OEBS-ov VODIČ ZA OBUKU
PRAKTIČARA IZ KRIVIČNOPRAVNIH ORGANA

Obezbeđivanje poštovanja ljudskih prava u istragama visokotehnološkog kriminala

oebs Organizacija za evropsku bezbednost i saradnju

Beč, oktobar 2023.

978-92-9271-245-7

Objavljuje Sekretarijat OEBS-a
Odeljenje za transnacionalne pretnje
Jedinica za strateška pitanja policije

Wallnerstrasse 6
1010 Beč, Austrija
Tel: +43-1 514 36 180
Faks: +43-1 514 36 105
email: info@osce.org | spmu@osce.org

www.osce.org

OEBS-ov VODIČ ZA OBUKU
PRAKTIČARA IZ KRIVIČNOPRAVNIH ORGANA

Obezbeđivanje poštovanja ljudskih prava u istragama visokotehnološkog kriminala

Organizacija za evropsku bezbednost i saradnju

IZRAZI ZAHVALNOSTI

Ovaj vodič za obuku je pripremila Jedinica za strateška pitanja policije (eng. *SPMU*) Odeljenja za transnacionalne pretnje Sekretarijata OEBS-a (eng. TNTD), uz doprinos Kancelarije OEBS-a za demokratske institucije i ljudska prava (eng. *ODIHR*). Ova jedinica želi da se zahvali gospodinu Robertu Golobineku i gospodinu Hejnu Drisu na doprinosu koji su dali izradi ovog vodiča. Vodič je izrađen u okviru vanbudžetskog projekta OEBS-a "Izgradnja kapaciteta za borbu protiv visokotehnološkog kriminala u centralnoj Aziji" koga finansiraju Sjedinjene Američke Države, Nemačka i Republika Koreja.

SADRŽAJ

SKRAĆENICE

SPEU	Sud pravde Evropske unije
SE	Savet Evrope
KEBS	Konferencija za evropsku bezbednost i saradnju
EKLJP	Evropska konvencija o ljudskim pravima
ESLJP	Evropski sud za ljudska prava
EU	Evropska unija
FATF	Radna grupa za finansijsku akciju
GPS	Globalni pozicioni sistem
ICCPR	Međunarodni pakt o građanskim i političkim pravima
IP adresa	Adresa internet protokola
ISP	Pružalac internet usluga
NVO	Nevladina organizacija
ODIHR	Kancelarija (OEBS-a) za demokratske institucije i ljudska prava
OHCHR	Kancelarija Visokog predstavnika Ujedinjenih nacija za ljudska prava
OEBS	Organizacija za evropsku bezbednost i saradnju
UDLJP	Univerzalna deklaracija o ljudskim pravima
UN	Ujedinjene nacije
UNODC	Kancelarija Ujedinjenih nacija za borbu protiv droge i kriminala
VPN	Virtuelna privatna mreža

OKVIRI SA INFORMACIJAMA

1

Uvod

Naša društva se sve više oslanjaju na digitalne tehnologije u svim aspektima života, od poslovanja, nauke i obrazovanja, do komunikacija, putovanja, rekreacije i zabave. Usled brzog razvoja ovih tehnologija poslednjih godina, ukazale su se mnoge prilike, ali je došlo i do novih bezbednosnih rizika i izazova. Oblast na koju su ovi događaji značajno uticali je kriminal.

Digitalne tehnologije su preobrazile kriminalno okruženje. Dovele su do novih oblika kriminala (npr. kriminala koji zavisi od visokih tehnologija kao što je ucenjivački softver (eng. *ransomware*), kao i fišing (eng. *phishing*) i kriptodžeking (eng. *cryptojacking*) i promenile način izvršenja postojećih oblika krivičnih dela (npr. krivična dela čije izvršenje omogućava internet, kao što je seksualna eksploatacija putem interneta ili trgovanje nedozvoljenom robom i uslugama na internetu). Mnoge digitalne tehnologije su, takođe, postale korisna sredstva za tradicionalna krivična dela u fizičkom svetu (npr. provalne krađe, krađe i prevare). Pored toga, zbog raširene upotrebe digitalnih uređaja (lični računari, laptopovi, tableti, mobilni telefoni, pametni satovi, itd.), elektronski dokazi sada igraju važnu ulogu u gotovo svim vrstama krivičnih istraga.

