6

UDK 342.721:004

Primož Križnar[*]

Varstvo lokacijske zasebnosti s pomočjo mozaične teorije podatkov[**]

1. Uvodoma o lokacijski zasebnosti

Pred skokovitim razvojem tehnološko dovršene informacijske tehnologije je lahko oseba tisto informacijo, ki jo je štela za zasebno, kot tako obdržala brez pomoči pravnih norm. Ni ji bilo namreč treba skrbeti, da bi podatek nenadzorovano ušel izpod njenega nadzora in postal dostopen splošni javnosti oziroma da bi ga sama nevede izpostavila splošni javnosti, saj za kaj takega preprosto ni bilo tehničnih možnosti oziroma če so že bile, so bile take, da je bila oseba sposobna vplivati tudi nanje (na primer svoje pismo je osebno, brez posrednikov dostavila naslovniku, imela je hitrejšega konja od tistih, ki so ji sledili, uporabljala je lastne šifrante, zaradi manjše populacije si je lahko zapomnila obraz opazovalca itd.). Danes pa ni več tako, saj posamezniki vsak dan o sebi in svojih vsakdanjih aktivnostih z lastnimi ravnanji in z informacijsko tehnologijo izdamo kopico informacij, ki lahko o našemu videzu, mišljenju, aktivnostih in preferencah povedo marsikaj. Tako ravnanje olajšuje delo tistega, ki o nas hoče izvedeti čim več, posamezniki pa zaradi digitalizacije izgubljamo moč odločanja, s kom bomo delili katere podatke in zakaj.[1] Če ob tem upoštevamo tudi dejstvo, da je taka tehnologija čedalje cenejša, je vdor

---

[*] Magister prava, sodniški pripravnik na Višjem sodišču v Ljubljani, asistent na Inštitutu za kriminologijo pri PF Univerze v Ljubljani; primoz.kriznar@guest.arnes.si.

[**] Prispevek je bil pripravljen v okviru projekta Pravo v dobi velikega podatkovja - reguliranje zasebnosti, transparentnosti, tajnosti in drugih nasprotujočih vrednot v 21. stoletju, ki ga izvaja Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, financira pa ga Agencija za raziskovalno dejavnost Republike Slovenije (2014-2017).

[1] Tomšič, Smo dovolj pametni za pametne naprave (2015), str. 130.

v zasebnost nekoga postal, milo rečeno, poceni. Seveda pa je vprašanje, ali nekdo želi take informacije ohraniti kot zasebne ali jih deliti s širšim krogom svoje okolice, vedno odvisno od subjektivne volje vsakega posameznika,[2] na katerega se take informacije nanašajo, deloma pa je odvisno tudi od splošnega znanja z upravljanjem tehnoloških naprav, na primer pametnih telefonov.

Splošno znano je, da je zasebnost v različnih državah različno opredeljena, globalno gledano pa bi se lahko strinjali, da je v najširšem smislu oblikovana kot osebnostna pravica vsakega posameznika, na podlagi katere lahko ta zahteva, da se ga pusti pri miru oziroma uveljavlja svojo svobodo pred poseganjem in vmešavanjem sočloveka ali države kot institucije v njegove lastne osebne zadeve, ki jih ocenjuje kot tako pomembne, da jih ne želi deliti. Zasebnost bi lahko opredelili tudi kot sfero s konkretnimi informacijami, ki pripadajo izključno notranjemu svetu konkretne osebe in ki jih ta ne želi deliti z nikomer, temveč te informacije varno hrani znotraj te sfere, ki je dostopna le tej osebi prek živčnih dražljajev. Taka opredelitev je v nekaterih primerih pretirana, saj zaradi socialno -družbenega razvoja nekaterih informacij, ki bi jih sicer želeli ohraniti kot zasebne, pred nadobudnimi očmi okolice ne moremo več skriti. Zato se prav v tem vidiku kaže razlika glede subjektivnega dojemanja pojma zasebnosti, saj nekateri v javnosti sodelujejo na način, da se o njih s strani tretjih oseb ne zbira podatkov o taki participaciji in o njih samih, spet drugi se v družbo vključijo, vendar želijo nadzor nad tokom informacij, ki ga o svoji osebnosti delijo z družbo, tretji pa v svoji okolici radi delijo širok nabor osebnostnih informacij. Dejstvo je, da je v družbi precej trdno izoblikovano stališče, da kljub voljni in zavestni izpostavitvi posameznikove osebnosti v razmerju do drugih, tak posameznik glede nekaterih dejstev, ki zadevajo njegovo vsakdanje življenje, želi ohraniti zasebnost, vendar ne zato, ker jih želi ohraniti zasebne,[3] temveč zato, ker preprosto ne pričakuje, da bo družba želela vpogled vanje in s tem vedenje o celotnem poteku njegovih dnevnih dogodkov.[4] S takim stališčem se je danes mogoče poistovetiti, saj na tistem, kar izpostavimo javnosti, zasebnosti ne moremo pričakovati zato, da izpostavljenega ne bo nihče videl, temveč zato, da bo izpostavljeno sicer videno, vendar ne sistematično beleženo[5] oziroma pomnjeno za vse večne čase.[6]

---

[2] Van Loenen, Location privacy and national security: contradiction in terminus?, URL: http://www.gsdi.org/gsdiconf/gsdi12/papers/92.pdf, str. 2

[3] Stališče v zadevi Katz vs. United States, 389 U.S. 347 (1967), tč. 351–352.

[4] Kot o tem Gatewood, District of Columbia Jones and the Mosaic Theory – In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory (2014), str. 535.

[5] Ford, Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology (2011), str. 1363.

[6] Z izjemo kakšnih posebnih dogodkov, ki so z vidika javnosti tako zanimivi, da bodo ljudem dalj časa ostali v spominu oziroma bodo take dogodke ali stvari obelodanili z avdio-video posnetki.

1.1. Kaj je lokacijska zasebnost?

V sklopu našega življenja se je treba zaradi zadovoljevanja osebnih potreb prek storitev, nabave blaga, opravljanja dela in izvedbe športnih aktivnosti vedno fizično premikati od ene do druge lokacije. Tako premikanje praviloma poteka na očeh javnosti oziroma tistega, ki je naš premik sposoben zaznati s svojimi čutili, pri čemer uporabljamo najrazličnejše načine transporta. Glede na do zdaj zavzeto stališče pa ne pričakujemo, da si bo konkretna oseba zapomnila vse naše premike v prostoru, s čimer ti lokacijski premiki z vidika zasebnosti postajajo vse pomembnejši. Prav v tem se skriva tudi samo bistvo lokacijske zasebnosti, ki po definiciji pomeni zmožnost vsakega, da se giblje v javnem prostoru s pričakovanjem, da se njegovih lokacij v običajnih okoliščinah sistematično ne beleži in ne shranjuje za nadaljnjo uporabo.[7] Vsebina lokacijske zasebnosti je torej v tem, da naj bi bil vsak posameznik ob svojem premiku sposoben nadzirati informacije, s katerimi izdaja svojo trenutno ali preteklo lokacijo,[8] oziroma preprečiti, da se s to lokacijo seznani nekdo tretji,[9] vendar zaradi razvoja sofisticirane moderne tehnologije ni vedno tako, saj povprečen posameznik svojo lokacijo največkrat nevede izda prav s pomočjo te tehnologije.

1.2. Lokacijski podatki in problem zaznave

S posegom v lokacijsko zasebnost se lahko seznanimo s širokim naborom podatkov, ki se nanašajo na zasebno sfero konkretnega posameznika. Tako lahko na primer na podlagi vzorca gibanja posameznika izvemo, katero pot uporablja za opravljanje dela, kateri lokal ali restavracija sta mu najljubša, v kateri fitnes in katero trgovino z živili zahaja, ali hodi v cerkev, ali se je udeležil volitev, kdo je njegov partner oziroma ali uporablja drugačen tip storitev, kateri so njegovi prijatelji, s katero banko posluje, kje se zdravi, ali se zadržuje v soseskah, v katerih je stopnja delinkventnosti višja, itd.[10] Iz ene same pridobljene informacije ne moremo vedno izluščiti namena obiska,[11] vendar lahko to popravimo s stopnjevanjem intenzitete opazovanja posameznikovega gibanja, s čimer razkrijemo še več o osebnosti opazovanega, saj ugotovimo, ali gre za redne navade, enkratne obiske ali pa celo pripadnost neki skupini, pa naj bo ta politična ali teroristična. S stopnjevanjem lokacijskega nadzorovanja lahko celo dosežemo, da se nam razkrije del posameznikovih značajskih lastnosti, ki mogoče navzven sploh niso razvidne, na primer njegova nezvestoba, zasvojenost, nedružabnost, upornost, begosumnost in vztrajnost. Vse to pa so podat-

---

7 Blumberg, Eckersley, On Location Privacy and How to Avoid Losing it Forever (2009), str. 1.

8 Michael, Clarke, Location privacy under dire threat as ‚uberveillance' stalks the streets (2012), str. 25.

9 Van Loenen, Location privacy and national security: contradiction in terminus?, str. 2.

10 Podobno o tem v zadevi United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), tč. 562.

11 Zaradi popačenja realnosti lahko to v praksi povzroča probleme, kot sem že pojasnil.

ki o osebnosti posameznika,[12] na podlagi katerih lahko oblikujemo profil opazovanega (angl. *totality of information*).[13] S tem se nedvomno posega v zasebnost in je ustrezen sklep, da povezovanje lokacijskega podatka z vsebino okolice te lokacije pomeni informacijo, ki se izrecno nanaša na del tistega, kar bi povprečno razumen človek smel v primeru nenehnega beleženja upravičeno šteti za zasebno.[14]

Informacije, pridobljene s posegom v lokacijsko zasebnost, lahko opazovalcu, torej tistemu, ki s temi informacijami razpolaga, povedo, kje se oziroma kje se je posameznik nahajal. S tem je mogoče ustvariti vedenjski profil posameznika, saj njegovi premiki zaradi umeščenosti v določeno okolico družbe nikakor niso naključni.[15] Prav to pa lahko vodi v neljube situacije, v katerih se posameznik znajde »na nepravem mestu ob nepravem času«. Predstavljajmo si situacijo, ko nekdo odide v trgovino na območju, kjer tistega dne potekajo množični protesti proti trenutni politični oblasti. Njegova lokacija je sicer res zabeležena na tem območju, vendar pa namen te osebe ni bila udeležba na protestih, temveč nakupovanje živil. Ker pa za ugotovitev lokacije te osebe ni bilo uporabljeno tipično policijsko opazovanje, s katerim bi lahko dognali namen te osebe, temveč je bila ugotovljena le lokacija njenega mobilnega telefona, o njenem pravem namenu zadrževanja na specifičnem območju ni mogoče pravilno sklepati. Gre torej za napako v zaznavi situacije, ki vodi do izkrivljanja stvarnosti, in to izključno zaradi odsotnosti človeškega elementa, ki bi bil sposoben situacijo ob njenem videnju »v živo« oceniti drugače in bolj življenjsko. Argument bolj konservativno naravnanih ljudi, ki jim moderna tehnologija in njena uporaba sicer nista tuji, v smislu, da nimajo namena ničesar skrivati in da javnost lahko prosto dostopa do vseh njihovih podatkov, zato torej v celoti propade.[16] Temelji namreč na subjektivnem dojemanju realnosti, ki je v primeru uporabe moderne tehnologije objektivizirana brez oziranja na namene ali motive. Slednje lahko vodi v zmotno interpretacijo dejanskega stanja, česar ne bo več mogoče popraviti, saj gre v večini primerov za enkratne življenjske dogodke v okviru specifičnih obkrožajočih okoliščin, ki so neponovljive in bo zato na primer omenjena oseba v trgovini večno zaznamovana. Ker je artikulacija specifične življenjske situacije v rokah organa pregona, lahko slednji arbitrarno subsumira dejansko stanje pod pravno normo, s čimer krši temeljno načelo zakonitosti v kazenskem pravu.

---

12 Tako stališče zavzema tudi Goetz, Locating Location Privacy (2011), str. 850.

13 Prav tam, str. 848.

14 Van Loenen, Location privacy and national security: contradiction in terminus?, str. 3.

15 Odvisni so od dela, prostočasnih obveznosti, kroga prijateljev in znancev, širine posameznikove družine, posameznikovih hobijev ter dostopnosti točk, na katerih lahko posameznik opravi oziroma zadovolji vse navedeno. Posameznik je torej v svojih premikih omejen in mora tako živeti v nenehnem sobivanju med izpolnjevanjem vsakodnevnih opravil v točno določenem območju, kjer opravila sploh lahko v celoti izpolni.

16 Blumberg, Eckersley, On Location Privacy and How to Avoid Losing it Forever (2009), str. 7.

Družba danes s strahospoštovanjem gleda na lokacijske podatke, kar potrjujejo tudi statistične analize. Slednje kažejo,[17] da se v družbi poraja skrb glede vprašanja, kdo vse lahko dostopa do lokacijskih podatkov, ki se beležijo z moderno tehnologijo, izražena pa sta tudi zaskrbljenost in tveganje glede koriščenja lokacijskih storitev v smislu primerjave med njenimi koristmi in škodljivimi vplivi. Koristi moderne tehnologije v zvezi s pridobivanjem lokacije ljudje pričakovano vidijo predvsem v reševanju človeških življenj v primeru nujne pomoči (na primer poškodovani planinec v gorah), nasprotno pa tveganja uporabe iščejo v razkritju svoje lokacije tistim, s katerimi je ne želijo deliti (med drugim državni oblasti), zalezovanju in vdoru v zasebni prostor.[18] Sklep, sprejet v prejšnjem odstavku tega prispevka je tako potrjen, saj iz tveganj uporabe lokacijske tehnologije izhaja, da osebe pridobivanje lokacijskega podatka štejejo za vdor v tisti del njihove sfere, ki ga želijo ohraniti le zase, kar torej posega v bistvo zasebnosti, posledično pa je treba tudi lokacijski podatek ob umestitvi v kontekst okolice obravnavati kot osebni podatek ter ga kot takega obvarovati. Tako mišljenje sovpada s stališčem Evropskega sodišča za človekove pravice (ESČP), ki v sklopu 8. člena Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (EKČP)[19] ščiti tako fizično kot tudi duševno integriteto posameznika v interakciji s preostalimi osebami,[20] in to celo v primeru, ko do interakcije prihaja v javnosti.[21] Ob tem velja izraziti skrb, da ljudje lokacijske tehnologije, čeprav se z njo srečujejo dnevno, ne razumejo najbolje, niti se ob njeni uporabi ne zavedajo njenih potencialov in nevarnosti.[22] Zato so omejeni pri preprečevanju uhajanja lokacijskih podatkov, ki postajajo splošno dostopni, s takim ravnanjem pa z lastno, vendar nevedno voljo odkrivajo tisto, kar želijo ohraniti kot zasebno. Ne glede na to je treba pred poseganjem v zasebnost učinkovito zaščititi tudi osebe, ki bi svojo intimo razgalile prav zaradi neznanja z upravljanjem s to tehnologijo, kar izhaja iz smisla enake obravnave vseh ljudi. Lahko bi celo rekli, da je pametna tehnologija, prek katere naj bi bilo naše življenje lahkotnejše, postala prepametna.

---

17 Tsai, Kelley, Cranor in Sadeh, Location-Sharing Technologies: Privacy Risks and Controls (2010), str. 119–151.

18 Prav tam, str. 144.

19 Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin (EKČP), Uradni list RS z dne 13. junija 1994, MP, št. 7/1994 (RS 33/1994).

20 Niemietz v. Germany, Eur. Ct. H. R., 16. december 1992, tč. 29; in Botta v. Italy, Eur. Ct. H. R., 24. februar 1998, tč. 32.

21 P.G. and J.H. v. the United Kingdom, Eur. Ct. H. R., 25. december 2001, tč. 56–57; in Peck v. The United Kingdom, Eur. Ct. H. R., 28. april 2003, tč. 57.

22 Tsai, Kelley, Cranor in Sadeh, Location-Sharing Technologies: Privacy Risks and Controls (2010), str. 138.

1.3. Sfere zasebnosti[23]

Kljub zgoraj poudarjenemu načelu enakosti pa si nekatere osebe zaradi svojega družbenega statusa preprosto ne morejo privoščiti, da bi njihovo življenje v celoti ostajalo zastrto s tančico skrivnosti, saj so lahko pravni standardi pravnega varstva življenja posameznika, ob upoštevanju njegove družbeno-socialne funkcije, različni.

