izgovarjati abecedo. Snovalci obeh platform poudarjajo, da ne gre za aplikacije, ki bi nadomestile zdravnika. Vendar je to, kljub opozorilu, dvorezen meč, saj bodo uporabniki lahko lahkomišelnosklepali, da niso okuženi, ker jim bo tako rekla aplikacija.

17F3C28169F1&at_custom3=BBC+News&at_custom2=facebook_page&at_medium=custom7&at_custom1=%5Bpost+type%5D&at_campaign=64> (21.6.2020).

²³ Marshall Allen: You Snooze, You Lose: Insurers Make The Old Adage Literally True, Propublica, 2018, <<https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true>> (1.6.2020).

²⁴ Leo Kelion: Coronavirus: Covid-19 detecting apps face teething problems, <<https://www.bbc.com/news/technology-52215290>> (19.4.2020).

Kaj pa mobilne aplikacije, ki si jih avtomatsko naložimo na svoje mobilne aparature in se pogosto sploh ne vprašamo, kaj se bo zgodilo z vsemi podatki, ki jih bo aplikacija pridobila? Članek²⁵ navaja, da je dejstvo, koliko varnosti lahko pričakujemo, odvisno od tega, kateri telefon uporabljamo, kje bivamo in kako smo previdni. Na primer gigant Apple naj bi od aplikacij, ki so prilagojene za Iphone, pred uvrstitvijo v ponudbo v Apple trgovini zahteval, da zadoščajo kriterijem o varovanju zasebnosti. Vendar pa neodvisne komercialne aplikacije skozi to sito ne gredo, kar pomeni da se lahko podatki uporabnika na koncu uporabijo za marsikaj. Uporabniki Androida pa naj bi bili, glede na članek, bolj ogroženi. Podlaga za to trditev naj bi bila nemška raziskava, ki je ob pregledu šestdesetih aplikacij za zdravje ugotovila, da nobena izmed pregledanih aplikacij ni vsebovala podobne seznanitve uporabnika z varstvom njegove zasebnosti in podatkov. Veliko opozorila je uporabniku lahko že dejstvo, da je določena aplikacija za prenos na voljo brez plačila, medtem ko so primerljive aplikacije plačljive. Pogosto se »brezplačne« aplikacije financirajo iz oglaševanja, vendar je vir dohodka verjetno pogosto tudi posredovanje dragocenih podatkov 3. osebam. Uporabnik pa se temu skorajda ne more izogniti, saj je sprejem pogojev pogoj za uporabo aplikacije, velikokrat pa je besedilo, ki pojasnjuje obdelavo podatkov zelo kompleksno in dolgo, tako da ga uporabnik največkrat enostavno preskoči. In zakaj so lahko podatki o zdravstvenem stanju tako zelo vredni? Zato ker so uporabni na področju profiliranja za oglaševalske storitve. Na primer, oseba je sladkorni bolnik in si ravni sladkorja v krvi ter količino dnevnega odmerka insulina vpisuje v elektronsko tabelo aplikacije. Končni prejemnik teh podatkov bo lahko tej isti osebi na vse mogoče načine oglaševal izdelke za diabetike, izdelke brez sladkorja in morebiti tudi storitve strokovnjakov s tega področja. Oseba, ki ji bo v zameno za deljenje podatkov obljubljeni, da bo to lažje pripeljalo do zdravljenja ali pa pripomoglo k uspešnejšemu zdravljenju.²⁶

Zdravstvene institucije v Združenih državah Amerike opozarjajo, da bi zdravstveni podatki v aplikacijah lahko na široko odprli vrata zlorabam, zato se temu aktivno upirajo. Ameriška vlada namreč pripravlja regulacijo pretoka z informacijami na področju zdravstva. Regulacija pa naj bi izvajalcem zdravstvenih storitev nalagala obveznost, da zdravstvene podatke posredujejo aplikacijam, kot so Apple's Health Records, v kolikor pacienti s tem soglašajo. Ameriška zdravstvena organizacija in

²⁵This Is What Your Phone Does with Your Personal Health Data, Mark Henricks, <<https://www.shape.com/fitness/trends/health-apps-privacy-personal-information-shared>> (19.4.2020).

²⁶ Lee, S.: Who uses my health data, <<https://www.goinvo.com/vision/who-uses-my-health-data/>> (19.4.2020).

sektorske zdravstvene organizacije pa opozarjajo, da vnašanje podatkov v komercialne aplikacije morda ni korak v pravo smer, saj tako tudi zakonodaja, ki omejuje razpolaganje s podatki zdravstvenih kartotek sicer ne bo imela učinka, ko bodo podatki enkrat vneseni v komercialne baze. Aplikacije bi lahko s svetom delile tudi podatke o zgodovini predpisanih zdravil in o družinski zdravstveni zgodovini. To bi se lahko pokazalo škodljivo v primerih zaposlovanja, saj bo delodajalec, ob vseh podatkih, raje izbral kandidata, ki je zdrav. Prav tako pa bi zavarovalnica lahko na podlagi teh podatkov oblikovala višjo premijo za zavarovanje osebe. Vendar pa verjetno za vsemi temi prizadevanji tičijo tudi interesi multikorporacij kot so Google, Amazon, Microsoft in Apple, ki bodo s podporo vlade prodri tudi na zdravstveni trg. Vsi naštetih giganti pa so se zavezali, da bodo njihove platforme med seboj združljive in kompatibilne. Microsoft je na primer razvil storitve v oblaku, ki uporabniku omogočajo, da po predurku določene vsebine tudi umakne. Z uveljavitvijo regulacije naj bi izvajalci zdravstvenih storitev in nosilci zdravstvenih evidenc imeli na voljo dveletni rok za izpolnitev zahtev. V kolikor bi to zavrnilo, bodo prejeli globo in bo zoper njih uvedena preiskava. Vendar pa se kot največjo past pridobivanja zdravstvenih podatkov izpostavlja dejstvo, da so aplikacije narejene po sistemu vse ali nič. Torej če bo oseba soglašala s posredovanjem podatkov o zgodovini zdravljenja prehlada, bo hkrati posredovala tudi podatek o tem, da je na primer okužena z virusom HIV. To pomeni, da bodo slabi vidiki lahko zanemarili vse pozitivne učinke tovrstne ureditve.²⁷

