Prikazi, ocene, recenzije

Stéphane Leman-Langlois (ed.): Technocrime. Technology, crime and social control

(Tehnokriminaliteta. Tehnologija, kriminaliteta in družbeni nadzor, Cullompton [England], Portland, Or.: Willan Publishing, 2008)

"Tehnokriminaliteta" obeta čtivo o kiberkriminaliteti (cybecrime), hiperkriminaliteti (hypercrime, McGuire) ali "visoko tehnološki kriminaliteti" (high-tech crime), naslov privabi predvsem bralce subkriminološkega geta, ki jih zanima kriminaliteta povezana s tehnologijo. Žal, saj je zbornik precej ambicioznejši in sega nad analizo fenomenologije posamične vrste kriminalitete. Povezuje temo tehnologije, prava in družbe, družbenega nadzora, kriminologije in deviantnosti. Ne analizira zgolj "tehnokriminalitete", oblike kriminalitete, ki se izvaja z ali zoper računalnike, temveč prikaže tudi spremembe, ki jih tehnologija prinaša za družbeno nadzorovanje (kar seveda ne pomeni zgolj odzivanja na kriminaliteto). Kakor v uvodu zapiše Gary Marx, zbornik opisuje, kako tehnologija briše meje časa, prostora, lastnine, obstoječih hierarhij, medosebne meje in meje med državami. Pokaže, kako "tehnološko nadzorovalni etos" razpira tradicionalno ločevanje javnega in zasebnega nadzorovanja kriminalitete, razlikovanje med kazenskopravnim sistemom in organi nacionalne varnosti, med kriminalitetno in obveščevalno politiko, med policijskim delovanjem in vojaškim posredovanjem, med organi kazenskega pregona in obveščevalnimi agencijami, med nacionalnimi in mednarodnimi oblikami uveljavljanja kazenskega prava ter med lokalnimi in mednarodnimi kriminalnimi dejavnostmi in organizacijami.

Zbornik kritično obravnava uvajanje različnih tehnoloških iznajdb v mehanizme "odkrivanja in pregona kaznivih dejanj", v mehanizme represivne moči države in v mehanizme delovanja korporacij ter nakaže procese "opolnomočenja" državljanov pri nadzoru oblasti. Tehnološke rešitve so vstopile v odnose moči med številnimi akterji (državami, podjetniškimi akterji, civilno družbenimi akterji itd.) in spreminjajo razmerja med posamezniki, med skupnostjo in posamezniki, kako misliti kriminaliteto, zločince, kazenskopravni sistem, ter dojemanje in odzivanje na deviantnost. Obseg vpliva tehnologije na kriminaliteto in na odzivanje nanjo ostaja danes večinoma neznan, zbornik pa z analizo, izvedeno na različnih ravneh splošnosti, in z analizo različnih vrst tehnoloških proizvodov, uporabljenih bodisi za izvrševanje kaznivih dejanj bodisi v postopku "spopadanja" s kriminaliteto (pogosto so metode enake, kakor kritično opozorijo avtorji pri analizi kibernetskega vojskovanja), kritično osmišlja prve epistemološke reze na kriminološkem podpodročju "tehnologija in kriminaliteta".

Hiter tehnološki napredek je v 20. stoletju sprožil potrebo, da je treba hitre in (pre)učinkovite rešitve osmisliti in ovrednotiti tudi z družbenega vidika, t. j. glede na učinke, ki jih ima tehnologija na družbo, na razmerja med posamezniki in na odnose moči v družbi. Tehnologija se namreč pogosto "zdravorazumsko" zdi kakor nekaj, kar je bliže naravnim kakor družbenim zakonom. Pogosto jo zaradi delovanja po fizikalnih zakonitostih dojemamo kot nekaj, kar najbolj poznajo naravoslovci in tehniki, ne pa družboslovci, ki so "zgolj" njeni uporabniki. A ta tehnična dovršenost posamičnih tehničnih proizvodov, ki sicer deluje po fizikalnih zakonih, ničesar ne pove o tem, kakšne učinke imajo, ko so umeščeni v družbeni prostor. Še več, tehnološki proizvodi so nastali in so oblikovani na način, ki ni odvisen samo od fizikalnih zakonov, temveč je bistveno soodvisen od številnih družbenih, gospodarskih, političnih in kulturnih dejavnikov. Določen tehnični proizvod (na primer steklenica za vodo) je rezultat kulturne zaznave (na primer tega, kaj je "kulturno" ali "primerno" pitje), gospodarske učinkovitosti (da je na primer steklenico v določeni družbi v določenem trenutku mogoče izdelati glede na cene produkcijskih faktorjev), družbeno moč gospodarskih subjektov (na primer steklarn pred podjetji, ki se ukvarjajo s polimeri) itn. Steklenica je v obliki, kakršno poznamo, oblikovana ne zato, ker bi bila ta oblika ali steklo najbolj tehnično primerna ali "najboljša" s tehničnega vidika . Nasprotno, takšna oblika morda po fizikalnih zakonih niti ni najboljša (morda je celo nefunkcionalna, kakor na primer opozarjajo naravovarstveniki za plastične "steklenice"), a takšna oblika in snov sta v določenih družbenih okoliščinah obveljali kot "pravi".

