Zbornik znanstvenih razprav
Letnik 73 (2013) / Volume 73 (2013)
Oktober / October 2013

Spletna stran Zbornika: / Journal website:
http://zbornik.pf.uni-lj.si
http://journal.pf.uni-lj.si

8

UDK 343:621.39

*Dr. Katja Šugman Stubbs**

Nove tehnologije in njihov vpliv na pojavnost in pregon kriminalitete

1. Uvod

Tehnologija in kriminaliteta hodita z roko v roki že celotno zgodovino.[1] Kot je nemogoče ustaviti razvoj tehnologije, je nemogoče podati dokončno sodbo o tem, ali je razvoj tehnologije dober ali slab, oziroma odgovoriti na vprašanje, ali razvoj tehnologije koristi predvsem »kriminalcem« ali, na drugi strani, državi. Kot pravi Byrne, je razvoj tehnologije omogočil nove priložnosti za kriminaliteto, nove oblike kriminalitete, nove tehnike storitve kaznivih dejanj in nove kategorije storilcev in žrtev.[2] Eno pa je gotovo: nobena veja prava si pred novimi tehnološkimi spoznanji ne more zatiskati oči. Razumevanje tega področja zahteva stalno izobraževanje, saj edino tako sploh razumemo, kako lahko tehnologije uporabljajo storilci kaznivih dejanj. Ne smemo pa zanemariti tudi drugega vidika uporabe novih tehnologij: razumeti moramo, kako lahko nova tehnološka spoznanja uporablja država za nadzorovanje ljudi in za preiskovanje kaznivih dejanj. Navsezadnje pa razvoj tehnologije na novo postavlja stara kazenskopravna vprašanja tehtanja med različnimi nameni in cilji kazenskega postopka: kje se konča dovoljena učinkovitost pregona in začne čezmerno poseganje v človekove pravice in kakšna je pri tej presoji vloga sodne veje oblasti, koliko sme kazenskopravni sistem uporabljati tehnološko podprte preventivne metode nadzora in kateri dokazi, pridobljeni z novimi tehnologijami, se smejo uporabiti na sojenju.

* Redna profesorica na Pravni fakulteti Univerze v Ljubljani, katja.sugman@pf.uni-lj.si.

1 Wall, Cybercrime (2007), str. 2–3.

2 Med novimi tipi žrtev lahko recimo navedemo žrtve kraje identitete. Byrne, The Best Laid Plans, v: Federal Probation, 72 (2008), str. 11.

Brez težnje po tem, da bi bila izčrpna, se bom posvetila prikazu in analizi nekaterih problemov, ki jih nove tehnologije postavljajo preiskovanju kriminalitete, problematizirala bom nekatere pravne rešitve, do katerih je privedla uporaba sodobnih tehnologij, in poskušala umestiti ta razmišljanja v kontekst vrednot in načel kazenskega prava.

2. Zasebnost in posegi države

Eden ključnih konceptov, ki državi preprečujejo, da posega v posameznikove pravice, je zasebnost. Zasebnost naj bi zagotovila, da imamo polje, v katero država ne sme in ne more posegati, če ni za to izpolnjenih strogih pogojev. V različnih pravnih sistemih je pravica države, da zvočno oziroma slikovno snema in take posnetke uporabi kot dokaz, urejena na zelo različne načine.[3] V ozadju strahu pred oblastnikovim neupravičenim in prevsiljivim nadzorovanjem v obliki snemanja je klasično tičal strah pred družbo, ki jo je Orwell opisal v svojem romanu 1984. Strah pred t. i. očesom na nebu ali Velikim bratom (*Big Brother*), naj bo ta v obliki države ali zasebnika, je tolikšen, da večina pravnih sistemov natančno ureja možnosti posega v posameznikovo temeljno pravico, da ga »pustijo pri miru«[4] – pravico do zasebnosti.[5] Razlikovati pa moramo med dvema različnima vidikoma poseganja v zasebnost: (1) tem, ki ga izvaja država prek svojih organov pregona in ki navadno poteka v kazenskem postopku,[6] in (2) drugim, ki ga izvajajo zasebniki.

Drugi tip nadzora je danes mnogo bolj razširjen in precejo manj pravno urejen; lahko bi celo trdili, da je mnogo bolj invaziven, vseobsegajoč in nevaren, saj ni podvržen strogim kazenskopravnim testom in varovalkam. Poleg tega ga lahko izvajajo zelo raznoliki subjekti, kar še poslabša preglednost tega področja. Lahko

[3] V ZDA je koncept recimo oblikovan kot razumno pričakovanje zasebnosti. Več o tem glej v Wilkins, Defining the Reasonable Expectation of Privacy, v: Vanderbilt Law Review, 40 (1987), str. 1077–1129. Tako gledanje na zasebnost je bilo kasneje sprejeto tudi v Evropi, (npr. Lüdi proti Švici (Ser. A, no. 238), Halford proti Združenemu kraljestvu (20605/92, 1997, ECHR 32) in v Sloveniji (npr. odločba US RS U-I-25/95, z dne 27. 11. 1997).

[4] Tako je to pravico opredelil sodnik ameriškega Vrhovnega sodišča Brandais v slovitem ločenem odklonilnem mnenju v primeru Olmstead v. US, 277 US 438 (1928).

[5] Nadzorovanje je nadležno, ker se ljudje počutijo neprijetno, če vedo, da so nadzorovani, hkrati pa začnejo spreminjati svoje vedenje; nastopita samocenzura in težnja, da bi se vedli socialno zaželeno. Solove, A Taxonomy of Privacy, v: University of Pennsylvania Law Review, 154 (2006), str. 493–495.

[6] Lahko gre tudi za druge tipe postopkov, ki jih vodi država, recimo carinski postopek.

gre za posege delodajalca,[7] različnih podjetij (recimo trgovin) ali celo samih telekomunikacijskih operaterjev.[8] Opozoriti je treba še na (3) vidik nadzorovanja, ki sicer ne pomeni klasičnega posega v posameznikovo zasebnost, lahko pa se dotika tudi teh vprašanj. Nadzorovani zasebniki imamo namreč številne možnosti, da državo ali druge nadzornike tudi sami nadzorujemo (*sousveillance*);[9] tako nekateri pravijo, da smo se znašli v družbi, ki je vsenadzorovalna (*omniveillance*).[10] Svoje prispeva še možnost hitrega posredovanja takšnih informacij oziroma posnetkov naprej (npr. internet). Če k temu prištejemo še, da ni več jasno, kdo nadzira in kdo je nadziran, ter narcistično-ekshibicionistično nagnjenost sodobne (mladostniške) kulture k temu, da vsakdo z javnostjo deli svoje zasebne misli (blogi), intimne podatke (FormSpring, Asq.fm), posnetke (Youtube, Facebook ipd.), potem se lahko zdi, da smo prešli v družbo, v kateri je zasebnost samo še nepomembna vrednota. Vendar pa boj zanjo še vedno poteka na več frontah; ena od njih je kazenskopravna.

Kljub zanimivosti in obči razsežnosti vseh oblik nadzorovanja bom svoje razpravljanje zaradi kazenskopravnega okvira omejila samo na državo kot nadzornika. Tudi v tem dokaj omejenem okviru obstajata (vsaj) dva različna načina nadzorovanja: (1) ciljno nadzorovanje, pri katerem je nadzorovanje del preiskovanja kaznivega dejanja in se nanaša na določeno osebo ali vsaj na določeno sredstvo,[11] in (2) splošno nadzorovanje, ki je generični, preventivni varnostni ukrep in se lahko nanaša na kogarkoli,[12] ne glede na to, ali je v kazenskem po-

---

7 Miller, Weckert, Privacy, the Workplace and the Internet, v: Journal of Business Ethics, 28 (2000) 3, str. 255–265. S tem v zvezi glej recimo The Employment Practices Data Protection Code, ki ga je izdal angleški informacijski pooblaščenec, URL: https://www.ico.org.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/the_employment_practices_code.ashx (16. 8. 2013).

8 Recimo Facebook. Glej npr. Acquisiti, Gross, Imagined Communities, v: Privacy Enhancing Technologies (2006), str. 36–58; Hodge, Fourth Amendment and Privacy Issues on the New Internet, v: Southern Illinois University Law Journal, 31 (2006), str. 95–123.

9 Glej opis številnih primerov, ko so zasebniki snemali policijsko nasilje, v: Robinson, Bad Footage: Surveillance Laws, v: Georgetown Law Journal, 100 (2011), str. 1399–1435.

10 Blackman, Omniveillance, Google, Privacy in Public, v: Santa Clara Law Review, 49 (2009), str. 313.

11 Takšna so po naši zakonodaji recimo preiskovalna dejanja nadzora elektronskih komunikacij s prisluškovanjem in snemanjem ali s prisluškovanjem in snemanjem pogovorov s privolitvijo vsaj ene osebe, udeležene v pogovoru, iz 150. člena ZKP.

12 V tem pogledu je zanimiv projekt Echelon, ki so ga vlade nekaterih zahodnih držav (npr. Velika Britanija, ZDA) ustanovile z namenom, da bi nadzorovale komunikacijo s takratno Sovjetsko zvezo, kasneje pa se je težišče premaknilo na boj proti terorizmu in celo industrijsko vohunjenje. Program analizira komunikacijo glede na vsebino. Sloan, ECHELON and Legal Restraints on Signals Intelligence, v: Duke Law Journal, 50 (2001) 5, str. 1467–1510, in Lawner,

stopku ali ne.[13] V tem primeru je nadzorovanje usmerjeno na neko neželeno ali prepovedno vsebino (*monitoring, filtering*).[14] S kazenskopravnega vidika je prav gotovo zanimivejša druga vrsta nadzorovanja, ki se je pojavila šele z novimi tehnologijami.[15] Pred kazensko pravo pa ta širša oblika nadzorovanja postavlja številne izzive, ker revolucionarno spreminja nekatere klasične varovalne mehanizme. Poglejmo, kako.