4.2.4 Tehnologija prepoznave obraza

V delu te tematike sem si ogledala oddajo Ugriznimo v znanost, v kateri je bilo dodobra predstavljeno, v kateri fazi razvoja je trenutno tehnologija za prepoznavanje obraza.²⁸ Ljudje naj bi si, po raziskavi izvedeni na Univerzi York, bili sposobni zapomniti povprečno pet tisoč obrazov.²⁹ Na Kitajskem nadzorne kamere ves čas nadzorujejo ljudi v urbanem okolju in bi naj z lahkoto prepoznavale osnovne značilnosti oseb. V času priprave zgoraj omenjene oddaje, si je Kitajska lastila bazo z več kot sedemsto milijoni obrazov, kar bi pomenilo, da bi posameznikov obraz

²⁷ Singer, N.: When Apps Get Your Medical Data, Your Privacy May Go With It, The New York Times, <<https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html>> (20.4.2020).

²⁸ Radio televizija Slovenija, Oddaja Ugriznimo v znanost: Prepoznavanje obrazov, 13.12.2018, <<https://4d.rtvsl.si/arhiv/ugriznimo-znanost/174582438>> (3.5.2020).

²⁹ Never forget a face? Research suggests people know an average of 5,000 faces, University of York, <<https://www.york.ac.uk/news-and-events/news/2018/research/never-forget-a-face/>> (3.5.2020).

lahko našla v nekaj sekundah. Ta način za zagotavljanje večje »varnosti« pa si želijo tudi ostale svetovne velesile. Tehnologija prepoznave obrazov naj bi se izkazala kot koristna na primer v primeru, da bi prepoznala potencialne teroriste znotraj množice obiskovalcev razvpite tekme. Po besedah gosta oddaje, dr. Vitomirja Štruca, zelo velika baza ni potrebna. Policija v več državah deluje po sistemu vodenja ožje baze potencialno nevarnih oseb. V kolikor med množico zazna nekoga s podobnimi lastnostmi, ga primerja direktno s podatki s seznama nevarnih oseb. To namreč vzame bistveno manj časa, kot da bi moral sistem pregledovati bazo z neskončnim številom zadetkov. Vendar pa pomirja dejstvo, da računalnik v tem trenutku še ni sposoben prepoznavanja v enaki meri kot človek. Tudi slovenska policija že s pridom uporablja tehnologijo prepoznave obrazov, vendar bi bolj omejenem obsegu kot svetovne velesile, ki preverjajo tudi identiteto mimoidočih na ulici, saj tega slovenska policija ne počne. Uporablja jo preko spletne aplikacije, ki pomaga hitreje najti osumljenca v policijski bazi fotografij.³⁰ Morebitno ujemanje nato preverjajo še ročno. Vendar pa se tehnologija za prepoznavanje obrazov ne uporablja zgolj za namene varnosti, temveč imamo z njo opravka preko aplikacij in naših elektronskih naprav. Po besedah Štruca tehnologija znotraj aplikacij predstavlja podobno tehnologijo za detekcijo obraza. To lahko najprej vidimo na socialnem omrežju Facebook, kjer nam, ko naložimo sliko, preko obrazov napravi okvirčke in že predlaga, katero osebo naj označimo. Prav tako pa se mogoče še premalo zavedamo nevarnosti uporabe tridimenzionalnih filtrov, ki naš obraz spremenijo v kakšno pošast ali v prikupnega kužka. Da je to mogoče, mora naprava prepoznati dimenzije obraza. S tem pa aplikacija razbere tudi določene podatke s samega obraza, na primer koliko je oseba stara ter katerega porekla in spola je. Na podlagi tega pa se lahko tudi aplikacija odloči, ali nam bo na pregled podala oglas za ličila ali za ribiško opremo. Seveda vsaka ponudba ne bo popolnoma prilagojena, pa vendar v večini primerov bo smiselna. Na Kitajskem je z obrazom že mogoče dostopati do bančnih računov, nakupovati in vstopati na letala. Tehnologija prepoznave obraza se uporablja v skoraj bizarni situaciji in sicer prepoznava, kdo krade toaletni papir na javnem stranišču.³¹ Poletne olimpijske igre, ki bi se morale izvesti letos, naj bi predstavljale prvi dogodek, na katerem bi se za varnost poskrbelo s prepoznavo obraza, saj bi tako preprečili krajo identitet in prevare.³²

³⁰Tudi slovenska policija uporablja avtomatsko prepoznavo obrazov, RTV SLO, <<https://www.rtv slo.si/znanost-in-tehnologija/tudi-slovenska-policija-uporablja-avtomatsko-prepoznavo-obrazov/510776>> (3.5.2020).

³¹China's High-Tech Tool to Fight Toilet Paper Bandits, New York Times, <<https://www.nytimes.com/2017/03/20/world/asia/china-toilet-paper-theft.html>> (3.5.2020).

