Zapisi

»Digitalni forenzični forum« (Digital Forensic Forum)

Praga, november 2007

Konec novembra 2007 sem se udeležila dvodnevnega posveta, poimenovanega »*Digital Forensic Forum*«, ki je potekal v Pragi. Kljub temu da sem bila edina pravnica med skupaj 35 udeleženci, sem na konferenci dobila odlična izhodišča za razmišljanje o pravnih vprašanjih, povezanih z digitalno forenziko. Dvanajst predavateljev iz šestih držav in štirih celin je predstavilo različne vidike digitalne forenzike – področja, ki mu nekateri napovedujejo celo bolj revolucionarno vlogo pri odkrivanju in preiskovanju kaznivih dejanj, kot jo ima metoda DNK analize. Konferenca je potekala v konstruktivnem vzdušju, prežetem s pristnim angleškim humorjem, za katerega so vztrajno skrbeli predavatelji in udeleženci z Otoka.

Ker so se predavatelji dotaknili precej različnih tem, povezanih z digitalno forenziko, je težko podati poročilo z zapisom rdeče niti, zato bom uporabila zapisniško obliko. Ker gre za zelo zanimivo področje, upam, da mi bralci tega na bodo zamerili.

Vlasti Broucek, raziskovalec Univerze v Tasmaniji (University of Tasmania, Avstralija), je skladno s temo svojega predavanja *Forenzično računalništvo – potreba po celovitem pristopu* (*Forensic Computing – the Need for Holistic Approach*) celovito predstavil forenziko na področju računalništva, in sicer je izhajal iz zgodovinske perspektive. Kot je slikovito predstavil, se je vse začelo pred približno dvajsetimi leti. Leta 1988 je Clifford Stoll objavil članek *Zalezovanje Wilyja Hackerja* (*Stalking the Wily Hacker*) in dve leti kasneje še knjigo *Kukavičje jajce* (*The Cuckoo's Egg*), v katerih je dokumentiran prvi primer organizirane oziroma sistematične preiskave kaznivega dejanja, storjenega s pomočjo takrat še ne zelo razširjene računalniške tehnologije. Kot je poudaril predavatelj, je bilo med to preiskavo postavljenih kup napačnih domnev, preiskovalci pa niti sami niso verjeli v lastne ugotovitve (kar ni nenavadno, saj so v tistem času verjetno res spominjale na znanstveno fantastiko). In zakaj je pravzaprav šlo? C. Stoll je bil zaposlen kot astronom v Lawrence Berkeley laboratoriju (ZDA), to je v raziskovalni instituciji, ki je med drugim opravljala določene zadeve za vojsko. Leta 1986 so v računalniškem sistemu LBL opazili vsiljivca. Stoll je dobil nalogo, da zadevo reši. Namesto da bi vse sile usmeril v to, da neželenemu gostu onemogoči nadaljnje vdiranje v sistem, se je – med prvimi v zgodovini – odločil za nov pristop: vsiljivcu je pustil dostop, sam pa je s sodelavci spremljal njegove aktivnosti, mu sledil po medmrežju in skušal odkriti, od kod prihaja in kaj želi. Ugotovili so, da storilca zanimajo vojaški podatki. Begalo pa je dejstvo, da so se vdori večinoma pojavljali okrog poldneva. Leta 1986 so bili na voljo le modemski dostopi do interneta in ti so bili ponoči znatno cenejši kot podnevi. Na podlagi tega dejstva je Stoll postavil revolucionarno hipotezo, da vsiljivec ni iz ZDA, pač pa da prihaja iz vzhodne(ejše)ga dela sveta (gledano iz smeri ZDA). Na podlagi Stollove iznajdljivosti in zvijače, s katero so storilca zvabili k vdoru v določen sistem in ga tam z nastavljenimi podatki zadržali dovolj dolgo, da so telefonski operaterji lahko določili njegovo lokacijo, so v končni fazi ugotovili, da vdori »prihajajo« iz Hannovra v Zahodni Nemčiji. Storilec naj bi podatke zbiral in prodajal ruskemu KGB.

S tem ko so se začeli v informacijsko razvitejših družbah zavedati pomena in problemov informacijske varnosti, so nastala ugodna tla za razvoj računalniške oziroma digitalne forenzike. Pred približno desetimi leti so se pričeli pojavljati prvi strokovni članki na to temo, večji proizvajalci programske opreme pa so pričeli razvijati prve komercialne programe za računalniške forenzične preiskave. Danes so na voljo različna forenzična orodja, ki omogočajo preiskave različnih segmentov računalnika oziroma računalniškega sistema (ta orodja so večinoma visokega cenovnega razreda, predavatelj pa je kratko predstavil tudi orodje Sleuthkit, ki je na voljo brezplačno), prav tako se iz dneva v dan povečuje oziroma širi znanje na področju računalniške forenzike.