Poanta je seveda v tem, da ni samo zločin, kakor je prepričljivo pokazala že teorija etiketiranja, družbeni proizvod, temveč so tudi različni tehnološki proizvodi, kakor so internet, video nadzorstvene kamere, navigacija GPS, satelitsko cestninjenje itn., ki vstopajo v mehanizme družbenega nadzora, tudi družbeni proizvodi. Ali z besedami Leman-Langloisa (s. 2): tehnologijo predstavljajo objekti, ki jih ni lahko opazovati ali meriti. To so sociološki objekti: spreminja jih kultura in tudi sami povratno spreminjajo kulturo. Pri opazovanju pomena tehnologije za kriminaliteto in odzivanje nanjo lahko zato pridemo do povsem nasprotujočih ugotovitev o njenem pomenu. Tako kakor ugotavlja Leman-Langlois, tehnologijo na področju kriminologije lahko razumemo na naslednje nasprotujoče si načine:

1. Tehnologija omogoča nove načine izvrševanja kaznivih dejanj: tehnološki pripomočki, kakor so na primer prenosni telefoni, omogočajo učinkovito, hitro in prožno dogovarjanje pri izvrševanju kaznivih dejanj. Policijsko sledenje geografsko razpršenim in mobilnim članom kriminalne združbe je zelo težavno, njihovi načrti se hitro spreminjajo, kar omogoča brezžična komunikacija v "realnem" (*real-time*) času.

2. Tehnologija omogoča nove načine odzivanja na kriminaliteto: po drugi strani je tehnologija okrepila (razširila in poglobila) policijsko delovanje. Na primer satelitska navigacija (GPS) omogoča sledenje označenim predmetom in vozilom, zaščita digitalnih avtorskih del je mogoča s tehnološkimi blokadami, podatke v komunikacijskih omrežjih pa je mogoče prestrezati in shranjevati ter oblikovati obsežne zbirke podatkov, nato pa preventivno v njih iskati vzorce vedenja posameznikov.

3. Tehnologija predstavlja novo grožnjo nacionalni varnosti: ocene, da se bliža "kibernetski cunami", ki bo v enem valu onemogočil delovanje kritične nacionalne infrastrukture (na primer dobavo električne energije, vodovodne sisteme, letalski promet), so precej pogoste, naravnane pa so na mobilizacijo javnosti in prerazporeditve javnih finančnih sredstev v vlaganje v tehnološke zaščite teh infrastrukturnih sistemov.

4. Tehnologija ponuja nove možnosti za zaščito nacionalne varnosti: zbirke podatkov o naših nakupovalnih navadah (na primer s karticami zvestobe), o našem fizičnem gibanju (na primer s sledenjem našim prenosnim telefonom, ki jih zvesto nosimo s seboj), o naših elektronskih komunikacijah (na primer s hrambo prometnih podatkov) itn., omogočajo nepredstavljive zmožnosti preventivnega in obveščevalnega delovanja, ki se nanaša na vsakogar izmed nas.

5. Tehnologija predstavlja nove možnosti za kršenje temeljnih človekovih pravic in svoboščin: fizično nadzorovanje z nadzorstvenimi kamerami, sistemi za prepoznavo obraza, biometrične metode identifikacije, sledenje s čipi RFiD itn. omogočajo oblikovanje osebnih profilov o posameznikih, poseg v zasebnost, ustvarjajo nove vednosti o posamezniku, njegovih navadah, interesih, nazorih.

6. Tehnologija predstavlja nove možnosti za zaščito temeljnih človekovih pravic in svoboščin: na drugi strani tehnološke rešitve, kakor so avtomatizirani sistemi za identifikacijo in avtentikacijo omogočajo nediskriminatorno delovanje.

Opisane ocene učinkov tehnologije so zato lahko pravilne, čeprav si nasprotujejo. Bistveno je, da sta tehnologija in tehnokriminaliteta gordijski vozel političnih in gospodarskih interesov, pravnih pravil in tehnološkega razvoja, križišče interesov različnih akterjev, od policije, zasebne varnostne industrije in forenzičnih strokovnjakov, in odražajo masovne individualne želje, geopolitične strategije in druge oblike moči.

