

David S. Wall: *Cybercrime: The Transformation of Crime in the Information Age*

(Kibernetska kriminaliteta: Preobrazba kriminalitete v informacijski dobi, Cambridge, Malden: Polity Press /Crime and Society Series/, 2007.)

Raziskovalna domena, ki vznika na križišču kriminalitete in tehnologije, postavlja pod vprašaj doslejšnja razumevanja kriminalitete in odzivanja nanjo. Na primer temeljno načelo sodobnih kazensko-pravnih odzivov na kriminaliteto *de minimis non curat lex* v času avtomatizirane kibernetske kriminalitete (tj. minornih, a množičnih viktimizacij) postavlja pod vprašaj lokalizirano osredotočanje kazensko-pravne mašinerije. Danes namreč posamezniku ni več potrebno storiti enega ropa za milijon evrov, temveč lahko do enakega cilja pride z avtomatizirano izvršitvijo milijon tatvin po en evro na različnih koncih sveta. Tovrstna »prava« kibernetska kazniva dejanja zato spreminjajo odgovore na vprašanje, kdo in kako naj preprečuje tovrstne »podjetniške« podvige: ali je to po regionalnem (nacionalnem) principu organizirana (lokalizirana) policija, ki še vedno v veliki meri sloni na paradigmi, ki izhaja iz njene zgodovinske naloge »odganjanja nevarnih razredov z ulic«, ali pa nemara kaže tovrstne nevarnosti prepustiti kar tehnologiji sami, na primer programom za filtriranje e-poštnih sporočil po ključnih besedah? Ali se torej kaže zavzeti za popolno odpravo vseh deviantnih ravnanj v kibernetskem prostoru s tehnološkimi ukrepi, ki jih je mogoče vtakati v »arhitekturo« kibernetskega prostora ali pa nasprotno kaže tolerirati določena nevarna ravnanja in s tem omogočiti večjo raven svobode in enakost med uporabniki?

Publikacija prek navidezno manj pomembnih problemov (kot je neželena e-pošta) odstira bolj temeljna vprašanja nadzora kibernetskega prostora in zagotavljanja temeljnih človekovih pravic in svobod v kibernetskem prostoru oziroma pri njegovi »uporabi« (na primer pravico do zasebnosti, svobodo govora, enakosti). Avtor izhaja iz t.i. »transformacijske teze«, po kateri kibernetska kriminaliteta spreminja delitev dela in procese izvrševanja kaznivih dejanj, zagotavlja nove priložnosti in tudi nove oblike kaznivih dejanj. V skladu s to tezo označuje za »pravo« kibernetsko kriminaliteto zgolj dejanja, ki umanjajo, če iz »enačbe« odstranimo informacijsko-komunikacijsko omrežje.

Transformacijska teza, na katero prisega avtor, omogoča predstavitev razvojnih dimenzij kibernetske kriminalitete in konceptualizacijo izjemno heterogene množice deviantnih ravnanj. Omogoča predstavitev paradoksalnega učinka tehnologij, ki po eni strani predstavljajo nove kriminalne priložnosti in ustvarjajo nove oblike kriminalitete, po drugi strani pa te

iste tehnologije omogočajo tudi povsem nove (»orwellovske«) priložnosti za nadzorovanje.

Publikacija je strukturirana zelo pregledno, po sklopih, ki predstavljajo temeljne izzive za kriminološko preučevanje novih pojavnih oblik kriminalitete, tj. kaj sploh predstavlja to novo pojavno obliko kriminalitete in kako se nanjo (naj) družba odziva. Predstavlja torej fenomenološka, etiološka in kriminalitetnopolitična vprašanja, povezana s kibernetsko kriminaliteto, bistvena kakovost publikacije pa je perspektiva, ki končna vprašanja nadzorovanja in »upravljanja« locira v kombinacijo (kazensko in civilno) pravne justice in nad/izvenpravnih mehanizmov. Konkretnije to pomeni, da upravljanje in nadzorovanje kibernetskega prostora ne mora biti izključna odgovornost/dolžnost akterjev kazensko-pravnega sistema na eni in tudi ne varnostnih (tehničnih) ekspertov na drugi strani. Publikacija je spisana tekoče, številne splošne ugotovitve pa so ponazorjene s konkretnimi primeri in to na način, ki je razumljiv tudi »povprečnemu« internetnemu uporabniku.¹

V poglavju *Razumevanje zločina v informacijski dobi* prikazane dileme dovoljujejo sklep, da v bližnji prihodnosti še vedno ni pričakovati bolj »stabilnih« opredelitev tega fenomena. Nove tehnologije vedno znova *ex post* spreminjajo naš zorni kot in prejšnje konceptualizacije postavljajo pod vprašaj. Ta del je kljub navidezno suhoparni »definijski« naravi presenetljivo razgiban. Avtor prikaže zapletene procese produkcije vednosti o tem, kaj je »kibernetsko« (»cyber«), in raznoliko naravo vednosti o tem, kaj je kibernetski kriminal. Prikaže razvoj akademskega diskurza o tehnologiji (na primer računalniško pravo, preučevanje vplivov tehnologije na družbo), ki sega vse do frankfurtske šole (ta obravnava tehnologijo kot sredstvo racionalizacije moči kapitala s specializacijo dela in zmanjševanjem stroškov proizvodnje), katere zavest o pomenu tehnologije se je kasneje prenesla v pravno-sociološke

¹ Žal se je pri predstavitvi tematike, povezane s sodobno informacijsko-komunikacijsko tehnologijo, v slovenščini številnim anglicizmom (in še skovankam povrh) zelo težko izogniti, zato naj mi bralka in bralec oprostita. Povečan trud bi zahteval pisanje večjih delov besedila v navednicah, ob dodatni pretnji z nejasnostjo pri pojmi, ki so postali *terminus technicus*. Koristen pripomoček predstavlja slovensko-angleški terminološki slovar informatike Islovar, dosegljiv na URL www.islovar.org.

diskurze o svobodi izražanja, o zasebnosti in o temeljnih človekovih pravicah in svoboščinah.

Glavna vrednost tega dela se nanaša na identifikacijo štirih diskurzov o kibernetiki kriminaliteti, sklopov misli o tem, ali ta sploh predstavlja »problem«, kako jo opredeliti, kakšne so njene oblike itn. Gre za diskurze, ki vsebujejo različne fenomenološke, etiološke in epidemiološke razlage ter odgovore na vprašanje, kako naj se družba in kazenskoopravni sistem na kibernetiko kriminaliteto odzivata. Ti diskurzi so (a) zakonodajni/administrativni, (b) akademski, (c) ekspertni in (č) popularni, emocionalni ali laični diskurz, ki si pogosto nasprotujejo. Wall tako na primer opozarja na navzkrižja med laičnim diskurzom o kiber kriminaliteti, ki ga v pretežni meri oblikujejo senzacionalnih novic že(lj)ni mediji, in akademskim diskurzom. Slednjega opredeljuje kot diskurz, ki išče kriminološke, pravno-sociološke, sociološke, računalniške, ekonomske ali tehnične razlage tega, kar se je sploh zgodilo. Te razlage v nasprotju z medijskimi obravnavami posamičnih primerov opozarjajo, da je kibernetike kriminalitete razmeroma malo, da je relativno nepomembna v primerjavi z drugimi hujšimi oblikami kriminalitete ipd. Nasprotja avtor ugotavlja tudi med akademskim in ekspertnim diskurzom. Zadnji je namenjen raziskovanju trendov v pojavnih oblikah in razsežnostih kibernetike kriminalitete, da bi lahko zagotovil razlage za ozaveščene odločitve. A gonilna sila ekspertnih razmislekov so prepogosto ekonomski izračuni varnostne industrije (zaščitne programske opreme), ki je zato prepogosto nagnjena k pretiravanju v ocenah varnostnih razmer v kibernetičnem prostoru.

