SPERRVERFÜGUNGEN IM INTERNET
Nationale Rechtsdurchsetzung im globalen Cyberspace?
von Ulrich Sieber und Malaika Nolde

Duncker & Humblot, Berlin, 2008, XX + 263 str.

„The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had."

Ove reči Eric-a Schmidt-a, člana Upravnog odbora Google-a, osobe očito vrlo kompetentne da se oglašava u datom kontekstu, u prvi mah mogu da deluju kao apokaliptično preterivanje, ali nakon prvobitnog skepticizma, ostaje pitanje nije li ipak donekle u pravu, barem u pogledu nesagledivih posledica koje će internet imati po ljudsko društvo. Nastanak interneta,[1] jednog od najvažnijih tehnoloških dostignuća čiji je uticaj već sada vidljiv u svim sferama života, vezuje se za šezdesete godine prošlog veka i ministarstvo odbrane vlade SAD koje je tada osnovalo *Advanced Research Project Agency* (ARPA) čiji je zadatak bio da, u to doba Hladnog rata, od centralizovanog i osetlijivog, stvori decentralizovani vojni informacioni sistem, sastavljen iz više autonomnih mreža koji bi preživeo mogući nuklearni rat.[2] 1969. godine stvorena je prva takva računarska mreža pod nazivom ARPANET. Nedugo potom, *National Defense Foundation* (NSF) stvorio je kompatibilnu mrežu za naučna, ne-vojna istraživanja,[3] kojoj se između ostalog, priključio i Univerzitet Harvard. 1983. godine se sa NCP-a (*Network Control Protocol*) prešlo na TCP/IP (*Transmission Control Protocol/Internet Protocol*), što predstavlja jedan od najbitnijih koraka, jer je to upravo tehnologija kakva se i danas koristi. Kako se kao argument za pojačanu krivičnopravnu represiju često koristi slikovita konstatacija da „kriminalitet ne poznaje granice", jasno je da upravo ovaj (relativno) novi, brzi, jeftin i lako dostupan medij kriminalitetu daje jednu sasvim novu dimenziju; on čini nacionalne granice još poroznijim; moglo bi se reći da ih zapravo virtuelno briše, dok kriminalitet sa svojim posledicama ostaje stvaran. U novonastalom ambijentu, u kom je sve teže kontrolisati protok informacija, neophodno je stoga da i krivičnopravne aktivnosti država pokažu veći stepen prilagodljivosti i brzog reagovanja nego što je to do sada bio slučaj.

Jednom od mogućih odgovora na pitanje kako u okviru ustavnih i zakonskih mogućnosti preprečiti put neželjenim informacijama upravo je posvećena knjiga koautora Ulrich-a Sieber-a i Malaike Nolde, a koja nosi naslov „Nalozi za blokiranje na inter-

1 Internet bi se mogao označiti kao međunarodna mreža mreža („international network of networks"). To je globalni, decentralizovani konglomerat velikog broja malih lokalnih mreža koje komuniciraju putem standardnih protokola. Slikovito govoreći, to je „okvir koji se može ispuniti različitim sadržajima". Više o tome: M. Burnstein, *A Global Network in a Compartmentalised Legal Environment*, p. 23; V. Pavić /2001/: Internet-problemi zakonodavne i sudske nadležnosti, Strani pravni život 1–3, Beograd, str. 266; F. C. Matthias /2004/: *Der kollisionsrechtliche Verbraucherschutz in der EU,* Wien, p. 2.