³²NEC unveils facial recognition system for 2020 Tokyo Olympics,

Zanimiva sodba glede tehnologije prepoznave obraza prihaja iz Francije.³³ Južna regija je pripravila načrt za vzpostavitev tehnologije za prepoznavo obraza na srednjih šolah v Nici in Marseillu. Nevladne organizacije, starši in sindikati so se zoper ta načrt pritožili. Sodišče same eksperimentalne uporabe tehnologije ni prepovedalo, temveč je poudarilo, da regionalne oblasti, kot je na primer južna regija, niso pristojne za sprejemanje tovrstnih odločitev. To lahko po mnenju sodišča vzpostavi le individualna izobraževalna institucija. V sodbi je sodišče navajalo določbo uredbe GDPR, ki pravi, da je za uporabo tehnologije prepoznavanja obraza nujno potrebno soglasje snemanih, saj gre za osebne biometrične podatke (14. točka, 4. člena Uredbe). Biometrične podatke je sicer v skladu z 9. členom uredbe prepovedano zbirati, soglasje pa predstavlja izjemo od te prepovedi. Sodišče je ukrep označilo kot nesorazmeren, saj naj bi po njegovih besedah »Regionalne oblasti uporabljajo kladivo, da bi zdobile mravljo«.

Glede na podatke poročila EU o varstvu podatkov in digitalne identitete, iz leta 2011, je več kot tretjina evropskih državljanov aktivna na socialnih omrežjih, kar polovica od teh pa uporablja spletne strani tudi za deljenje fotografij, video posnetkov in drugega.³⁴

Zanimivo je stališče, ki opozarja na nevarnost vpeljave tehnologije prepoznave obraza v socialno omrežje Facebook, ki bi brez dodatnega privoljenja lahko na fotografiji označil osebe, ki so bile kadarkoli označene na katerikoli drugi fotografiji. Veliko uporabnikov tega ne ve, oziroma to opazi šele, ko so že avtomatsko označeni na fotografijah. Neregistrirani uporabniki in uporabniki, ki bodo odklonili podajo soglasja, da se njihov obraz vključi v bazo za prepoznavo obrazov na novih fotografijah, tako v bazo ne bodo vključeni in se njihovo ime ne bo avtomatsko prikazalo med predlogi za označbo. Problem avtorica vidi v sistemu opting-out soglasja (to pomeni, da se soglasje domneva, razen če se ga izrecno odkloni). Soglasje bi moralo biti namreč individualizirano za vsako aktivnost socialnega omrežja posebej, ne pa izpeljano zgolj iz podane generalne privolitve za vse bodoče

<<https://www.theverge.com/2018/8/7/17659746/tokyo-2020-olympic-games-face-recognition-nec>> (3.5.2020).

³³Sodišče prepovedalo testno prepoznavanje obrazov na šolah v Marseillu in Nici, RTV SLO, dostopno na: <<https://www.rtvsl.si/znanost-in-tehnologija/sodisce-prepovedalo-testno-prepoznavanje-obrazov-na-solah-v-marseillu-in-nici/516064>> (3.5.2020).

³⁴ SPECIAL EUROBAROMETER 359 Attitudes on Data Protection and Electronic Identity in the European Union REPORT Fieldwork: November – December 2010, objavljeno junija 2011.

aktivnosti. Problem zbiranja podatkov se skriva tudi v na videz popolnoma nenevarnemu všečku (angl. Like), ki na podlagi vseh všečkanih vsebin povzroči, da se osebi nadalje prikazuje samo prilagojena vsebina. Torej če všečka fotografije z dopustov, se mu bodo verjetno v večji meri prikazovale vsebine povezane s potovanji in turizmom.³⁵

S podobnim vprašanjem glede zbiranja in hranjenja biometričnih podatkov se je v zadevi

Marper proti Združenemu Kraljestvu ukvarjalo Evropsko sodišče za človekove pravice (v nadaljevanju ESČP).³⁶ Ugotovilo je, da mora biti hramba osebnih podatkov glede na ključna načela iz zadevnih instrumentov Sveta Evrope ter zakonodajo in prakso drugih pogodbenic sorazmerna glede na namen zbiranja in časovno omejena, zlasti v policijskem sektorju.

4.2.5 Nadzor in sledenje lokacije

Slovenska Vlada je v predlogu prvega interventnega zakona oblikovala dva, z vidika varstva osebnih podatkov, sporna člena, in sicer 103. in 104. člen.³⁷

V 103. členu zakon širi že obstoječa pooblastila policistov za namen zagotovitve spoštovanja ukrepov, ki so potrebni za zaježitev in obvladovanje epidemije COVID-19. Določba po mnenju Informacijske pooblaščenke, predstavlja širitev pooblastil do te mere, da je mogoče zajeti potencialno celotno prebivalstvo Republike Slovenije in v praksi bi to pomenilo vzpostavitev policijske države. Posegi v pravice posameznikov so po mnenju informacijske pooblaščenke preveč nedoločno in zelo široko opredeljeni. Ukrepi lahko namreč posežejo tudi v pravice posameznikov, ki niso predmet ukrepov zakona o nalezljivih boleznih in bi bili na primer podvrženi zahtevam po samoizolaciji, zdravljenju ali karanteni.³⁸

³⁵ Monteleone, S.: Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?, *European Journal of Law and Technology*, letnik 3, številka 3.

³⁶ *Združene zadeve S. in Marper proti Združenemu kraljestvu*, 4. decembra 2008, št. 30562/04 in 30566/04.

³⁷ Zakon o interventnih ukrepih za zaježitev epidemije covid-19 in omilitev njenih posledic za državljane in gospodarstvo, PREDLOG, NUJNI POSTOPEK, EVA 2020-1611-0028.

³⁸ Mnenje informacijske pooblaščenke Mojce Prelesnik o Predlogu Zakona o interventnih ukrepih za zaježitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo –EVA 2020-1611-0028, z dne 30.3.2020,

<https://www.iprs.si/fileadmin/user_upload/Pdf/pripombe/2020/DZ_interventni_zakon_MNENJE_30032020_koncno.pdf> (27.4.2020).