3. Kibernetska kriminaliteta

Verjetno je največji razcvet kriminalitete, ki uporablja nove tehnologije, povezan z razvojem računalnikov in interneta. Tako za zakonodajalce kot za sodno vejo oblasti je učinkovito preganjanje kibernetske kriminalitete trd oreh, krhajo pa se tudi klasični kazenskopravni koncepti. Nekateri avtorji celo trdijo, da bi bilo zaradi velikih razlik med stvarnim in kibernetskim svetom prav za to področje treba izdelati »novo kazensko pravo«.[16]

Najširše lahko kibernetsko kriminaliteto opredelimo kot kazniva dejanja, ki se storijo z uporabo interneta. Pri tem preučevalci tega pojava, ki je danes zelo razširjen, razlikujejo med dvema tipoma tovrstne kriminalitete:[17] (1) dejavnosti, ki so usmerjene na (vdor v) računalnike in informacije, ki jih je mogoče najti v njih,[18] in (2) dejavnosti, pri katerih je računalnik uporabljen kot orodje, s katerim se kazniva dejanja izvršujejo.[19] Začetki kriminalitete, povezane z računalniki, segajo v šestdeseta leta prejšnjega stoletja, prve kriminološke raziskave na tem področju pa so bile narejene v sedemdesetih letih.[20] Konec sedemdesetih je sledil val zakonov, ki so večinoma varovali pravico do zasebnosti, v osemdesetih letih pa so prve države začele sprejemati zakone, ki so bili namenjeni posebej

---

Post-September 11th International Surveillance Activity, v: Pace International Law Review, 14 (2002), str. 4350.

13 Walden, Computer Crimes (2007), str. 215.

14 Lahko gre za povsem transparentne prakse, kot recimo postavljanje požarnih zidov, ki blokirajo neželeno pošto, lahko pa gre za iskanje prepovedanih vsebin na internetu, ki jih išče država (recimo otroška pornografija, varnost države). Prav tam, str. 223–229.

15 Več o tem glej v Kovačič, Nadzor in zasebnost v informacijski družbi (2006), str. 46–48, 143–176.

16 Brenner, Toward a Criminal Law for Cyberspace, v: Boston University Journal of Science and Technology Law, 10 (2004), str. 1–109, in Brenner, Toward A Criminal Law for Cyberspace, Rutgers Computer & Technology Law Journal, 30 (2004), str. 1–104.

17 C. Decker, Cyber Crime 2.0, v: Southern California Law Review, 81 (2008), str. 963.

18 Kot recimo dejavnosti hekerjev, ki se poskušajo dokopati do določenih informacij.

19 Gre lahko za kazniva dejanja goljufije.

20 Sieber, Legal Aspects of Computer-Related Crime in the Information Society (1998).

za zaščito pred kibernetsko kriminaliteto.[21] Temu so sledile še mednarodne in nadnacionalne institucije, recimo OECD,[22] Svet Evrope[23] in EU,[24] ki so bistveno pripomogle k harmonizaciji zakonodaje na tem področju. Vendar pa Goodman in Brennerjeva duhovito ugotavljata: »Čeprav je v to področje vložen velik trud, je globalna kibernetska zakonodaja še vedno krpanka novih zakonov, starih zakonov in nobenih zakonov.«[25]

Prav kibernetsko področje je za pravno urejanje še posebej težavno, saj ima značilnosti, ki se klasičnemu pravnemu urejanju izmuznejo: (1) klasično kazensko pravo je izrazito nacionalne narave, kibernetska kriminaliteta pa praviloma čezmejna;[26] (2) zakonodaja zaostaja za hitrim razvojem novih oblik te kriminalitete;[27] (3) klasični pravni koncepti so zasnovani na realnosti fizičnega sveta in ne za kibernetski svet, kar je morda najbolj vidno pri (4) dokazih, ki so v kibernetskem svetu neotipljivi podatki minljive narave (*transient nature*);[28] (5) v kibernetskem svetu se z majhnimi sredstvi in majhnim človeškim potencialom lahko povzroči velika škoda; (6) obseg te kriminalitete je neprimerno večji kot pri klasični kriminaliteti; (7) dejanje se lahko z enega računalnika izvrši po vsem svetu, kar povzroča težave z identifikacijo žrtev in jurisdikcijo; (8) med storilcem in žrtvijo ni fizičnega stika, pogosta pa je tudi popolna anonimnost vsaj ene

---

21 Goodman, Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, v: UCLA Journal of Law & Technology, 3 (2002), str. 14–15.

22 Npr. OECD Guideliness for the security of information systems (1992), leta 2002 nadomeščeni z novo različico.

23 Council of Europe Recommendation No. R (89) on computer-related crime (1990) in kasneje Council of Europe Recommendation No. R (95) 13 concerning problems of criminal procedural law connected with information technology (1995), Konvencija o kibernetski kriminaliteti (ETS 185, 2001). Več o slednji glej pri Selinšek, Odzivi slovenskega kazenskega prava na kibernetski kriminal, v: Pravna praksa, 28 (2005) 5, str. 19.

24 Okvirni sklep Sveta 2005/222/PNZ z dne 24. 2. 2005 o napadih na informacijske sisteme, predlog Direktive Evropskega parlamenta in sveta o napadih na informacijske sisteme in razveljavitev Okvirnega sklepa Sveta 2005/222/PNZ. Najnovejša ideja EU na tem področju je predlagana ustanovitev Evropskega centra za boj proti kibernetski kriminaliteti in zaščito e-potrošnikov.

25 Goodman, Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, v: UCLA Journal of Law & Technology, 3 (2002), str. 22.

26 To je tudi eden temeljnih razlogov, zakaj Brennerjeva predlaga novo kazensko pravo prav za kibernetsko kriminaliteto. Glej op. 16.

27 Goodman in Brennerjeva opisujeta nekaj primerov, ko klasično pravo preprosto ni poznalo kaznivega dejanja, pod katero bi lahko uvrstili neko zelo škodljivo delovanje. Tak je bil računalniški virus LoveBug, v drugem primeru pa je neki trinajstletnik z računalniškimi sredstvi zablokiral vse komunikacijske kanale računalniškega podjetja in ga tako uničil. Pri tem ga niso mogli preganjati ne za poškodovanje tuje stvari, ne za tatvino, ne za vlom, ne za izsiljevanje. Prav tam, str. 4–5, 18–20.

28 Kerr, Law in a Networked World, v: University of Chicago Legal Forum (2008), str. 415–430.

od strani;[29] (9) specifične so tudi metode zasega teh podatkov, ki so pogosto predmet napada obrambe po izločitvi dokazov.[30] Preučevalci pravnih vidikov tega fenomena pojava omenjajo predvsem tri polja, ki so težavna za učinkovito pravno preganjanje: (1) jurisdikcija, (2) tehnike prikrivanja in (3) poročanje.[31] Poglejmo si podrobneje nekatere od težav, s katerimi se organi pregona srečujejo pri preiskovanju kibernetske kriminalitete.

3.1. Težave z identifikacijo in prijetjem storilca

Če pri klasični kriminaliteti obstaja neki praviloma fizični stik med storilcem in žrtvijo ali pa vsaj pripadata neki širši skupnosti, tega za kibernetski svet nikakor ne moremo trditi. Zato je tudi klasično policijsko delo (recimo zaslišanje prič, ogled kraja kaznivega dejanja) pri tej kriminaliteti popolnoma neuporabno. Preučevalci kibernetskega prostora pravijo, da se v teh primerih vedno najprej pojavi problem ugotavljanja identitete: kako lahko najdemo povezavo med podatki in virtualno identiteto storilca ter nato v drugem koraku povezavo med virtualno identiteto in fizično osebo.[32] V postopku identifikacije navadno iščejo dve vrsti sledi, ki naj bi pomagale izslediti storilca: (a) sledi, ki jih povzroča osumljenčeva uporaba računalnika (ali drugega podobnega komunikacijskega sredstva), in (b) vsebino komunikacije. V prvem primeru preiskovalci iščejo izvor in naslovnika komunikacije prek edinstvenega identifikacijskega sredstva (terminal, IP-naslov ipd). Zaplete se, kadar gre za računalnik, ki ga uporablja več ljudi, in takrat je identifikacija pravega storilca težavna. V drugem primeru pa preiskovalci sledijo vsebinam, ki jih je osumljenec zavestno ali nezavedno razkril pri uporabi računalnika.[33]

Tudi če organom pregona uspe najti storilca kaznivega dejanja, ga je pogosto zelo težko prijeti in izročiti. Pogosto imajo storilci tovrstne kriminalitete lažne identitete, kar otežuje identifikacijo. Praviloma je skorajda nemogoče odkriti pravi kraj storitve, saj uporabljajo internetne povezave, ki potekajo skozi več držav, prek različnih omrežij ipd. Pri prijetju storilca so ključni tudi jurisdikcijski razlogi; storilec lahko deluje v državi, s katero druge države slabo sodelujejo ali ki nima zakonodaje, primerne za učinkovit pregon kibernetskega kriminala, ipd. Pogosto si storilci ravno zaradi takih razlogov izbirajo t. i. varne države.

[29] Brenner, The Privacy Privilege, v: Journal of Technology Law & Policy, 7 (2002), str. 136–150.
[30] Walden, Computer Crimes (2007), str. 205–206.
[31] Herrera Flanigan, Ghosh, Criminal Regulations, v: Cybercrimes (2010), str. 286.
[32] Walden, Computer Crimes (2007), str. 206.
[33] Gre recimo za t. i. piškote ali uporabo kreditne kartice. Proces odkrivanja teh forenzičnih sledi je zelo dolg in težaven. Povzeto po Walden, Computer Crimes (2007), str. 209–211.