2 V. Pavić, *Ibid.*

3 S. Đorđević /2006/: *Merodavno pravo za internet-delikte*, magistarski rad, Beograd, str. 6.

netu – Nacionalno sprovođenje prava u globalnom sajber prostoru?" (*Sperrverfügungen im Internet – Nationale Rechtsdurchsetzung im globalen Cyberspace?*). Pogled na biografije autora ove knjige u kojima je uočljiva njihova dugogodišnja posvećenost kompjuterskom kriminalitetu, potvrđuje odlično poznavanje ove problematike. Ulrich Sieber je jedan od dva direktora Max-Planck-Instituta za strano i međunarodno krivično pravo iz Frajburga, honorarni profesor na Albert-Ludwig Univerzitetu u istom gradu i na Ludwig-Maximilians Univerzitetu u Minhenu, gde ujedno vodi i Centar za pravnu informatiku, dok na Institutu drži predavanja iz Informacionog krivičnog prava. Doktorirao je upravo na temu „Kompjuterski kriminalitet i krivično pravo" (*Computerkriminalität und Strafrecht*, 1977). Pored toga, objavio je više radova iz pomenute oblasti: „Kompjuterski kriminalitet" (Computerkriminalität, in: Sieber, U.; Brüner, F.-H.; Satzger, H.; von Heintschel-Heinegg, B. (Hrsg.): *Europäisches Strafrecht*, 2011), „Savladanje kompleksnosti u globalnom sajber prostoru: Harmonizacija računarskog krivičnog prava" (Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law", in: Delmas-Marty, M.; Pieth, M.; Sieber, U. (Hrsg.): *Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15,* 2008), „Sajber-terorizam i drugo korišćenje interneta u terorističke svrhe – analiza opasnosti i evaluacija međunarodnih konvencija" (Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions, in: Council of Europe (Hrsg.): *Cyberterrorism – the use of the Internet for terrorist purposes,* 2007), „Međunarodni priručnik za kompjuterski kriminalitet" (*The International Handbook on Computer Crime*, 1986). Slična interesovanja ima i koautor Malaika Nolde koja se, pored advokature, bavi i naučnim radom kao saradnik na Max-Planck-Institutu za strano i međunarodno krivično pravo na odeljenju „Informaciono pravo i pravna informatika". Objavljeni radovi, poput članaka „Ustavnopravne granice državne kontrole sadržaja na internetu" (*Verfassungsrechtliche Grenzen der staatlichen Inhaltskontrolle im Internet*, 2007) i „Prikriveni pristup računarskim podacima kod krivičnopravnih istraga" (*Heimlicher Zugriff auf Computerdaten bei strafrechtlichen Ermittlungen*, 2007) potvrđuju usmerenost njenih interesovanja na oblast kompjuterskog kriminaliteta.

Knjiga „Nalozi za blokiranje na internetu – Nacionalno sprovođenje prava u globalnom sajber prostoru?" nastala je kao rezultat istraživačkog rada u okviru projekta Max-Planck-Instituta koji se, kako je na unutrašnjim koricama ukratko objašnjeno, bavi izazovima „svetskog društva", „informacionog društva" i „novog društva rizika". Glavna motivacija za naučnu obradu ove teme, kako u predgovoru detaljnije piše, jeste činjenica da su nadležnosti država omeđene upravo državnim granicama. Čak i ako se primena nacionalnog krivičnog prava proširi na strane servere, ostaje problem sprovođenja istražnih radnji i izvršenja odluka u inostranstvu. To će posebno biti slučaj kada neko ponašanje u stranoj zemlji nije inkriminisano. Mnogobrojne države stoga rešenje ovih problema vide u tehničkim blokadama domaćih internet provajdera. Međutim, kod sprovođenja ove mere postoje brojne tehničke i pravne nedoumice, što je navelo Komisiju za zaštitu omladine u medijima (*Kommission für Jugendmedienschutz – KJM*), ustanovu koja je u Nemačkoj nadležna za izdavanje naloga za sprovođenje pomenute mere, da se obrati Max-Planck-Institutu za izradu studije o tome da li KJM može da naloži nacionalnim access-provajderima da blokiraju pristup određenim sadržajima na internetu na stranim serverima, ukoliko nije moguće direktno postupanje protiv ponuđača tih sadržaja. Institut je, potpomognut informacionotehničkom analizom Tehničkog univerziteta iz Drezdena, istraživanje proširio i na pitanja nacionalne kontrole globalnog sajber prostora i sa time povezanih zadiranja u osnovna prava građana. Struktura knjige postavljena je tako što nakon pomenutog predgovora i spiska

skraćenica, sledi šest delova rada, od kojih su četiri centralna, jedan uvodni i jedan zaključni, dok se u prilogu nalaze izvodi odgovarajućih pravnih akata i spisak literature.

