DOI
https://doi.org/10.18690/um.pf.4.2023.3

ISBN
978-961-286-774-4

3 PRAVICA DO ZASEBNOSTI V POVEZAVI Z UMETNO INTELIGENCO

ELENA OSRAJNIK
Univerza v Mariboru, Pravna fakulteta, Maribor, Slovenija
elena.osrajnik@student.um.si

Ključne besede:
umetna inteligence,
zasebnost,
osebni podatki,
obdelava podatkov,
povezane naprave

V prihodnosti bodo sistemi umetne inteligence vedno bolj inkorporirani v naš vsakdan, kar bo naše življenje zagotovo izboljšalo, prav tako pa bomo lahko z njihovo uporabo izpostavljeni večjim tveganjem, tudi na področju varstva temeljnih pravic. Škoda, ki jo lahko umetna inteligenca povzroči, je lahko stvarna, torej varnost in zdravje posameznika in škoda na premoženju, lahko pa je tudi nestvarna, kar zajema omejitev svobode izražanja in spoštovanja človekovega dostojanstva, diskriminacijo ter izgubo zasebnosti. V tem sklopu sem se osredotočila predvsem na zadnje, torej izgubo zasebnosti. Preučila sem, kako je zasebnost posameznika zaščitena pri uporabi sistemov umetne inteligence, kot so internet stvari, avtonomna vozila, deepfake posnetki in prilagojeni oglasi. Možnosti za kibernetski vdor je pri sistemih interneta stvari in avtonomnih vozil veliko, saj so medsebojno povezane naprave priključene na internet, kamor pošiljajo zbrane podatke. Prav tako pravico do zasebnosti kršijo deepfake posnetki, ki temeljijo na tehnologiji prepoznave obraznih potez, ter prilagojeni oglasi, ki zbirajo in obdelujejo podatke o iskalnih navadah in preferencah uporabnika. Grožnjo zasebnosti predstavljajo tudi številne aplikacije, ki so uporabljene za pridobivanje osebnih podatkov uporabnikov, ki se tega sploh ne zavedajo.

Univerzitetna založba Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.pf.4.2023.3

ISBN
978-961-286-774-4

Keywords:
artificial intelligence,
privacy,
personal data,
data processing,
connected devices

University of Maribor Press

3 The Right to Privacy in Connection With Artificial Intelligence

Elena Osrajnik
University of Maribor, Faculty of Law, Maribor, Slovenia
elena.osrajnik@student.um.si

In the future, the systems of artificial intelligence will be increasingly incorporated into our lives. On one hand, this will improve our daily struggles, however, on the other hand these systems my induce violations of basic human rights. The potential damage, which may be caused by AI can be material, compromising individual's safety, health and assets, or non-material, that is freedom of speech, respect, discrimination and interference with privacy. In this section, I focused mainly on the latter, interference with privacy. I asked myself how protected is the privacy of the users of AI systems, like internet of things, autonomous driving solutions, deepfakes and targeted advertising. Both internet of things and autonomous cars may violate the privacy rights, as their connection to internet enables cybernetic irruption. In the same manner, deepfake technologies, which are based on identification of facial features, andtargeted advertisement, , which note the searching habits and preferences of the users, invade the individual's privacy. The menace of privacy interference is also represented by numerous apps, which collect private information of the users without their knowledge.

3.1 Uvod

Umetna inteligenca je koncept, ki zajema veliko področij, kot so kognitivno računalništvo, strojno učenje, obogatena inteligenca in inteligentna robotika. Kognitivno računalništvo temelji na algoritmih, ki sklepajo in se učijo na višji ravni, torej je njihovo »razmišljanje« bolj podobno človeškemu. Strojno učenje temelji na algoritmih, ki se avtonomno učijo izvajanja nalog s pomočjo prejšnjih vnesenih podatkov o opravljeni nalogi. Obogatena inteligenca pa temelji na sodelovanju med človekom in strojem, inteligentna robotika pa je umetna inteligenca, ki je vgrajena v robote.

Razvoj umetne inteligence in raziskave na vseh prej naštetih področjih so v glavnem namenjene avtomatiziranju inteligentnega obnašanja, vključno z zmožnostjo logičnega sklepanja, zbiranja informacij, načrtovanja, učenja, komuniciranja, manipuliranja, signaliziranja in celo ustvarjanja, sanjanja in zaznavanja. Ločimo dva tipa umetne inteligence in sicer inteligenco v ožjem pomenu, kjer gre za zmožnost izvajanja točno določenih nalog, in umetno inteligenco v splošnem pomenu, kjer gre za zmožnost izvajanja vseh intelektualnih nalog, ki jih je sposoben opraviti človek.

Do danes so razviti številni načini uporabe umetne inteligence v splošnem pomenu, kot so virtualni pomočniki, avtonomni avtomobili, samodejno združevanje informacij oz. internet stvari, prepoznavanje glasu, programska oprema za prevajanje, programska oprema za pretvorbo besedila v govor, avtomatizirane finančne transakcije, e-odkrivanje v sodstvu itd. In čeprav imajo te implementacije umetne inteligence veliko korist človeku, s seboj prinašajo tudi nevarnosti za ohranjanje njegove zasebnosti, saj je za delovanje katerekoli uporabe umetne inteligence potrebna izmenjava informacij in podatkov.

Evropski ekonomsko-socialni odbor je glede varstva zasebnosti že izrazil skrb glede ciljno naravnane uporabe sistemov umetne inteligence, ki se že uporabljajo. Takšne oblike so recimo filtrni mehurčki, ki posamezniku ponujajo zgolj tiste vsebine, za katere je v preteklosti pokazal zanimanje, lažne novice na družbenih omrežjih, prilagojeni oglasi in volilne kampanje, združevanje informacij v pametnih stanovanjih in avtonomnih avtomobilih itd.

3.2 Pravna ureditev

3.2.1 Zakonodaja v Evropski uniji

3.2.1.1 Primarno pravo Evropske unije

V Pogodbi o delovanju Evropske Unije (v nadaljevanju PDEU)[1] 16. člen opredeljuje osebne podatke in njihovo obdelavo. V njem je zapisano, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. Prav tako so v PDEU zapisana pravila o varstvu fizičnih oseb pri obdelavi podatkov s strani institucij, organov, uradov in agencij Unije ter držav članic v okviru dejavnosti s področja uporabe prava Unije, in o prostem pretoku takih podatkov. Ta pravila sta določila Evropski parlament in Svet po rednem zakonodajnem postopku, upoštevanje teh pravil pa nadzirajo neodvisni organi.

Pravica do spoštovanja zasebnega je opredeljena tudi v 8. členu Evropske konvencije o varstvu človekovih pravic (v nadaljevanju EKČP)[2], ki opredeljuje zasebno in družinsko življenje. V EKČP je zapisano, da ima vsak posameznik pravico do spoštovanja njegovega zasebnega in družinskega življenja, doma in dopisovanja, pri čemer se javna oblast ne sme vmešavati v izvrševanje te pravice, razen če je to določeno z zakonom in nujno v demokratični družbi. To pomeni, da se v zasebno življenje sme posegati zgolj 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.

Varstvo zasebnosti in osebnih podatkov pa sta opredeljena tudi v Listini Evropske unije o človekovih pravicah (v nadaljevanju Listina)[3], kjer 7. in 8. člen opredeljujeta spoštovanje zasebnega in družinskega življenja ter varstvo osebnih podatkov. V 7. členu Listine je zapisano, da ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, stanovanja ter komunikacij. V 8. členu Listine pa piše, da ima vsakdo pravico do varstva osebnih podatkov, ki se nanj nanašajo. Osebni podatki posameznikov se morajo obdelovati pošteno, za določene namene in na

[1] Pogodba o delovanju Evropske Unije, Uradni list Evropske unije, C 326/47, str. 47-390.
[2] 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).
[3] Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

podlagi privolitve prizadete osebe ali na drugi legitimni podlagi, določeni z zakonom. Ta člen zagotavlja tudi, da ima vsakdo pravico dostopa do svojih podatkov in pravico zahtevati, da se ti podatki popravijo. Spoštovanje teh pravil nadzira neodvisen organ.

Generalni pravobranilec P. Cruz Villalón je zadevah C-293/12 in C-594/12 ugotovil, da Direktiva o hrambi podatkov[4] nasprotuje Listini, saj omogoča ponudnikom telefonskih in elektronskih komunikacijskih storitev, da zbirajo in hranijo podatke o lokaciji in prometu teh komunikacij, s čimer ustvarijo zanesljivo in natančno sliko o identiteti uporabnika storitev. To pa je v nasprotju z Listino, saj direktiva izrazito posega v pravico državljanov do spoštovanja zasebnega življenja. Zbranih podatkov ne hranijo javni organi, temveč zasebna podjetja, prav tako pa v direktivi ni določeno kje se morajo podatki hraniti, zato lahko pride do kopičenja podatkov na nedoločenih krajih v kibernetičnem prostoru. Po mnenju pravobranilca direktiva prav tako ni združljiva z načelom sorazmernosti, saj se morajo podatki hraniti za obdobje najmanj šestih mesecev in največ dveh let. Direktiva je zato neveljavna, saj niso dovolj natančno opredeljeni zaščitni ukrepi, s katerimi bi bila urejena dostop do zbranih in hranjenih podatkov ter njihova uporaba.

V zadevi C-207/16 je Sodišče ugotovilo, da se lahko posega v pravici do zasebnega življenja in varnosti osebnih podatkov, ki sta opredeljeni v Listini, v primeru dostopa do osebnih podatkov, ki jih hranijo ponudniki elektronskih komunikacij, če poseg ne pomeni hude kršitve zasebnega življenja. Dostop do identifikacijskih podatkov imetnikov kartic SIM, kot so priimek, ime in po potrebi naslov teh imetnikov, resda pomeni poseg v temeljne pravice, zagotovljene z Listino, vendar so v Direktivi 2002/58/ES[5] natančno opredeljeni cilji, ki lahko upravičijo dostop do osebnih podatkov s strani javnih organov.

3.2.1.2 Sekundarno pravo Evropske unije

Do leta 2018 je veljala Direktiva (EU) 2016/680[6], ki je opredelila varstvo posameznika pri obdelavi osebnih podatkov. S tem so se zavarovale temeljne pravice

[4] Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES, Uradni list Evropske unije, L 105/54, 13.4.2006.
[5] Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, Uradni list Evropske unije, L 201/37, 31.7.2002.
[6] Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali

in svoboščine posameznikov, zlasti njihova pravica do varstva osebnih podatkov. Prav tako se je zagotovila neomejena in ne prepovedana izmenjava osebnih podatkov med pristojnimi organi v Uniji, če je izmenjava določena v pravu Unije ali držav članic. To direktivo je leta 2018 zamenjala Uredba (EU) 2018/1725[7] (v nadaljevanju Splošna uredba o varstvu podatkov), ki določa pravila o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Unije in pravila o prostem pretoku osebnih podatkov med njimi ali drugimi uporabniki, ustanovljenimi v Uniji.

Splošna uredba o varstvu podatkov varuje temeljne pravice in svoboščine posameznikov, zlasti njihovo pravico do varstva osebnih podatkov, kar je temeljna človekova pravica. Splošna uredba o varstvu podatkov se uporablja predvsem za obdelavo osebnih podatkov, ki se delno ali v celoti izvajajo z avtomatiziranimi sredstvi, in za obdelavo osebnih podatkov, ki so del zbirke ali so namenjeni oblikovanju dela zbirke, ki se izvaja z avtomatiziranimi sredstvi.

Splošna uredba o varstvu podatkov določa, da sta v obdelavo podatkov navadno vključeni dve stranki – posameznik, o katerem se zbirajo podatki in upravljavec, ki podatke zbira, obdeluje in analizira. Posameznik mora jasno, prostovoljno, konkretno in informirano privoliti v zbiranje njegovih osebnih podatkov, upravljavec pa privolitve ne sme izrabiti za posredovanje podatkov tretji osebi, saj s tem krši varnost osebnih podatkov. Najbolj varovani morajo biti genski podatki, saj predstavljajo edinstvene in nenadomestljive informacije o fiziologiji ali zdravju posameznika, in biometrični podatki, ki prav tako predstavljajo edinstveno identifikacijo posameznika glede ne njegovo podobo obraza ali daktiloskopske podatke.

Podatki, ki se zbirajo v zbirkah podatkov, morajo biti obdelani zakonito, pošteno in na pregleden način, prav tako pa morajo biti zbrani za določene namene in se ne smejo obdelovati na način, ki ni združljiv s temi nameni. Osebni podatki morajo biti točni in posodobljeni ter obdelani na način, ki zagotavlja ustrezno varnost podatkov. Prav tako morajo predstavljati najmanjši obseg podatkov, potrebnih za obdelavo in

pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, Uradni list Evropske unije, L 119/89, 4.5.2016.

[7] 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) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.

hranjeni v obliki, ki dopušča identifikacijo posameznika le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki shranjujejo.

Kadar je obdelava podatkov omogočena s privolitvijo posameznika, mora slednja biti jasna, razumljiva in v lahko dostopni obliki. Posameznik, na katerega se obdelava podatkov nanaša, ima pravico kadarkoli preklicati privolitev, kar more biti enako enostavno kot privoliti v obdelavo. Osebni podatki se lahko obdelujejo tudi brez privolitve posameznika, na katerega se nanašajo, če upravljavec oceni, da ima nadaljnja obdelava povezavo z namenom prvotne obdelave in če so ti podatki ustrezno zaščiteni s šifriranjem ali psevdonimizacijo. Psevdonimizacija pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče povezati s specifičnim. Prav tako pa mora upravljavec biti pozoren na okoliščine v katerih so bili zbrani osebni podatki, na njihovo naravo in na morebitne posledice predvidene nadaljnje uporabe.