104. člen predloga interventnega zakona določa ti. druga pooblastila policiji. Besedilo tega člena je bilo naslednje: *Če ni mogoče drugače zagotoviti spoštovanja z odločbo ali drugim aktom odrejenih ukrepov iz zakona, ki določa nalezljive bolezni, smejo policisti brez odredbe sodišča od operaterjev mobilnih omrežij pridobivati podatke o lokaciji komunikacijskega sredstva osebe, na katero se ukrep iz tega odstavka nanaša, vendar le pod pogojem, da je oseba s tem pisno soglašala pred izdajo odločbe ali drugega akta, v katerem je osebi odrejen ukrep.*

Informacijska pooblaščenka opozarja, da zakonsko pooblastilo za sledenje posameznikom iz 104. člena pomeni resen poseg v ustavno pravico do varstva osebnih podatkov in komunikacijske zasebnosti. Ustava v 37. členu takšen poseg v ustavno pravico dopušča le z izdajo sodne odredbe. Kot zaskrbljujoče pa izpostavlja tudi dejstvo, da bo za pridobitev podatkov predpogoj posameznikovo soglasje, ker naj bi že samo besedilo predloga zakona nakazovalo, da gre za »prisilno« in zgolj navidezno soglasje, posledično naj bi šlo za pravno zlorabo pojma soglasje. Prav tako zakon jasno ne opredeljuje, kdo soglasje sploh pridobi. Največja pomanjkljivost pa se zdi dejstvo, da se lahko sledenje in pridobivanje podatkov razširi tudi na osebe, zoper katere ukrep iz Zakona o nalezljivih boleznih³⁹ sploh ni bil izrečen. Vendar pa bi lahko tudi slednji postali predmet nazora zgolj zaradi situacije, ker bi bili v stiku ali lokacijski bližini osebe, zoper katero pa je ukrep izrečen. Informacijska pooblaščenka je Državnemu zboru predlagala, da omenjenih členov v predlagani obliki ne podpre, saj ukrepi po njenem mnenju niso sorazmerni. Dodaja še, da iz pretekle inšpekcijske prakse Informacijskega pooblaščenca izhaja nemalo primerov, ko je policija podatke pridobivala nezakonito ter jih hranila predolgo, zato je skrb ob trenutnem stanju vsekakor upravičena.

Interventni zakon je stopil v veljavo 11. aprila 2020.⁴⁰ Državni zbor je zavrnil predlog 104. člena in podprl 103. člen zakona. Informacijska pooblaščenka je na Državni zbor Republike Slovenije in na Vlado Republike Slovenije naslovila odprto pismo.⁴¹ Podprla je zahtevo za presojo ustavnosti 103. člena Zakona o interventnih ukrepih za zaježitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo, ki so jo na Ustavno sodišče Republike Slovenije naslovile opozicijske politične stranke. V času pisanja tega poglavja, je zahteva za presojo ustavnosti še

³⁹ Zakon o nalezljivih boleznih (Uradni list RS, št. 33/06 – uradno prečiščeno besedilo in 49/20 – ZIUZEOP).

⁴⁰ Zakon o interventnih ukrepih za zaježitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo (Uradni list RS, št. 49/20).

⁴¹ Odprto pismo Informacijske pooblaščenke, z dne 24.4.2020, <https://www.ip-rs.si/fileadmin/user_upload/Pdf/Covid19/Odprto_pismo.pdf>, (27.4.2020).

nerešena. Informacijska pooblaščenka meni, da bo Ustavno sodišče tako lahko preverilo nujnost ukrepov, z vidika ocen zdravstvene stroke ter pretehtalo vse vidike utemeljenosti, legitimnosti in sorazmernosti teh posegov. Vendar pa vsekakor meni, da določba 103. člena zakona sporna, saj bodo na podlagi določbe lahko represivni organi pridobivali podatke za nejasne namene, množično in na zalogo. Gre za ti. »ribarjenje po podatkih brez vnaprejšnjega suma kršitve – »fishing expedition«. Tovrstni ukrepi po njenem mnenju, tudi v času trenutnih spremenjenih razmer, ne bi smeli biti dopuščeni. Sklicuje se na smernice Evropskega odbora za varstvo podatkov (EDPB), ki izpostavljajo, da Splošna uredba o varstvu podatkov (GDPR) in Direktiva o zasebnosti in elektronskih komunikacijah že vsebujeta določbe, ki omogočajo uporabo osebnih podatkov, za podporo javnim organom in drugim akterjem, za spremljanje in omejevanje širjenja COVID-19. Vendar pa morajo vsi ukrepi držav članic temeljiti na splošnih načelih učinkovitosti, nujnosti in sorazmernosti. Kot sprejemljivo EDPB navaja aplikacijo, ki bi sledila razdalji med posameznimi uporabniki aplikacije, nasprotuje pa vsesplošnemu sledenju gibanja posameznika. Odprto pismo informacijska pooblaščenka zaključuje z navedbo, da se spoštovanje zrcali med drugim ali predvsem tudi v načelu sorazmernosti –da torej oblast državljanse spoštuje do te mere, da ji ti lahko zaupajo, da bo pri posegih v njihove pravice zmerna in bo vanje posegala le toliko, kolikor je to nujno potrebno za doseg ustavno dopustnega cilja.

