CHALLENGES OF THE DIGITAL ENVIRONMENT FOR PERSONAL DATA PRIVACY AND SECURITY

Nina Gumzej
Faculty of Law, University of Zagreb, Zagreb, Croatia /1/

Abstract
In the introduction the author explains the more recent challenges for individuals' rights in relation to protection of security and privacy of their personal data processed in the digital globalized environment, which is characterized by rapid development of information and communication technologies and services. This is followed by analysis of a number of EU and Croatian legal sources relevant for that area. Case law of the EU Court of Justice with a focus on online personal data processing issues is further examined, including the most recent judgments on invalidity of the Data Retention Directive and on the right to be forgotten online. After explaining recent developments in the field and the requirements to adjust the legal framework to contemporary data processing conditions the author next analyses selected solutions of proposed new EU general legal framework, *i.e.* General Data Protection Regulation. In concluding remarks the author points *inter alia* to the need for raising awareness of all stakeholders on issues examined in this paper and ensuring conditions towards a more effective domestic general data protection framework.

Keywords: personal data protection, privacy, electronic communications, Internet, proposal for EU General Data Protection Regulation

1. Uvod

Brojne koristi koje donosi i omogućuje globalno umrežavanje kao i brz i propulzivan razvoj informacijskih i komunikacijskih tehnologija i sustava u modernom društvu danas se moraju sagledavati i iz aspekta pojavnosti mogućih povezanih rizika za umrežene pojedince i njihova temeljna prava i slobode. Posljednjih godina svjedoci smo, naime, naglog razvoja visokih tehnologija koje omogućuju, između ostalog, sve složenije i sofisticiranije načine obrade osobnih podataka, tj. radnji koje se vrše nad podacima koji se odnose na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (ispitanik). Osobni podaci smatraju se „novom naftom interneta i novom valutom digitalnog svijeta" /2/, što potvrđuje snažan razvoj tržišta tih podataka. U isto vrijeme jasno je i da se digitalna ekonomija zasniva na povjerenju korisnika da će se njihovi podaci zakonito prikupljati i obrađivati te da će poduzimati odgovarajuće mjere njihove zaštite od bilo kojeg oblika zlouporabe. Tako je, unatoč specifičnoj prirodi interneta kao otvorene globalne mreže koja dopušta prijenos informacija, važno raditi na osiguravanju jamstava pravne zaštite u vezi s obradom osobnih podataka umreženog pojedinca koji se obrađuju *online,* isto kao što se ta zaštita jamči prilikom obrade njihovih podataka u zatvorenom, *offline* okruženju /3/.

Današnja je tehnologija uz digitalizaciju mreža i usluga usmjerena prema daljnjem razvoju ultrabrzih mreža i sve naprednijoj konvergenciji raznih elektroničkih komunikacijskih uređaja i usluga (podaci, glas, radio/TV i dr.), a elektroničke komunikacije sve više postaju temeljna infrastruktura koja omogućava obavljanje i zadovoljavanje najrazličitijih poslovnih i osobnih potreba poput informiranja i obrazovanja, elektroničke trgovine, zabave i društvenog života itd. Tehnološki razvoj u području elektroničkih komunikacija te informacijskih i komunikacijskih tehnologija i usluga i njihova dostupnost građanima danas više nego ikada prije podrazumijeva postojanje mogućnosti, odnosno sredstava za identifikaciju, praćenje i analizu njihova ponašanja. Razlog je tome pohrana podataka koji se generiraju već samim njihovim korištenjem elektroničkih komunikacija i različitih komunikacijskih usluga i koji se sve više smatraju podacima koji se tiču njihova privatnog života. Osim toga, u visoko kompetitivnoj ekonomiji digitalnog tržišta sve veći je broj usluga i proizvoda koji se zasnivaju na personalizaciji, tj. individualnim navikama i željama korisnika, što se omogućuje njihovim praćenjem i profiliranjem, kako bi se što je moguće više točnije ciljale njihove predviđene potrebe i interesi. Praćenje pojedinaca i njihovih aktivnosti na mreži uz pomoć tehnologije kao i mogućnosti obrade velike količine digitalnih podataka koji se na njih odnose omogućuju se na sve sofisticiraniji način. Nadalje, mogućnost identifikacije umreženog pojedinca više ne podrazumijeva potrebu dobivanja odgovora na pitanje može li se saznati njegovo ime jer se praćenjem sredstava za nadzor prometa u mreži omogućuje utvrđivanje ponašanja uređaja koji služi za spajanje na internet s ciljem da se tako identificiranog pojedinca, izdvojenog od korisnika drugih uređaja, tretira na određeni poseban način i profilira s obzirom na ponašanje u mreži (navike, interesi, osobnost) /4/. *Profiliranje* u najširem smislu tog pojma uključuje rudarenje velike količine podataka koji su se prikupljali u postupku skladištenja podataka da bi se potom donijeli zaključci o poveznicama između određenih vrijednosti koje se žele primijeniti na konkretne osobe kako bi se polučio željeni rezultat (kao što je to, npr., postizanje toga da se osoba ponaša na određeni željeni način) /5/. Pritom se koriste različite moderne tehnologije kao što su nadzor i praćenje putem GPS tehnologija /6/ i dubinsko pregledavanje sadržaja paketa prometa koji se prenose mrežom /7/, videonadzor i dr. Osim u komercijalne svrhe, profiliranje se koristi u svrhu borbe protiv teških kaznenih djela poput terorizma (npr. u kontekstu predviđanja terorističkih prijetnji i napada) /8/. Postupci profiliranja sve su popularniji i zato što ne podrazumijevaju pretjerano visoke troškove za postizanje željenih rezultata. Oni mogu uključivati i praćenje ponašanja pojedinaca tijekom njihova korištenja elektroničkih komunikacijskih usluga i usluga informacijskog društva kako bi se u odnosu na njih poduzimale ciljane radnje poput ponude personaliziranih oglasa (*online* ciljano ili bihevioralno oglašavanje). To je čest slučaj kod pružanja internetskih usluga koje su za korisnike besplatne i koje se u većoj ili manjoj mjeri financiraju na temelju suradnje davatelja navedenih usluga s oglašivačima. Takvo oglašavanje traži što veću predvidljivost mogućeg ponašanja pa prema tome i sve detaljnije podatke o ponašanju korisnika radi izrade što točnijeg profila. U razmatranju takvog oglašavanja posebna se pozornost, među ostalim, upućuje pitanju razmjene informacija o *online* ponašanju pojedinca unutar mreže većeg broja oglašivača /9/.

Značajno širenje opsega prikupljanja, razmjene, korištenja i svih drugih oblika obrade osobnih podataka te najrazličitiji, sve kompleksniji oblici njihove obrade u digitalnim globaliziranim uvjetima naglašavaju i pitanje mogućnosti održavanja „kontrole" nad njima i njihovim upravljanjem u kibernetičkom prostoru koji ne poznaje teritorijalne granice. Društveno-ekonomski trendovi značajno doprinose iznimnoj popularnosti usluga koje se pretežito zasnivaju na konceptu prikupljanja, razmjene i najrazličitijih oblika obrade sve većih količina osobnih podataka kojima ne pripadaju samo „klasično" pribavljeni osobni podaci koje korisnici svjesno i svojevoljno

pružaju (objavljuju) nego i podaci koji se generiraju kroz njihovo korištenje internetskih usluga i na isto odnose. Sve je više dostupnih besplatnih ili barem ekonomski isplativih rješenja koji nude virtualnu pohranu osobnih podataka i druge usluge njihove obrade *online*. Tima svakako pripadaju i osobito popularne tzv. *web 2.0 usluge uz sadržaj koji stvaraju sami korisnici* /10/ kao što su, primjerice, usluge *online* društvenih mreža, a koje zauzimaju bitan dio digitalnog tržišta i čije korištenje pretpostavlja, ovisno o pojedinom modelu korištenja, različite razine gubitka kontrole nad osobnim podacima. *Usluge računarstva u oblaku* mogu ovisno o pojedinom modelu podrazumijevati pohranu osobnih podataka na poslužiteljima koji se nalaze pod kontrolom trećih strana (to jest davatelja tih usluga) i kojima korisnik koji je ugovorio korištenje odgovarajuće usluge u oblaku pristupa udaljenim pristupom. U određenim slučajevima podaci pohranjeni u oblaku prenositi će se na poslužitelje u trećim zemljama koje i nemaju osiguranu odgovarajuću razinu zaštite osobnih podataka. Postavljaju se ovdje i brojna druga pitanja, među ostalim pitanja odgovornosti za provedbu zaštite u multinacionalnom okruženju, tko i u kojim uvjetima može pristupati navedenim podacima (uključujući tijela za provedbu zakona), vlasništva nad podacima pa sve do načina na koji se osigurava njihova zaštita od gubitka ili uništenja, odnosno bilo kojeg oblika zlouporabe, mjerodavnog prava i načina rješavanja sporova u multinacionalnom okruženju. Ta se pitanja intenzivno razmatraju na razini EU-a osobito u kontekstu jedinstvene europske strategije za razvoj računalstva u oblaku koja je donesena 2012. godine /11/.
Osim toga, kada je riječ o naprednim tehnologijama, posljednjih godina razmatraju se i pitanja u vezi s primjenom tehnologije identifikacije putem radiofrekvencije (dalje: RFID), posebice RFID uređaja i aplikacija funkcionalnih za obradu osobnih podataka i povezivanje na komunikacijske mreže. Naime, ugradnjom RFID etikete svakoj se stvari dodjeljuje jedinstveni identitet. Riječ je o o elektroničkom čipu s pohranjenim informacijama koji ima mogućnost komunikacije radiosignalima (radiovalovima) s RFID čitačem. Tako RFID čitač koji komunicira s etiketom može učitati, na primjer, svojstva stvari u kojoj je etiketa ugrađena. U RFID etiketi se također mogu pohranjivati osobni podaci koje RFID uređaji/aplikacije mogu čitati, odnosno obrađivati, a uz povezivanje na komunikacijsku mrežu ti se podaci mogu i dalje prenositi i obrađivati također i u, primjerice, javnoj elektroničkoj komunikacijskoj mreži. RFID tehnologija nije sama po sebi novost, no uslijed sve intenzivnije primjene RFID sustava putem kojih se omogućuje obrada podataka koji se odnose i na pojedince, uz mogućnosti daljnjeg povezivanja na komunikacijske mreže (a u okviru kojih se onda ti podaci dalje obrađuju), posljednjih su godina na razini EU-a posebno aktualna nastojanja da se utvrde postupci ranog prepoznavanja i minimalizacije rizika koje njezina uporaba može imati na niz aspekata prava na privatnost pojedinaca, osobito u vezi s obradom njihovih osobnih podataka. To treba imati na umu i s obzirom na to da se s razvojem RFID tržišta omogućuje pojavnost posebnog umreženog stanja koje karakterizira povezanost i komunikacija između svih međusobno povezanih stvari u komunikacijskoj infrastrukturi pa tako i povezanost i komunikacija korisnika stvari sa stvarima (tzv. internet stvari, engl. *Internet of things*). Sudjelovanje osoba u takvu okruženju omogućava obavljanje brojnih automatiziranih i za korisnika potencijalno nevidljivih modaliteta obrade niza različitih podataka koji se na njih odnose, stoga je nužno raditi i na prilagodbi pravnog okvira radi uvažavanja uključenih rizika za privatnost i zaštitu osobnih podataka i osiguravanja njihove odgovarajuće zaštite, uz nužnu podršku odgovarajućih tehnoloških mjera. Kao i kod usluga računarstva u oblaku, time se ujedno stvaraju preduvjeti za nužno jačanje povjerenja korisnika u vezi s korištenjem internetskih usluga i novih tehnologija, stoga se i ta pitanja ozbiljno razmatraju na razini EU-a /12/.

Sve ranije izloženo predstavlja novije izazove pred pravno područje zaštite osobnih podataka, posebice u današnje, kako se katkad naziva, doba velikih podataka (engl. *Big Data*) /13/ u kojem se sve više i sve lakše omogućuje identifikacija, tj. prepoznavanje umreženih sudionika na temelju digitalnih identifikatora (Internet Protokol adresa /14/, RFID etiketa, kolačića /15/ i dr.), osobito uz pomoć modernih sustava za rudarenje podataka koji se povezuju s velikim bazama podataka. U takvim uvjetima postupci anonimizacije, kojima bi se moralo osigurati da se više ne radi o podacima koji se odnose na osobu koja bi mogla biti identificirana, sve više predstavljaju poseban izazov s obzirom na najnovija dostignuća u razvoju tehnologije koja omogućuje njihovu povratnu identifikaciju /16/.

Osim toga, u globalno umreženom komunikacijskom okruženju osobito je važno kontinuirano pratiti prijetnje i opasnosti za sigurnost i integritet informacijskih sustava, mreža i usluga, odnosno prijetnje koje u digitalnom okruženju predstavljaju sve brojniji oblici kibernetičkog kriminala /17/. Globalni razvoj informacijskih tehnologija i mreža pogodovao je, naime, razvoju kaznenih djela koja se čine u kibernetičkom prostoru ili uz njegovu pomoć /18/. Također, potrebno je imati na umu i različite mjere koje države koriste radi suzbijanja posebno teških kaznenih djela kao što su ona koja se odnose na terorizam i organizirani kriminal te sve sofisticiraniju tehnologiju i sustave nadzora nad podacima pojedinaca i sve naprednije mogućnosti njihove obrade. Mjere poput obveznog zadržavanja podataka u elektroničkim komunikacijama koje se u pravilu utvrđuju u svrhu borbe protiv teških kaznenih djela, ali koje podrazumijevaju praćenje i pohranu navedenih podataka svih građana za dulji rok, bez obzira na postojanje sumnje u njihovo počinjenje takvih djela, nužno traže uspostavu odgovarajućih pravnih mehanizama radi sprečavanja samovolje i bilo kojih drugih oblika zlouporabe.

Zaštita osobnih podataka područje je prava na čiji je razvoj u Republici Hrvatskoj osobito snažno utjecala relevantna prava stečevina EU-a. Posljednjih je godina upravo na razini prava EU-a prepoznata nužnost osiguravanja novog pravnog okvira, nužno podržanog tehnološkim rješenjima, koji će se učinkovito uhvatiti u koštac s brojnim novijim izazovima i rizicima globaliziranog digitalnog okruženja i brzog tehnološkog razvoja, a koji, među ostalim, omogućuju sve različitije, intenzivnije i rasprostranjenije aktivnosti obrade osobnih podataka. U navedenim je uvjetima, naime, nužno osigurati mehanizme smislene i doista učinkovite zaštite prava pojedinaca u vezi s obradom njihovih osobnih podataka. Neodvojivo od toga je i osiguravanje provedbe potrebnih sigurnosnih mjera radi zaštite podataka, mreža i informacijskih sustava, kao i primjerenog sustava sankcioniranja svih oblika zlouporaba. U radu će se stoga analizirati ključni propisi u relevantnom domaćem pravnom okviru i okviru EU-a s posebnim težištem na općim propisima o zaštiti osobnih podataka i propisima koji uređuju pitanja obrade osobnih podataka i zaštite privatnosti u području elektroničkih komunikacija te ispitati odabrana sudska praksa Suda pravde EU-a kojom se tumači primjena važećeg okvira EU-a u pogledu pitanja zaštite osobnih podataka u digitalnom okruženju. Nakon analize aktualnog stanja na razini prava RH i EU-a analizirat ću ključne novosti u razvoju ovog pravnog područja na razini prava EU-a posljednjih godina. Pritom ću se posebno usredotočiti na ispitivanje odabranih značajki predloženog novog općeg okvira zaštite osobnih podataka koji je danas u zakonodavnom postupka na razini EU-a, a koji je nužno na odgovarajući način pratiti u Republici Hrvatskoj, osobito iz svih ovdje navedenih razloga i zbog značajnog utjecaja na važeći domaći pravno-regulatorni okvir.

2. Važeći pravni okvir RH i EU-a

Temeljni akt EU-a kojim se zaštita osobnih podataka uređuje na općoj razini je Direktiva 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i njihovog slobodnog protoka /19/ (dalje: Direktiva ZOP). Direktiva ZOP implementirana je u domaći pravni okvir država članica EU-a kao i država članica Europskog gospodarskog prostora (EGP - Norveška, Island i Lihtenštajn). Ona je donesena s ciljem postizanja ujednačene razine zaštite prava i sloboda pojedinaca u državama članicama EU-a, poglavito prava na privatnost u vezi s obradom njihovih osobnih podataka sukladno članku 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda te u skladu s temeljnim načelima zaštite osobnih podataka iz Konvencije Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka (dalje: Konvencija 108) /20/. Osim toga, cilj Direktive ZOP je i uklanjanje prepreka slobodnom protoku osobnih podataka, tj. slobodnom razvoju unutarnjeg tržišta. Naime, sustav prijenosa osobnih podataka između navedenih država članica EU-a/EGP-a funkcionira s početnom vrijednosti da sve spomenute zemlje imaju odgovarajuću razinu zaštite osobnih podataka. To podrazumijeva neometani prijenos podataka između tih zemalja kao država s uređenom zaštitom osobnih podataka, što predstavlja temeljni ekonomski smisao Direktive ZOP (neometani razvoj unutarnjeg tržišta). To će načelo također vrijediti kod izvoza osobnih podataka u treće države, tj. države koje nisu spomenute države članice EU-a/EGP-a za koje je Europska komisija posebno utvrdila da imaju odgovarajuću razinu zaštite osobnih podataka. Izvoz podataka moguć je i u drugim, posebno uređenim slučajevima.

Države članice EU-a nisu bile dužne provesti Direktivu ZOP u domaći pravni okvir u područjima koja su do ukidanja stupova EU-a bila izvan okvira prvog stupa Zajednice (funkcioniranje unutarnjeg tržišta) kao što su zajednička vanjska i sigurnosna politika te policijska i pravosudna suradnja u kaznenim stvarima. Zaštita osobnih podataka u vezi s potonjim područjem (bivši treći stup EU-a) uređena je Okvirnom odlukom Vijeća 2008/977/JHA o zaštiti osobnih podataka obrađivanih u okviru policijske i pravosudne suradnje u kaznenim predmetima /21/. Osim toga, zaštita osobnih podataka u vezi s njihovom obradom u tijelima i institucijama EU-a posebno je uređena Uredbom br. 45/2001 Europskog parlamenta i Vijeća o zaštiti osoba pri obradi osobnih podataka u institucijama i tijelima Zajednice te o slobodnome protoku takvih podataka /22/.