Visokotehnološki kriminal ima neke posebne karakteristike zbog kojih se istrage tih krivičnih dela razlikuju od istraga drugih krivičnih dela. Konkretno, učinilac ne mora da bude fizički prisutan na mestu izvršenja ili u blizini žrtve, a može se nalaziti i u inostranstvu. Pored toga, internet pruža velike mogućnosti kriminalcima da sakriju svoj identitet iza nadimaka i ukradenih akreditiva, a različiti alati za šifrovanje ili anonimizaciju mogu se koristiti za prikrivanje kriminalnih aktivnosti. Kriptovalute omogućavaju korisnicima da vrše bezbedna plaćanja bez direktne veze sa njihovim identitetom iz stvarnog sveta, što olakšava kupovinu zabranjene robe i usluga i pranje imovine stečene izvršenjem krivičnog dela.

Identifikacija, oduzimanje i analiza elektronskih dokaza o visokotehnološkom ili drugom kriminalu takođe se umnogome razlikuju od postupanja sa fizičkim dokazima. Relevantni elektronski dokazi se možda ne čuvaju na nekom ličnom uređaju, već na serverima na klaudu pod kontrolom privatnih kompanija koje se često nalaze u inostranstvu. Pored toga, elektronski podaci su nepostojani i mogu se lako premestiti, izmeniti ili obrisati.

Visokotehnološki kriminal[1] i elektronski dokazi zato predstavljaju značajne izazove za krivičnopravne sisteme i vladavinu prava u čitavom regionu OEBS-a. Istrage visokotehnološkog kriminala i elektronski dokazi zahtevaju posebna znanja i veštine, adekvatna tehnička sredstva i zakonodavne okvire, kao i efikasnu i delotvornu međunarodnu saradnju sa stranim krivičnopravnim akterima i privatnim subjektima. Države su se prilagođavale ovom razvoju događaja tako što su menjale svoje zakone, gradile tehničke kapacitete i uvodile nova procesna ovlašćenja u istragama. Sve ove mere i alati moraju biti razvijeni i raspoređeni u skladu sa odgovornostima država na osnovu međunarodnog prava ljudskih prava.

Kao i sve druge krivične istrage, i istrage visokotehnološkog kriminala i korišćenje posebnih procesnih ovlašćenja utiču na ljudska prava i slobode utvrđene međunarodnim instrumentima na globalnom i regionalnom nivou. Ti instrumenti uključuju Univerzalnu deklaraciju o ljudskim pravima (UDLJP), Međunarodni pakt o građanskim i političkim pravima (ICCPR) i Evropsku konvenciju o ljudskim pravima (EKLJP).

Napomena: Svim elektronskim izvorima je pristupljeno 1. juna 2023.

1 U ovom tekstu, termin "visokotehnološki kriminal" se koristi kao krovni termin koji se odnosi i na krivična dela koja zavise od visoke tehnologije i ona koja omogućava visoka tehnologija, osim ako nije drugačije navedeno.

Iako se ova prava i slobode moraju poštovati i štititi u svakoj krivičnoj istrazi, ova potreba je možda još izraženija u kontekstu visokotehnološkog kriminala i elektronskih dokaza. Podaci koje digitalni uređaji i internet servisi prikupljaju o svojim korisnicima su dosad nezabeleženi u pogledu područja primene i obima. Ovi podaci mogu da sadrže mnoge lične detalje o životima ljudi, uključujući i one o njihovom zdravlju, privrednoj aktivnosti, privatnim odnosima i političkim afinitetima. Prilikom prikupljanja elektronskih dokaza tokom istrage, praktičari iz krivičnopravnih organa često pronalaze relevantne dokaze zajedno sa velikom količinom drugih, često ličnih, podataka. Ova vrsta istraga zato potencijalno mnogo više narušava privatnost od tradicionalnih istraga izvan interneta u okviru kojih se prikupljaju samo fizički dokazi.