Zbornik (259 strani) ima deset poglavij, z urednikovim uvodnim in zaključnim poglavjem, ter predgovorom, prispevke pa je pripravilo 12 avtorjev. Vsako poglavje navaja seznam literature, na koncu je dodano stvarno kazalo.

Zbornik obravnava stičišče tehnologije, kriminalitete in družbenega nadzorstva večplastno. Ker gre za zbornik prispevkov in ne za sistematično in izčrpno analizo vseh oblik tehnokriminalitete in tehnološko podkrepljenega odzivanja nanjo ("*technopolicing*"), je skupni imenovalec vseh prispevkov v cilju in vrednotah, ki vodijo pisce. Glavna ugotovitev, ki jo povzema urednik zbornika, je, da "*technopolicing* ne deluje":

1. ne zmanjšuje kriminalitete, ne zmanjšuje strahu pred kriminaliteto, akterjem in pravnim odločevalcem v kazenskopravnem sistemu pa ne prinaša večjega zadovoljstva z njihovim delom,
2. na tehnični ravni in iz povsem tehničnih razlogov ne deluje (na primer video nadzorstveni sistemi so slabo vodeni, sistemi imajo slabo kakovost slike, če pa je razpoznavnost dovolj visoka, ni dovolj tistih, ki bi uspeli vse to nadzirati), in
3. ker ne ustreza predstavam, ki jih ima policija o svojem poslanstvu.

Zbornik po uvodnem poglavju predstavi optimistično analizo Davida Brina "Crime and lawfulness in the age of all-seeing techno-humanity", kjer avtor tehnologijo daje v roke državljanom. Nasproti tezi o povečanem nadzorovanju v "informacijski družbi" postavi tezo, da je zaradi večje demokratizacije pri uporabi tehnologije ta lahko tudi sredstvo v rokah šibkejšega posameznika nasproti državi. Tehnologija vsebuje tudi možnost, da jo uporabimo kot sredstvo nasprotnega vohunjenja, gledanja pod prste tistim, ki naj bi nas nadzorovali ("*counter-surveillance*"). Bistvo tiranije, kakršno ponazarja Orwellov Veliki brat, je, da tisti "zgoraj" (nadzorniki) gledajo in pri tem niso vidni, torej se izognejo odgovornosti za svoje početje. Prav demokratizacija in dostopnost tehnologije vsakomur pa bi omogočali, da posamezniki in skupine z družbeno močjo upoštevajo pravila strokovnosti, drugače jih bodo uporabniki oziroma državljani sami odkrili in jim odvzeli moč, ki jim je bila zaupana. Tehnologija naj zato ne bi bila vnaprej slaba ali naperjena proti posamezniku. Avtor se zavzema za cilje gibanja "vseprisotnega pogleda" ("sousveillance movement") Steva Manna, po katerem bi morali državljani prevzeti nalogo gledanja "od spodaj" in s tem potrjevati, da smo suvereni, in ne brezupne ovce, ki jim vladajo drugi.

Poglavje "The local impact of police videosurveillance on the social construction of security" avtorja Leman-Langloisa

predstavi izsledke empirične študije zaznave in učinkov video nadzorstvenega sistema v Montrealu. Glavne ugotovitve niso presenetljive in so v skladu z znanstveno metodološko pravilno izvedenimi študijami video nadzorstvenih sistemov po vsem svetu: da so nadzorstvene kamere nepomembne glede zaznave (ne)varnosti. Občutek (ulične) varnosti pogojejo drugi dejavniki, kakor so na primer vidni znaki vandalizma, grafiti, uporabljene na tleh ležeče igle ipd. Varnostne kamere so tako kakor druge oblike tehnologije nevtralne v tehničnem smislu, a ne obstajajo v nevtralnem prostoru. Raziskava je pokazala, kako se zaznave ljudi, ki živijo v različnih delih mesta, zaradi varnostnih kamer spreminjajo: nekaterim so v opozorilo, da živijo v nevarnem delu mesta (kar pomeni, da kamere še povečujejo strah pred kriminaliteto), drugim, da se policija boji patruljiranja po ulicah in se s tem odtujuje od dejanskega dogajanja (skratka, kamere navajajo na misel, da na policijo ob težavah ni mogoče računati). Še največjo stopnjo zadovoljstva kažejo lastniki trgovin, ki na "svojih" ulicah ne želijo skvotarjev, žeparjev, postopaške mladine in preprodajalcev mamil, ker to povzroča strah med njihovimi potencialnimi strankami. Glavna ugotovitev avtorja je, da so kamere preprosto nepomembne za življenje in varnost na območjih, kjer so nameščene.