Govoreći u uvodu (str. 1–8) o izazovima informacionog društva za zaštitu omladine, autori ističu da pored internacionalizacije i međunarodnopravnih problema (gde je krivičnopravno posebno relevantan problem određivanja mesta izvršenja krivičnog dela), teškoće postoje kod utvrđivanja identiteta i uzrasta korisnika. Nalozi za blokiranje se pojavljuju kao „alternativna strategija sprovođenja prava", kao „način da građani i prilikom ulaska u virtuelni svet ostanu vezani za legislativne vrednosne odluke svojih država" (str. 3). Na taj način bi se „održale pozitivne funkcije državnih granica (pravna sigurnost i smanjenje hiperkompleksiteta u društvu rizika), bez odricanja od globalnih prednosti sajber prostora" (str. 4). No, ovaj pokušaj „(re)teritorijalizacije" sajber prostora, uz uključivanje (državnih) nadzornih organa i provajdera kao „obezbeđenja na ulazu" zahteva čvrstu pravnu osnovu postupanja, što je posebno bilo predmet rasprave u Nemačkoj nakon što je 2002. godine Vlada okruga Dizeldorfa izdala naloge za blokiranje internet stranica sa (neo)nacističkim sadržajem.

Centralni deo knjige započinje drugim delom („Problemstellung", str. 9–57) u kom je postavljen problem kroz pregled mogućih slučajeva primene naloga (pornografija, nacistički sadržaji, podsticanje nasilja i povrede ljudskog dostojanstva, igre na sreću, uvrede i povrede verskih opredeljenja, vrbovanje za /reklamiranje terorizma, zaštita privatnih prava). U nastavku se analiziraju strategije suverenih vlasti, podeljene na postupanje protiv ponuđača sadržaja, protiv korisnika i protiv ponuđača usluga u domaćoj državi. Govoreći o prvima, autori su se, između ostalog, posvetili i pitanjima „zoning"-a (tj. tehničke izvodljivosti ciljanog isključenja pojedinih oblasti od mogućnosti prijema određenih internet sadržaja putem njihovih IP adresa) i izvršenja odluka na poznatom primeru Yahoo v. LICRA iz 2000. godine. Kada se radi o korisnicima, oni će biti odgovorni ukoliko poseduju dečiju pornografiju, dok se *de lege ferenda* nazire širenje zone kažnjivosti i na posedovanje materijala nacionalsocijalističke i ekstremističke sadržine, kao i na omogućavanje maloletnicima da bez nadzora surfuju internetom, čime se dovodi u pitanje fragmentarni i supsidijarni karakter krivičnog prava. Iscrpnim objašnjenjem tehničkih pretpostavki, diferenciranjem potencijalnih adresata naloga za blokiranje i pregledom četiri aktuelna modela blokiranja (preko DNS servera, upisom u routing tabele, korišćenjem proxy servera i hibridnim modelom), prikazano je postupanje protiv ponuđača usluga. Drugi deo se zaokružuje pregledom inostranih iskustava u vezi sa merama kontrole i blokade, pri čemu se na spisku stranih država (Kina, Iran, Izrael, Italija, Švajcarska, Tajland, Turska, SAD) nalaze i zemlje čije se „demokratsko opredeljenje" ne dovodi u sumnju.