S sistemskimi vprašanji, povezanimi z digitalno forenziko, se je v svojem predavanju ukvarjal tudi ***Allen C. Clarkson***, samostojni raziskovalec in svetovalec iz ZDA. V sklopu teme *Digitalna forenzika: težaven problem* (*Digital Forensics: a Compound Problem*) je med drugim opozoril na enega temeljnih namenov digitalne forenzike, ki je: zagotoviti dokaze v kazenskih postopkih zaradi kaznivih dejanj, povezanih z računalniki. To je povezano z razlago, tolmačenjem in predstavitvijo digitalnih dokazov na sodišču, kar je lahko težavna naloga, saj je digitalna forenzika izrazito tehnično področje s posebnim izrazoslovjem in logiko. Poleg tega so tehnike in orodja, ki jih uporabljajo digitalni forenziki, zelo različna, kar pomeni, da strokovnjakov v digitalni forenziki na splošno ni – lahko so le strokovnjaki za posamezno orodje ali posamezno vrsto tehnologije.

O kriminalističnih vidikih digitalnih dokazov je razpravljal ***Roman Rak***, bivši kriminalist, sedaj zaposlen v češkem telekomunikacijskem podjetju O2. Predstavil je pojem digitalnega dokaza v luči klasične kriminalistične teorije o sledeh (*Digital Evidence in Classic Criminalistic Theory of Traces*)). Predavatelj

je nazorno in poučno predavanje pričel s predstavitvijo vsakodnevnih predmetov, ki ustvarjajo digitalne sledi, česar se njihov uporabnik pogosto niti ne zaveda. Poleg najrazličnejših računalnikov (stacionarnih, prenosnih, računalnikov v avtomobilih in drugih prevoznih sredstvih itd.) so to tudi npr. mobilni in stacionarni telefoni, dlančniki, fotoaparati. Pomen digitalnega dokaza kljub mnogim definicijam ni nesporen. Med konferenco smo se malce prerekali o tem, ali je digitalni dokaz npr. elektronski nosilec z obremenilnim materialom, zapis obremenilnega materiala na tem nosilcu, morda izpis tega materiala z elektronskega nosilca ali celo kaj četrtega. Roman Rak je skušal ta nesoglasja preseči s klasificiranjem digitalnih dokazov v tri skupine: na kriminalistične digitalne dokaze, forenzične digitalne dokaze ter digitalne dokaze za drugo uporabo.

Johan ten Houten iz nizozemskega Deloitte je svoje predavanje naslovil *Izziv digitalnega Everesta (Challenging the Digital Everest)*, pri čemer je ta izziv zajemal predstavitev dela in uspehov ene največjih globalnih zasebnih forenzičnih institucij, Deloitte&Touche Forensic & Dispute Services. Deloitte&Touche je sicer računovodsko podjetje, ki svojim strankam med drugim ponuja tudi preiskave finančnih goljufij in podobnih špekulacij, ki jih prevzame poseben oddelek, v katerem so zaposleni forenzični računovodje, menedžerji, forenziki za informacijsko tehnologijo, bivši agentje raznih preiskovalnih institucij (npr. FBI) ter tudi pravniki, zlasti bivši sodniki in tožilci (to podjetje je med drugim igralo pomembno vlogo pri preiskovanju primera Enorn). Kot je pojasnil ten Houten, se pri preiskavi primera osredotočijo na naslednje: iščejo izvršitveni način, skušajo razkriti naklep, iščejo elemente zarote, ugotavljajo, kdo vse je bil seznanjen z določenimi zadevami, ugotavljajo razsežnosti goljufije in načine, kako zaobiti nadzorne mehanizme, pozorni pa so tudi na druge pomembne dogodke; vse z namenom zgraditi primer in najti dokaze. Z asociacijo na 8848 metrov visok Mount Everest je predavatelj nazorno prikazal, kako obsežno je lahko delo na posameznem primeru, saj je običajno potrebno pregledati na tone dokumentacije. Podatki, sestavljeni iz enega milijona črk, natisnjeni znesejo približno 200 strani. Kup 200 strani papirja je debel približno 5 centimetrov. Podatki iz povprečnega prenosnega računalnika s 40 gigabajtnim diskom bi torej (pod predpostavko, da je disk polno zaseden) natisnjeni in zloženi na kup segali približno 2.000 metrov visoko; podatki iz povprečnega strežnika s 400 gigabajtnim diskom pa kar 20.000 metrov visoko, kar pomeni, da bi za skoraj 2,3-krat presegli Mount Everest. Ob upoštevanju dejstva, da je pri preiskavi posameznega primera običajno treba pregledati precej več kot le en računalnik oziroma strežnik, bi šlo za misijo nemogoče, če ne bi različna forenzična orodja preiskovalcem pomagala po čim krajši poti izluščiti tiste podatke, ki so povezani s primerom.