Prikaz prepletov med različnimi diskurzi o kibernetiki kriminaliteti predstavlja svojevrstno kulturno in medijsko analizo. Avtor na primer prikaže različne medijske etike o kibernetiki kriminaliteti (kot na primer »Cyber-Tsunami«, »Electronic Pearl Harbor«, »Cyberia«) in različne filmske reprezentacije kibernetičnih delinkventov. Tovrsten imaginarij šoka, ki se ustvarja, namreč povečuje tesnobo javnosti ob posamičnih primerih in implicitno vsebuje mandat oblastem za strožje ravnanje/kaznovanje s kiber kriminalci. Čemur smo danes priča pri regulaciji kibernetičnega prostora, je zato po avtorjevem mnenju »ideologija regulacije«, krojena po potrebah državne oblasti in korporativnih interesov na račun temeljnih človekovih pravic in svoboščin.

V tretjem poglavju *Kibernetični prostor in transformacija kriminalne aktivnosti* avtor odgovarja na vprašanje, kako so mrežne tehnologije ustvarile nove priložnosti kriminalnih dejavnosti. Transformacijske učinke kibernetičnega prostora presoja po omenjenem transformacijskem testu: da neko dejanje označimo za dejanje kibernetične kriminalitete, mora njegov konstitutiven del predstavljati mrežna tehnologija. Pri iskanju nujnih lastnosti kiber kriminalitete izhaja iz Castellsovih ugo-

tovitev iz trilogije *The Information Age*,² na primer o vplivu kibernetičnega prostora na posameznika, njegovih pojmov, kot so mrežna družba, informacijska ekonomija itd. Sledječ Castellsu analizira tri vrste sprememb, ki učinkujejo na kriminalne priložnosti v kibernetičnem prostoru in ki hkrati predstavljajo temeljne značilnosti kibernetične kriminalitete: omrežnost, informacijskost in globalnost. V nadaljevanju avtor te tri elemente aplicira na kiber kriminaliteto in njene transformacijske učinke kriminalne aktivnosti.

Preobrazba se kaže v (1) organizaciji kriminalne dejavnosti. Posamezniku tehnologija nudi večji nadzor nad izvedbo kriminalnega dejanja, dejanja lahko dodatno izvršijo tudi posamezniki, ki pred tem niso imeli zadostnih resursov (organizacijske, finančne moči) za izvedbo dejanja. Avtor tako transformativne učinke identificira v novih oblikah kriminalne organizacije, v katerih sodelujejo različne prestopniške skupine, v uveljavljanju mrežne organiziranosti skupin, veliki specializaciji dela in tudi v učinku izgube in pridobitve novih veščin (»*deskilling & reskilling effect*«).

(2) Transformacija se nadalje kaže v obsegu kriminalnih priložnosti. Pri prvi generaciji kibernetične kriminalitete so bili računalniki uporabljeni kot »zgolj« pomožna sredstva za izvrševanje kaznivih dejanj. Omrežne tehnologije so sicer omogočale izvršitve kaznivih dejanj, a niso bile njihov nujni pogoj. Če omrežno tehnologijo umaknemo iz enačbe, tovrstne oblike kriminalitete ostanejo. Druga generacija kibernetične kriminalitete odraža nove priložnosti za izvrševanje kriminalnih dejanj kot na primer *hacking* (etično motivirana dejanja, navdahnjena s protikulturnimi idejami šestdesetih, z zavestjo o političnih svoboščinah in suspektnostjo do vlad in korporacij) in *cracking*. Ta dejanja so bila po avtorjevem mnenju »zgolj« »hibridna« oziroma »prilagojena« (McQuade). Brez omrežja bi še vedno obstajala. Avtorjevo klasificiranje je na tem mestu nekoliko nekonsistentno in kaže določeno mero poenostavljanja. Gotovo vsaj za *hacking* in *cracking* velja, da izgine, če »iz enačbe odstranimo omrežno tehnologijo«, kar bi pomenilo, da gre za »pravo« kiber kriminaliteto. Kvalitativno transformacijo kriminalnih aktivnosti za Walla predstavlja šele t.i. tretja generacija kibernetične kriminalitete. Ta združuje avtomatizirana in »distribuirana« dejanja, katerih vpliv se potencirana z razvojem širokopasovne povezave. Gre za primere dejanj vedno manj odvisnih od »socialnega inženiringa«³ in oblikovanje

² Del trilogije je predstavljen v Reviji za kriminalistiko in kriminologijo, let. 57, št. 3 (jul. –sept. 2006), str. 290–293.

³ Modni pojem »socialni inženiring« označuje dejstvo, da na primer vdor v računalniški sistem ni uspel s tehničnimi mahinacijami, temveč s prelisičenjem uporabnika, da je tretjemu zaupal podatke za vstop (na primer uporabniško ime in geslo). Ne gre torej za tehnične, temveč za socialne veščine.

mrež »ugrabljenih« računalnikov (*botnets*).⁴ To so torej računalniki, ki so še vedno v (realni) posesti uporabnika, a ki ob izvajanju njegovih ukazov izvajajo še druge naloge, za katere ta niti ne ve, da se izvajajo na njegovem sistemu (to se na primer odraža v bolj počasnem delovanju računalnika). Šele ta dejanja tretje generacije so lahko storjena zgolj v kibernetnem prostoru.

Transformacija kriminalne aktivnosti pa se nazadnje kaže tudi (3) na materialnem področju z nastankom novih oblik kriminalitete, tj. kriminalitete, naperjene zoper integriteto računalniškega sistema (*computer integrity crime*), kriminalitete, povezane (olajšane) z računalniki (*computer-mediated/assisted/related crime*), in kriminalitete, povezane z vsebino (*content-related crime*). Meje med njimi postajajo vse bolj nejasne, kljub temu pa avtor v četrtem, petem in šestem poglavju natančno predstavi pojavne oblike vseh treh skupin.