Treći deo knjige („Beteiligte Grundrechtsträger und berührte Grundrechte", str. 58–90) posvećen je osnovnim pravima i njihovim nosiocima na koje se nalozi za blokiranje odnose. U okviru prethodnih pitanja zaključeno je da privatizacija sektora pošte i telekomunikacija predstavlja izazov za očuvanje garantija osnovnih prava, pošto su se oni time približili nedržavnim upravnim jedinicama, a time ujedno doveli u pitanje svoju vezanost za poštovanje osnovnih prava (koja se shvataju kao „odbrambena prava nasuprot državi"). Međutim, oni su, uprkos tom principu udaljenosti od države (*Prinzip der Staatsferne*), u lancu država/pokrajinski medijski zavod/ponuđač ipak obavezni da poštuju naloge koje im izdaje država; oni predstavljaju neku vrstu njene produžene ruke, tako da je njihovo postupanje ipak i sa aspekta zaštite osnovnih prava relevantno. U nastavku trećeg dela, najveća pažnja je usmerena ka pomenutim pravima i njihovom mogućem uskraćivanju. Tako se kao prava provajdera i pretraživača detaljno opisuje veza između tehničkih intervencija i slobode zanimanja, slobode imovine, ravnopravnosti pred zakonom, slobode mišljenja, slobode štampe i naučne slobode; kao prava

ponuđača sadržaja sloboda mišljenja, sloboda štampe i elektronskih medija, sloboda zanimanja i opšta sloboda delovanja; kao i sloboda informisanja i pravo na tajnost pisama, pošte i telekomunikacija korisnika interneta.

Naredni, četvrti deo knjige („Voraussetzungen der Eingriffsgrundlage gemäß § 20 Abs. 4 JMStV i.V.m. § 59 Abs. 4 RStV"; str. 91–175) posvećen je detaljnom pojašnjenju pretpostavki postupanja; počev od samog osnova postupanja, tj. njegovih pravaca razvoja i alternativnih osnova, preko usaglašenosti sa višim pravom, pa do formalnih i materijalnih uslova. U tom kontekstu je, kako se iz samog naslova vidi, posebno značajan Državni ugovor o zaštiti omladine u medijima koji je stupio na snagu aprila 2003. godine, kao i Zakon o telemedijima i 9. Državni ugovor o izmeni elektronskih medija iz marta 2007. godine. Posmatrajući odnos pravnog akta iz 2003. godine i čl. 5. Osnovnog zakona, iskristalisala se zapravo ideja vodilja zaštite omladine: slobodu prijema informacija maloletnika treba ograničiti, ali tako da se time ne opravda jedna kompletna blokada komunikacija za ponuđače sadržaja, niti blokada informacija za odrasle korisnike. Premda ovaj akt u §§ 4 i 5 sadrži katalog slučajeva u kojima su pomenute blokade dozvoljene, postoje situacije koje nisu tim odredbama regulisane, a koje predstavljaju kršenja odredbi Krivičnog zakonika. Tada nadzor vrši i naloge izdaje ustanova određena prema pokrajinskom zakonu; čime, drugim rečima, preti opasnost od fragmentacije prava zbog neujednačene upravne prakse. Još jedan nedostatak ovakvog rešenja i ujedno korak dalje od željene objektivnosti jeste taj što ova tela, za razliku od Komisije za zaštitu omladine u medijima, ne predstavljaju kontrolni gremijum koji se nalazi izvan sistema državne uprave.

U nastavku četvrtog dela, pažnja je posvećena usklađenosti sa pravom višeg ranga, gde je, između ostalog, zaključeno da odluka o dizeldorfškim nalozima za blokiranje ne krši međunarodnopravno načelo nemešanja, s obzirom na to da je bila usmerena isključivo prema domaćim pravnim licima, i da postoji odgovarajuća povezanost sa Saveznom Republikom Nemačkom zbog „osetne opasnosti po javni red". Dejstvo ove mere prostire se samo u okviru nacionalnih granica; u drugim državama internet ponuda ostaje dostupna. Zabrana cenzure iz čl. 5. Osnovnog zakona i uopšte određivanje i tumačenje pojmova formalne i materijalne; prethodne i naknadne cenzure predmet je naredne podceline u okviru četvrtog dela knjige. Još jednom je pomenuta težnja da se izbegne tzv. chilling effect, tj. paralisanje duhovnog života kroz faktičku samocenzuru. Formalnim pretpostavkama norme, tj. određivanju funkcionalne i mesne nadležnosti, postupku i pojedinim pitanjima upravnopravne prirode, slede materijalne pretpostavke. Kada govore o kršenju odredaba Državnog ugovora, autori naglašavaju da ne postoji više pozivanje na Krivični zakonik putem jedne generalne klauzule, već su te povrede pojedinačno opisane i ne zahtevaju uvek ispunjenje svih uslova koje predviđa KZ. Izvršena je kategorizacija 11 povreda, tako da se razlikuju ponude koje su apsolutno nedopuštene, one koje su nedopuštene za decu i maloletna lica i naposletku one koje po mogućstvu treba zabraniti deci i maloletnim licima određene starosne dobi. Govoreći o svakoj od pomenutih stavki, autori navode primere sadržaja na internetu koji bi se mogli podvesti pod ovu normu, poput tzv. tasteless ponuda, tj. prikazivanja scena ljudi izloženih jakim fizičkim ili psihičkim bolovima, ili tzv. snuff videa, tj. prikaza (navodno) realnih radnji lišenja života, koji bi se mogli obuhvatiti tačkom 8 kataloga („ponude protiv dostojanstva ljudi").