Svest o posledicama istraga visokotehnološkog kriminala i drugih istraga koje uključuju elektronske dokaze na ljudska prava je zato važna za policijske istražitelje, tužioce i sudije. Kršenje ljudskih prava tokom krivičnih istraga i postupaka može dovesti do neosnovanih osuda ili do odbacivanja dokaza, što rezultira oslobađanjem učinioca. Nepoštovanje ljudskih prava takođe narušava poverenje na nacionalnom i međunarodnom nivou. To je prepreka međunarodnoj saradnji, kako sa organima za sprovođenje zakona i drugim organima u partnerskim zemljama, tako i sa privatnim kompanijama u inostranstvu. Štaviše, poštovanje i zaštita ljudskih prava u praksi pomaže da se ojača poverenje između krivičnopravnih organa i šireg društva, i na taj način podstiče pojedince da sarađuju sa – i daju važne informacije – istražiteljima visokotehnološkog kriminala. Zauzimanje pristupa zasnovanog na ljudskim pravima stoga povećava efikasnost istraga visokotehnološkog kriminala.

Cilj ovog vodiča je da podigne svest praktičara iz krivičnopravnih organa o posledicama koje istrage visokotehnološkog kriminala i drugih krivičnih dela koja uključuju elektronske dokaze mogu imati na ljudska prava, i da ih podrži u poštovanju ljudskih prava prilikom svakodnevnog rada na istragama. On to čini tako što se usredsređuje na ona ljudska prava na koja posebno utiču istrage visokotehnoloških i drugih krivičnih dela koja uključuju elektronske dokaze, a to su:

- pravo na privatnost;
- pravo na pravično suđenje;
- pravo na slobodu izražavanja/govora;
- pravo na zaštitu imovine.

Da bi objasnio i ilustrovao kako se ljudska prava primenjuju u kontekstu istraga visokotehnološkog kriminala i prikupljanja i korišćenja elektronskih dokaza, ovaj vodič se oslanja na sudsku praksu Evropskog suda za ljudska prava (ESLJP) i, povremeno, Suda pravde Evropske unije (SPEU).

8

2

Pravni okvir ljudskih prava koji se primenjuje na istrage visokotehnološkog kriminala

2.1 ŠTA SU LJUDSKA PRAVA?

Ljudska prava su zakonska prava fizičkih lica na zaštitu dostojanstva i sloboda. Ljudska prava su svojstvena svim ljudskim bićima, bez razlike u pogledu rase, boje kože, roda, jezika, veroispovesti, političkog ili drugog opredeljenja, nacionalnog ili socijalnog porekla, imovine, rođenja ili bilo kog drugog statusa. Bilo da su građanska i politička (kao što je pravo na život, jednakost pred zakonom i sloboda izražavanja); ekonomska, socijalna i kulturna (kao što je pravo na rad, socijalno osiguranje i obrazovanje); ili kolektivna (kao što je pravo na razvoj i samoopredeljenje), sva ljudska prava su nedeljiva, međusobno povezana i međuzavisna. Poboljšanje jednog olakšava unapređenje drugih prava.

Univerzalna ljudska prava su izražena i garantovana zakonom u obliku ugovora, međunarodnog običajnog prava, opštih načela i drugih izvora međunarodnog prava. Međunarodno pravo ljudskih prava nameće posebne obaveze državama, uključujući parlamente, ministarstva, lokalne vlasti, organe za sprovođenje zakona i krivičnopravne organe, kao „nosioce dužnosti“ koji su odgovorni za poštovanje, zaštitu i sprovođenje ljudskih prava. To uključuje i takozvane „negativne“ obaveze uzdržavanja od određenih radnji (npr. od nezakonitog mešanja u privatni život nekog lica), kao i odgovornost za preduzimanje „pozitivnih“ radnji za zaštitu prava nekog lica (npr. kroz delotvornu istragu i procesuiranje krivičnih dela) i promovisanje ljudskih prava i osnovnih sloboda (npr. pružanjem javnih informacija i obukom za relevantne državne službenike).