Upravljavec baze podatkov mora posamezniku, od katerega pridobiva osebne podatke, zagotoviti svojo identiteto in kontaktne podatke, kontaktne podatke osebe pooblaščene za varstvo podatkov, namene, za katere se osebni podatki obdelujejo, uporabnike ali kategorije uporabnikov osebnih podatkov ter, če je to potrebno, tudi dejstvo, da upravljavec namerava prenesti osebne podatke v tretjo državo. Prav tako mora upravljavec posameznika seznaniti z obdobjem hrambe osebnih podatkov, možnostjo, da posameznik zahteva dostop do svojih osebnih podatkov, podatke izbriše ali jih popravi, ter obstojem avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov.

Posameznik ima pravico do popravka osebnih podatkov kadarkoli, upravljavec pa mora njegove zahteve upoštevati in brez nepotrebnega odlašanja popraviti netočne podatke, ali pa jih popolnoma izbrisati iz baze. Posameznik pa ima tudi pravico do omejitve obdelave, če oporeka točnosti osebnih podatkov, če je obdelava nezakonita, če upravljavec podatkov ne potrebuje več v namene obdelave, vendar jih posameznik potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov in med potekom postopka ugotovitve zakonitih razlogov za ugovarjanje obdelavi podatkov. Vsi podatki, ki jih posameznik pridobi od upravljavca morajo biti oblikovani v strukturirano, splošno uporabljano in strojno berljivo obliko. Posameznik lahko te podatke brez vednosti prvotnega upravljavca posreduje drugemu izbranemu upravljavcu, če je bila obdelava izdelana z avtomatiziranimi sredstvi in je temeljila na privolitvi posameznika.

Upravljavec mora, ob upoštevanju narave, obsega, okoliščin in namenov obdelave, izvesti ustrezne tehnične in organizacijske ukrepe, s katerimi dokaže, da je obdelava v skladu z uredbo, kar pomeni, da mora izvajati ustrezne politike za varstvo podatkov. Posluževati se mora psevdonimizacije, upoštevati mora načelo najmanjšega obsega podatkov ter v obdelavo vključiti potrebne zaščitne ukrepe. Upravljavec mora zagotoviti, da se obdelajo samo tisti osebni podatki, ki so potrebni za določen namen obdelave, prav tako pa mora to upoštevati tudi pri količini zbranih podatkov, njihovem obsegu obdelave, obdobjem hrambe in njihovi dostopnosti.

Upravljavci lahko najamejo obdelovalca podatkov, ki zgolj sodeluje z upravljavci, ki so pravno odgovorni za pravično obdelavo osebnih podatkov. Obdelovalec mora o vseh spremembah sproti obveščati upravljavca, njegovo obdelavo pa ureja pogodba ali drug pravni akt v skladu s pravom Unije ali pravom države članice. Vsak upravljavec mora voditi evidenco dejavnosti obdelave v okviru svoje odgovornosti, ki mora vsebovati ime in kontaktne podatke upravljavca, pooblaščene osebe za varstvo podatkov in, kadar je ustrezno, obdelovalca in skupnega upravljavca. Prav tako mora biti v njej zapisan namen obdelave, opis kategorij posameznikov in vrst osebnih podatkov, kategorije uporabnikom, katerim bodo razkriti osebni podatki, kadar je ustrezno tudi informacije o prenosu podatkov v tretjo državo.

Za varnost obdelave morata obdelovalec in upravljavec poskrbeti za izvajanje ustreznih tehničnih in organizacijskih ukrepov, kot sta psevdonimizacija in šifriranje osebnih podatkov. Prav tako morata v celotnem procesu obdelave podatkov poskrbeti za stalno zaupnost, celovitost, dostopnost in odpornost sistemov za obdelavo, v primeru fizičnega ali tehničnega incidenta pa morata biti zmožna pravočasno povrniti razpoložljivost in dostop do osebnih podatkov. Varnost obdelave osebnih podatkov mora biti zagotovljena tudi s postopkom rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov.

Če pride do kršitve varnosti osebnih podatkov, je upravljavec obvezan o tem obvestiti Evropskega nadzornika za varstvo podatkov najkasneje 72 ur od kršitve. Upravljavec mora o kršitvi zasebnosti osebnih podatkov obvestiti tudi posameznika, na katerega se podatki nanašajo, če bi kršitev povzročila veliko tveganje za pravice in svoboščine posameznikov. V obvestilu mora jasno in v preprostem jeziku opisati vrsto kršitve, ter navesti ukrepe za preprečitev kršitve. Če upravljavec o kršitvi ne

obvesti posameznika, lahko Evropski nadzornik za varstvo podatkov to od njega zahteva.

Splošna uredba o varstvu podatkov je uredila »pravico do pozabe« v zadevi Google Spain, kjer je bilo odločeno, da lahko posameznik od upravljalca zbirke podatkov zahteva izbris povezave s seznama zadetkov, ki so se prikazali po izvedenem iskanju, opravljenem na podlagi imena osebe in vsebujejo informacije o navedeni osebi. M. Costeja Gonzáleza je vložil pritožbo proti družbi Google, s katero je zahteval, naj sprejme ukrepe, potrebne za umik osebnih podatkov, ki se nanašajo nanj, s svojega seznama, in v prihodnje onemogoči dostop do njih. Ker podjetje Google »išče«, »zbira«, »beleži« in »ureja« podatke ter jih po potrebi »posreduje« svojim uporabnikom v obliki seznama zadetkov, ga lahko smatramo kot obdelovalca podatkov, mora upoštevati določila Splošne uredbe o varstvu podatkov. To pomeni, da je zavezana odstraniti povezave na spletne strani s seznama zadetkov, če se posamezni zanjo odloči.

Splošno uredbo o varstvu podatkov so kršile Združene države Amerike, kot je bilo ugotovljeno v zadevi C-362/14, kjer je Sodišče ugotovilo, da ne zagotavljajo ustrezne raven varnosti prenesenih osebnih podatkov. M. Schrems je vložil tožbo proti Data Protection Commissioner (pooblaščenec za varstvo podatkov), v zvezi s predhodno vloženo tožbo proti družbi Facebook Ireland Ltd, ki je v Združene države Amerike prenašala osebne podatke svojih uporabnikov in jih shranjevala na strežnikih v tej državi. V tej je tožnik zahteval, naj pooblaščenec družbi Facebook Ireland prepove prenašanje osebnih podatkov v združene države Amerike, saj veljavno pravo in praksa v tej državi ne zagotavljata zadostne zaščite osebnih podatkov. Sodišče je ugotovilo, da ameriški sistem varnega pristana, s čimer varujejo prenesene osebne podatke, omogoča, da ameriški javni organi posegajo v temeljne pravice posameznikov, še posebej do pravice do zasebnosti. Ker v Ameriki nimajo urejenega enakega sistema obdelave osebnih podatkov, kot je urejen v Evropski uniji, lahko dostopajo do podatkov in jih obdelujejo na način, ki ni v skladu z namenom njihovega prenosa, prav tako pa posamezniki nimajo dostopa do upravnega in sodnega varstva, ki bi jim omogočalo, da lahko dostopajo do svojih podatkov, jih popravijo ali izbrišejo. Tako je Sodišče odločbo Komisije o ustreznosti varstva prenesenih osebnih podatkov spoznalo za neveljavno in zahtevalo ponovno preučitev pritožbe M. Schremsa, ter odločitev o ustavitvi prenosa podatkov evropskih uporabnikov družabnega omrežja Facebook v Združene države.

V zadevi Scarlet Extendet SA proti Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) je Sodišče ugotovilo, da je sodba nacionalnega sodišča glede nezakonitega prenašanja datotek kršila pravico do varstva osebnih podatkov, ki ga ureja Splošna uredba o varstvu podatkov. Belgijsko sodišče je na predlog družbe SABAM od družbe Scarlet Extendet SA zahtevalo, da na lastne stroške vzpostavi sistem za filtriranje elektronskih komunikacij, ki bi pregledoval kateri prenosi datotek so nezakoniti in tako kršijo avtorske pravice. Takšen sistem bi pregledoval celotno spletno komunikacijo med uporabniki storitev družbe Scarlet Extendet SA, kar bi pomenilo vzpostavitev splošnega nadzora nad strankami. Vendar pa direktiva o elektronskem poslovanju nacionalnim organom prepoveduje sprejemati ukrepe, s katerimi bi bila ponudniku internetnega dostopa naložena obveznost splošnega nadzora podatkov, ki jih prenaša v svojem omrežju. Prav tako pa bi takšen nadzor posegal v pravico do varstva osebnih podatkov, zato je Sodišče odgovorilo, da nasprotuje odločitvi belgijskega sodišča o odreditvi sistema za filtriranje vseh elektronskih komunikacij uporabnikov storitev družbe Scarlet Extendet SA.

Spor o vzpostavitvi splošnega sistema filtriranja informacij in s tem kršenja pravice do varstva osebnih podatkov se je nadaljeval v zadevi C-360/10, vendar v tem primeru med družbama SABAM in Netlog NV. V tej zadevi je družba SABAM prav tako zahtevala vzpostavitev sistema filtriranja vseh informacij, ki si jih med seboj pošiljajo uporabniki storitev družbe Netlog NV, ki bi pregledoval in poiskal nezakonito preneseno glasbeno in avdiovizualno vsebino. Sodišče je bilo v tej zadevi mnenja, da takšen sistem, ki bi pregledoval celotno komunikacijo med vsemi uporabniki storitev, preveč posega v pravico do varstva osebnih podatkov. Takšna odreditev bi pomenila sistematično obdelavo in analizo informacij uporabnikov storitev družbe Netlog, te informacije pa so varovani osebni podatki, saj omogočajo identifikacijo uporabnika, zato bi odreditev sistema filtriranja informacij kršila pravico do varstva osebnih podatkov.

3.2.2 Zakonodaja v Sloveniji

Splošna uredba o varstvu podatkov se v Sloveniji uporablja neposredno, v veljavo je stopila leta 2016, uporablja pa se od maja 2018. Do tedaj je v Sloveniji zbiranje, obdelavo in uporabo osebnih podatkov narekoval Zakon o varstvu osebnih podatkov (v nadaljevanju ZVOP-1). [8]

[8] Zakon o varstvu osebnih podatkov, Uradni list RS, št. 94/07 – uradno prečiščeno besedilo.

Ker je zaradi izjemnega razvoja informacijsko-komunikacijske tehnologije v količini in kakovosti obdelave osebnih podatkov in so ti postali vedno bolj dostopni državi, zasebnemu sektorju ter posameznikom, so se začele izvajati vedno bolj sistemske povezave med zbirkami osebnih podatkov. S tem pa so se povečala tveganja zlorabe osebnih podatkov, kot so nepooblaščeni dostopi, množična razkritja in profiliranje posameznikov. Evropska komisija je v te namene predlagala sprejetje dveh novih pravnih aktov Evropske unije in sicer Splošno uredbo o varstvu podatkov in Predlog Direktive Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ.[9]

Zaradi sprejetja teh aktov, se je morala tudi slovenska zakonodaja spremeniti in prilagoditi, zato je bilo pripravljeno besedilo predloga novega Zakona o varstvu osebnih podatkov (v nadaljevanju **ZVOP-2**).[10] S tem bi se zagotovilo izvrševanje določb Splošne uredbe o varstvu podatkov in visok nivo varstva osebnih podatkov v Republiki Sloveniji ter uresničevanje osebne človekove pravice do varstva osebnih podatkov, vsakršno neupoštevanje teh določil pa bi bilo kaznovano z natančno določenimi sankcijami. Tudi informacijski pooblaščenec je izrazil svoje mnenje o predlogu novega zakona o varstvu podatkov, kjer je tudi opozoril na še ne dorečene zadeve. Jasno je potrebno določiti kakšen nadzor bo veljal glede zakonitosti obdelave osebnih podatkov, ki jih izvajajo varnostnoobveščevalne službe in takšno določitev jasno zakonsko predeliti in urediti. Prav tako je med drugim potrebno tudi uskladit in jasno uredit pritožbeni postopek glede izvajanja pravic ter nameniti dodatno pozornost ureditvi kazenski določb v predlogu.

V 2020 pa je bil še zmeraj v veljavi ZVOP-1, v katerem je zapisano, da se osebni podatki obdelujejo zakonito in pošteno, ter morajo biti ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. Varstvo osebnih podatkov je zagotovljeno vsakemu posamezniku ne glede na njegovo narodnost, raso, barvo, veroizpoved, etično pripadnost, spol, jezik,… Osebni podatki se lahko obdelujejo le, če je posameznik privolil v obdelavo ali če to določa zakon.

[9] Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, Uradni list Evropske unije, L 359/60, 30.12.2008.

[10] Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20).

Posameznik mora biti o obdelavi osebnih podatkov seznanjen pisno ali na drug ustrezen način, oz. če je obdelava določena v zakonu.

Osebne podatke lahko obdeluje obdelovalec, če je podpisal pogodbo z upravljavcem in je registriran za opravljanje takšne dejavnosti. Občutljivi osebni podatki, kot so podatki o rasnem, narodnem poreklu, političnem, verskem ali filozofskem prepričanju, spolnem življenju itd. se lahko obdelujejo zgolj v uredbi določenih primerih. Prav tako morajo biti pri obdelavi posebej označeni in zavarovani s kriptografskimi metodami in nečitljivostjo elektronskih podpisov.