Potrebno se je zavedati, da policijski nadzor s pomočjo tehnologije iz dneva v dan napreduje. Tovrstne prakse se poslužujejo tudi policijske uprave v več mestih. V Vancouvru je vzpostavljen sistem ti. »prediktivne policije«. Na podlagi dosedanjih izkušenj z vlomi na področju Vancouvra je napravljena statistika, ki ob določeni uri prikaže potencialna žarišča in pojave vlomov. V skladu s prikazom se na določene lokacije napoti policiste. Po njihovih navedbah naj bi bilo število vlomov trenutno na najmanjši stopnji, zahvaljujoč tej tehnologiji. Glede nadzora pa se javnost pomirja z besedami, da ne nadzoruje oseb temveč le lokacije.⁴² Algoritmov se poslužujejo tudi v Los Angelesu.⁴³ Zagotovo ima takšen sistem pozitivne in negativne vidike. Kaj se zgodi, če se oseba naključno znajde na ti. ogroženem potencialnem mestu za vlom? Lahko se zgodi, da bo policist prehitro domneval, da ima oseba namen storiti

⁴² Matt Meuse: Vancouver police now using machine learning to prevent property crime, CBC, 2017, <<https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111>> (5.6.2020).

⁴³Nate Berg: Predicting crime, LAPD-style, The Guardian, 2014, <<https://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report#maincontent>> (5.6.2020).

odklonilno dejanje. Kot že rečeno je algoritem lahko pripomoček ne pa nadomestilo za zdravo kmečko pamet.

4.2.6 Internet stvari

Si lahko predstavljamo potek našega povprečnega dneva v prihodnosti, da bomo zjutraj vstali, ko nas bo zbudil telefon na podlagi predhodnega izračuna, da smo se dovolj naspali in ponoči nismo imeli slabih sanj in drugih motenj? Nato bomo uporabili pametni WC, ki lahko spreminja lučke in spremlja, če je naš metabolizem zdrav. Nato si bomo roke umili s pametno pipo, ki deluje na ukaz. Nato bomo kosilo pripravili v pametni pečici, ki na podlagi izbire jedi sama prilagodi način peke in pa vročino. Pred tem pa bomo za nasvet o izbiri kosila seveda vprašali našega elektronskega asistenta na telefonu, ki naše navade in želje pozna že boljše kot mi sami. Zatem bomo ostanke odvrgli v pametni smetnjak, ki bo sproti beležil vsebino in nam preko opozorila na telefonu javil, kdaj ga bo potrebno izprazniti. Umazana oblačila bomo samo postavili v pralni stroj, potem pa ga bomo vključili preko mobilne aplikacije, ko se nam bo to zdelo primerno. Naš odhod na dopust ne bo več problem, saj bomo lahko na daljavo nahranili tudi naše hišne ljubljence in na daljavo spremljali kje v hiši se nahajajo in kaj počnejo. Tudi skrb za otroke ne bo več problem, saj že v tem trenutku poznamo prototipe za pametne pleničke, ki spremljajo zdrav metabolizem in starše preko aplikacije obvestijo, kdaj je otroka potrebno previti. Če smo se do sedaj osredotočali na enoto doma, pa si poskusimo predstavljati, da se to preslika še na področje celotnega kraja mesta, države, celo sveta? Vse to bo lahko omogočil internet stvari, ki bo med seboj povezal svetovni splet in vse naprave v našem domu in okolici. Do leta 2020 naj bi bilo v omrežje interneta stvari priključenih kar 30 milijard naprav.⁴⁴ To zajema tako pametne merilce vlage v stanovanju kot visokotehnološka letala. To želi vzpostaviti podjetje SideWalk Labs, ki spada pod istega lastnika kot Google. Namen te družbe je vzpostavitev pametnega mesta in družbe, preko vzpostavitve videonadzora in digitalizacije vseh spektrov življenja. Projekt je že v teku in sicer se vzpostavitev

⁴⁴ Gaylor, B.: Internet vsega, dokumentarni film, Kanada, 2020, <<https://4d.rtvsl.si/arhiv/tuji-dokumentarni-filmi-in-oddaje/174697585>> (3.6. 2020).

načrtuje v Torontu, vendar pa se nevladne organizacije in različna združenja proti temu vztrajno borijo.⁴⁵⁴⁶

Vendar pa ne smemo vseh tehnologij metati v isti koš, določene inovacije so lahko namenjene tudi koristi uporabnikov. Tovrsten primer je naprava KEGG, ki skrbi za zbiranje podatkov o plodnosti ženske in po zagotovitvi vodstva podjetja, naj podatkov ne bi delila s svetom. To bi namreč lahko pomenilo, da bi bile ženske, ki imajo težave s plodnostjo, slabše obravnavane pri zavarovanju.⁴⁷

4.3 Vpliv digitalizacije na družinsko življenje

Družina je življenjska skupnost otroka, ne glede na starost otroka, z obema ali enim od staršev ali z drugo odraslo osebo, če ta skrbi za otroka in ima po tem zakoniku do otroka določene obveznosti in pravice. Družina zaradi varstva koristi otroka uživa posebno varstvo s strani države.⁴⁸

Digitalizacija povzroča razdor med tradicionalnimi vlogami staršev in otrok.⁴⁹ V zadnjih dveh desetletjih so otroci, ki so aktivno gledali televizijo, ponotranjili informacijo, da so njihovi starši sebični, neodrasli, neizobraženi in na splošno nevedni. Kot primer televizijske vsebine, ki je tovrstne informacije podala otrokom, avtor navaja televizijske nadaljevanke *Malcolm in the Middle* (Glavca),⁵⁰ *Family Guy* (Griffinovi),⁵¹ *Two and a Half Men* (Dva moža in pol),⁵² ter resničnostne šove o super varuškah. Vendar pa že sama uporaba tehnologije v smislu različnih klepetalnic in igranja video iger povzroči, da se komunikacija med otroci in starši močno poslabša. Zanimiva so opažanja, da uporaba tehnologije za učne namene ni prizadela komunikacije v isti meri, kot uporaba tehnologije za socialna omrežja in prosti čas. Otroci, ki neprestano uporabljajo socialna omrežja, naj bi imeli s strani svojih staršev

⁴⁵ Barreto, D.: Normalizing mass surveillance: Sidewalk Labs' threat to human rights, *Now Magazine*, 2019, <<https://nowtoronto.com/news/sidewalk-labs-privacy-human-rights/>> (6.6.2020); Yasmin Aboelsau, Y.: Canadian Civil Liberties Association threatening lawsuit over Google's Sidewalk Labs, *Venture Toronto*, 2019, <<https://dailyhive.com/toronto/canadian-civil-liberties-association-sidewalk-labs-open-letter-2019>> (6.6.2020).