Valja napomenuti da Direktiva ZOP ostavlja državama članicama određenu razinu slobode prilikom provedbe pojedinih njezinih odredbi u domaći pravni okvir /23/. One, međutim, to pravo smiju koristiti samo na način predviđen Direktivom i na način kojim se osigurava postizanje njezinih ciljeva /24/. Prema tumačenju Suda pravde EU-a, države članice ne bi smjele na različite načine tumačiti pojedine pojmove Direktive (u pogledu kojih se izričito ne predviđa određena razina slobode kod provedbe u unutarnje pravo) zbog cilja osiguravanja ujednačene razine zaštite osobnih podataka u EU-u. Usklađivanje domaćih propisa ne bi smjelo biti minimalno, tj. ono treba biti *općenito potpuno* (engl. *generally complete*) /25/.

Republika Hrvatska ratificirala je obje ranije navedene konvencije Vijeća Europe /26/, a Ustavom RH još se od 1990. godine svakome jamči sigurnost i tajnost njegovih osobnih podataka (čl. 37.). Međutim, to je područje cjelovito uređeno zakonom tek 2003. godine donošenjem Zakona o zaštiti osobnih podataka (dalje: ZZOP) /27/. Odredbe ZZOP-a od donošenja do danas usklađivale su se poglavito s odredbama Direktive ZOP, a to je i

izričito utvrđeno u okviru izmjena i dopuna tog zakona iz 2011. godine (čl. 1.a, NN br. 130/11). ZZOP uređuje zaštitu osobnih podataka svih fizičkih osoba u RH bez diskriminacije, tj. bez obzira na njihovo državljanstvo i prebivalište te neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili drugim osobinama kao i nadzor nad obradom tih podataka u RH. Zbirke osobnih podataka strukturirani su skupovi osobnih podataka fizičkih osoba (ispitanika) koji su dostupni prema posebnim kriterijima, dok su voditelji zbirki osobnih podataka fizičke ili pravne osobe, državna ili druga tijela koja određuju svrhu i način obrade osobnih podataka. Što se tiče materijalnog područja primjene, ZZOP se primjenjuje na sve aktivnosti obrade osobnih podataka i u javnom i u privatnom sektoru, uz iznimku obrade koju fizičke osobe obavljaju isključivo za osobnu primjenu ili za potrebe kućanstva. To, dakako, ne utječe na mogućnost ograničenja primjene pojedinih odredbi ZZOP-a sukladno posebno propisanim uvjetima i slučajevima. Što se tiče teritorijalnog područja primjene, uvodno treba istaknuti odredbe Direktive ZOP kojima se određuje mjerodavno pravo za obradu osobnih podataka. Mjerodavno pravo za obradu osobnih podataka u pravilu će biti pravo države članice EU-a gdje je osnovan tzv. kontrolor (engl. *controller*), tj. voditelj zbirke osobnih podataka prema terminologiji ZZOP-a, odnosno pravo države članice gdje on ima poslovni nastan (engl. *establishment*). Ako on nije osnovan, tj. nema poslovni nastan u EU-u, ali se oprema koju koristi u svrhu obrade osobnih podataka nalazi na području jedne od država članica EU-a, tada će biti mjerodavno pravo te države članice (osim ako se ta oprema isključivo koristi za svrhe prijenosa podataka preko teritorija EU-a). Navedena odredba prenesena je u ZZOP koji utvrđuje primjenu tog zakona i kada voditelj zbirke nema prebivalište ili sjedište u jednoj od država članica EU-a, ako on koristi automatiziranu i drugu opremu koja se nalazi na području RH za potrebe obrade osobnih podataka (osim ako tu opremu koristi samo za prijenos podataka preko teritorija EU-a). U takvom slučaju voditelj zbirke mora imenovati zastupnika u RH /28/.

Direktiva ZOP nalaže obvezu uspostave nadzornih tijela za zaštitu osobnih podataka koja će s potpunom neovisnošću nadzirati primjenu domaćih propisa koje države članice usvajaju na temelju te direktive. Tu funkciju u RH obavlja Agencija za zaštitu osobnih podataka (dalje: AZOP) koja je, prema tome, zadužena za nadzor nad provedbom zaštite osobnih podataka u RH. ZZOP predviđa samostalnost AZOP-a u obavljanju poslova utvrđenih zakonom i odgovornost prema Hrvatskom saboru kojem podnosi izvješća o radu. Sredstva za rad AZOP-a osiguravaju se u državnom proračunu. Ravnatelja i zamjenika ravnatelja AZOP-a imenuje i razrješava Hrvatski sabor na prijedlog Vlade RH, a uvjeti za njihov izbor odnose se na to da oni moraju biti hrvatski državljani visoke stručne spreme te imati najmanje 10 godina radnog iskustva. Ti uvjeti nisu mijenjani od donošenja ZZOP-a 2003. godine, a to znači i da se do danas za imenovanje nije propisao važan uvjet stručnosti u području zaštite osobnih podataka, odnosno u području zaštite ljudskih prava.

U ZZOP-u su implementirane odredbe Direktive ZOP koje sadrže temeljna pravila o kvaliteti osobnih podataka i zakonitosti njihove obrade kao što su među ostalim osnove kada je dopušteno obrađivati osobne podatke (uz privolu ispitanika, u zakonom određenim slučajevima, itd.). Osobni podaci smiju se prikupljati u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu sa zakonom te se mogu dalje obrađivati samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarna sa svrhom prikupljanja. Oni moraju biti bitni za postizanje utvrđene svrhe i ne smiju se prikupljati u većem opsegu nego što je to nužno da bi se postigla utvrđena svrha. Osim toga, osobni podaci ne smiju se čuvati u obliku koji dopušta identifikaciju ispitanika duže no što je to potrebno za svrhu u koju se podaci prikupljaju ili dalje obrađuju (odgovarajuće mjere zaštite za osobne podatke koji se pohranjuju na duže razdoblje za povijesnu, statističku ili znanstvenu uporabu propisuju se posebnim zakonima). Osobito je važna obveza zaštite osobnih podataka od slučajnoga gubitka ili uništenja i od nedopuštenog pristupa, nedopuštene promjene i objavljivanja te svake druge zlouporabe, a u posebnoj je odredbi u okviru izmjena i dopuna toga zakona iz 2011. godine utvrđeno da mjere zaštite moraju biti razmjerne naravi djelatnosti (voditelja zbirke, odnosno primatelja) i sadržaju zbirke osobnih podataka. U relevantnom prijedlogu izmjena i dopuna ZZOP-a pojašnjava se da je time izvršeno usklađivanje s odgovarajućom odredbom Direktive ZOP (čl. 17.) koja nalaže da se mjerama mora osigurati odgovarajuća razina sigurnosti u odnosu na rizike koji su prirođeni pojedinoj vrsti obrade kao i prirodi podataka koji se obrađuju, uzimajući u obzir najnovija dostignuća (engl. *state of the art*) i troškove provedbe mjera. ZZOP također utvrđuje posebna pravila u vezi s obradom osobnih podataka koji su osjetljive prirode (posebna kategorija osobnih podataka), a među koje pripadaju i podaci o zdravlju. Posebne mjere zaštite tih podataka propisane su Uredbom o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN br. 139/04).

Prema Direktivi ZOP voditelj zbirke može imenovati službenika za zaštitu osobnih podataka koji vodi brigu o zakonitosti obrade osobnih podataka i ostvarivanju prava na zaštitu osobnih podataka i ta je mogućnost uvedena u ZZOP izmjenama i dopunama toga zakona 2008. godine (NN br. 41/08). Postroženim odredbama u okviru izmjena ZZOP-a 2011. godine imenovanje navedenih službenika postala je obveza kada voditelj zbirke zapošljava više od 20 radnika, a tada su nadodane i ponešto detaljnije odredbe o imenovanju službenika i njegovim zadacima.

ZZOP utvrđuje i niz prava ispitanika, a to su, među ostalim, pravo na dobivanje obavijesti o njihovim osobnim podacima koje voditelj zbirke obrađuje i o tome tko je i za koje svrhe i po kojem pravnom temelju te podatke dobio na korištenje i dr. Propisane su i pojedine posebne obveze u specifičnim slučajevima obrade osobnih podataka kao što je to slučaj povjeravanja poslova njihove obrade drugoj osobi ili tijelu kao tzv. izvršitelju obrade koji u tom slučaju vrše obradu isključivo po nalogu voditelja zbirke te u njegovo ime. ZZOP specifično uređuje uvjete pod kojima voditelji zbirki smiju dati osobne podatke na korištenje tzv. primateljima kojima su podaci potrebni radi obavljanja poslova u okviru njihovih zakonom utvrđenih djelatnosti (npr. uvjet prethodnog pisanog zahtjeva primatelja s propisanim obveznim sadržajem). Zakon također sadrži pravila za slučaj izvoza, tj. prijenosa osobnih podataka u treće zemlje kao što je to osobito (ali ne isključivo) pravilo utvrđenja da pojedina zemlja ima uspostavljenu odgovarajuću razinu zaštite osobnih podataka.

Svaka osoba koja smatra da joj je povrijeđeno pravo zajamčeno ZZOP-om ima pravo podnijeti AZOP-u zahtjev za utvrđivanje povrede prava. Rješenje AZOP-a upravni je akt protiv kojeg nije dopuštena žalba, ali se može pokrenuti upravni spor. Zakon također predviđa pravo ispitanika da sukladno općim propisima o naknadi štete pred sudom opće nadležnosti zatraži od voditelja zbirke osobnih podataka naknadu štete koja je nastala zbog obrade njegovih osobnih podataka protivno odredbama tog zakona. U obavljanju nadzora AZOP ima pravo pristupa osobnim podacima, spisima i drugoj dokumentaciji koja se odnosi na obradu osobnih podataka kao i sredstvima elektronske obrade te ima pravo prikupljati sve informacije koje su potrebne za provedbu nadzora. Ako su podaci klasificirani, njima se pristupa sukladno posebnim propisima /29/. Utvrdi li kod obavljanja nadzora povredu zakona, AZOP ima pravo upozoriti ili opomenuti voditelja zbirke (kao i primatelja te izvršitelja obrade) na nezakonitosti u obradi osobnih podataka te rješenjem narediti da se nepravilnosti uklone u određenom roku, odnosno privremeno zabraniti obradu podataka protivno zakonu, narediti brisanje podataka prikupljenih bez pravne osnove, zabraniti iznošenje podataka iz RH itd. Protiv navedenog rješenja AZOP-a nije dopuštena žalba, ali se može pokrenuti upravni spor. AZOP također može predložiti pokretanje postupka kaznene ili prekršajne odgovornosti pred nadležnim tijelom. ZZOP ne predviđa ovlast AZOP-a da izravno izriče sankcije kod utvrđenih povreda.

Prema Direktivi ZOP države članice dužne su osigurati prikladne mjere radi osiguravanja njezine potpune provedbe, a poglavito propisati sankcije za povredu domaćih propisa donesenih na temelju Direktive. U ZZOP-u se prekršajna odgovornost i novčane kazne izričito utvrđuju samo za slučaj povreda pojedinih njegovih odredbi. Tako se, na primjer, izričito ne utvrđuje prekršajna odgovornost u slučaju nezakonitog prikupljanja tj. obrade osobnih podataka, osobito ako je riječ o osjetljivim podacima (posebna kategorija osobnih podataka) i podacima djece. Međutim, prekršajna odgovornost mogla bi posredno nastupiti i kod takvih povreda koje nisu izričito predviđene kao prekršaji jer ZZOP utvrđuje kao prekršaj nepostupanje po naredbi ili zabrani odnosno izdanom rješenju AZOP-a (u vezi s uočenim povredama Zakona) u zadanome roku. Što se tiče iznosa novčane kazne, ZZOP predviđa jedinstveni raspon (20.000,00 do 40.000,00 kuna te 5.000,00 do 10.000,00 kuna za odgovornu osobu u pravnoj osobi, odnosno državnom tijelu te jedinici lokalne i područne samouprave). Posebno se ne propisuju kriteriji za utvrđivanje iznosa kazne u pojedinom slučaju (npr. ako je riječ o lakšoj ili težoj povredi Zakona, ako je riječ o prvoj ili ponovljenoj povredi). Navedeni iznosi nisu se mijenjali od donošenja zakona 2003. godine.

Direktiva ZOP (kao i naš ZZOP) ima opće područje primjene, što znači da se ona primjenjuje na pitanja obrade osobnih podataka ako drugačije nije utvrđeno posebnim propisom koji će se u tom slučaju primjenjivati kao *lex specialis*. Takav je slučaj s Direktivom 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama, skraćeno dalje: Direktiva o e-privatnosti) /30/ koja sadrži posebne odredbe u vezi s obradom osobnih podataka i zaštitom privatnosti u elektroničkim komunikacijama /31/. Ta je Direktiva zadnji puta mijenjana Direktivom 2009/136/EZ o pravima građana u kontekstu novog regulatornog okvira u elektroničkim komunikacijama iz 2009. godine /32/ i tada je, među ostalim, proširenо njezino područje primjene na način da se ona primjenjuje na obradu osobnih podataka u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama, uključujući javnim komunikacijskim mrežama koje podržavaju prikupljanje podataka i identifikacijske uređaje (naglašenim tekstom ističe se relevantna dopuna). Sukladno pojašnjenjima (iz uvodnih izjava) oko proširenja područja primjene Direktive o e-privatnosti, ovdje poglavito treba imati na umu primjenu RFID tehnologije, na koju sam uputila u uvodu rada. Naime, proširenjem područja primjene Direktive osigurava se njezina primjena i onda kada su RFID uređaji, putem kojih se mogu prikupljati, odnosno obrađivati osobni podaci, priključeni na javno dostupnu elektroničku komunikacijsku mrežu ili kada koriste elektroničku komunikacijsku uslugu kao temeljnu infrastrukturu /33/.

Važeći domaći pravni okvir u kojem su implementirane odredbe Direktive o e-privatnosti je Zakon o elektroničkim komunikacijama *(*NN br. 73/08, 90/11, 133/12 i 80/13). Sukladno tome, područja koja se uređuju Zakonom o elektroničkim komunikacijama (dalje: ZEK) obuhvaćaju i zaštitu podataka te zaštitu sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga. S obzirom na ranije navedeno područje primjene Direktive o e-privatnosti, uvodno je bitno pojasniti pojedine osnovne pojmove. U nastavku ću uputiti na odgovarajuće definicije tih pojmova prema ZEK-u.

Pojam elektroničkih komunikacijskih usluga označava usluge koje se, u pravilu, pružaju uz naknadu, a sastoje se u cijelosti ili većim dijelom od prijenosa signala u elektroničkim komunikacijskim mrežama, uključujući telekomunikacijske usluge i usluge prijenosa u radiodifuzijskim mrežama. Javna (elektronička komunikacijska) usluga javno je dostupna na tržišnoj osnovi. Elektroničke komunikacijske usluge ne obuhvaćaju usluge pružanja sadržaja koji se prenosi korištenjem elektroničkih komunikacijskih mreža i usluga i obavljanja uredničkog nadzora nad sadržajem koji se prenosi korištenjem elektroničkih komunikacijskih mreža i usluga. Osim toga, one ne obuhvaćaju niti one usluge informacijskog društva koje se u cijelosti ili većim dijelom ne sastoje od prijenosa signala u elektroničkim komunikacijskim mrežama. Nadalje, pojam elektroničke komunikacijske mreže označava prijenosne sustave i, prema potrebi, opremu za prospajanje (komutaciju) ili usmjeravanje i druga sredstva, uključujući dijelove mreže koji nisu aktivni, što omogućuju prijenos signala žičnim, radijskim, svjetlosnim ili drugim elektromagnetskim sustavom, što uključuje satelitske mreže, nepokretne zemaljske mreže, zemaljske mreže pokretnih komunikacija, elektroenergetske kabelske sustave u mjeri u kojoj se upotrebljavaju za prijenos signala, radiodifuzijske mreže i mreže kabelske televizije, bez obzira na vrstu podataka koji se prenose. Javna je komunikacijska mreža elektronička komunikacijska mreža koja se u cijelosti ili većim dijelom upotrebljava za pružanje javno dostupnih elektroničkih komunikacijskih usluga i podržava prijenos obavijesti između priključnih točaka mreže.

Među zadatke nacionalnog regulatornog tijela - Hrvatske agencije za poštu i elektroničke komunikacije (dalje: HAKOM) pripada i promicanje interesa korisnika usluga osiguravanjem visoke razine zaštite osobnih podataka i privatnosti kao i osiguravanjem održavanja cjelovitosti i sigurnosti javnih komunikacijskih mreža. Slijedom navedenog ZEK također utvrđuje da u njegovoj provedbi HAKOM osobito surađuje (i) s AZOP-om te s tijelima nadležnim za usklađivanje prevencije i zaštitu od računalnih ugroza sigurnosti informacijskih sustava, a u skladu s posebnim zakonom kojim je uređena informacijska sigurnost te u skladu s preporukama Europske agencije za sigurnost mreža i podataka (engl. *European Network and Information Security Agency*, skraćeno: ENISA). Nadzor nad provedbom usklađenosti poslovanja operatora elektroničkih komunikacijskih mreža i/ili usluga s odredbama ZEK-a o sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga te zaštiti osobnih podataka izričito se utvrđuje kao jedan od poslova u nadležnosti HAKOM-a koji se obavlja kao javna ovlast. HAKOM je u obavljanju svojih poslova ovlašten zahtijevati dostavu potrebne dokumentacije, odnosno ostvariti neposredan uvid u istu. Protiv odluka i drugih upravnih akata HAKOM-a nije dopuštena žalba, ali se protiv njih može pokrenuti upravni spor pred Visokim upravnim sudom RH (iznimno se protiv odluka u sporovima između krajnjih korisnika usluga i operatora može pokrenuti upravni spor pred mjesno nadležnim upravnim sudom).

Od podzakonskih akata koje Vijeće HAKOM-a donosi na temelju ZEK-a, a koji su relevantni u području sigurnosti i zaštite podataka posebno upućujem na *Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga* (NN br. 109/12, 33/13 i 126/13), *Pravilnik o načinu i uvjetima obavljanja djelatnosti elektroničkih komunikacijskih mreža i usluga* (NN br. 154/11 i 149/13), *Pravilnik o univerzalnim uslugama u elektroničkim komunikacijama* (NN br. 146/12) i *Pravilnik o načinu i uvjetima sprječavanja i suzbijanja zlouporaba i prijevara u pružanju usluga elektroničke pošte* (NN br. 42/09).