V poglavju o *kriminaliteti, naperjeni zoper integriteto računalniškega sistema*, avtor obravnava različne oblike *hackanja* in *crackanja*. Analizira motivacijo, stratifikacijo *hackerjev* in *crackerjev*, razvoj *hackerstva*, distinkcije med »*white hat hackers*« kot etičnimi delinkventi in »*black hat crackers*« kot neetičnimi delinkventi, med utopisti, kiber-punki, »*script kiddies*«, kiber-vojniki in kiber-teroristi. Pri tem ostaja kritičen do socialne skonstruiranosti (etiket) kibernetnih delinkventov. Del je namenjen tudi predstavitvi hekerskih taktik onesposabljanja s socialnim inženiringom, vohunsko in nadzorovalno programsko opremo, z uporabo zlonamerne programske opreme (trojanski konji) in zlonamerne kodo (črvi in virusi) ter DDoS napadom (*distributed denial of service attack* oziroma *cyber-barrage*).

Osrednji del predstavitve oblik *kriminalitete, povezane z računalniki*, je namenjen obravnavi virtualnega bančnega ropa in virtualnim tatvinam (informacijske in intelektualne lastnine). Poglavje je precej kazuistično, a je morda ravno v tem njegova kvaliteta: na enem mestu je predstavljena fenomenologija tovrstne oblike kibernetne kriminalitete, ki je gotovo znana zgolj posebej zainteresiranim bralcem. Poleg predstavitve virtualnega bančnega ropa (bolj znanega kot kraje identitete oziroma goljufije, kot bi dejali v naši kazenskopравни terminologiji), ki izkorišča finančne *online* sisteme bank in e-podjetij, avtor tehnično poglobljeno analizira številne vrste goljufij:

(1) *input* goljufije, ki so lahko izvršene s (a) *trashingom* (oziroma »smetiščnim potapljanjem« /*«dumpster diving»*/, beri: brskanjem po zavrženih listinah), (b) *phishingom*, ki temelji na uporabnikovi nezmožnosti prepoznati resnično sporočilo od lažnega (na primer bančna spletna stran se predstavlja in zgleda kot prava, čeprav gre za ponarejen duplikat), (c) *pharmingom*, kot avtomatizirano obliko *phishinga* in (č) z uporabo vohunskega programja (*spyware*);

(2) *output* goljufije, storjene z uporabami kreditnih kartic, pridobljenih na nelegitimni način, in plačilne prevare v sistemih, kjer kartica za plačila ni podana na vpogled (t.i. »*card-not-present payment frauds*«);

(3) izigravanje pravil trga oziroma pravil, ki veljajo na določenem teritoriju. Čezmejna narava interneta omogoča izigravanje pravil glede dovoljenosti prodaje farmacevtskih proizvodov, dragih kamnov, antikvitet, telesnih delov, spolnih uslug, iger na srečo ipd. Sem sodijo še internetne oglaševalne goljufije, ki se nanašajo na »*pay-per-click*« reklame, prevare sistemov upravljanja ugleda (na primer na e-Bay) s t.i. »*short-firm fraud*«, ko je ugled prodajalca, ki ga vsakokratni kupci ocenjujejo, lažno velik, da bi lahko nato na koncu prodajalec izvedel goljufijo;

(4) goljufije v e-trgovini, kot so piramidne prodaje, investicijske prevare, ugodna kreditiranja, zavajajoča oglaševanja (za domnevno dobrodelne namene, lažne loterije ipd.), avkcijske goljufije, nigerijske goljufije oziroma prevare,⁵ ki od uporabnika zahtevajo predujem (članarino), ki naj bi ji domnevno sledilo nakazilo ogromne vsote denarja;

(5) kršitve intelektualne (informacijske) lastnine: avtor prepričljivo opozori na probleme neuravnotežene kazenskopravne zaščite imetnikov pravic intelektualne lastnine. Omembe vredna je zlasti ugotovitev, da ideje, ki niso več nujno vezane na mehansko proizvedene procese, postajajo »nepremičnine« kibernetnega prostora, kar olajšuje razumevanje boja za nadzor na temi »intelektualnimi nepremičninami«. Posebej obravnava primer glasbe, videa in programske opreme, dilem, povezanih s P2P (*peer-to-peer*) tehnologijo, kjer opozarja na dinamiko moči med kulturno in programsko industrijo in v medijih ustvarjen (pristranski) imaginarij o povezanosti piratstva z organiziranim kriminalom in terorizmom.

V poglavju o *kibernetki kriminaliteti, povezani z vsebino*, so obravnavani že uveljavljeni konceptualni sklopi. (1) Obsceno gradivo oziroma »ekstremni seksualni imaginarij«, kot ga imenuje Wall, in otroška pornografija: povezava

⁴ Bot (okrajšava za robot) so programski roboti, ki delujejo povsem samostojno tako, da vprežejo in izkoriščajo mreže okuženih in prevzetih računalnikov (v računalniškem žargonu imenovanih *zombiji*). *Botnet* je mreža takšnih prevzetih in na daljavo vodenih *zombijev*.

⁵ Izvirajo iz Nigerije in se nanašajo na 419. člen Kazenskega zakonika Nigerije.

interneta s pornografijo je dobro znana, gotovo jo nazorno ponazarja podatek, da je bila beseda »pornografija« do leta 1999 najbolj iskan pojem internetnega brskanja. Kakor koli je pornografija predstavljala »gorivo« internetnemu razvoju in komercialni ekspanziji, je kasneje postala argument proti razširjanju interneta, ker naj bi spolni iztirjenci čakali mladino za vsakim klikom. V tem sklopu avtor obravnava pornografijo po kazenski zakonodaji VB in ZDA in predstavi nekatere sodne primere, hkrati pa analizira tudi nadpravne vidike pornografije. Predstavi konkretne primere odkritja t.i. kriminalnih »bročev«, različne tipologije otroškega seksualnega gradiva in analizira javno podobo storilcev, po kateri so dejanja gledanja (otroške pornografije) izenačena s posilstvom. Ta ideologija pedofilije zamegljuje razumevanje, raziskovanje in odpravljanje problema. Kar je morda najpomembnejše, pa je, da inkriminacije postopoma brišejo mejo med dejanji in mislimi, med tistimi storilci, ki si zaslužijo zapor, in tistimi, ki potrebujejo pomoč ali sploh nevmešavanje državne oblasti.

V poglavju obravnava tudi (2) nasilno in škodljivo vsebino, motive storilcev in fenomenološke oblike, kot so (a) sovražni govor, (b) podobe nasilja/umorov (»snuff movies«, »eksekucijski« video posnetki kot sredstvo kiber terorja), (c) navodila za izdelavo orožij in droge, (č) uporabo spletnih strani, ki omogočajo razširjanje informacij za izvajanje kriminalnih dejanj in (d) širjenje neresničnih (škodljivih) informacij.

Nazadnje v to obliko vključuje še (3) žaljivo komunikacijo po e-pošti, spletnih dnevnikih (*blogs* oziroma *weblogs*), novičarskih skupinah (*newsgroups*) in klepetalnicah (*chatrooms*), obravnava scenarije kibernetkega zalezovanja (*cyberstalking*) in internetnega zapeljevanja (*internet grooming*), ki je namenjeno pridobivanju zaupanja v *online* komunikaciji s ciljem prenosa zveze v svet *offline*, kjer se zgodi zloraba.