Izvršni tehnični direktor podjetja OrbisIP iz Velike Britanije, ***dr. Rob Rowlingson***, se je posvetil vprašanjem pripravljenosti podjetij na uporabo metod, ki jih nudi digitalna forenzika s predavanjem, naslovljenim z *Orodja in tehnologije za forenzično pripravljenost (Tools and Techologies for Forensic Readniess))*. *Forensic Readiness* (forenzična pripravljenost) je danes uveljavljen izraz, ki pomeni sposobnost posamezne organizacije maksimirati uporabo digitalnih dokazov ob hkratnem minimaliziranju stroškov preiskave. Preprosteje povedano, gre za vprašanje osveščenosti poslovnih subjektov na področju informacijske varnosti. Kot je poudaril predavatelj, so digitalni dokazi povsod, podjetja pa jih lahko uporabijo v dveh smereh: za svojo obrambo (npr. za dokazovanje kaznivih dejanj ali drugih nepravilnosti s strani zaposlenih) in za svoje poslovne interese, zlasti v smeri zmanjšanja poslovnih rizikov. Predavatelj se je sicer osredotočil na podjetniške vidike informacijske varnosti, opozoril pa je, da ima to področje tudi številne druge razsežnosti, npr. pravne (kot pravi K. Whithers: »*Some day toaster ovens will be digital and will carry a warning: 'Whatever you eat for breakfast may be used against you in a court of law.*«).

S čisto konkretnimi vprašanji, povezanimi s praktično uporabo digitalne forenzike, se je ukvarjal ***John Mitchell*** iz LHS Business Control (Velika Britanija), in sicer je v izjemno zanimivem predavanju razpravljal o pomembnosti natančne določitve časa v sklopu digitalne analize (*The Importance of Accurate Time Determination in Digital Analysis)*). Uvodoma je predstavil štiri temeljna vprašanja pri preiskovanju z uporabo digitalne forenzike: 1) kaj je tam (*what's there?*), 2) kako je prišlo tja (*how did it get there?*), 3) kdaj je prišlo tja (*when did it get there?*) in 4) kdo je to spravil tja (*who put it there?*). Najzahtevnejši sta vprašanji kdo in kdaj, pri čemer se je predavatelj ukvarjal zlasti s slednjim. Opozoril je, da obstajajo (antiforeznična) orodja, ki omogočajo, da se po dejanju spremeni časovnica (*timestamp*), ki se nanaša bodisi na čas ustvaritve dokumenta (*created*), čas zadnje spremembe (*modified*) ali čas zadnjega dostopa do tega dokumenta (*accessed*). Če preiskovalci to spregledajo, si lahko storilec uspešno zagotovi sicer lažni alibi, v še slabšem primeru pa lahko za dejanje obsodijo nedolžno osebo. Tudi sicer je treba biti pri določanju časa računalniško izvedenega dejanja zelo previden, saj vedno ni jasno, kako različne operacije vplivajo na časovnice v različnih operacijskih sistemih. Povsem mogoče je, da je npr. datum zadnje spremembe dokumenta starejši od datuma ustvaritve tega dokumenta, kar morajo forenziki znati ustrezno in verodostojno pojasniti, sicer njihova preiskava ne bo imela (bistvene) dokazne vrednosti.

Marian Svetlik Jr. iz češkega podjetja Risk Analysis Consultants (to podjetje je bilo organizator konference) je v predavanju z naslovom *Mali forenzični laboratorij (Small Forensic Laboratory)* predstavil opremo, ki je nujna za zagon laboratorija za digitalno forenziko in ilustriral delovanje majhnega forenzičnega laboratorija.

Viktor Porada z Inštituta za kriminalistiko in forenzične znanosti Univerze Karlovy Vary (Republika Češka) je pripravil izhodišča za razpravo o izobraževanju digitalnih forenzikov (*Concept of Digital Forensic Experts Education System*). Ob tej temi se je razvnela živahna razprava najprej o tem, ali bi morali laboratoriji in podjetja, ki se ukvarjajo s tem področjem, izpolnjevati kakšne pogoje ali standarde. Medtem ko je v ZDA jasno, da lahko preiskave v primerih, v katerih je mogoče pričakovati sodni epilog, opravljajo le institucije (javne ali zasebne) s posebnim certifikatom, v Evropi standardov zaenkrat ni. Udeleženci iz zasebnega sektorja so ocenili, da niti niso potrebni, saj selekcijo opravlja konkurenca na trgu. Ob takem pristopu pa se lahko postavi vprašanje (ne)pristranskosti forenzične institucije, ki je pri svojem delu obremenjena z vprašanji ekonomskega preživetja. Vprašanje, ali naj bo digitalna forenzika v domeni zasebnega sektorja, je aktualno zlasti v državah, ki se (še) ne zavedajo pomena in obsega računalniške kriminalitete (npr. Slovenija). Države, ki resno pristopajo k odkrivanju in preiskovanju kriminalitete, povezane z računalniki, imajo za javne potrebe ustanovljene neprofitne laboratorije za digitalno forenziko, ki so financirani iz proračuna. Razprava se je razvnela tudi ob vprašanju, kakšno izobrazbo naj bi imeli digitalni forenziki. Zanimivo je, da so udeleženci, ki vodijo ali delajo v institucijah, ki v praksi opravljajo digitalne forenzične preiskave, vsi po vrsti povedali, da se izogibajo zaposlovanju kadra z univerzitetno izobrazbo, ker je pri tehničnih opravilih v veliki večini neuporaben (kot je dejal A. Wagner: »Če dam univerzitetnemu diplomiranemu inženirju v roke kladivo, sem napravil zgolj eno stvar: ustvaril precejšnjo nevarnost, da se bo poškodoval.«). Osebno me je ta podatek presenetil in mi hkrati povedal, da na univerzah očitno delamo nekaj hudo narobe. Sicer pa sem si zelo zapomnila opozorilo enega od udeležencev, ko je razprava tekla o tem, ali morajo imeti digitalni forenziki tudi pravna znanja. *Just don't teach them too much law*! (Ne učite jih preveč prava!). Ugovor!