Benoît Gagnon v poglavju "Cyberwars and cybercrimes" prikaže trend militarizacije interneta: države, ki ob nastanku interneta niso imele pretiranega interesa za njegovo delovanje, so danes po komercializaciji interneta zainteresirane za suverenost tudi v tem "prostoru". A ta "prostor" zaradi decentraliziranega načina tehničnega delovanja uhaja običajnim koncepcijam suverenosti in "nacionalnega" prostora. Koncept "kibernetske varnosti" ("cybersecurity"), ki označuje državne težnje povečevanja navzočnosti in nadzora v kibernetskem prostoru, dobiva vedno večji pomen, in avtor pokaže, kako uspešni sta pri tem ZDA in Kitajska. Število državnih agencij in organov, odgovornih za uveljavljanje moči v kibernetskem prostoru, je v teh državah približno enako: 30.000 kitajskih državnih uslužbencev sistematično nadzoruje elektronsko pošto, pogovore na forumih in druge *on-line* dejavnosti državljanov, podobno število nadzornikov pa je tudi v ZDA, kjer so v "boj" zoper kibernetsko kriminaliteto vključene: Department of Justice, FBI, Department of Homeland Security, Department of Defense, Federal Trade Commission, Federal Inspectors General itd. Boj za oblast se je preselil tudi v kibernetski prostor. Prihaja do brisanja meja med kibernetskimi kaznivim dejanji, kibernetskim terorizmom in kibernetskim obveščevalnim delovanjem držav: kar je posameznikom prepovedano, izvajajo države v imenu nacionalne varnosti.

Poglavje "Policing through nodes, clusters and bandwidth", katerega soavtorja sta Johnny Nhan in Laura Huey, analizira odzivanje na kibernetsko kriminaliteto, za katero se je v kriminološki teoriji uveljavil izraz "*surveillant assemblage*". Policija in drugi akterji kazenskopravnega sistema, zasebna varnostna podjetja, posamezniki, civilne organizacije itn. sodelujejo pri uveljavljanju reda v kibernetskem prostoru. Mrežni in vozliščni modeli upravljanja z odklonskostjo, kjer prihaja do "javnozasebnega" partnerstva med organi, tradicionalno odgovornimi za odkrivanje in pregon kaznivih dejanj, in med novimi državnimi, paradržavnimi, zasebnimi in civilnimi organizacijami, ki so vključene v opravljanje policijskih in varnostnih dejavnosti in nalog. Akterji, katerih delovanje je podrobno analizirano, so: organi odkrivanja in pregona kaznivih dejanj, vlada, zasebna industrija in javnost.

Poglavje "Second Life and governing deviance in virtual worlds", katerega soavtorja sta Jennifer Whitson in Aaron Doyle, je kibernetsko v drugem pomenu: analizira "teritorij" prosto dostopnega virtualnega sveta podjetja Linden Lab z imenom "Second Life". Avtorja iščeta odgovor na vprašanje, kakšna sta zločin in kazen v virtualnem svetu. Ali tam prav tako prihaja do oblikovanja pravil in njihovih kršitev? Kako se stanovalci virtualnih skupnosti odzivajo na kršitve, kaj počnejo s kršilci?

Poglavje Leman-Langloisa "Privacy as currency: crime, information and control in cyberspace" ponuja novo pojmovanje zasebnosti, ki je domnevno najbolj ogrožena temeljna človekova pravica v "informacijski družbi". A vendar avtor ugotavlja, da je napadeno le obstoječe pojmovanje zasebnosti. Pomen zasebnosti, razmerje med javnim in zasebnim ter naše samodojemanje se v internetnih svetovih spreminjajo. Avtor ponuja razumevanje zasebnosti kot valute, kot dobrine, s katero trgujemo: za večje udobje smo pripravljeni žrtvovati tudi delček naše zasebnosti. Na primer na letališču lahko čakamo v vrsti nekaj ur, če pristanemo na biometrično identifikacijo, pa smo na vrsti v nekaj minutah: kaj bomo torej izbrali? Zasebnosti ne pojmuje kot našega notranjega svetišča, kamor nima nihče dostopa, temveč kot lastnino, ki jo zadržujemo tako dolgo, dokler zanjo nekaj ne dobimo v zameno.