V poglavju o *prihodnosti kibernetke kriminalitete* avtor analizira fenomen avtomatizacije kriminalne aktivnosti. Gre za kvalitativno novo generacijo kibernetke kriminalitete, ki v skladu s »transformacijsko tezo« brez informacijske mreže sploh ne bi obstajala. Paradigmatski primer avtomatiziranega spopada med storilcem in žrtvijo Wallu predstavlja na videz nepomembno asimetrično in avtomatizirano pošiljanje neželene pošte (*spam, junk mail*). *Spam* je zanemarljiv kot kriminalitetno političen problem, strokovnjaki ga obravnavajo kot zgolj tehničen problem, laična javnost pa kot nadležnost, ki ne dosega stopnje resne nevarnosti. Wall pa nasprotno opozarja, da bi ga morali jemati resno, saj preobrača temeljne koncepte kazenskopravnega interveniranja in vzpostavljanja reda v kibernetnem prostoru saj ruši doslejšnjo svobodno naravo kibernetkega prostora. Na kakšen način bi lahko *spam*, ki smo se ga že »naučili« ignorirati, zamajal »arhitekturo« kibernetkega prostora?

Problem avtomatiziranega pošiljanja neželene pošte je v prvi vrsti njen agregatni učinek in dejstvo, da je praviloma pripravljalna faza kasnejših resnih kaznivih dejanj. Med glavnimi negativnimi lastnostmi *spama* se večinoma navaja vpliv na zmanjševanje pretočnosti informacijsko-komunikacijskih kanalov. Vendar Wall opozarja, da se je pošiljanje neželene pošte razvilo v razvejano industrijo: zgolj na primer faza oblikovanja seznamov e-poštnih naslovov poteka na pravno dovoljene načine, po evropski direktivi (2002/58/EC) zgolj s posameznikovim soglasjem (t.i. *opt-in* sistem), in na nezakonite načine (s strani uslužbencev ISP-jev, avtomatizirano s pomočjo programskih robotov (»*spider-bots*«).

Wall z razgradnjo industrije *spama* predstavi njegovo »anatomijo«, ki pa nas v nasprotju z njegovimi uvodnimi tezami, da kibernetna kriminaliteta še zdaleč ne dosega družbene nevarnosti, kakršno ji pripisujejo mediji in varnostna industrija, mora skrbeti. Izsledki longitudinalnih študij o vsebini *spama* (na primer največ vsebine se nanaša na zdravstvene storitve, zdravila in osebne finance), tehnikah pošiljanja, odzivih prejemnikov in značilnostih (razmeroma redkih) pošiljateljev *spama* (predvsem iz ZDA, daljnega vzhoda), ki jih predstavi, kažejo, da gre za dejanja, ki temeljijo na ekonomiji obsega in so medij resnih viktimizacij. Posameznik s tovrstnimi dejanji dosega nedoločen globalen krog žrtev, dejanja pa predstavljajo »multiplikator moči« in predstavljajo premik v delitvi kriminalnega dela.

Poleg *spama* pa avtomatiziran spopad med storilcem in žrtvijo nastaja tudi prek zlonamerne programske opreme. Nova generacija kriminalitete se namreč povezuje s *spamom*: sporočila sama nosijo zlonamerno programsko opremo (viruse, črve). V tem delu avtor natančno prikaže mehanizme delovanja črvov in virusov: medtem ko drugi zahtevajo (so)delovanje uporabnika, ki s svojo normalno uporabo sproži delovanje virusa in okuži statične datoteke, drugi deluje samodejno. Sodoben razvoj pa ti dve vrsti trojanskih konjev postopoma združuje: nove oblike »trojancev« so večmodalne, penetrirajo lahko na več načinov. Znamenite so zlasti »logične bombe«, ki se sprožijo ob nekem določenem trenutku v prihodnosti (na primer ob izvedbi določene operacije ali ob določenem datumu) ali »ransomware« – zlonamerna programska oprema, ki jo storilec deaktivira po plačilu odkupnine. Bistvena lastnost tovrstne zlonamerne programske opreme je, da »okužbe« delujejo vedno hitreje – včasih v nekaj tednih, danes le v nekaj urah.

Kvaliteta tega dela se kaže v prikazu novih načinov okužb (na primer z neželjeno reklamno programsko opremo (»*adware*«), prek katere se prenese virus), novih multiplih groženj, ki združujejo doslej ločene pojavne oblike zlonamernih dejanj. Wall jih zato imenuje kar meta-trojanski konji, ki vsebujejo

večplastne virusne okužbe, ki torej kombinirajo različne viruse, črve in drugo zlonamerno kodo. Kar je zares novega pri teh oblikah avtomatizirane kriminalitete, je, da je okužene računalnike (»zombije«) mogoče upravljati na daljavo. Te mreže *zombijev* pridobivajo v kibernetnem kriminalnem podzemlju posebno vrednost, mogoče jih je najemati, prodajati in naposled uporabljati za simultane napade (»*ratware*« – *remote administration mailing trojans*). *Zombi* je tako sredstvo napada, masovnega pošiljanja e-pošte (»poplavljanja«), trojanci pa omogočajo »sovražnemu prevzemniku« brskanje po podatkih uporabnika in omogočajo odtok podatkov iz njegovega sistema. Sodobni trojanci so različnih oblik, običajno skriti v različnih delih operacijskega sistema, poleg tega pa sami generirajo lastne klone, ki se sprožajo ob (ne)določenih trenutkih. Združitev doslej ločenih oblik delinkvence, *spama* in zlonamerne kode tako postavlja nove izzive za sisteme nadzorovanja, vloge prava, policije in drugih akterjev, ki (so)nadzorujejo kibernetni prostor, se postopoma spreminjajo.

V zadnjih dveh poglavjih se avtor loti teme nadzorovanja in *skrb* za red (*policing*) v kibernetnem prostoru. »Red in pravo« (in ne »*law and order*«) se v kibernetnem prostoru izvaja prek številnih mehanizmov, akterjev, koalicij in tehnologije. Bistvena avtorjeva izhodiščna ugotovitev je, da bolj ko neko kriminalno vedenje postaja posredovano s tehnologijo, bolj učinkovito ga je mogoče nadzorovati s to isto tehnologijo (in *de facto* manj preko prava). Tovrstna delovna hipoteza tako resno postavlja pod vprašaj vlogo prava in organov, zadolženih za njegovo izvajanje. Med njimi avtor posebno pozornost namenja zlasti policiji in njenemu mestu v heterogeni množici sredstev, ki zagotavljajo red *online*.