⁴⁷ Lunden, I.: Kegg tracks your fertility by measuring vaginal mucus with a kegel ball, 2018, <<https://techcrunch.com/2018/09/05/kegg-kegel-ball-fertility/>> (6.6.2020).

⁴⁸ Družinski zakonik (Uradni list RS, št. 15/17, 21/18 – ZNOrg, 22/19 in 67/19 – ZMatR-C).

⁴⁹ Taylor, J.: Is Technology Creating a Family Divide? <<https://www.psychologytoday.com/intl/blog/the-power-prime/201303/is-technology-creating-family-divide>> (6.6.2020).

⁵⁰ <<https://www.imdb.com/title/tt0212671>> (6.6.2020).

⁵¹ <https://www.imdb.com/title/tt0182576/?ref_=nv_sr_srsg_0> (6.6.2020).

⁵² <https://www.imdb.com/title/tt0369179/?ref_=nv_sr_srsg_3> (6.6.2020).

občutek manjše podpore. Prav tako do nedavnega naši starši še niso bili večji tehnologije, v zadnjih letih se ta trend seveda obrača, vendar otroci in mladostniki tehnologijo jemljejo kot samoumevno, saj so jo lahko ponotranjali od samega začetka njihovega zavedanja. Zato lahko omejitve glede časovne uporabe in načina uporabe tehnologije, postavljene s strani staršev, vrzel v odnosu z otroci še povečajo. Nezmožnost vzpostavitve kakovostnega odnosa pa privede do tega, da starši ne morejo več vedeti, kaj se v življenju njihovih otrok sploh dogaja. Vendar pa grešni kozel ni vedno otrok, saj je tehnologija omrežila tudi starše, ki z neprestanim govorjenjem po telefonu, pregledovanjem elektronske pošte in gledanjem televizije, otrokom povzročijo občutek nezanimanja. Obstajajo primeri, ko so starši želeli komunikacijo z otroci vzpostaviti preko tehnologije, tako da so se tudi sami pridružili socialnim omrežjem, vendar to v nikakršni meri en more zamenjati navadne primarne komunikacije. K fenomenu razpada družine pa vsekakor prispeva tudi dejstvo, da so se domovi družin povečali za kar petdeset odstotkov, število družinskih članov pa v povprečju zmanjšalo, kar pomeni, da ima vsak član družine možnost popolne izolacije. Razkorak pa privede do tega, da družinski člani med sabo niso več sposobni imeti kakovostnega pogovora. To pa se pokaže predvsem v izrednih časih, kot smo jim priča v času pandemije Korona virusa.

Zagotovo so se razmere za vstop v družbo skozi zgodovino spremenile do te mere, da so primeri iz zgodovine (mentorstva starejši učenjakov, ki so že uveljavljeni v družbi, vključevanje v elitna združenja idr.), popolno nasprotje današnji praksi. Z razvojem tehnologije so mentorji mladostnikom postali predvsem drugi mladi, saj trenutna starejša generacija še zaostaja z znanjem. Ta vzorec pa se bo verjetno čez čas spremenil. Vzrok za ustvarjanje velike razlike med mlajšo in starejšo generacijo pa naj bi bil tudi v tem, da se dandanes od mladih zahteva velika mera samostojnosti in s tem povezanega sprejemanja pomembnih življenjskih odločitev.⁵³ V zadnjih letih je stroka namreč opozarjala na to, da način vzgoje ti. helikopterskih staršev, lahko otrokovemu razvoju osebnosti tudi škodi.⁵⁴

⁵³ Doward, J. in Hall, S.: Technology cuts children off from adults, warns expert, The Guardian, 2019, <<https://www.theguardian.com/society/2019/apr/27/technology-threatens-child-development-psychology-expert-warns>> (8.6.2020).

⁵⁴ Angleško Helicopter parents, Razjasnitev pojma v oddaji Dobro jutro, RTV Slovenija, 1.6.2017, <<https://4d.rtvsl.si/arhiv/dobro-jutro/174474629>> (8.6.2020).

Področje vpliva digitalizacije na družinsko življenje, je za raziskovalce zelo zahtevno, saj so rezultati anket in raziskav pogosto lahko odvisni od okolja in družbe v kateri se izvajajo. Prav tako pa je zelo težko preučevati najbolj intimna razmerja med družinskimi člani. Problem nastane pri raziskovanju vsebin, ki družinske člane razdvajajo ali pa jih zblížujejo, saj tretje osebe nimajo vpogleda v vsebino, ki jo določena oseba spremlja in je zato nemogoče razvozlati, kaj ljudje počnejo s svojimi prenosniki, tablicami ali pametnimi telefoni. Kot primer, v preteklosti je bilo lažje pridobiti podatke o tem, kaj družina glede preko TV, saj so podatke o številkah lahko posredovali televizijski ponudniki, v primeru brskanja in uporabljanja aplikacij pa je to veliko težje in seveda tudi sporno z vidika varstva osebnih podatkov.⁵⁵

Seznam literature in virov

Monografije

Korpič-Horvat, E.: Razvoj socialne varnosti in varovanje človekovega dostojanstva v odločitvah Ustavnega sodišča Republike Slovenije, Podjetje in delo, št. 6-7, 2018.