Pretposlednje, peto poglavlje („Verhältnismäßigkeit der Maßnahme", str. 176–227) posvećeno je pitanjima legitimnosti svrhe, podobnosti, nužnosti i prikladnosti mere. Odgovor na ovo prvo sadržano je u obrazloženju Državnog ugovora o zaštiti omladine u medijima, gde je rečeno da „je njegov cilj zaštita dece i omladine od ponuda koje mogu da otežaju ili ugroze njihov razvoj ili njihovo vaspitanje. On pored toga, pak, slu-

ži i *uopšteno* zaštiti od ponuda u elektronskim medijima koje povređuju dostojanstvo čoveka ili druga pravna dobra zaštićena Krivičnim zakonikom" (str. 176). Autori skreću pažnju da je pojam „dostojanstvo čoveka" u ovoj relaciji neodređen, da medijsko prikazivanje ljudi njih čini „predmetima posmatranja", zbog čega je prikladnije govoriti o poštovanju autonomije i samoodređenja prikazanih ljudi. Kao pravna dobra koja štiti KZ, u prvom redu su označeni demokratska pravna država, politički i javni mir, a kao cilj se mimo zaštite omladine pominje još i izbegavanje neželjenog susretanja odraslih ljudi sa pornografijom. U nastavku je definisana ciljna grupa ovih zaštitnih mera, gde je shvatanje da se tu misli na „prosečne mlade", tj. „normalne korisnike" kojima treba „vremenski i tehnički otežati pristup" nadvladalo shvatanje koje je taj krug suzilo na one „mlade koji su skloni opasnostima", tj. koji se „rizično ponašaju ili koji još uvek ne mogu pravilno da procene ostvarivanje kontakata na četu" (str. 179). U okviru trećeg pitanja, nužnosti njihove primene, pomenuto je da bi harmonizacija internet krivičnog prava bila dobro rešenje, ali da su izgledi za to malo verovatni, između ostalog i zbog činjenice da ublažavanje uslova obostrane kažnjivosti kod međunarodnopravne pomoći vodi ka olakšanom postupanju protiv ponuđača sadržaja, čime supsidijarno postupanje protiv ponuđača usluga čini izlišnim. Peto poglavlje se, pre tumačenja adekvatnosti ove mere, prevashodno u svetlu osnovnih prava, snošenja troškova i jednog sveobuhvatnog odmeravanja, zaokružuje razmatranjem mogućnosti samoregulisanja interneta (Cyberlaw – Lex informatica) koje propagiraju tzv. internet-separatisti, smatrajući da će se time prevazići problemi u primeni tradicionalnih pravnih pravila teritorijalno ograničenih, povećati prihvaćenost i poštovanje od strane korisnika, izvršiti efikasniji nadzor u odnosu na državnu kontrolu i sačuvati posebna dostignuća interneta.