3.2. Sledovi in dokazi

Zasegi so se klasično nanašali na fizične dokaze, na tehniki iskanja fizičnih sledov pa so temeljile tudi klasične preiskovalne tehnike, na primer ogled kraja kaznivega dejanja, telesni pregled žrtve in podobno.[34] Izhodišče klasične kriminalistične tehnike in kazenskopravne doktrine je namreč predpostavka, da sta bila žrtev in storilec v fizičnem stiku.[35] V kibernetskem svetu pa je vse drugače: storilec in žrtev najpogosteje nimata fizičnega stika, oba imata lahko lažno identiteto, obstajajo samo računalniški sledovi, ki jih je treba iskati po več državah, ipd. Zato je preiskovanje te vrste kriminalitete bistveno težje in od preiskovalcev zahteva stalno izpopolnjevanje in dopolnjevanje znanja ter obvezno sodelovanje z računalniškimi strokovnjaki. Podatki, do katerih preiskovalci pridejo, so navadno tako obsežni, da morajo imeti posebno znanje in tehnologijo, da jih sploh lahko pregledajo in iz njih izluščijo pravno relevantne.[36] Kot pravi Walden, imajo kibernetski podatki še dve neprijetni značilnosti: so zelo hitro spremenljivi in hkrati zelo lepljivi. To pomeni, da lahko ob tem, ko se dela kopija zaseženega trdega diska, zelo hitro pride do sprememb teh podatkov (*integrity problem*). Prav to dejstvo bo storilčeva obramba lahko uporabila v svoj prid in trdila, da so bili podatki med preiskavo spremenjeni.[37] Po drugi strani pa so ti podatki izredno trdovratni oziroma lepljivi (*stickiness problem*): tako rekoč nemogoče jih je na primer odstraniti z interneta, ker se v trenutku ustvarijo številne kopije.[38]

Obstajata vsaj dva različna tipa računalniških podatkov, ki jih lahko pridobijo računalniški forenziki: (1) podatki, ki so shranjeni na nekem nosilcu podatkov v digitalnem zapisu (*data at rest*), in (2) podatki, ki se prenašajo z enega nosilca podatkov na drugega, recimo po internetu t. i. tranzitni podatki (*data in motion, data in transmission, data in transit*). Pri tem se shranjeni podatki pridobivajo z zasegom, medtem ko se podatki, ki so v prenosu, pridobivajo z drugimi metodami, na primer s prisluškovanjem oziroma nadzorovanjem strežnika ipd. Proces pridobivanja digitalnih podatkov je navadno sestavljen iz štirih faz: (a) najprej je treba ugotoviti, kakšni podatki so na voljo in kje bi jih lahko našli; (b) te podatke je treba shraniti oziroma ohraniti na tak način, da se vanje minimal-

---

[34] Kerr, Digital Evidence and the New Criminal Procedure, v: Columbia Law Review, 105 (2005), str. 279–318.

[35] Brenner, Cybercrime Metrics, v: Virginia Journal of Law and Technology, 9 (2004) 13, str. 6.

[36] Barrett opisuje iskanje relevantnega podatka na enem računalniku kot iskanje šivanke v senu. Barrett, Traces of Guilt (2004), str. 14.

[37] Walden, Computer Crimes (2007), str. 205–207.

[38] Prav tam.

no posega;[39] sledita (c) analiza podatkov z namenom pridobiti veljavne dokaze in (d) uporaba zaseženih podatkov kot dokaza pred sodiščem.[40]

Kakšna je torej uporabnost klasičnih konceptov preiskave in zasega v virtualnem svetu? Prvo, kar lahko ugotovimo, je, da je logiko fizične hišne preiskave težko prenašati iz realnega sveta v kibernetskega. Kot dokazuje Brennerjeva, ima kibernetski svet nekaj podobnosti z realnim svetom, vendar pa se vseeno v bistvenih lastnostih razlikujeta.[41] Če vzamemo za primer odredbo za hišno preiskavo, potem je jasno, da mora ta natančno določiti lokacijo te preiskave.[42] Določenost kraja ima več namenov: s tem, ko je določeno, kam policist sme iti, je določeno tudi, kaj bo lahko tam videl, slišal ipd.[43] Določitev točke vstopa je določitev meje med zasebnim in javnim. V kibernetskem svetu ta logika ne velja. Ko odredba recimo določi, da se neki računalnik sme nadzirati, se odpre mnogo širši svet; tako rekoč nemogoče je nadzorovati, kaj se bo tam odkrilo. Prav tako ne moremo nadzorovati filtrov, ki se uporabljajo pri iskanju. Določitev točke vstopa nikakor ne zareže več meje med zasebnim in javnim, temveč postaja samo še predpostavka za pridobivanje dokazov.[44] Še večji problem se pojavlja pri prestrezanju tranzitnih podatkov.[45] Na internetu je tudi tako rekoč nemogoče razlikovati med javnim in zasebnim – noben iskalni filter ne more razlikovati med tema dvema pojmoma in tako je obseg preiskovanja po definiciji mnogo širši, odredba pa pri tem ne more več odigrati omejevalne vloge.

Podobno odpove primerjava med klasičnimi hišnimi preiskavami in zasegi realnih predmetov ter zasegom in preiskavo računalnika. V klasični hišni preiskavi mora biti v odredbi navedeno, kaj se lahko zaseže. Vse drugo se lahko zaseže po eni od izjem.[46] Fizični svet sam postavlja omejitve, kaj se lahko preišče in zaseže:

---

39 Pri tem se navadno izdela natančna kopija nosilca digitalnih podatkov (*imaging*). Prav tam, str. 213.

40 Povzeto po Walden, Computer Crimes (2007), str. 211–212.

41 Brenner, The Privacy Privilege, v: Journal of Technology Law & Policy, 7 (2002), str. 160.

42 Do kakšnih problemov in neutemeljenih nadlegovanj lahko pride pri določitvi prostora, si lahko predstavljamo ob primeru, da se med preiskavo izkaže, da se kršitev sploh ni zgodila z uporabo računalnika v stanovanju, v katerem je potekala preiskava, temveč z uporabo njihovega brezžičnega interneta, ki ga je v sosednjem stanovanju, za preiskavo katerega pa policija nima odredbe, uporabljal sosed.

43 Več o slovenski ureditvi hišne preiskave glej v Šugman, Gorkič, Dokazovanje v kazenskem postopku (2011), str. 122–136.

44 Kerr, Digital Evidence in the New Criminal Procedure, v: Columbia Law Review, 105 (2005), str. 297.

45 Sporna je recimo uporaba naprave, imenovane IMSI-catcher. Gre za mobilno »lažno« telefonsko centralo, ki prestreza telefonske klice mobilne telefonije. Uporablja jo policija, da lahko pridobi podatke o tajnih telefonskih številkah.

46 Pri nas recimo po 217. členu ZKP, v ZDA pa praviloma po doktrini *plain view*.

če se recimo išče večje orožje, potem preiskovanje knjig, manjše omarice, kuhinjskih predmetov, kjer predmeta že zaradi velikosti ne more biti, ni dovoljeno. Ko pa se preiskava in zaseg nanašata na računalnik, teh omejitev ni. Vedno se zaseže ves računalnik, ne glede na to, ali nas zanima samo majhen del njegove vsebine, in vedno se naredi kopija vsega računalnika. Po klasični doktrini sta zaseg in kopija vsega trdega diska, da najdemo samo en detajl, preširoko pooblastilo; analogija bi bila zaseg celotne hiše, da bi pogledali, kaj je v omarici. Poleg tega pregled zahteva mnogo več časa (lahko traja več tednov) in tehničnega znanja. Omejitve, ki jih je pravni sistem postavil v fizičnem svetu, torej v digitalnem svetu težje delujejo. Zato se Brennerjeva zavzema, da se v primeru preiskave elektronske naprave (recimo računalnika) natančno določi vsebina odredbe: ali se recimo preiskujejo slike, elektronska pošta ali morda dokumenti.[47] Prav tako bi morali biti natančno določeni metode in časovni okvir preiskovanja.[48]

4. Preiskave brez suma in brez odredbe

Načeloma sme država posegati v posameznikove pravice samo, če je to utemeljeno zaradi varovanja neke druge pomembne (navadno ustavno) varovane vrednote. Ena teh vrednot je tudi učinkovito preganjanje storilcev kaznivih dejanj, na katero se pogosto sklicujejo norme, ki dovoljujejo poseg v določeno pravico. Namen takih posegov, ki se izvajajo v kazenskem postopku, je seveda zagotavljanje dokazov za kazenski postopek.

Tako pri nas kot v ZDA, od koder prihaja večina garantne ideologije kazenskega postopka, je recimo razvita bogata sodna praksa v zvezi z vprašanjem, kdaj lahko organi oblasti opravijo preiskavo brez naloga oziroma brez predhodne sodne kontrole sodišča. Tako kot pri nas tudi tam velja pravilo, da morajo organi pregona imeti za hišno ali osebno preiskavo veljavno sodno odredbo, ki mora temeljiti na neke vrste dokaznem standardu, ki ga navadno primerjamo z našimi utemeljenimi razlogi za sum (*probable cause*).[49] Samo na podlagi takšne odredbe je mogoče priti do dokazov, kadar brskamo po zasebnosti doma ali osebe. Za naše razpravljanje je pomembno uvideti, da se v praksi pojavlja vse več izjem od tega splošnega pravila, ki med pogoji za opravo posega v pravico zahteva veljavno sodno odredbo in predhodnost dokaznega standarda. Vsem tem izjemam je

[47] Brenner, Frederiksen, Computer Searches and Seizures, v: Michigan Tel. and Technology Law Review, 8 (2002), 70–71.

[48] Prav tam, str. 81–82.

[49] Glej Zupančič in drugi, Ustavno kazensko procesno pravo (2000), str. 479–499.

skupno tudi to, da so nastale prav zaradi možnosti, povezanih z uporabo sodobnih tehnologij, ki omogočajo hitro preiskovanje velikih skupin ljudi.

V teoriji so izjeme od tega pravila, recimo privolitev in doktrina *plain view*, že dobro znane.[50] Za naše razpravljanje so še posebej zanimive tiste izjeme, do katerih je prišlo zaradi uporabe sodobnih tehnologij, oziroma tiste izjeme, ki jih je omogočila uporaba sodobnih tehnologij.[51] Pri tem velja omeniti ameriško doktrino o izjemi posebnih potreb (*special needs searches*). Gre za preiskave in zasege, ki se opravijo brez upoštevanja navedenih standardov, ne da bi pred tem imeli potrjen dokazni standard. Ti posegi so torej nedoločeni (nespecifični) in nekonkretizirani, manjkata pa tudi elementa predhodnosti in artikulabilnosti.[52] Posledica vsega tega je širjenje polja nadzorovanja: ti posegi se namreč opravljajo zoper veliko število ljudi, preventivno, ne da bi bile osebe, zoper katere se tak ukrep izvaja, glede česarkoli sumljive.

Za presojo upravičenosti oziroma zakonitosti takega poseganja je ameriška sodna praksa izdelala dva kriterija, ki ju je treba pretehtati, če hočemo utemeljiti takšen poseg: (1) potrebnost takšne preiskave in (2) ustavna invazivnost takšne preiskave.[53] Klasični primeri preiskav brez suma in brez odredbe so: (a) varnostni pregledi na letališčih ali na carini; (b) naključni pregledi študentov z detektorjem kovin; (c) preiskava študentovega računalnika, če temelji na informaciji, da študent vdira v računalniški sistem fakultete.[54] Za razlikovanje teh posegov od preiskav in zasegov je ključen njihov namen: ne iskanje dokazov, temveč varovanje javnosti.[55] Še več: take splošne preiskave izrecno ni mogoče uporabiti, kadar je odredba očitno namenjena pridobivanju dokazov v kazenskih postopkih. Namen take prepovedi je preprečevanje zlorabljanja pravila, da se smejo preiskave opraviti samo na podlagi sodne odredbe in upoštevajoč druge varovalne pogoje (recimo dokazni standard, sorazmernost).