Vsi osebni podatki, vneseni v zbirko podatkov, morajo biti točni in ažurni, prav tako pa mora upravljavec o obdelavi obvestiti posameznika. V zbirk podatkov ni dovoljena uporaba istega povezovalnega znaka, da ostane identiteta posameznika prikrita. Osebni podatki se lahko shranjujejo le toliko časa, kolikor služijo doseganju namena, za katerega so se zbirali in obdelovali, po izpolnitvi namena se izbrišejo, uničijo, blokirajo ali anonimizirajo.

Zbirke osebnih podatkov se morajo varovati pred slučajnimi ali namernimi nepooblaščenimi uničenjem podatkov tako, da se varujejo prostori, oprema in sistemska programska oprema zbirke, ter aplikativna programska oprema s katero se obdelujejo podatki. Preprečevati se mora nepooblaščen dostop do osebnih podatkov med njihovim prenosom in zagotavljati učinkovit način uničenja, izbrisa ali anonimizacije osebnih podatkov. Zbirke osebnih podatkov se med seboj lahko povezujejo le, če zbirke ne vsebujejo občutljivih podatkov ali podatkov iz kazenske evidence in prekrškovnih evidenc. O združevanju so upravljalci dolžni obvestiti posameznike, o katerih se podatki zbirajo.

Državni nadzorni organ za varstvo osebnih podatkov vodi in vzdržuje register zbirk osebnih podatkov, ki mora biti dostopen vsakemu posamezniku. Prav tako ima posameznik možnost zaprositi za vpogled v katalog zbirke osebnih podatkov upravljavca osebnih podatkov, ki mu mora omogočiti tudi potrditev, ali se podatki v zvezi s posameznikom obdelujejo, posredovanje izpisa posameznikovih osebnih podatkov iz zbirke in seznam uporabnikov, katerim so bili podatki posredovani. Vsak posameznik ima pravico do dopolnitve, popravka, blokiranja in izbrisa lastnih podatkov iz baze, prav tako pa ima pravico do ugovora, s čimer se njegovi osebni podatki prenehajo obdelovati. Če posameznik ugotovi, da so mu kršene njegove pravice, zapisane v zakonu, lahko zahteva sodno varstvo ves čas, dokler kršitev traja.

Upravljavcu osebnih podatkov je dovoljeno uporabljati osebne podatke posameznikov tudi za namene neposrednega trženja, torej ponujanja blaga, storitev, zaposlitve, itd. V ta namen lahko uporablja zgolj osebne podatke posameznikov, kot so osebno ime, naslov prebivališča, telefonsko številko, naslov elektronske pošte in številko telefaksa. O lastni uporabi osebnih podatkov za neposredno trženje je upravljavec primoran obvestiti posameznika, prav tako tudi ob posredovanju podatkov drugim uporabnikom podatkov za namene neposrednega trženja. Posameznik pa ima pravico kadarkoli prekiniti obdelavo podatkov za namene neposrednega trženja, kar mora upravljavec upoštevati.

3.2.2.1 Informacijski pooblaščenec

Informacijski pooblaščenec med drugim skrbi tudi za to, da je obdelava osebnih podatkov v skladu z trenutno veljavno zakonodajo. To je Splošna uredba o varstvu podatkov, ki velja na Evropski ravni, ter nacionalna zakonodaja, ki ureja varstvo osebnih podatkov. Informacijski pooblaščenec lahko tudi preprečuje in odpravlja kršitve na tem področju.

Če posameznik meni, da so mu bile kršene pravice v zvezi z varovanjem zasebnosti in se njegovi podatki ne obdelujejo zakonito, lahko poda prijavo informacijskemu pooblaščencu. Pred vložitvijo prijave lahko posameznik zahteva seznanitev z lastnimi osebnimi podatki, lahko pa zahteva tudi popravek, omejitev obdelave ali popoln izbris svojih nezakonito obdelovanih podatkov. Posameznik lahko pri upravljavcu uveljavlja svojo pravico do prenosljivosti, ki jih je posameznik posredoval na podlagi privolitve ali pogodbe z upravljavcem. Ta pravica omogoča posamezniku, da pridobi svoje osebne podatke v strukturirani, splošno uporabljeni in razumljivi obliki, katere lahko dalje posreduje drugemu upravljavcu, ne da bi ga prvi pri tem oviral.

Informacijski pooblaščenec lahko, po relevantnih določbah Zakona o varstvu osebnih podatkov, Splošne uredbe o varstvu podatkov in subsidiarno na podlagi določb Zakona o inšpekcijskem nadzoru ter Zakona o splošnem upravnem postopku, izvaja inšpekcijski nadzor. Informacijski pooblaščenec lahko v okviru inšpekcijskega nadzora preverja ravnanje zavezancev za varstvo osebnih podatkov, če je skladno z zakonodajo. Nadzira, da se osebni podatki obdelujejo zakonito in pregledno, so ukrepi, da se zagotovi varovanje osebnih podatkov po členu 32 Splošne uredbe o varstvu podatkov, da se izvajajo določbe te uredbe, ki urejajo

posebna izraze načela odgovornosti, kot so uradno obveščanje nadzornih organov in posameznikov o kršitvi varnosti, ocene učinka, evidence dejavnosti obdelave, itd. S Splošno uredbo o varstvu podatkov ima informacijski pooblaščenec preiskovalna in popravljalna pooblastila, prav tako pa skrbi za informacijsko varnost državljanov.

3.2.3 Pravni in politični okvir za umetno inteligenco v Evropski uniji

3.2.3.1 Program digitalne Evrope za obdobje 2021-2027

Umetna inteligenca, napredno računalništvo in obdelava podatkov ter kibernetska varnost, bodo v prihodnosti temelj digitalne preobrazbe gospodarstva in družbe EU. Cilj predloga Uredbe Evropskega parlamenta in sveta o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027[11] je podpreti digitalno preobrazbo evropskega gospodarstva in družbe. Predlagana pravila iz vseh področij upoštevajo pravico posameznika do varstva zasebnosti, v skladu z 8. členom Listine. S Splošno uredbo o varstvu podatkov se bo zagotovil prost pretok osebnih podatkov med državami članicami EU, prav tako pa se bo okrepilo zaupanje ter varnost posameznikov. Na področju umetne inteligence bi morali vsi ukrepi, ki vključujejo obdelavo osebnih podatkov, podpirati Splošne uredbe o varstvu podatkov. V sklopu programa bi se na področju umetne inteligence povečala njena zmogljivost in zbiranje ter obdelava podatkov. Za izboljšanje kibernetske varnosti bi Unija podprla javno naročanje napredne opreme, orodij in podatkovnih infrastruktur, prav tako pa bi zagotovila široke uvedbe najnovejših rešitev za kibernetsko varnost.

3.2.3.2 Pravila civilnega prava o robotiki

Leta 2017 so bila sprejeta Pravila civilnega prava o robotiki, v Resoluciji Evropskega parlamenta s priporočili Komisiji o pravilih civilnega prava o robotiki (2015/2103(INL)) (2018/C 252/25)[12] , ki je med drugim opredelila tudi varstvo zasebnosti v dobi digitalizacije in vzpona robotike. Evropski parlament je ugotovil, da bi bilo potrebno nameniti pozornost robotom, ki pridobivajo in posredujejo osebne in občutljive podatke, saj lahko z nepravilnim ravnanjem ogrozijo zaupnost. Prav tako pa je potrebno zagotoviti skladna čezmejna pravila, katera bodo upoštevale

[11] Predlog UREDBA EVROPSKEGA PARLAMENTA IN SVETA o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027, COM/2018/434 final - 2018/0227.
[12] Resolucija Evropskega parlamenta s priporočili Komisiji o pravilih civilnega prava o robotiki (2015/2103(INL)), Uradni list Evropske unije, C 252/239, 18.7.2018, str. 239–257.

vse članice Unije, saj je za zavarovanje podatkov nujno potrebno sodelovanje med državami. Predpisi civilnega prava v sektorju robotike se morajo prilagoditi v skladu s Splošno uredbo o varstvu podatkov, prav tako pa se mora spoštovati pravico o varstvu osebnih podatkov, zapisano v 8. členu Listine EU o temeljnih pravicah.

Natančneje se morajo opredeliti pravila in merila za uporabo kamer in senzorjev v robotih, ki pridobivajo osebne podatke o posameznikih. Spoštovati pa se morajo tudi ostala načela o varstvu podatkov, kot so vgrajena in privzeta zasebnost, zmanjšanje količine podatkov, omejitev namena zbiranja podatkov, ter pregledni nadzorni mehanizmi za posameznike. Ker je prost pretok podatkov bistven za digitalno gospodarstvo sektorja umetne inteligence, je potrebno zagotoviti visoko raven varnosti v robotskih sistemih in v omrežjih povezave robotov, zasebnost pa je potrebno spoštovati tudi v komunikaciji med ljudmi, roboti in umetno inteligenco. Načrtovalci umetne inteligence imajo odgovornost razvijati varne, zaščitene in namenu prilagojene izdelke, ki ne smejo ogrožati varnosti zasebnosti posameznika.

Evropski parlament poziva evropsko Komisijo, da bo razvoj avtonomnih vozil zelo vplival na zasebnost posameznika, še posebej na področjih dostopa do podatkov, varstva podatkov in njihove izmenjave med povezanimi napravami. Ker je Evropski parlament predlagal tudi, da se pridobi večja avtonomnost avtonomnih vozil preko senzorjev in/ali z izmenjavo podatkov z lastnim okoljem in analizo le teh, bo potrebno večjo pozornost nameniti zavarovanju zasebnosti pred neželenimi vdori v sistem. Zasebnost državljanov bo potrebno bolje zavarovati na področju brezpilotnih zrakoplovov, saj bo moral imeti vsak brezpilotni zrakoplov vgrajen sistem za sledljivost in identifikacijo. Prav tako bo potrebno na področju popravljanja in izboljšanja človeka zagotoviti varnost pred vdorom v kibernetsko-fizične sisteme robotike, kot so recimo robotske proteze, kar bi lahko ogrozilo človeško zdravje, v skrajnih primerih pa tudi življenje.

Prav tako pa Evropski parlament poziva vse raziskovalce in načrtovalce, da naj ravnajo odgovorno in pri svojem delu upoštevajo potrebo po spoštovanju zasebnosti in dostojanstva ljudi, čeprav je kodeks prostovoljen. Vse raziskovalne dejavnosti bi bilo treba izvajati v skladu s previdnostnim načelom, torej s predvidevanjem morebitnih varnostnih vplivov, tudi na varovanje zasebnosti posameznika, kar spodbuja napredek v korist družbe.

3.2.3.3 Strategija za kooperativne inteligentne prometne sisteme

Leta 2018 je stopila v veljavo Resolucija Evropskega parlamenta o evropski strategiji za kooperativne inteligentne prometne sisteme (2017/2067(INI))[13], v kateri Evropski parlament med drugim, z ozirom na 7. in 8. člen Listine Evropske unije o temeljnih pravicah, glede prihodnosti storitev C-ITS opozarja na pomen izvajanja zakonodaje EU na področju zasebnosti in varstva podatkov. Opozarja, da je podatke potrebno uporabljati zgolj za namene C-ITS in se ne smejo hraniti ali uporabljati v druge namene, pametni avtomobili pa morajo biti povsem v skladu s Splošno uredbo o varstvu podatkov in povezanimi predpisi. Povečati je potrebno preglednost in algoritmično odgovornost obdelave in analize podatkov, ki ju izvajajo obdelovalci, prav tako pa se lahko s tehnikami anonimizacije poveča zaupanje uporabnikov v storitve C-ITS.

Varstvo podatkov in zaupnost je potrebno upoštevati skozi celotno obdelavo, Evropski parlament pa predlaga tudi oblikovanje aplikacij in sistemov z ozirom na vgrajeno in privzeto zasebnostjo in varnostjo podatkov. Predvsem pa poudarja, da je potrebno v pametnih vozilih omogočiti možnost »nepovezanega načina«, kar bi omogočilo, da bi uporabniki vozili avtomobil, ne da bi se osebni podatki prenašali v druge naprave. Za zagotavljanje varnosti komunikacij med sistemi C-ITS bo potrebno vzpostaviti visoke standarde kibernetske varnosti za preprečevanje vdorov in kibernetskih napadov. Z oblikovanjem skupne politike za varnost in potrdila v zvezi z uvedbo C-ITS, bo Evropski parlament poskušal preprečiti kakršnakoli tveganja za vdor v podatkovne zbirke avtomatiziranih vozil, saj so le-te najbolj izpostavljene kibernetskim napadom. V vseh državah članicah je potrebno izvajati visoke in harmonizirane varnostne standarde, ki bi tretjim strankam onemogočali dostop do vgrajenih sistemov, s čimer bi se lastnikom omogočila neodvisnost od proizvajalcev avtomobilov.

3.2.3.4 Posledice umetne inteligence za enotni (digitalni) trg

Leta 2017 je Evropski socialno-ekonomski odbor (EESO) sprejel mnenje o umetni inteligenci in njenih posledicah za enotni (digitalni) trg, proizvodnjo, potrošnjo, zaposlovanje in družbo[14], v katerem je opozoril na uporabo inteligence na

[13] Resolucija Evropskega parlamenta z dne 26. maja 2016 o strategiji za enotni trg (2015/2354(INI)), Uradni list Evropske unije, C 76, 28.2.2018, str. 112–127.