Socialna umeščenost osebe znotraj družbe namreč vpliva na stopnjo zasebnosti, ki jo lahko konkretna oseba uživa. Ta je odvisna zlasti od značaja, dejanj in mišljenja posameznika glede na njegovo javno udejstvovanje. Zato je treba razlikovati med osebnostmi iz sodobnega življenja, ki zanimajo javnost in ki z zavestno ali voljno izpostavitvijo javnosti pridobivajo družbeni vpliv (t. i. absolutne osebe javnega življenja), osebami, ki javnost zanimajo samo v zvezi z nekim konkretnim dogodkom in ki so javnosti nehote izpostavljene v zvezi z njim (t. i. relativne osebe javnega življenja), in preostalimi osebami – »navadnimi smrtniki« oziroma zasebniki, katerim niti enkratna in z vidika javnosti nepomembna ravnanja še ne odvzamejo značaja zasebnega subjekta, saj se javnosti izpostavijo le priložnostno in kratkoročno.

Podobno lahko razdelimo tudi področja zasebnosti, in sicer na:

– področje intimnega in družinskega življenja, ki je tisti del posameznikovega življenja, ki se odvija zunaj kroga družine oziroma onkraj družinskega življenja in zajema posameznikove misli, čustva, spolno opredelitev, zapise v dnevnik in posameznikovo telo itd.;
– področje zasebnega življenja, ki se ne odvija v javnosti in je sfera, ki je prepletena s segmenti sfere intimnosti ter sfere javnega življenja, zato znotraj tega razlikujemo med mešano sfero intimnosti in zasebnosti,[24] srednjo stopnjo zasebnosti[25] in povezavo zasebnosti in javnosti;[26] ter
– področje življenja posameznika v javnosti.

Sfere zasebnosti z vidika lokacijske zasebnosti imajo poseben pomen, saj se lahko na njihovi osnovi določa stopnja pričakovane zasebnosti na lokacijskem podatku za vsakega posameznika. Pri tem moramo spoštovati dve temeljni pravili stopnjevitosti: a) manj kot je področje zasebnega življenja posameznika intimno, tem manjšo pravno zaščito uživa, kadar pride v kolizijo z interesi in pravicami drugih posameznikov, in b) manjše varstvo

---

[23] Poglavje povzeto po Von Hannover v. Germany, Eur. Ct. H. R., 24. september 2004, Von Hannover v. Germany (No. 2), Eur. Ct. H. R., 7. februar 2012, odločba Ustavnega sodišča RS Up-50/99 z dne 14. decembra 2000 ter Teršek, Svoboda medijev in varstvo zasebnosti: kritika dveh precedensov, predlog razvrstitve »javnih oseb« in predlog ustavnopravnih standardov (2006), str. 128–132.

[24] Na primer romantičen sprehod dveh zaljubljencev po gozdu.

[25] Na primer posameznik je pripadnik prostozidarjev.

[26] Na primer posameznik na javnem kraju zaradi narave ravnanj ali priložnostno vzpostavi določeno zasebno povezavo z drugimi ljudmi, to razmerje pa je mogoče opazovati s strani tistih ljudi, ki vanj niso vključeni, denimo kopanje v javnem bazenu.

zasebnosti uživa oseba, ki je na socialni lestvici umeščena višje. Samo ocenjevanje pričakovane zasebnosti pa je odvisno od okoliščin vsakega konkretnega primera.

2. Lokacijska tehnologija

Spremljanje položaja, gibanja ter aktivnosti posameznika je mogoče z neprekinjenim ali ponavljajočim se opazovanjem ter sledenjem z uporabo tehničnih naprav za ugotavljanje položaja in gibanja in tehničnih naprav za prenos in snemanje glasu, fotografiranjem in video-snemanjem.[27]

2.1. Globalni sistem pozicioniranja (GPS)[28]

Gre za t. i. mrežo satelitov GNSS (*Global Navigation Satellite System*), ki delujejo na osnovi radijskih valov in nenehno oddajajo signal z zapisom zelo natančnega časa. Ta signal na zahtevo uporabnika dotične elektronske naprave (na primer z vklopom lokacijskih storitev na pametnem mobilnem telefonu), slednja sprejme, ga obdela in uporabniku prikaže kot 1.) lokacijo, 2.) višino, 3.) čas, 4.) hitrost in 5.) smer gibanja elektronske naprave. Za določitev svojega položaja mora elektronska naprava prejeti oddajni signal vsaj štirih satelitov, ki krožijo v orbiti. Za tem elektronska naprava s postopkom trilateracije določi svoj položaj na Zemlji, in sicer tako, da na osnovi razlike med časom, ko je bil oddajni signal poslan, in časom, ko je bil sprejet, izračuna razdaljo med elektronsko napravo in posameznim satelitom, s temi podatki pa nadalje poišče svoj položaj na zemeljskem površju v treh dimenzijah z namišljenim nizom šestil. Položaj elektronske naprave je tako določen s presekom štirih krogelnih lupin.

Sistem GPS danes najdemo v večini elektronskih naprav, ki so v naši družbi nenehno prisotne, na primer v pametnih telefonih, urah in zapestnicah, vozilih z vgrajenim navigacijskim sistemom, prenosnih računalnikih itd. Določanje lokacije v okviru trilateracijskega izračuna je po javno dostopnih podatkih natančno do 3,5 metra (kar je odvisno od kakovosti sprejetega signala satelitov), pri čemer je ta natančnost še večja, če elektronska naprava svoj položaj določa v kombinaciji z drugimi sistemi,[29] na primer z globalnim sistemom za mobilno komuniciranje (GSM) ali prek t. i. WiFi točk, kar bo predstavljeno v nadaljevanju. Podatke o lokaciji lahko prek tega sistema pridobimo na več načinov: 1.

---

[27] Vsaj tako o tem tretji odstavek 149.a člena Zakona o kazenskem postopku (ZKP, Uradni list RS, št. 63/1994 in nasl.).

[28] Bertagna, How does a GPS tracking system work? URL: http://www.eetimes.com/document.asp?doc_id=1278363, BrickHouse Security, How does GPS tracking work, URL: http://www.brickhousesecurity.com/category/gps+tracking/how+does+gps+tracking+work.do in MIO, Kaj je trilateracija, URL: http://eu.mio.com/sl_sl/z-razlago-gps_kaj-je-trilateracija.htm.

[29] U.S. Government, GPS Accuracy, URL: http://www.gps.gov/systems/gps/performance/accuracy/.

z namestitvijo GPS-oddajnika v osebo, na njena oblačila ali vozilo; 2. z ogledom lokacij mobilne naprave te osebe[30] oziroma z vpogledom v napravo, če ta sistematično beleži lokacijo;[31] 3. prek spremljanja profila družabnega omrežja osebe, ki omogoča objavljanje lokacije,[32] ali pa z vpogledom v mobilno aplikacijo, nameščeno v elektronski napravi;[33] in 4. z namestitvijo škodljive programske opreme na mobilno napravo osebe, s katero lahko nenehno pridobivamo podatke oziroma sledimo gibanju te naprave (angl. *backdoor*).[34]

Kljub izredni natančnosti ima sistem eno od večjih pomanjkljivosti, in sicer 1. le na osnovi tega sistema ne moremo z gotovostjo trditi, da oseba, katere lokacijo želimo ugotoviti, na neki specifični lokaciji res je; 2. niti ni iz pridobljenega podatka mogoče ugotoviti, s kakšnim namenom je oseba na ugotovljenem območju (t. i. odsotnost subjektivne vezi[35] oziroma povezanosti posameznika z okolico).

Če naprava GPS ni subjektivno povezana z osebo (na primer vstavljena v podkožje), ne moremo, niti ne smemo z gotovostjo trditi, da se je konkretna oseba v tistem trenutku res nahajala na ugotovljeni lokaciji. Ni namreč rečeno, da bo naprava GPS (na primer na plašču, v žepu, v mobilnem telefonu itd.) vedno na dosegu roke te osebe oziroma da bo po njej zares posegala oseba, katere lokacijo želimo ugotoviti (na primer telefon ji lahko nekdo ukrade; plašč, v žepu katerega se nahaja naprava, lahko posodi svojemu prijatelju; prav tako mu lahko posodi tudi vozilo z vgrajeno navigacijo ali avtomatiziranim sistemom cestninjenja). Le z različnimi stopnjami verjetnosti lahko trdimo, da je naprava GPS posredovala lokacijski podatek opazovane osebe, saj moramo upoštevati tudi napako, ki se kaže v tem, da naprava prikazuje napačno lokacijo opazovane osebe oziroma prikazuje lokacijo osebe, ki sploh ni subjekt opazovanja. Taki napaki se lahko tudi izognemo, na primer s pridobitvijo podatka o tem, da je pametni telefon zaklenjen z vzorcem ali geslom, ki je poznan le opazovani osebi. Če ta oseba pametni telefon uporabi na določeni lokaciji, tako da izda lokacijski podatek, lahko s stopnjo, ki že meji na gotovost, sklepamo, da se prav opazovana oseba nahaja na tej lokaciji. Bolj zaskrbljujoče pa je,[36] da lahko z napravo GPS ugotovimo le objektivne informacije (lokacijo, višino, čas, hitrost in smer) gibanja, ne pa tudi tistih, ki so to gibanje povzročile, *ergo* namen oziroma motiv tega potovanja. Slednje je namreč izključno v mislih opazovane osebe, te

[30] Na primer prek URL: https://maps.google.com/locationhistory/.

[31] Google Inc., Upravljanje z godovine lokacij, URL: https://support.google.com/gmm/answer/3118687?hl=sl, pri čemer je možen tudi vpogled v druge naprave, na primer v navigacijsko napravo Garmin ali v vgrajeno navigacijo osebnega avtomobila.

[32] Na primer prek družabnih omrežij Facebook, Povio, Instagram ipd., ki ob objavi omogočajo oddajo lokacije naprave, prek katere se objava izvrši.

[33] Na primer prek aplikacije »Sledi kraj«, dostopne za androidne naprave v trgovini Google Play.

[34] Kaspersky Lab, What is a Trojan Virus? – Definition, URL: http://usa.kaspersky.com/internet-security-center/threats/trojans.

[35] Avtorjevo poimenovanje.

[36] V tem delu se sklicujem na primer, predstavljen pod tč. 1.2 tega prispevka.

pa je mogoče ugotoviti le posredno, s fizičnim opazovanjem te osebe, s čimer se lahko točno ugotovi, kaj je oseba počela na določenem območju, s kom se je sestala, koga je obiskala, kakšni so bili njeni gibi, ali je prek slednjih izdajala katero od čustvenih stopenj itd. Ker vsega tega prek naprave GPS ne moremo ugotoviti brez pomoči opazovalcev v neposredni bližini opazovanega, niti ni naprava GPS zanesljiva v tem, da na spremembo njene lokacije sploh vpliva opazovana oseba, si v tej luči upam trditi, da lahko uporaba tega sistema pripelje do zmotne ugotovitve dejanskega stanja, kar lahko pozneje težko in nepopravljivo vpliva na poseg v osebnostne pravice opazovane osebe. Situacija pa je lahko tudi obratna, saj lahko storilec kaznivega dejanja poskrbi, da bo njegova elektronska naprava z vgrajenim GPS modulom v času izvršitve kaznivega dejanja daleč stran od kraja dejanja, nato pa lokacijski podatek s te naprave (ki jo ima prikladno njegovemu zagovoru vedno pri sebi, na primer mobilni telefon) uveljavlja kot alibi. Tudi slednje privede do napačne ugotovitve dejanskega stanja, le da v tem primeru škoda ni povzročena osebnosti posameznika, temveč dokaznemu gradivu organov pregona kaznivih dejanj, nad katerim bo zaradi ravnanja storilca morebiti prevladala domneva nedolžnosti.

2.2. Globalni sistem za mobilno komuniciranje (GSM)[37]

Komunikacijsko območje, ki ga pokrivajo različni telekomunikacijski operaterji, je razdeljeno na območja – celice. Vsaka celica je sestavljena iz: a) številke, ki identificira celico – CELL ID, b) področne kode celice – LAC (*Local Area Code*), c) kode, ki identificira, kateremu nacionalnemu omrežju pripada celica – MCC (*Mobile Country Code*) in č) kode telekomunikacijskega operaterja, ki si lasti bazno postajo – MNC (*Mobile Network Code*). Identiteta pa ni le enostranska, saj na drugi strani telekomunikacijski operater prejme jasen podatek, katera elektronska naprava se je na bazno postajo povezala. V primeru mobilnih telefonov so to kar trije unikatni podatki,[38] in sicer telefonska številka uporabnika – MSISDN (*Mobile Station International Subscriber Directory Number*), IMEI[39] in IMSI.[40]

---

[37] Povzeto po Mnenju št. 13/2011 o geolokacijskih storitvah na pametnih prenosnih napravah Delovne skupine za varstvo podatkov iz člena 29. Direktive 94/46/ES z dne 16. maja 2011, str. 4, Landoni, How to find the location with GSM cells, URL: http://www.open-electronics.org/how-to-find-the-location-with-gsm-cells/, My Phone Locater, Tracking GSM phone, URL: http://myphonelocater.com/2014/01/18/tracking-gsm-phone/.

[38] Povzeto po Quora, What is the difference between ICCID, IMSI and IMEI numbers? URL: https://www.quora.com/What-is-the-difference-between-ICCID-IMSI-and-IMEI-numbers.

[39] International Mobile Station Equipment Identity (IMEI) – unikatna številka 15 decimalnih števil elektronske naprave, ki identificira napravo samo. V primeru prenosnih telefonov IMEI lahko razumemo kot številko, ki identificira, kateri telefon se povezuje na bazno postajo.

[40] International Mobile Subscriber Identity (IMSI) – unikatna številka 15 decimalnih števil, ki jo elektronska naprava pošlje bazni postaji, na katero se povezuje. V primeru prenosnih telefonov

Za uporabo omrežja GSM kot pomožnega sredstva za ugotavljanje lokacije posameznika se mora elektronska naprava prek komunikacijske tehnologije 2G, 3G ali 4G[41] povezati z anteno oziroma bazno postajo, ki pokriva specifično celico. Elektronska naprava mora biti vklopljena, poleg tega pa mora biti priključena na omrežje operaterja, ki si lasti bazno postajo celice (z vstavljeno kartico SIM). Elektronska naprava se prek svojega notranjega oddajnika (antene) s pomočjo radijskih valov določene frekvence vsakih 7 sekund povezuje z določeno bazno postajo,[42] telekomunikacijski operater pa te povezave ves čas beleži. Ko je znano, v kateri celici se elektronska naprava nahaja in na katero bazno postajo je priključena (če je baznih postaj v celici več), je na podlagi dometa radijskih valov posamezne bazne postaje mogoče ugotoviti, katera elektronska naprava se nahaja znotraj dometa specifične bazne postaje. Telekomunikacijski operater in številne prenosne naprave pa pri tem lahko uporabijo tudi signale, ki jih oddajajo prekrivajoče se celice (sosednje bazne postaje), da določijo položaj prenosne naprave s še večjo natančnostjo – triangulacija.[43] Operaterju je tako omogočeno, da o lokaciji elektronske naprave zbere historične lokacijske podatke (v smislu, na katero bazno postajo se je naprava povezala v trenutku komunikacije), pridobiva trenutno lokacijo naprave s ponavljajočim se oddajnim signalom elektronske naprave ter triangulacije ali pa elektronski napravi pošlje kratek podatkovni paket, na podlagi katerega naprava s povezovanjem na bazno postajo izda svoj položaj (t. i. pinganje naprave).[44]

Subjektivna vez med napravo, ki uporablja sistem GSM, ter opazovano osebo je v tem primeru večja. Uporabniki pametnih telefonov te praviloma zavarujejo z geslom, vzorcem ali PIN kodo, ki jo je treba vnesti pred uporabo. Ker je ta znana le uporabniku naprave, bi ob izvedenem klicu lahko sklepali, da je klic prek konkretne bazne postaje izvršila prav preiskovana oseba, saj je za funkcionalnost telefona morala poznati ključ, potreben za delovanje te naprave. Da je klic izvršila prav oseba, katere lokacijo želimo pridobiti, bi lahko potrdili tudi z vsebino pogovora ali SMS-sporočilom, ki bi se specifično dotikala intimnih vsebin, ki so znane le tej osebi, navsezadnje pa pride v primeru

IMSI razumemo kot številko, ki identificira uporabnika s pomočjo vstavljene SIM – *Subscriber Identity Module* kartice, saj je IMSI številka shranjena na njej. Prve tri številke IMSI predstavljajo MCC (Mobile Country Code), naslednji dve MNC (Mobile Network Code), preostalih deset števil pa MSIN (Mobile Subscription Identification Number) – torej unikatno številko naročniškega razmerja, sklenjenega med posameznikom in telekomunikacijskim operaterjem.

41 Več o teh tipih omrežij Ziegler, 2G, 3G, 4G, and everything in between: an Engadget wireless primer, URL: http://www.engadget.com/2011/01/17/2g-3g-4g-and-everything-in-between-an-engadget-wireless-prim/.