Zelo zanimivo je bilo tudi predavanje ***Keitha Foggona***, vodje enote za digitalno forenziko pri britanskem Uradu za boj proti resnemu kriminalu (*Serious Fraud Office*). G. Foggon je predstavil delo svoje enote. S pribl. 3 mio funtov letnega proračuna imajo zagotovljeno vrhunsko strojno in programsko opremo, vključujejo pa se v preiskave različnih oblik finančnih goljufij, pa tudi drugih resnih oblik kriminala (praviloma takega, kjer gre za sum protipravne premoženjske koristi vsaj v višini enega milijona funtov). Poudaril je, da uspehi urada temeljijo na usklajenem multidisciplinarnem pristopu pri preiskovanju, kar v praksi pomeni, da so preiskovalne skupine za vsak konkreten primer sestavljene iz različnih strokovnjakov. Preiskovalno skupino vedno vodi tožilec, v njej pa sodelujejo agentje urada, pravniki, ena ali več policijskih enot, svetovalci, IT forenziki iz enote za digitalno forenziko, po potrebi pa tudi zunanji sodelavci (računovodje in podobno).

Andreas Wagner, v Savdski Arabiji živeči Nemec, ki v podjetju Al-Hisn Al Waqi For Techonology Services iz Riada orje ledino pri postavljanju temeljev informacijske varnosti v tej državi, nam je predstavil drugačen svet. Do nedavna je bila Savdska Arabija zaprta država, kar se tiče sodobnih tehnologij. To se spreminja, s tem pa Savdijci postajajo lahka tarča različnih struktur IT-kriminala. K temu precej pripomoreta njihova kulturno pogojena poštenost in zaupljivost, česar se kralj oziroma vlada zavedata, zato vlagajo ogromna sredstva ne le v informatizacijo države, ampak tudi v zagotavljanje informacijske varnosti njenih prebivalcev.

David Pretty iz Guidance Software Inc. (ZDA) je predstavil BitLocker, to je posebno programsko orodje operacijskega sistema Windows Vista, ki uporabnikom omogoča kvakovostno zaščito podatkov. Poleg tehničnih značilnosti je predavatelj opisal prednosti uporabe tega orodja, ki se pokažejo zlasti v primeru kraje računalnika ali vdora vanj. Do podatkov, kriptiranih z orodjem BitLocker, tat oziroma vsiljivec ne bo prišel, četudi ima vrhunsko hekersko znanje. To, kar utegne biti za uporabnika zoprno, pa je, da v primeru izgube ključa za dostop tudi sam svojih podatkov ne bo več videl. Seveda do teh podatkov brez ključa (zaenkrat) ne morejo niti digitalni forenziki.

Predavanje ***Russla Maya*** iz podjetja AcessData (ZDA) je izzvalo največ vprašanj in je bilo za večino udeležencev najbolj zanimivo. Žal kaj več kot naslova ne morem zapisati: *Računalniško forenzično preiskovanje z uporabo FTK 2.0* (*Computer Forensic Investigations Using FTK 2.0*). Predavatelj je predstavil Forensic Toolkit 2.0, to je nova različica forenzičnega orodja, ki ga razvija podjetje AcessData. Predavanje je bilo povsem tehnične narave in kljub pozornemu poslušanju, resnici na ljubo, nisem razumela ničesar. Lahko pa sem razbrala, da gre za dobro, pogosto uporabljano (in drago) orodje za forenzične preiskave računalniške opreme, ki naj bi prišlo na trg februarja 2008.