Članki in poglavja iz knjig

Monteleone, S.: Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?, European Journal of Law and Technology, letnik 3, številka 3.

Pravni viri

Ustava Republike Slovenije (Uradni list RS, št. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99 in 75/16 – UZ70a).

Zakon o nalezljivih boleznih (Uradni list RS, št. 33/06 – uradno prečiščeno besedilo in 49/20 – ZIUZEOP).

Zakon o interventnih ukrepih za zajezitev epidemije COVID-19 in omilitev njenih posledic za državljane in gospodarstvo (Uradni list RS, št. 49/20).

Zakon o interventnih ukrepih za zajezitev epidemije covid-19 in omilitev njenih posledic za državljane in gospodarstvo, PREDLOG, NUJNI POSTOPEK, EVA 2020-1611-0028.

Družinski zakonik (Uradni list RS, št. 15/17, 21/18 – ZNOrg, 22/19 in 67/19 – ZMatR-C).

Nemška zvezna ustava, Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 28. Juni 2022 (BGBl. I S. 968) geändert worden ist.

Zakon o ratifikaciji Konvencije o varstvu človekovih pravic in temeljnih svoboščin, spremenjene s protokoli št. 3, 5 in 8 ter dopolnjene s protokolom št. 2, ter njenih protokolov št. 1, 4, 6, 7, 9, 10 in 11 (Uradni list RS – Mednarodne pogodbe, št. 7/94)

Listina unije o temeljnih pravicah, UL EU C 303 z dne 14.12.2007, str. 1-16.

⁵⁵ Anja Riitta Lahikainen in Ilkka Arminen: Family, media and digitalization of childhood, 2017, <https://helda.helsinki.fi/bitstream/handle/10138/231835/12_Chapter12final2017.pdf?sequence=1> (9.6.2020).

Direktiva Evropskega parlamenta in Sveta 98/44/ES z dne 6. julija 1998, o pravnem varstvu biotehnoloških izumov, Uradni list Evropske unije, L 213, 30.7.1998, str. 13–21.
Evropska komisija, BELA KNJIGA o umetni inteligenci - evropski pristop k odličnosti in zaupanju, COM(2020) 65 final.

Sodna praksa

Zadeva »Titova cesta«, Ustavno sodišče RS, Sodba U-I-109/10 z dne 26. septembra 2011.
Zadeva C-377/98, *Kraljevina Nizozemska proti Parlamentu in Svetu*, ECLI:EU:C:2001:523.
Zadeva C-131/12, *Google Spain SL in Google Inc. proti Agencia Española de Protección de Datos (AEPD) in Mariu Costeji Gonzálezu*, ECLI:EU:C:2014:317.
Združene zadeve S. in Marper proti Združenemu kraljestvu, 4. decembra 2008, št. 30562/04 in 30566/04.

Spletni viri

<https://www.imdb.com/title/tt0182576/?ref_=nv_sr_srsrg_0> (6.6.2020).
<<https://www.imdb.com/title/tt0212671>> (6.6.2020).
<https://www.imdb.com/title/tt0369179/?ref_=nv_sr_srsrg_3> (6.6.2020).
Alexa has been eavesdropping on you this whole time, Geoffrey Fowler, The Washington Post, <<https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/>> (4.5.2020).
ALGORITHMS AND HUMAN RIGHTS, Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, Svet Evrope 2018, <<https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>> (2.6.2020).
An Amazon Echo recorded a family's conversation, then sent it to a random person in their contacts, report says, Hamza Shaban, The Washington Post, <<https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-family-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/?noredirect=on>> (4.5.2020).
Anja Riitta Lahikainen in Ilkka Arminen: Family, media and digitalization of childhood, 2017, <https://helda.helsinki.fi/bitstream/handle/10138/231835/12_Chapter12final2017.pdf?sequence=1> (9.6.2020).
Barreto, D.: Normalizing mass surveillance: Sidewalk Labs' threat to human rights, Now Magazine, 2019, <<https://nowtoronto.com/news/sidewalk-labs-privacy-human-rights/>> (6.6.2020);
Yasmin Aboelsau, Y.: Canadian Civil Liberties Association threatening lawsuit over Google's Sidewalk Labs, Venture Toronto, 2019, <<https://dailyhive.com/toronto/canadian-civil-liberties-association-sidewalk-labs-open-letter-2019>> (6.6.2020).
Berg, N.: Predicting crime, LAPD-style, The Guardian, 2014, <<https://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report#maincontent>> (5.6.2020).
Cadwalladr C., Graham-Harrison, E.: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 2018, <<https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>> (1.6.2020).
China's High-Tech Tool to Fight Toilet Paper Bandits, New York Times, <<https://www.nytimes.com/2017/03/20/world/asia/china-toilet-paper-theft.html>> (3.5.2020).
Dobro jutro, RTV Slovenija, 1.6.2017, <<https://4d.rtvsllo.si/arhiv/dobro-jutro/174474629>> (8.6.2020).
Doward, J. in Hall, S.: Technology cuts children off from adults, warns expert, The Guardian, 2019, <<https://www.theguardian.com/society/2019/apr/27/technology-threatens-child-development-psychology-expert-warns>> (8.6.2020).