Šesti, ujedno poslednji deo knjige („Zusammenfassung und Ergebnis", str. 228–236) jeste, kako sâm naslov kaže, sažetak postavljenih problema i ocena mogućih rešenja. Još jednom su osmotrene tehničke mogućnosti i vrste naloga za blokiranje, kao i ustavnopravne osnove, pri čemu je nanovo podvučeno da su dozvoljene samo one mere koje ne diraju u pravo na tajnost telekomunikacija. Sveukupna ocena glasi da je važeće stanje u nemačkom pravu po pitanju naloga za blokiranje nedovoljno i tek u maloj meri promišljeno, posebno u pogledu efektivnosti mera i zaštite osnovnih prava, što je uočljivo kada se imaju u vidu „rasparčana" nadležnost kod više institucija, pravne nedoumice, čitavi lanci upućivanja, sistemski prekidi i nedostajući strategijski koncepti. Autori zaključuju da, ukoliko se zakonodavac zadovoljava simboličnom politikom koja mere sporovodi tek na pojedinim mestima i u ograničenom obimu, onda se postojeće stanje može oceniti kao prihvatljivo. Međutim, u slučaju postojanja želje za postavljanjem sveobuhvatne strategije i odgovarajućim zakonskim izmenama, morala bi se prethodno povesti rasprava o tehničkim konceptima i mogućnostima „teritorijalizacije interneta" u slobodarskom društvu uopšte, o ustavnopravnim granicama i o alternativnim zaštitnim strategijama.

Čini se legitimnim nastojanje nacionalnog zakonodavca da sporovođenjem mera blokiranja internet servis provajdera, domaćim korisnicima u jednom pravno kontrolisanom postupku onemogući pristup ilegalnim sadržajima sačuvanim u inostranstvu, sve dok ne postoji harmonizacija zakonskih rešenja, niti međunarodno koordinisano postupanje čak ni naspram jezgra protivpravnih ponašanja, i sve dok ne stoje na raspolaganju ni pravne, ni vanpravne strategije; sve dotle je procena zakonodavca da treba da se suprotstavi postojećim sadržajima na internetu ne više samo offline, već i da onemogući online pristup, opravdana i razumljiva. Ono što se najviše može prigovoriti postojećem rešenju u nemačkom pravu jeste komplikovana mreža upućivanja kroz pravna akta različite pravne snage (koja se, pritom, začuđujuće često menjaju) i fokusiranost na zaštitu omladine od eksplicitnih

sadržaja na internetu koja naloge za blokiranje prikazuje tek kao kap u moru (krivično) pravnog reagovanja na sajber kriminalitet, a istovremeno budi sumnju u mogućnost ograničenja osnovnih prava građana u slučaju daljih širenja zabrana i blokada. U mnoštvu upućivanja, izmenjenih koncepata postupanja, oprečnih mišljenja po pitanju nužnosti i srazmernosti mera, za pravnu analizu nezaobilaznih, ali i komplikovanih tehničkih rešenja, knjiga „Nalozi za blokiranje – Nacionalno sprovođenje prava u globalnom sajber prostoru" autora Ulrich-a Sieber-a i Malaike Nolde deluje kao svojevrsni svetionik kojim se želi razbiti magla koja prekriva nepregledno more zvano internet. Ona pruža sveobuhvatan, temeljan, teorijski vrlo ozbiljan prikaz celokupne, usko stručne problematike, premda stil pisanja, kao uostalom i tema kao takva, nije „lagan", tj. zahteva se određeni nivo predznanja, posebno tehničkih preduslova i načina funkcionisanja interneta. Globalni sajber prostor i dešavanja u njemu koja se nastoje učiniti što jasnijim odavno zaokupljaju pažnju zakonodavca koji se sada nalazi pred sasvim novim izazovima (krivično)pravnog reagovanja na sve veći i brži protok „neuhvatljivih" informacija neograničenom broju korisnika. Želja da se u potpunosti „omeđi" virtuelni prostor kosi se sa njegovom prirodom i načinom funkcionisanja, ali se čini da prepreke određenim sadržajima imaju svoje pravno utemeljenje, što je iscrpno, objektivno, uz povremena, u razumnoj meri prisutna iznošenja ličnih stavova i ocena, vrlo stručno objašnjeno upravo u prikazanoj knjizi.

Ivana Marković