Digitalni forenzični forum je pokazal, da je na področju digitalne forenzike znanje skoncentrirano zlasti v ZDA in Veliki Britaniji, ki v to področje vlagata tudi največ sredstev. Vendar se pri želji po čim večji učinkovitosti ter izrabi vseh možnosti, ki jih nudi sodobna tehnologija, ti dve državi soočata s pomembnimi vprašanji pravne narave. Ena izmed zelo vročih točk je trenutno privilegij zoper samoobtožbo. Ameriška in od oktobra 2007 tudi britanska zakonodaja namreč določata zaporno kazen za osumljenca, ki preiskovalcem ne da ključa za dostop do kriptiranih dokumentov na svojem računalniku. Ta vrsta prisile je predmet burnih razprav, sodna praksa v ZDA je glede tega neenotna, v Veliki Britaniji pa je zaenkrat še ni. Izzivov za naslednji Digitalni forenzični forum, na katerem bo treba reči tudi kakšno o pravu, torej ne manjka!

Liljana Selinšek

Konferenca o zaščiti finančnih interesov Evropske unije in Švice

Basel, 10. - 12. december 2007

Basel, tretje največje švicarsko mesto in obenem tudi glavno mesto enega od šestindvajsetih kantonov, je 10. in 11. decembra 2007 gostil konferenco, ki je osvetlila izzive, s katerimi se skupaj in vsaka posebej soočata Evropska unija in Švica pri zaščiti svojih finančnih interesov.

Konferenco sta organizirala *Academy of European Law (ERA)* in *Basel institute of governance* s finančno pomočjo *Evropskega urada za boj proti goljufijam (OLAF)*, namenjena pa je bila predvsem strokovnjakom s področja zaščite finančnih interesov, raziskovalcem s tega področja, pravnikom v evropskih institucijah ter pravosodnim organom držav članic EU in Švice. Udeležba na konferenci, ki je potekala v treh jezikih, je bila zavidljiva, organizacija pa prav po švicarsko brezhibna.

Uvodna razprava je ponudila kratek pregled nad problematiko in prerez glavnih vprašanj, s katerimi se soočata EU in Švica. Glavni govorec je bil ***Paolo Casaca***, poslanec Evropskega parlamenta in član parlamentarnega Odbora za proračunski nadzor, ki je pristojen za nadzor izvrševanja proračuna Unije, obravnavo goljufij in nepravilnosti pri tem izvrševanju, ukrepe za preprečevanje in pregon takšnih primerov, zaščito finančnih interesov Unije na splošno ter nekatere druge naloge. Casaca je v svojem nagovoru izpostavil enega od ključnih problemov te konference. Sredstva, ki jih EU vsako leto izgubi na račun goljufij zaradi davka na dodano vrednost, znašajo dobro polovico evropskega letnega proračuna. Stanje, ki je posledica dolgoročne uveljavitve »začasne« rešitve, po kateri davek plačuje končna država porabe, ni vzdržno in terja spremembe, vendar teh v bližnji prihodnosti zaradi pomanjkanja politične volje še ne gre pričakovati. Ravno zaradi tega je nujno, da se v danih okvirih vzpostavi kar najučinkovitejši nadzor in možnosti ukrepanja, ki bi trenutno situacijo vsak nekoliko omilile.

Kakšna je v tem oziru vloga Švice? Švica, ki je v očeh mnogih še vedno raj za finančne sleparje, je po eni strani v resnici država, kjer tudi v škodo evropskega proračuna potekajo nezakoniti posli, po drugi strani pa je Švica eden od partnerjev EU v boju proti takšnim goljufijam. Zavezo Švice po mnenju švicarskih govorcev, predvsem ***Rudolfa Wyssa***, podpredsednika Zveznega pravosodnega urada, potrjuje tudi (zaenkrat enostranska) ratifikacija bilateralnega sporazuma med Švico in Evropsko unijo v boju proti goljufiji. Wyss je s tem odprl drugo ključno vprašanje, ki se je nadaljevalo skozi celotno razpravo, izpostavil je namreč dejstvo, da je EU po večletnih pritiskih na Švico, ki so po trdih pogajanjih leta 2004 vendarle privedli do bilateralnega sporazuma, sama zaustavila možnosti sodelovanja, saj je sporazum zaenkrat ratificirala le slaba polovica vseh držav članic.

Da je to velika težava, s katero se je nujno soočiti, je priznal tudi ***Lothar Kuhl***, vodja OLAF-ove enote za zakonodajo. Težava je tudi v tem, da je sporazum bilateralen med Švico in Evropsko unijo kot celoto, zato se niti za razmerja med Švico in posamezno državo članico, ki ga je že ratificirala, ne more izvajati. Kuhl je poudaril tudi, da tudi OLAF ni pričakoval takšnega zastoja, saj sporazum ne cilja na notranje pravo držav članic in bi te zato ne smele imeti toliko težav pri ratifikaciji. Kljub temu pa od Švice ob danih predpisih pričakuje večjo pripravljenost na sodelovanje, predvsem pa hitrejše postopanje.