- Gaylor, B.: Internet vsega, dokumentarni film, Kanada, 2020, <<https://4d.rtvlo.si/arhiv/tuji-dokumentarni-filmi-in-oddaje/174697585>> (3.6. 2020).
- Lee, S.: Who uses my health data, <<https://www.goinvo.com/vision/who-uses-my-health-data/>> (19.4.2020).
- Leo Kelion: Coronavirus: Covid-19 detecting apps face teething problems, <<https://www.bbc.com/news/technology-52215290>> (19.4.2020).
- Lunden, I.: Keggs tracks your fertility by measuring vaginal mucus with a kegel ball, 2018, <<https://techcrunch.com/2018/09/05/kegg-kegel-ball-fertility/>> (6.6.2020).
- Marshall Allen: You Snooze, You Lose: Insurers Make The Old Adage Literally True, Propublica, 2018, <<https://www.propublica.org/article/you-snooze-you-lose-insurers-make-the-old-adage-literally-true>> (1.6.2020).
- Meuse, M.: Vancouver police now using machine learning to prevent property crime, CBC, 2017, <<https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111>> (5.6.2020).
- Mnenje informacijske pooblaščenke Mojce Prelesnik o Predlogu Zakona o interventnih ukrepih za zaježitev epidemije COVID-19 in omilitve njenih posledic za državljane in gospodarstvo – EVA 2020-1611-0028, z dne 30.3.2020, <https://www.iprs.si/fileadmin/user_upload/Pdf/pripombe/2020/DZ_interventni_zakon_MNENJE_30032020_koncno.pdf> (27.4.2020).
- Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v Evropski uniji – Del II, Agencija FRA, 2018, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2-summary_sl.pdf> (4.5.2020).
- Nadzor, ki ga izvajajo obveščevalne službe: zaščitni ukrepi in pravna sredstva v zvezi s temeljnimi pravicami v EU – Del I: Pravni okvir državljanov članic, Agencija FRA, 2015, <<https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELLAR:35149923-8c2c-11e5-b8b7-01aa75ed71a1&from=FR>> (4.5.2020).
- NEC unveils facial recognition system for 2020 Tokyo Olympics, <<https://www.theverge.com/2018/8/7/17659746/tokyo-2020-olympic-games-face-recognition-nec>> (3.5.2020).
- Never forget a face? Research suggests people know an average of 5,000 faces, University of York, <<https://www.york.ac.uk/news-and-events/news/2018/research/never-forget-a-face/>> (3.5.2020).
- Newman Forbes, D.: What Is Privacy In The Age Of Digital Transformation? <<https://www.forbes.com/sites/danielnewman/2019/05/02/what-is-privacy-in-the-age-of-digital-transformation/#8050c9c628ed>>, (4.5.2020).
- Odprto pismo Informacijske pooblaščenke, z dne 24.4.2020, <https://www.iprs.si/fileadmin/user_upload/Pdf/Covid19/Odprto_pismo.pdf>, (27.4.2020).
- Radio televizija Slovenija, Oddaja Ugriznimo v znanost: Prepoznavanje obrazov, 13.12.2018, <<https://4d.rtvlo.si/arhiv/ugriznimo-znanost/174582438>> (3.5.2020).
- Rory Cellan-Jones: Coronavirus: What went wrong with the UK's contact tracing app?, BBC, 20.6.2020, <https://www.bbc.com/news/technology-53114251?at_custom4=8D4889AE-B307-11EA-A6BA-17F3C28169F1&at_custom3=BBC+News&at_custom2=facebook_page&at_medium=custom7&at_custom1=%5Bpost+type%5D&at_campaign=64> (21.6.2020).
- RTV SLO, <<https://www.rtvlo.si/znanost-in-tehnologija/tudi-slovenska-policija-uporablja-avtomatsko-prepoznavo-obrazov/510776>> (3.5.2020).
- Singer, N.: When Apps Get Your Medical Data, Your Privacy May Go With It, The New York Times, <<https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html>> (20.4.2020).
- SPECIAL EUROBAROMETER 359 Attitudes on Data Protection and Electronic Identity in the European Union REPORT Fieldwork: November – December 2010, objavljeno junija 2011

- <<https://joinup.ec.europa.eu/collection/eidentity-and-esignature/document/eu-attitudes-data-protection-and-electronic-identity-european-union>> (3.5.2020).
- Sodišče prepovedalo testno prepoznavanje obrazov na šolah v Marseillu in Nici, RTV SLO, <<https://www.rtvlo.si/znanost-in-tehnologija/sodisce-prepovedalo-testno-prepoznavanje-obrazov-na-solah-v-marseillu-in-nici/516064>> (3.5.2020).
- Štempihar, A.: Kaj je zares digitalno poslovanje?, IIBA Slovenija, april 2017, <https://slovenia.iiba.org/sites/slovenia/files/IIBA_mesecniki/mesecniki_clanki/Mesecnik_IIBA_april_2017-Clanek_%20Kaj_zares_je_digitalno_poslovanje_AS.pdf> (20.4.2020).
- Taylor, J.: Is Technology Creating a Family Divide? <<https://www.psychologytoday.com/intl/blog/the-power-prime/201303/is-technology-creating-family-divide>> (6.6.2020).
- Tehnologija, ki stoji za kriptovalutami, bi lahko reševala življenja, <<http://m.racunalniskenovice.com/index.php?id=tehnologija-ki-stoji-za-kriptovalutami-bi-lahko-resevala-zivljenja.html>> (19.4.2020).
- This Is What Your Phone Does with Your Personal Health Data, Mark Henricks, <<https://www.shape.com/fitness/trends/health-apps-privacy-personal-information-shared>> (19.4.2020).
- Zdravstveni podatki, Informacijski pooblaščenec, <<https://www.ip-rs.si/varstvo-osebnihpodatkov/inspekcijski-nadzor/najbolj-pogoste-krsitve/zdravstveni-podatki>> (19.4.2020).