Ena od izjem je tudi ukrep naključnega pregledovanja potnikov in prtljage na podzemni železnici, ki so ga uvedli v New Yorku. Seveda so ga izvajali brez

---

[50] Brennerjeva pravi, da je ta doktrina v kibernetskem svetu popolnoma neuporabna. Brenner, Computer Searches and Seizures, v: Michigan Telecommunications and Technology Law Review, 8 (2002), str. 94–95.

[51] Več o uporabi doktrine *plain view* glej pri Selinšek, Digitalni dokazi v kazenskem postopku, v: KRIMINALITETA IN TEHNOLOGIJA (2010), str. 110–112.

[52] Več o tem glej v: Zupančič in drugi, USTAVNO KAZENSKO PROCESNO PRAVO (2000), str. 481–499.

[53] Henderson v. City of Semi Valley (9th Cir. 2002) 305 F.3rd 1052, 1059; ki se sklicuje na Ferguson v. City of Charleston (2001) 532 U.S. 67, 78 [149 L.Ed.2nd 205].)

[54] United States v. Heckenkamp (9th Cir. 2007) 482 F.3rd 1142.

[55] Gre za t. i. doktrino omejene uporabe (*narrow use requirement*). Glej Covey, Pervasive Surveillance and the Future of Forth Ammendment, v: Mississippi Law Journal, 80 (2011), str. 1306–1307.

predhodnega specifičnega suma in brez odredbe. V primeru MacWade v: Kelly[56] je sodišče presojalo, ali tak ukrep prestane test zasebnosti iz četrtega amandmaja k ameriški ustavi, katerega ključni element je razumnost (*reasonableness*) preiskave. Ugotovilo je, da je takšno preiskovanje na podlagi doktrine posebnih potreb razumno, saj naj bi potreba po varnosti pred terorističnimi napadi odtehtala poseg v zasebnost. Pri tem tehtanju bi seveda moralo biti ključno vprašanje, koliko takšni pregledi v resnici preprečujejo teroristične napade, saj bi le tako lahko ugotovili, ali je poseg v pravico do zasebnosti upravičen in razumen. Vendar pa tega tehtanja sodišče ni opravilo, ker je odločilo, da je treba odločitev o tem prepustiti tistim, ki imajo za to specifično varnostno znanje.

Kot pronicljivo ugotavlja Solove, je sodišče odpovedalo prav tam, kjer bi moralo nadzirati ukrepe oblasti. Če bi sprejeli takšno logiko, potem bi lahko uvedli vsake vrste preiskovanje, ne da bi pred tem zahtevali obstoj nekega dokaznega standarda, in to celo brez sodne odredbe, ne glede na to, kako učinkovito ali neučinkovito bi bilo.[57] Prav oceno učinkovitosti bi moralo opraviti sodišče: tehtati bi moralo učinkovitost programa, ki naj bi zagotovil cilj varnosti, in nato oceniti, ali ta učinkovitost odtehta tolikšen poseg v zasebnost. Če sodišče tega tehtanja ne opravi, potem varnost vedno lahko dobi prednost pred svobodo. Poleg vsega drugega so takšne preiskave zelo neučinkovite: preiščejo zgolj miniaturni del populacije in tako obstaja minimalna verjetnost, da bodo na podlagi tega ukrepa prijeli terorista. Hkrati pa bodo teroristi ravno zaradi takih ukrepov svojo dejavnost zelo verjetno prenesli nekam drugam. Zato je mnogo bolj verjetno, da bodo zaradi takega ukrepa trpeli samo nedolžni.[58] Edini učinek takih ukrepov je vzbujanje lažnega občutka varnosti (pa tudi odpora).

Postavlja se še dodatno vprašanje: ali res lahko trdimo, da splošno preiskovanje zaradi nevarnosti terorizma ni delovanje, ki je namenjeno iskanju dokazov za kazenski postopek? Pogosto ju je namreč skoraj nemogoče razlikovati. Kako lahko potem presojamo dokaze, ki so bili pridobljeni s takšnim preventivnim, splošnim in neomejenim preiskovanjem, pri katerem smo obšli vsa v dolgih stoletjih oblikovana varovala? Ali to pomeni, da ima varnost javnosti absolutno prednost pred človekovimi pravicami in da lahko dokazni material, pridobljen s popolnoma nespecifičnim, množičnim preiskovanjem, postane dokaz v kazenskem postopku?

Če bi strogo upoštevali doktrino namena (*narrow use requirement*), po kateri je ključen namen, s katerim je bil dokazni material pridobljen, potem takšnega

[56] MacWade v. Kelly, 460 F3d 260 (2nd Cir 2006).

[57] Solove, Data mining, v: University of Chicago Law Review, 75 (2008), str. 348.

[58] Londonska policija je med izvajanjem podobnih ukrepov ubila nedolžno osebo. URL: http://news.bbc.co.uk/2/hi/uk_news/4711021.stm (16. 8. 2013).

materiala (ker ukrep, s katerim je bil pridobljen, izrecno ni smel biti namenjen pridobivanju dokazov) ne bi smeli uporabiti na sojenju. Lahko bi ga uporabili samo za to, da bi preprečili nevarnosti, ki se pojavljajo. Če bi torej na letališču pri rutinskem pregledu odkrili eksploziv, ki bi ga nekdo skušal vtihotapiti v letalo, ali potem tega eksploziva res ne bi smeli uporabiti v potencialnem kazenskem postopku zoper to osebo?[59] Natančno tako stališče je namreč v skladu z doktrino ozke uporabe oziroma namenom poseganja. Če je ta namen varovanje javnosti, potem se mora poseg tukaj tudi končati; javnost smo zavarovali s tem, da smo našli eksploziv. Ker je bil poseg, s katerim smo do dokaza prišli, izveden mimo strogih pravil kazenskega postopka, naj se tak dokaz ne bi smel uporabiti v kazenskem postopku.

Ali pa je treba sprejeti, da lahko preiskovanje brez predhodne sodne odredbe in dokaznega standarda zaradi pomena varovane dobrine (v tem primeru varovanja javnosti) preraste svoj namen in preide v kazensko preiskovanje brez odredbe? V tem primeru bi država lahko uporabila tako pridobljene dokaze v potencialnem kazenskem postopku. Covey recimo zareže ločnico pri uporabi tako pridobljenega dokaznega materiala prav tukaj. Trdi, da se tako pridobljeni material lahko uporabi samo v kazenskih postopkih, ki se nanašajo na terorizem (zaradi katerih je bila izjema sploh uvedena), ne sme pa se uporabiti v kazenskih postopkih zaradi drugih kaznivih dejanj.[60] Tako naj bi se preprečila zloraba teh širokih metod nadzorovanja za pridobivanje dokazov v drugih zadevah. Če ne bi bilo tako, bi takšno nadzorovanje kmalu lahko postalo primarni način pridobivanja dokazov za vsa kazniva dejanja, ne samo tista, pred katerimi naj bi takšni posegi varovali.[61] Tako bi bilo treba pri vseh primerih, ko obstaja neka izjema za izvedbo preiskav in zasegov brez odredbe, ki je utemeljena na razlogu varovanja javnosti, paziti, da se ta izjema ne sprevrže v splošno preiskovanje z namenom

[59] Simmons trdi, da protiteroristično preiskovanje ni dovoljeno niti po doktrini posebnih potreb niti po četrtem amandmaju k ameriški ustavi, ki varuje zasebnost. Rešitev vidi v tem, da se ti pregledi sicer izvajajo, vendar pa se material, ki se s takimi pregledi dobi, ne bi smel uporabiti na sojenju. Simmons, Why Public Safety, v: Duke Law Journal, 59 (2010), str. 843–927.

[60] Covey, Pervasive Surveillance and the Future of Forth Ammendment, v: **Mississippi Law Journal**, 80 (2011), str. 1309.

[61] Vendar pa tudi Covey v nadaljevanju odstopi od tako strogega pogleda, sklicujoč se na doktrino implicitnega soglasja. Zamislimo si primer, ko pri pregledu na letališču pri nekom najdejo droge. Postavlja se vprašanje, ali se te droge smejo uporabiti kot dokaz v kazenskem postopku. Covey trdi, da je odgovor na to vprašanje pritrdilen, saj je ta oseba vedela, da bo na letališču varnostno pregledana; s tem je pravzaprav implicitno privolila v možnost, da bodo najdene tudi droge. Ta oseba je torej imela možnost, da se temu pregledu izogne tako, da ne potuje, ali pa da s seboj na potovanje ne nese drog; zato bi po Coveyevem mnenju takšne droge lahko uporabili kot dokaz. Prav tam, str. 1310.

iskanja dokazov za potencialne kazenske postopke.[62] Na tak način je namreč mogoče obiti vse varovalke, ki jih pozna kazenski postopek.

5. Nedoločeno prisluškovanje[63]

Zaradi težav pri uporabi klasičnih tehnik prisluškovanja in nadzorovanja različnih pošiljk so zakonodajalci našli nove rešitve. Poleg osnovnega pridobivanja podatkov o komunikacijskem prometu (ki ga v ZDA še vedno pogovorno imenujejo *pen register*)[64] in popolnega prisluškovanja so uvedli še nedoločeno prisluškovanje (*roving wiretap*). V ZDA tudi klasična kazenskopravna zakonodaja pozna institut odredbe za nedoločeno prisluškovanje (*roving intercept orders*), s katerim se takšne vrste nadzorovanje odredi. To je odredba za nadzorovanje ustne ali elektronske komunikacije določene osebe, ne glede na to, kje je (seveda pod jurisdikcijo, za katero je ta odredba odrejena), in ne glede na to, katero napravo za komuniciranje uporablja (telefon, računalnik ipd.). Gre torej za izjemo od običajne zahteve po tem, da se natančno določi in omeji lokacija, kje naj se nadzoruje, ali elektronsko sredstvo, ki naj se nadzoruje.[65] Pogoji za odreditev so strožji kot za odreditev klasičnega prisluškovanja. Med drugim lahko zahtevo vloži samo najvišji del tožilske hierarhije, sodišče pa mora prepričati o tem, da oseba, za katero se prisluškovanje odreja, izvršuje kaznivo dejanje in da obstaja dokazni standard (*probable cause*), da bi njena dejanja lahko učinkovala tako, da bi preprečevala prisluškovanje s točno določene lokacije.[66] Ravno zato pa se odreja splošno prisluškovanje, ki ni omejeno na specifično lokacijo; to se odredi za razumen čas.