42 Kalis, Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance (2012–2013), str. 3.

43 Podobno kot opisano pod točko 2.1 – trilateracija.

44 Bedi, The curious case of cell phone location data: Fourth Amendment doctrine mash-up (2015-2016), str. 510–511.

pogovora v poštev tudi identifikacija glasu preiskovane osebe. Ne glede na izkazan prvi element subjektivne vezi (da napravo v času beleženja lokacije uporablja opazovana oseba), pa še vedno ne moremo biti prepričani o njenih dejanskih namenih na zabeleženi lokaciji (drugi element subjektivne vezi).

2.2.1. IMSI lovilec[45]

Je sredstvo informacijske tehnologije, ki deluje na principu MITM – *man-in-the-middle* napad, kar pomeni, da simulira bazno postajo, s tem pa povzroči, da se mobilna naprava zaradi optimizacije signala poveže z lovilcem in ne z bazno postajo, saj lovilec oddaja močnejši signal kot pa sama bazna postaja. IMSI-lovilec prav tako prikrito poveča moč signala mobilne naprave (in s tem poseže v integriteto same naprave), saj tako lažje ugotovi njen položaj in pridobi želene podatke, pri čemer sodelovanje telekomunikacijskega operaterja sploh ni potrebno. Z lovilcem je mogoče beležiti vsaj tri vrste podatkov, in sicer: a) podatke, ki jih mobilni aparat posreduje v omrežje neodvisno od uporabnikove želje oziroma zahteve (IMEI), b) prometne podatke (IMSI, MSISDN, datum, čas, trajanje komunikacije, količino prenesenih podatkov in med drugim seveda tudi lokacijo mobilne naprave) ter c) vsebino same komunikacije (prestrezanje pogovorov, SMS-sporočil ter paketkov internetnega protokola).

Z vidika zasebnosti gre za problematično orodje preiskovalnih organov, saj neselektivno (angl. *phishing expedition*) pridobiva podatke o lokacijah vseh komunikacijskih naprav, ki so v njenem dometu. Osebe, ki niso subjekti preiskave, sploh ne vedo, da je IMSI-lovilec pridobil podatke o njihovi elektronski napravi, niti nimajo možnosti, da bi zbiranje teh podatkov preprečile ali pa vsaj nadzirale njihovo poznejšo anonimizacijo. Da je naprava zmožna takega neselektivnega ravnanja in pridobivanja lokacije mobilnih naprav (angl. *triggerfish technology*),[46] kaže primer protestov v Ukrajini, med katerimi so protestniki na svoje mobilne telefone prejeli elektronsko sporočilo, da so registrirani kot udeleženci nemirov,[47] kar je na določenem območju mogoče storiti izključno z napravo, ki na določenem območju zaznava vse elektronske naprave, to pa ustreza delovanju IMSI-lovilca.

---

[45] Povzeto po Android IMSI-Catcher Detector, URL: https://secupwn.github.io/Android-IMSI-Catcher-Detector/; Septier Communication, Septier IMSI catcher, URL: http://www.septier.com/146.html; Gorkič, Sodobni prikriti preiskovalni ukrepi, prvič: lovilec IMSI (2014), str. 47–53 ter Bernstein, The Need for Fourth Amendment Protection from Government use of Cell Site Simulators (2016), str. 192–194.

[46] Kot o tem Oliver, Location, Location, Location: Balancing Crime Fighting Needs and Privacy Rights (2013), str. 490.

[47] Walker, Grytsenko, Text messages warn Ukraine protesters they are participants in mass riot, URL: http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot.

2.3. Dostopovne točke WiFi in naslov IP[48]

Dostopovne točke WiFi so utemeljene na tehnologiji, podobni uporabi zgoraj opisanih baznih postaj. Temeljijo na enoličnem identifikatorju (dostopovni točki WiFi), ki jo lahko prenosna mobilna naprava zazna. Enolična identifikacijska številka vsake dostopovne točke WiFi je njen naslov MAC – *Media Access Control*, ki se dodeli omrežnemu vmesniku in je običajno označen na strojni opremi. Ker so dostopovne točke WiFi stalno vklopljene, so pomemben vir geolokacijskih informacij. Večina širokopasovnih internetnih dostopovnih točk ima namreč tudi anteno WiFi, s katero se lahko prenosna naprava brezžično poveže z dostopovno točko, ta povezava pa se vzpostavi tudi v primeru, če prenosno napravo z brezžično dostopovno točko povežemo z žičnim kablom. Dostopovna točka WiFi podobno kot radio stalno oddaja svoje lastno ime omrežja in naslov MAC, tudi če povezave nihče ne uporablja in tudi če so vsebine brezžičnih sporočil šifrirane s tehnologijami WEP, WPA ali WPA2.

Tako ima vsaka dostopovna točka WiFi prek svoje antene določen domet signala, zato bi lahko tudi v tem primeru govorili o tem, da *radius* antene točke WiFi predstavlja celico dostopovne točke. Elektronska prenosna naprava se praviloma povezuje s tisto anteno, katere signal je najmočnejši (izbira je prepuščena programski opremi oziroma algoritmu elektronske naprave). Ob vzpostavitvi povezave je mogoče s pregledom dostopovne točke sprva določiti, katera elektronska naprava je z njo povezana (s pregledom naslovov MAC na dostopovno točko povezanih elektronskih naprav), nato pa je mogoče s pomočjo metode RSSI – *Recieved Signal Strenght Indication*[49] izračunati natančen položaj prenosne naprave, povezane z dostopovno točko. Za natančnejše rezultate je mogoče uporabiti tudi metodo triangulacije oziroma trilateracije, pri kateri prenosna naprava pošlje svojo zahtevo po vzpostavitvi povezave vsaj trem dostopovnim točkam WiFi, pri čemer povezavo vzpostavi s tisto, ki oddaja najmočnejši signal, kljub temu pa drugi dve točki pripomoreta k lažjemu določanju lokacije prenosne naprave. Ko je lokacija znana, jo prenosna naprava sporoči svojemu uporabniku ali pa aplikaciji pametnega telefona, ki je zahtevo po lokaciji prva sploh podala. Vse to pa ne odtehta težave subjektivne vezi, ki se zaradi objektiviziranja podatkov pojavi tudi v tem primeru.

---

[48] Mnenje št. 13/2011 o geolokacijskih storitvah na pametnih prenosnih napravah, str. 5–7, Shah, Shah, Basic of Wi-Fi based positioning system, URL: http://www.researchgate.net/profile/Darshan_Shah/publication/232729025_Basic_of_Wi-Fi_based_positioning_system/links/0fcfd509529419d523000000.pdf, Telekom Slovenije: Statični ali dinamični IP-naslov, URL: http://www.telekom.si/pomoc-in-podpora/teme-pomoci/internet/internet-siol/staticni-ali-dinamicni-ip-naslov.

[49] Več o tej metodi Estimote, What are Broadcasting Power, RSSI and other characteristics of beacon's signal? URL: https://community.estimote.com/hc/en-us/articles/201636913-What-are-Broadcasting-Power-RSSI-and-other-characteristics-of-beacon-s-signal-.

Ne smemo pozabiti na naslov internetnega protokola (IP), s katerim se identificiramo v medmrežju in je podoben naslovu prebivališča. Poznamo statični in dinamični naslov IP, pri čemer je statični naslov IP ob vsaki vzpostavitvi internetne povezave enak, dinamični pa se ob vsaki vzpostavitvi internetne povezave praviloma spreminja, oba pa še pred vzpostavitvijo povezavo z internetom dodeli ponudnik internetnih storitev. Glede na dejstvo, da je treba s ponudnikom skleniti pogodbo, v katero je treba navesti naslov prebivališča, poleg tega pa se mora v prebivališču nahajati internetni priključek, je ugotavljanje lokacije dokaj preprosto, saj operater preveri le, kateremu naročniku pripada naslov IP, na podlagi slednje ugotovitve pa z vpogledom v sklenjeno naročniško razmerje ugotovi lokacijo dostopanja v internet.

Pri pridobivanju lokacije s pomočjo naslova IP je treba razlikovati med funkcijo statičnega in dinamičnega naslova IP. Oba v trenutku vzpostavitve internetne povezave pripadata točno določeni lokaciji, vendar menim, da je treba dinamičnemu naslovu IP zagotoviti višjo raven varstva zasebnosti kot pa statičnemu. Spletne strani namreč beležijo naslove IP elektronskih naprav, ki do nje dostopajo, kar z vidika statičnega naslova IP pomeni večji vpogled v preference posameznika. Dinamični naslov IP pa spletni strani onemogoči razkrivanje navad enega posameznika, saj slednji do nje z vsako vzpostavitvijo internetne povezave dostopa z drugim naslovom IP. Pri tem ne gre spregledati, da je treba zahtevek za dodelitev dinamičnega naslova IP utemeljiti in za tako storitev na mesečni ravni tudi dodatno plačati. Ob vsem tem se je treba – enako kot v vseh primerih do zdaj predstavljene moderne tehnologije – zavedati odsotnosti subjektivne vezi, zaradi česar plačnika konkretnega naslova IP ne smemo vedno enačiti z dejanskim uporabnikom te povezave (na primer kibernetični kriminalec plačniku internetnega priključka prek njegovega modema prenese večjo količino bančnih podatkov, za kar plačnik sploh ne ve).[50]

Obe tehnologiji k ugotavljanju lokacije doprineseta preprosto z vpogledom v programsko opremo dostopovne točke WiFi, ki je zmožna shranjevati nanjo povezane naprave, ali pa z zahtevo, naslovljeno na telekomunikacijskega operaterja, ki bo sporočil, prek katerega naslova IP je bila izvršena določena zahteva na svetovnem spletu.

2.4. Termovizijska naprava

Termovizijsko napravo policisti uporabljajo pri nadzoru državne meje, iskanju pogrešanih oseb ter drugih preiskovalnih aktivnostih, predvsem pri preiskovanju gojenja marihuane.[51] Termovizijska kamera meri infrardeče sevanje določenega objekta in ga pretvarja v sliko. Vsak objekt s površinsko temperaturo nad absolutno ničlo (–273 °C) namreč

[50] O tem na primer U.S. District Court of Illinois v zadevi VPR Internationale v. Does 1-1017 z dne 29. aprila 2011 in U.S. District Court, Eastern District of New York v zadevi 2:11-cv-03995-DRH -GRB z dne 1. maja 2012.

[51] Severs, Dark visions (2007), str. 20–21 ter MNZ Policija, Delo in oprema, URL: http://www.policija.si/index.php/policijske-uprave/pu-koper/enote/630.

oddaja toplotno sevanje, ki ga termovizijska naprava zazna. Posameznik toplotno sevanje lahko občuti, videti pa ga ne more. Ko termovizijska kamera ustvari sliko toplotnega sevanja, je iz nje mogoče razbrati temperaturne razlike, saj so te vidne s pomočjo različnih barv, na primer modra – brez toplotnega sevanja, zelena – minimalno toplotno sevanje, rumena – zmerno toplotno sevanje in rdeča – intenzivno toplotno sevanje, oziroma je proizvedena slika toplotnih sevanj površin ob drugačnem tipu termovizijske naprave črno-bela, pri čemer črna predstavlja nično toplotno sevanje, bela izredno močno toplotno sevanje, odtenki sive pa glede na intenziteto sevanja površin variirajo.[52] Posameznika je tako zaradi stalne telesne temperature okrog 36 °C v urbanem okolju in tudi naravi z uporabo te naprave dokaj lahko odkriti.

Zaenkrat njena uporaba v smislu iskanja lokacije posameznika ni sporna oziroma je dobrodošla, saj se z njo skuša najti predvsem tiste osebe, ki so se na primer izgubile v gorah in jim grozi smrtna nevarnost. Različen pogled na posege v zasebnost z njeno pomočjo pa je mogoče najti na evropski in ameriški celini. Vrhovno sodišče ZDA je opozorilo,[53] da pridobitev informacij, ki se nanašajo na notranjost doma, s pomočjo tehnologije, ki omogoča ojačenje prirojenih zaznavnih možnosti občutenja, in ki ne morejo biti pridobljene drugače kot s fizičnim vstopom v ustavno varovano območje, pomeni preiskavo v primerih, ko za to uporabljena tehnologija ni v splošni javni uporabi.[54] Nasprotno je v evropski sodni praksi njena uporaba kot ena od proaktivnih metod preiskovanja v zvezi z distribucijo prepovedane konoplje nekoliko samoumevna in šele nadaljnji razvoj prava s tega področja bo pokazal, ali gre slediti ameriški doktrini.

V primeru uporabe termovizijske naprave je subjektivno vez mogoče vzpostaviti le deloma. Lokacijsko opazovana oseba namreč na zaslonu naprave predstavlja rdeč ali bel madež, kar je treba za vzpostavitev vezi preveriti z bolj osebnim stikom, med katerim lahko ugotovimo, ali gre res za konkretno osebo ali ne, v nasprotnem primeru pa moramo biti pripravljeni trpeti posledice, ki se kažejo v napačno ugotovljenem dejanskem stanju. Seveda motiva kot drugega elementa subjektivne vezi (zakaj se oseba zadržuje na nekem območju) s termovizijsko kamero ne moremo spoznati.

[52] Dumpert, Night vision for law enforcement & national security (2002), str. 75.

[53] Šlo je za uporabo termovizijske naprave, s katero so policisti opazovali osumljenčev dom in zaznali znatna temperaturna odstopanja, s čimer so utemeljevali pozneje izvedeno hišno preiskavo.

[54] Kyllo v. United States, 533 U.S. 27 (2001).

2.5. Videonadzorni sistem z vgrajenim sistemom prepoznave obraza in drugih biometričnih značilnosti

Lokacijo posameznika je možno pridobivati tudi s pomočjo sledenja prek zaprtega sistema kamer – CCTV ali *Closed Circuit Television system*[55] na določenem območju, in sicer v realnem času[56] ali pa historično.[57] Ker so danes ti sistemi že sposobni zajemati t. i. gigapiksel fotografije, ki omogočajo visoko ločljivost in prikaz podrobnosti,[58] lahko ob poznavanju biometričnih značilnosti opazovanega (na primer obraznih potez, brazgotin, tetovaž, barve kože, oči, las itd.) slednjega v množici ljudi hitro lociramo oziroma bi ga, v primeru velikanske baze podatkov, lahko prepoznali tudi v širši okolici, ki bi bila nadzorovana s takim sistemom.[59] Ta bi namreč na osnovi naprednih algoritmov na posnetku ali sliki prepoznal unikatne značilnosti posameznika, ki bi ga nato na določeno mesto umestil tako časovno kot tudi lokacijsko, saj bi nam bil znan položaj, na katerem je nameščena kamera, ki je takega posameznika »ujela«. Zaradi posegov v osebnost posameznika, zlasti v njegovo fizično integriteto v zvezi s sistematičnim beleženjem telesnih potez, ki jih je sistem sposoben zaznati, se v evropskem pravnem prostoru v večini držav zaradi varovanja osebnih podatkov zahteva jasna oznaka takega sistema, ki mora biti opazovanemu vidna in na kateri mora biti jasno označeno, da se na posameznem območju tak sistem uporablja.

Poudarjam, da je tak sistem za potrebe določanja lokacijske zasebnosti vsekakor primeren, saj temelji na močni subjektivni vezi med objektiviziranimi podatki in opazovanim posameznikom. Pogoj, da bo dotični posameznik najden, je namreč prav v vnosu objektivnih podatkov in karakteristik, ki so značilne iskanemu subjektu, zato bo do najmanjših napak in odstopanj prišlo ravno v takem sistemu, pri čemer bo zaradi vizualne umestitve posameznika na lokacijo praviloma mogoče dognati tudi njegov namen obiska te lokacije.

3. Mozaična teorija lokacijskih podatkov

Eden od teoretičnih pristopov pri ustvarjanju ravnotežja med koristmi in tveganji posega v lokacijsko zasebnost je zagotovo teoretični pristop po vzorcu mozaika oziroma krajše t. i. mozaična teorija.

---

55 Norris, McCahill, Wood, Editorial. The Growth of CCTV, 2(2/3), URL: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3369/3332, str. 110–135.

56 Na primer s sistemom Trapwire.

57 Na primer s sistemom FBI-jevega Next Generation Identification system.

58 Fallows, Technology is our friend … except when it isn't, URL: http://www.theatlantic.com/technology/archive/2011/08/technology-is-our-friend-except-when-it-isnt/244233/.