[14] Mnenje Evropskega ekonomsko-socialnega odbora – Umetna inteligenca – Posledice za enotni (digitalni) trg, proizvodnjo, potrošnjo, zaposlovanje in družbo (mnenje na lastno pobudo), Uradni list Evropske unije, C 288, 31.8.2017, str. 1–9

mednarodni ravni in skrbi za uveljavljanje etičnega kodeksa v Evropski uniji. Prav tako je EESO priporočil vzpostavitev sistema standardizacije, ki bi omogočil stalno preverjanje, potrjevanje in nadzor umetne inteligence, ter temeljito oceno evropske zakonodaje in predpisov, ki jih bo v prihodnosti potrebno prilagoditi.

Ker se je uporaba umetne inteligence implementirala na številna področja vsakodnevne uporabe, kot so gospodinjski aparati, pametne ure in zapestnice, igrače ter avtomobili, je potrebno poskrbeti za varnost zasebnosti, saj vse te naprave zbirajo osebne podatke, prodaja podatkov, ki jih zbere proizvajalec, pa je trenutno v polnem razmahu. Prav tako je s pomočjo umetne inteligence možno zbirati in analizirati veliko količino osebnih podatkov, katerih obdelava se kasneje uporabi za manipulacijo na številnih področjih, kot so poslovne odločitve in volitve itd. EESO opozarja tudi, da se je pri uporabi umetne inteligence potrebno izogniti omejevanju svobode posameznikov ter poskrbeti da bo razvoj na tem področju skladen z uredbo o varstvu podatkov. Pri prenosu podatkov mora tako biti spoštovana pravica do privolitve v obdelavo na podlagi seznanitve, prav tako pa tudi pravica dostopa do prenesenih podatkov, spremembe in preverjanja podatkov.

3.3 Uporaba umetne inteligence

3.3.1 Internet stvari

Internet stvari je skupek tehnologij za prepoznavanje stvari, senzornega zaznavanja in zmožnosti komuniciranja naprav z okoljem. Tehnologija interneta stvari temelji na komuniciranju preko tehnologije RFID. Za delovanje potrebuje podatke, ki jih pridobivajo in zbirajo vse medsebojno povezane naprave. Na osebni ravni je internet stvari uporaben za povečanje učinkovitosti gospodinjstva, saj dovoljuje da povezane naprave med seboj komunicirajo in reagirajo. Primer dobre prakse je recimo prižiganje pralnega stroja, ko je elektrika cenejša, pregled hladilnika in ustvarjanje seznama stvari, ki jih je zmanjkalo, ali pa prilagajanje svetlobe in glasbe glede na zvočni ukaz posameznika.

Za delovanje interneta stvari morajo senzorji z vseh povezanih naprav sprejemati in shranjevati osebne podatke, ki jih potrebujejo za usklajeno delovanje. Ker imajo senzorji, ki sprejemajo in posredujejo podatke povezanim napravam, zelo majhno zmogljivost shranjevanja podatkov, se le ti shranjujejo na spletu. Na vseh ravneh povezane verige je mogoč dostop hekerjev v sistem in dostop do zbirke podatkov.

Največkrat se vdor zgodi na Wi-Fi ruterju, saj se tukaj zberejo vsi podatki, preden se kompresirajo in pošljejo na splet v nadaljnjo obdelavo. Na tej fazi podatki še niso zakodirajo in anonimizirani, zato je zasebnost posameznika na tej točki najbolj ogrožena.

Takšni podatki so navadno zavarovani z različnimi tehnikami, kot je recimo tehnologija PPDM, PET, ki vsebuje virtualne zasebne spletne mreže, varnost transportnega sloja, DNS varnostna razširitev, čebulno usmerjanje in zasebno iskanje informacij. Prav tako je bila ustvarjena tehnologija PbD, ki skrbi za varnost in ohranjanje zasebnosti na vseh nivojih delovanja interneta stvari in je skladna s Splošno uredbo o varstvu podatkov. Te tehnologije skrbijo za varen prenos podatkov med napravami in tudi za ohranjanje identitete posameznika, vendar je v baze podatkov vseeno mogoče vdreti in jih posredovati tretjim osebam.

Da se zagotovi visoka stopnja varnosti podatkov, je nujno potrebno zagotoviti varen sistem kodiranja povezanih naprav, ki so odporne proti zlonamernim prilagoditvam kode. Z integracijo informacijskih tehnologij je postala zaščita proti spletnih vdorom vedno bolj pomembna funkcija povezanih naprav, zato dandanes oblikovalci industrijskega interneta stvari varnosti naprav posvečajo veliko pozornosti. Ker pa se prilagoditve informacijskih komponent na spletne vdore lahko ustvarijo šele po zlonamernem napadu, so industrijski sistemi interneta stvari ranljivi za različne spletne napade.

Napadi na industrijski internet stvari so lahko izvedeni na vseh abstraktnih ravneh delovanja, torej človeški, mehanski, spletni, programski in elektronski. Prva je človeška raven, kjer lahko hekerji pridobivajo podatke preko socialnega inženiringa ali lažnega predstavljanja (ang. *»phishing«).* Druga raven je mehanska, kjer lahko hekerji vdrejo v računalnike in pridobijo podatke na takšen način. Naslednja raven je mreženje, kjer se lahko zasebni podatki pridobivajo preko spletnega prisluškovanja, napada preko tretje osebe ali navidezno preobremenjenostjo sistema. Napadi pa se lahko zgodijo tudi na programsko opremo, kjer zlonamerni hekerji pridobivajo informacije z obratnim inženiringom, vdorom v računalniški sistem in invazivnimi napadi.

Cilji zavarovanja mreže povezanih naprav so velika razpoložljivost naprav, preprečevanje sistemskih napak, shranjevanje zgodovine delovanja posameznih naprav in najpomembnejši, zavarovanje integritete in zaupnosti podatkov. Na

podlagi teh ciljev se lažje ustvari varovanje pred spletnimi napadi, da lahko mreža naprav kljub vdoru v sistem deluje skoraj normalno. Skozi celotno delovanje mreže povezanih naprav morata biti zagotovljena aspekta varnosti in zasebnosti podatkov.

Zasebnost vključuje skrivanje zasebnih podatkov in tudi skrb za pravilno obravnavo podatkov. To pomeni, da lastniki zbirk podatkov ne smejo zbranih podatkov posredovati tretjim osebam, kot so recimo država, privatni sektorji in marketinškim podjetjem. Baza podatkov mora prav tako biti odporna na kakršnikoli napad, ter prilagoditi svoje delovanje v primeru napada. Vsebovati mora avtentične podatke, ki so preverjeni, lastnik baze pa mora imeti dostop do vseh podatkov, ter jih po potrebi posredovati lastnikom podatkov. Do podatkov je omogočen dostop le osebam, o katerih so podatki zbrani. Za varovanje zasebnosti morajo biti vsi podatki anonimni, kar pomeni, da iz njih ne moremo ugotoviti identitete posameznika. Vsi podatki morajo zato biti šifrirani, nepovezani in nedoločljivi, kar znižuje možnost identificiranja posameznika pri posredovanju podatkov tretji osebi.

Najbolj zaskrbljujoče tveganje za kršitev pravice do zasebnosti pa je zbiranje zasebnih informacij o posamezniku preko številnih medsebojno povezanih naprav, kot so identifikacijski podatki in vedenjski vzorci. Z napredkom tehnologij za pridobivanje, shranjevanje in obdelavo teh podatkov mora biti tudi pravilo prilagojena zakonodaja glede varovanja človekove zasebnosti. Direktiva, ki je že bila sprejeta na tem področju je Direktiva 95/46/ES in trenutno veljavna Uredba (EU) 2016/679. Vendar pa zgolj to ni dovolj, saj se neobdelani podatki, pridobljeni iz naprav, povezanih v internet stvari, ne smatrajo kot strogo osebni, saj preko njih ne moremo identificirati posameznika. Tako se ti podatki ne morejo zaščititi z uredbo GDPR, saj podatki tehnično gledano niso osebni. Ti podatki postanejo osebni zgolj z analiziranjem in različnimi kombinacijami v kasnejših fazah obdelave podatkov.

Prav tako so velika grožnja varovanju zasebnosti tudi tehnološke inovacije, ki omogočajo razvoj interneta stvari. Vendar pa so tehnologije lahko tudi del rešitve zasebnosti, če so ustvarjene in uporabljene na način, ki se sklada s standardi zasebnosti. Z naraščanjem števila zbranih podatkov s senzorjev, ki zbirajo informacije tudi o napravi sami, bo še bolj ogrožena varnost posameznika, saj kontekstualni podatki predstavljajo dodatno znanje o posamezniku in njegovi zasebnosti. Ti podatki niso šifrirani, saj je njihova pomembnost zelo majhna, vendar eksponentno narašča, če te podatke povežemo v celoto, zato bi bilo potrebno tudi takšne podatke zaščititi že v najzgodnejši fazi.

3.3.2 Avtonomna vozila

Avtonomna vozila so vsa računalniško nadzorovana vozila, ki se za samostojno vožnjo zanašajo na številne podatke, pridobljene iz različnih senzorjev vozila ali drugih vozil. S temi podatki lahko računalnik v vozilu prilagaja vožnjo okolju in nadzira delovanje vozila. Avtonomna vozila s funkcijami, kot so samodejno krmiljenje in parkiranje, samodejna menjava voznega pasu ter preprečevanje stranskih trkov, lahko zelo izboljšajo naša življenja. Vožnja bo postala enostavnejša, vozila bodo ljudem omogočala večjo produktivnost, saj bodo lahko med vožnjo opravljali druge funkcije, ne zgolj upravljanje vozila. Zaradi odstranitve človeškega faktorja (nepravilna ocena situacije, vinjenost zmanjšanost koncentracije, brezbrižnost ali prevelika naglica voznika ter napačno predvidevanje vožnje drugih voznikov), bo vožnja avtonomnih vozil varnejša.

Tehnologija, ki je vgrajena v avtonomne avtomobile, omogoča avtomatizacijo številnih funkcij, ki služijo kot pomoč pri vožnji, kot so tempomat, prostoročno telefoniranje, navodila po korakih in satelitske storitve. Vse te funkcije povečujejo število zbranih podatkov o vozniku in avtomobilu kot so podatki o lokaciji avta, stanje avtomobila, merjenje dostopa do podatkovnih storitev, čas, preživet v avtomobilu, itd. Avti tako postajajo vedno bolj integrirani z računalniškimi in telekomunikacijskimi tehnologijami, kar pomeni nov vir zbiranja podatkov o posamezniku.

Osebni avtomobili z različnimi senzorji nenehno zbirajo podatke o samem avtomobilu in tudi okolju, da se lahko nanj pravilno odzovejo v določeni situaciji. Zbirajo se podatki o tem kam se avto vozi, kje je bil, kaj se je z vozilom dogajalo med vožnjo in navade voznika. Vozilo tudi zbira podatke o tem kje je »voznik«, kaj počne, katere kraje je obiskal in katere še namerava. Te informacije so lahko povezane z drugimi informacijami. Lokacija parkiranega vozila sporoča o tem, kje stanuje lastnik, iz česar lahko ugotovimo njegovo splošno finančno stanje, ter napovemo njegova prihodnja dejanja. Če se ti podatki povežejo s posameznikom, ki ga je mogoče identificirati, podatki postanejo osebni, ti pa se nekje zbirajo in shranjujejo, kar predstavlja veliko grožnjo posameznikovi zasebnosti.

Ker avtonomna vozila za svoje delovanje potrebujejo nenehen pretok podatkov v realnem času med uporabnikom in okoljem ter med uporabnikom in shrambo podatkov, je kibernetski napad na sistem vozila mogoč preko različnih vstopnih

točk. Vendar pa proizvajalci avtov ne morejo izolirati vsakega senzorja, saj morajo ti komunicirati med sabo.

Evropska komisija je v svojem sporočilu Na poti do avtomatizirane mobilnosti: strategija EU za mobilnost prihodnosti[15] maja 2018 potrdila, da še vedno obstaja možnost kibernetskega napada in posledično prevzema nadzora nad vozilom. Do zdaj še ne obstaja sektorski pristop v zvezi z zaščito vozil pred kibernetskimi napadi, vendar v zvezi z varstvom podatkov v EU veljajo predpisi za vso obdelavo podatkov, tudi tistih, pridobljenih iz avtonomnih vozil. V Ameriki so bile pripravljene smernice za zaščito vozil pred kibernetskimi napadi, Komisija pa jih namerava uvesti tudi v Evropsko zakonodajo. Do zdaj so bile objavljene le smernice o politiki za potrdila in varnost komunikacije med vozili in ostalo infrastrukturo.

Pri vzpostavitvi nove zakonodaje o avtonomnih vozilih je potrebno vključiti varstvo osebnih podatkov uporabnikov povezanih vozil, saj morajo ti imeti zagotovilo, da so njihovi podatki skrbno obdelani ter biti obveščeni kako in za kakšne namene se uporabljajo in da lahko svoje podatke učinkovito nadzirajo. Podatki, pridobljeni iz avtonomnega vozila, bodo veljali za osebne, zato mora biti njihova obdelava skladna z že obstoječo zakonodajo, prav tako pa more v njihovo obdelavo privoliti uporabnik sam. Odzivi na javno posvetovanje so pokazali, da so lastniki avtonomnega vozila pripravljeni v deljenje osebnih podatkov, če so ti uporabljeni za povečanje varnosti v cestnem prometu ali izboljšanja upravljanja prometa.