Zakon *Foreign Intelligence Surveillence Act* (FISA), ki ga je kasneje, po terorističnem napadu 9. novembra 2001, dopolnil *Patriot Act* (PA), pa je dovolil uporabljati takšne vrste prisluškovanje tudi za potrebe varnostno-obveščevalnih služb.[67] Pred uvedbo *Patriot Act* so bila torej nedoločena prisluškovanja (*roving*)

---

62 Prav tam, str. 1312.

63 Glagol *to rove* v angleškem jeziku pomeni klatiti se ali potepati se. Tako bi lahko izraz *roving wiretap* še najbolj dobesedno prevedli kot klateče se ali potepinsko prisluškovanje. Vendar pa se to sliši nekoliko nenavadno, zato sem se raje odločila za izraz nedoločeno prisluškovanje.

64 Pri nas je ta ukrep urejen v 149.b členu ZKP.

65 Electronic Surveillance, v: Georgetown Law Journal Annual Review of Criminal Procedure, 38 (2009), str. 147.

66 18 U.S.C. § 2518(11).

67 Pri tem prihaja tudi do nevarnega prehajanja podatkov od varnostnih služb do organov pregona. Več o tem glej pri Završnik, Blurring the Line between Law Enforcement and Intelligence, v: Journal of Contemporary European Research, 9 (2013) 1, str. 181–202.

dovoljena samo v kazenskem pravosodju, če je predlagatelju uspelo dokazati, da osumljenec dejansko uporablja napravo, ki se nadzoruje, po sprejetju PA pa se je uporaba tega ukrepa razširila tudi na delovanje tujih obveščevalnih služb, ne da bi bilo treba izpolnili navedeni pogoj.[68] Ta vrsta nadzora se lahko uporablja, kadar je pomemben del nadzorovanja želja, da bi dobili tuje obveščevalne podatke, ki jih ni mogoče dobiti z drugimi preiskovalnimi metodami. [69]

Čeprav je ta poseg v posameznikovo zasebnost zelo invaziven, je postopek odrejanja neprimerno blažji kot drugi podobni postopki, hkrati pa so opuščene tudi nekatere druge varovalke. To pooblastilo lahko v ZDA uporabijo zoper obveščevalne agente na teritoriju ZDA z namenom pridobivanja obveščevalnih podatkov iz tujine. Za odreditev takega ukrepa mora zaprositi urad generalnega tožilca, o odreditvi odredbe pa lahko odloča eden od posebej izbranih sodnikov, ki so jih za to določile zvezne države. Ti skupaj sestavljajo *Federal Intelligence and Security Court* (FISC), ki deluje v tajnosti in posluša samo predlog tožilstva (torej ni zagotovljena nikakršna kontradiktornost). Takšen ukrep se lahko uporablja v preiskavah, ki zahtevajo »večplastne odgovore na terorizem, ki vključuje tuje obveščevalne podatke in kazensko preiskavo«. Pogoj za odreditev je sicer nekakšen ekvivalent utemeljenega suma (*probable cause*), ki pa je v tem primeru postavljen bistveno nižje kot standard, ki se uporablja v rednem kazenskem postopku.[70] V nasprotju s klasičnim kazenskim postopkom podatkov, do katerih so prišli na tak način, tudi ni treba razkriti posamezniku, ki so mu prisluškovali, razen če bodo uporabljeni zoper njega v postopku pred sodiščem.[71] Nikakor pa se ne smejo razkriti podatki, na podlagi katerih je bil ukrep sploh uveden, kar seveda povzroča tudi težave z naknadno kontrolo utemeljenosti uvedbe takega ukrepa.[72]

Kritike tega instituta so bile zelo ostre, saj je poseg zelo invaziven. Zajame lahko tudi nedolžne posameznike, ki z odredbo nimajo nikakršne povezave. Omogoča splošno nadzorovanje, ne da bi zoper osebo, ki po naključju uporablja komunikacijsko sredstvo, ki ga je prej uporabljal osumljenec, obstajal kakršenkoli sum.[73] Hkrati so bile predmet kritike tudi druge spremembe zakonodaje,

---

[68] Henderson, The Patriot Act's Impact, v: Duke Law Journal, št. 52 (2002), str. 197.

[69] Prav tam.

[70] Walton, Prosecuting International Terrorism Cases in Article III Courts, v: Georgetown Law Journal Annual Review of Criminal Procedure, 39 (2010), str. xviii.

[71] Foreign Intelligence Surveillence Act 50 U.S.C. (FISA), 106.

[72] Etzioni, Implications of Select New Technologies, v: Harvard Journal of Law & Technology, 15 (2002), str. 267.

[73] Kritiki so upravičeno navedli primer, ko bi lahko na podlagi tega pooblastila na primer nadzorovali računalnik v javni knjižnici tudi še po tem, ko bi osumljenec nehal delati na njem. American Civil Liberties Union, How the Anti-Terrorism Bill Limits Judicial Oversight of

ki so olajšale in pospeševale pridobivanje odredb. Tako zdaj v eni zvezni državi pridobljena odredba velja tudi v drugih,[74] poenostavljeni so bili pogoji za pridobitev take odredbe[75] in tudi pogoji za posredovanje teh podatkov drugim vladnim agencijam.[76] Kritiki trdijo, da sodišča odrejajo takšne odredbe nekritično, in treba je priznati, da podatki o teh vrstah odredb njihove kritike potrjujejo. Od leta 1979, ko so uvedli to vrsto odredb, so jih vsako leto odredili približno 1000, v vseh teh letih pa so sodišča zavrnila samo eno zahtevo za izdajo takšne odredbe, kar res zbudi dvome o sodnih standardih presoje.[77]

6. Rudarjenje po podatkih

Rudarjenje po podatkih, kot prevajamo angleško frazo *data mining*, je preučevanje in kombiniranje ogromnega števila podatkov iz različnih virov (npr. nakupovalni vzorci, bančne informacije, strani, ki jih pregledujemo na internetu, zdravstveni podatki) z namenom, da bi dobili podatke o vrednotah, političnem prepričanju, navadah in vedenjskih vzorcih, ki so značilni za določene profile ljudi. Tako bi lahko recimo na podlagi teh vzorcev identificirali potencialne storilce kaznivih dejanj, npr. teroriste.[78]

Zasebnost posameznikov, o katerih se zbirajo podatki, je kršena na treh ravneh: na ravni zbiranja, obdelovanja in posredovanja teh podatkov. Pri tem je še posebej problematična povezava med zasebnimi in javnimi subjekti.[79] Država

---

Telephone and Internet Surveillance, URL: http://www.aclu.org/national-security/how-anti-terrorism-bill-limits-judicial-oversight-telephone-and-internet-surveilla (16. 8. 2013).

74 S tem je omogočen tudi t. i. *forum shopping* – iskanje sodnikov, ki so bolj naklonjeni izdajanju določenih odredb. Henderson, The Patriot Act's Impact, v: Duke Law Journal, 52 (2002), str. 202.

75 Po novi ureditvi mora vladna stran recimo samo pokazati, da je informacija, do katere bi lahko s tem posegom prišli, relevantna za preiskavo, ki poteka, medtem ko so prej morali dokazati, da obstaja verjetnost, da bo nadzorovano napravo uporabil nekdo, ki je vpleten v teroristično dejavnost ali je agent tuje države. Prav tam, str. 199.

76 Prav tam, str. 204–205.

77 Carlsen, Secretive U.S. Court May Add to Power, cit. po Etzioni, Implications of Select New Technologies, v: Harvard Journal of Law & Technology, 15 (2002), str. 284.

78 Posamezen podatek ima omejeno vrednost. Če nekdo recimo bere knjige o vojskovanju, nam to pove samo, da se zanima za vojskovanje. Podatki o njegovem nakupovanju, da kupuje stvari, ki se lahko uporabijo za eksploziv, prek interneta gleda strani o tem, kako se sestavi eksplozivno telo, in pogosto kupuje letalske vozovnice za določeno mesto, pa nam povedo mnogo več.

79 Tako so tudi v Sloveniji recimo krožile ideje, da bi se podjetja, ki prodajajo bencin, lahko povezala s policijskimi bazami, v katerih so podatki o ukradenih registrskih tablicah. V hipu, ko bi se na bencinsko črpalko pripeljal avto z ukradeno tablico, bi ga kamere na črpalki zaznale in črpalko zaprle, ker je velika verjetnost, da bo oseba, ki ima tak avto, zbežala, ne da bi plačala

ima težnjo, da bi dobila vpogled v zbirke, ki jih vodijo zasebni subjekti. Viri so številni: operaterji internetnih strani, telefonska podjetja, delodajalci, potovalne agencije, nakupovalni centri, banke, zavarovalnice, najemodajalci ipd. Dostop do podatkov postaja ključen.[80]

Čeprav so vlade nad temi programi precej navdušene,[81] je njihova dodana vrednost zelo dvomljiva. Ti programi so precej uspešni pri ugotavljanju in napovedovanju vedenja potrošnikov, pri identificiranju potencialnih teroristov pa so mnogo manj natančni, saj so dejavniki, ki jih preučujejo, mnogo manj jasni. Hkrati je posledica napake pri potrošniku skoraj nična, pri identifikaciji nedolžne osebe kot terorista pa ogromna.[82] Problematičen je tudi vidik udeležbe in pravic posameznika, čigar podatki se zbirajo na ta način, ali posameznika, čigar profil je izbran kot nevaren. Kakšne možnosti ima recimo nekdo, ki je bil označen za potencialnega terorista, da izpodbija to oznako? V ZDA se mu lahko zgodi, da ne bo mogel potovati z letalom, ne bodo ga spustili v nekatere institucije ipd. Komu se lahko pritoži zoper to označbo in ali ima pravico do popravka, izbrisa? Večinoma sploh ne bo vedel, zakaj ga ne spustijo na letalo, kaj šele, od kod prihajajo podatki o njem. Pri tem pa gre za podatke, ki temeljijo na verjetnosti, da bo nekdo naredil nekaj prepovedanega, in ne za podatke o tem, da je nekaj naredil. Kako se lahko posameznik upre napačni napovedi?