59 O tem tudi Tomšič, Lokacijska zasebnost – naslednje bojno polje varstva zasebnosti (2011), str. 16.

3.1. Opredelitev mozaične teorije

V obliki, kot je v praksi poznana še danes, se je mozaična teorija prvič pojavila v sodni praksi Združenih državah Amerike (ZDA)[60] v zvezi z vprašanjem razkritja tajnih podatkov s strani nekdanjega delavca CIE.[61] Svoj pravi pomen je dobila po terorističnih napadih 11. septembra 2001, pri čemer je ta po mnenju nekaterih čedalje večja.[62] Iz obrazložitve citirane zadeve izhaja, da je relevantnost enega podatka v soodvisnosti od drugih zbranih podatkov, in sicer tako, da en podatek tistemu, ki drugih podatkov ne pozna, ne pomeni veliko, nasprotno pa za tistega, ki je seznanjen s preostalimi podatki in tako vidi celotno sliko zadeve, tak posamičen podatek lahko pomeni pomembno vsebino in se popolnoma vključuje v videni kontekst, s katerim razpolaga informirana oseba. Iz mozaične teorije tako izhaja, da različni podatki sami zase nimajo neke dramatične vsebinske vrednosti, ko pa nekdo te podatke združi v celoto, slednja zaradi tega pridobi močan vsebinski pomen. Delci informacij so torej sami zase nekoristni, celota kot vsota teh delcev pa neprecenljiva.[63]

Do uveljavitve te teorije[64] je v kazenskih postopkih ZDA sicer prevladovalo razlogovanje,[65] da v javnosti oseba ne more upravičeno pričakovati zasebnosti, ki je temeljilo predvsem na okoliščini uporabe manj invazivne tehnologije, ki se jo je uporabljalo le za enkraten nadzor opazovane osebe. S tem ni bilo rešeno vprašanje modernih tehnologij, s katerimi lahko o posamezniku hkrati izvemo ne le njegove lokacije, temveč tudi, kaj na tisti lokaciji počne, niti ni bilo govora o celostnem nadzorovanju oziroma preiskovanju,[66] ki bi trajalo dalj časa. V zvezi s tem pa se je oblikovala mozaična teorija.

To lahko preprosto implementiramo v sklop varstva lokacijske zasebnosti. Kot je že bilo navedeno, lahko z moderno informacijsko tehnologijo o lokaciji posameznika pridobimo veliko količino podatkov. Razpolagamo torej z določenimi podatki, ki so sami zase pogosto brez pravega pomena – na primer nekdo je v enem mesecu med službenim časom šestkrat zapustil svoje delovno mesto zaradi nakupovanja v bližnjih trgovinah. Tako pridobljen podatek je precej samoumeven in ga nihče ne šteje za relevantnega. V času teh izhodov pa se je na poteh, ki vodijo od delovnega mesta do obiskanih trgovin, zgodilo šest ropov manjših bančnih poslovalnic. Prek lokacij gibanja te osebe, ki je trgovine obiskala v

---

60 United States v. Marchetti, 466 F.2d 1309, 1318 (4th Cir. 1972).

61 Central Intelligence Agency.

62 Gatewood, District of Columbia Jones and the Mosaic Theory – In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory (2014), str. 524.

63 Ostrander, The Mosaic Theory and Fourth Amendment Law (2011), str. 1734–1735.

64 Z zavzetim stališčem v zadevi United States v. Maynard, 615 F.3d 544, 561-562 (D.C. Cir. 2010).

65 United States v. Knotts, 460 U.S. 276, 283–284 (1983).

66 V nadaljevanju se prispevek osredotoča na zbiranje ter analiziranje lokacijskih podatkov za potrebe preiskovanja konkretnega kaznivega dejanja in ne na morebitno obdelavo lokacijskih podatkov za obveščevalno-varnostne potrebe države.

času ropov, lahko osebo lokacijsko in časovno umestimo v okoliščine kaznivih dejanj. Gre torej za povezovanje podatkov (po pravilu sestavljanja mozaika), s čimer zgradimo smiselno celoto in izoblikujemo končno sliko o historičnem poteku dogodka. Podoben je tudi primer, ko po vzorcu gibanja posameznika vidimo, da se je med drugim gibal na lokaciji, na kateri deluje znani preprodajalec orožja. To seveda sam zase ni presenetljiv podatek, vendar ob umestitvi v okoliščine skrivnostnega umora partnerke tega posameznika, ki je bila ubita s strelnim orožjem manjšega kalibra, kakršnega redno v odkup ponuja znani preprodajalec, lahko posameznika, ki je celo sam povedal, da sta se s partnerko sprla, povežemo z dostopom do strelnega orožja, čeprav sam zase trdi, da ga zaradi odsotnosti ustreznih dovoljenj sploh ne more dobiti, niti ga ne poseduje. Kot vidimo, je pomembna umeščenost podatka v ustvarjeno podobo, saj si lahko o dogodku le tako ustvarimo jasno predstavo oziroma tak podatek zoper nekoga uporabimo kot ključen dokaz.

S pomočjo tehnologije, ki nam ne pove le točne lokacije in nam ne odgovori le na vprašanje, kje se je nekdo gibal ali kam je šel, temveč nam posredno lahko zaupa tudi politične, verske, prijateljske, ljubezenske, profesionalne in prostočasne aktivnosti te osebe,[67] sprva dobimo ključen podatek, ki ga pozneje uvrstimo med celo kopico preostalih podatkov, na taki osnovi pa si ustvarimo sliko oziroma vpogled praviloma v tisto sfero, ki jo posameznik želi ohraniti kot zasebno. Bistvena je torej zmožnost zbiranja lokacijskih točk in ne sledenje gibanja, saj so lokacijske točke tiste, prek katerih se o posamezniku ustvari profil,[68] ki je tak, da ga povprečen opazovalec življenja opazovanega posameznika z lastnimi čutili in opazovanji ne bi bil zmožen ustvariti. Ključna je torej vsebina lokacijskih podatkov, prek katerih z miselno operacijo ustvarimo sliko o intimi opazovanega, taka agregacija lokacijskih podatkov in izoblikovanje celostne podobe pa je predmet varstva zasebnosti, ki jo posamezniku namenimo prav z uporabe mozaične teorije[69] kot nadgradnje koncepta pričakovane zasebnosti.

3.2. Vpliv pričakovane zasebnosti in njenih izjem na uporabo mozaične teorije

Teorija je neločljivo povezana s konceptom pričakovane zasebnosti, ki je splošno sprejet tako v ZDA[70] kot tudi v Evropi.[71] Po tem konceptu je smisel zaščite celostna integriteta posameznika (in ne več prostorov), pričakovanje zasebnosti pa upravičeno,

[67] People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009), podobno tudi v State v. Jackson, 76 P.3d 217 (Wash. 2003).

[68] In re Application of the United States of America, 736 F. Supp. 2d, 579.

[69] Kerr, The Mosaic Theory of the Fourth Amendment (2012-2013), str. 320, 328.

[70] Že od sprejema odločitve v zadevi Katz v. United States, 389 U.S. 347, 353 (1967).

[71] Kjer na rabo koncepta kažeta zadevi Halford v. the United Kingdom, Eur. Ct. H. R., 25. junij 1997, tč. 45 in Copland v. the United Kingdom, Eur. Ct. H. R., 3. julij 2007, tč. 42, v Sloveniji na primer odločba Ustavnega sodišča RS Up-3381/07 z dne 4. marca 2010, sodba Vrhovnega sodišča RS I Ips 63358/2010-170 z dne 4. oktobra 2012.

če posameznik na posameznem kraju upravičeno pričakuje zasebnost z dejanskim izražanjem zasebnosti, hkrati pa mora biti njegovo pričakovanje zasebnosti tako, da ga je družba pripravljena sprejeti kot upravičenega.

Od tega splošno sprejetega koncepta obstajajo tudi izjeme. Gre za 1.) doktrino tretje stranke (angl. *third-party doctrine*), po kateri posameznik, ki prostovoljno razkrije svoje osebne podatke oziroma informacije tretjim osebam, na primer bankam, telefonskim ponudnikom in ponudnikom internetnih storitev, glede razkritih podatkov oziroma informacij ne uživa upravičenega pričakovanja zasebnosti;[72] 2. doktrino prosto vidnih dokazov (angl. *plain-view doctrine*), po kateri je pravosodnim organom ob izvajanju zakonitih opravil znotraj njihovih okvirov, ki nenamerno[73] naletijo na dokaz obremenilnega značaja, tak dokaz dovoljeno uporabiti v poznejšem kazenskem postopku;[74] ter 3. doktrino razkritja javnosti (angl. *public disclosure doctrine*), po kateri posameznik ne more upravičeno pričakovati zasebnosti glede svojega gibanja, ki ga je zavestno izpostavil javnosti.[75] Bistvo vseh izjem je, da tisto, kar posameznik vestno in voljno izpostavi širši javnosti, ne more uživati statusa zasebnosti. Na osnovi koncepta pričakovane zasebnosti in teh izjem bi lahko torej na prvi pogled sklepali, da lokacije oziroma gibanja v javnosti pač ne moremo šteti za zasebno in da smo za doseganje lastnih potreb gibanje in našo lokacijo žrtvovali kot nujno zlo, saj smo ob tem nenehno izpostavljeni očem javnosti. V pomoč nam *prima facie* ne priskoči niti mozaična teorija, saj je po njej vsota podatkov, na katerih zasebnosti ni, nična (0 + 0 + … + 0 = 0),[76] s čimer je slika o podobi posameznika, ustvarjena prek teh podatkov, nezasebna. S tem se ni mogoče strinjati.

V tem delu je že bilo zastopano stališče, da družba ne bo vedno želela vpogleda o naših celodnevnih opravkih, pri katerih lahko izdamo našo lokacijo.[77] Nadalje naših premikov, ki so zaznavni javnosti, ne bo vedno spremljala enaka javnost, temveč različni subjekti, ki bodo lahko na naše gibanje pozorni ali pa ne. Tako si bodo nekateri dogodek našega obiska ali mimohoda zapomnili, spet drugi ne. Poleg tega javnost tudi ne bo

---

72 United States v. Miller, 425 U.S. 435 (1976), Smith v. Maryland, 442 U.S. 735 (1979) in United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012), v Sloveniji na primer odločba Ustavnega sodišča RS Up-540/11 z dne 13. februarja 2014.

73 Z uporabo čutil, na primer vonja, vida, sluha.

74 Tako o tem Arizona v. Hicks, 480. U.S. 321 (1987) in Horton v. California, 496 U.S. 128 (1990).

75 Stališče v United States v. Knotts, 460 U.S. 276, 278-279 (1983), o tem tudi Bedi, Social Networks, Government Surveillance and the Fourth Amendment Mosaic Theory (2014), str. 1826–1827.

76 Kot o tem tudi Sentelle, glavni sodnik v zadevi United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010).

77 Ford, Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology (2011), str. 1368. Državljani namreč ne pričakujejo, da bo nekdo brez odredbe sodišča neprekinjeno spremljal njihovo gibanje zaradi oblikovanja natančnega profila njihovega življenja, niti tega ne pričakujejo od svoje države, saj bi tako ravnanje nasprotovalo povprečnemu življenjskemu izkustvu.

vedno sposobna spremljati celotnega gibanja, temveč le njegov del, kot recimo v primeru vožnje z avtomobilom skozi središče mesta, kjer hitro menjavamo vozne pasove in se izgubljamo v stranskih ulicah. Čeprav bo nekaterim jasno, da smo bili v določenih okoliščinah na dotičnem kraju, tega ne bodo sposobni povezati z drugimi obiski tega kraja, saj nas ob neki drugi priložnosti tam niso bili sposobni zaznati.[78] Iz tega izhaja argument, da lahko na gibanju ali lokaciji, ki je zavestno in voljno izpostavljena javnosti, danes upravičeno pričakujemo zasebnost, saj preprosto ne sumimo, da nas nekdo na vsakem koraku opazuje in beleži naše nahajališče, s tem pa si ustvarja podobo o naši osebnosti. Zasebnosti ne moremo pričakovati na vsakem individualnem potovanju, ker z njim še ne pride do poseganja v zasebnost, temveč šele takrat, ko se z nenehnim lokacijskim sledenjem teh posamičnih gibanj na podlagi tako pridobljenih podatkov o posamezniku ustvari jasna slika, ki nam razkriva tisto, kar posameznik upravičeno šteje za zasebno (na primer obiske v psihiatrični bolnišnici, pri verski sekti, prostitutki itd.). Gre torej za to, da vsebinska vsota vseh posamičnih gibanj ni konstruktivno izpostavljena povprečnemu opazovalcu in ta vsota o nekom razkrije bistveno več, kot pa le vpogled v podatke, pridobljene z enkratnim opazovanjem. V tem je očitna razlika, saj vsota vsebin o posamezniku navzven pokaže njegove navade in vzorce gibanja, s čimer si je mogoče izoblikovati podobo o načinu njegovega življenja in ne le o dejavnikih njegovega posameznega dne, kar bi pridobili z opazovanjem enega konkretnega gibanja oziroma lokacije.[79] Sestavljanje podatkov, ki smo jih pridobili z opazovanjem enega gibanja, pri čemer smo posameznika preiskovali dalj časa, pa v primeru kakovostnih informacij pomeni sestavljanje celostne podobe posameznika in s tem sestavljanje mozaika.

Če je en lokacijski podatek prostovoljno podan, to še ne pomeni, da je podana prostovoljnost v zvezi z zbirko lokacijskih podatkov. Prostovoljnost namreč temelji na zavestni in voljni komponenti, pri čemer zavestni del (torej zavest o tem, da bo nekdo posegel v naše gibanje s sledenjem) v primeru nenehnega sledenja ne obstaja, niti družba kopičenja lokacijskih podatkov v zbirko ne želi,[80] s čimer prostovoljnost ni podana.[81]

Matematično sicer drži gornji pristop, da je seštevek vseh gibanj, na katerih ni zasebnosti, enak nič, vendar je treba posamično izpostavitev javnosti gledati globlje oziroma

---

78 Mesta so tipičen primer okolja, v katerem je mogoče zasebnost pričakovati zaradi nejasnosti (angl. *privacy by obscurity*) – lokacijski podatki niso obdani s fizičnimi ovirami (kot na primer v hiši), vendar jih je vse le z bežnim opazovanjem še vedno težko pridobiti. Povzeto po Sloan, Warner, The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State (2016), str. 354, 365.

79 Tako o tem v zadevi United States v. Maynard, 615 F.3d 544, 561-562 (D.C. Cir. 2010).

80 Tsai, Kelley, Cranor, in Sadeh, Location-Sharing Technologies: Privacy Risks and Controls (2010), str. 144.

81 Tomšič, Lokacijska zasebnost – naslednje bojno polje varstva zasebnosti (2011), str. 16 – prostovoljnost je podana šele tedaj, ko je posameznik ustrezno informiran o tem, da se bo njegovi lokaciji sistematično sledilo.

širše, s čimer opazimo, da z vsako izpostavitvijo posameznik pokaže del svoje osebnosti, torej psihične in fizične integritete, ki je pri varstvu zasebnosti bistvena. Seštevek teh delcev pa nikakor ni nič, temveč ravno obratno – je slika o profilu opazovane osebe.[82] S tega vidika torej ne moremo trditi, da posameznik upravičeno ni mogel pričakovati zasebnosti[83] oziroma da se ji je z izpostavitvijo javnosti sam odpovedal,[84] saj se je odpovedal le zasebnosti v okviru enkratne izpostavitve, ne pa tudi izoblikovanju zbirke podatkov, do katere je mogoče priti s povezovanjem koščkov relevantnih informacij. Kot korektiv »zastarelemu« subjektivnemu delu koncepta pričakovane zasebnosti[85] lahko uporabimo mozaično teorijo, ki nam omogoča, da zavarujemo tudi tista dejanja oziroma gibanja posameznikov, ki so navzven zaznavna, vendar šteta kot zasebna[86] in bi se lahko na njihovi podlagi dognale intimne informacije o posameznikovem življenju. Objektivni del koncepta pričakovane zasebnosti pa ostaja izkazan, saj lahko zaskrbljenost nad uporabo lokacijskih podatkov[87] (upravičeno) štejemo kot potrditev, da družba izoblikovanje osebnostnega profila šteje kot zasebno. Poleg tega tudi ni verjetno, da bi bil nek povprečen posameznik sposoben opazovati vsa gibanja osebe,[88] saj to ni v družbenih navadah[89] oziroma je to težko celo v primeru dobro opremljene policijske enote.[90] Če do predlaganega popravka ne bo prišlo, bo lokacijska zasebnosti izvotljena, nastopila pa bo absurdna situacija, v kateri se bo uporabo napredne tehnologije utemeljevalo s sklicevanjem na to,

---

82 Kalis, Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance (2012–2013), str. 14.

83 Subjektivni del testa upravičenega pričakovanja zasebnosti.

84 Selinšek, Razumno pričakovanje zasebnosti v dobi velikih podatkov (2015), str. 122. Avtorica se pridružuje stališču, da z uporabo sodobnih naprav in storitev sami razkrivamo podatke, zato pričakovanje zasebnosti ni več razumno.