Relevantnim pravilima ZEK-a uređuju se, među ostalim, posebne obveze operatora u svrhu zaštite sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga (čl. 99.), u slučaju povreda osobnih podataka u elektroničkim komunikacijama (čl. 99.a), ali i u svrhu sprečavanja neželjenih elektroničkih komunikacija (čl. 107.). Nadalje, utvrđuju se posebne obveze radi osiguravanja tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama (čl. 100.) te posebna pravila o prikupljanju tj. obradi i zaštiti prometnih podataka koji se odnose na pretplatnike ili korisnike javno dostupnih elektroničkih komunikacijskih usluga (čl. 102.) kao i podataka o lokaciji bez prometnih podataka (čl. 104.) /34/. Potonje tri posebne obveze propisane su u svrhu osiguravanja zaštite određenih podataka koji se odnose na pretplatnike i korisnike usluga u elektroničkim komunikacijama, a to su prometni podaci, podaci o lokaciji i komunikacija. U nastavku ću pojasniti navedene pojmove prema definicijama koje su u domaći okvir (ZEK) pretočene u skladu s odgovarajućim definicijama iz Direktive o e-privatnosti (čl. 2. ZEK-a). Tako pojam *prometnih podataka* označava bilo koje podatke koji se obrađuju u svrhu prijenosa komunikacije elektroničkom komunikacijskom mrežom ili u svrhu obračuna i naplate troškova, dok su *podaci o lokaciji* bilo koji podaci obrađeni u elektroničkoj komunikacijskoj mreži ili putem elektroničke

komunikacijske usluge koji označavaju zemljopisni položaj terminalne opreme korisnika javno dostupne elektroničke komunikacijske usluge. Komunikacijom se označava svaka obavijest razmijenjena ili prenesena između konačnog broja sudionika putem javno dostupne elektroničke komunikacijske usluge (ona ne obuhvaća obavijesti koje se prenose javnosti elektroničkom komunikacijskom mrežom u sklopu djelatnosti radija i televizije, osim obavijesti koje se mogu povezati s odredivim pretplatnikom ili korisnikom usluga koji ih prima).

Direktivom o e-privatnosti te ZEK-om također su posebno uređeni uvjeti pristupanja terminalnoj opremi korisnika i informacijama koje su u njima pohranjene, odnosno uvjeti za njihovu daljnju obradu. Naime, iako se smatra da terminalna oprema (kao što je to, primjerice, tvrdi disk osobnog računala korisnika elektroničke komunikacijske mreže), odnosno u njoj pohranjene informacije pripadaju korisniku i čine dio njegovog privatnog života, oni mogu biti kompromitirani tako što bi treće osobe bez znanja i privole korisnika pristupile terminalnoj opremi kojom se on služi kako bi pohranili određene informacije, odnosno pristupali podacima koji su u njoj pohranjeni. Štetne posljedice nedopuštenih aktivnosti trećih osoba nad terminalnom opremom korisnika i njegovim podacima osobito su prisutne kod različitih malicioznih virusa i softvera koji omogućavaju tajni nadzor aktivnosti korisnika terminalne opreme i kontrolu nad radom te opreme, poput *spywarea*. Takvim se radnjama zadire u privatan život pretplatnika i korisnika javno dostupnih elektroničkih komunikacijskih usluga korisnika, a osobito u Direktivom o e-privatnosti i ZEK-om zajamčenu tajnost elektroničkih komunikacija i pripadajućih prometnih podataka /35/. Osim u vezi s navedenim potrebama zaštite od djelovanja zlonamjernih i štetnih programa, ta se pitanja posljednjih godina osobito na razini EU-a sagledavaju u kontekstu prakse instalacije kolačića i sličnih tehnologija u terminalnoj opremi korisnika te nastavnog prikupljanja i daljnje obrade informacija koje se odnose na korisnika i koje su sadržane u (već) pohranjenim kolačićima. U velikom broju slučajeva ovdje će biti riječ o praksi koja je nužna iz sigurnosnih razloga ili kako bi se korisniku mogle pružiti pojedine usluge informacijskog društva koje je zatražio. Međutim, zabrinjavajuće je učestala praksa gdje se kolačići koriste netransparentno, tj. u skrivenom postupku praćenja ponašanja korisnika na internetu u svrhu njegova profiliranja, odnosno radi poduzimanja ciljanih aktivnosti prema njemu (*online* bihevioralno oglašavanje) /36/. Iz svih navedenih razloga Direktiva o e-privatnosti posebno uređuje uvjete pristupanja terminalnoj opremi korisnika i njihovim podacima koji su u njoj pohranjeni te uvjete daljnje obrade takvih podataka. Ta su pravila s određenim razlikama uvedena i u naš ZEK (čl. 100. st. 4.) /37/.

U nastavku ću pojasniti pravila koja se u ZEK-u propisuju u svrhu zaštite sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga (čl. 99.), a koja u velikoj mjeri sadrže rješenja regulatornog okvira EU-a za područje elektroničkih komunikacija. Tim se pravilima, naime, utvrđuju posebne obveze operatora javnih komunikacijskih usluga radi zaštite sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga koje uključuju obvezu primjene odgovarajućih tehničkih i ustrojstvenih mjera kako bi se zaštitila sigurnost njihovih usluga kao i obvezu poduzimanja potrebnih mjera radi zaštite sigurnosti elektroničke komunikacijske mreže i usluga (zajedno s operatorima javnih komunikacijskih mreža). Navedenim se mjerama mora osigurati razina sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže, vodeći pritom računa o raspoloživim tehničkim i tehnološkim rješenjima i troškovima tih mjera. Mjere se osobito provode kako bi se spriječio i umanjio utjecaj sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže i njima se osobito mora osigurati to da osobnim podacima mogu pristupati samo ovlaštene osobe u zakonom dopuštene svrhe kao i to da se preneseni ili pohranjeni osobni podaci zaštite od slučajnog ili nezakonitog uništenja, slučajnog gubitka ili izmjene te neovlaštene ili nezakonite pohrane, obrade, pristupa ili razotkrivanja, a mora se osigurati i primjena sigurnosne politike u odnosu na obradu osobnih podataka. Potonja mjera provedbe sigurnosne politike potrebna je radi utvrđivanja ranjivosti u sustavu, a redovito bi se trebale provoditi i nadzorne, preventivne te korektivne aktivnosti kao i radnje radi ublažavanja štetnih posljedica, odnosno rizika /38/. Operatori javnih komunikacijskih mreža također su dužni su poduzimati sve odgovarajuće mjere kako bi zajamčili cjelovitost svojih mreža u svrhu osiguravanja neprekinutog obavljanja usluga koje se pružaju putem tih mreža. Pored navedenog, operator javno dostupnih elektroničkih komunikacijskih usluga mora obavijestiti korisnike svojih usluga u slučaju osobite opasnosti za sigurnost mreže, a ako je opasnost izvan opsega mjera koje operator poduzima, mora obavijestiti korisnike i o raspoloživim mjerama za uklanjanje opasnosti i/ili njezinih posljedica, uključujući naznaku mogućih troškova takvih mjera. U slučaju povrede sigurnosti ili gubitka cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga operatori javnih komunikacijskih mreža i operatori javno dostupnih elektroničkih komunikacijskih usluga moraju o tome bez odgode izvijestiti HAKOM pisanim putem. HAKOM može obavijestiti javnost ili zahtijevati od operatora da obavijeste javnost o takvoj povredi sigurnosti ili gubitku cjelovitosti ako utvrdi da je takva obavijest u javnom interesu.
Operator javno dostupnih elektroničkih komunikacijskih usluga mora odrediti odgovornu osobu za provedbu ovdje izloženih mjera. Ovlaštena tijela za nadzor mjera koje operatori poduzimaju radi provedbe navedenih obveza kao i za davanje preporuke o najboljoj praksi u vezi s razinom sigurnosti koju te mjere moraju ostvariti su HAKOM i AZOP. Način i rokovi u kojima operatori javnih komunikacijskih mreža moraju poduzimati

odgovarajuće mjere kako bi zajamčili cjelovitost svojih mreža te način izvješćivanja HAKOM-a o povredi sigurnosti ili gubitku cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga detaljno su uređeni *Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga* (NN br. 109/12, 33/13 i 126/13).

Pored izloženih posebnih pravila radi zaštite sigurnosti cjelovitosti mreža i usluga, vrlo je važno skrenuti pažnju na propisani postupak povodom povreda osobnih podataka (engl. *personal data breach*), tj. povreda sigurnosti koje uzrokuju slučajno ili nezakonito uništenje, gubitak, izmjenu, neovlašteno razotkrivanje ili pristup osobnim podacima što se prenose, pohranjuju ili na drugi način obrađuju u vezi s obavljanjem javno dostupnih elektroničkih komunikacijskih usluga u EU-u. Osim relevantnih pravila ZEK-a (čl. 99.a), odnosno Direktive o e-privatnosti ovdje je posebno važna *Uredba Komisije br. 611/2013 o mjerama koje se primjenjuju na obavijesti o povredama osobnih podataka prema Direktivi o e-privatnosti* (dalje: Uredba Komisije br. 611/203), koja je stupila na snagu 25. kolovoza 2013. godine /39/. Naime, propisani postupak u slučaju povrede osobnih podataka prema ZEK-u uključuje, na prvome mjestu, obvezu operatora javno dostupnih elektroničkih komunikacijskih usluga da o povredi bez odgode obavijesti HAKOM i AZOP. Uredbom Komisije br. 611/2013 detaljno se uređuju pojedinosti u vezi s obavještavanjem nadzornog tijela (kao i osobe čiji su podaci pogođeni povredom), a kao načelni rok za obavještavanje nadzornog tijela utvrđuje se rok od 24 sata od otkrivanja povrede, gdje je to moguće. Pored nadzornog tijela, o povredi se u određenim slučajevima mora obavijestiti i korisnika, tj. drugu fizičku osobu čiji su podaci pogođeni povredom. ZEK utvrđuje takvu obvezu, sukladno Direktivi o e-privatnosti, ako je vjerojatno da će nastala povreda osobnih podataka štetno utjecati na osobne podatke ili privatnost te osobe. Prema Uredbi Komisije br. 611/2013 kod utvrđivanja toga je li vjerojatno da će povreda štetno utjecati na osobne podatke ili privatnost trebaju se osobito uzeti u obzir priroda i sadržaj osobnih podataka o kojima je riječ, posebice kada su podaci financijske prirode, posebne kategorije osobnih podataka iz Direktive ZOP, kao i podaci o lokaciji, internet log (dnevničke) datoteke, povijest pretraživanja u pregledniku, podaci o e-pošti, podrobni ispisi računa (detaljni ispisi poziva). Osim toga, moraju se uzeti u obzir i moguće posljedice povrede, posebice kada povreda može prouzročiti krađu identiteta ili prijevaru, fizičku povredu, psihološku patnju, sramoćenje ili štetu za ugled. Konačno, moraju se osobito uzeti u obzir i okolnosti povrede, osobito ako su podaci ukradeni ili gdje operator zna da su oni u posjedu treće neovlaštene strane.
Obveza obavještavanja korisnika se prema ZEK-u ne primjenjuje ako HAKOM, na temelju obavijesti o povredi, utvrdi u mišljenju da je operator na osobne podatke na zadovoljavajući način primijenio odgovarajuće tehnološke mjere zaštite koje moraju učiniti osobne podatke nerazumljivim bilo kojoj osobi koja im neovlašteno pristupa. U tom pogledu vrlo su važni Uredbom Komisije br. 611/2013 propisani kriteriji koje trebaju zadovoljiti navedene tehničke mjere i u vezi s čijom se primjenom smatra da su osobni podaci učinjeni nerazumljivima. Daljnji postupak propisan ZEK-om je taj da HAKOM dostavlja mišljenje o potrebi obavješćivanja korisnika usluga ili druge fizičke osobe operatoru kao i AZOP-u koji je ovlašten i neovisno o navedenom mišljenju HAKOM-a zahtijevati od operatora koji još nije obavijestio korisnika, tj. drugu fizičku osobu o povredi osobnih podataka da to učini ako procijeni da bi nastala povreda mogla na njega ili nju štetno djelovati. Skrećem pažnju na Uredbom Komisije br. 611/2013 propisanu mogućnost da operator u iznimnim slučajevima odgodi obavještavanje osobe ako bi to moglo ugroziti istragu povrede, nakon što se usuglasilo nadzorno tijelo, sve dok to tijelo ne utvrdi da je takvo obavještavanje moguće.

Što se tiče inspekcijskog nadzora nad primjenom ZEK-a i podzakonskih propisa, njega obavlja HAKOM, tj. inspektori elektroničkih komunikacija kao ovlašteni radnici HAKOM-a prilikom kojeg su ovlašteni i pregledavati relevantnu dokumentaciju, opremu i poslovne prostorije te pisano zatražiti od nadzirane osobe podatke i drugu dokumentaciju potrebnu radi provedbe nadzora. Svojim rješenjem ovlašteni su, među ostalim, narediti usklađivanje obavljanja djelatnosti elektroničkih komunikacijskih mreža i usluga s odredbama ZEK-a i propisa donesenih na temelju njega. HAKOM je ovlašten izravno sankcionirati povrede ZEK-a, što nije slučaj s AZOP-om kako sam pokazala ranije u radu. Inspektori su, naime, ovlašteni izdati prekršajni nalog kojim izriču novčane kazne i zaštitne mjere propisane ZEK-om ili predložiti HAKOM-u podnošenje optužnog prijedloga radi pokretanja prekršajnog postupka. Protiv rješenja inspektora nije dopuštena žalba, ali se protiv njega može pokrenuti upravni spor pred mjesno nadležnim upravnim sudom. Iznimno, protiv rješenja inspektora u vezi s osobito teškim i teškim povredama ZEK-a može se pokrenuti upravni spor pred Visokim upravnim sudom RH.

Sukladno Direktivi o e-privatnosti u ZEK-u se utvrđuje ovlast i HAKOM-a i AZOP-a da narede prestanak povreda odredaba tog Zakona koje su pretežito (ali ne isključivo) donesene u skladu s odgovarajućim odredbama Direktive o e-privatnosti (čl. 99. – 107.). Takvu odluku ta tijela mogu donijeti po službenoj dužnosti ili na zahtjev zainteresirane strane. Osim toga, ta su nadzorna tijela ovlaštena u tu svrhu zatražiti sve podatke koje smatraju potrebnima za utvrđivanje mogućih povreda, odnosno za nadzor i primjenu tih odredaba.

Naposljetku skrećem pažnju na obvezu država članica iz Direktive o e-privatnosti da u domaćem okviru predvide sankcije za povredu odredaba propisa usvojenih na temelju Direktive, koje mogu biti i kaznenopravne prirode, a koje u svakom slučaju moraju biti učinkovite, razmjerne i s s odvraćajućim učinkom. Većina povreda odredaba ZEK-a na koje sam uputila u radu smatra se bilo teškim bilo manje teškim povredama zakona za koje se propisuju sankcije pa se tako, što se tiče novčanih kazni, za pravne osobe utvrđuje kazna u iznosu od 100.000,00 do 1.000.000,00 kuna (teška povreda ZEK-a), odnosno u iznosu od 50.000,00 do 500.000,00 kuna za manje teške povrede ZEK-a.

Što se tiče kaznenih djela koja se najčešće dovode u vezu s povredom privatnosti i sigurnosti osobnih podataka u Republici Hrvatskoj, na prvome mjestu treba istaknuti kazneno djelo nedozvoljene uporabe osobnih podataka (čl. 146.) /40/, koje pripada djelima protiv privatnosti u važećem *Kaznenom zakonu RH* /41/. Tim djelima (Glava XIV.) pripadaju i narušavanje nepovredivosti doma i poslovnog prostora (čl. 141.), povreda tajnosti pisama i drugih pošiljaka (čl. 142.), neovlašteno zvučno snimanje i prisluškivanje (čl. 143.), neovlašteno slikovno snimanje (čl. 144.) te neovlašteno otkrivanje profesionalne tajne (čl. 145.).
U odnosu na ranije kazneno djelo nedozvoljene uporabe osobnih podataka /42/, u važećem Kaznenom zakonu to je djelo pretežito usklađeno s odredbama ZZOP-a. Predviđa se tako da to djelo čini bilo tko tko protivno uvjetima određenima u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba. Novina je da se to kazneno djelo više ne pokreće po prijedlogu već po službenoj dužnosti te se kao sankcija predviđa isključivo kazna zatvora koja u osnovnom obliku ovog djela može biti izrečena u najduljem trajanju od godine dana zatvora (što je postroženo u odnosu na dotadašnjih najviše šest mjeseci zatvora). Nadalje, predviđaju se novi kvalificirani oblici toga djela, npr. obrada osobnih podataka protivno zakonu, odnosno obrada protivno zakonu čime je pribavljena znatna imovinska korist ili prouzročena znatna šteta (vrijednost imovinske koristi, tj. štete koja prelazi 60.000,00 kn /43/). Kvalificirani oblik predviđa se i u slučaju nedopuštene obrade osjetljivih osobnih podataka, tj. posebne kategorije osobnih podataka prema ZZOP-u. Teži oblik predviđa se i kod nedopuštenog izvoza osobnih podataka iz RH radi daljnje obrade, odnosno objave podataka ili njihova činjenja dostupnima drugima na koji drugi način. U vezi sa svim navedenim se kao daljnji kvalificirani oblik djela propisuju slučajevi počinjenja ovih djela od strane službene osobe u obavljanju njezinih ovlasti i u tom se slučaju predviđa kazna zatvora od najmanje 6 mjeseci do najviše pet godina zatvora.