Informacijska tehnologija je temeljito spremenila policijsko delovanje in delovanje organov odkrivanja in pregona kaznivih dejanj in poglavje avtorja Frédérica Lemieuxa "Information technology and criminal intelligence: a comparative perspective" analizira te spremembe. Zbiranje, shranjevanje, analiziranje ter izmenjava podatkov in informacij o kaznivih dejanjih in storilcih niso novi in niso značilni samo za sodobno policijsko delovanje. A vendarle velike količine podatkov (ki obsegajo v posamičnem kazenskem primeru lahko tudi nekaj terabajtov) o posameznikovem delovanju, ki jih doslej ni bilo mogoče sistematično analizirati (na primer vzorce gibanja in sledenja s programsko opremo, povezano z video nadzorstvenimi sistemi) in celo ustvarjanje novih podatkov

o posamezniku (ki se jih ta niti sam ne zaveda; na primer z rudarjenjem (*data mining*) in povezovanjem podatkov iz različnih zbirk podatkov) so danes nekaj novega. Obveščevalno policijsko delovanje je pridobilo pomen in predstavlja prototip novega policijskega delovanja.

Poglavje "Scientific policing and criminal investigation" avtorja Jean-Paula Brodeurja je študija policijske uporabe forenzike in drugih tehnologij, uporabljenih pri odkrivaju in pregonu kaznivih dejanj umora. Visoko tehnološko opremljeni kriminalisti se v preiskovanje kaznivega dejanja vključijo šele na koncu, ko so vse druge preiskovalne metode že odpovedale. A kakor ugotavlja avtor, tudi te visoko tehnološke preiskovalne metode pogoste odpovedo, vendarle je njihova odpoved veliko dražja.

David Lyon v poglavju "Sorting systems: identification by database" analizira vpeljavo osebnih izkaznic v 20. stoletju in metode sortiranja, klasificiranja in nadziranja populacije, ki so temeljna značilnost moderne države. Avtor kritično ovrednoti povečevanje zahtev, bodisi iz političnih, gospodarskih ali birokratskih razlogov, ki jih države nalagajo državljanom, ne da bi se pri tem kakor koli upoštevalo družbene, politične in zlasti kulturne stroške in pomanjkljivosti. Boj zoper povečevanje obveznosti osebnega identificiranja na vsakem koraku je zanj boj zoper poživinjenje (nič presenetljivega, če vemo, da se je večina tehnološko sofisticiranih sledilnih naprav razvila prav pri sodobni vzreji živine).

Zadnje poglavje Petra Manninga "A view of surveillance" predstavlja svojevrstno streznitev: dejansko policijsko delovanje je še vedno usmerjeno v tradicionalne naloge. Tehnično dovršeno delovanje policije ostaja neizvedljivo v praksi, saj tehnologija (še) ni dovolj zanesljiva, boji za moč, pomanjkanje interesa zaposlenih, nezdružljivost tehnoloških rešitev itn. so dejavniki, ki policijsko delo in naloge ohranjajo v okviru že preživetih doktrin policijskega dela.

Tehnokriminaliteta ("*technocrime*") in tehnološko podkrepljeno odzivanje nanjo ("*technopolicing*") sta abstraktna pojma, ki kazenskopravne dogmatike puščata hladne. A pojma sta namenoma oblikovana tako, da omogočata vključitev novih, še neobstoječih ali še nepojasnjenih oblik kriminalitete povezane s tehnologijo in tehnološko podkrepljenega odziva nanjo. Omogočata razumeti kriminaliteto, delinkvenco in nadzorovanje v pogojih povečane uporabe domnevno objektivnih, a dejansko politično, interesno in vrednostno pristranskih tehnoloških instrumentov in rešitev. Kakovost zbornika se kaže v njegovi kritičnosti do tehnološko podkrepljenega nadzora, ki s proizvodnjo vedno novih tehnoloških naprav morda ustvarja v sodobni družbi sicer močno želeni cilj — gospodarsko rast, a glede razumevanja kriminalitete in primernosti odzivanja nanjo z vidika dolgoročnega ohranjanja relativnega družbenega miru učinkuje v nasprotni smeri od želene, ustvarja več težav, kakor jih rešuje. Pomanjkljivost zbornika je njegova necelovitost, analiza izredno raznolikih tehnoloških pojavov, ki imajo razen elektronskih vezij le malo skupnega. Analiza nekaterih avtorjev je izredno splošna in abstraktna, drugih pa municiozna in preveč usmerjena v podrobnosti. Kar ni samo po sebi pomanjkljivost nobenega posamičnega prispevka, a vendarle daje vtis "nezaokrožene", nekonsistentne obravnave tematike.

dr. Aleš Završnik