85 Da je koncept pričakovane zasebnosti neprimeren, ker ljudje pri vsakdanjih opravilih o sebi izdamo veliko podatkov predvsem zaradi življenja v t. i. digitalni dobi, poudarja tudi sodnica Sotomayor v zadevi United States v. Jones, 565 U.S. (2012).

86 Kalis, Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance (2012–2013), str. 16 ter Gray, Citron, A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy (2012–2013), str. 402. Mozaična teorija ob upoštevanju vsote zbranih podatkov o gibanju posameznika in njihovega pomena nadvlada izjeme koncepta pričakovane zasebnosti in posamezniku zagotavlja varstvo zaradi seštevka zbranih informacij, ki ne izdajajo le lokacije, temveč podatke iz osebne sfere posameznika.

87 Tsai, Kelley, Cranor, in Sadeh, Location-Sharing Technologies: Privacy Risks and Controls (2010), str. 144.

88 Verjetnost tega meji na nično – United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010).

89 In zato tega družba ne pričakuje – podobno o tem Sloan, Warner, The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State (2016), str. 354, tudi United States v. Maynard, 615 F.3d 559 (D.C. Cir. 2010).

90 United States v. Knotts, 460 U.S. 276, 278–279 (1983).

da je bila tehnologija uporabljena v javnem okviru.[91] Taka argumentacija pa bo vodila v to, da se ljudje ob izvajanju vsakodnevnih opravil ne bodo več gibali svobodno in bodo na vsakem koraku v dvomu, ali jim kdo ne sledi, s čimer jim bo kršena ena od temeljnih pravic in svoboščin – pravica do svobodnega in nenadzorovanega gibanja.[92]

3.3. Problematičnost sestavljanja mozaika

Kljub vsemu pa teorija le ni tako popolna in preprosta, kot na to trenutno namigujejo črke na papirju. Na prvem mestu je vredno omeniti, da že ob opazovanju ni jasno, kdaj (tako časovno[93] kot tudi vsebinsko) pride do vzpostavitve vzorca in vpogleda v osebnost, s tem pa do razgaljenja posameznikove zasebnosti na njegovem gibanju.[94] Opazovalci so v tem predvidevanju prepuščeni sami sebi in morajo dejansko delovati kot varuhi zakonitosti temeljnih pravic opazovane osebe,[95] kar ni skladno z njihovo funkcijo odkrivanja, preiskovanja in preprečevanja kaznivih dejanj, prav tako pa se posega v temelj odločanja sodišč, saj je na slednjih presoja upravičenosti in zakonitosti posameznega tipa nadzora. S tega vidika je torej v prihodnosti vsekakor bolje razmišljati o pregledni in natančni zakonski ureditvi, ki bo poleg časovnih omejitev prinesla tudi sodni nadzor nad izvajanjem poseganja v lokacijsko zasebnost, s čimer bo zadovoljena potreba po preverjanju zakonitosti takega posega. V pravni teoriji se že oblikujejo kriteriji,[96] s katerimi bi si pravosodni organi lahko pomagali pri vprašanju, ali je bilo poseženo v posameznikovo zasebno sfero. Sodnik bi moral pri rešitvi slednjega ugotoviti 1.) dolžino dejanskega opazovanja;[97] 2.) invazivnost pri tem uporabljene tehnologije;[98] 3.) ali je prišlo do beleženja podrobnosti

[91] O tem tudi Dickman, Untying Knotts: The application of Mosaic Theory to GPS surveillance in United States v. Maynard (2011), str. 735.

[92] Saj je njihovo pričakovanje zasebnosti tako signifikantnega pomena tudi izven njihovega domovanja – *a simili ad simile* Perry v. The United Kingdom, Eur. Ct. H. R., 17. oktober 2003, tč. 37.

[93] T. i. dragnet type surveillance – prolongirano opazovanje.

[94] United States v. Sparks, No. 10-10067-WGY, slip op. At 9 (D. Mass. Nov. 10, 2010).

[95] Gray, Citron, A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy (2012–2013), str. 409.

[96] Dickman, Untying Knotts: The application of Mosaic Theory to GPS surveillance in United States v. Maynard (2011), str. 741–742.

[97] Kerr, The Mosaic Theory of the Fourth Amendment (2012-2013), str. 333 – Kerr opozarja, da je treba raziskati, v kakšnih intervalih je naprava, s katero smo posegli v lokacijsko zasebnost nekoga, delovala, saj bi lahko delovala na primer v intervalu enkrat mesečno, s čimer pa ne bi bil izpolnjen pogoj dalj časa trajajoče preiskave, po drugi strani pa bi lahko (Gray, Citron, A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy (2012–2013), str. 419) enodnevna tehnološko okrepljena preiskava presegla dovoljeni prag in izoblikovala tisto, kar je v sklopu mozaične teorije treba zaščiti.

[98] V smislu v 2. poglavju tega prispevka predstavljenih možnosti, pri čemer je na tem mestu ključna rešitev vprašanja, ali je bila uporabljena tehnologija, s katero se lahko dejansko pridobi lokacijski podatek.

osebnega življenja;[99] 4.) ali so bila gibanja posameznika izpostavljena širši javnosti, na tej podlagi pa je bila izoblikovana njegova osebnostna podoba; in 5.) ali je bilo delo policistov tehnološko tako nadomeščeno, da njihova ravnanja (v smislu neposrednega opazovanja) niso bila potrebna, niti jih ne bi bili zmožni izvršiti na način in v obsegu, kot je bila to sposobna »izvajati« tehnologija. Šele nato bo lahko sodnik sprejel sklep, ali je bilo s pridobitvijo lokacijskih podatkov dejansko poseženo v zasebnost.

Problematičen je tudi odgovor na vprašanje, s katerim dejanjem policistov se vzorec sploh začne oblikovati, saj policisti v sklopu svojega dela pogosto sprva dalj časa preverjajo okoliščine kaznivega dejanja oziroma njegove bodoče izvršitve, šele za tem se odločijo posegati po bolj »urejenih« ukrepih, za katere je potrebna sodna odločba.[100] Do te točke je namreč lahko profil posameznika že v celoti izoblikovan, slednji pa bo le težko užival pravico do učinkovite obrambe, saj ne bo vedel, kako so bili relevantni podatki zbrani.[101]

Nadalje tak pristop vpliva tudi na razporeditev dokaznega bremena v morebitnem kazenskem postopku.[102] Tako mora za izločitev dokaza, pridobljenega s takim opazovanjem, v postopku aktivno vlogo imeti obdolženec, ki mora izkazati, da se je prek opazovanja ustvarila jasna podoba njegove zasebnega življenja, do katere je prišlo prav s sestavljanjem koščkov, pridobljenih ob posamičnih opazovanjih. Tožilcu zagotovo ni v interesu, da bi kritični dokaz (na primer lokacijsko umestitev obdolženca na kraj kaznivega dejanja) izpustil iz rok in s tem tvegal oprostilno sodbo. Seveda pa se s tem posega v obdolženčev privilegij zoper samoobtožbo. Lokacijski podatek je lahko ključen element kaznivega dejanja. Hočeš nočeš pa se bo obdolženec za svojo uspešno obrambo glede tega podatka moral opredeliti, s čimer bo nedvomno poseženo v temelj privilegija, po katerem lahko posameznik z organi pregona sodeluje le toliko, kot sam prostovoljno želi in hoče. Zmanjšana bo tudi učinkovitost take obrambe (obrambe s sklicevanjem na zlaganje mozaika), saj bo moral obdolženi podati ustrezne dokazne predloge, s katerimi si bo prizadeval doseči izvedbo dokazov, prek katerih bo sodišču predstavil, da je neko informacijo, ki se je s takim daljšim preiskovanjem lokacije dognala, štel za zasebno.[103] Ob tem ni pa rečeno, da bodo ti predlogi uspešni,[104] saj obdolžencu ne bo znano, katero je bilo prvo ravnanje, ki je privedlo do izoblikovanja mozaika oziroma katera so bila preostala preiskovalna dejanja, ki so izoblikovala dokazno gradivo.

[99] Oziroma katere podrobnosti so bile vsebinsko sploh zaznane (presoja vsebine).

[100] Gray, Citron, A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy (2012–2013), str. 399.

[101] Avtorju je iz narave njegovega poklicnega dela znano, da policisti svoje delo pogosto opravičujejo s sklicevanjem na taktiko in metodiko policijskega dela, zaradi katere zavračajo odgovore na vprašanja o načinu pridobivanja podatkov.

[102] Ostrander, The Mosaic Theory and Fourth Amendment Law (2011), str. 1749.

[103] O tem tudi Kerr, The Mosaic Theory of the Fourth Amendment (2012-2013), str. 330–331.

[104] Neracionalno in pretirano dokazno breme v zvezi z učinkovitim varstvom zasebnega življenja pomeni kršitev 8. člena EKČP – Turek v. Slovakia, Eur. Ct. H. R., 13. september 2006, tč. 116.

Mozaični pristop tudi ne ponuja razlogovanja o njegovem dometu. V primeru sočasne uporabe več metod preiskovanja, pri čemer je ugotavljanje lokacije le ena od njih, lahko zaradi poznejše implementacije mozaika na preiskovani primer po doktrini zastrupljenega sadeža propade celoten primer.[105] Domet je tako neomejen in se, če oseba izkaže, da so si opazovalci ustvarili sliko o njenem zasebnem življenju, celoten postopek izkaže za nezakonitega, saj je varstvo zasebnosti, upoštevajoč mozaično teorijo, naklonjeno vsem delcem, ki so privedli do izoblikovanja profila.[106]

Te posledice teorije mozaika so nesorazmerne v primerjavi z drugimi oblikami preiskovanja. Na primer sledenje prek naprave GPS nam o neki osebi ustvari sliko in vzorec njenih ravnanj, na kar bo mogoče vplivati s sklicevanjem na predstavljeno teorijo, na drugi strani pa lahko na primer preiskavo smeti oziroma odpadkov osebe, ki po moji oceni[107] pomeni še večji poseg v posameznikovo zasebnost,[108] izvedemo brez sodnih garancij izključno v policijski režiji. Manjši poseg v zasebnost je tako sankcioniran močneje kot pa bolj kritično brskanje po smeteh, s katerim se očitno posega v osrčje varstva zasebnosti – posameznikovo fizično in psihično integriteto.[109]

Obstoj mozaičnega pristopa navsezadnje ni ustaljen niti v ZDA, od koder izvira. V tamkajšnji sodni praksi so se namreč pojavila različna stališča v zvezi z uporabo moderne tehnologije, ki po svoji vsebini (in specifičnih okoliščinah) nasprotujejo uporabi te teorije.[110] Kakšna je ob teh stališčih njena nadaljnja usoda, ni jasno, niti ni razvidno, kako se izogniti argumentu, da je tehnologija, ki jo za potrebe preiskovanja in odkrivanja kaznivih ravnanj uporablja policija, že postala splošno dostopna javnosti, s tem pa po mnenju nekaterih[111] primerna za izvedbo preiskovanja in nadzorovanja. Eno od odprtih vprašanj je tudi razlikovanje med tehnologijo, ki opazovalcu razširi njegove čute, ter tehnologijo, s katero je mogoče pridobiti informacije, ki jih na drugačen način, na primer izključno z delom opazovalca, ni mogoče pridobiti.[112]

---

105 Kerr, The Mosaic Theory of the Fourth Amendment (2012-2013), str. 335–336.

106 *A contrario* o tem Kerr, The Mosaic Theory of the Fourth Amendment (2012-2013), str. 343.

107 O tem tudi Ostrander, The Mosaic Theory and Fourth Amendment Law (2011), str. 1751.

108 Predvsem zato, ker v smeteh končajo zabeležke, računi, dotrajani izvidi, neuporabni in pokvarjeni predmeti itd., iz katerih se lahko razbere veliko več o posamezniku, kot pa bi to lahko dognal le s pomočjo nenehnega preverjanja lokacije.

109 Niemietz v. Germany, Eur. Ct. H. R., 16. december 1992, tč. 29 in Botta v. Italy, Eur. Ct. H. R., 24. februar 1998, tč. 32.

110 United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010), United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) in United States v. Garcia, 474 F.3d 994, 997-96 (7th Cir. 2007).

111 Eden od bistvenih argumentov v zadevi Kyllo v. United States, 533 U.S. 27 (2001) je bil, da tehnologija, uporabljena za izvedbo preiskave, ni bila dostopna splošni javnosti.

112 Goetz, Locating Location Privacy (2011), str. 833–834.

Razdelek bom sklenil s pozitivnim mišljenjem, in sicer z mnenjem, da je kljub predstavljenim težavam mozaični pristop vsekakor dobrodošel, saj je prožen[113] in s tem prilagodljiv »krušenju« zasebnosti, do katerega prihaja z velikanskim razvojem informacijske tehnologije, ki ima v moderni družbi čedalje pomembnejšo vlogo. Teorija mozaika lahko tudi vzpostavi ravnotežje med proaktivnim in reaktivnim odzivanjem na preiskovanje kriminalitete ter družbenim interesom po zasebnosti na lokaciji,[114] ki sta v večnem boju, ki mu še posebej zaradi razvoja tehnologije preprosto ni videti konca. Gre za pomemben učinek, ki kaže na prilagodljivost teorije, saj če sodnik spozna, da je sprememba tehnologije oziroma socialnega pričakovanja oslabila metode preiskovanja (na primer delinkventi za izvršitev kaznivih ravnanj uporabljajo napredne metode šifriranja njihove komunikacije[115]), varstvo zasebnosti lokacije lahko zniža (saj tudi s pomočjo napredne tehnologije ne bo mogoče posegati v njihovo zasebnost) in obratno.[116] Zato je mozaični pristop vredno vzeti v presojo[117] predvsem z vidika razvijajoče se tehnologije,[118] saj lahko s prepričanjem pričakujemo, da bo njen razvoj zaradi cenitve resursov v prihodnosti še večji in še hitrejši.

4. Evropski pravni standardi varstva lokacijske zasebnosti

Uporaba predstavljenega pristopa prevladuje na ozemlju Združenih držav Amerike, kjer to področje urejajo procesna in materialna pravila, ki se razlikujejo od evropskih. Zato se bom v nadaljevanju osredotočil predvsem na implementacijo mozaične teorije v evropski pravni prostor, in sicer z razlago primerne pravne podlage ter sodne prakse Evropskega sodišča za človekove pravice (ESČP).

4.1. Pravna podlaga varstva lokacijskih podatkov

Pojem zasebnega življenja, v katerega moderna tehnologija nedvomno posega, je urejen v Evropski konvenciji o človekovih pravicah in temeljnih svoboščina (EKČP). Gre za zavezujoč pravni akt, ki z ratifikacijo zavezuje 47 držav članic Sveta Evrope, za zago-

[113] Ford, Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology (2011), str. 1365.

[114] Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment (2011), str. 487–488.

[115] Oliver, Location, Location, Location: balancing Crime Fighting Needs and Privacy Rights (2013), str. 486, 508.

[116] Gatewood, District of Columbia Jones and the Mosaic Theory – In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory (2014), str. 533.

[117] *A simili ad simile* tudi Wagner, Stopping Police in Their Tracks: Protecting Cellular Location Information Privacy in the Twenty-First Century (2014), str. 212.

[118] Goetz, Locating Location Privacy (2011), str. 854.

tovitev spoštovanja obveznosti tega akta pa je pristojno ESČP,[119] ki njene pravne norme tudi razlaga.

Po 8. členu EKČP ima vsakdo pravico do spoštovanja svojega zasebnega in družinskega življenja, svojega doma in dopisovanja, javna oblast pa se v izvrševanje te pravice ne sme vmešavati, razen če je to določeno z zakonom in v demokratični družbi nujno zaradi državne varnosti, javne varnosti ali ekonomske blaginje države zato, da se prepreči nered ali zločin, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.