Prijetnje za sigurnost i integritet informacijskih sustava, mreža i usluga, odnosno sve brojniji oblici kibernetičkog kriminala predstavljaju značajan rizik za sigurnost i privatnost osobnih podataka u modernom globalno umreženom komunikacijskom okruženju. Tako je posebna glava Kaznenog zakona posvećena kaznenim djelima protiv računalnih sustava, programa i podataka /44/ koja su usklađena s Konvencijom Vijeća Europe o kibernetičkom kriminalu /45/. Prilikom izrade pojedinih zakonodavnih rješenja uziman je u obzir i prijedlog *Direktive o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PU*P /46/. Do završetka zakonodavnog postupka u EU-u taj je prijedlog u određenoj mjeri mijenjan, a prihvaćena *Direktiva 2013/40/EU o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP* stupila je na snagu 4. rujna 2013. godine /47/. Kaznena djela protiv računalnih sustava, programa i podataka u Kaznenom zakonu RH obuhvaćaju neovlašten pristup računalnom sustavu ili računalnim podacima (čl. 266.) /48/, ometanje rada računalnog sustava (čl. 267. - onemogućavanje ili otežavanje rada ili korištenja računalnog sustava, računalnih podataka ili programa ili računalne komunikacije); oštećenje računalnih podataka (čl. 268. - neovlašteno oštećenje, izmjena, brisanje, uništenje, činjenje neuporabljivim ili nedostupnim ili prikazivanje nedostupnim tuđih računalnih podataka ili programa); neovlašteno presretanje računalnih podataka (čl. 269. - neovlašteno presretanje ili snimanje nejavnog prijenosa računalnih podataka, odnosno činjenje drugome dostupnim tako pribavljenih podataka); računalno krivotvorenje *(*čl. 270. - neovlaštena izrada, unos, izmjena, brisanje ili činjenje neuporabljivim ili nedostupnim računalnih podataka koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao vjerodostojni, odnosno uporaba takvih podataka ili njihova nabava radi uporabe) te računalna prijevara (čl. 271.) - unos, izmjena, brisanje, oštećenje, činjenje neuporabljivim ili nedostupnim računalnih podataka ili ometanje rada računalnog sustava s ciljem pribavljanja protupravne imovinske koristi te posljedicom prouzročene štete za drugog). Dodatno se u pogledu svih spomenutih djela predviđa sankcioniranje i pripremnih radnji za njihovo počinjenje. Tako se kaznenim djelom zlouporabe naprava (čl. 272.) sankcionira izrada, nabava, prodaja, posjedovanje ili činjenje dostupnim drugima uređaja ili računalnih programa ili računalnih podataka stvorenih ili prilagođenih za počinjenje tih kaznenih djela i s ciljem da se njih uporabi za počinjenje tih kaznenih djela, odnosno izrada, nabava, prodaja, posjedovanje ili činjenje dostupnim drugima računalnih lozinki, pristupnih šifri ili drugih podataka kojima se može pristupiti računalnom sustavu, s ciljem da ih se uporabi za počinjenje gore spomenutih kaznenih djela. Naposljetku treba skrenuti pažnju i na teška kaznena djela protiv računalnih sustava, programa i podataka (čl. 273.), tj. teže oblike kaznenih djela ometanja rada računalnog sustava, oštećenja računalnih podataka, neovlaštenog presretanja računalnih podataka i računalnog krivotvorenja u slučaju kada se navedena djela počine u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, tijela jedinica lokalne ili područne samouprave, javne ustanove ili trgovačkog društva od

posebnog javnog interesa, odnosno teže oblike kaznenih djela neovlaštenog pristupa, ometanja rada računalnog sustava, oštećenja računalnih podataka i neovlaštenog presretanja računalnih podataka kada su ta djela počinjena prikrivanjem stvarnog identiteta i uzrokovanjem zablude o ovlaštenom nositelju identiteta. Konačno, kvalificirani se oblik predviđa i kod počinjenja kaznenih djela ometanja rada računalnog sustava, oštećenja računalnih podataka i neovlaštenog presretanja računalnih podataka sredstvom namijenjenim za izvršenje napada na veći broj računalnih sustava ili kojima je prouzročena znatna šteta (ako vrijednost štete prelazi 60.000,00 kn /49/).

Pored navedenih je djela korisno skrenuti pažnju i na to da se Kaznenim zakonom utvrđuju kvalificirani oblici kaznenih djela protiv časti i ugleda (kao što su uvreda i kleveta) kada su ona učinjena dostupnima većem broju ljudi pa tako i onda kada su počinjena putem računalnog sustava i mreže /50/. Osim toga, valja imati na umu i druga kaznena djela, primjerice, nametljivo ponašanje (engl. *cyberstalking)* koja se mogu počiniti putem elektroničke komunikacijske mreže (čl. 140.) /51/.

Naposljetku skrećem pažnju i na novo uvedenu sigurnosnu mjeru zabrane pristupa internetu u Kaznenom zakonu, a koja se može izreći u trajanju od najmanje šest mjeseci do najviše dvije godine (računajući od izvršnosti sudske odluke). Ona će se izreći počinitelju koji je počinio bilo koje kazneno djelo „putem interneta“, postoji li opasnost da će „zlouporabom interneta“ ponovno počiniti kazneno djelo. Osim zbog niza nejasnoća u korištenoj terminologiji, među kojima je i pojam „interneta“, navedena je mjera opravdano polučila kritike u domaćoj znanstvenoj literaturi /52/ i s obzirom na predviđenu primjenu bez obzira na težinu počinjenja kaznenog djela, ali i osnovane dvojbe oko mogućnosti osiguravanja njezine provedbe. Zakonodavac je zadužio HAKOM za provedbu mjere, a predvidio je i donošenje propisa o izvršavanju ove sigurnosne mjere (ministar nadležan za poslove pomorstva, prometa i infrastrukture). Navedeni je akt donesen tijekom 2013. godine pod nazivom *Pravilnik o izvršavanju sigurnosne mjere zabrane pristupa internetu* (NN br. 34/13). Iz Pravilnika je razvidno da se za provedbu sigurnosne mjere zabrane pristupa internetu zadužuju operatori u RH koji su dužni ne samo obustaviti pružanje usluge počinitelju nego i raskinuti pretplatnički odnos s njim, a potom (svi operatori) paziti na to da tijekom trajanja mjere počinitelj ne sklopi novi pretplatnički ugovor. Naime, operatori su dužni odmah nakon obavijesti HAKOM-a o izrečenoj sigurnosnoj mjeri, po naredbi HAKOM-a i prema obvezi iz samog Pravilnika, obustaviti pružanje usluge pristupa internetu (obveza operatora koji je s počiniteljem sklopio ugovor za samostalnu uslugu pristupa internetu ili bilo koju drugu elektroničku komunikacijsku uslugu koja uključuje uslugu pristupa internetu ili putem koje je moguć pristup internetu, neovisno o načinu pristupa). Osim toga, Pravilnikom se propisuje obveza (relevantnog) operatora da u roku od tri dana od zaprimanja obavijesti HAKOM-a raskine pretplatnički ugovor s počiniteljem. Nadalje, utvrđuje se izričita ovlast HAKOM-a da zabrani svim operatorima sklapanje novoga pretplatničkog ugovora za tu uslugu, za vrijeme trajanja izrečene sigurnosne mjere.

Od drugih značajnijih propisa za sigurnost i privatnost osobnih podataka u digitalnom okruženju osnovno skrećem pažnju na odabrane važnije propise u području zaštite tajnosti podataka i sigurnosti informacijskih sustava. Što se domaćeg pravnog okvira tiče, ovdje izdvajam *Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske* (NN br. 79/06 i 105/06), *Zakon o sigurnosnim provjerama* (NN br. 85/08 i 86/12), *Zakon o tajnosti podataka* (NN br. 79/07 i 86/12) i *Zakon o informacijskoj sigurnosti (*NN br. 79/07). U nastavku ću obratiti više pažnje na potonja dva zakona. Njima se među ostalim uređuju obveze državnih tijela, tijela jedinica lokalne i područne samouprave, pravnih osoba s javnim ovlastima, ali i svih pravnih i fizičkih osoba koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima, u pogledu postupanja s tim podacima i njihove zaštite. Način i provedba zaštite ovih podataka propisani su Zakonom o informacijskoj sigurnosti u kojem se utvrđuje pojam, mjere, standardi i područja informacijske sigurnosti te nadležna tijela za donošenje, provedbu i nadzor mjera i standarda. Mjere informacijske sigurnosti propisuju se Uredbom Vlade RH *(Uredba o mjerama informacijske sigurnosti,* NN br. 46/08), dok se standardi za provedbu mjera propisuju pravilnicima koje donose čelnici središnjih državnih tijela za informacijsku sigurnost. Središnja su državna tijela za informacijsku sigurnost *Ured Vijeća za nacionalnu sigurnost* (UVNS) i *Zavod za sigurnost informacijskih sustava* (ZSIS). U sustavu informacijske sigurnosti RH vrlo bitnu ulogu igra *CARNet CERT* (engl. *Computer Emergency Response Team*, skraćeno dalje: CERT) - nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u RH. Što se tiče značajnijih aktualnosti u ovom području na razini prava EU-a potrebno je uputiti na Strategiju kibernetičke sigurnosti Europske unije: Otvoren, siguran i zaštićen kibernetički prostor koja je donesena poglavito u svrhu osiguravanja sigurnosne otpornosti na kibernetičke napade, razvoja resursa za kibernetičku sigurnost i razvoja obrambene politike EU-a /53/. Također skrećem pažnju na prijedlog Direktive o mjerama za osiguravanje visoke zajedničke razine sigurnosti mrežnih i informacijskih sustava u Uniji koji je trenutno u zakonodavnom postupku /54/. Ta se Direktiva, naime, predlaže s ciljem osiguravanja ujednačeno visoke razine zaštite mrežne i informacijske sigurnosti unutar EU-a. Njome se

uređuju obveze država članica na uspostavu minimalne razine mrežne i informacijske sigurnosti, usvajanje nacionalnih strategija i utvrđivanje nadležnih tijela i CERT-ova. Predviđa se i suradnja između nadležnih tijela unutar EU-a, uključujući s Europskom agencijom za sigurnost mreža i podataka radi suzbijanja prijetnji i incidenata za mrežnu i informacijsku sigurnost. Od posebne je važnosti osiguravanje jačanja kibernetičke otpornosti u kritičnoj infrastrukturi (npr. bankarski sektor, infrastruktura financijskih tržišta, energetski, prometni i zdravstveni sektori). To zahtijeva i provedbu odgovarajućih postupaka procjene rizika i odgovarajućih mjera radi osiguravanja mrežne i informacijske sigurnosti kao i uređenje postupaka izvješćivanja o sigurnosnim incidentima. Od povezanih važnijih aktualnosti u RH skrećem pažnju na (pripremne radnje za) izradu *Nacrta prijedloga nacionalne strategije kibernetičke sigurnosti* /55/.

U uvodu rada ukratko sam uputila na pitanje sustava obveznog preventivnog zadržavanja podataka koji se odnose na korištenje elektroničkih komunikacijskih usluga svih pretplatnika i korisnika usluga kojim se intenzivno zadire u njihova temeljna prava i slobode i koji zahtijeva uspostavu odgovarajućih zaštitnih mjera radi sprečavanja zlouporaba. Takav je sustav na razini prava EU-a uspostavljen *Direktivom 2006/24/EZ o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža* (dalje: Direktiva o zadržavanju podataka) /56/. Tom se Direktivom, naime, utvrđuje obveza zadržavanja podataka koji se obrađuju u tijeku pružanja javno dostupnih elektroničkih komunikacijskih usluga i javnih komunikacijskih mreža za rok od najmanje 6 mjeseci do 2 godine. Propisana je svrha zadržavanja istraga, otkrivanje i progon teških kaznenih djela, kako to svaka država članica utvrđuje u svojem unutarnjem pravu. U domaćem okviru zadržavanje podataka prema toj Direktivi uređeno je odredbama ZEK-a (čl. 109. – 110.) i *Uredbe Vlade RH o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama* (NN br. 64/08 i 76/13) /57/, i to za rok od 12 mjeseci od komunikacije. Utvrđena svrha zadržavanja je omogućivanje provedbe istrage, otkrivanja i kaznenog progona kaznenih djela u skladu s posebnim zakonom iz područja kaznenog postupka te u svrhu zaštite obrane i nacionalne sigurnosti u skladu s posebnim zakonima iz područja obrane i nacionalne sigurnosti. Pored navedenog, zadržavanje podataka u unutarnjem pravu uređeno je i neovisno o Direktivi o zadržavanju podataka, i to za rok od godine dana, na temelju ranije spomenutog Zakona o sigurnosno-obavještajnom sustavu RH i Uredbe Vlade o obvezama iz područja nacionalne sigurnosti RH za pravne i fizičke osobe u telekomunikacijama.

Obvezno zadržavanje podataka, budući da podrazumijeva praćenje i pohranu za dulji rok podataka koje se odnosi na korištenje elektroničkih komunikacijskih usluga svih pretplatnika i korisnika usluga *(*bez obzira na sumnju u počinjenje relevantnih kaznenih djela), već samo po sebi predstavlja vrlo intenzivno zadiranje u njihova temeljna prava i slobode te otvara brojna pitanja o mogućim zlouporabama. Stoga ne iznenađuje da je provedba Direktive o zadržavanju podataka nailazila na niz prepreka u pojedinim državama članicama EU-a /58/. Osim toga, posebno su važni postupci pokretani pred Sudom pravde EU-a, u kojima se tražila ocjena sukladnosti Direktive o zadržavanju podataka s temeljnim pravima i slobodama pojedinaca, posebice pravom na privatnost i na zaštitu osobnih podataka kao i sa slobodom izražavanja. U idućem dijelu rada, u okviru analize sudske prakse tog Suda analizirat ću nedavno donesenu važnu presudu kojom se utvrđuje nevaljanost Direktive.

3. Odabrana sudska praksa Suda pravde EU-a

Sud pravde EU-a u dosadašnjoj se praksi bavio različitim pitanjima zaštite osobnih podataka u digitalnom okruženju tumačeći relevantne odredbe Direktive ZOP, Direktive o e-privatnosti, ali i Direktive o zadržavanju podataka. U nastavku ću stoga izložiti odabrane predmete i odluke Suda, kako bih približila i pojasnila njegovo tumačenje *acquisa* u ovome području.

Kazneni postupak protiv Bodil Lindqvist

Predmet Lindqvist /59/ bavio se pitanjem neovlaštene objave podataka na internetu. Naime, osoba je objavila podatke o suradnicima (imena, telefonski brojevi, podaci o hobijima i radnim uvjetima/okolnostima, ali i osjetljiviji podaci kao što su podaci o zdravlju), na svojoj internetskoj stranici vezano za angažman u lokalnom društvenom centru u vezi s aktivnostima crkve. Stranica je bila na švedskom jeziku, a poveznica na nju bila je postavljena na stranicama jedne švedske crkve. Sud pravde EU-a utvrdio je da se navedena objava smatra obradom osobnih podataka u smislu Direktive ZOP. Nadalje, budući da je njihovom objavom na internetu omogućena dostupnost ovih podataka neodređenom broju osoba, ona ne predstavlja obradu koja je namijenjena isključivo za osobnu primjenu ili za potrebe kućanstva. Drugim riječima, objava podataka u takvom slučaju nije obrada koja bi bila isključena od materijalnog područja primjene Direktive ZOP. Sud je također utvrdio da nema prijenosa osobnih podataka u treću zemlju u smislu Direktive ZOP kada osoba u državi članici objavi osobne podatke na stranici koja se pohranjuje kod davatelja usluge pohrane informacija osnovanog u toj državi ili drugoj državi članici, zbog čega su ti podaci dostupni svakome tko se može spojiti na internet. Sud nije u tom predmetu dalje utvrđivao je li netko iz treće zemlje pristupao toj stranici. Smatrao je važnim da ovdje nije bilo izravnog prijenosa osobnih podataka između pošiljatelja i primatelja (kao što bi to npr. bilo kod slanja e-pošte) jer se

podaci prenose preko računalne infrastrukture davatelja usluge pohrane informacija gdje se relevantna stranica pohranjuje. Osim toga, u okolnostima i vremenu predmeta primatelj informacija bi radi pronalaska relevantnih osobnih podataka morao ne samo imati pristup internetu nego i poduzeti određene radnje da bi podatke pronašao kao što je otvaranje odgovarajuće poveznice na stranicama lokalne crkve, dok bi danas vjerojatno bilo dovoljno samo unijeti ključne riječi u kojem boljem pretraživaču. Utvrdio je, nadalje, da se odredba Direktive u kojem se utvrđuju uvjeti prijenosa osobnih podataka u treću zemlju ne bi trebala tumačiti tako da svaki put kada se osobni podaci objave na nekoj internetskoj stranici to istovremeno podrazumijeva prijenos tih podataka u sve (pa i treće) zemlje gdje postoji mogućnost pristupa internetu. Smatra da se ne može samo tako pretpostaviti da su se specifična pitanja prijenosa podataka preko interneta, pogotovo u okolnostima današnjeg interneta, razmatrala u vrijeme donošenja Direktive ZOP. U suprotnom bi se poseban režim Direktive ZOP o prijenosu podataka u treće zemlje uvijek primjenjivao na aktivnosti na internetu. To bi značilo da i onda, kada bi Europska komisija utvrdila da i samo jedna treća zemlja nema odgovarajuću razinu zaštite podataka, država članica ne bi smjela objaviti osobne podatke na internetu uopće, tj. ne bi to smjela učiniti bez prethodnog ispunjavanja uvjeta propisanih Direktivom ZOP.

C-70/10 (Scarlet Extended SA protiv SABAM) i C-360/10 (SABAM protiv Netlog NV) /60/
U predmetu C-70/10 /61/ Sud pravde EU-a odlučivao je o mjeri filtriranja prometa koju je nadležni sud izrekao u domaćem građanskom postupku protiv davatelja usluge pristupa internetu – posrednika, a u svrhu sprečavanja neovlaštene razmjene datoteka sa zaštićenim djelima od strane korisnika ove usluge. Iako je bila riječ o internetskom posredniku, mjera je naložena protiv njega jer je njegova usluga korištena u povredi prava nositelja. Davatelj usluge trebao je o vlastitom trošku i za neograničeno vremensko razdoblje filtrirati sve elektroničke komunikacije koje se prenose putem njegove usluge, a posebice *peer-to-peer* komunikaciju te potom blokirati prijenos utvrđenih datoteka sa zaštićenim djelima. Nakon proučavanja specifičnih obilježja naložene mjere i njezinih učinaka na davatelja usluge (neograničeni rok primjene, skupa i komplicirana provedba isključivo o njegovom trošku) i njegove korisnike te niza relevantnih propisa EU-a (uključujući, među ostalim, propise o zaštiti prava intelektualnog vlasništva i o elektroničkoj trgovini u vezi s davateljima usluge pristupa internetu kao posrednicima i zabrani općeg nadzora nad informacijama koje se prenose te propise o zaštiti podataka), Sud je utvrdio da je određivanje mjere s navedenim obilježjima protivno pravu EU-a. Ovdje nije, naime, postignuta pravedna ravnoteža između prava nositelja autorskog prava na zaštitu intelektualnog vlasništva s jedne strane te prava i sloboda davatelja usluge (poglavito sloboda poduzetništva) i korisnika njegovih usluga (zaštita osobnih podataka, sloboda izražavanja) s druge strane. Naglasak u presudi Sud je dao pitanju osiguravanja pravedne ravnoteže različitih suprotstavljenih prava i sloboda, poglavito slobode poduzetništva s obzirom na zaštitu prava intelektualnog vlasništva, zbog gore opisanih specifičnih obilježja te mjere. Značajno je i utvrđenje Suda o IP adresama na temelju kojih davatelji usluga pristupa internetu mogu identificirati korisnike svojih usluga (osobni podaci), a čije je prikupljanje i daljnja obrada također dio navedene mjere.

Pozivajući se pretežito na presudu u gore izloženom predmetu, Sud pravde EU-a odlučivao je o gotovo istovjetnoj mjeri u kasnijem predmetu C-360/10 /62/. Takvu je mjeru u domaćem postupku sud naložio protiv *online* društvene platforme kao davatelja usluge pohrane informacija (*hosting*) - posrednika, također u svrhu sprečavanja neovlaštene razmjene datoteka sa zaštićenim djelima, odnosno budućih povreda autorskog i srodnih prava u tom obliku.