7. Zaščitne tehnologije

Z izrazom zaščitne tehnologije poimenujemo tehnologije, ki poskušajo zaščiti javnost pred nevarnostmi. Problem, ki se pri tem pojavi, pa je, da se z »varnostjo« širijo tudi pooblastila in nadzorstvene možnosti države, hkrati pa se lahko kršijo številne posameznikove pravice. Ena teh tehnologij je recimo *Carnivore*, FBI-jev program iz leta 2000, ki lahko analizira ogromno število elektronskih sporočil tako, da išče posamezno besedo ali besedno zvezo ali pa med poslanimi sporočili išče tista, ki so poslana z določenega naslova ali

bencin. Korist pa bi imela tudi policija, saj bi tako ujela tatu tablic. V ZDA pa vlada kupuje podatke o zasebnikih: recimo zasebno podjetje ChoicePoint ima pogodbo s približno 35 zveznimi agencijami, vključno s FBI, da jim posreduje zasebne informacije o posameznih.

80 Več o nevarnostih tega glej pri Solove, Digital Dossiers, v: Southern California Law Review, 75 (2002), str. 1083–1167.

81 Glej recimo prispevek, ki opisuje ravnanje ameriške vlade, pri Solove, Data mining, v: University of Chicago Law Review, 74 (2008), str. 343–362.

82 Prav tam, str. 353.

na določen naslov.[83] Ima dve možnosti uporabe: lahko se uporablja samo za preučevanje podatkov o prometu v elektronskem komunikacijskem omrežju, njegova uporaba pa se lahko razširi tudi na preiskovanje vsebine.[84] Za vsakega od teh posegov je potrebna posebna sodna odredba.[85] Obstajajo tudi drugi podobni programi, katerih namen je odkrivati računalniška gesla in razbiti zaščitne kode, s katerimi so zavarovana določena sporočila (npr. *Key Logger System* (KLS) in *Magic Lantern*).[86] Ko preiskovalci naletijo na kodirano sporočilo, lahko zaprosijo za posebno odredbo o namestitvi in uporabi enega od navedenih programov, s katerim lahko razkrijejo računalniško geslo. Zanimivo pa je, da tega gesla ne morejo pridobiti, če je računalnik priključen na internet, saj bi s tem omogočili tudi nadzor komunikacije. Za to pa potrebujejo posebno odredbo.

Pri teh programih skrb zbuja zlasti to, da vedno zajamejo več, kot je bilo mišljeno ob izdaji sodne odredbe. Čeprav je v največjem številu primerov njihov namen preučevati samo podatke o komunikaciji (torej naslovnike sporočil, ne same vsebine), je pogosto težko razlikovati med enim in drugim in se pri uporabi programa pregleduje tudi vsebina.[87] Izredno težko je tudi *ex post* preveriti, ali so programe res uporabili samo v tistih mejah, ki so bile začrtane s sodno odredbo. Eden od problemov je tudi to, da naj bi bili preiskovalci s sodno odredbo pooblaščeni, da lahko iščejo samo specifične informacije, ki so zajete z odredbo, vendar obstaja več različic tega progama, za katere ni povsem jasno, v kakšne namene so lahko uporabljeni. Glavni pomislek pa je nepregledna količina elektronskih sporočil, ki so s temi pregledi zajeta, in seveda števila informacij, ki so s tem pridobljene. Ker program »prečeše« milijone sporočil, seveda zajame tudi (oziroma predvsem) povsem nedolžno komunikacijo.

---

83 Lewis, Carnivore – The FBI's Internet Surveillance System, v: Whittier Law Review, 23 (2001), str. 317–354, Nabbali, Perry, Going for the Throat: Carnivore in an Echelon World, Part 1, v: Computer Law & Security Review, 19 (2003) 6, str. 456–467.

84 Walden utemeljeno opozarja na to, da je razlikovanje med enim in drugim pogosto težko. Walden, Computer Crimes (2007), str. 272–275.

85 Etzioni, Implications of Select New Technologies for Individual Rights and Public Safety, v: Harvard Journal of Law and Technology, 15 (2002), str. 274–275.

86 Medtem ko morajo KLS namestiti fizično, se lahko Magic Lantern instalira, ne da bi imeli fizični dostop do računalnika. Prav tam.

87 Segura, Is Carnivore Devouring Your Privacy, v: Southern California Law Review, 75 (2001), str. 235.

8. Razprava

Pojmovanje zasebnosti se povsod, celo v ZDA, v državi, katere sodna veja je prek svoje sodne prakse izumila sloviti koncept pričakovanja zasebnosti,[88] prav zaradi capljanja za novimi tehnologijami krha kos za kosom. Zato se lahko resno vprašamo, koliko je od tega koncepta sploh še ostalo. Kot ugotavlja Covey, je četrtemu amandmaju, ki naj bi ljudem, njihovim domovom in dokumentom zagotavljal zaščito pred neutemeljenimi preiskavami in zasegi, popolnoma spodletelo.[89] Stoično ugotavlja, da se moramo z državo nadzorovanja, ki ne bo namenoma »gledala stran«, preprosto sprijazniti.[90] Vsesplošna razširjenost invazivnega nadzorovanja je tako neobvladljiva, da bi morali po njegovem mnenju središče razprave preusmeriti od želje po urejanju vprašanja, kako država prihaja do informacij (s tem naj bi se bilo torej treba sprijazniti), k urejanju vprašanj, kaj lahko država s temi podatki dela in kam jih lahko posreduje.[91]

Takšno razmišljanje ima pomembne procesnopravne posledice. Če naj bi se v prihodnosti sodna presoja res ukvarjala samo še z vprašanjem uporabe možnosti določenih podatkov (in torej ne več z načinom njihove pridobitve), potem to še bolj postavlja v ospredje ekskluzijsko pravilo. Prav izločitev dokazov je namreč – ob obstoju vsesplošnega, nekonkretiziranega in nespecifičnega prido-

---

[88] Kriterij razumnega pričakovanja zasebnosti se je oblikoval v slovitem primeru ameriškega Vrhovnega sodišča Katz v. US, 389 U.S. 347 (1967). S tem primerom je sodišče oblikovalo test, s katerim se presoja zakonitost posegov države v zasebnost posebnost in vprašanje, kdaj tak poseg pomeni nezakonito preiskavo po četrtem amandmaju k Ustavi ZDA. Gre za test razumnega pričakovanja zasebnosti (*reasonable expectation of privacy*), ki ga je kasneje prevzelo tudi Evropsko sodišče za človekove pravice. V skladu s tem testom lahko razumemo kot poseg v zasebnost v obliki preiskave tudi takšen poseg, ki ni ozko vezan na dom (v konkretnem primeru je šlo za javno telefonsko govorilnico) in pri katerem ne pride do fizičnega posega, temveč za poseg, ki je narejen s sodobno tehnologijo (v konkretnem primeru je šlo za prisluškovanje). Za nas je zanimiv drug del te ugotovitve, saj je bilo prvič potrjeno, da se lahko tudi z uporabo tehnologije izvrši nezakonita preiskava. Ashdown, The Fourth Amendment and the »Legitimate Expectation of Privacy«, 34 (1981), v: Vanderbilt Law Review, str. 1289–1345.

[89] Covey, Pervasive Surveillance and the Future of Forth Ammendment, v: **Mississippi Law Journal**, 80 (2011), str. 1300. K temu je morda največ prispevala t. i. doktrina *third party*, po kateri podatki, ki jih je nekdo vedoma oziroma zavestno razkril tretji stranki, niso predmet varstva zasebnosti. Če namreč oseba vedoma razkrije neko informacijo tretji stranki, potem naj bi se odrekla razumnemu pričakovanju zasebnosti. To doktrino so ameriška sodišča uporabila v različnih primerih: najprej v zvezi s tajnimi sodelavci v On Lee v. United States in kasneje še za komunikacijo na internetu, saj jo oseba vedno vedoma razkrije operaterju. Kerr, The case for the third-party doctrine, Michigan Law Review, 107 (2009), str. 561. Glej še kritike te doktrine pri Defilippis, Securing Informationships, v: Yale Law Journal, 115 (2006), str. 1086–1121.

[90] Covey, Pervasive Surveillance and the Future of Forth Ammendment, v: **Mississippi Law Journal**, 80 (2011), str. 1301.

[91] Prav tam, str. 1302.

bivanja dokazov brez sodne odredbe, torej od tako rekoč kogarkoli in kjerkoli – edini učinkovit način, da se državi vsaj prepreči, da takšne podatke uporabi sebi v prid.[92] Zdi se, da je prav izločitev dokazov za kazenski postopek pravzaprav edini način, da se država ne more sklicevati na dokaze, ki so bili morda pridobljeni s čezmernim splošnim in preventivnim posegom. Težava pa je, da se v mnogih državah tudi ekskluzija razlaga vse bolj utilitaristično.[93]

Pri tem, ko širimo možnost, da se država izogne nekaterim varovalkam pri posegih v zasebnost ali, z drugimi besedami, ko pridobiva čedalje več možnosti, da pride do dokaznega materiala mimo strogih pogojev, ki so bili zasnovani za varovanje zasebnosti, moramo poskrbeti za ravnotežje na drug način. Če recimo širimo cono pregledov, ki se lahko opravljajo preventivno oziroma mimo zahteve, da zanje obstajata predhodna sodna kontrola in določen varovalni dokazni standard, potem moramo poostriti zahteve na drugi strani. Treba se je osredotočiti na standarde, pod katerimi pogoji lahko država takšen dokaz uporabi. Če torej dopustimo, da se izvajajo široki protiteroristični ukrepi, ne da bi pred tem obstajala konkretizirana, artikulirana verjetnost, da je prav oseba, ki jo pregledujemo, storila nekaj prepovedanega, potem moramo biti vsaj pri nadaljnjem ravnanju s takšnim dokaznim gradivom zelo strogi: treba se je omejiti na namen, s katerim je bil dokaz pridobljen.[94]

Podobna logika mora veljati pri uporabi čedalje bolj vseobsežne tehnologije. Ker se torej sodobne metode preiskovanja kot predmeti preiskovanja (recimo računalnik, internet) tako kvalitativno kot kvantitativno razlikujejo od klasičnih, je s klasičnimi kazenskopravnimi koncepti možnosti pretiranega poseganja in nadzorovanja skoraj nemogoče zajeziti. Ravno zato pa je treba biti zelo natančen pri postavljanju meril za tako preiskovanje in hkrati izredno natančno določiti ravnanje z dobljenimi informacijami. Lahko bi postavili pravilo, da čim več podatkov lahko pridobimo z določenim načinom nadzorovanja, tem bolj natančno morajo biti postavljena pravila, ki določajo, kaj se s temi podatki lahko dela in v kakšnih primerih. Če imamo neko napravo, ki lahko recimo nediskriminatorno prisluškuje pogovorom ali pridobi prometne podatke o velikem številu ljudi naenkrat,[95] potem je treba postaviti zelo stroge pogoje, katere od teh podat-

[92] Če nam oko seže prek kazenskega postopka, potem pa se moramo seveda spraševati tudi o tem, komu in s kakšnim namenom lahko država takšne podatke posreduje. Pri tem so posebej problematična javno-zasebna partnerstva.