Iz tega lahko sklepamo, da bi bili uporabniki pripravljeni deliti svoje osebne podatke v zvezi z avtonomnim vozilom, če bi ponudniki C-ITS (sodelovalni inteligentni prometni sistemi) storitev natančno opredelili pogoje uporabe, ter jih zapisali v jasnem in preprostem jeziku, na razumljiv način. Vendar pa bo uvedba C-ITS sistema v EU bo začasno odložena, dokler se ne vzpostavi zakonodaja za varovanja vozil pred vdori v sisteme in kibernetskimi napadi, s čimer se bo zagotovila tudi večja varnost osebnih podatkov končnih uporabnikov. Za vzpostavitev vseevropskega varnostnega okvirja za avtonomna vozila, bo potrebno upoštevati vse vključene strani, tako javne organe, kot tudi upravljalce cest, proizvajalce vozil ter dobavitelje in operaterje storitev C-ITS.

[15] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Na poti do avtomatizirane mobilnosti: strategija EU za mobilnost prihodnosti, COM/2018/283 final.

Evropska Komisija je v Sporočilu Evropskemu parlamentu, svetu, Evropskemu ekonomsko-socialnemu odboru in odboru regij predstavila Evropsko strategijo za kooperativne inteligentne prometne sisteme, ki predstavlja mejnik na poti h kooperativni, povezani in avtomatizirani mobilnosti[16]. V njem je zapisala, da bi lahko osebni podatki, zbrani v osebnih avtonomnih vozilih, bili zlorabljeni v različne namene, recimo s strani oglaševalskim agencije, kjer bi zbrane osebne podatke posameznika uporabili za prilagojene oglase in oglaševalske kampanje. Prav tako bi se lahko podatki zbirali v namene deanonimizacije posameznika, pri čemer bi lahko iz zbranih, sicer neosebnih podatkov, kot je lokacija avtomobila, ugotovili identiteto posameznika. Da bi se povečalo zaupanje v avtonomna vozila med ljudmi, so strokovnjaki predlagali večjo transparentnost zbiranja, obdelovanja, shranjevanja in uporabe podatkov. Grožnjo zasebnosti posameznika predstavljajo tudi avtonomna vozila, uporabljena v javnem prevozu ali podjetjih, saj bi se lahko sledilo vožnji avtomobila med celotno potjo, kar bi ogrozilo človekovo zasebnost in njegovo svobodo.

Osebno avtonomno vozilo je lahko ustvarjeno tako, da zbira minimalno količino osebnih podatkov lastnika, prav tako pa so podatki samega avtonomnega avta šifrirani in anonimni. Ker se po Uredbi GDPR podatki smejo hraniti le toliko časa, dokler služijo nekemu namenu, se lahko zasebnost lastnika ohrani na ta način, da se po določenem času izbrišejo podatki o njegovi lokaciji. To bi zmanjšalo tveganje, da bi se podatki zlorabljalo v prihodnje namene. Prav tako lahko k varovanju zasebnosti pripomoremo s pravilno zaščito podatkov, torej z anonimizacijo in šifriranjem.

Za zavarovanje posameznikove zasebnosti so nekatere države v EU sprejele neobvezne smernice o zasebnosti, ki jih proizvajalci avtonomnih vozila lahko upoštevajo. Evropska unija se je že leta 2009 začela zavedati tveganj, ki jih zasebnosti prinašajo avtonomna vozila in je od proizvajalcev zahtevala, da se tudi med proizvajanjem vozil upošteva varovanje osebnih podatkov posameznika. Zasebnost posameznika se je zelo zavarovala z uvedbo Uredbe GDPR med drugim tudi tako, da so okrepili pogoje za strinjanje z zbiranjem podatkov, prav tako pa so se zvišale kazni za kršitve uredbe.

[16] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Evropska strategija za kooperativne inteligentne prometne sisteme – mejnik na poti h kooperativni, povezani in avtomatizirani mobilnosti, COM/2016/0766 final.

3.3.3 Deepfakes

Umetno oblikovani videoposnetki oziroma deepfakes so ustvarjeni s pomočjo umetne inteligence, natančneje mehansko naučenih algoritmov, ki delujejo na podlagi nevronskih povezav in programske opreme za kartiranje obraza. Na teh posnetkih so obrazi ljudi zamenjani z obrazi drugih ljudi, ki niso v povezavi z videoposnetkom. To so digitalno manipulirani posnetki zvoka, slike ali videa tako, da osebe na posnetku lažno predstavljajo nekoga. S tem se na enostaven način lahko ukrade identiteta posameznika in se ustvari lažna percepcija druge osebe, katere obrazne poteze in zvok so dodane umetno ustvarjenemu posnetku. Na takšen način se kratijo pravice do zasebnosti osebi ali osebam na originalnem posnetku in tudi osebi ali osebam na umetno ustvarjenem posnetku. Takšen poseg v zasebnost posameznika lahko povzroči psihično škodo zaradi osramotitve in zadrege, lahko pa tudi vodi v izgubo kariere in ugleda posameznika v družbi.

Deepfake se po taksonomiji raziskave na Oxfordu leta 2020 razdeli na štiri kategorije, maščevalna pornografija, politične kampanje, zmanjšanje transakcijskih stroškov ter kreativni in originalni deepfake. Vendar pa pri vseh kategorijah obstaja grožnja zasebnosti posameznika.

Prva kategorija, maščevalna pornografija, je ustvarjena z namenom povzročitve ponižanja posameznika, navadno znane osebe. Pri tem se obraz osebe na izvirnem posnetku zamenja z obrazom znane osebe, katera ni dovolila takšne uporabe, saj zanjo ni vedela. Takšna uporaba slik in videoposnetkov posameznika se tretira kot poseg v spolno zasebnost posameznika, ki je nujna za razvoj osebnosti, intimnosti in enakosti. Deepfake posnetki so velikokrat del spolnega ponižanja in izkoriščanja ter fizične, mentalne ali finančne zlorabe.

Druga kategorija, politične kampanje, je ustvarjena z namenom zavajanja množice o izjavah politikov. Leta 2018 je podjetje Buzzfeed ustvarilo deepfake, s katerim je želel opozoriti javnost, kako enostavno je ustvariti neresničen video, ki se zdi, da je resničen. Na njem je bivši predsednik Barack Obama, ki v svojem glasu govori stvari, ki jih sam nikoli ne bi izrekel. Video je bil ustvarjen tako, da se je obrazna mimika Obame prilagajala obrazni mimiki osebe iz Buzzfeed, tako da je izgledalo, kot da sam govori besedilo. Takšne oblike deepfake posnetkov lahko zmanjšajo ugled posameznika v družbi, prikazujejo napačne ali izmišljene dogodke, ali pa vplivajo na demokratične procese države, kot so politične volitve.

Nevarnost deepfake posnetkov je ta, da ustvarjajo iluzijo resničnosti, ki je tako prepričljiva, da zavede gledalce v mišljenje, da so njihovi politiki in znane osebe govorili in delali stvari, ki jih nikoli ne bi, kar lahko privede do nezaupanja v te osebe. Prav tako ne bi več mogli zaupati video vsebinam, daj bi jih lahko kdorkoli spreminjal. Nekateri strokovnjaki trdijo, da imajo lahko »fake news«, vključno z deepfake posnetki bolj razpršen učinek kot navadne politične kampanje. Prav tako so študije pokazale, da ljudje precenjujemo lastno zmožnost ločevanja resničnega od neresničnega in da precenjujemo politične novice, ki so v skladu z našim mišljenjem, podcenjujemo pa novice, ki niso. Zato bomo verjeli le tistemu, kar se za nam zdi smiselno, torej tudi deepfake posnetkom, če bodo v skladu z našimi prepričanji.

Deepfakes posnetki lahko ostanejo na spletu za vedno in jih je zelo težko odstraniti, saj lahko se po izbrisu z določene platforme ponovno pojavijo na njej ali pa se pojavijo na novi platformi. Deepfake se večinoma uporabljajo za posmehovanje slavnih oseb, saj njihov obraz »nadenejo« drugi osebi, ki počne nekaj, kar javnost smatra za sramotno. Posnetki so uporabljeni tudi za izsiljevanje, umetno ustvarjen slikovni material, politično sabotažo, propagando in celo »fake news«. Deepfake posnetki predstavljajo veliko grožnjo zasebnosti posameznika, saj omogočajo komurkoli, da ponaredi video ali avdio posnetek osebe, v katerem sporoča želeno idejo ustvarjalca. Ker ljudje navadno verjamemo kar vidimo in sta video ali slika najmočnejši obliki prepričevanja, ne bomo podvomili v besede osebe na posnetku, saj bo zaradi napredne tehnologije izgledala zelo resnično.

Veliko grožnjo zasebnosti posameznika je predstavljala aplikacija za izdelavo deepfake posnetkov, imenovana ZAO. Aplikacija, s katero je lahko uporabnik nastopil v filmu ali televizijski seriji po izbiri, je bila na Kitajskem izdana septembra leta 2019. Uporabnik je posnetek oblikoval tako, da je posnel sebek (ang. *»selfie«*) ali naložil svojo fotografijo, izbral ustrezen film in s pomočjo tehnologije mehanskega učenja in biometrične prepoznave obraza poustvaril film tako, da je sam »nastopil« v njem. Uporabniki so morali pred samo uporabo aplikacije soglašati s pogojem, da lahko razvijalci aplikacije uporabljajo ustvarjene videoposnetke za kakršnokoli uporabo, brez nadaljnjega dovoljenja uporabnikov. Ker so razvijalci aplikacije s tem zelo posegli na področje varovanja zasebnosti, je bila aplikacija po dveh dnevih uporabe umaknjena iz platforme, na kateri je bila ustvarjena.

Aplikacija je z zbiranjem biometričnih podatkov zelo posegala v območje zasebnosti posameznika, ker so poteze obraza, glas, prstni odtisi in šarenica najstrožje varovani podatki, saj je identiteta posameznika z njihovo uporabo takoj prepoznana. Biometrični podatki so dandanes uporabljeni za potrditev identitete posameznika na različnih področjih, kot so spletno bančništvo, nadzor dostopa, e-poslovanje. Takšen sistem za preverjanje identitete posameznika omogoča visoko stopnjo zanesljivosti in prepoznavanja identitete, prav tako pa mora biti zaščita takšnih podatkov nujno potrebna, zlasti zato, ker jih ni mogoče nadomestiti ali spremeniti.

Najboljša rešitev za prepoznavanje deepfake posnetkov bi bil simultani razvoj programske opreme, ki bi bila sposobna hitro in zanesljivo prepoznati deepfake posnetek in ga označila kot ponarejenega. Prav tako bi se morala programska oprema prilagajati na nove tehnološke inovacije in tehnologije deepfake-ov. Vendar pa je realnost drugačna, saj po besedah profesorja Hany Farida, pionirja photoDNA tehnologije, današnja tehnologija ni dovolj razvita, da bi bila sposobna razločevati realen posnetka od ponarejenega.

3.3.4 Prilagojeno oglaševanje

Vsako dejanje, ki ga izvršimo na spletu, pusti za sabo sledi (ang. *»breadcrumbs«*), ki odražajo naše spletno obnašanje in vedenje. Ob analiziranju teh podatkov s pomočjo umetne inteligence, dobijo oglaševalska podjetja boljši vpogled v posameznikovo osebnost, s tem pa lahko posamezniku prilagodijo oglase, namenjene posebej zanj. Zaradi uporabe napovedovalske analitike, programskega oglaševanja in odzivnih iskanj, postajajo oglasi vedno bolj prilagojeni vsakemu uporabniku posebej.

Algoritmi umetne inteligence uporabljajo mehansko učenje pri zbiranju podatkov o tem, kaj vnašamo v iskalno okno, kdaj to iščemo, ter kaj počnemo neposredno po vnosu iskanega v brskalnik. Prav tako algoritmi ugotavljajo kaj počnemo z informacijami, ki jih dobimo kot rezultat iskanja in to ne zgolj na eni napravi, temveč na vseh z istim računom povezanih napravah.

S pomočjo napovedovalske analize se predvidijo prihodnje akcije posameznika, glede na vse zbrane podatke. Ustvari se osebnost posameznika, ki kasneje služi za prilagojeno oglaševanje, torej oglaševanje, namenjeno zgolj ljudem, ki so bili v procesu označeni kot določen tip osebnosti. Tak način poenostavi oglaševanje, saj so oglasi namenjeni točno določeni fokusni skupin. Podjetja tako prihranijo čas, ko

bi splošen oglas predstavljala večji skupini, katera nima interesa v oglaševan izdelek ali storitev, temveč se posvetijo manjšim skupinam, za katere je bolj verjetneje, da bodo kupile izdelek, saj so se že prej zanimale za podobne stvari.

Odzivno iskanje pa je novo oglaševalsko orodje Google oglaševalske platforme, ki omogoča oglaševalskim podjetjem enostavnejše prilagojeno oglaševanje s pomočjo umetne inteligence. Podjetja v oglaševalsko platformo vnesejo predloge oglasov in meta podatke, nato pa Googlovi algoritmi določijo kateri oglas iz zbirke je najprimernejši za posameznika. To pomeni, da bodo ljudje z enako določeno spletno osebnostjo dobili enake oglase, glede na njihovo zgodovino iskanja, navade in preference. Primer prilagojenega oglaševanja je ponudnik medijskih storitev Netflix, ki zbira podatke o serijah in filmih, katere je uporabnik pogledal in mu sestavi seznam vsebin, ki bi mu ustrezale glede na zgodovino ogledov.