C-314/12 UPC Telekabel Wien GmbH protiv Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH
U ranije navedenim presudama Sud pravde EU-a utvrdio je kakvi sudski nalozi, tj. mjere nisu dopuštene. No brojne su mogućnosti izricanja mjera s manje drastičnim obilježjima od navedenih, osobito što se tiče stupnja zadiranja u slobodu poduzetništva internetskih posrednika, a koje bi mogle biti dopuštene. Stoga je potrebno skrenuti pažnju na nedavnu presudu tog Suda u vezi s nalogom koji je domaći sud izrekao protiv davatelja usluge pristupa internetu radi blokiranja pristupa internetskoj stranici na kojoj se neovlašteno prikazuju zaštićena autorska djela. U toj presudi, naime, Sud izlaže značajke sudskog naloga, odnosno mjere koja bi bila dopuštena kao i jamstva zaštite temeljnih prava i sloboda koja se s time u vezi moraju osigurati u domaćem pravnom okviru uključujući osobito jamstva zaštite slobode informiranja (pravo primanja informacija) korisnika interneta /63/.

C-275/06 (Promusicae protiv Telefónica), C-557/07 (LSG protiv Tele2) i C-461/10 (Bonnier Audio AB i dr. protiv Perfect Communication Sweden AB) /64/
U predmetu C-275/06 /65/ Sud se bavio odnosom između različitih temeljnih prava zajamčenih pravom EU-a s obzirom na zahtjev udruge za kolektivno ostvarivanje autorskog prava da joj u svrhu pokretanja građanskog postupka zbog neovlaštene *peer-to-peer* razmjene zaštićenih djela davatelj usluge pristupa internetu (posrednik) dostavi podatke njegovih korisnika (ime, prezime, adresa). Korisnike je davatelj usluge trebao identificirati na

osnovu podataka o IP adresama za koje je udruga sumnjala da su povezani s navedenom povredom. U analizi niza uključenih propisa Sud pravde EU-a utvrdio je da isti ne nalažu državama članicama da u domaćem okviru utvrde obvezu dostave osobnih podataka u postupku pred sudom u svrhu osiguranja učinkovite zaštite autorskog prava za potrebe građanskog postupka, *ali im istovremeno to ne brane*. Nadalje je utvrdio da su kod provedbe relevantnih direktiva u domaći okvir države članice *dužne oslanjati se na njihovo tumačenje na način koji dopušta pravednu ravnotežu između različitih temeljnih prava zaštićenih pravom EU-a*. Osim toga, sudovi i tijela vlasti dužni su kod provedbe mjera kojima se te direktive transponiraju *tumačiti svoje unutarnje pravo na dosljedan način u odnosu na te direktive, ali i osigurati da se ne oslanjaju na njihovo tumačenje koje dovodi do sukoba s relevantnim temeljnim pravima ili drugim općim načelima prava EU-a, kao što je načelo razmjernosti*.

U kasnijoj odluci povodom predmeta sa sličnim obilježjima (C-557/07) /66/ Sud pravde EU-a potvrdio je ovdje navedena ključna stajališta. U daljnjem predmetu C-461/10 /67/ Sud se ponovo bavio pitanjem zahtjeva nositelja autorskog prava da mu davatelj usluge pristupa internetu – posrednik dostavi identifikacijske podatke njihovih korisnika, prema IP adresama za koje su nositelji prava sumnjali da su povezane s neovlaštenom razmjenom zaštićenih djela. No ovdje je Sud analizirao uvjete propisane u švedskom Zakonu o autorskom pravu za izricanje mjere dostave osobnih podataka protiv posrednika u građanskom postupku. Utvrdio je da se tim odredbama osigurava pravedna ravnoteža uključenih temeljnih prava, poglavito s obzirom na propisanu obvezu sudova da ocijene suprotstavljene interese na osnovi činjenica svakog slučaja i uzimajući u obzir zahtjeve načela razmjernosti.

C-119/12 (Josef Probst protiv mr.nexnet GmbH)

U drugom dijelu ovog rada pojasnila sam da pravila Direktive o e-privatnosti koja uređuju pitanja zaštite osobnih podataka i prava na privatnost u elektroničkim komunikacijama obuhvaćaju i posebne odredbe u vezi s prikupljanjem i daljnjom obradom prometnih podataka koji se odnose na pretplatnike i korisnike usluge. Ti se podaci, naime, smiju prikupljati i dalje obrađivati u određene ograničene svrhe kao što je to i naplata troškova pružene usluge. Osim toga, propisuju se i pravila ograničenja roka zadržavanja podataka, opsega njihove obrade i podataka koji se obrađuju s obzirom na svrhu obrade (čl. 6. Direktive o e-privatnosti i čl. 102. ZEK-a). Ta pravila odražavaju primjenu općih načela o zaštiti osobnih podataka u specifičnom okruženju elektroničkih komunikacija. U tom je pogledu Sud pravde EU-a nedavno donio presudu u predmetu C-119/12 /68/. Sporna situacija u domaćem postupku odnosila se na dostavu prometnih podataka pretplatnika od strane operatora trećoj strani, i to u svrhu naplate njegovih potraživanja. Sud pravde EU-a utvrdio je da dopuštena obrada prometnih podataka prema Direktivi o e-privatnosti radi obračuna troškova također uključuje naplatu potraživanja (duga) za pruženu elektroničkukomunikacijsku uslugu. Nadalje, pojam ovlaštenih osoba operatora, tj. osoba koje djeluju pod ovlasti operatora (engl. *acting under the authority of),* a koje imaju pravo pristupiti prometnih podacima i obrađivati ih u svrhu obračuna troškova, tj. naplate potraživanja, može uključivati i treće strane. To tumačenje, međutim, *mora biti striktno* jer je obrada navedenih prometnih podataka iznimka od pravila o čuvanju tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka. Oslanjajući se i na odredbe Direktive ZOP o povjeravanju poslova obrade osobnih podataka izvršiteljima obrade Sud je utvrdio da treća strana smije djelovati *samo pod ovlasti operatora, po njegovu nalogu i u skladu s njegovim uputama* i da se takva obrada prometnih podataka mora ograničiti *isključivo na ono što je nužno kako bi se omogućila svrha obrade* (naplata potraživanja). Sklopljeni ugovor između operatora i treće strane mora sadržavati i pravila kojima se *jamči zakonita obrada prometnih podataka od strane treće osobe* i kojima se *operatoru omogućuje pravo kontrole nad njezinim pridržavanjem tih pravila u svako doba*.

Spojeni predmeti C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger i dr.

U prošlom dijelu ovog rada osnovno sam pojasnila problematiku sustava obveznog preventivnog zadržavanja podataka koji se odnose na korištenje elektroničkih komunikacijskih usluga svih pretplatnika i korisnika usluga, a koji je na razini prava EU-a uspostavljen Direktivom o zadržavanju podataka. Uputila sam i na postupke u kojima se od Suda pravde EU-a traži ocjena sukladnosti Direktive s temeljnim pravima i slobodama građana. Taj je sud 8. travnja 2014. godine donio vrlo važnu presudu /69/ kojom je utvrdio da se kod donošenja Direktive nije poštovalo načelo razmjernosti (proporcionalnosti) i stoga ju je proglasio nevaljanom. Sud je presudu obrazložio, kako slijedi. Direktiva zahtijeva zadržavanje vrlo širokog opsega podataka vezi s načinom korištenja elektroničkih komunikacija koje se naširoko koriste i imaju sve veću važnost u svakodnevnom životu građana. Njihovim zadržavanjem duboko se zadire u temeljna prava gotovo čitave europske populacije jer se obvezno zadržavaju podaci i onih osoba za koje nema ikakvog dokaza koji bi upućivao na ikakvu njihovu povezanost s teškim kaznenim djelom u svrhu čijeg je suzbijanja zadržavanje propisano. Direktivom se ne utvrđuju ikakva razlikovanja, ograničenja ili iznimke u odnosu na njezin cilj - borbu protiv teških kaznenih djela. Ona, nadalje, ne određuje objektivne kriterije u svrhu propisivanja ograničenja prava pristupa podacima od strane nadležnih nacionalnih tijela i njihova daljnjeg korištenja radi sprečavanja, otkrivanja ili progona kaznenih djela koja se mogu smatrati, s obzirom na širinu i težinu zadiranja u temeljna prava, dovoljno teškima kako bi se opravdalo

takvo zadiranje. Naprotiv, njome se samo općenito upućuje na teška kaznena djela kako ih svaka država članica definira u svojem domaćem pravu. Osim toga, Direktiva ne sadrži ni materijalne ni procesne uvjete u vezi s pristupom podacima i njihovim daljnjim korištenjem od strane nadležnih tijela. Pristup nadležnih tijela podacima ne uvjetuje se prethodnim pregledom od strane suda ili neovisnog upravnog tijela. Što se tiče roka zadržavanja, ne radi se razlika između kategorija podataka koji se moraju zadržati, a kod definiranog roka od najmanje 6 mjeseci do 2 godine za utvrđivanje razdoblja zadržavanja u domaćem pravu ne utvrđuje se ni pravilo da se definiranje tog razdoblja mora temeljiti na objektivnim kriterijima, kako bi se osiguralo ograničenje roka na ono što je strogo nužno. Konačno, Direktiva ne zahtijeva da se podaci zadržavaju na području EU-a, čime nije ispunjena obveza osiguravanja neovisnog nadzora (za zaštitu osobnih podataka) u pogledu zahtjeva zaštite i sigurnosti zadržavanih (osobnih) podataka. Budući da Sud nije posebno utvrdio rok kojim se takva njegova presuda ograničava, Direktiva se smatra nevaljanom od njezinog donošenja.

Predmet C-131/12 Google Spain, S.L., Google Inc. protiv Agencia Española de Protección de Datos, Mario Costeja González

U jednom su časopisu objavljene najave javnih dražbi radi prodaje nekretnina u vezi s potraživanjima za socijalno osiguranje koje su kasnije postale dostupne i na internetu. Više od petnaest godina nakon objave, osoba koja je bila navedena kao vlasnik nekretnine zatražila je od nakladnika da se najava izbriše jer je postupak davno okončan i u današnje doba više nema nikakvu važnost. To je osoba zatražila nakon što je utvrdila da se pretragom njezina imena i prezimena u Google pretraživaču dostavlja rezultat s poveznicom na navedenu objavu dražbe. Nakladnik je odbio brisanje jer je objavu naredilo španjolsko Ministarstvo rada i socijalne skrbi. Potom je osoba o kojoj je riječ kontaktirala društvo kćer Googlea u Španjolskoj (Google Spain) i zatražila da rezultati pretraživanja ne prikazuju poveznicu na časopis kada se u pretraživač unesu njezino ime i prezime. Nakon toga podnijela je zahtjev španjolskoj Agenciji za zaštitu osobnih podataka i protiv nakladnika i protiv Googlea. Agencija je odbila zahtjev protiv nakladnika jer je objava bila u skladu sa zakonom. Međutim, Agencija je naredila Googleu da povuče navedene podatke iz svojeg indeksa i onemogući da im se ubuduće pristupi. Na to se rješenje Google žalio u sudskom postupku, povodom čega je pokrenut postupak pred Sudom pravde EU-a koji je donio presudu 13. svibnja 2014. godine /70/.

Ovdje je riječ o vrlo zanimljivom predmetu u kojem se tražilo tumačenje Suda može li se smatrati da davatelj usluge internet pretraživanja u okviru pružanja te usluge obrađuje osobne podatke, kada je riječ o osobnim podacima izvorno objavljenim na internetskim stranicama trećih te smatra li se davatelj usluge internet pretraživanja voditeljem zbirke tih osobnih podataka. Sud je utvrdio da pružanje te usluge obuhvaća pretraživanje osobnih podataka objavljenih na internetu, njihovo indeksiranje, privremenu pohranu i prikaz, tj. činjenje tih podataka dostupnima trećima prema određenom redoslijedu na stranici s rezultatima pretraživanja. To predstavlja obradu tih podataka u smislu ZOP Direktive. Nadalje, Sud je utvrdio da u tom smislu Google odlučuje o svrhama i načinima obrade osobnih podataka i da je on stoga voditelj zbirke tih podataka. Pored navedenog, u predmetu se tražilo i tumačenje teritorijalnog područja primjene Direktive ZOP u digitalnom okruženju, tj. s obzirom na aktivnosti obrade osobnih podataka u kontekstu pružanja usluge internet pretraživanja od strane američke kompanije (Google Inc.) čiji se poslovni model zasniva na ponudi i prodaji oglasnog prostora i koja ima podružnice u državama članicama EU-a. Sud je presudio da je u konkretnom predmetu mjerodavno španjolsko pravo, budući da Google Inc. ima tvrtku kćer u Španjolskoj u svrhu promoviranja i prodaje oglasnog prostora čije su aktivnosti usmjerene prema građanima te države.

U predmetu se postavlja i pitanje je li ispitanik ovlašten ishoditi brisanje navedenih osobnih podataka iz indeksa, tj. rezultata pretraživanja internet pretraživača. Sud pravde EU-a presudio je da ispitanik na to ima pravo i prema važećem *acquisu* te da je davatelj usluge internet pretraživanja pod određenim uvjetima dužan izbrisati poveznice prema internetskim stranicama trećih (koje sadrže osobne podatke o kojima je riječ). Ako ispitanik postavi zahtjev za brisanje njegovih podataka (u skladu s Direktivom ZOP), a utvrdi se da u to vrijeme uključivanje poveznica prema internetskim stranicama s točnim informacijama o njemu koje su treće osobe zakonito objavile nije u skladu s Direktivom, jer se s obzirom na sve okolnosti slučaja o kojem je riječ pokazuje da su te informacije neprikladne ili da one nisu relevantne ili nisu više relevantne, odnosno da su suvišne u odnosu na svrhu obrade koju provodi davatelj usluge internet pretraživanja, tada se te informacije i poveznice moraju obrisati iz popisa rezultata pretraživanja. Sud je također skrenuo pažnju na značajnu ulogu usluga internet pretraživanja u modernom društvu i učinak koji njihovo korištenje, tj. pretraživanje internetskih stranica prema imenu ispitanika može imati na temeljna prava ispitanika na privatnost i zaštitu njegovih osobnih podataka. Sukladno tome utvrdio je da pravo na poštovanje privatnog života i na zaštitu osobnih podataka ispitanika u pravilu prevaguje nad ekonomskim interesom davatelja usluge internet pretraživanja. S druge strane, kod sagledavanja odnosa između navedenih prava ispitanika i legitimnog interesa korisnika interneta koje moguće interesira pristup tim podacima (na temelju pretrage po imenu) Sud je utvrdio da je između njih

potrebno pronaći pravednu ravnotežu. Ta ravnoteža može se razlikovati od slučaja do slučaja s obzirom na prirodu informacija o kojima je riječ i njihovu osjetljivost za privatan život ispitanika, te javnom interesu za tu informaciju koji može varirati, osobito s obzirom na ulogu ispitanika u javnom životu.

Navedena presuda osobito je aktualna u kontekstu prijedloga budućeg novog općeg okvira zaštite osobnih podataka EU-a. U njemu se, naime, podrobno uređuje i dodatno osnažuje pravo na brisanje osobnih podataka, i to osobito radi bolje prilagodbe navedenog prava uvjetima obrade podataka u digitalnom okruženju, zbog čega se popularno i naziva pravom biti zaboravljen (engl. *right to be forgotten*). Predložena rješenja novog okvira EU-a analizirat ću u idućem dijelu ovog rada.

4. Prijedlog Uredbe EU-a o općoj zaštiti osobnih podataka

Tijekom godina se pokazalo da je neujednačena provedba Direktive ZOP u državama članicama dovela do niza značajnih razlika između domaćih rješenja zaštite osobnih podataka unutar EU-a. Osim toga, pokazalo se da pojedina rješenja Direktive ne osiguravaju potrebnu razinu zaštite osobnih podataka u modernim uvjetima njihove obrade ili da su ona neprovediva, nepraktična, odnosno pretjerano otegotna s obzirom na cilj koji se htio osigurati njihovim uvođenjem /71/.

Po stupanju na snagu Lisabonskog ugovora 2009. godine /72/ i ukidanju stupova EU-a stvoreni su uvjeti za temeljite izmjene u pristupu uređenju zaštite osobnih podataka na razini prava EU-a. Danas se tako svima jamči pravo na zaštitu osobnih podataka prema čl. 16. *Ugovora o funkcioniranju Europske unije* (dalje: UFEU), a riječ je i o zasebno zajamčenom temeljnom pravu prema čl. 8. *Povelje temeljnih prava Europske unije* /73/. UFEU sadrži novu pravnu osnovu za uređenje zaštite osobnih podataka u EU-u /74/, u skladu s čime je Europska komisija u siječnju 2012. godine podnijela prijedlog Uredbe o općoj zaštiti osobnih podataka (dalje: Uredba ZOP) koji je danas u zakonodavnom postupku /75/. Osim Uredbe ZOP, u zakonodavnom postupku EU-a danas je i prijedlog nove direktive o zaštiti osobnih podataka u području kaznenopravne i policijske suradnje *(*prijedlog Direktive o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija te slobodnom kretanju takvih podataka) /76/.

U nastavnoj ću se analizi usredotočiti isključivo na odabrana rješenja predložene Uredbe ZOP kojima se žele postići značajna poboljšanja pravnog okvira u svjetlu brzog tehnološkog razvoja i drugih novijih izazova modernih uvjeta obrade osobnih podataka na koje sam uputila ranije u radu. U tu ću svrhu ispitati odabrane ključne novosti prema nedavno usvojenom kompromisnom tekstu Uredbe od strane Europskog parlamenta (12. 3. 2014.) koji sadrži brojne usvojene amandmane na izvorni prijedlog Europske komisije /77/. Prije toga valja skrenuti pažnju i na aktualnosti u području zaštite osobnih podataka na *međunarodnopravnoj razini*. Danas je, naime, u tijeku razmatranje izmjene, tj. *modernizacije Konvencije 108* koja do danas predstavlja jedini međunarodnopravno obvezujući instrument koji u sebi objedinjava temeljna načela zaštite osobnih podataka. Modernizacija Konvencije 108 također je potaknuta potrebom prilagodbe pravnog okvira novijim izazovima digitalnog globaliziranog okruženja za obradu osobnih podataka i relevantna prava ispitanika /78/.

Predloženom Uredbom ZOP stavila bi se izvan snage Direktiva ZOP. Kako su, za razliku od direktiva, uredbe izravno primjenjivi i obvezujući pravni akti EU-a, u slučaju prihvaćanja u ovome obliku, Uredba ZOP će se izravno primjenjivati i u Republici Hrvatskoj.

Uvodno skrećem pažnju na predloženo široko teritorijalno područje primjene Uredbe ZOP. Naime, njezina primjena predlaže se u pogledu obrade osobnih podataka u okviru aktivnosti poslovnog nastana voditelja zbirke ili izvršitelja obrade u Uniji, bilo da se obrada vrši u EU-u ili ne, ali i onda kada osobne podatke ispitanika u Uniji obrađuju voditelji zbirki ili izvršitelji obrade bez poslovnog nastana u EU-u, ako se aktivnosti obrade odnose na ponudu roba ili usluga ovim ispitanicima ili na njihovo praćenje (to može uključivati i radnje profiliranja ispitanika, npr. radi analize ili predviđanja njihovih sklonosti, ponašanja i stavova).