»Večslojen zbir mrež in vozlov«, ki zagotavljajo varnost v kibernetnem prostoru, predstavlja za lokalno oblikovano policijo in druge akterje kazenskopravnega sistema, ki so pretežno reaktivni in konzervativni, po Wallovem mnenju posebne izzive. Kibernetna kriminaliteta ni lokalna, temveč globalizirana. Policija ne le, da ni primerno opremljena (na primer z drago tehnološko opremo), temveč v organizacijskem smislu še vedno sloni na paradigmi iz 19. stoletja, ko je imela nalogo »odganjanja nevarnih razredov z ulic«. Izzivi za sodobno policijo, ki jih identificira, so: (1) problem »*de minimism*«: sodobna avtomatizirana kiber kriminaliteta je minornega značaja za posamezno žrtev, njen agregaten pomen se kaže na globalni ravni. To pa pomeni, da lokalno organizirana policija, osredotočena na posamično žrtev, v številnih primerih ne ukrepa; (2) *nullum crimen* razkorak pomeni, da so kazniva dejanja še vedno določena na nacionalni ravni in v večji meri neharmonizirana, kar predstavlja ovire za kazenski pregon; (3) jurisdikcijske razlike generirajo težave pri zagotavljanju dokaznega gradiva; (4) ne rutinska narava kibernetne kriminalitete postavlja izzive hierarhični rutinizirani policijski she-

mi; (5) slabo poročanje žrtev o lastnih viktimizacijah zaradi velike sekundarne viktimiziranosti policiji onemogoča zadostno frekvenco intervencij.

Skrb za red se v kibernetnem prostoru torej zagotavlja na drugačne načine, prek številnih interesnih skupin. Kazenskopravna justica se kaže za preveč okorelo in je nepripraven forum za razreševanje deviantnih in škodnih dejanj. Katere so te druge interesne skupine, ki tvorijo »vozle omrežne internetne vladavine« (»večslojen zbir mrež in vozlov«)? V prvi vrsti so to (1) internetni uporabniki in njihove skupine, ki imajo na voljo cenzuro, izločanje »problematičnih« posameznikov iz virtualnih skupnosti. Posebno instanco v zagotavljanju varnosti predstavljajo (2) upravljavci virtualnih skupnosti (na primer moderatorji v otroških klepetalnicah), (3) ISP-ji (*internet service provider*), ki zagotavljajo red s »pogodbeno vladavino«, (4) večji uporabniki/udeleženci, kot so korporacije, ki imajo lastne e-varnostnike, (5) nevladne hibridne (javno/zasebne) organizacije (na primer *Internet Watch Foundation* v VB), (6) vladne (nepolicijske) službe (na primer carina, pošta) in šele nazadnje (7) policija. Razčlenjena narava interneta tako pomeni, da vlada nima monopolne nadzorstvene vloge nad internetom in uporabniki. K čemur nas Wall prepričuje, so več-agencijska čez-sektorska partnerstva, oblasti in koalicije.

V zadnjem poglavju avtor sintetizira ugotovitve o nadzorovanju in skrbi za red v kibernetnem prostoru in prikaže svoj pogled na to, kako *nadzorovati in preprečevati kibernetno kriminaliteto* v prihodnje. Izhaja iz »digitalnega realizma«, ki označuje dejstvo, da bolj ko je vedenje posredovano s tehnologijo, bolj ga je s to samo tehnologijo mogoče tudi nadzorovati. A ravno v tem se skriva njegova poanta: kljub temu da tehnologija omogoča popoln nadzor nad deviantnimi ravnanji v kibernetnem prostoru, saj ga (tj. kiber prostor) tehnologija sama vzpostavlja, moramo preprečiti obravnavanje kibernetne kriminalitete kot tehnični problem. V trenutku, ko nanjo »pogledamo« skozi ta »očala«, se namreč izgubi ves potencial svobodnega prostora, ki ga predstavlja, izgubi se internetno osnovno načelo odprtosti in mrežne nevtralnosti. Da ne gre zgolj za teoretsko distopijsko špekulacijo o možnosti popolnega nadzora kibernetnega prostora, izhaja iz avtorjeve natančne analize uporabe tehnologij, ki tak nadzor omogočajo. Na primer vključevanje varnostnih elementov v operacijske sisteme je danes postalo pravilo, tehnologije »rudarjenja podatkov« (»*data mining*«) omogočajo analize zbranih (internetnih) prometnih podatkov in tako z »iskanjem »nepravilnih« vzorcev predstavljajo disciplinarne potenciale mrežnih tehnologij. Nauk, ki nam ga Wall, izhajajoč iz analize (kazensko)pravnega »boja« zoper *spamming*, podaja, je, da regulacija ne sme potekati zgolj preko tehnologije (kode), ki določa, kaj sploh je in kaj ni mogoče storiti v kibernetnem prostoru. Regulacija mora po-

tekati preko tehnologije, vendar »obrzdane« preko mehanizmov prava, družbenih vrednot in trga.

Poglavitna kakovost publikacije je interdisciplinarna obravnava kibernetike deviantnosti in reakcij nanjo. Zgolj pravna konceptualizacija praviloma stežka sledi škodnim ravnanjem, saj kot meni Moore, eno internetno leto ustreza približno trem realnim mesecem. Slabost pravnega diskurza predstavljenega v publikaciji je gotovo omejenost na ureditve VB in ZDA. Prikazani so torej številni diskurzi, ki skupaj s pravnimi določajo modelitete reakcije na to vrsto kriminalitete. Očitno je, da gre za tehnično dovzetnega avtorja, ki odlično pozna digitalno resničnost. To je po eni strani nujno za

razumevanje zlasti novejših, vedno bolj sofisticiranih pojavnih oblik te kriminalitete. Po drugi strani pa se ta dovzetnost kaže tudi v mestoma kazuističnem naštevanju vseh mogočih pojavnih oblik. Posebno kvaliteto publikacije vidim tudi v prikazu najnovejših oblik te vrste kriminalitete (novosti, kot so avtomatizirana dejanja – *botnets*), torej prikazu trendov tako na področju tehnološkega razvoja (na primer napredujoče konvergence tehnologij, razvoj ambientalnih tehnologij) kot kriminalitetnopolitičnih odzivov na to kriminaliteto (zlasti spremembe iz javnega k zasebnemu modelu varstva pred kibernetiko kriminaliteto, od ocene rizikov za družbo k oceni rizikov za posameznika ali organizacijo).

Aleš Završnik

R.A. Wilson (ur.): Human rights in the 'war on terror'

(Človekove pravice v 'vojni proti terorju'), Cambridge University Press, Cambridge, 2005, 347 strani.

V 60. letih (toliko časa je oz. bo decembra minilo od sprejetja Splošne deklaracije o človekovih pravicah) smo se že počteno navadili na človekove pravice, navadili vsaj toliko, da jih štejemo za samoumevne. Ne jemljemo sicer za samoumevno njihovo dejansko uresničitev, vsekakor pa to, da jih imamo. Tudi zavedanje, da so nam določene pravice kršene, namreč predpostavlja njihov obstoj. V kolikor jih namreč ne bi imeli, nam jih prav tako ne bi mogli kršiti.