Za takšno vrsto oglaševanja mora uporabnik sprejeti piškotke na strani, ki so majhne besedilne datoteke nameščene na uporabnikovo napravo, kamor se shranjujejo njegovi podatki o dejavnostih na določeni spletni strani. Poznamo sejne piškotke, ki olajšajo funkcionalnosti spletne strani, vanje se shranjujejo podatki o seji uporabnika, ter sledilne piškotke, kamor se shranjujejo osebne informacije posameznika, uporabljene za prilagojeno oglaševanje, navadno v obliki uporabe analitike, prikazovanja oglasov ali vdelane vsebine. Lastniki spletnih strani morajo o takšnih piškotkih obvestiti uporabnike ter zavarovati njihove podatke pred zlorabo s strani tretje stranke.

Piškotki so uporabljeni v namene vpogleda v uporabnikove preference in dejavnosti na določeni spletni strani ter identificiranja posameznika. Zasebnost končnih uporabnikov je vedno bolj ogrožena, še posebej zato, ker piškotke ne uporabljajo zgolj lastniki strani, temveč tretje stranke, ki izkoriščajo spletno stran, da bi prišle do podatkov o uporabnikov.

Velika večina piškotkov je ustvarjena tako, da se iz zbranih podatkov da ugotoviti identiteto končnega uporabnika. Takšni piškotki so recimo raziskave in orodja za klepet, ki omogočajo analitiko, oglaševanja in funkcionalnosti. Problem vseh piškotkov je vprašanje zasebnosti, torej kateri podatki o uporabniku se trenutno zbirajo, in vprašanje transparentnosti, torej kdo zbira informacije, v katere namene, kam se shranjujejo podatki in kako dolgo ostanejo v bazi shranjeni. Če podjetje na

svoji spletni strani zbira podatke, ki so osebni, ali pa se z združitvijo ali izpostavitvijo iz njih da ugotoviti identiteta posameznika, morajo upoštevati zakonodajo GDPR.

V Evropi je leta 2018 prišel v veljavo zakon o varstvu posameznikov pri obdelavi osebnih podatkov (uredba GDPR), ki določa, da se morajo uporabniki strinjati s piškoti, preden se začnejo zbirati podatki o njihovih dejavnosti na strani. Le na ta način lahko lastniki domene legalno zbirajo in obdelujejo osebne podatke uporabnikov. Vsak stran, ki ima evropske uporabnike, mora omogočiti seznanjene in strinjanje s piškotki uporabniku iz EU.

3.3.5 Umetna inteligenca in COVID-19

Zaradi pandemije je veliko držav uvedlo nujno potrebne omejitve za državljane, s čimer so posegale v temeljne človekove pravice, predvsem v pravico do zasebnosti. Za preprečevanje širjenja virusa v delno odprtem gospodarstvu, se je kot učinkovito pokazala zgolj kombinacija obsežnega testiranja, široka uporaba osebne zaščitne opreme in tehnologija digitalnega nadzora državljanov.

Čeprav je pravica do zasebnosti ena izmed temeljnih človekovih pravic, se le-ta lahko omeji, če pride do navzkrižja z nacionalnim zdravjem, vendar je potrebno poiskati razumno ravnovesje med pravicama; pravica do zasebnosti je lahko omejena zgolj, če je to nujno potrebno in omejena mora biti proporcionalno. Zbiranje in deljenje osebnih podatkov v takšni količini in kontekstu v boju proti koronavirusu predstavlja globalni test za varovanje zasebnosti posameznika.

V namene zaustavitve hitrega širjenja virusa COVID-19 so številna podjetja in raziskovalni centri združili moči in ustvarili aplikacije in modele, ki prikazujejo gibanje posameznikov. Podjetje Google je delilo obsežne zbirke podatkov o lokaciji posameznikov z raziskovalci javnega zdravja in epidemiologi, v namen modeliranja gibanja uporabnikov. S tem bi lahko ugotovili kje se je okužena oseba gibala in koliko ljudi je potencialno lahko okužila. Ekipa z Inštituta za tehnologijo v Massachusettsu je razvila aplikacijo za sledenje vsem uporabnikom, okuženih z virusom. Google in Apple sta napovedala uvedbo vmesnikov za programiranje aplikacij Android in iOS aplikacijo, s čimer bi se lažje prostovoljno sledilo stikom oseb preko Bluetooth Low Energy povezave. Severna Koreja sledi potencialno okuženim posameznikom preko lokacijskih podatkov z njihovega telefona in GPS-a, prav tako pa zajema tudi podatke z javnega prevoza, kreditnih kartic itd. Na Kitajskem je v uporabi aplikacija,

ki z barvnimi znaki prikazuje zdravstveno stanje posameznika, pred vstopom v nakupovalni center ali vstop na vlak. Prav tako se je na Kitajskem pojavila aplikacija, ki uporabnikom omogoča pregled nad lokacijo potrjenih in predvidenih okužb s koronavirusom v realnem času, tako da se lahko uporabniki izognejo tistim lokacijam.

Vendar pa morajo vse nadzorovalne in sledilne aplikacije, biti popolnoma proporcionalne, reverzibilne in transparentne, prav tako pa mora biti tudi njihov proces odstranitve definiran v trenutku, ko so bile implementirane. Digitalni odzivi na pandemijo ne smejo preseči demokratičnih vrednot države, prav tako tudi v prihodnosti ne sme priti do masovnega nadzorovanja in manipuliranja državljanov. Izdelovalci aplikacij morajo zbrane podatke uporabljati zgolj za namene preprečevanja širjenja okužbe in ne za iskanje profita, čeprav bi podatki koristili družbi v smislu izboljšanju javnega prevoza, zdravstvene infrastrukture...

Nekatere države so izkoriščale pandemijo za pridobivanje podatkov državljanov pod pretvezo da zbirajo podatke o okuženih in jih posredujejo državljanom za namene zajezitve širjenja virusa. V Izraelu so letos v začetku marca uvedli aplikacijo, ki naj bi zbirala in beležila podatke o vseh obolelih za virusom, vendar je v resnici zbirala podatke o uporabniku aplikacije, s čimer je vlada grobo posegala v pravico do zasebnosti državljanov. Tudi v Iranu se je istega leta pojavila aplikacija, ki naj bi domnevno pomagala identificirati simptome nove okužbe, vendar je bila zgolj pretveza za zbiranje podatkov o lokaciji uporabnikov. V Severni Koreji so ustvarili podobno aplikacijo, ki naj bi prikazala premike z virusom okuženih državljanov s čimer bi pomagali identificirati nove primere okužbe, vendar so zbrani podatki pogosto služili zgolj razkritju intimnih informacij.

V Evropi sta trenutno dve najpomembnejši direktivi glede varstva podatkov, in sicer uredba GDPR in direktiva o e-zasebnosti. Zadnja se ukvarja z vzpostavitvijo okvirjev za varovanje zasebnosti posameznika pri celotni komunikaciji preko javnih omrežij, ne glede na uporabljeno tehnologijo. Čeprav zakonodaja še ni prišla v veljavo, se ta nanaša na varovanje zasebnosti posameznika v digitalni dobi, predvsem z posameznikovo odobritvijo uporabe piškotkov na spletnih straneh ter seznanitvijo posameznika in nacionalnega organa ob vdoru v bazo podatkov.

V prihodnosti pa se bo ta direktiva razširila tudi na druge aplikacije, kot so WhatsApp, Facebook Messenger in Skype, kjer bo urejala da te aplikacije zagotavljajo enako stopnjo zaupnosti komunikacije kot ostali telekomunikacijski operaterji. Prav tako bo direktiva zagotavljala zasebnost in anonimiziranost metapodatkov pri komunikaciji, enostavnejšo odobritev piškotkov za boljšo uporabniško izkušnjo, zaščito pred nezaželeno pošto in oglaševalskimi klici, itd.

3.4 Primeri posega v zasebnost in sodne prakse

3.4.1 Poseg v pravico do zasebnosti

Ena izmed groženj zasebnosti je deanonimizacija, ki pomeni prepoznavo identitete posameznika iz podatka. Čeprav je podatek pri obdelavi ločen od ostalih podatkov posameznika, lahko zaradi specifičnega rezultata prepoznamo lastnika podatka in njegovo identiteto. To je izrazito predvsem na manjših vzorcih podatkov, kjer je mogoče posameznika prepoznati zgolj po enem podatku. Prav tako je posameznika možno prepoznati s kombiniranjem podatkov iz različnih zbirk podatkov, saj lahko s primerjavo obdelava natančno določimo izvor podatka. Posameznikova identiteta pa je lahko razkrita s pomočjo načina tipkanja na računalnik, kjer si računalnik zapomni hitrost, moč in vzorec pisanja posameznika, ter ga ob naslednji uporabi računalnika prepozna. Za zaščito zasebnosti uporabnika se je začela razvijati nova veja umetne inteligence imenovana diferencialna zasebnost, ki poskuša razviti algoritme strojnega učenja, ki bodo zagotavljali robustne rezultate obdelave, kateri ne bodo omogočali povratnega inženirstva podatkov.

3.4.1.1 Clearview AI in zbiranje osebnih podatkov

Ameriško podjetje Clearview AI se ukvarja z ustvarjanjem zbirk obrazov ljudi, katere kasneje posreduje organom kazenskega pregona, ki lahko enostavneje identificirajo storilce kaznivih dejanj in žrtve zločinov. Novo razvita tehnologija omogoča iskanje fotografij posameznikov preko družbenih omrežij, torej preko odprtega spleta in naj ne bi posegala v zasebne ali zaščitene informacije posameznika. Tehnologija podjetja je torej ustvarjenja zgolj za iskanje obrazov in ne za nadzor nad posamezniki a ravno zaradi te ogromne zbirke osebnih podatkov je podjetje v očeh javnosti videno kot kontroverzno. Do sedaj so zbrali več kot 3 milijarde slik, predvsem z družbenih omrežij kot so Facebook, Instagram, Twitter in YouTube, Clearview pa ohrani te slike v zbirki podatkov tudi po tem, ko so jih uporabniki že izbrisali iz svojih profilov.

Februarja letos zabeležili vdor v bazo podatkov, pri čemer je vsiljivec pridobil dostop do seznama strank podjetja, ki vsebuje policijske sile, organe pregona in banke. Družba je dejala, da oseba, ki je vdrla v sistem, ni pridobila nobene zgodovine iskanja, ki jo izvajajo stranke. Vendar pa je bilo podjetje po vdoru v bazo podatkov, soočeno z obtožbami glede njihovega delovanja. Clearview je posredovalo podatke iz svoje baze več kot 2200 policijskim upravam, vladnim agencijam in zasebnim podjetjem v več kot 27 državah, kateri so bili kasneje uporabljeni v različne namene, kot so iskanje osumljencev in prilagojeno oglaševanje. Ker je podjetje zbiralo osebne podatke posameznikov brez njihovega dovoljenja ali seznanitve, je kršilo številne zakone, med drugim tudi Zakon o zasebnosti biometričnih informacij v Illinoisu in zakon, ki prepoveduje zbiranje biometričnih podatkov o državljanov brez njihovega dovoljenja. Proti podjetju sta bili vloženi dve tožbi, in sicer s strani Generalnega državnega tožilca v Vermontu in Ameriške zveze državljanskih svoboščin, ki pa še nista razrešeni. Obe stranki se zavzemata za ustavitev nezakonitega in naključnega zajemanja in shranjevanja milijonov občutljivih biometričnih identifikatorjev, ter njihovega posredovanja tretji stranki.

3.4.1.2 Google in obdelava podatkov o lokaciji uporabnikov

Irska komisija za varstvo podatkov (DPC) je februarja letos oznanila ponovno preiskavo Googlove obdelave podatkov, ki je sledila vrsti obtožb več nacionalnih skupin potrošnikov po vsej Evropski uniji iz leta 2018. Podjetje naj bi na nepravilen način pridobivalo podatke o lokaciji uporabnikov, kasneje pa z njihovo obdelavo prišlo do zaključkov o posameznikovih osebnih lastnostih, kot so osebnost, vera ali spolna usmerjenost. Potrošniške organizacije trdijo, da posamezniki niso prostovoljno dali soglasja o deljenju svoje lokacije, saj so bili zavedeni k sprejetju pogojev poseganja v zasebnost. Takšne prakse pa niso skladne z evropsko zakonodajo, ki v Splošni uredbi o varstvu podatkov navaja, da mora biti posameznik seznanjen z zbiranjem njegovih osebnih podatkov.

Irska DPC se je odločila preiskavo začeti zato, da bi ugotovila kako podjetje pridobiva podatke o uporabnikovi lokaciji. Ta preiskava bo določila, ali ima Google sploh veljavno pravno podlago za zbiranje in obdelavo lokacijskih podatkov svojih uporabnikov ter če izpolnjuje svoje obveznosti upravljavca podatkov glede preglednosti. Irska DPC trdi, da noben potrošnik ne bi smel biti pod komercialnim nadzorom določenega podjetja, zato bo natančno pregledal, če družba upošteva Splošno uredbo o varstvu podatkov. Ker je problem posega v pravico do zasebnosti

zajemal milijone evropskih potrošnikov, bo preiskava glavna prioriteta Irske komisije za varstvo podatkov. Irska DPC trenutno aktivno preiskuje 20 večnacionalnih tehnoloških firm, ki naj bi podobno kot Google, posegale v pravico do varstva zasebnosti posameznika.