Ker so v primerih goljufij pomemben dejavnik banke, ki imajo v Švici prav posebno mesto, je na njihove dileme opozorila ***Renate Schwob***, članica izvršnega odbora Združenja švicarskih bank. Kot je bilo pričakovati, je opozorila na zaupnost odnosa med banko in njenimi strankami ter zatrdila, da švicarske banke že sedaj v celoti sodelujejo tudi z evropskimi organi.

Različni govorci so nato prikazali obstoječe sisteme, namenjene zaščiti finančnih interesov, ter različne pristope k problematiki. Skupna ocena evropske zaščite je bila, da ta sicer na nek način deluje, da je pa še vedno daleč od tiste zaščite, ki bi si jo v dobro evropskih državljanov želeli. Ob tem je bilo s stališča Švice poudarjeno tudi, da ta že nekaj časa ni več center za pranje denarja in podobne nezakonite posle, saj se ti selijo v npr. Dubaj ter druge države z ohlapnejšo zakonodajo in manjšo mednarodno vpetostjo.

V nadaljevanju je bilo predstavljeno švicarsko stališče do Evropske unije, predvsem strah pred pretirano vpetostjo v to organizacijo na eni strani ter želja po sodelovanju na drugi. Profesorica Pravne fakultete Univerze v Baslu, ***Sabine Gless***, je poudarila, da je Švica do nedavnega trdno vztrajala, da bo z EU na pravnem področju sodelovala le pri tistih primerih, ki so kaznivi tudi v Švici, s podpisom sporazuma o boju proti goljufiji pa je (za to področje) privolila v sodelovanje z zelo malo zadržki. Odločitev o vstopu v schengensko območje (za kar so se državljani odločili na referendumu leta 2005, dejanski datum vstopa pa se vztrajno odmika v prihodnost) ter pristop k Dublinskemu sporazumu sta njeno avtonomnost še znatno omejili.

Glavna problema švicarskega sodelovanja z EU v primerih zaščite finančnih interesov sta dva; izogibanje davkom (tukaj pomenijo težavo predvsem tradicionalna švicarska za-

upnost podatkov o bančnih računih ter politika ne-izročanja, ne-zaplembe ipd.) ter pranje denarja. Kljub zatrjevanju predstavnikov bank, da na tem področju sodelujejo s tujimi službami, kolikor je le mogoče, je bilo s strani praktikov izraženo precejšnje nezadovoljstvo z njihovo dejansko angažiranostjo. Prav zato so spremembe, ki jih uvajajo nove pogodbe med Švico in EU, tako težko pričakovane.

Drugi dan konference je bil zasnovan bolj interaktivno, saj so bili v manjših skupinah predstavljeni posamezni primeri, pri katerih je prišlo do sodelovanja med Švico in posameznimi telesi EU. Sama sem sodelovala v skupini, ki jo je vodil ***Stefan Obermaier***, predstavnik OLAF-a. Predstavil je uspešno posredovanje svojega urada v primeru korupcije v Lesotu. EU je namreč Lesotu podarila večji del sredstev (3,6 milijarde evrov) za izgradnjo vodnih jezov za hidroelektrarne, zaradi česar je imela ob sumu korupcije neposredni pravni interes za uspešen pregon. Izkazalo se je, da je kraljevi uradnik, odgovoren za gradnjo jezov, od štirih večjih mednarodnih gradbenih podjetij prejel velike zneske podkupnine, ki so zagotovili njihovo udeležbo pri gradbenih delih. Za afriško državo je bil postopek zelo zahteven, OLAF pa je pomoč nudil predvsem pri pravnih vprašanjih s področja nasledstva (saj so se gradbena podjetja na vso moč trudila zabrisati sledi) ter pri vzpostavljanju stikov s Švico, v kateri so bile na raznih računih shranjene vse podkupnine. Primer, za katerega sta glavna lesoška tožilca prejela tudi mednarodno tožilsko nagrado, je pozitiven z dveh vidikov, prvič zato, ker so v bitki med Davidom in Goljatom mednarodni gradbeni giganti potegnili ta kratko in poleg velikih denarnih kazni svoja dejanja plačali tudi s prepovedjo dela na nadaljnjih projektih Mednarodne banke, drugič pa zato, ker se je OLAF izkazal za koristnega in uspešnega posrednika pri preiskovanju velikih goljufij.

Za drugi primer, ki bi pokazal nekoliko manj svetlo plat OLAF-ovega delovanja, predvsem zaradi nezmožnosti poplačila, povezane z uspešnim prelivanjem sredstev z računa na račun in posledično izgubo pravih sledi za denarjem, je na konferenci zmanjkalo časa, saj je bila razprava ob prvem primeru poglobljena in precej obširna. Precej se je vrtela tudi okrog OLAF-a in njegove vloge ter pooblastil.