Izčrpne opredelitvi pojma zasebno življenje, ki jo je treba podati za potrebe tega dela, ni,[120] saj gre za širok pojem,[121] ki je v primerjavi s pravico do zasebnosti širši in se nanaša na sfero, znotraj katere lahko vsak svobodno razvija in izpopolnjuje svojo osebnost.[122] Pojem zajema telesno, psihološko in moralno nedotakljivosti,[123] vključno z zdravljenjem[124] in vidiki telesne in družbene identitete posameznika;[125] prostor, kjer posameznik svobodno uresničuje razvoj in izpopolnitev svoje osebnosti;[126] pravico do podobe ali do fotografij osebe,[127] osebni ugled[128] in življenje,[129] pravico do vzpostavljanja in razvijanja odnosov z drugimi ljudmi,[130] pri čemer pojem varuje tudi učinkovitost vzpostavljanja odnosov,[131] pravico do osebnega razvoja in osebne svobode[132] ter podatke o političnih dejavnostih oseb, ki jih zberejo in hranijo varnostne službe ali druge državne oblasti.[133]

ESČP o vprašanju, ali posamezne informacije spadajo v kontekst zasebnega življenja iz 8. člena EKČP, presoja na podlagi specifičnih okoliščin vsakega primera. Vendar pa lahko s stopnjo gotovosti trdimo, da lokacijski podatki, s katerimi se odkriva posameznikova osebnost, spadajo pod okrilje predstavljenega varstva. Varstvo se namreč *prima*

[119] Člen 19 EKČP.

[120] Niemietz v. Germany, Eur. Ct. H. R., 16. december 1992, tč. 29.

[121] Costello-Roberts v. The United Kingdom, Eur. Ct. H. R., 25. marec 1993, tč. 36.

[122] Kilkelly, The right to respect for private and family life (2003), str. 11.

[123] X and Y v. The Netherlands, Eur. Ct. H. R., 26. marec 1985, tč. 22.

[124] Glass v. The United Kingdom, Eur. Ct. H. R., 9. marec 2004, tč. 70–72.

[125] Mikulić v. Croatia, Eur. Ct. H. R., 4. september 2002, tč. 53; in Smirnova v. Russia, Eur. Ct. H. R., 24. oktober 2003, tč. 95–97.

[126] Brüggemann and Scheuten v. Federal Republic of Germany, Eur. Ct. H. R., 12. julij 1997, tč. 55.

[127] Von Hannover v. Germany, Eur. Ct. H. R., 24. september 2004, tč. 50–53. in Recklos and Davourlis v. Greece, Eur. Ct. H. R., 15. april 2009, tč. 40.

[128] Polanco Torres and Movilla Polanco v. Spain, Eur. Ct. H. R., 21. februar 2011, tč. 40.

[129] A.D.T. v. The United Kingdom, Eur. Ct. H. R., 31. oktober 2000, tč. 21–26.

[130] Niemietz v. Germany, Eur. Ct. H. R., 16. december 1992, tč. 29.

[131] McFeely & Ors v. The United Kingdom, Eur. Ct. H. R., 15. maj 1980, 20 DR 44.

[132] Friend v. The United Kingdom in Countryside Alliance and other v. The United Kingdom, Eur. Ct. H. R., 24. november 2009, tč. 40–43.

[133] Amann v. Switzerland, Eur. Ct. H. R., 16. februar 2000, tč. 65–67; in Rotaru v. Romania, Eur. Ct. H. R., 4. maj 2000, tč. 43–44.

facie naklanja postavkam, ki se osredotočajo na posameznika kot center pojma,[134] poleg tega pa so osebnostne predispozicije (celostna integriteta subjekta, njegova identiteta, ugled in življenje, v sklopu katerega izvaja aktivnosti in se socialno povezuje) varovane tudi v prostoru (ki je lahko zaseben ali pa javen[135]), kjer prihaja do osebnostnega razvoja posameznika. Z osebnostnimi lastnostmi se prekriva narava pridobljenih lokacijskih podatkov, saj s sestavljanjem fragmentov dosežemo vpogled v posameznikovo zasebno sfero, pridobivanje lokacijskih podatkov, ki se praviloma pridobivajo v javnosti, pa je varovano tudi v javnosti, saj tam prihaja do medsebojne interakcije z družbo.

Seveda ima tisti, ki je zakonito na ozemlju kake države, tudi pravico do svobodnega gibanja po tem ozemlju.[136] Gre za pravico, zaradi katere se lahko posameznik po ozemlju države, v kateri se zakonito nahaja, giblje prosto in nenadzorovano, brez morebitnih ovir in brez pridobivanja avtoritativnih dovoljenj, pri čemer ne sme trpeti nobenih nerazumnih omejitev, razen tistih, ki so določene z zakonom in ki so v demokratični družbi nujne zaradi državne in javne varnosti, za vzdrževanje javnega reda, za preprečevanje kaznivih dejanj, za zaščito zdravja ali morale ali za varstvo pravic in svoboščin drugih ljudi.[137] Zato v primeru prikritega opazovanja posameznikovega gibanja posežemo v človekovo eksistenco in s tem v osrčje pravice do svobodnega gibanja, saj to ni več popolnoma svobodno in ne pomeni več izraza njegove lastne in svobodne volje.

Očitno je torej, da so lokacijski podatki predmet varstva 8. člena EKČP,[138] saj lahko z njihovo pridobitvijo gradimo identifikacijski profil opazovanega in se s sklicevanjem na javnost teh podatkov dokopljemo do »najtemnejših kotičkov« tistega, kar nekdo šteje za zasebno. Tako varnost se jim zagotavlja kljub elementu javnosti, prek katerega bi lahko sklepali na zavestno in prostovoljno izpostavitev naše zasebnosti širšemu krogu družbe. Varnost podatkov pa uživa pravno dobroto 8. člena EKČP že, če za potrebe poznejših postopkov zoper opazovanega pride do obdelave teh podatkov, ki so bili pridobljeni prav zaradi racionaliziranja stroškov, torej z uporabo tehnologije.

4.2. Način pridobivanja podatkov in uporaba mozaične teorije

Lokacijske podatke lahko torej umestimo med informacije, varovane v okviru 8. člena EKČP, vendar pa so načini oziroma metode zbiranja teh podatkov odvisni od specifičnih nacionalnih zakonodaj, zaradi česar moramo razlikovati vsaj tri položaje.

---

134 Varstvo zasebnosti je namreč izoblikovano in namenjeno posamezniku kot subjektu.

135 P.G. and J.H. v. the United Kingdom, Eur. Ct. H. R., 25. december 2001, tč. 56–57. in Peck v. The United Kingdom, Eur. Ct. H. R., 28. april 2003, tč. 57.

136 T. i. svoboda gibanja, ki izhaja iz prvega odstavka 2. člena Protokola št. 4 k EKČP.

137 Drugi odstavek 2. člena Protokola št. 4 k EKČP.

138 Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 49–52.

Za ESČP so oblike poseganja v pravico do spoštovanja zasebnega življenja iz do zdaj obravnavanih primerov predvsem: preiskave in zasegi,[139] nadzor nad sporazumevanjem in telefonskimi pogovori,[140] video nadzor javnih mest,[141] GPS-nadzor[142] in video nadzor delodajalca nad delavcem.[143] Tako poseganje v zasebnost oziroma zbiranje lokacijskih podatkov s pomočjo napredne tehnologije mora biti urejeno na zakonodajni ravni,[144] zato mozaične teorije ni mogoče uporabiti. Če take zakonodaje ni, gre za kršitev 8. člena EKČP,[145] in sicer v delu, v katerem citirani paragraf določa, da je v zasebnost dovoljeno posegati le »v skladu z zakonom«[146] (prvič).

Kljub različnim evropskim zakonskim ureditvam lahko v primeru uporabe moderne tehnologije za potrebe kazenskega pregona varstvo iz 8. člena EKČP izgubi svoj pomen (drugič). Tega jasnega dejstva se zaveda tudi ESČP, ki v primerih uporabe sofisticiranih tehnoloških naprav za potrebe učinkovite izvedbe kazenskega postopka opozarja, da bi lahko njihova uporaba »za vsako ceno« in brez pazljivega uravnoteženja ob upoštevanju interesov zasebnega življenja nesprejemljivo oslabila garancije, ki jih zagotavlja 8. člen EKČP.[147] Države v sklopu svoje diskrecijske zakonodajne pravice tudi niso pooblaščene sprejemati kakršnihkoli tehnološko dovršenih ukrepov, ki se jim zdijo primerni in s katerimi bi se posegalo v zasebnost posameznika, kar velja celo v primerih, ko *ratio* za tako nomotehnično urejanje izvira iz boja proti vohunstvu ali terorizmu.[148] Zato morajo biti posegi v zasebnost utemeljeni na določeni pravni podlagi, ki mora biti dosegljiva in predvidljiva. Pravno pravilo je predvidljivo le takrat, kadar je oblikovano natančno in jasno,[149] pravna pravila pa morajo natančno urejati tudi uporabo naprav in sredstev za izvedbo poseganja v zasebnost, pri čemer morajo biti ta pravila dostopna širšemu krogu javnosti.[150] Tako predvsem zato, ker tehnologija danes postaja vse bolj sofisticirana in

[139] McLeod v. The United Kingdom, Eur. Ct. H. R., 25. avgust 1998, tč. 36; Funke v. France, Eur. Ct. H. R., 25. februar 1993, tč. 48; in Foka v. Turkey, Eur. Ct. H. R., 26. januar 2009.

[140] Weber and Saravia v. Germany, Eur. Ct. H. R., 29. junij 2006, tč. 76–79.

[141] Peck v. The United Kingdom, Eur. Ct. H. R., 28. april 2003, tč. 57–63.

[142] Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 52.

[143] Köpke v. Germany, Eur. Ct. H. R., 5. oktober 2010, v delu A./2./predzadnji odstavek.

[144] Na primer 100.h–100.j člen Strafprozessordnung (StPO) Zvezne republike Nemčije, 149.a–149.b člen Zakona o kazenskem postopku (ZKP) Slovenije, 130. člen Strafprozessordnung (StPO) Avstrije, 15.a poglavje Zakona o kazenskem postopku Kraljevine Norveške, IV. poglavje Zakonika o kazenskem postopku Romunije itd.

[145] P.G. and J.H. v. the United Kingdom, Eur. Ct. H. R., 25. december 2001, tč. 37–38; in Taylor-Sabori v. The United Kingdom, Eur. Ct. H. R., 22. januar 2003, tč. 16–19.

[146] V angleškem izvirniku: »*in accordance with the law*«.

[147] S. and Marper v. The United Kingdom, Eur. Ct. H. R., 4. december 2008, tč. 112.

[148] Klass and others v. Germany, Eur. Ct. H. R., 6. september 1978, tč. 49.

[149] Amann v. Switzerland, Eur. Ct. H. R., 16. februar 2000, tč. 55–56.

[150] Khan v. The United Kingdom, Eur. Ct. H. R., 4. oktober 2000, tč. 27.

zmožna prikritega poseganja v naše zasebnost.[151] V nasprotnem primeru lahko uporaba nejasnih in nedostopnih pravnih pravil pripelje do različne uporabe zakona in arbitrarnosti državnih ali drugih organov,[152] kavtele posameznika pa so neučinkovite, saj mu pravna podlaga, ki je privedla do oblikovanja zbirke podatkov, sploh ni znana oziroma razumljiva. Zakonodaja mora tako vsebovati podrobna pravna pravila, ki hkrati po eni strani preprečujejo arbitrarnost, po drugi strani pa preprečujejo zlorabe uporabljenih sredstev moderne tehnologije.[153] Če pravila nekaterih omejitev izrecno ne vsebujejo – na primer dokaznega standarda, ki je potreben za izvedbo poseganja v zasebnost, izvajalca ukrepa, čas trajanja ukrepa, tehnoloških naprav, ki se za ukrep uporabljajo, način ravnanja z njimi ter druge omejitve, ki jih je treba ob tem zaradi varstva zasebnosti spoštovati –, gre za kršitev 8. člena EKČP.

Tretjič pa zakonodaja s predmetnega področja lahko obstaja in je jasna ter transparentna, vendar jo državni organi, pristojni za odkrivanje, preiskovanje ter pregon kaznivih dejanj, zaobidejo s svojimi ravnanji, ki sicer sama po sebi niso protipravna ali nezakonita, vendar se lahko na njihovi osnovi globoko poseže v zasebnost. Tako na primer policisti v sklopu taktike in metodike policijskega dela:

– opazujejo in patruljirajo, s čimer se lahko seznanijo z lokacijo in območjem posameznikovega gibanja.[154] Enkraten vpogled v tako pridobljene podatke seveda še ne prinese varstva zasebnosti, je pa tako v primeru, če je preiskovanje tako kakovostno, da si lahko na taki osnovi ustvarimo podobo posameznikovega življenja;[155]
– sledijo lokaciji prek svetovnega spleta in družabnih omrežij (na primer Facebooka),[156] na katerih posameznik sicer voljno izpostavi svojo lokacijo, pri čemer se ne zaveda, da je lokacija sistematično zabeležena. Ob takem ravnanju je poseg še hujši, če ob izražanju lokacije pride do objave statusa ali fotografije,[157] ki sta lahko inkriminirajoča, kar je za organe pregona še večji uspeh in podpora njihovi »domnevi krivde«. Tako sledenje je lahko marsikdaj prikrito, na primer eden od opazovalcev se kot prijatelj opazovanega infiltrira in tako dostopa do družabnega omrežja in zato tudi v primeru,

[151] Weber and Saravia v. Germany, Eur. Ct. H. R., 29. junij 2006, tč. 93; in Iordachi and others v. Moldova, Eur. Ct. H. R., 14. september 2009, tč. 39.

[152] S tem se evidentno posega tudi v možnost sodnega nadzora nad njihovim delom.

[153] Tako o tem tudi Križnar, Uporaba tehnologij nadzora skozi novejšo slovensko sodno prakso (2015), str. 20.

[154] Gray, Citron, A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy (2012–2013), str. 404.

[155] Odločba Ustavnega sodišča RS U-I-272/98 z dne 8. maja 2003, tč. 22.

[156] Več o Facebooku in lokaciji Facebook Inc., Facebook and Location, URL: https://www.facebook.com/help/337244676357509/.

[157] Nekatere spletne aplikacije (Snapchat, Povio) zahtevajo, da uporabniki za njihovo uporabo delijo tako lokacijo kot tudi drugo vsebino s te lokacije, na primer fotografijo, s čimer svojim prijateljem pokažejo, kaj tam počno.

ko opazovani svojo objavo deli le s krogom prijateljev, infiltrirani tako objavo zazna in si lokacijo zabeleži;[158]
– pridobivajo posnetke videonadzornih kamer, ki v svoj vidni objektiv zajemajo javna območja (ki na primer posnamejo demonstracije ali pa vsak dan v objektiv ujamejo osebo, ki je predmet državnega zanimanja);[159]
– uporabijo dovršene tehnološke naprave, na primer IMSI-lovilec,[160] s katerim se lahko potrdi, da se zanimanja vredna telefonska številka nahaja na posameznem območju, ali pa termovizijsko napravo,[161] s katero je mogoče tudi v nočnem času spremljati gibanje opazovanega v urbanem ali naravnem okolju, pri čemer opazovani zoper delovanje s tema dvema napravama nima možnosti učinkovitega pravnega varstva, saj, kot že rečeno, njuna uporaba ni predmet izrecnega zakonskega urejanja (oziroma v nekaterih državah take pravne podlage sploh ni);
– pridobivajo podatke s strežnika podjetja, ki prostovoljno sodeluje v preiskavi, s čimer si pridobijo podatke o naslovih IP, ki so obiskali spletno stran podjetja;
– kljub odsotnosti presoje zakonitosti ukrepa s strani nepristranskega in objektivnega sodišča in ob nespoštovanju zakonskega ravnanja na avtomobil ali drug osebni predmet opazovanega namestijo GPS oddajnik ter mu sledijo;[162]
– pridobivajo podatke z vgrajene navigacijske naprave najetega vozila, ki ga je pred tem uporabljala preiskovana oseba,[163] nato pa njen lastnik privoli v tak poseg;
– zbirajo obvestila o gibanju posameznika s strani očividcev;[164]
– pridobijo sledi DNK s kraja nahajanja itd.

Očitno je, da gre v teh primerih za pridobivanje lokacijskih podatkov na načine, s katerimi se na povsem legalne načine (razen protizakonitega delovanja policije) v okviru temeljnih delovnih nalog ter ob odsotnosti sodne presoje zbira lokacijske podatke, na osnovi katerih je mogoče izoblikovati posameznikov osebni profil. Če se ob tem pridobi-

---

158 Avtorju je iz njegovega poklicnega dela znano, da (vsaj slovenska) policija pri svojem delu uporablja družabna omrežja v zvezi s preverjanjem okoliščin kaznivih dejanj, teoretično pa je opisal, kako lahko z izrabo zaupanja pride do nezaželenega razkritja podatkov in s tem kršitve načela zakonitosti pri opravi procesnih dejanj, kot jih dopušča ZKP, seveda če po tem prikritem načinu poseže policist.

159 To omogočata 113. in 114. člen Zakona o nalogah in pooblastilih policije (ZNPPol), Uradni list RS, št. 15/13 in 23/15 – popr.