3.4.1.3 Aplikacija Grindr kršila Splošno uredbo o varstvu podatkov

Norveška potrošniška organizacija Forbrukerrådet je vložila več pritožb proti aplikaciji za zmenke Grindr in še pet podjetij za spletno oglaševanje, saj so ta podjetja zbirala osebne podatke o uporabnikih, katere so prodajala oglaševalskim agencijam in tržnikom, ki so ustvarili prilagojene oglase brez legalne podlage ali vedenja potrošnikov. Raziskave potrošniške organizacije so pokazale kako podjetja izkoriščajo zbrane podatke o uporabnikovem zdravju, spolni orientaciji, lokaciji in interesih, uporabniki aplikacije pa ne morejo storiti nič proti takšni uporabi njihovih podatkov. Takšno zbiranje podatkov lahko vodi do družbene izključitve, diskriminacije, goljufije in tudi manipulacije.

Uporabniki teh aplikacij nenehno nosijo telefon s seboj in ga uporabljajo za številne namene, kar pomeni, da lahko podjetja konstantno pridobivajo informacije o uporabniku. Študije so pokazala, da večino časa sploh ni nobene pravne podlage za takšen neomejen nadzor s strani takšnih podjetij, saj so uporabniki zavarovani s Splošno uredbo o varstvu podatkov, ki jih varuje pred takšnimi podjetji, katera ne spoštujejo zasebnosti posameznika. Poziv k poglobljeni preiskavi podjetja Grindr so vložile tudi skupine potrošnikov iz Združenih držav Amerike, Evropska potrošniška organizacija (v nadaljevanju BEUC) pa naproša Evropsko komisijo, naj ukrepa proti sistematičnemu in nezakonitemu komercialnemu nadzoru s strani podjetij, ki zbirajo osebne podatke uporabnikov na podlagi poslovnega modela ad-tech.

V pismu so zapisane ključne identificirane težave izkoriščanja osebnih podatkov uporabnikov aplikacij, kot je sistematično zbiranje in izkoriščanje podatkov za namene, s katerimi uporabniki niso seznanjeni ali pa niso podali izrecnega soglasja. Prav tako je BEUC opozorila na škodo, ki jo utrpijo potrošniki zaradi profiliranja, kot so diskriminacija, manipulacija, razširjena prevara… Potrošniki se zbiranju podatkov ne morejo izogniti, ker pred prvo uporabo niso primerno seznanjeni s potrebnimi informacijami in ker je sistem sledenja informacijam in njihove delitve tretjim strankam za uporabnike nerazumljiv. In četudi bi uporabniki aplikacij imeli dovolj znanja za razumevanje zbiranja osebnih podatkov, ne bi mogli nadzorovati

njihove obdelave ali ukrepati proti njihovem izkoriščanju. V pismu je BEUC naprosila za vzpostavitev alternativnega poslovnega sistema, ki bo uporabnikom omogočal uporabo digitalnih storitev in produktov, pri katerih bodo ohranili svojo avtonomijo, predvsem pa zasebnost.

3.4.2 Mnenje informacijskega pooblaščenca glede situacije v času pandemije

3.4.2.1 Zbiranje podatkov v zvezi s COVID-19

Informacijski pooblaščenec je prejel zaprosilo za mnenje glede zbiranja podatkov v zvezi s COVID-19, kjer je bilo navedeno, da želi delodajalec vpeljati sistem, pri katerem bi evidentiral vse obiskovalce, ki so zunanji izvajalci storitev. Takšna evidenca je sicer že bila vzpostavljena, sedaj pa jo želi delodajalec razširiti z izjavami, na katerih bi izvajalci navajali tudi zdravstveno stanje, zgodovino potovanj in zgodovino stikov.

Informacijski pooblaščenec navaja, da je potrebno v času pandemije, ko vsi prizadevamo za čim hitrejšo zajezitev bolezni, vseeno upoštevati veljavno zakonodajo na področju varstva osebnih podatkov. To pomeni, da mora imeti vsakršna obdelava zakonito in ustrezno pravno podlago, zaradi obdelave posebne vrste osebnih podatkov, kamor sodijo podatki v zvezi z zdravjem posameznika, pa se morajo upoštevati pogoji iz člena 9(2) Splošne uredbe o varstvu podatkov. Obdelava osebnih podatkov bi v tem primeru bila potrebna za izpolnjevanje pravne obveznosti, ki velja za delodajalca, kot so obveznosti v zvezi z zdravjem in varstvom pri delu, ali javnim interesom, kot je interes za nadzor nad boleznimi ali drugimi nevarnostmi za zdravje. Zaradi teh razlogov informacijski pooblaščenec meni, da delodajalec lahko zbira in obdeluje osebne podatke v zvezi s COVID-19 od obiskovalcev, ki so zunanji izvajali storitev, vendar le v utemeljenih okoliščinah na podlagi področne nacionalne zakonodaje, pri čemer pa mora upoštevati načelo najmanjšega obsega podatkov.

3.4.2.2 Varstvo osebnih podatkov pri poučevanju na daljavo

Informacijski pooblaščenec je dobil dopis z vprašanjem glede varstvom osebnih podatkov pri poučevanju učiteljev preko videokonferenčnih sistemov za poučevanje na daljavo. Ker informacijski pooblaščenec ne more presojati obdelave podatkov

izven inšpekcijskega postopka nadzora ter ne more presojati in komentirati konkretnih orodij za izvajanje izobraževanja na daljavo, podaja zgolj splošno mnenje glede podlag za obdelavo osebnih podatkov ter njihove varnosti, ki ga je naslovil tudi na Ministrstvo za zdravje, znanost in šport, katero zajema obdelavo osebnih podatkov tako učiteljev kot tudi učencev.

V svojem mnenju se je informacijski pooblaščenec dotaknil tematike zbiranja, objavljanja in shranjevanja video posnetkov učnih ur učiteljev na zavarovanem spletnem strežniku oz. učiteljevem e-okolju. To bi bilo dopustno zgolj na podlagi določne 48. člena Zakona o delovnih razmerjih pod pogojem, da gre za obdelavo, ki je potrebna za izvrševanje pravic in obveznosti iz delovnega razmerja. Informacijski pooblaščenec prav tako meni, da snemanje učne ure ne bi smelo temeljiti zgolj na podlagi privolitve učitelja, saj se lahko video posnetki izbrišejo, če se učitelj z obdelavo podatkov ne strinja več, kar ne bi zagotavljajo primerne kontinuitete in kvalitete dela. Zato morajo upravljavci, v tem primeru šole, urediti primerne roke hrambe, poskrbeti za ustrezno varnost obdelave osebnih podatkov, ter nasloviti morebitna vprašanja avtorskih pravic.

Prav tako je informacijski pooblaščenec predstavil svoje mnenje glede obdelave osebnih podatkov učencev, za katere meni, da za namene izvajanja izobraževanja na daljavo, zgolj privolitev starša (ali zakonitega zastopnika) ni ustrezna pravna podlaga, po kateri naj bi obdelava podatkov potekala. V trenutni situaciji bi bila edina primerna pravna podlaga 6(1)(c) Splošne uredbe o varstvu podatkov, saj je obdelava podatkov potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca. Zaradi izjemnih okoliščin v katerih se trenutno nahajamo, je informacijski pooblaščenec pozval Ministrstvo za izobraževanje, znanost in šport k oblikovanju enotnih navodil za šole glede obdelave osebnih podatkov.

3.4.2.3 Sledenje obolelim za COVID-19 preko mobilne aplikacije

Informacijski pooblaščenec je prejel zaprosilo za mnenje glede zakonske dopustnosti uporabe mobilne aplikacije, ki bi sledila posameznikom, s čimer bi zagotavljala, da se okuženi posamezniki ne gibljejo izven svojih bivališč. Pošiljatelj sporočila se sicer zaveda, da bi aplikacija posegala v posameznikovo pravico do varstva zasebnosti in osebnih podatkov. Sledenje bi potekalo tako, da bi naložena aplikacija bila aktivna 14 dni, po tem času bi se vsi podatki v zvezi z njo (in aplikacija sama) izbrisali. Vsebovala bi določen radij gibanja posameznika, ki je še dopusten, zajemala bi zgolj

podatke o lokaciji in ne bi imela dostopa do drugih podatkov, prav tako pa bi uporabniku nudila podporo v obliki enostavnega stika z zdravnikom.

Za odobritev uporabe aplikacije bi bilo najprej potrebno izvesti oceno učinkov z jasnimi tehničnimi parametri aplikacije glede na cilje, ki se jih zasleduje in z vidika načela sorazmernosti, šele nato bi bilo potrebno opredeliti zakonski okvir za uporabo aplikacije. Informacijski pooblaščenec pri tem opozarja na nujno prisotno transparentnost aplikacije, ki bi zagotavljala, d so uporabniki aplikacije obveščeni o tem, kateri podatki se bodo obdelovali in za kakšen namen, ter kdo bo upravljavec podatkov, kje se bodo podatki hranili in kako dolgo časa, ter kako bo zagotovljeno brisanje podatkov. Vsi osebni podatki bodo morali biti obdelani zakonito, pošteno in na pregleden način.

Informacijski pooblaščenec navaja tudi, da pravna podlaga klasične privolitve ne bi bila primerna, saj podaja privolitve med posameznikom in državo težko dosega standarde svobodne podaje. Poleg tega opozarja tudi na dejstvo, da se morajo izdelovalci te aplikacije najprej posvetovati s stroko glede nujnosti tehnične rešitve pri obvladovanju epidemije. Pojavilo se je tudi vprašanje glede natančnosti samega nadzora nad posamezniki, saj lahko uporabnik pusti telefon na določeni lokaciji in odide na drugo mesto brez njega, prav tako pa je znotraj večstanovanjske stavbe natančnost lokacije prav tako vprašljiva. Na tej točki je informacijski pooblaščenec predstavil pomislek glede tega, v kolikšni meri bi sledenje posameznikom sploh učinkovito pripomoglo k nadzoru posameznika z ukrepom in k širšemu cilju omejevanja epidemije COVID-19.

3.5 Smernice za razvoj umetne inteligence

3.5.1 Dosedanja prizadevanja

Do sedaj so bile na področju umetne inteligence vzpostavljene iniciative, ki so se ukvarjale z etičnimi in pravnimi vprašanji v povezavi z odgovornostjo in pravičnostjo odločanja. Najpomembnejša uredba je Splošna uredba o varstvu podatkov, ki predstavlja pomemben pristop h krepitvi zaupanja v umetno inteligenco. Prav tako je Evropska komisija sprejela iniciative, kot so Etične smernice za zanesljivo umetno inteligenco iz leta 2019, Poročilo o odgovornosti za umetno inteligenco in druge nastajajoče tehnologije iz leta 2019, in Deklaracijo o sodelovanju na področju umetne inteligence, katero je leta 2018 podpisalo 25 držav.

Evropska komisija je predlagala tako imenovan Evropski pristop k umetni inteligenci in robotiki, v katerem se raziskujejo tehnološki, etični, pravni in socialno-ekonomski vidiki uporabe umetne inteligence. Umetna inteligenca je v zadnjih letih postala ključno gonilo gospodarskega razvoja, zato je potrebno skrbno obravnavati njene socialno-ekonomske, pravne in etične učinke, da bo delovala v dobrobit celotne družbe. Pristop k umetni inteligenci je sestavljen iz treh temeljnih vidikov glede razvoja umetne inteligence in njenega vpliva na delovanje Evropske unije.

Prvi je ta, da mora Evropska unija v prihodnosti skrbno spremljati razvoj tehnologije in ga tudi podpirati, prav tako pa mora spodbujati uporabo umetne inteligence v javnem in zasebnem sektorju. Komisija je v sklopu raziskav in inovativnega programa Horizon 2020 povečala svoj letni vložek v umetno inteligenco za 70%, ki je tako v obdobju 2018 – 2020 dosegel 1,5 milijarde evrov. V naslednjem desetletju se namerava za raziskave in razvoj umetne inteligence nameniti več kot 20 milijard evrov letno. Prav tako je v načrtu okrepiti raziskovalne centre po vsej Evropi, še naprej podpirati razvoj projekta »AI-on-demand«, ki ko zagotavljal dostop do relevantnih virov umetne inteligence v Evropi vsem uporabnikom, ter spodbujati razvoj aplikacij umetne inteligence v ključnih sektorjih.

Drugi vidik je ta, da se mora Evropska unija temeljito pripraviti na socialno-ekonomske spremembe, ki jih bo prinesel razvoj umetne inteligence. Komisija bo, kot podpora državam članicam, okrepila poslovno-izobraževalna partnerstva na področju umetne inteligence v Evropi, vzpostavila namenske programe usposabljanja in prekvalifikacije za strokovnjake na področju umetne inteligence, predvidevala spremembe na trgu dela, podpirala digitalne veščine in kompetence v znanosti, tehnologiji, inženirstvu in matematiki, prav tako pa bo vzpodbujala države članice, da modernizirajo njihove sisteme izobraževanja in usposabljanja na področju umetne inteligence.

V sklopu tretjega vidika pa bo Komisija zagotovila primeren etični in pravni okvir glede umetne inteligence in njenega razvoja. V Beli knjigi, ki jo je Komisija objavila 19. februarja 2020, je že ustvarila smernice za spodbujanje evropskega sistema odličnosti in zaupanja v umetno inteligenco. V njej je predlagala ukrepe, ki bodo racionalizirali preiskave, spodbujali sodelovanje med državami članicami in povečali naložbe v razvoj umetne inteligence. Prav tako so v Beli knjigi zapisane možnosti politike prihodnjega regulativnega okvira Evropske unije, ki bi določal vrste zakonskih zahtev, s posebnim poudarkom na aplikacijah z visokim tveganjem.