Poslanstvo OLAF-a je zaščita finančnih interesov Evropske unije, ob tem pa tudi boj proti goljufijam, korupciji in drugim nepravilnostim, vključno z nepravilnostmi znotraj institucij EU. Za opravljanje naštetih nalog ima OLAF več možnosti, med drugim lahko samostojno opravlja notranje in zunanje preiskave, možno pa je tudi sodelovanje s pristojnimi organi znotraj držav članic ter predvsem koordiniranje njihovega delovanja v primeru udeležbe več držav članic. Ključno je tudi, da državam članicam zagotavlja strokovno znanje in izkušnje ter tehnično opremo za preganjanje primerov goljufij. Preiskovalna dejanja, ki jih opravlja OLAF, ne vodijo do konkretnih kazenskopravnih rezultatov, niti OLAF od posameznih organov držav članic ne more zahtevati uvedbe konkretnega postopka. Kljub temu pa se samo po sebi postavlja vprašanje zaščite preiskovancev, ki je prav zaradi upravne narave postopka na bistveno nižji ravni, kot bi sicer bila v kazenskem postopku, posledice takih preiskovalnih dejanj in posegi v posameznikove pravice pa so lahko izjemno agresivni. Težavo, ki nikakor ni majhna, zaenkrat skušajo reševati postopkovna pravila, ki pa si jih postavlja OLAF sam, ter zaupanje v samoomejevanje posameznih preiskovalcev in spoštovanje deklariranih načel Urada, kot so nepristranskost, profesionalnost ter predvsem spoštovanje človekovih pravic.

Konferenca se je zaključila s sklepnimi mislimi razpravljavcev, ki so povzeli dvodnevno razpravo, popoldne pa je ostalo za spoznavanje švicarskega sira in čokolade ter za sprehod po »najdaljši božični ulici v Evropi«.

Mojca Mihelj Plesničar

Poročilo s 15. kongresa Mednarodnega združenja za družbeno obrambo in humano kriminalitetno politiko

Toledo (Španija), 20. – 22. september 2007

Med 20. in 22. septembrom je v Toledu v Španiji potekal 15. kongres Mednarodnega združenja za družbeno obrambo in humano kriminalitetno politiko na temo »Kazensko pravo med vojno in mirom: pravičnost in sodelovanje v kazenskih zadevah v mednarodnih vojaških posegih«.

Mednarodno združenje za družbeno obrambo je bilo ustanovljeno po drugi svetovni vojni z namenom ponuditi znanstvene odgovore na probleme, povezane s kriminaliteto in njenim preprečevanjem. Znanstveni pristop združenja je veliko bolj kot eksegeza pravnih pojmov zaznamovala socialna naravnanost: v ospredju zanimanja je bil storilec in njegovo (potencialno kriminogeno) družbeno okolje, manj pa operiranje z abstraktnimi pravnimi pojmi in pravna dogmatika. Glavnega cilja kazenske intervencije združenje ni videlo v represiji in retributivnosti, temveč predvsem v preventivnem delovanju

in resocializaciji storilcev kaznivih dejanj. Ob zavedanju, da takšno terapevtsko naravnano kazensko pravo v sebi nosi nevarnost zlorab in kršitev človekovega dostojanstva, združenje ni spregledalo, da socialno-preventivno delovanje ne sme iti na račun zakonitosti, pravne varnosti, spoštovanja človekovih pravic, dostojanstva in humanosti. Pozneje je v svoj naziv posebej dodalo humano kriminalitetno politiko, tako da je polni naziv združenja danes Mednarodno združenje za družbeno obrambo in humano kriminalitetno politiko.

Kljub temu, da sta povojni optimizem in navdušenje nad terapevtskim modelom kazenskega prava v sedemdesetih letih minulega stoletja začela postopno usihati, vse bolj pa ju je izpodrival pesimizem v smislu »nič ne deluje« in čedalje večja naklonjenost bolj represivni kriminalitetni politiki, se je združenje ohranilo in nadaljuje s svojim delom. Ideje, ki jih razvija, skušajo ostati »v mejah možnega« in niso več tako radikalne kot tiste *Filipa Gramatice* (ustanovitelja združenja), ki je menil, da je treba koncept kazenske odgovornosti nadomestiti s konceptom antisocialnosti, kazni pa z ukrepi družbene obrambe. Kljub manjši vlogi kot nekoč pa združenje ostaja ena izmed institucij, ki so sposobne in pripravljene kritično pretresati razvoj kazenskega prava in opozarjati na potencialne nevarnosti, ki jih prinaša »rekonceptualizacija« kazenskega prava, katere edina vodilna misel je večja učinkovitost.