[93] Tudi Slovenija ni izjema, saj kljub uzakonjeni radikalni ekskluziji sodna praksa postopno uvaja tehtanje. Glej recimo sodne odločbe Vrhovnega sodišča RS z opr. št. I Ips 46/2011 in Višjega sodišča v Ljubljani z opr. št. I Kp 1011/2004 in opr. št. II Kp 9220/2011.

[94] Covey, Pervasive Surveillance and the Future of Forth Ammendment, v: Mississippi Law Journal, 80 (2011), str. 1306.

[95] Značilen primer je IMSI-Catcher.

kov sme država uporabiti. Vse drugo pa mora biti takoj uničeno ali zbrisano. Če zaradi lastnosti tehnologije torej ne moremo zajeti samo relevantnih podatkov, potem moramo z vsemi podatki, ki smo jih zajeli naključno, ravnati strogo – ne smejo biti uporabljeni. Pri sodobnih tehnologijah postaja torej ključno vprašanje namena, s katerim so bili neki podatki zbrani.

9. Sklep

Nobenega dvoma ne more biti o tem, da mora tudi kazensko pravo ponuditi nove odgovore na nove izzive. Če kriminaliteta dobiva nove razsežnosti, moramo organom pregona omogočiti, da se na te spremembe učinkovito odzovejo. Ob uvajanju novih rešitev pa se vedno postavlja vprašanje tehtanja med tema vrednotama oziroma ciljema kazenskega postopka: učinkovitostjo pregona in varovanjem pred čezmernimi posegi v pravice posameznikov. Hitro se znajdemo v položaju, ko se zdi, da je neka učinkovita rešitev tudi nujna za zagotavljanje določenega cilja. Tako se diskusije glede uvedbe bolj ali manj invazivnega preiskovalnega dejanja navadno začnejo z razpravo o tem, kako velika je specifična nevarnost, ki naj bi jo ta ukrep preprečeval. Zagovorniki takega ukrepa pri tem uporabljajo vsa orožja jezikovnega arzenala, da prikažejo razsežnost in usodnost določenega pojava.[96] Navadno je moč takšnega uvodnega prikaza bolj v besedah kot pa v realističnem navajanju podatkov, statistik in verjetnosti. Ob prebiranju takšnih retoričnih ognjemetov človeka navadno kar samega zanese v edini mogoči sklep: da je ukrep, ki ga predlagajo, pa naj še tako posega v obstoječe pravice, najmanj, kar lahko storimo za svojo varnost. Še več, da je žrtev odpovedi pravicam, ki jo moramo za to sprejeti, nična v primerjavi z vsemi nevarnostmi, ki grozijo. Strah pred nevarnostjo nam zamrači presojo in nas sili, da gledamo samo v smer varnosti, ne da bi dobro ocenili (1) njeno razsežnost, (2) realno verjetnost, da predlagani ukrep *res* prinese obljubljene rešitve, in (3) to, kar bomo zaradi uvedbe tega ukrepa zgubili. Problem je tudi v tem, da navadno ni takoj razvidno, kaj bomo zaradi uvedbe ukrepa izgubili; pokaže pa se na dolgi rok v izgubi svobode, neodvisnosti in transparentnosti. V izgubi osnovnih značilnosti demokracije torej.

Nekateri gredo celo tako daleč, da trdijo, da se mora v situaciji, ko je ogrožena varnost, celotna sodna veja odpovedati svoji vlogi kontrole nad pooblastili izvršilne oblasti, saj naj bi slednja bolj vedela, kakšne so realne nevarnosti, in

[96] To še posebej velja v primeru, ko je nevarnost, ki preži, terorizem.

imela pristojnost tehtati med varnostjo in svobodo.[97] S tem se ne morem strinjati. Zgodovina nas uči, da si izvršilna oblast vedno prizadeva za več moči, kar pomeni tudi oblast nad sodno vejo. Prav neodvisnost sodstva (predvsem od izvršilne oblasti) in možnost sodne veje, da nadzoruje dejanja izvršilne, sta pravni varovalki, ki v družbo vnašata elemente demokratičnosti in transparentnosti. Če želimo ti dve lastnosti vreči na odpad, potem je seveda jasno, da moramo slepo verjeti temu, kar predlaga izvršilna veja. Če pa še imamo upanje, da je mogoča demokratična družba, ki deluje transparentno tudi v času nevarnosti ali krize,[98] potem moramo imeti močno in neodvisno vejo sodne oblasti, ki kritično presoja delovanje izvršilne. Izvršilna oblast je prav gotovo najbolj usposobljena za to, da snuje različne varovalne ukrepe in nova preiskovalna pooblastila, zato pa presoje o tem, ali so ta primerna in sorazmerna, ne smemo prepustiti (samo) njej. In to velja tudi za čas izrednih razmer ali ekonomske krize.

Prav tako se je pri razmišljanju o tem, ali je res treba uvesti neki ukrep, ki se zdi nujen in neizbežen, vedno treba ustaviti in vprašanje presoditi globalno, razumsko in vrednostno. Lahko se zdi, da je tak ukrep res edini mogoč in nujen, da prepreči določeno nevarnost. Navadno ni tako. Če pa je, je do tega sklepa treba priti s tehtanjem vseh elementov načela sorazmernosti in zdravega razuma, oprtega na podatke. V zadnjem desetletju se še posebej pogosto zdi, da je miselni rezultat te naloge redko v prid zagotavljanju svobode.[99] Zdi se, da smo se za (fiktivno) zagotavljanje varnosti pripravljeni odreči vsem pravicam in svoboščinam. Družba mora sprejeti tudi tveganja, da ostane demokratična. Ali, kot je na koncu dolgega razburjanja o pretiranih in ponižujočih varnostnih ukrepih na letališčih, čeprav je že vnaprej jasno, da se jim lahko dobro organizirana teroristična mreža izogne, napisala neka angleška novinarka: raje se prepustim tveganju, da se razletim v zraku z letalom, kot pa da moram vsakič, ko želim potovati z letalom, prenašati te postopke.[100]

---

97 Posner, Not a Suicide Pact, v: Posner, Vermeule, Terror in the Balance: Security, Liberty, and the Courts (2007).

98 Ali kot lepo pravi Solove: »Potreba po varovanju svobode mora biti največja v času, ko jo najmanj želimo zavarovati.« Solove, Data mining, v: University of Chicago Law Review, 74 (2008), str. 350.

99 Glej recimo kritiko brezglavo sprejetih ukrepov EU po terorističnih napadih v: Šugman, Jager, Post 9/11 developments of the EU criminal law-related initiatives, v: Crime Business and Crime Money in Europe, (2007), str. 247–267.

100 Ta trditev še posebej velja, če si ogledamo verjetnost, da umremo v terorističnem napadu. Solove navaja študije, ki ugotavljajo, da je celo vključno z žrtvami 11. 9. 2001 smrt zaradi terorizma v ZDA toliko verjetna kot smrt zaradi naleta srne v avto ali smrt zaradi udara strele. Solove, Data mining, v: University of Chicago Law Review, 74 (2008), str. 350. V osmih najbolj množičnih terorističnih napadih v zgodovini ZDA je umrlo približno 4000 ljudi, medtem ko jih vsako leto zaradi gripe in pljučnice umre približno 60.000.

Literatura

Acquisiti, Alessandro, Gross, Ralph: Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, v: Privacy Enhancing Technologies (ur. G. Danezis, P. Golle), Springer, Berlin/Heidelberg 2006, str. 36–58.

Ashdown, Gerald G.: The Fourth Amendment and the »Legitimate Expectation of Privacy«, v: Vanderbilt Law Review, 34 (1981), str. 1289–1345.

Barrett, Neil: Traces of Guilt, Bantam Press, London 2004.

Blackman, Josh: Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet, v: Santa Clara Law Review, 49 (2009), str. 313–392.

Brenner, Susan, W., Frederiksen, Barbara A.: Computer Searches and Seizures: Some Unresolved Issues, v: Michigan Telecommunications and Technology Law Review, 8 (2002), str. 39–114.

Brenner, Susan, W.: The Privacy Privilege: Law Enforcement, Technology, and the Constution, v: Journal of Technology Law & Policy, 7 (2002), str. 136–150.

Brenner, Susan, W.: Toward a Criminal Law for Cyberspace: Distributed Security, v: Boston University Journal of Science and Technology Law, 10 (2004), str. 1–109

Brenner, Susan, W.: Toward A Criminal Law for Cyberspace: A New Model of Law Enforcement, v: Rutgers Computer & Technology Law Journal, 30 (2004), str. 1–104.

Brenner, Susan, W.: Cybercrime Metrics, v: Virginia Journal of Law and Technology, 9 (2004) 13, str. 1–52.

Byrne, James M.: The Best Laid Plans: An Assessment of the Varied Consequences of New Technologies for Crime and Social Control, v: Federal Probation, 72 (2008), str. 10–21.

Covey, Russel: Pervasive Surveillance and the Future of the Fourth Amendment, v: Mississippi Law Journal, 80 (2011), str. 1289–1318.

Decker, Charlotte: Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, v: Southern California Law Review, 81 (2008), str. 959–1016.

Defilippis, Andrew, J.: Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence, v: Yale Law Journal, 115 (2006), str. 1086–1121.

Electronic Surveillance, Georgetown Law Journal Annual Review of Criminal Procedure, 38 (2009).

Etzioni, Amitai: Implications of Select New Technologies for Individual Rights and Public Safety, v: Harvard Journal of Law & Technology, 15 (2002), str. 257–290.