160 Njegova ureditev je predlagana v noveli ZKP-N.

161 Na podlagi 113. člena ZNPPol.

162 Ford, Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology (2011), str. 1369–1370. Fordova opozarja, da ne gre za osamljene primere ter da se intenziteta takega dela policije v ZDA po 11. septembru 2001 le še stopnjuje, pri čemer se usmerja predvsem zoper osebe določenega porekla, vere, političnega in drugačnega prepričanja od tistega, ki stoji za državnim.

163 Prav tam, str. 1371.

164 Drugi odstavek 148. člena ZKP, 11. člen ZNPPol.

jo podatki, ki posameznika prek njegove lokacije umestijo na kraj kaznivega dejanja ali ga povežejo z lokacijo, ki razkriva njegovo pripadnost, prepričanje, mišljenje ali aktivnosti, oziroma je možno take informacije s selekcioniranjem izločiti iz množice pridobljenega, je po vsebini že dosežen standard, potreben za sprožitev sistema varstva iz 8. člena EKČP. Gre namreč za primer, ko si opazovalec ustvari sliko tistega, kar se posameznik trudi ohraniti kot zasebno ali vsaj upa, da bo zaradi hitrega življenjskega ritma in miselne odsotnosti okolice to uspel ohraniti zase. S tem je podan presežek informacij v smislu, da povprečen opazovalec življenja opazovanega z lastnimi čutili in opazovanji take slike in videnja zadeve ne bi bil zmožen ustvariti.

Za opisano ravnanje, ki je sicer v mejah zakonitega, je treba uporabiti mozaično teorijo in njene učinke. Lokacijski delci, ki se pridobijo z enim posegom v zasebnost in ki ostajajo na meji zakonitega, lahko v primeru združitve v celoto o opazovanem pokažejo jasno sliko, s katero si lahko tisti, ki njeno kreacijo nadzoruje, na podlagi vpogledanih podatkov o osebi izoblikuje mnenje in stališče. Posamezni drobci so lahko sami zase brezpomenski, ko pa se med seboj povežejo, dobijo neprecenljiv vsebinski pomen. In če se v specifičnem primeru na podlagi tako zbranih informacij izoblikuje profil preiskovane osebe, gre za očiten poseg v osebnostne pravice, še zlasti v posameznikovo splošno pravico do zasebnega življenja ter svobodnega gibanja. Menim, da je zato mogoče z uporabo mozaičnega učinka tako zbrane podatke (ki so lahko dokaz) šteti za nezakonite in nezdružljive s posameznikovim pričakovanjem zasebnosti. Tak pristop tudi pripomore pri sodniškem odločanju, saj sodnik kot varuh zakonitosti presodi, ali je s pomočjo tehnologije oziroma ravnanja policije res prišlo do čezmernega posega v lokacijsko zasebnost na način, da je iz lokacijskih podatkov mogoče razbrati intimne vidike posameznikovega življenja. V takem primeru sodnik lahko zaradi prilagodljivosti mozaične teorije zbrane podatke izloči oziroma jih pri svojem odločanju ne upošteva (s čimer dvigne raven zasebnosti) oziroma sprejme sklep, da so take informacije povsem dopustne in sprejemljive z vidika 8. člena EKČP (pridobljene skladno z zakonodajo neke evropske države).

4.3. Ex-ante

Menim, da glede na do zdaj sprejeta stališča v praksi ESČP že obstaja možnost uporabe mozaične teorije. Dejstvo je, da se ob zbiranju lokacijskih podatkov ustvarjajo njihove baze in da se podatki v njih hranijo vse do trenutka, ko postanejo relevantni za tekočo preiskavo ali prestop iz ene v drugo fazo postopka. Hranjenje takih podatkov, ki so bili pridobljeni z zbiranjem posameznih drobcev in brez vednosti osebe, pa lahko pomeni poseg v zasebno življenje te osebe[165] in to celo ne glede na to, ali so bili ti podatki sploh uporabljeni za potrebe kazenskega pregona ali ne.[166]

[165] Leander v. Sweden, Eur. Ct. H. R., 26. marec 1987, tč. 48; in Amann v. Switzerland, Eur. Ct. H. R., 16. februar 2000, tč. 78–80.

[166] Kopp v. Switzerland, Eur. Ct. H. R., 25. marec 1998, tč. 53.

Tudi podatek, ki je javno dostopen in poznan mimoidočim (na primer naše vsakodnevno gibanje), pa ga javne oblasti sistematično shranijo, je predmet varstva 8. člena EKČP,[167] in sicer je tako stališče sprejeto zaradi učinka domin, saj ESČP varuje tudi posameznikovo interakcijo z družbo in izgradnjo njegove osebne integritete,[168] do katere pride prav v socialnem okolju, ki je v večini primerov javno in v katerega je posameznik aktivno vpet. Lokacijski podatki pa so že po svoji naravi javni in, kot je že bilo pojasnjeno, lahko iz njih razberemo večjo količino informacij, predvsem o tem, kakšne so posameznikove aktivnosti v družbi in zaradi nje.

ESČP je problematiko lokacijskih podatkov že obravnavalo,[169] vendar je pravkar predstavljeni primer obravnavalo predvsem v luči jasnosti in predvidljivosti zakonodaje, pri čemer kršitve 8. člena EKČP iz tega razloga ni spoznalo. Je pa v tej zadevi vzpostavilo vsebinske kriterije, na podlagi katerih je dejansko uporabilo načelo mozaične teorije oziroma s tem vsaj vzpostavilo za njen obstoj potrebne kriterije. Upoštevalo je namreč dejstvo zavestne izpostavitve javnosti,[170] sistematičnega zbiranja in hranjenja podatkov[171] ter vprašanje, ali nekdo sploh lahko pričakuje tak obseg o njem zbranih podatkov.[172] Poleg tega je iz časa in metode ter vsebine zbranih podatkov tudi presodilo, da je bil poseg v lokacijsko zasebnost v demokratični družbi potreben.[173] Zato bi lahko sklenili, da so kriteriji, ki jih je ESČP uporabilo pri svoji presoji, vsebinsko enaki tistim, ki se kot predlagani pojavljajo v zvezi z mozaično teorijo, in sicer so to: javna izpostavitev lokacije, čas preiskovanja, metodika opazovanja (s pomočjo policijske enote ali pa tehnologije[174]), vsebina tako pridobljenih podatkov, sistematičnost beleženja ter obseg zbranih podatkov.[175]

Na tem mestu je postalo že očitno, da prikrito opazovanje in sledenje gibanju osebe lahko pomeni poseg v njeno zasebno življenje,[176] če nista upravičena oziroma potrebna

---

167 Rotaru v. Romania, Eur. Ct. H. R., 4. maj 2000, tč. 43–44. V tej zadevi ESČP med drugim že navaja, da tudi delci javnih informacij (kazenska evidenca, študije posameznika in njegove politične aktivnosti) uživajo varstvo 8. člena EKČP.

168 Niemietz v. Germany, Eur. Ct. H. R., 16. december 1992, tč. 29; in Botta v. Italy, Eur. Ct. H. R., 24. februar 1998, tč. 32.

169 Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 49–52.

170 Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 44.

171 Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 46.

172 Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 48.

173 Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 80.

174 Česar ESČP zaradi narave pridobljenih podatkov sploh ne ločuje – Herbecq and the Association »Ligue des droits de l'homme« v. Belgium, Eur. Ct. H. R., 14. januar 1998.

175 Iz podatkov je namreč mogoče ugotoviti, ali je šlo za t. i. totalen nadzor ali le za bežno interakcijo s posameznikom, kar nam omogoča presojo, ali je do posega v zasebnost sploh prišlo.

176 Shimovolos v. Russia, Eur. Ct. H. R., 28. november 2011, tč. 66., podobna problematika pa se pojavlja tudi v čakajoči zadevi Big Brother Watch and others v. The United Kingdom, Eur. Ct. H. R., 4. september 2013.

v demokratični družbi,[177] kar je treba ocenjevati z zgoraj navedenimi kriteriji.[178] Zaradi preverjanja primernosti in zakonitosti posega mora imeti prizadeta oseba na voljo ustrezna in učinkovita pravna sredstva, s katerimi se bo zaščitila pred arbitrarnimi posegi v njeno zasebnost.[179] In ker v predstavljenih primerih[180] pravnih sredstev zoper zbiranje in hrambo podatkov ni vse do začetka morebitnega kazensko-preiskovalnega postopka, niti niso taka sredstva učinkovita v slednjem predvsem zaradi časovne odmaknjenosti, nezmožnosti zapomniti si vsak svoj korak ter delcev, zbranih s pomočjo enkratnih posegov, ki so vsak zase sicer zakoniti, je uporaba mozaične teorije neizogibna. Le z njo bo namreč mogoče ugoditi vzpostavljenemu standardu učinkovitega pravnega varstva, ki bo v tem, da bo sodnik ob presoji, ali je prišlo do posega v zasebnost, ocenjeval tako kvantiteto kot tudi kvaliteto zbranih podatkov, ki so bili sicer pridobljeni »nedolžno«, v celoti pa tvorijo krivdno sliko preiskovane osebe.

V kontekstu take presoje pa ne bodo varovani le lokacijski podatki, s katerimi se lahko dokopljemo do zasebnega, temveč tudi drugi, občutljivejši podatki o posameznikovi zasebnosti, ki se lahko pridobijo s pomočjo napredne informacijske tehnologije (na primer posnetki pogovorov, video zapisi, testimonialne izjave ipd.). ESČP namreč poseg v zasebnost z napravo GPS šteje za manj invaziven[181] in mu zato daje tudi manj varnosti, čeprav ne bi smelo biti tako, na kar opozarja mozaični pristop reševanja problematike poseganja v posameznikovo zasebnost. O tem je navsezadnje mogoče sklepati z argumentom *a minori ad maius*, saj če pravne posledice mozaične teorije nosijo že izključno lokacijski podatki, bodo morali njene učinke trpeti tudi preostali podatki, ki so z lokacijo eksistencialno povezani, o posamezniku tvorijo osebnostno podobo in jih je mogoče vse pridobiti hkrati s pomočjo moderne tehnologije.

5. Sklep

Pravna varnost lokacijske zasebnosti je v evropskem pravnem prostoru tako rekoč odvisna od veljavne zakonodaje, njene jasnosti in transparentnosti ter okoliščin vsakega posameznega primera. Tak pravni položaj pa posamezniku vedno ne zagotavlja potrebnega pravnega varstva, ki ga zaradi uporabe tehnologije ta nujno potrebuje. Problem se kaže

[177] Drugi odstavek 8. člena EKČP.

[178] The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Eur. Ct. H. R., 30. januar 2008, tč. 77.

[179] Weber and Saravia v. Germany, Eur. Ct. H. R., 29. junij 2006, tč. 94; in Liberty and others v. The United Kingdom, Eur. Ct. H. R., 1. oktober 2008, tč. 62.

[180] Glej razdelek 4.2 tega dela.

[181] Uzun v. Germany, Eur. Ct. H. R., 2. december 2010, tč. 52, o tem tudi Tratnik, Sledenje z GPS-om »blažji« poseg v zasebnost (2010), str. 25–26.

tudi v nevednosti uporabnikov tehnologije, ki jo sicer sprejemajo kot nekaj pozitivnega, njen izplen pa je lahko negativen.

Zato je treba za varstvo zasebnosti gibanja na prvem mestu poskrbeti pri nas samih, s spremembo miselne paradigme. Tehnologije namreč ne smemo vedno dojemati kot naše prijateljice, saj zaradi nje, vsaj mislim tako, zanemarjamo temeljne človeške odnose in se nagibamo v družbeno osamo. Posledično slabimo v medsebojnih interakcijah,[182] kar skušamo popraviti z deljenjem podatkov prek tehnoloških naprav, katerih delovanje, splošno gledano, ne razumemo najbolje. Ker boj proti sistemu karikirano pomeni »boj z mlini na veter«, se moramo posamezniki takemu boju prilagoditi, kar bomo dosegli predvsem z razumevanjem vseh tveganj na področju zasebnosti, ki jih prinaša nova tehnologija. Videti je namreč, da bo ta čedalje bolj v uporabi, saj je stroškovno učinkovita in v smislu pridobivanja objektivnih informacij zelo zanesljiva. Kljub temu tehnologija ne zmore nadomestiti tistega, kar je človeški rasi unikatno – svobodnega mišljenja in naših ravnanj skladno s čustvi in motivi. Zaradi trenutne nezmožnosti povezovanja lokacije in namena človeškega ravnanja na njej tehnologiji še ni mogoče zaupati in ji predajati usode naših življenj, saj to lahko pripelje do apercepcije doživljanja resničnosti, kar lahko vodi v zelo zmotno sklepanje. Silogistično izoblikovanje sklepanja o dejanskem stanju dogodka moramo zato prepustiti človeškemu umu (na primer sodečemu sodniku), ki bo sprva presodil, ali sta bila oba elementa subjektivne vezi[183] v okoliščinah konkretnega primera izkazana, za tem pa bo ocenil, ali se je prek zbranih lokacijskih podatkov *de facto* poseglo v zasebno sfero opazovanega. Ko pa bo človeška miselnost vsaj na ravni povprečno razumnega posameznika sposobna dojeti pasti uporabe take tehnologije, bo mogoče narediti naslednji korak, da se bo lahko posameznik navkljub težkemu boju zoper sistem pred posegi v svojo zasebnost ustrezno zavaroval sam, prav z uporabo take tehnologije, ki v nasprotju s posegi dobro podkovanemu uporabniku omogoča tudi močno varstvo.[184]

Do tedaj nam na bojnih poljih varstva lokacijske zasebnosti preostane le mozaična teorija, ki s svojim učinkom ob dokončanju sestavljanja mozaika izniči vsakršen poseg, ki je pripomogel k dokončanju mozaika s pridobitvijo manjkajočega koščka. Z njenim retroaktivnim učinkom se bo stopilo na prste vsem, ki bodo poseg v osebnostne pravice posameznika opravičevali z enkratnimi vpogledi v posameznikovo zasebnost v okviru legalnega, s katerimi so se pridobili ključni podatki o profilu opazovane ali nadzirane osebe, na tej podlagi pa se je ustvarila slika o zasebnem življenju posameznika. Menim, da se kljub pomanjkljivostim tehtnica pravičnosti še vedno nagiba v korist tej teoriji, saj je zelo prilagodljiva in nadgrajuje do zdaj ustaljeni koncept pričakovane zasebnosti.

[182] To je temelj varstva zasebnosti po mnenju ESČP.

[183] To pomeni, dDa se je s pomočjo elektronske naprave dejansko pridobila lokacija opazovane osebe ter da je bil pridobljen lokacijski podatek skladen z motivom opazovanega posameznika glede obiska lokacije.

[184] Tehnologija kot jin in jang.

Družba namreč popolnoma upravičeno pričakuje, da se kljub gibanju v javnem prostoru lokacija v običajnih okoliščinah sistematično ne beleži in shranjuje za nadaljnjo uporabo. Menim, da lahko uporabo te teorije priporočimo sodnikom in ne zakonodajalcu. Slednji tehnološkemu razvoju preprosto ni sposoben slediti in je pravo, ki ga ustvarja, togo in neprilagodljivo. Sodnik kot varuh zakonitosti bi lahko z mozaičnim pristopom hitro spoznal, ali je glede na okoliščine konkretnega primera treba nameniti varstvo zasebnosti zaradi neprimerne uporabe informacijske tehnologije.

Pri ohranjanju naše zasebnosti nam lahko pomagajo tudi sodno izoblikovani pravni standardi, ki temeljijo na presoji specifik dogodka. Vendar pa je treba kljub tem unikatnostim poudariti, da je bistvo zaščite zasebnosti posameznik in njegovi odnosi v družbi. Na tem temelji tudi demokratična ureditev, ki jo lahko izvaja le ljudstvo z večinskim konsenzom – torej z vzdrževanjem medsebojnih razmerij, ki se jih zaradi uporabe tehnologije vse bolj zanemarja, kar lahko na koncu pripelje do rušenja temeljev demokracije. Taki asocialni odnosi bodo nedvomno vplivali na zasebnost, saj se jih v družbi ne bo več štelo kot običajne, posledično pa njihovo varstvo ne bo več potrebno, s čimer bo propadel tudi predstavljeni koncept mozaične teorije. Družba bo zato nepretrgoma izpostavljena dvomu nadzora, ki ga preprečujemo prav z varovanjem tistega, kar štejemo za zasebno. To stanje pa lahko slabo vpliva na družbeno blaginjo in svobodo gibanja, ki je že od nekdaj ena od osnov življenja. Zato ne pustimo tehnologiji, da prikrito vstopi v naša življenja in poseže v našo zasebnost, temveč jo kot njeni inženirji nadzorujmo in omejujmo, za vzdrževanje človeških odnosov pa je ne uporabljajmo, temveč ohranjajmo stike v stvarnosti, ki vsebujejo čustva in omogočajo človeško mišljenje, česar pa tehnologija ne premore.