15. kongres Združenja je zaznamovalo obravnavanje aktualnih vprašanj mednarodnega kazenskega in humanitarnega prava. Med temami so bile na dnevnem redu: vloga kazenskega prava v zvezi z mednarodnimi mirovnimi misijami (kazenska odgovornost pripadnikov mirovnih operacij), pravna sprejemljivost novih zamisli o načinih »boja proti terorizmu«, smiselnost delitve kazenskega sodstva na civilno in vojaško in še nekatere druge.

Kljub temu, da je bila vsebina referatov precej heterogena, je mogoče izluščiti nekaj težišč izvajanj, od katerih bi tukaj rad opozoril predvsem na dve.

Pomembno mesto je imela razprava o kazenski odgovornosti pripadnikov mirovnih operacij za kazniva dejanja, ki jih izvršijo v državi gostiteljici. Izkušnje kažejo, da tovrstna kaznivа dejanja niso redka, le redko pa jim sledi ustrezen kazenski pregon. Države gostiteljice teh dejanj kljub podani represivni oblasti (teritorialno načelo) pogosto ne morejo preganjati zaradi dejanskih ovir (nedelovanje pravosodnega sistema) ali pravnih ovir (imunitete, sporazumi o izključni jurisdikciji države pošiljateljice). Po drugi strani pa države pošiljateljice pogosto niso zelo zavzete za pregon tovrstnih kaznivih dejanj, med drugim zato, ker nerade javno priznajo možnost, da so njihovi vojaki na mirovnih operacijah izvršili kazniva dejanja. Če pa do pregona pride, so precej verjetne težave pri dokazovanju, saj je bilo dejanje izvršeno daleč stran, neredko na drugi celini, s čimer je dostop sodišča do žrtev, prič in drugih dokazov otežen. In končno, če do pregona pride in je na voljo tudi dovolj dokazov za obsodbo, je kaznovalna politika sodišč držav pošiljateljic do svojih vojakov lahko tudi izrazito protekcionistična. Kot za možni rešitvi težave so se referenti zavzemali predvsem za zamisel ustanavljanja posebnih hibridnih sodišč kot dela pravnega sistema države gostiteljice, v katerih bi sodelovali predstavniki obeh držav, in za sojenje v državi gostiteljici s pomočjo ZN (ki naj obdolžencu zagotovi spoštovanje mednarodnih standardov človekovih pravic).

Drugo pomembno vprašanje, o katerem je bil govor na kongresu, je bilo vprašanje uporabe univerzalnega načela v praksi. Čeprav poznajo kazenske zakonodaje številnih držav univerzalno načelo, ki omogoča kazenski pregon tudi, kadar gre za primere »tujega državljana, ki v tujini izvrši kaznivo dejanje zoper tujega državljana ali zoper tujo državo«, pride v praksi do takšnih pregonov sorazmerno redko. Iz medijev so še posebej znani primeri ovadb zoper pomembne ameriške politike, ki so bile vložene v Belgiji in Nemčiji. Čeprav bi bil pregon teh oseb na podlagi univerzalnega načela teoretično možen, občutek za politični realizem pove, da je komaj verjeten. Referent iz Nemčije je obširno poročal o »zadevi Rumsfeld«, v kateri so nevladne organizacije vložile ovadbo zoper Donalda Rumsfelda, saj naj bi bil na podlagi določb o poveljniški odgovornosti (ki jih vsebuje nemški mednarodni kazenski zakonik – *Völkerstrafgesetzbuch*) odgovoren za nečlovečno ravnanje z zaporniki v Abu Grajbu in Guantanamu. Nemško generalno državno tožilstvo je ovadbo zavrglo z argumentom, da je ustrezen kazenskopravni odziv mogoče pričakovati v ZDA (sic), zato nemška kazenskopravna intervencija ni potrebna. Referent je opozoril, da je bilo od sprejetja nemškega mednarodnega kazenskega zakonika (ki omogoča zelo široko uporabo univerzalnega načela) vloženih še približno 60 drugih kazenskih ovadb, a v nobeni zadevi ni prišlo niti do preiskave. Izrazil je zaskrbljenost, da imajo pri odločanju o uporabi univerzalnega načela politična tehtanja popoln primat nad pravnimi.

Konferenco so sklenili splošnejši referati o vlogi kazenskega prava v času globalizacije (*Mireille Delmas-Marty*) oziroma o izzivih za tradicionalno kazensko pravo v času »družbe tveganja« (*Ulrich Sieber*). Kot je za združenje značilno, so na kongresu prevladovali udeleženci z romanskim poreklom: Francozi, Italijani, Španci ter udeleženci iz Latinske Amerike. Obiskovalec, bolj navajen na germansko pravno okolje, bi utegnil zaznati nekaj pomanjkanja »časovne discipliniranosti« (podaljševanje sekcij ter odmorov). Vendar pa tega ne kaže jemati kot hibo, temveč nasprotno, kot simpatičen izraz predanosti – tako sekcijam kot odmorom.

Matjaž Ambrož