Također valja uputiti na pojedine definicije u kojima se jasno odražava potreba primjene novih pravila u modernim uvjetima obrade osobnih podataka. Njima pripadaju, primjerice, izrijekom utvrđeni identifikatori putem kojih je moguće izravno ili neizravno identificirati fizičku osobu, a koji uključuju podatke o lokaciji i jedinstvene identifikatore. Prema pojašnjenjima (iz uvodnih izjava) Uredba bi se primjenjivala i na obradu koja uključuje identifikatore koje pružaju uređaji, aplikacije, alati i protokoli, kao što su IP adrese, identifikatori kolačića i RFID etikete (osim ako se ti identifikatori ne odnose na identificiranu fizičku osobu ili fizičku osobu koju se može identificirati, tj. ako je riječ o anonimnim podacima). Pored navedenog, prijedlog Uredbe ZOP sadrži i definiciju nove kategorije osobnih podataka, a to su pseudonimni podaci. Iako ti podaci pripadaju kategoriji osobnih podataka, njihova je značajka da se oni ne mogu pripisati određenom ispitaniku bez korištenja

dodatnih informacija sve dok se takve dodatne informacije čuvaju odvojeno i dok podliježu tehničkim i organizacijskim mjerama za osiguravanje nepovezivanja. Također se uvodi definicija kodiranih podataka. Riječ je o osobnim podacima koji su pomoću tehnoloških mjera zaštite učinjeni nerazumljivima bilo kojoj osobi koja im nije ovlaštena pristupiti.

Posebnim rješenjem u nacrtu Uredbe ukidaju se znatne otegotnosti koje voditelji zbirki danas snose s obzirom na obvezu osiguravanja usklađenog postupanja s nizom različitih propisa o zaštiti osobnih podataka, ovisno o broju država članica u kojima posluju. U tu se svrhu, naime, predviđa važna uloga nadzornog tijela glavnog poslovnog nastana voditelja zbirke ili izvršitelja obrade. Riječ je o nadzornom tijelu poslovnog nastana poduzetnika ili grupe poduzetnika u Uniji, gdje se donose glavne odluke o svrhama, uvjetima i načinima obrade osobnih podataka. To nadzorno tijelo postalo bi, naime, vodeće tijelo (engl. *lead authority*) koje je odgovorno za nadzor postupaka obrade voditelja zbirke ili izvršitelja obrade u svim državama članicama. Takvo rješenje primjenjivalo bi se onda kada se obrada podataka provodi u okviru djelatnosti nastana voditelja zbirke (ili izvršitelja obrade) u Uniji, a voditelj zbirke (ili izvršitelj obrade) ima nastan u više država članica ili obrađuje osobne podatke ispitanika koji borave u više država članica.

Postrožena odgovornost jedna je od temeljnih značajki prijedloga Uredbe ZOP /79/. Predlaže se, naime, utvrđivanje niza obveza kao što su prihvaćanje odgovarajućih politika i provedba odgovarajućih i dokazivih tehničkih i organizacijskih mjera kako bi voditelji zbirki osigurali i bili sposobni transparentno dokazati da se obrada podataka provodi u skladu s Uredbom, uzimajući u obzir najnovija dostignuća, prirodu obrade, kontekst, opseg i svrhe obrade, rizike za prava i slobode ispitanika i vrstu organizacije, i u vrijeme utvrđivanja sredstava obrade i u trenutku same obrade. Osim toga, redovita opća izvješća o aktivnostima voditelja zbirke (npr. obvezna izvješća trgovačkih društava uvrštenih na burzama) moraju sadržavati sažet opis navedenih politika i mjera. Pored navedenog napominjem i predloženo rješenje prema kojem su i voditelji zbirki i izvršitelji obrade dužni voditi *redovito* ažuriranu dokumentaciju potrebnu za ispunjavanje uvjeta utvrđenih Uredbom.

Prijedlog Uredbe ZOP sadrži i niz odredaba kojima se pojašnjavaju i osnažuju prava ispitanika u modernom okruženju obrade njihovih osobnih podataka. Ta prava uključuju i pružanje jasnih i lako razumljivih informacija u vezi s obradom njihovih podataka, pravom pristupa, ispravljanja i brisanja njihovih podataka, pravom na dobivanje njihovih podataka, pravom prigovora na profiliranje, pravom podnošenja žalbe nadležnom tijelu za zaštitu osobnih podataka i pravom pokretanja sudskih postupaka kao i pravom na naknadu pretrpljene štete zbog nezakonitog postupka obrade. Skrećem pažnju i na postrožene uvjete za davanje privole koja predstavlja jednu od osnova za zakonitu obradu osobnih podataka, a označava se kao slobodno dano, određeno, izričito očitovanje volje utemeljeno na informacijama kojim ispitanik, izjavom ili jasnom potvrdnom radnjom označava suglasnost za obradu osobnih podataka. Privola bi se, naime, morala davati afirmativno, tj. treba biti riječ o izjavi ili jasnoj potvrdnoj radnji kojom se osigurava to da su pojedinci doista svjesni toga da daju svoju privolu za obradu osobnih podataka u konkretnom slučaju. Tako bi se, primjerice, na internetu privola valjano davala označavanjem polja na internetskoj stranici. Prema pojašnjenjima (iz uvodnih izjava) šutnja, samo korištenje pojedine usluge ili neaktivnost ispitanika ne bi trebali predstavljati privolu. Nadalje, temelji li se obrada podataka na privoli, nalaže se da teret dokazivanja oko dane privole snosi voditelj zbirke.

U prijedlogu Uredbe ZOP sadržane su i vrlo detaljne odredbe o obvezi obavještavanja ispitanika. Voditelj zbirke se, naime, u pogledu obrade osobnih podataka i radi ostvarenja prava ispitanika mora voditi sažetim, transparentnim, jasnim i lako dostupnim politikama, a svaka informacija u vezi s obradom osobnih podataka ispitaniku se mora dati na razumljiv način, jasnim i jednostavnim jezikom. Prije pružanja detaljnijih informacija voditelj zbirke dužan je ispitaniku dati propisani minimum informacija o obradi koje se prikazuju u posebnom obliku (ikone) i to na lako vidljiv i jasno čitljiv način i na jeziku koji lako razumiju relevantni potrošači. Ako se informacije prikazuju elektroničkim putem, one moraju biti strojno čitljive.

Uz obvezu obavještavanja ispitanika voditelji zbirki također su dužni udovoljiti njihovim zahtjevima na pristup podacima koji uključuju pravo na dobivanja potvrde o tome obrađuju li se ili ne njihovi podaci te pravo dobivanja drugih obavijesti kao što su obavijesti o svrsi obrade, važnosti i posljedicama obrade, razdoblju pohrane podataka, primateljima i dr. Od važnijih rješenja u nacrtu Uredbe vezano za ovo pravo ispitanika skrećem pažnju na obvezu voditelja zbirke da ispitaniku pruži informacije u elektroničkom i strukturiranom obliku ako je on podnio zahtjev za pristup podacima u elektroničkom obliku (osim ako ispitanik sam ne zatraži drugačiji način dobivanja informacije). Nadalje, kada je to moguće voditelj zbirke može omogućiti daljinski pristup zaštićenom sustavu putem kojeg se ispitaniku, na njegov zahtjev, omogućuje izravan pristup njegovim podacima.

Novouvedeno pravo na prenosivost osobnih podataka opravdava se potrebom njihova što lakšeg prijenosa u *online* automatiziranim aplikacijama kao što su to usluge društvenih mreža. Predviđa se, naime, da ako ispitanik ustupi osobne podatke i oni se obrađuju elektroničkim putem, on ima pravo dobiti od voditelja zbirke njihovu kopiju u elektroničkom i interoperabilnom formatu koji se uobičajeno koristi i koji mu omogućuje daljnje korištenje bez da ga u tome voditelj zbirke sprečava. Podaci bi se na zahtjev ispitanika trebali i izravno prenositi između voditelja zbirki, kada je to tehnički izvedivo i dopušteno.

U prošlom dijelu rada uputila sam na vrlo važnu presudu Suda pravde EU-a u predmetu C-131/12 u vezi s tumačenjem prava na brisanje osobnih podataka prema *acquisu* u odnosu na podatke sadržane u indeksu davatelja usluga internet pretraživanja. U nacrtu Uredbe ZOP detaljno se uređuje pravo na brisanje podataka koje se, kako sam ranije navela, od uvođenja u prijedlogu Uredbe popularno naziva *pravom biti zaboravljen*. Naime, u nacrtu Uredbe se u određenim slučajevima predviđa ne samo pravo ispitanika da ishodi brisanje njegovih osobnih podataka od voditelja zbirke nego i suzdržavanje od daljnjeg širenja tih podataka kao i pravo da se ishodi brisanje svih poveznica prema tim podacima od trećih strana, odnosno brisanje svih kopija ili replika tih podataka. Slučajevi kada bi se to primjenjivalo obuhvaćaju povlačenje jednom dane privole ispitanika za obradu ili njegov prigovor obradi ili utvrđenje da podaci više nisu potrebni u vezi sa svrhama za koje su prikupljeni ili obrađeni na drugi način, odnosno da su se podaci nezakonito obrađivali kao i slučaj konačne i pravomoćne odluke suda ili regulatornog tijela u EU-u o brisanju. Radi jačanja tog prava ispitanika u globalnom digitalnom okruženju predviđa se i obveza voditelja zbirke koji javno objavi osobne podatke bez pravne osnove da poduzme sve razumne korake kako bi se podaci izbrisali, uključujući od strane trećih osoba. Nadalje, voditelj zbirke i u slučaju primjene, treća strana dužni su bez odgode provesti brisanje podataka, osim do mjere u kojoj je njihovo zadržavanje nužno zbog ostvarivanja prava slobode izražavanja, zbog javnog interesa u području javnog zdravlja, u svrhu povijesnog, statističkog i znanstvenog istraživanja, u slučaju zakonske obveze zadržavanja tih podataka kao i u slučaju postojanja razloga za ograničenjem njihove obrade umjesto brisanja.

U prijedlogu Uredbe ZOP očekivano se utvrđuju i detaljne odredbe o sigurnosti obrade osobnih podataka s osnovnom zadaćom voditelja zbirki i izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali razinu sigurnosti koja odgovara rizicima obrade, uzimajući u obzir rezultate procjene učinka obrade na zaštitu osobnih podataka te uz obraćanje pažnje na najnovija dostignuća i trošak njihove provedbe. Osim toga, novouvedeno načelo predefinirane zaštite osobnih podataka (engl. *data protection by default*) nalaže obvezu voditelja zbirke da osigura to da se kao početna vrijednost obrađuju samo oni osobni podaci koji su nužni za svaku određenu svrhu obrade i osobito da se ne prikupljaju, zadržavaju ili šire više od nužnog minimuma za te svrhe (to i u pogledu količine podataka i u pogledu razdoblja njihove pohrane). Tim se mehanizmom posebno treba osigurati kao početna vrijednost to da osobni podaci ne budu automatski dostupni neodređenom broju osoba i da ispitanici budu u mogućnosti nadzirati dijeljenje, tj. distribuciju svojih osobnih podataka. Nadalje, u nacrtu Uredbe izričito se uvodi i načelo zaštite osobnih podataka po **dizajnu** (engl. *data protection by design*) koje predstavlja obvezu prema kojoj su voditelj zbirke (i izvršitelj obrade, ako postoji) dužni i u vrijeme utvrđivanja svrha i sredstava obrade i u vrijeme same obrade provoditi odgovarajuće i razmjerne tehničke i organizacijske mjere i postupke tako da obrada bude u skladu s odredbama *Uredbe i da se osigurava zaštita prava ispitanika*, osobito u vezi s načelima obrade osobnih podataka, sve to uzimajući u obzir najnovija dostignuća, trenutačno tehničko znanje, međunarodnu najbolju praksu i rizike koje predstavlja obrada podataka.

Valja skrenuti pažnju i na odredbe kojima se predviđaju postupci certificiranja te izdavanja tzv. europskog pečata za zaštitu osobnih podataka (engl. *European Data Protection Seal*) u svrhu potvrde toga da se obrada podataka provodi u skladu s Uredbom. Ispitanicima se na taj način omogućuje brza, pouzdana i provjerljiva procjena razine zaštite osobnih podataka za relevantne proizvode i usluge. Osim toga, u prijedlogu Uredbe ZOP na različite se načine daju poticaji za poduzimanje mjera radi izdavanja pečata pa se tako, između ostalog, voditelji zbirki (izvršitelji obrade) s pečatom neće novčano kazniti ako nisu prekršili Uredbu s namjerom ili krajnjom nepažnjom.

Posebna se pažnja u nacrtu Uredbe ZOP posvećuje procesu upravljanja zaštitom osobnih podataka tijekom njihova cijelog životnog ciklusa (*engl. lifecycle data protection management)*. Naime, voditelji zbirki trebali bi se usredotočiti na zaštitu osobnih podataka tijekom cjelokupnog životnog vijeka podataka, od njihovog prikupljanja preko obrade do brisanja, od početka ulažući u održiv okvir za upravljanje podacima i nastavljajući ga sveobuhvatnim mehanizmom za usklađenost. Predviđa se i obveza imenovanja službenika za zaštitu osobnih podataka (i od strane voditelja zbirki i od strane izvršitelja obrade) u sljedećim slučajevima: kada obradu vrši javna ustanova ili tijelo, ili kada obradu provodi pravna osoba i ona se odnosi na više od 5000 ispitanika u bilo kojem uzastopnom razdoblju od 12 mjeseci, ili kada se osnovne djelatnosti voditelja zbirke/izvršitelja obrade sastoje od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika, ili kada se osnovne djelatnosti voditelja zbirke/izvršitelja obrade sastoje od obrade posebnih

kategorija podataka, podataka o lokaciji ili o djeci ili podataka o radnicima u opsežnim zbirkama osobnih podataka. Pored navedenog, u prijedlogu Uredbe uređuju se pitanja imenovanja tih službenika i njihova položaja kao i njihovih zadataka. Nadalje, voditelj zbirke (ili gdje je primjenjivo, izvršitelj obrade) trebao bi provoditi analizu rizika potencijalnog učinka namjeravane obrade podataka na prava i slobode ispitanika, pri čemu procjenjuje je li vjerojatno da njegovi postupci obrade predstavljaju određene rizike (u Uredbi se izričito predviđaju takvi primjeri). Novouvedenim postupcima procjene učinka obrade na zaštitu osobnih podataka (engl. *data protection impact assessment*) želi se osigurati njihova svijest o svim mogućim posljedicama postupaka obrade podataka (uz opis predviđenih postupaka obrade, rizika za prava i slobode ispitanika, predviđenih mjera odgovora na rizike, zaštitnih i sigurnosnih mjera te mehanizama kako bi se osigurala usklađenost s Uredbom). Provedbom provjera sukladnosti sa zaštitom osobnih podataka periodično najmanje jednom u svake dvije godine ili odmah kada nastupi promjena u određenim rizicima koje predstavljaju postupci obrade trebala bi se osigurati potvrda toga da se obrada provodi u skladu s ranije navedenom procjenom učinka. Osim toga, predloženim se postupkom prethodnog savjetovanja (prije obrade podataka) voditelja zbirke (ili izvršitelja obrade koji djeluje u ime voditelja zbirke) sa službenikom za zaštitu podataka, odnosno s nadzornim tijelom ako službenik nije imenovan, predlaže ublažiti rizike za ispitanike kada, npr., procjena učinka obrade upućuje na visok rizik.

U drugom dijelu rada pojasnila sam postupak obavještavanja nadzornih tijela i ispitanika kao i druge obveze u slučajevima povreda osobnih podataka koje su danas na snazi jedino u području elektroničkih komunikacija (Direktiva o e-privatnosti, Uredba Komisije br. 611/2013, ZEK). Prijedlogom Uredbe navedeni postupci i obveze napokon se jednoznačno uređuju za sve voditelje zbirki, što je od iznimne važnosti s obzirom na rastuću obradu osobnih podataka u globalnom digitalnom okruženju. Pritom valja napomenuti da se Uredbom ne bi nametale dodatne obveze u vezi s obradom osobnih podataka u vezi s pružanjem javno dostupih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama u pogledu onih pitanja koja su već uređena Direktivom o e-privatnosti. Stoga se predviđa brisanje pojedinih odredbi te Direktive, uključujući posebne obveze u vezi sa sigurnošću obrade i prijavama povreda osobnih podataka. Osim toga, predviđa se i da će Europska komisija bez odlaganja te najkasnije do dana početka primjene Uredbe predložiti izmjene pravnog okvira za obradu osobnih podataka i zaštitu privatnosti u elektroničkim komunikacijama, kako bi uskladila propise s Uredbom i osigurala dosljedne i ujednačene odredbe koje se odnose na temeljno pravo na zaštitu osobnih podataka u EU-u.
Što se tiče postupaka povreda osobnih podataka, u nacrtu Uredbe se po uzoru na rješenja iz Direktive o e-privatnosti predviđa obveza obavještavanja nadzornog tijela u slučaju povrede osobnih podataka (u smislu slučajnog ili nezakonitog uništavanja, gubitka, izmjene, neovlaštenog otkrivanja ili neovlaštenog pristupa osobnim podacima koji se prenose, pohranjuju ili na drugi način obrađuju), i to bez nepotrebnog odgađanja. Prema pojašnjenjima smatra se da taj rok ne bi trebao biti dulji od 72 sata. Također se utvrđuje obveza obavještavanja ispitanika kada je vjerojatno da će povreda osobnih podataka štetno utjecati na zaštitu osobnih podataka, privatnost, prava ili legitimne interese, osim ako voditelj zbirke pokaže da je na pogođene podatke primijenio odgovarajuće mjere tehničke zaštite koje čine podatke nerazumljivima osobama koje im nisu ovlaštene pristupiti, s kojima je nadzorno tijelo zadovoljno.

U pogledu rješenja u prijedlogu Uredbe ZOP o **pravnim lijekovima** skrećem pažnju na predviđeno pravo ispitanika da podnose pritužbe (u slučaju povrede prava, tj. Uredbe ZOP) nadzornom tijelu u bilo kojoj državi članici. Osim toga, predviđa se pravo pokretanja sudskog postupka i protiv nadzornog tijela i protiv voditelja zbirki i izvršitelja obrade. Ta prava predviđaju se i za tijela, organizacije ili udruge koje djeluju u javnom interesu, a osnovane su u skladu sa zakonodavstvom države članice. Ta su tijela ovlaštena podnijeti pritužbu pred nadzornim tijelom u ime jednog ili više ispitanika, ali i neovisno o žalbi ispitanika ako smatraju da je povrijeđena Uredba. Nadalje, kada su na to ovlaštena od strane ispitanika ona imaju pravo pokrenuti sudski postupak protiv nadzornog tijela, voditelja zbirki i izvršitelja obrade kao i tražiti naknadu štete pred sudom (protiv voditelja zbirki ili izvršitelja obrade).