Literatura

Android IMSI-Catcher Detector, URL: https://secupwn.github.io/Android-IMSI-Catcher-Detector/ (18. 10. 2015).

Bedi, Monu: The curious case of cell phone location data: Fourth Amendment doctrine mash-up, v: Northwestern University Law Review, 11 (2015-2016), str. 507–524.

Bedi, Monu: Social Networks, Government Surveillance and the Fourth Amendment Mosaic Theory, v: Boston University Law Review, 94 (2014), str. 1809–1880.

Bernstein, Henry: The Need for Fourth Amendment Protection from Government use of Cell Site Simulators, v: Santa Clara Law Review, 56 (2016), str. 177–206.

Bertagna, Patrick: How does a GPS tracking system work? URL: http://www.eetimes.com/document.asp?doc_id=1278363 (18. 10. 2015).

Blumberg, Andrew; Eckersley, Peter: On Location Privacy and How to Avoid Losing it Forever, v: Electronic Frontier Foundation (eff.org), avgust 2009, str. 1–7.

BrickHouse Security: How does GPS tracking work, URL: http://www.brickhousesecurity.com/category/gps+tracking/how+does+gps+tracking+work.do (18. 10. 2015).

Dickman, Bethany: Untying Knotts: The application of Mosaic Theory to GPS surveillance in United States v. Maynard, v: American University Law Review, 60 (2011), str. 731–743.

Dumpert, Dwight: Night vision for law enforcement & national security, v: Intersec: The Journal of International Security, Vol. 12, no. 3 (marec 2002), str. 75–77.

Estimote: What are Broadcasting Power, RSSI and other characteristics of beacon's signal? URL: https://community.estimote.com/hc/en-us/articles/201636913-What-are-Broadcasting-Power-RSSI-and-other-characteristics-of-beacon-s-signal- (18. 10. 2015).

Facebook Inc.: Facebook and Location, URL: https://www.facebook.com/help/337244676357509/ (24. 10. 2015).

Fallows, James: Technology is our friend…except when it isn't, URL: http://www.theatlantic.com/technology/archive/2011/08/technology-is-our-friend-except-when-it-isnt/244233/ (18. 10. 2015).

Ford, Madelaine Virginia: Mosaic Theory and the Fourth Amendment: How Jones Can Save Privacy in the Fact of Evolving Technology, v: American University Journal of Gender Social Policy and Law, 19 (2011), str. 1351–1372.

Gatewood, Jace: District of Columbia Jones and the Mosaic Theory – In Search of a Public Right of Privacy: The Equilibrium Effect of the Mosaic Theory, v: Nebraska Law Review, 92 (2014), str. 504–536.

Goetz, David: Locating Location Privacy, v: Berkeley Technology Law Journal, 26 (2011), str. 823–857.

Google Inc.: Upravljanje zgodovine lokacij, URL: https://support.google.com/gmm/answer/3118687?hl=sl (18. 10. 2015).

Gorkič, Primož: Sodobni prikriti preiskovalni ukrepi, prvič: lovilec IMSI, v: Odvetnik, Revija Odvetniške zbornice Slovenije, leto XVI, št. 2 (65) – april 2014, str. 47–53.

Gray, David; Citron Keats, Danielle: A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, v: North Carolina Journal of Law and Technology, 14 (2012-2013), str. 381–430.

Kalis, Michael: Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance, v: Pittsburgh Journal of Technology Law and Policy, 13 (2012-2013), str. 1–18.

Kaspersky Lab: What is a Trojan Virus? – Definition, URL: http://usa.kaspersky.com/internet-security-center/threats/trojan (18. 10. 2015).

Kerr, Orin: An Equilibrium-Adjustment Theory of the Fourth Amendment, v: Harvard Law Review, 125 (2011), str. 476–543.

Kerr, Orin: The Mosaic Theory of the Fourth Amendment, v: Michigan Law Review, 111 (2012-2013), str. 311–354.

Kilkelly, Ursula: The right to respect for private and family life, Human rights handbooks, No. 1, Council of Europe, Strasbourg 2003.

Križnar, Primož: Uporaba tehnologij nadzora skozi novejšo slovensko sodno prakso, magistrsko delo, Pravna fakulteta Univerze v Ljubljani, Ljubljana 2015, str. 1–117.

Landoni, Boris: How to find the location with GSM cells, URL: http://www.open-electronics.org/how-to-find-the-location-with-gsm-cells/ (18. 10. 2015).

Michael, Katina; Clarke, Roger: Location privacy under dire threat as 'uberveillance' stalks the streets, v: Precedent 2012, 108 (N/A), str. 24–29.

MIO: Kaj je trilateracija, URL: http://eu.mio.com/sl_sl/z-razlago-gps_kaj-je-trilateracija.htm (18. 10. 2015).

Mnenje št. 13/2011 o geolokacijskih storitvah na pametnih prenosnih napravah Delovne skupine za varstvo podatkov iz člena 29. Direktive 94/46/ES z dne 16. 5. 2011.

MNZ Policija: Delo in oprema, URL: http://www.policija.si/index.php/policijske-uprave/pu-koper/enote/630 (18. 10. 2015).

My Phone Locater: Tracking GSM phone, URL: http://myphonelocater.com/2014/01/18/tracking-gsm-phone/ (18. 10. 2015).

Norris, Clive; McCahill, Mike; Wood, David: Editorial. The Growth of CCTV, 2(2/3), URL: http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3369/3332 (18. 10. 2015).

Oliver, Nancy: Location, Location, Location: balancing Crime Fighting Needs and Privacy Rights, v: University of Baltimore Law Review, 42 (2013), str. 485–512.

Ostrander, Benjamin: The Mosaic Theory and Fourth Amendment Law, v: Notre dame Law Review, 86 (2011), str. 1733–1766.

Quora: What is the difference between ICCID, IMSI and IMEI numbers? URL: https://www.quora.com/What-is-the-difference-between-ICCID-IMSI-and-IMEI-numbers (18. 10. 2015).

Selinšek, Liljana: Razumno pričakovanje zasebnosti v dobi velikih podatkov, v: Zbornik 1. Dnevov prava zasebnosti in svobode izražanja (ur. N. Pirc Musar, A. Zalar), GV Založba, Ljubljana 2015, str. 113–125.

Septier Communication: Septier IMSI catcher, URL: http://www.septier.com/146.html (18. 10. 2015).

Severs, Jon: Dark visions, v: Intersec: The Journal of International Security, 17 (2007) 10, str. 20–22.

Shah, Darshan; Shah, Kavish: Basic of Wi-Fi based positioning system, URL: http://www.researchgate.net/profile/Darshan_Shah/publication/232729025_Basic_of_Wi-Fi_based_positioning_system/links/0fcfd509529419d523000000.pdf (18. 10. 2015).

Sloan, Robert; Warner, Richard: The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State, v: Minnesota Journal of Law Science & Technology, 17 (2016), str. 347–408.

Telekom Slovenije: Statični ali dinamični IP-naslov, URL: http://www.telekom.si/pomoc-in-podpora/teme-pomoci/internet/internet-siol/staticni-ali-dinamicni-ip-naslov (18. 10. 2015).

Teršek, Andraž: Svoboda medijev in varstvo zasebnosti: kritika dveh precedensov, predlog razvrstitve »javnih oseb« in predlog ustavnopravnih standardov, v: Zbornik inštituta za primerjalno pravo pri pravni fakulteti v Ljubljani (ur. M. Seliškar Toš), Inštitut za primerjalno pravo pri Pravni fakulteti, Ljubljana 2006, str. 111–134.

Tomšič, Andrej: Lokacijska zasebnost – naslednje bojno polje varstva zasebnosti, v: Pravna praksa, 30 (2011) 39/40, str. 14–16.

Tomšič, Andrej: Smo dovolj pametni za pametne naprave, v: Zbornik 1. Dnevov prava zasebnosti in svobode izražanja (ur. N. Pirc Musar, A. Zalar), GV Založba, Ljubljana 2015, str. 129–133.

Tratnik, Andreja: Sledenje z GPS-om »blažji« poseg v zasebnost, v: Pravna praksa, 29 (2010) 37, str. 25–26.

Tsai, Janice; Kelley, Patrick Gage; Cranor, Lorrie Faith in Sadeh, Norman: Location-Sharing Technologies: Privacy Risks and Controls, v: A Journal of Law and Policy for the Information Society, 6 (2010), str. 119–151.

U.S. Government: GPS Accuracy, URL: http://www.gps.gov/systems/gps/performance/accuracy/ (18. 10. 2015).

Van Loenen, Bastiaan: Location privacy and national security: contradiction in terminus? URL: http://www.gsdi.org/gsdiconf/gsdi12/papers/92.pdf (17. 10. 2015).

Walker, Shaun; Grytsenko, Oksana: Text messages warn Ukraine protesters they are participants in mass riot, URL: http://www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot (18. 10. 2015).

Wagner, Stephen: Stopping Police in Their Tracks: Protecting Cellular Location Information Privacy in the Twenty-First Century, v: Duke Law & Technology Review, 12 (2014), str. 200–218.

Ziegler, Chris: 2G, 3G, 4G, and everything in between: an Engadget wireless primer, URL: http://www.engadget.com/2011/01/17/2g-3g-4g-and-everything-in-between-an-engadget-wireless-prim/ (18. 10. 2015).

Protection of The Locational Privacy Using Mosaic Theory of Data
(Summary)

An individual's movement is a basic element of human life. It is without a doubt perceptible to public that is why we could expect, that our movements just cannot be kept private. But I believe that this is not the case because of our modern and fast lifestyle, for which we expect our movements to be visible in public, but they will not be systematically recorded. That is the main reason we can reasonably expect privacy on our movements in public places which are, due to integration into society and social sphere surrounding area, never completely random. So the definition of this so called locational privacy is the expectation that our locations are not systematically recorded and stored for future use in normal circumstances.

On the other hand, we have the individual's right to privacy, which is one of the fundamental human rights. Its use depends on at least 3 factors, which are individual subjective belief of what is private to them, interventions, which someone has to suffer due to their social status or position and common knowledge about managing technological devices.

When we breach someone's privacy, we can get acquainted with a wide array of information taken directly from private sphere of individual's life. The sum of that information is called totality of information (TOI), through which we can learn where someone is, why he is there and in what kind of psychophysical condition that person is. We can see that this type of data is unique to specific individual and can be gathered through the use of modern technology from which we learned »only« locational data. But most of the time the use of technology only answers the where question and that can lead to distortion of reality and the so called absence of subjective ties. With this kind of observation we neglect why someone is there and in what kind of condition he is there and this is a problem, commonly known to society.

The individuals are worried about the question who can access the location and they also express concern and fear before stalking and invasion of privacy through the use of modern technology. Their concern is justified, especially after the events in Ukraine where people on a specific area, regardless of their intentions, received text-messages, that they are participants in mass riots. But the technology can also be useful as can be seen from Facebook Security Checks after the latest Paris terrorist attacks.

Monitoring of the situation, movement and activities of individuals is possible by using technical devices to detect the position and movement. The most common techniques are tracking GPS transmitter in smart phones with the process of trilateration, tracking smart phone signal through GSM network with the process of triangulation, man-in-the-middle attack with the help of IMSI catcher, checking if the electronic device was connected to a specific WiFi hotspot or if it used an IP address for its commu-

nication, usage of thermovision device, observing persons through CCTVs with build-in face recognition systems and following someone's locations with the help of his social networks posts.

One of the theoretical approaches in creating a balance between the benefits and risks of prejudice to locational privacy is certainly a theoretical approach based on the model of the mosaic or shorter mosaic theory. According to this theory the relevance of a figure is in dependence on the collected data. One particular piece of data does not mean much to an average observer, however, for the one who is familiar with other data and able to see the whole picture this figure may represent an important content and is fully integrated into viewed context, which the informed person has in front of him. Mosaic theory thus frames the basis for concluding that the various data themselves do not have some dramatic substantive value, but when someone merges this independent data together into a whole, the latter due to the merger can acquire a strong substantive meaning. With the help of technology, which does not just communicate someone's whereabouts, but can indirectly entrust us with political, religious, friendship, love, professional and leisure activities of that particular person, we can get the key information, which is subsequently classified as a cluster of other data. And on such a basis, we can later create an image or insight of that realm which the individual wishes to preserve as private. The point is not just in following the individual's movement but in gathering locational information, which can communicate a lot about someone's life.

What about the concept of a reasonable expectation of privacy? Some say the concept is ill-suited due to the fact that we are living in a digital age. I agree with that opinion, which can be supported by next statements:

1. The society will not always want a complete insight into our whole day errands;
2. The public is not capable of monitoring the whole of our movement but only its part;
3. Individuals simply do not expect consistent and systematical monitoring of their movements;
4. Covered location tracking can be justified with referring to the fact, that movement was public, which is neither justly nor moral;
5. An individual does not have the element of conscious exposure of his location;
6. By each subjection of location an individual exposes a part of his personal integrity and the sum of these particles, according to the mosaic theory does not constitute a zero-sum but can show a complete profile of the individual.

Of course, the theory has some problems, because it is unclear when the profile with which the privacy is ruined is created. It is also hard to recognize the first action which lead to the creation of the mosaic which is important due to the question of legality of this action. We also cannot determine by which actions the information was gathered so the effectiveness of defence in future criminal procedure is lost, and that leads to the fact that this theory passes the burden of proof to the defendant who has to prove that legal

actions against him lead to the creation of mosaic which is according to previous two points nearly impossible. With the theory's effect of exclusion of evidence per fruit of the poisonous tree concept, we cannot determine its range and last but not least, there is a disproportion between higher intrusion into privacy which sometimes is not sanctioned (for example garbage search) and lesser intrusion (like GPS tracking) which can become illegal according to this theory. Despite those facts, I still believe, that this theory is quite persuasive, especially with its equilibrium effect, upon which we can achieve the balance between the technological development and the benefits of criminal procedure. This means, that in cases, where it is found, that the technology has weakened investigative methods, we can lower the level of privacy protection and otherwise – if the technology becomes more intrusive, we will be capable of protecting our privacy by granting it a higher level of protection.

In Europe, protecting privacy is focused mostly on an individual and his personal predispositions, development and social interactions. That is why the locational data is protected under Article 8 of the European Convention on Human Rights (ECHR) and also under Article 2(2) of the Protocol n. 4 to the ECHR which grants everyone the freedom of movement. Location data collection method on the other hand depends on the national legislations of the European countries and from that aspect we must distinct three different situations; a) if there is no such law, which would predict the gathering of such information, this is a direct violation of Article 8 of the ECHR, b) if there is/are such laws, they must be transparent, predictable, clear and accurate in their articles, otherwise there are options of arbitrary practices, ineffective defence and the abuse of technology in unilateral purposes, which all brings us back to the violations of Article 8 of the ECHR and c) both, a) and b) points are considered, but despite that the law enforcement agents bypass guarantees the protection of privacy and gather data, upon which they create a personal profile of the observed individual. There are indeed legal methods, from which we can gather crucial data, but those methods are not object of judicial assessment and they are (at least in most European countries) most common police tasks, for example observing and patrolling the area, gathering information about someone's location from public announcements on social networks, gathering information about individual's movement from eyewitnesses and reviewing CCTV footages of public areas. The last situation (c) can be resolved by using the mosaic theory, which is only a theory, currently not used in the ECtHR case law. However, the arguments for the existence of the theory have already been established in some of the most important cases regarding locational privacy.

Data retention, with or without the purpose of the criminal proceedings, may constitute a violation of the right under Article 8 of the ECHR. Our movements are mostly public, but even public information stored systematically can be subject to the protection under Article 8 of the ECHR in order to protect the integrity of an individual. In

one of the cases regarding locational privacy the ECtHR already established criteria necessary for the existence of the mosaic theory. They are relevant in cases, from which arises the question whether there has been a breach of privacy with legal actions that created a complete profile of individual's life. Those criteria are: public nature of gathered information, the time of observation, methods used in covert actions and questions: were figures collected systematically, what is the volume of the gathered data and what is the collected data content and nature. Of course while assessing the intervention in locational privacy we should check it in the light of the relevance and necessity to achieve the objective in a democratic society, last but not least mosaic theory approach through the use of argumentum *a minori ad maius* also protects other data existentially related to the location, disclose an individual personal appearance and can be obtained all at the same time by using modern technologies to track our location.

There are some legal options available but they are not 100% certain and they depend on specific circumstances of the case. That is why I suggest a change in our mental paradigm by discontinuation of perception of the technology as our ally. Because of it we ignore the fundamental human relationships and lead our lives toward a social isolation. In my opinion, the first solution so far would be in better understanding of all possible risks of modern technology on the locational privacy battlefield rather than the use of mosaic theory in practice.