Nato nastopi novo tisočletje, odjekne nekaj bomb, na katere se nalepi oznaka drugačnosti. Omenjena teroristična dejanja se začnejo interpretirati drugače kot poprej, njihova drugačnost pa naj bi označevala nastop nekega novega časa, v katerem naj nič več ne bi bilo tako, kot je bilo. Ta »novi čas«, v katerem igra glavno vlogo (običajno neopredeljena) 'varnost', pogosto potisne človekove pravice nekam med stransko vlogo in statiste. Povedano malce drugače, »medtem ko so človekove pravice navdihovale humanitarne intervencije v 90. letih, jih vladi, ki sta najbolj naklonjeni 'vojni proti terorju' – ZDA in Velika Britanija – uporabljata subsidiarno in kot *ex post facto* racionalizacijo za militaristične intervencije po 11. septembru« (Wilson, str. 10). Vojno v Afganistanu Wilson ne označi kot humanitarne intervencije, temveč kot samoobrambno vojno, temelječo na prepričanju mnogih, da je talibanski režim skrival in pomagal teroristom, ki so napadli ZDA, medtem ko vojno v Iraku kot »preemptivno vojno« (*preemptive war*), ki je temeljila na domnevi, da Saddam Hussein poseduje in namerava posedovati orožje za množično uničevanje. Šele potem, ko sta se obe domnevi izkazali za napačni, je po njegovem stopilo v ospredje opravičevanje posegov v človekove

pravice – češ, da gre za režime, ki množično kršijo človekove pravice (str. 11).

Ker je »vojna proti terorju« iz naslova v narekovajih, bralec takoj začuti določeno levo-liberalno usmeritev knjige. Po pregledu kazala še vedno ostane približno 80-odstotni občutek, da gre za knjigo strokovnjakov, profesorjev, ki v vojni proti terorju vidijo zlasti nevarnost za človekove pravice. Nekaj naslovov je namreč bolj dvoumnih ali celo namigujočih na to, da njihovi avtorji spadajo v tisto šolo filozofije (in javne uprave), ki trdi, da svet po 9/11 »ni več takšen, kot je bil«. Da potešim bralčevo radovednost že kar na začetku, naj dodam, da po branju knjige omenjeni odstotek ponovno naraste, nikoli pa ne doseže 100 odstotkov, kar urednik zbornika šteje kot poseben uspeh oz. posebej izpostavi – morebiti sicer čisto instrumentalistično (tj. da bi knjigo kupili tudi oni »na drugi strani«) – da avtorji prispevkov ne zagovarjajo absolutističnega pristopa k človekovim pravicam, npr. tako, da bi trdili, da so človekove pravice transcendentalne zahteve ali privilegiji, v katere ni nikoli upravičeno podvomiti. Gre torej za zbirko člankov profesorjev (sociologije, mednarodnega prava, zgodovine znanosti in fizike, prava, filozofije, mednarodnih odnosov, politologije, antropologije itd.), odvetnikov in aktivistov za človekove pravice, ki so nastali iz njihovih prispevkov na konferenci človekovih pravic, organizirani točno tri leta po 11. septembru, po terorističnem napadu na NY. Temeljni namen knjige naj ne bi bil le predstaviti različne poglede na protiteroristično zakonodajo in njene učinke na človekove pravice, temveč razviti takšno protiteroristično strategijo, ki bi resno upoštevala človekove pravice.

Prvi prispevek, prispevek urednika Wilsona, odpre s citatom Michaela Ignatieffa v *New York Timesu*, 5.2.2002, v katerem se slednji sprašuje, ali ni obdobje človekovih pravic – ki so po koncu hladne vojne postale del prevladujočega besedišča zunanjih zadev – minilo z 11. septembrom 2001. Razhajanje med človekovimi pravicami in varnostjo je po Wilsonovem mnenju še toliko bolj v oči bijoče, ker do razkola prihaja po desetletju, v katerem so človekove pravice igrale močnejšo vlogo kot kdaj koli prej. Igrale so vlogo ne le pri vzpostavljanju geopolitične stabilnosti, temveč pri razpravah o razvoju, okolju in sodelovanju pri političnih odločitvah. Kljub temu da so postavile temelje globalnemu sistemu pravosodja prek delovanja mednarodnih kazenskih sodišč za Ruando in bivšo Jugoslavijo, pa so mnogi v dejstvu, da je do genocidov na obeh območjih prišlo, videli tudi neuspeh človekovih pravic. Wallach v svojem prispevku zanimivo meni, da so se človekove pravice tako prominentno razvile prav zaradi njihove ideološke fluidnosti in dvoumnosti oz. nejasnosti, ki jim je omogočila, da so postale orodje močnih. Po eni strani pomenijo zavoro, ki omejuje politične akterje in institucije, po drugi strani pa mogočni moralni vir, ki zasleduje socialni razvoj. Wilson trdi, da naj bi v 90. letih definicija človekovih pravic prešla iz prve v drugo kategorijo in tako oskrbela države z »etiko moči«, prek katere lahko oblikujejo domačo politiko, zunanjo politiko in vojaško intervenirajo v regijah politične nestabilnosti. Po 2001 pa je Busheva administracija začela propagirati formulacijo mednarodne varnosti, ki je iz varnostnih vprašanj izločila človekove pravice. Naraščajoči prepad med obema se je izrazil na različne načine – v negativnem odnosu ameriške vlade do mednarodnega kazenskega sodišča (ICC) in njenih poskusov, da spodbolje ICC s pomočjo bilateralnih sporazumov, ki uvajajo posebne izjeme oz. imuniteto pred pregonom za ameriške vojake. Drugič, postkonfliktni rekonstrukcijski napor v državah, kot sta Afganistan in Irak, so namenili dosti manjšo pomembnost pri vzpostavitvi temeljnih človekovih pravic, vladavine prava in odgovornosti kot humanitarne intervencije v 90. letih. Wilson opozarja, da je sicer mamljivo povezati to zmanjšano vlogo človekovih pravic z neokonzervativno vlado Busheve administracije, da pa to ni celotna zgodba. Razloge je po njegovem treba iskati tudi v spremenjeni naravi varnostnih groženj po 2001. Združeni narodi in Rimski statut nista bila ustvarjena za spopadanje z mednarodnim terorizmom. Medtem ko so ZN namenjeni reševanju masovnih kršitev človekovih pravic v internem konfliktu, se Rimski statut naslanja na model suverenosti, ki se zdi presežen z modernimi islamiističnimi terorističnimi mrežami, ki ne delujejo centralno, temveč celično in decentralizirano. Ne le, da je struktura teroristov po 11. septembru drugačna, drugačna je tudi njihova motivacija, ideološka soglasnost in posvečenost, ki ne dopušča sklepanja kompromisov, pogajanj ali dialogov med stranmi. Kultura smrti, ki vlada med privrženci, jih dela imune na strah pred prijetejem in s tem njihove napade bolj smrtonosne. Podobno