U završnim napomenama o prijedlogu Uredbe ZOP usredotočit ću se na odabrana rješenja u pogledu nadzornih tijela koja odražavaju priznanje njihove ključne uloge u državama članicama radi osiguravanja ujednačene i učinkovite zaštite osobnih podataka diljem EU-a /80/. Poseban naglasak daje se odredbama kojima je cilj osigurati njihovu potpunu neovisnost i nepristranost u provođenju dužnosti i ovlasti koje su im povjerene, što uključuje i propisane uvjete za imenovanje koji obuhvaćaju i zahtjeve u pogledu njihove neovisnosti te dokazanog iskustva i vještina poglavito u području zaštite osobnih podataka, te uvjete njihova razrješenja. U navedenim se odredbama u tom pogledu odražava i relevantna sudska praksa Suda pravde EU-a koji je u svojoj praksi tumačio zahtjev neovisnosti ovih tijela prema Direktivi ZOP (čl. 28. st. 1.). Naime, koncept potpune neovisnosti traži da nadzorna tijela budu slobodna od bilo kakva utjecaja, izravnog ili neizravnog, u svojem radu i donošenju odluka te čak i sam rizik političkog utjecaja nad njihovim odlukama utječe na neovisno obavljanje zadataka. Osim toga, uvjet neovisnosti nije ispunjen samo s utvrđenom funkcionalnom neovisnošću nadzornih

tijela ako još uvijek ima mogućnosti da se na ta tijela izvrši vanjski utjecaj. Osim u presudama koje je po navedenim pitanjima Sud donio protiv Njemačke i Austrije, ta su načela potvrđena i u nedavno donesenoj presudi protiv Mađarske (8. travnja 2014.) /81/.

U nacrtu Uredbe ZOP detaljno se utvrđuju i zadaci i ovlasti nadzornih tijela koji trebaju biti ujednačeni diljem EU-a. Osobito jačanje njihovih ovlasti predstavlja prijedlog uvođenja ovlasti izravnog kažnjavanja kršenja odredaba Uredbe, a to se u određenim slučajevima odnosi i na ovlast izricanja novčanih kazni do najviše 100 milijuna eura ili 5 % ukupnoga godišnjeg prometa ako je riječ o poduzeću, ovisno o tome koji je od dvaju iznosa veći. U Uredbi se predviđaju i razni mehanizmi suradnje između nadzornih tijela u EU-u, a to, među ostalim, i radi osiguravanja usklađene razine sankcija u Uniji.

5. Zaključne napomene

Kod utvrđivanja mjera obrade osobnih podataka i njihove provedbe osobito je važno prepoznavanje rizika s obzirom na sve okolnosti te obrade kao i razumijevanje informacijskih i komunikacijskih tehnologija i usluga o kojima je riječ, odnosno postupaka putem kojih se omogućuju različite vrste i funkcionalnosti navedene obrade. Posebno je to važno u uvjetima opće globalizacije, digitalizacije i permanentne znanstveno-tehnološke revolucije. Ovo treba biti briga svih. Svatko u svojem području sukladno ovlastima mora dati doprinos - od zakonodavca i tijela primjene (sudova, nadležnih nadzornih tijela i dr.) te voditelja zbirki osobnih podataka do industrije koja sudjeluje u razvoju, prilagodbi i implementaciji informacijskih i komunikacijskih tehnologija i usluga. Osobito je to značajno kod onih koji su nadležni takve mjere donositi i provoditi. Kao pozitivan primjer može poslužiti pristup koji u svojem radu ima njemački Savezni ustavni sud /82/. U svojim odlukama taj sud poziva i tijela vlasti da prilikom uređivanja područja koja uključuju primjenu naprednih informacijskih i komunikacijskih tehnologija kao i kod razmatranja izmjena relevantnih propisa uzmu u obzir dotičnu tehnologiju i njezin razvoj, osobito u području koje predstavlja potencijalno zadiranje u osobna prava pojedinca /83/.

Takav ozbiljan i usredotočan pristup nužno je razvijati u Republici Hrvatskoj. Uz analizu *acquisa* i niza domaćih propisa relevantnih za navedeno područje u radu su pojašnjene i aktualnosti u razvoju pravnog okvira EU-a radi prilagodbe novijim izazovima koje za sigurnost i privatnost osobnih podataka predstavljaju uvjeti brzog tehnološkog napretka u globalno umreženom komunikacijskom okruženju. Sve navedeno, a osobito posebna pažnja koju pitanjima sigurnosti i privatnosti osobnih podataka u takvim uvjetima daje europski zakonodavac upućuje na potrebu intenzivnog dijaloga na tu temu između svih relevantnih dionika u Republici Hrvatskoj. Osim razvoja *acquisa* po navedenim pitanjima, uključujući važna tumačenja koja je do danas u svojim odlukama dao Sud pravde EU-a, tome u prilog idu osobito prijedlozi rješenja novog općeg pravnog okvira EU-a u području zaštite osobnih podataka koje sam analizirala u radu. Njima pripada i niz odredbi u kojima se odražava ključna uloga nadzornih tijela u domaćem i europskom sustavu zaštite osobnih podataka. Stoga je jedan od zaključaka analize važećeg domaćeg općeg okvira zaštite osobnih podataka, na koji ovdje posebno treba uputiti, potreba što skorijeg osiguravanja odgovarajućih uvjeta za jačanje uloge i ovlasti domaćeg nadzornog tijela za zaštitu osobnih podataka. Osim toga, s posebnim se zanimanjem očekuje daljnji razvoj relevantne domaće prakse, a osobito ciljanih aktivnosti sa svrhom podizanja osviještenosti relevantnih dionika i šire javnosti. Po mojem mišljenju ovdje osobito spada i utvrđivanje smjernica i preporuka kojima se odražava najbolja praksa u svrhu utvrđivanja rizika za sigurnost i privatnost osobnih podataka u modernom digitalnom okruženju i primjene mjera radi njihovog izbjegavanja, odnosno ublažavanja te u svrhu pravilne primjene odgovarajućih zahtjeva mjerodavnog pravnog okvira. U tom izrazito dinamičnom području potrebno je i ažurno te kritički pratiti razvoj tehnologije kao i *acquisa* te odgovarajućih aktivnosti na međunarodnopravnoj razini. Bitna je ovdje i uloga akademske zajednice koja osobito unošenjem sadržaja iz tog područja u svoje obrazovne programe može dati važan doprinos boljem razumijevanju i učinkovitijem ostvarivanju zaštite osobnih podataka u postmodernom digitalnom društvu.

BILJEŠKE

/1/ Imajući u vidu dinamičan razvoj relevantnog pravno-regulatornog okvira u radu se u određenoj mjeri nadograđuju rezultati istraživanja iz doktorske disertacije autorice: Gumzej Nina, Zaštita podataka u elektroničkim komunikacijama, doktorska disertacija, Pravni fakultet Sveučilišta u Zagrebu, 2011.

/2/ Kuneva Meglena, (bivša) europska povjerenica za zaštitu potrošača, Roundtable on online data collection, targeting and profiling, SPEECH/09/156, Brisel, 31. 3. 2009., http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm (zadnji pristup 08. 5. 2014.).

/3/ Za rana upozorenja na ovu temu u domaćoj znanstvenoj literaturi, vidi, na primjer: Dragičević Dražen, Kompjutorski kriminalitet i informacijski sustavi, Informator, Zagreb, 1999.; Dragičević Dražen, Privatnost u virtualnom svijetu. Zbornik Pravnog Fakulteta u Zagrebu, 51, 2001., 3-4, str. 615-644.

/4/ Podrobnije vidi u: Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, 20. 6. 2007. (zadnji pristup 08. 5. 2014.). Od relevantne sudske prakse Suda pravde EU-a vidi osobito presude u predmetu C-70/10 Scarlet Extended SA protiv SABAM, Zbornik sudske prakse 2011 I-11959

(ECLI:EU:C:2011:771), točka 51 kao i u predmetu C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) protiv Netlog NV, Zbornik sudske prakse - elektronički (ECLI:EU:C:2012:85), točka 49.

/5/ Za pojašnjenja koncepta rudarenja podataka (engl. *data mining*) vidi: http://en.wikipedia.org/wiki/Data_mining; skladištenja podataka (engl. *data warehousing*), http://en.wikipedia.org /wiki/Data_warehouse. Vidi i: Dinant Jean-Marc *et al*, Application of Convention 108 to the profiling mechanism – Some ideas for the future work of the consultative committee (T-PD). Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD), T-PD(2008)01, Strasbourg, 11.1.2008, 24th meeting, Strasbourg, G01, 13. - 14. 3. 2008., dostupno na:http://www.coe.int/t/dghl/standardsetting/ dataprotection/Reports/CRID_Profiling_2008_en. pdf (zadnji pristup 08. 5. 2014.).

/6/ Za pojašnjenja GPS tehnologije (engl. *Global Positioning System*) vidi: http://en.wikipedia.org/wiki/Global_ Positioning_System (zadnji pristup 08. 5. 2014.).

/7/ Engl. *Deep Packet Inspection*, skraćeno DPI. Iako se prvotno DPI tehnologija koristila u svrhu sigurnosti mreže, tj. zaštite korisnika Interneta od štetnih i zlonamjernih programa, sve su različitije namjene njezine primjene, odnosno postoje sve različiti ciljevi koji se žele postići njezinom uporabom (npr. upravljanje mrežom, uključujući upravljanje pojasnim širinama, nadzor Internet komunikacija u stvarnom vremenu koje u propisanim slučajevima poduzima ovlašteno državno tijelo, regulacija sadržaja npr. na način da se prepoznaje sadržaj koji se smatra nezakonitim te se potom blokira pristup istome, upravljanje zaštitom autorskih prava *online*, ciljano oglašavanje). Podrobnije vidi u: Daly Angela, The Legality of Deep Packet Inspection, International Journal of Communications Law & Policy, br. 14, 2011., dostupno na SSRN: http://ssrn.com/abstract=1628024 (osobito točka 3); Bendrath Ralf; Mueller Milton, The End of the Net as We Know it? Deep Packet Inspection and Internet Governance, 04. 8. 2010., osobito str. 5-6, 14-23, dostupno na SSRN: http://ssrn.com/abstract=1653259 (zadnji pristup 08. 5. 2014.).

/8/ S time u vezi valja osobito uputiti na izvješće posebnog izvjestitelja UN-a za promoviranje i zaštitu ljudskih prava i temeljnih sloboda u kontekstu borbe protiv terorizma: Scheinin Martin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Advance Edited Version, A/HRC/13/37, 28. 12. 2009., dostupno na:
http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf (zadnji pristup 08. 5. 2014.).

/9/ Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 17, 22. 6. 2010.

/10/ Za pojašnjenja vidi: Web 2.0, http://en.wikipedia.org/wiki/Web_2; User-Generated Content, http://en.wiki pedia. org/wiki/ User-generated_content (zadnji pristup 08. 5. 2014.).

/11/ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Unleashing the Potential of Cloud Computing in Europe, COM/2012/0529 final, Brisel, 27. 9. 2012. Za detaljniju autoričinu analizu (zaključno s pregledom ključnih aktualnosti do prve polovice 2012. g.), vidi: Gumzej Nina, Odabrani pravni aspekti usluge računalstva u oblaku, Zbornik konferencije CASE 24 – razvoj poslovnih i informatičkih sustava, 04. 6.- 05. 6. 2012., Zagreb, Case d.o.o., Rijeka, 2012., str. 123-134 (članak je moguće dostaviti e-poštom na zahtjev autorici na: nina.gumzej@pravo.hr).

/12/ Detaljnije vidi npr. u: European Commission, Internet of Things - An action plan for Europe, COM(2009) 278 final, 18. 6. 2009.; Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, SL L 122, 16. 5. 2009., str. 47–51; Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12. 1. 2011.,
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf; Article 29 Data Protection Working Party. Working document on data protection issues related to RFID technology, 10107/05/EN, WP 105, 19. 1. 2005., str. 8.; Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96, SL C 101, 23. 4. 2008., str. 1-12. Za pravno-regulatornu analizu autorice, vidi: Gumzej Nina, Protection of Data Relating to EU Consumers in the IoT Age, u: Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference Proceedings, 11. - 13. 9. 2012., Split, Croatia, IEEE Xplore, Print ISBN: 978-1-4673-2710-7, 2012., str. 1-6.

/13/ Za pojašnjenja vidi: Big Data, http://en.wikipedia.org/wiki/Big_data (zadnji pristup 08. 5. 2014.).

/14/ IP adrese predstavljaju jedinstvenu identifikacijsku oznaku računala i drugih uređaja spojenih na Internetu kojima se koriste pojedinci.

/15/ Kolačić (engl. *cookie*) je informacija koju generira (u pravilu) poslužitelj određenog web-mjesta i postavlja u terminalnu opremu korisnika, kao što je to tvrdi disk korisnikovog računala, zadržavajući kopiju za sebe.

/16/ Detaljnije na temu vidi npr. u: Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN, WP216, 10. 4. 2014.; Ohm Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, 57, 2010., 6, str. 1701-1777, dostupno na: http://uclalawreview.org/pdf/57-6-3.pdf (zadnji pristup 08. 5. 2014.).

/17/ Kibernetički kriminal (engl. *cybercrime*) može se definirati kao „ukupnost kaznenih djela koja su kroz određeno vrijeme počinjena unutar kibernetičkog prostora ili uz njegovu pomoć korištenjem ili zlorabljenjem njegovih resursa, servisa ili usluga uz pomoć informacijskih tehnologija koje čine njegovu infrastrukturu." Dragičević Dražen, Novi izazovi kibernetičkog kriminala, Hrvatska pravna revija, 5, 2005., 7-8, str. 150. Vidi i: Dragičević Dražen, Izazovi kibernetičkog kriminala – stanje i novi trendovi, u: Dražen Dragičević *et al*, Aktualna pitanja kaznenog zakonodavstva – 2005, Inženjerski biro, Zagreb, 2005., str. 58.

/18/ Kibernetički prostor (engl. *cyberspace*) može se definirati kao prostor koji obuhvaća „najrazličitije informacijske resurse, servise i usluge dostupne putem komunikacijskih mreža, posebno Interneta, kao i „zajednice" i njihove kulture nastale u takvom elektroničkom okruženju." *Ibid.*

/19/ Službeni list Europske unije (dalje: SL) L 281, 23.11.1995, str. 31-50.

/20/ Convention for the protection of human rights and fundamental freedoms, 4. 11. 1950.; Convention for the protection of individuals with regard to automatic processing of personal data, 28. 1. 1981.; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 08. 11. 2001.
/21/ Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, SL L 350, 30.12.2008, str. 60-71.
/22/ Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, SL L 8, 12.1.2001, str. 1-22. Ova se uredba primjenjuje na sva tijela i institucije Zajednice prilikom obrade osobnih podataka koja se provodi u okviru obavljanja djelatnosti koje su u potpunosti ili djelomično u području primjene prava EU (čl. 3. st. 1. Uredbe br. 45 / 2001).
/23/ Podrobnije vidi u uvodnoj izjavi br. 9 ZOP Direktive, a za primjer vidi čl. 8. st. 4. - 5. Direktive.
/24/ Radi se ovdje o cilju uspostave ravnoteže između slobodnog prekograničnog protoka osobnih podataka i zaštite privatnog života, kao i o cilju uspostave ravnoteže između različitih prava i interesa koji su pritom zahvaćeni. C-101/01 Kazneni postupak protiv Bodil Lindqvist, Zbornik sudske prakse 2003 I-12971 (ECLI:EU:C:2003:596); C-553/07 College van burgemeester en wethouders van Rotterdam protiv M. E. E. Rijkeboer, Zbornik sudske prakse 2009 I-03889 (ECLI:EU:C:2009:293).
/25/ C-524/06 Heinz Huber protiv Bundesrepublik Deutschland, Zbornik sudske prakse 2008 I-09705 (ECLI:EU:C:2008:724); C-101/01 Kazneni postupak protiv Bodil Lindqvist, Zbornik sudske prakse 2003 I-12971 (ECLI:EU:C:2003:596).
/26/ Zakon o potvrđivanju Konvencije za zaštitu ljudskih prava i temeljnih sloboda i Protokola br. 1., 4., 6., 7. i 11. uz Konvenciju za zaštitu ljudskih prava i temeljnih sloboda, Narodne novine – Međunarodni ugovori (dalje: NN-MU) br. 18/97 - pročišćeni tekst: NN-MU br. 6/99 i 8/99); Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka, NN-MU br. 4/05; Zakon o potvrđivanju izmjena i dopuna Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka (ETS br. 108) koje Europskim zajednicama omogućavaju pristupanje, NN-MU br. 12/05.
/27/ Zakon o zaštiti osobnih podataka, Narodne novine (dalje: NN) br. 103/03, 118/06, 41/08 i 130/11, pročišćeni tekst objavljen je u NN br. 106/12.
/28/ Za korisno (pravno neobvezujuće) tumačenje navedenog čl. 4. Direktive ZOP, vidi: Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law, 0836-02/10/EN, WP 179, 16. 12. 2010.
/29/ Vidi npr. Zakon o tajnosti podataka, NN br. 79/07 i 86/12.
/30/ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), SL L 201, 31. 7. 2002., str. 37-47. Ova Direktiva zamijenila je raniju Direktivu 97/66/EZ o obradi osobnih podataka i zaštiti privatnosti u području telekomunikacija, SL L 24, 30. 1. 1998., str. 1-8.
/31/ Podrobnije vidi u uvodnoj izjavi br. 10 Direktive o e-privatnosti kao i u čl. 1. st. 2. u vezi s čl. 1. st. 1. Direktive; Article 29 Data Protection Working Party, *supra* bilj. 9, str. 9-10; Roosendaal Arnold *et al*, The legal framework for location-based services in Europe, Future of Identity in the Information Society, Deliverable D 11.5, lipanj 2007., str. 26, dostupno na: http://www.fidis.net/resources/deliverables/mobility-and-identity/#cl (zadnji pristup 08. 5. 2014.); Schnabel Christoph, Privacy and Data Protection in EC Telecommunications Law, u: Koenig Christian *et al*, EC Competition and Telecommunications Law, 2. izdanje, Alphen aan den Rijn: Kluwer Law International, Nizozemska, International Competition Law Series, 6, 2009., str. 520.
/32/ Direktiva 2009/136/EZ kojom se mijenja Direktiva 2002/22/EZ o univerzalnim uslugama i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama, Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija, te Uredba 2006/2004 o suradnji između nacionalnih tijela vlasti odgovornih za provedbu zakona o zaštiti potrošača, SL L 337, 18. 12. 2009., str. 11-36.
/33/ Podrobnije vidi u uvodnoj izjavi br. 56 Direktive 2009/136/EZ (u vezi s čl. 3. Direktive o e-privatnosti - čl. 2. st. 3. Direktive 2009/136/EZ).
/34/ Za podrobniju analizu tih propisa kroz usporedni pregled prava EU-a i domaćeg prava, vidi: Gumzej Nina, Evolving challenges and legal safeguards in processing user data in electronic communications, Proceedings of the 12th International Conference on Telecommunications – ConTEL 2013, 3rd Workshop on Regulatory Challenges in the Electronic Communications Market, 26. – 28. 6. 2013., Zagreb, Fakultet elektrotehnike i računarstva, Zagreb, 2013., str. 271-281, dostupno na: http://icsl.tel.fer.hr/contel2013_proceedings.pdf (zadnji pristup 08. 5. 2014.).
/35/ Detaljnije vidi u uvodnim izjavama br. 24 - 26 Direktive o e-privatnosti, kao i uvodnim izjavama br. 65 - 66 Direktive 2009/136/EZ.
/36/ Za detaljnija pojašnjenja vidi, npr.: Article 29 Data Protection Working Party, *supra* bilj. 9.
/37/ Za analizu navedenih revidiranih pravila Direktive o e-privatnosti i načina osiguravanja usklađenog postupanja, ovisno o različitim vrstama i svrhama kolačića, ispitivanje provedbe unutar EU-a uz usporedni pregled domaćeg rješenja te pregled važnijih aktualnosti u području, vidi: Gumzej Nina; Grgić Snježana, ePrivacy rules and data processing in users' terminal equipment: a Croatian experience, MIPRO Proceedings 2013, 36th International Convention, 20 - 24. 5. 2013., Opatija, Croatian Society for Information and Communication Technology, Electronics and Microelectronics – MIPRO, Rijeka, 2013., str. 1501-1507, dostupno na: http://docs. mipro-proceedings. com/de/de_003_1992.pdf (zadnji pristup 08. 5. 2014.).
/38/ Podrobnije vidi u uvodnoj izjavi br. 57 Direktive 2009/136/EZ.
/39/ Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic

communications, SL L 173, 26. 6. 2013., str. 2–8. Za relevantna pravila Direktive o e-privatnosti vidi čl. 2.i i čl. 4. st. 3-5 Direktive.
/40/ Za pojašnjenja izmjena u odnosu na ranije važeće kazneno djelo, te novije komentare, vidi: Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 189-190 (uz prijedlog čl. 146.); Pavlović Šime, Kazneni zakon – Drugo, izmijenjeno, dopunjeno i prošireno izdanje, Libertin naklada, Rijeka, 2013., str. 376-378.
/41/ Kazneni zakon, NN br. 125/11 i 144/12.
/42/ Čl. 133. Kaznenog zakona (NN br. 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07 i 152/08).
/43/ Pravno shvaćanje Kaznenog odjela Vrhovnog suda Republike Hrvatske, Su-IV k-4/2012-57, 27. 12. 2012.
/44/ Vidi detaljnije u glavi XXV. Kaznenog zakona (čl. 266. – 273.) te za pojašnjenja i komentare: Vlada RH, *supra* bilj. 40, str. 242-244; Pavlović Šime, *supra* bilj. 40, str. 696- 709.
/45/ Konvencija o kibernetičkom kriminalu – Convention on Cybercrime (CETS No. 185), 23.11.2001. Vidi Zakon o potvrđivanju Konvencije o kibernetičkom kriminalu, NN-MU br. 9/02 i Objavu o stupanju na snagu Konvencije o kibernetičkom kriminalu, NN–MU br. 4/04.
/46/ European Commission, Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, Brussels, 30. 9. 2010. COM(2010) 517 final.
/47/ SL L 218, 14. 8. 2013., str. 8-14.
/48/ Neovlašteni pristup sankcionira se bez obzira na postojanje zaštitnih mjera, a kao kvalificirani oblik ovog djela utvrđuje se neovlašteni pristup počinjen u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, tijela jedinica lokalne ili područne samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa. Detaljnije vidi u čl. 266. Kaznenog zakona.
/49/ Pravno shvaćanje Kaznenog odjela Vrhovnog suda Republike Hrvatske, *supra* bilj. 43.
/50/ Vidi detaljnije u glavi XV. Kaznenog zakona (čl. 147. – 151.) te za pojašnjenja i komentare: Vlada RH, *supra* bilj. 40, str. 190-192 (uz čl. 147. – 151.); Derenčinović Davor *et al*, Posebni dio kaznenog prava: prvo izdanje, Pravni fakultet u Zagrebu, Zagreb, 2013., str. 133-153; Pavlović Šime, *supra* bilj. 40, str. 379-389.
/51/ Za komentare vidi: Vlada RH, *supra* bilj. 40, str. 187-188 (uz prijedlog čl. 140.); Bumči Koraljka, Kazneno djelo »Nametljivo ponašanje« u novom Kaznenom zakonu, Informator, 6039, 21. 1. 2012., str. 1-3; Pavlović Šime, *supra* bilj. 40, str. 366-367.
/52/ Cvitanović Leo; Glavić Ivan, Uz problematiku sigurnosne mjere zabrane pristupa internetu, Hrvatski ljetopis za kazneno pravo i praksu, 19, 2012., 2, dostupno na: http://hrcak.srce.hr/file/163407 (zadnji pristup 08. 5. 2014.); Pavlović Šime, *supra* bilj. 40, str. 175-176; Novoselec Petar; Bojanić Igor, Opći dio Kaznenog prava, Četvrto, izmijenjeno izdanje, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2013., str. 467-468; Matić Tin, Internet - pravo na komunikaciju i informaciju u odnosu na sigurnosnu mjeru zabrane pristupa internetu iz Kaznenog zakona RH, Hrvatska pravna revija, 13, 2013., 1, str. 28-36; Škrtić Dražen, Sigurnosna mjera - zabrana pristupa internetu, Zbornik prispevkov, 14. Slovenski dnevi varstvoslovja, Fakulteta za varnostne vede, Ljubljana, 05. - 06. 6. 2013., str. 1-13, dostupno na: http://www.fvv.uni-mb.si/DV2013/zbornik/informacijska_varnost/ skrtic.pdf (zadnji pristup 08. 5. 2014.).
/53/ European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brisel, 07. 2. 2013., JOIN/2013/01 final.
/54/ European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, Brisel, 07. 2. 2013., COM/2013/048 final - 2013/0027 (COD).
/55/ Prijedlog Odluke o osnivanju Povjerenstva za izradu Nacrta prijedloga nacionalne strategije kibernetičke sigurnosti, 153. sjednica Vlade RH, 30. 4. 2014., dostupno na: http://www.vlada.hr/naslovnica/sjednice_i_odluke_vlade_rh/2014/153_sjednica_vlade_republike_hrvatske (zadnji pristup 14. 5. 2014.).
/56/ SL L 105, 13. 4. 2006., str. 54-63.
/57/ Osobito vidi čl. 1.a (NN br. 76/13).
/58/ Za detaljnu analizu uređenja sustava obveznog preventivnog zadržavanja podataka u elektroničkim komunikacijama prema pravu EU-a i domaćem pravu u domaćoj znanstvenoj literaturi, vidi Dragičević Dražen; Gumzej Nina, Obvezno zadržavanje podataka i privatnost, Zbornik Pravnog fakulteta u Zagrebu, 64, 2014., 1, str. 39-79, dostupno na: http://hrcak.srce.hr/index.php?show=casopis&id_casopis=101 (zadnji pristup 08. 5. 2014.).
/59/ C-101/01 Kazneni postupak protiv Bodil Lindqvist, Zbornik sudske prakse 2003 I-12971 (ECLI:EU:C:2003:596).
/60/ Za detaljnu analizu predmeta, uključenih propisa i općenito problematike odgovornosti internetskih posrednika za povrede autorskog i srodnih prava na internetu u domaćoj znanstvenoj literaturi, vidi: Dragičević Dražen; Gumzej Nina, Odgovornost posrednika za povrede autorskog i srodnih prava na internetu, Zbornik Pravnog fakulteta u Zagrebu, 62, 2012., 4, str. 1003–1042, dostupno na: http://hrcak.srce.hr/index.php?show=clanak&id_clanak_jezik=139022 (zadnji pristup 08. 5. 2014.).
/61/ C-70/10 Scarlet Extended SA protiv SABAM, Zbornik sudske prakse 2011 I-11959 (ECLI:EU:C:2011:771).
/62/ C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers (SABAM) protiv Netlog NV, Zbornik sudske prakse - elektronički (ECLI:EU:C:2012:85).
/63/ Predmet C-314/12 UPC Telekabel Wien GmbH protiv Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH, ECLI:EU:C:2014:192 (još nije objavljeno u Zborniku sudske prakse), vidi osobito točke 52-57, 62-64.
/64/ Za detaljnu analizu predmeta, uključenih propisa i općenito pitanja zaštite temeljnih prava građana u kontekstu zaštite prava intelektualnog vlasništva na internetu u domaćoj znanstvenoj literaturi, vidi: Dragičević Dražen; Gumzej Nina, Temeljna prava građana u kontekstu pravne zaštite intelektualnog vlasništva na internetu, Društvo i tehnologija 2013 - dr.

Juraj Plenković, XX. Međunarodni znanstveni skup, Zbornik radova, International Federation of Communication Associations, Croatian Communication Association i Alma Mater Europaea – European Center Maribor, Zagreb, 2013., str. 381-402, dostupno na: https://bib.irb.hr/datoteka/659270.642946.DIT_2013_Book_of_Manuscripts.pdf (zadnji pristup 08. 5. 2014.).

/65/ C-275/06 Productores de Música de España (Promusicae) protiv Telefónica de España SAU, Zbornik sudske prakse 2008 I-00271 (ECLI:EU:C:2008:54).

/66/ C-557/07 LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH protiv Tele2 Telecommunication GmbH, Zbornik sudske prakse 2009 I-01227 (ECLI:EU:C:2009:107).

/67/ C-461/10 Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget Aktiebolag, Storyside AB protiv Perfect Communication Sweden, ECLI:EU:C:2012:219 (još nije objavljeno u Zborniku sudske prakse).

/68/ C-119/12, Josef Probst protiv mr.nexnet GmbH, ECLI:EU:C:2012:748 (još nije objavljeno u Zborniku sudske prakse).

/69/ Spojeni predmeti C-293/12 i C-594/12 Digital Rights Ireland i Seitlinger i dr., ECLI:EU:C:2014:238 (još nije objavljeno u Zborniku sudske prakse).

/70/ Predmet C-113/12 Google Spain SL, Google Inc. protiv Agencia Española de Protección de Datos (AEPD), Mario Costeja González, ECLI:EU:C:2014:317 (presuda još nije objavljena u Zborniku sudske prakse).

/71/ Za relevantne studije vidi npr.: Korff Douwe, EC study on implementation of data protection directive - Study Contract ETD/2001/B5-3001/A/49, Comparative summary of national laws, University of Essex: Colchester – Cambridge, 2002., dostupno na: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/univ essex-comparativestudy_en.pdf; Korff Douwe, LRDP KANTOR Ltd (Leader) - Centre for Public Reform, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments - Contract No. JLS/2008/C4/011 – 30-CE-0219363/00-28, Working paper No. 2: Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, 20. 1. 2010., dostupno na: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_ report_working_paper_2_en.pdf; LRDP KANTOR Ltd (Leader) - Centre for Public Reform, Comparative study of different approaches to new privacy challenges, in particular in the light of technological developments, Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28, Final Report, 20. 1. 2010., dostupno na: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf (zadnji pristup 08. 5. 2014.); European Commission, Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, SEC(2012) 72 final, Brisel, 25. 1. 2012.; Annex 2 Evaluation of the implementation of the Data Protection Directive.

/72/ Ugovor iz Lisabona o izmjenama i dopunama Ugovora o Europskoj uniji i Ugovora o osnivanju Europske zajednice - Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, SL C 306, 17. 12. 2007., str. 1-271.

/73/ Povelja temeljnih prava Europske unije, SL C 326, 26. 10. 2012., str. 391.

/74/ Pročišćena inačica Ugovora o funkcioniranju Europske unije, SL C 326, 26. 10. 2012., str. 47. Vidi i izjave uz Lisabonski ugovor (SL C 326, 26. 10. 2012., str. 337) i to: a) Izjavu 21 o tome da nova pravna osnova (čl. 16. UFEU-a) ne isključuje mogućnost uspostave pravila o zaštiti podataka u specifičnim područjima pravosudne suradnje u kaznenim stvarima i policijske suradnje; b) Izjavu 20 o potrebi uzimanja u obzir značajki posljedica novih pravila o zaštiti podataka prema čl. 16. UFEU-a, za nacionalnu sigurnost.

/75/ Europska komisija, Prijedlog Uredbe Europskog parlamenta i Vijeća o zaštiti pojedinaca pri obradi osobnih podataka i o slobodnom kretanju takvih podataka (Uredba o općoj zaštiti osobnih podataka), COM (2012) 11 final, 2012/0011 (COD), Brisel, 25. 1. 2012.

/76/ COM/2012/010 final, 2012/0010 (COD), 25. 1. 2012. (za pravnu osnovu vidi čl. 16. st. 2. UFEU-a). Vidi i Zakonodavnu rezoluciju Europskog parlamenta od 12. 3. 2014. o prijedlogu Direktive Europskog parlamenta i Vijeća o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija te slobodnom kretanju takvih podataka, P7_TA(2014)0219, Strasbourg, 12. 3. 2014.

/77/ Zakonodavna rezolucija Europskog parlamenta od 12. 3. 2014. o prijedlogu Uredbe Europskog parlamenta i Vijeća o zaštiti pojedinaca pri obradi osobnih podataka i o slobodnom kretanju takvih podataka (Uredba o općoj zaštiti osobnih podataka), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), P7_TA(2014)0212, Strasbourg, 12. 3. 2014.

/78/ Detaljnije vidi na: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp; http://www.coe.int/t/dghl/standard setting/dataprotection/Cahdata_en.asp. Za autoričinu detaljniju analizu aktivnosti Vijeća Europe u području zaštite osobnih podataka, s posebnim naglaskom na analizi prijedloga za modernizaciju Konvencije 108 prema zadnje ažuriranom tekstu od studenog 2012., uz ocjenu odnosa s prijedlogom novog općeg okvira EU-a, vidi: Gumzej Nina, The Council of Europe and the right to personal data protection: embracing postmodernity, Conference of the International Journal of Arts & Sciences Proceedings, UniversityPublications.net, 6, 2013., 2, str. 13-33 (članak je moguće dostaviti e-poštom na zahtjev autorici na: nina.gumzej@pravo.hr).

/79/ Za detaljniju autoričinu analizu izvornog prijedloga Europske komisije, osobito odredbi u kojima se očituje postrožena pravna odgovornost za obradu osobnih podataka uz naglasak na potrebu što skorije provedbe mjera i postupaka radi preventivnog usklađenja s propisima o zaštiti osobnih podataka, vidi: Gumzej Nina, Data Protection for the Digital Age: Comprehensive Effects of the Evolving Law of Accountability, Juridical Tribune, Editura ASE, Bukurešt, 2, 2012., 2, str. 82-108, dostupno na: http://www.tribunajuridica.eu/arhiva/An2v2/ art7.pdf (zadnji pristup 08.5.2014.)

/80/ Za detaljniju autoričinu analizu izvora prava, uklj. prakse Suda pravde EU-a o neovisnosti nadzornih tijela s težištem na novostima iz prijedloga Uredbe ZOP (zaključno s usvojenim amandmanima Odbora za građanske slobode, pravosuđe i

unutarnje poslove Europskog parlamenta od listopada 2013. g.) kao i za usporedni kritički pregled rješenja u domaćem okviru (ZZOP), vidi: Gumzej Nina, Selected Aspects of Proposed New EU General Data Protection Legal Framework and the Croatian Perspective, Juridical Tribune, Editura ASE, Bukurešt, 3, 2013., 2, dostupno na: http://www.tribunajuridica.eu/arhiva/An3v2 /13%20Gumzej%20.pdf (zadnji pristup 08.5.2014.).

/81/ C-518/07 Europska komisija protiv Savezne Republike Njemačke, Zbornik sudske prakse 2010 I-01885 (ECLI:EU:C:2010:125); C-614/10 Europska komisija protiv Austrije, ECLI:EU:C:2012:631 (nije još objavljeno u Zborniku sudske prakse); C-288/12 Europska komisija protiv Mađarske, ECLI:EU:C:2014:237 (nije još objavljeno u Zborniku sudske prakse).

/82/ „Tijekom više od dva desetljeća davao sam konzultantske usluge i savjetovao mnoge političare, političke stranke i politička tijela. Ali nikada nisam doživio toliki interes za razumijevanje IKT-a kao onda kada sam bio sudski vještak pri njemačkom Saveznom ustavnom sudu. Suci ovog suda stvarno su željeli razumjeti IKT zapanjujuće duboko. Oni su doista pročitali radove koje sam za njih pisao - pa i više: čitali su i razumjeli čak i radove koje sam im preporučio. Za mene kao računalnog stručnjaka bio je jedinstveni doživljaj slušati uvodne izjave suda, u kojima je više od 5 minuta posvećeno temeljnim pitanjima IKT-a, te imati snažan osjećaj da ih ni sam nisam mogao jasnije predstaviti. To je u potpunoj suprotnosti sa slušanjem vodećih njemačkih političara, koji ako ne govore o IKT-u u prvoj rečenici, tada u drugoj rečenici otkrivaju ozbiljno nerazumijevanje temeljnih svojstava IKT-a. Na ročištu su suci saslušali sve argumente i pobrinuli se da ih razumiju. Dodatno, suci su se pobrinuli da vještaci u njihovoj prisutnosti raspravljaju o svojim argumentima jedni s drugima (i ponekad su suci moderirali ili čak od njih zahtijevali da se drže biti stvari). To je nešto što njemački parlamentarni sustav izbjegava gdje god je moguće. Sveukupno, po načinu na koji su suci pripremili i organizirali ročište, oni su se pobrinuli za to da budu u mogućnosti stvoriti valjano vlastito mišljenje uzimajući u obzir i temeljna svojstva IKT-a i interese svih uključenih strana.“ Neslužbeni prijevod s engleskog jezika. Hornung Gerrit; Bendrath Ralf; Pfitzmann Andreas, Surveillance in Germany: Strategies and Counterstrategies, Gutwirth Serge; Poullet Yves; De Hert Paul (ur.), Data Protection in a Profiled World, Springer, Dordrecht, 2010., str. 146-147.

/83/ Vidi, na primjer: BVerfG, 2 BvR 1345/03 od 22. 8. 2006., točke br. (1 - 85), točka 84, dostupno na: http://www.bverfg.de/entscheidungen/rk20060822_2bvr134503.html (zadnji pristup 08. 5. 2014.).