3.5.2 Napovedi za prihodnost

Evropska komisija je februarja 2020 predstavila ideje in ukrepe za digitalno transformacijo Evrope v prihodnosti na področju umetne inteligence. Ukrepi pokrivajo področja kibernetske varnosti kritičnih infrastruktur, digitalnega izobraževanja, veščin uporabe umetne inteligence, demokracije in medijev. Cilj Komisije je vzpostaviti Evropsko družbo, ki bo zaupala v umetno inteligenco, bila odprta za nove poslovne možnosti in vzpodbujala razvoj v človeka usmerjene umetne inteligence.

Evropska tehnološka suverenost družbe se mora začeti z zagotavljanjem celovitosti in odpornosti podatkovne infrastrukture, omrežja in komunikacij, saj prebivalci Evropske unije menijo, da nimajo več nadzora nad tem, kaj se dogaja z njihovimi osebnimi podatki. Državljane se bi moralo spodbujati k sprejemanju boljših odločitev na podlagi razumevanja podatkov, pridobljenih s pomočjo umetne inteligence. Prav tako bi morali ti podatki biti na voljo vsem posameznikom in podjetjem. Digitalna Evropa bi morala odražati odprtost, poštenost, raznolikost, demokratičnost in samozavest.

V naslednjih petih letih se bo Evropska komisija zavzemala za tri temeljne cilje, s katerimi bo zagotavljala digitalne rešitve, ki bodo v pomoč pri doseganju digitalne transformacije Evrope. Prvi je ta, da se morajo razviti tehnologije, ki bodo človeku olajšale njegov vsakdan, te pa morajo upoštevati vrednote prebivalcev. Drugi cilj je doseganje poštenega in konkurenčnega gospodarstva, kjer lahko katerokoli podjetje deluje od enakimi pogoji, ter lahko razvija, trži in uporablja digitalne tehnologije za povečanje lastne produktivnosti, pri tem pa je potrošnikom zagotovljeno, da se spoštuje njihove pravice. Zadnji cilj je odprta, demokratična in trajnostna družba, ki bo omogočala državljanom, da izmenjujejo podatke v zaupanju vrednem okolju, pri čemer se bodo spoštovale temeljne pravice.

Komisija je v poročilu tudi opredelila nekatere načine digitaliziranja Evrope na področju umetne inteligence. Evropa bi tako morala združiti svoje investicije v raziskave in inovacije, ter deliti izkušnje in spodbujati sodelovanja med državami članicami. Prav tako mora promovirati digitalno transformacijo javne administracije, ter vlagati v strateške kapacitete, ki omogočajo razvoj in uporabo digitalnih rešitev. K tem rešitvam bo pripomogel večletni finančni okvir Evropske unije, namenjen izključno digitalizaciji, katerega cilj je doseči boljše strateške kapacitete kjer je to

potrebno. Zagotavljati mora kibernetsko varnost, prav tako pa mora tudi povečati zaupanje v samo tehnologijo, še posebej sisteme umetne inteligence. Zagotavljati mora napredku prilagojeno izobrazbo, ki bo na voljo vsem, ter spodbujati posameznike k vseživljenjskemu učenju, saj bodo v prihodnosti državljani potrebovali večinoma digitalne kompetence za uspeh na vedno bolj digitaliziranem trgu dela. Prilagoditi pa se mora tudi spremembam zunaj tehnološkega sektorja, kjer mora omogočati pravičnost in enakopravnost vsem državljanom Evropske unije.

3.6 Zaključek

Umetna inteligenca je tehnologija, s katero bo človek v prihodnosti zmožen reševati kompleksne probleme, kot so podnebne spremembe, dostop do pitne vode, ustvarjanje čiste energije in boj proti še neozdravljivim boleznim. Ker bodo sistemi umetne inteligence inkorporirani v naš vsakdan, se bomo morali prilagoditi njeni konstantni uporabi na številnih področjih, kot so gospodarstvo, industrija, šolstvo, zdravstvo, itd. Prav tako bomo morali, zaradi neprestanega razvoja in napredka tehnologije, prilagoditi njen pravni in etični okvir, da uporaba umetne inteligence ne bo posegala v temeljne človekove pravice.

Umetna inteligenca torej prinaša veliko pozitivnih sprememb in izboljšav za človeštvo, vendar pa predstavlja tudi nevarnost naši avtonomiji, ter moči in sposobnosti samostojnega odločanja. Zaradi napredka tehnologije vedno bolj zaupamo odločitvam pametnih naprav, saj menimo, da nam izboljšujejo življenje. Čeprav nam recimo tehnologija interneta stvari res lahko omogoči enostavnejše življenje, kjer je poskrbljeno za vsako našo potrebo, lahko predstavlja tudi tveganje za našo svobodo, saj lahko kdorkoli, ki uspe vdreti v sistem, pridobi vse podatke ali pa celo nadzoruje in upravlja z našim življenjem. Podobno velja za avtonomna vozila, kjer lahko kibernetski napad na sistem vozila onemogoči lastniku nadzor nad vozilom.

Pametne naprave vsakodnevno zbirajo ogromne količine podatkov o posameznikih, ki se lahko uporabijo za prilagojeno oglaševanje, napovedovanje kriminala, ali pa celo za nadzorovanje prebivalstva v pametnih mestih. Vsi ti podatki in informacije se zbirajo v oblaku na spletu, kjer dobijo vrednost šele, ko se povežejo s podatki, pridobljenimi iz drugih naprav, pri čemer se ustvari profil posameznika. Takšni zbrani podatki lahko kršijo pravico do zasebnosti med njihovim zbiranjem in obdelavo, saj se lahko izkoristijo za namene, katerih se posameznik sploh ne zaveda,

ali dovolil takšno uporabo. Čeprav je na tem področju že bil sprejet normativni okvir, se zaradi stalnega napredka umetne inteligence pojavljajo nove možnosti kršenja človekovih pravic, ki pa še niso pravno naslovljene.

Seznam literature in virov

Članki in poglavja iz knjig

Alexandrou, A., Maras, M-H., Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos, v: The International Journal of Evidence & Proof, 23 (2019) 3, str. 255–262

Collingwood, L.: Privacy implications and liability issues of autonomous vehicles, v: Information & Communications Technology Law, 26 (2017) 1, str. 32–45

Lim, H., Taeihagh, A.: Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications, v: Energies, 11 (2018), str. 1– 23

Meskys, E., in drugi: Regulating deep fakes: legal and ethical considerations, v: Journal of Intellectual Property Law & Practice, 15 (2020) 1, str. 24–31

Sadeghi A-R., Wachsmann, C., Waidner, M.: Security and privacy challenges in industrial Internet of Things, v: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), (2015), str. 1–6

Smit, E. G., Van Noort, G., Voorveld H. A. M.: Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe, v: Computers in Human Behavior, 32 (2014), str. 15–22

Ukil, A., Bandyopadhyay, S., Pal, A.: IoT-Privacy: To be private or not to be private, v: 2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), (2014), str. 123–124

Weber, R. H.: Internet of things: Privacy issues revisited, v: Computer Law & Security Review, 31 (2015) 5, str. 618–627

Pravni viri

Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20).

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).

Pogodba o delovanju Evropske Unije, Uradni list Evropske unije, C 326/47, str. 47-390.

Listina Evropske Unije o človekovih pravicah, Uradni list Evropske unije, C 83/389, str. 391–407.

Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, Uradni list Evropske unije, L 119/89, 4.5.2016.

Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij, Uradni list Evropske unije, L 201/37, 31.7.2002.

Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES, Uradni list Evropske unije, L 105/54, 13.4.2006.

Mnenje Evropskega ekonomsko-socialnega odbora – Umetna inteligenca – Posledice za enotni (digitalni) trg, proizvodnjo, potrošnjo, zaposlovanje in družbo (mnenje na lastno pobudo), Uradni list Evropske unije, C 288, 31.8.2017, str. 1–9

Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, Uradni list Evropske unije, L 359/60, 30.12.2008.

Predlog UREDBA EVROPSKEGA PARLAMENTA IN SVETA o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027, COM/2018/434 final - 2018/0227.

Resolucija Evropskega parlamenta s priporočili Komisiji o pravilih civilnega prava o robotiki (2015/2103(INL)), Uradni list Evropske unije, C 252/239, 18.7.2018, str. 239–257.
Resolucija Evropskega parlamenta z dne 26. maja 2016 o strategiji za enotni trg (2015/2354(INI)), Uradni list Evropske unije, C 76, 28.2.2018, str. 112–127.
Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Na poti do avtomatizirane mobilnosti: strategija EU za mobilnost prihodnosti, COM/2018/283 final.
Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Evropska strategija za kooperativne inteligentne prometne sisteme – mejnik na poti h kooperativni, povezani in avtomatizirani mobilnosti, COM/2016/0766 final.
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) (Besedilo velja za EGP), Uradni list Evropske unije, L 119, 4.5.2016, str. 1–88.

Sodna praksa

C-131/12, *Agencia Española de Protección de Datos (AEPD) in Mario Costeja González,* ECLI:EU:C:2014:317
C-136/17, *Commission nationale de l'informatique et des libertés (CNIL),* ECLI:EU:C:2019:773
C-207/16, *Ministerio Fiscal,* ECLI:EU:C:2018:788
C-293/12 in C-594/12, *Digital Rights Ireland Ltd (C-293/12) in Kärntner Landesregierung (C-594/12),* ECLI:EU:C:2014:238
C-362/14, *Maximillian Schrems in Data Protection Commissioner*, ECLI:EU:C:2015:650
C-70/10, *Scarlet Extended SA in Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* ECLI:EU:C:2011:771
C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) in Netlog NV,* ECLI:EU:C:2012:85

Spletni viri

< https://mladipodjetnik.si/novice-in-dogodki/novice/gdpr-uredba-o-varstvu-podatkov > (25. 5. 2020)
< https://epic.org/privacy/edrs/ > (12. 5. 2020)
< https://www.theguardian.com/technology/2016/jun/08/self-driving-car-legislation-drones-data-security > (22. 5. 2020)
< https://gadgets.ndtv.com/others/news/self-driving-car-technology-poses-high-hacking-risk-study-796978 > (15. 4. 2020)
< https://perma.cc/L6B5-DGNR > (22. 5. 2020)
< https://mastersofmedia.hum.uva.nl/blog/2019/09/22/the-worrisome-biometrics-deepfakes-zao-and-privacy-issue/ > (13. 4. 2020)
< https://azati.ai/artificial-intelligence-targeted-marketing/ > (5. 5. 2020)
< https://www.cookiebot.com/en/gdpr-cookies/?gclid=CjwKCAjwnIr1BRAWEiwA6GpwNdDbKnp028aCrerivdJ43SjTZDGZPzIDA4q8NEAvsctBBuDbNhOUrBoCdLsQAvD_BwE > (13. 4. 2020)
< https://foreignpolicy.com/2020/04/20/coronavirus-pandemic-privacy-digital-rights-democracy/ > (18. 5. 2020)
< https://www.dataguidance.com/opinion/international-coronavirus-privacy-dilemma > (11. 4. 2020)
< https://www.theguardian.com/world/2020/mar/17/israel-to-track-mobile-phones-of-suspected-coronavirus-cases > (27. 3. 2020)
< https://ec.europa.eu/digital-single-market/en/online-privacy > (3. 5. 2020)
< https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation > (3. 5. 2020)
< https://course.elementsofai.com/6/2 > (27. 3. 2020)
< https://edition.cnn.com/2020/02/26/tech/clearview-ai-hack/index.html > (17. 5. 2020)
< https://clearview.ai/ > (17. 5. 2020)
< https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies > (1. 5. 2020)
< https://www.theverge.com/2020/3/11/21174613/clearview-ai-sued-vermont-attorney-general-facial-recognition-app-database > (21. 5. 2020)
< https://nakedsecurity.sophos.com/2020/05/29/clearview-ai-facial-recogition-sued-again-this-time-by-aclu/ > (20. 5. 2020)
< http://www.beuc.eu/publications/google-cross-hairs-irish-data-protection-authority-location-tracking/html > (28. 5. 2020)

< https://digitalguardian.com/blog/irish-data-protection-puts-google-notice-data-privacy-again > (14. 5. 2020)
< https://www.euractiv.com/section/data-protection/news/google-hit-by-irish-data-protection-probe/ > (14. 5. 2020)
< https://www.ip-rs.si/varstvo-osebnih-podatkov/pravice-posameznika/ > (8. 6. 2020)
< https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/ > (8. 6. 2020)
< https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1530 > (8. 6. 2020)
< https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5BshowUid%5D=1508 > (8. 6. 2020)
< https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1%5bshowUid%5d=1504 > (8. 6. 2020)
< http://www.beuc.eu/publications/eu-consumer-groups-urge-immediate-investigation-systematic-breaches-gdpr-online/html > (9. 6. 2020)
< http://www.beuc.eu/publications/beuc-x-2020-002_letter_to_executive_vice-president_vestager.pdf > (18. 5. 2020)
< https://ec.europa.eu/digital-single-market/en/artificial-intelligenc > (18. 5. 2020)
< https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273 > (18. 5. 2020)
< https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf > (27. 3. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070sl.pdf > (19. 6. 2020)
< https://e-uprava.gov.si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=10208 > (19. 6. 2020)
< https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/2020/MP_ZVOP2_mnenje_IP_jan2020_koncno.pdf > (19. 6. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117sl.pdf > (30. 6. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011sl.pdf > (30. 6. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157sl.pdf > (9. 7. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/cp180141sl.pdf > (9. 7. 202)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117sl.pdf > (9. 7. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126sl.pdf > (9. 7. 2020)
< https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-02/cp120011sl.pdf > (9. 7. 2020)