erozijo zadržkov nad določenimi tipi terorističnega nasilja, ki so veljali v preteklosti, ko njihove politične ideologije še ni nadomestil verski fanatizem, opaža na nekem drugem mestu George Kassimeris (*Playing Politics with Terrorism: A User's Guide*), ki dodaja, da je »ena izmed bolj čudnih posledic terorizma zgodnjega 21. stoletja in vzpona militantnega islamizma ta, da poraja nostalgijo za zgodnejšim tipom terorista« (*idem*, str. 5). Prav tako ni res, poudarja Wilson, da bi enostranski vojaški posegi, utemeljeni na varnostni doktrini, privlačili le konservativce. Ameriške intervencije v Afganistanu in Iraku je podprlo tudi mnogo liberalcev (e.g. Paul Berman, Thomas Friedman, Michael Ignatieff). Slednji so videli in vidijo v tovrstnih napadih »manjše zlo« in opravičujejo slabe posledice ter nelegitimne posege s svetlimi vrednotami in dobrimi nameni. Ker so se ZN izkazali kot neučinkoviti, vidijo poslanstvo ZDA in VB v tem, da stopita na njihovo mesto in premagata religiozni fundamentalizem, ki ga primerjajo s fašizmom. V svojem oprijemanju teorije o pravični vojni (*just war theory*) so se mnogi liberalni pisci odmaknili od argumentiranja na podlagi pravic in ga zamenjali za politično etiko, ki naj bi bila primerna »eri terorja«. Človekove pravice naj bi se tako morale umakniti višjemu javnemu dobru, kot sta varnost in preživetje liberalnega demokratičnega sistema.

Pri iskanju pravega ravnovesja med pravicami in varnostjo se mnogi obračajo k filozofiji in zgodovini. Freeman tako v svojem prispevku primerja filozofiji Hobbesa in Locka. Za prvega je bil red temeljni predpogoj vseh družbenih institucij in civilne družbe in je tako zahteval od posameznikov, da se odrečejo svojim naravnim pravicam v zameno za varnost (str. 9). Locke pa je bil po drugi strani bolj pozoren na nagnjenost izvršilne oblasti k zlorabam in zato trdil, da mora slednja odgovarjati svojim državljanom, njihova primarna naloga pa je vzpostaviti zakonodajno oblast in vladavino prava, katere legitimnost izhaja iz družbenega konsenza. Teson na drugem mestu poudari, da so človekove pravice in varnost združljive zadeve in poskuša integrirati perspektivo pravic v hobbsovsko razmišljanje o varnosti oz. kako lahko ohranimo svobodo pred neposrednimi varnostnimi napadi, ne da bi kompromitirali težko pridobljene svoboščine. Meni, da so omejitve svoboščin lahko dopustne, vendar le, če se z njimi namerava ohraniti samo svoboda, in ne kot sredstvo za doseg drugih vrednot, kot je npr. varnost. Red zanj nima posebne intrinzične vrednosti. Le višje moralne vrednote, kot so svoboda, dostojanstvo in pravice, lahko legitimirajo dejanja države. Posledično se je država dolžna držati liberalne ustave in njene vizije svobode in pravic. Posegi oz. omejitve pravic pa so dopustne po njegovem, le kadar gre za grožnje s strani »načelnih zločincev« (*principled evildoers*), ki želijo popolnoma izničiti liberalno demokracijo.

Da si lahko nezadovoljen z obema načinoma reševanja problemov – tako z *Blitzkrieg* stilom ameriške vlade kot z od-

govorom mednarodnopравниh institucij – se jasno pokaže v Cushmanovem članku. Slednji analizira javno mnenje v Iraku po ameriški invaziji in opazi, da so Iranci na vojno v Iraku sprva gledali kot na humanitarno vojno. Kritično se opredeli tako do Busheve administracije kot do levičarske opozicije. Prvi očita, da so jo v vojno vodili drugi interesi in da je šele sekundarno pomislila na človekove pravice Irčanov. Opoziciji oz. kritikom vojne pa očita, da so spregledali oz. niso dovolj pozornosti namenili argumentu človekovih pravic kot moralni legitimaciji za poseg, temveč so se kot pijanec plota držali mednarodnega prava in multilateralnih institucij. Čeprav priznava, da ameriški unilateralizem ni najboljši način promoviranja človekovih pravic, meni, da je vseeno boljši od pasivnega multilateralizma, ki se zadovolji s krivičnim mirom in popušča diktatorjem.

Ovidijev verz »bili so nekaj zlati časi« se pojavi v pripetku Richarda Goldstona, ki poziva ZDA, naj se vrne v svoje zlato obdobje po II. svetovni vojni, ko so igrale pomembno vlogo pri izgrajevanju svetovnega pravosodnega sistema. Spomni jih, kako so od Nürnberga do ženevskih konvencij leta 1949 in mednarodnih razsodišč za bivšo Jugoslavijo in Ruando podpirale širitev načela univerzalne kazenske jurisdikcije za zločine proti človeštvu in zaprepaden ugotavlja, kako so kasneje same kršile številna načela vladavine prava (domneve nedolžnosti, pravico do sojenja pred pristojnim sodiščem) s svojim ravnanjem v primeru Guantanamo, pa tudi v Afganistanu in Iraku. Namesto poziva k mednarodnemu pogodbenemu in običajnemu pravu, ZDA raje spomni na svojo ustavno tradicijo vladavine prava in jih pozove, naj se vrnejo k svoji zgodovinski zavezanosti ustavnim pravicam.

Geoffrey Robertson se podrobneje loti procesov proti teroristom od 17. stoletja dalje. Poudari, kako je civilizacijski razvoj prinesel vzpostavitev sistema določenih pravic pridržanih oseb in kako dejanski mehanizmi, ki so jih ZDA uporabile proti post-9/11 teroristom, zavrtijo kolo časa precej nazaj. Loti se tudi političnih govorov, zlasti predsednika Busha in podpredsednika Cheneyja, ki sta pred izvedbo procesov osumljenca v Guantanamo označila kot »zle može« (Bush) in pozvala k njihovi hitri usmrtni v primeru, da so spoznani za krive (Cheney). Problemizira specialna vojaška razsodišča (pomenovana Kangaroo sodišča s strani New York Timesa) kot sodišča, ki ne zadoščajo zahtevam nepristranskosti oz. neodvisnosti od izvršilne veje oblasti. Mnogo vladnih dokumentov (od katerih se je vrh pogosto distanciral, ko so zadeve prišle v javnost), npr. dopis ameriškega Ministrstva za pravosodje z dne 1. avgusta 2002, kot tudi razmišljanje poprej liberalnih mislecev, ki so začeli podpirati vojno proti terorju, uporabljajo utilitaristični argument o manjšem zlu. Mučenje oz. kršenje človekovih pravic zapornikov označujejo kot manjše zlo, saj na tak način pridobijo mnogo, zanje pomembnih informacij,

in potencialno rešijo življenja bodočih žrtev. Filozofsko se tako naslanjajo na Jeremyja Benthama, angleškega filozofa 19. stoletja, za katerega pa je med drugim znano, da se je norčeval iz ideje o človekovih pravicah kot pravicah naravnega prava in jih znamenito poimenoval za »nesmisel na hoduljah«.