Goodman, Marc, D., Brenner, Susan, W.: The Emerging Consensus on Criminal Conduct in Cyberspace, v: UCLA Journal of Law and Technology, 3 (2002), str. 1–153.

Henderson, Nathan, C.: The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications, v: Duke Law Journal, 52 (2002), str. 179–209.

Herrera-Flanigan, J. R., Ghosh, S.: Criminal Regulations, v: Cybercrimes: A Multidiciplinary Analysis (ur. S. Ghosh, E. Turrini), Springer, Heidelberg 2010, str. 265–308.

Hodge, Matthew, J.: Fourth Amendment and Privacy Issues on the New Internet: Facebook.com and Myspace.com, v: Southern Illinois University Law Journal, 31 (2006), str. 95–123.

Kerr, Orin S.: Digital Evidence and the New Criminal Procedure, v: Columbia Law Review, 105 (2005), str. 279–318.

Kerr, Orin S.: Law in a Networked World: Criminal Law in Virtual Worlds, v: University of Chicago Legal Forum, (2008), str. 415–430.

Kerr, Orin S.: The case for the third-party doctrine, v: Michigan Law Review, 107 (2009), str. 561–601.

Kovačič, Matej: Nadzor in zasebnost v informacijski družbi, FDV, Ljubljana 2006.

Lawner, Kevin J.: Post-September 11th International Surveillance Activity – A Failure of Intelligence: The Echelon Interception System and the Fundamental Right to Privacy in Europe, v: Pace International Law Review, 14 (2002), str. 435–480.

Lewis, John: Carnivore – The FBI's Internet Surveillance System: Is It a Rampaging E-mailasaurus Rex Devouring Your Constitutional Rights, v: Whittier Law Review, 23 (2001), str. 317–354.

Miller, Seumas, Weckert, John: Privacy, the Workplace and the Internet, v: Journal of Business Ethics 28 (2000) 3, str. 255–265.

Nabbali, Talitha, Perry, Mark: Going for the Throat: Carnivore in an Echelon World, Part 1, v: Computer Law & Security Review, 19 (2003) 6, str. 456–467.

Posner, Richard A., Vermeule, Adrian: Terror in the Balance: Security, Liberty, and the Courts, Oxford University Press, Oxford 2007.

Robinson, Dustin, F.: Bad Footage: Surveillance Laws, Police Misconduct and the Internet, v: Georgetown Law Journal, 100 (2011), str. 1399–1435.

Segura, Maricela: Is Carnivore Devouring Your Privacy, v: Southern California Law Review, 75 (2001), str. 231–270.

Selinšek, Liljana: Odzivi slovenskega kazenskega prava na kibernetski kriminal, v: Pravna praksa, 24 (2005) 5, str. 19.

Selinšek, Liljana: Digitalni dokazi in računalniška forenzika, v: Kriminaliteta in tehnologija (ur. A. Završnik), Inštitut za kriminologijo, Ljubljana, 2010, str. 97–119.

Sieber, Ulrich: Legal Aspects of Computer-Related Crime in the Information Society, COMCRIME Study prepared for the European Commission 19 (januar 1998).

Simmons, Ric: Searching for Terrorists: Why Public Safety is not a Special Need, v: Duke Law Journal, 59 (2010), str. 843–927.

Sloan, Lawrence D.: ECHELON and Legal Restraints on Signals Intelligence: A Need for Reevaluation, v: Duke Law Journal, 50 (2001) 5, str. 1467–1510.

Solove, Daniel, J.: Digital Dossiers and Disparition of Fourth Amendment Privacy, v: Southern California Law Review, 75 (2002), str. 1083–1167.

Solove, Daniel J.: A Taxonomy of Privacy, v: University of Pennsylvania Law Review, 154 (2006), str. 493–495.

Solove, Daniel J.: Data Mining and the Security-Liberty Debate, v: University of Chicago Law Review, 74 (2008), str. 343–362.

Šugman, Katja, Jager, Matjaž: Post 9/11 developments of the EU criminal law-related initiatives and their implications on some basic criminal law principles, v: Crime Business and Crime Money in Europe: The Dirty Linen of Illicit Enterprise (ur. P. C. van Duyne). Wolf Press, Nijmegen: Wolf 2007, str. 247–267.

Šugman, Katja, Gorkič, Primož: Dokazovanje v kazenskem postopku, GV Založba, Ljubljana 2011.

Cybercrimes: A Multidiciplinary Analysis, S. Ghosh, E. Turrini (ur.), Springer, Heidelberg, 2010.

Walden, Ian: Computer Crimes and Digital Investigations, Oxford University Press, Oxford 2007.

Wall, David S: Cybercrime, Polity Press, Cambridge 2007.

Walton, Reggie, B.: Prosecuting International Terrorism Cases in Article III Courts, v: Georgetown Law Journal Annual Review of Criminal Procedure, 39 (2010), str. iii–xxii.

Wilkins, Richard, G.: Defining the Reasonable Expectation of Privacy: An Emerging Tripartite Analysis, Vanderbilt Law Review, 40 (1987), str. 1077–1129.

Završnik, Aleš: Blurring the Line between Law Enforcement and Intelligence: Sharpening the Gaze of Surveillance?, v: Journal of Contemporary European Research, 9 (2013) 1, str. 181–202.

Zupančič, Boštjan M., in drugi: Ustavno kazensko procesno pravo, Pasadena, Ljubljana 2000.

Effects of Contemporary Technologies on Crime and Criminal Investigations

Summary

The author analyses the development of certain contemporary technologies which can be used by criminals while committing a criminal offence as well as by the law enforcement investigating those offences. No field of law can be immune from technological developments, but criminal law is particularly sensitive to it since new forms of criminal offences taking advantages of new technologies are constantly being invented. At the same time the state is looking for ways to use new technology in criminal investigations and also for the preventive surveillance of citizens. This article addresses some classical criminal law questions raised by this issue: (1) where does the border lie between effective criminal prosecution and the infringement of human rights law enforcement; (2) what is the role of judiciary in assessing this boundary; (3) which evidence gathered using new technological solutions may be produced as evidence in court?

The right to privacy, as a crucial legal concept can help us answer the question as to where a limit should be placed on the state's enthusiasm for investigating criminal offences. It presents a court with a duty to balance the two rights: right to privacy and the right to live in a safe society free of crime. The area of cybercrime poses a particular challenge to the right to privacy since this field of criminality has different characteristics to conventional crime. It is especially difficult to apply classic criminal law concepts to this field: for example the safeguard provided by a judicial warrant for house search. While investigating conventional crime criminal law attempts to protect privacy by specifying the location and the objects of the search. The purpose of this specification is to limit exactly the places police may search from those they may not and to define precisely what might be found there. The point of entrance therefore defines the boundary between the private and the public. This logic does not work in cyberspace: when a warrant states that it is possible to search a certain computer it is impossible to control what will be found there. The warrant therefore does not define the entrance spot and does not set a boundary between private and public areas, but is a purely technical condition for evidence-gathering to take place.

The next trend connected with new technologies lies with the opportunity they provide the state to perform preventive surveillance on a large scale in a way which avoids classical criminal law safeguards: the requirements that a judicial order (warrant) be issued and a specified evidential standard be met before a

certain investigative act may be conducted. It is becoming much easier to conduct general investigations which are indefinite in scale and nature without prior judicial control. As a result we live in a »surveillance society« where preventative measures may be used without the existence of specific level of suspicion (standard of proof). Legally the criterion which distinguishes investigative from preventative measures is the purpose for which they are conducted: preventative measures should be used for protecting the public and not searching for evidence. Some of those measures require special attention: the so-called »special need searches« (e. g. safety checks in airports or customs offices) which allow exemptions to the rule to proliferate, and other forms of the new technology use which threaten the right privacy as it has traditionally been defined: roving wiretaps, data-mining and the use of »protective technologies«. Such measures are all preventative and general, meaning that they are conducted without judicial approval, against masses of people not accused of any criminal offence. Such people are subjected to these measures simply because they find themselves in a certain place or use a certain device (e. g. a public computer). Research shows that such surveillance is ineffective in any case: despite its generality it only controls a minor segment of the population, resulting therefore in a minimal chance that offenders will be caught while making it very likely that professional offenders will use other ways of conducting their illicit activities. The result of those measures is therefore mostly data gathered through general surveillance from people who have not done anything wrong and an illusory sense of public safety.

There are two crucial questions regarding the use of these technologies in criminal procedure: (1) what are the procedural consequences of such use, especially with regards to data or evidence gathered by surveillance; (2) what is the role of the judiciary in keeping surveillance under control?

With regard to question (1), since the traditional procedural safeguards of criminal procedure have been undermined, the author takes the view that the balance of conflicting rights (i.e., to privacy and effective prosecution) must be achieved by focusing on the standards which should regulate the state's use of data gathered by new preventative measures utilizing new technologies. Firstly, the conditions for handling this sensitive data must be very strictly provided for and secondly, there must be a strict exclusionary rule for data which was not gathered in accordance with the given purpose of a specific surveillance measure. It is therefore only the exclusion of evidence which can guarantee that the state cannot profit from evidence gathered with over-extensive, general and preventative measures which circumventing all classical safeguards.

As for the second question, the author points out the worrying trend seen in some American courts, where the court gives up its judicial role by deciding not to weigh the reasonableness and necessity of a certain measure against the right to privacy. While weighing up these rights, the crucial question should be to what extent surveillance measures in fact prevent a certain danger (e. g. terrorist threats). Answering this question is the only way of assessing whether a certain measure is reasonable and necessary. Instead of deciding this question the courts chose to approve and *a priori* trust measures supported by claims that the executive branch knows best what is good for the security of the state.

History teaches us that the independent will of the judiciary is essential to control, assess and limit the acts of the executive branch if society is to remain democratic. The executive branch is certainly the most capable, motivated and best equipped to design different safety and security measures and new investigative authorizations, but whether these are proportionate and just it is the judiciary's prerogative to decide. Every new measure should be assessed carefully, rationally, and checked against the values of a certain society, proportionality and common sense based on real data. At first glance it may often seem that a certain measure is necessary to prevent a great harm, but frequently this is not true. These very invasive measures should only be adopted with an awareness of what they take from a democratic society – the right to privacy, the limits on the power of the executive - as well as the benefits they supposedly bring. No society is democratic if the measures protecting it leave very little freedom to defend.