Wilson meni, da so prav pogoji v zaporih, ki držijo teroristične osumljence in politične zapornike (od Robben Islanda v Južni Afriki do Maze zapora na Severnem Irskem in Camp Delta v vojaški bazi Guantanamo), tisti, ki pomenijo latmušov test demokratičnega političnega sistema, in dodaja, da so ZDA na tem testu grdo pogrnilo. Zloraba zapornikov je vrgla senco nelegitimnosti na ameriško pravosodje. Potrebna bodo desetletja, da se ta vtis popravi, kar pa posledično dejansko zmanjšuje ameriško varnost s tem, da spodkopava legitimnost in sodelovanje zunaj ZDA. Neier med drugim pribeleži, da so se bili mnogi liberalni reformisti in demokrati v arabskem in muslimanskem svetu zaradi porasta antiamerikanizma, ki je sledil napadom na Irak, prisiljeni distancirati od ameriške politike, da bi preživel. A ZDA se niso ustavile samo pri tem. Na primeru Guantanamo in Abu Ghraiba je svet nazorno videl, kako pošastno lahko ZDA kršijo najbolj temeljne človekove pravice osumljenca in zapornikov. Če ZDA sedaj uporabijo besedišče človekovih pravic za argumentacijo svojih ravnanj, jim svet lahko kaj hitro očita hinavščino.

Novo protiteroristične strategije pa ne le kršijo človekove pravice, ampak tudi krepijo druge antidemokratične politične trende. Greenhouse opazi, kako so izvršilna veja oblasti in nacionalne vladajoče stranke uporabile 'vojno proti terorju' za medsebojno konsolidacijo in pridobitev moči nasproti opoziciji in ljudskim strankam in s tem povečale t.i. »demokratični deficit«. Vojna proti terorju je dala nov polet neoliberalizmu, uporabljena pa je bila tudi za oslabitev lokalnega nasprotovanja protiterorističnim ukrepom. Tako prihajajo pod udar ne le separatisti (npr. v Rusiji ali Filipinih), ampak tudi aktivisti človekovih pravic (npr. v Kolumbiji ali na Tajskem), ki so z novega vidika vojne proti terorju vsi enačeni s teroristi.

V zborniku je tudi nekaj bolj »klasičnih« prispevkov. Osiatynski se npr. sprašuje o univerzalnosti človekovih pravic in v razpravi o univerzalnosti vidi različne načine, na katere se družbe soočajo z globalizacijskimi pritiski. Četudi morda ne bo nikoli mogoče doseči vsekulturnega konsenza glede univerzalnosti človekovih pravic, meni, da to ne pomeni, da ni možen univerzalni sporazum glede osnovnih pravil za zaščito človekovih pravic. Kritizira trenutno pravno ubeseditiv človekovih pravic, konkretnije konvencije o človekovih pravicah, ki zamenjujejo filozofska načela in pravna pravila. Mary Robinson pa po drugi strani poziva k spoštovanju Berlinske deklaracije Mednarodne komisije pravnikov oz. doslednem upoštevanju ČP standardov v boju proti terorizmu, hkrati

pa opozarja, da mora mednarodna skupnost ne le spoštovati vladavino prava, temveč si prizadevati za odpravo revščine in pomanjkanja – pogojev, ki ustvarjajo teroriste.

Čeprav je od leta 2001 minilo že kar nekaj časa in nihče ni več ne presenečen ne začuden nad kršitvami človekovih pravic s strani ameriške in britanske vlade, pa zbornik vseeno bralca seznani z vrsto novih podrobnosti, strategij in prikritih taktik vladajočih, ki so v imenu učinkovitosti in lastnih interesov pripravljene zavreči vrsto temeljnih civilizacijskih dosežkov sodobne pravne družbe. Za razliko od široko publiciranih nelegalnih dogajanj npr. v Guantanamo, vsakodnevna medijska pojavljanja in pisanje t.i. »opinion makerjev« ter visokih državnih uradnikov, ki so po malem, a vztrajno legitimirala omenjena nezakonita ravnanja, nekako redkeje dosežejo bralca na tej strani luže. Zato ponuja zbornik bogato branje, pravo zakladnico biserov in njihovih svinj. Vendar to ni vse, kar najdemo v knjigi. Enako zanimivi kot konkretni epifenomeni 'vojne proti terorju' so opisani zgodovinski primeri obravnavanja teroristov. Brez odvečnih besed postane bralcu kaj kmalu jasno, kako smo in hkrati nismo kot civilizacija prišli daleč od 17. stoletja in razpenjanja osumljencev na križe, dokler niso priznali in podpisali svoje dokončne obsodbe (na podlagi katere so jih potem pogosto milostno razčetrverili).

Kdor visoko leta, nizko pade, je še ena misel, ki se bralcu pogosto prikrade med prebiranjem zbornika. Težko si je namreč predstavljati, da je pravno okolje, ki nam je dalo privilegij zoper samoobtožbo, prvo, ki je odpravilo in izničilo omenjeno temeljno procesno pravico, kljub temu da so bile vse oči sveta (tudi sveta, ki se v določenih vidikih zgleduje po njem) uprte vanj. Posebej zanimivi so tudi prispevki oz. deli knjige, kjer je podrobneje kvalitativno analizirana vsebina besedil in argumentacija zagovornikov vojne proti terorju oziroma moralna filozofija, iz katere izhajajo. Slednja je namreč univerzalna in nam pomaga odkrivati diktatorje in druge oblastizeljne osebe v naši sredini. V okviru psihometričnih besedil, ki se ponekod že uporabljajo za ugotavljanje, kdo je in kdo ni primeren za določena vodilna mesta, bi tako lahko kandidatu ponudili v razrešitev tudi moralni problem, zmodeliran po teroristično-vojni situaciji, v kateri se nahajamo. Odgovori bi odkrili, kako oseba razmišlja v kriznih situacijah – ali poseže po »manjšem zlu« ali je bolj brezkompromisna, načelna, kolikšno vlogo pri tem igrajo lastni interesi itd. (pri čemer seveda ne bi smeli pozabiti na kontrolna vprašanja).

Zbornik vsebuje lep popis kršitev človekovih pravic, ki se prodajajo pod oznako 'vojna proti terorju', ter zanimivo analizo tako kršitev prava kot družbenih reakcij na kršitve prava (Sutherland). Prek različnih pogledov ponuja celosten pogled na kompleksno tematiko, ki prodira v vse pore našega trenutnega žitja in bitja, legitimira nadzorovalne mehanizme in prek

strahu, ki ga vnaša v posameznikovo življenje, uspešno goji samodiscipliniranje (Faucault), posledično pa ustvarja tudi vrsto frustracij. Slednje se ponekod in pri nekaterih kanalizirajo tudi v družbeno nezaželeno ravnanja, katerih razpon sega od vandalizma nad uličnimi kamerami, ki izvajajo video nadzor, do terorističnega mladca, ki je prepričan, da bo s svojim uničujočim dejanjem zadal ameriškemu velenadzorovalcu pomemben udarec in mu bo hkrati odprl nebeška vrata. Zakaj svet sovraži Ameriko? Kar nekaj namigov najdete tudi v tej knjigi.

Nina Peršak