2.2 MEĐUNARODNI PRAVNI INSTRUMENTI I TELA ZA LJUDSKA PRAVA

Države su posle Drugog svetskog rata prepoznale značaj zaštite ljudskih prava osnivanjem Ujedinjenih nacija (UN) i Saveta Evrope (SE) i izradom međunarodnih instrumenata o ljudskim pravima u okviru ovih organizacija. Evropska unija (EU) je takođe istakla važnost ljudskih prava usvajanjem posebne povelje o ljudskim pravima. U okviru 1 su predstavljeni međunarodni pravni instrumenti za ljudska prava koji su posebno relevantni za kontekst visokotehnološkog kriminala.

OKVIR 1 MEĐUNARODNI PRAVNI INSTRUMENTI ZA LJUDSKA PRAVA KOJI SU NAROČITO RELEVANTNI ZA ISTRAGE VISOKOTEHNOLOŠKOG KRIMINALA

- Univerzalna deklaracija UN o ljudskim pravima iz 1948. godine[2] (UDLJP) (a naročito čl. 8-11, 12 i 19);
- Međunarodni pakt o građanskim i političkim pravima UN iz 1966[3] (ICCPR) (a naročito čl. 14, 17 i 19);
- Evropska konvencija SE o ljudskim pravima iz 1950[4] (EKLJP) (a naročito čl. 6, 8 i 10);
- Povelja Evropske unije o osnovnim pravima[5] iz 2000.

U prilogu 1 se nalazi kompletan tekst pomenutih članova ICCPR i EKLJP.

Izuzev Svete stolice, sve države učesnice OEBS-a su ratifikovale ICCPR i zato ih obavezuju njene odredbe. Većina država učesnica OEBS-a su i članice SE, a samim tim i potpisnice EKLJP. Neke države učesnice OEBS-a su i članice EU i zato ih prilikom sprovođenja prava EU obavezuje Povelja Evropske unije o osnovnim pravima (član 51 stav 1 povelje).

Postoji izvestan broj institucija za ljudska prava koje imaju mandat za tumačenje i unapređenje ljudskih prava sadržanih u ovim pravnim tekstovima. Na nivou UN-a, Komitet za ljudska prava je ugovorno telo ICCPR-a. Sastoji se od 18 nezavisnih eksperata koji prate kako države potpisnice primenjuju ICCPR.[6] On razmatra primenu pakta kroz periodične izveštaje i može da ispita pojedinačne žalbe u vezi sa navodnim kršenjem ICCPR od strane država koje su pristupile Fakultativnom protokolu uz pakt.[7]

Na regionalnom nivou, Evropski sud za ljudska prava (ESLJP) donosi presude o predstavkama koje podnose fizička lica, grupe fizičkih lica ili jedna ili više država članica SE, u kojima se navode kršenja prava iz EKLJP. Iako su presude ESLJP pravno obavezujuće za države članice SE o kojima se radi, njegova sudska praksa takođe može da obezbedi važne smernice drugim zemljama u pogledu obima i primene građanskih i političkih prava. Sud pravde Evropske unije (SPEU) tumači pravo EU, uključujući i Povelju Evropske unije o osnovnim pravima.[8] INjegove presude su pravno obavezujuće za države članice EU.

Druga tela imaju savetodavni mandat za jačanje unapređenja i zaštite ljudskih prava. Na međunarodnom nivou, ona uključuju Savet UN za ljudska prava[9] i različite posebne funkcije uspostavljene

2 Univerzalna deklaracija UN o ljudskim pravima, 10. decembar 1948, Rezolucija 217 A (III) Generalne skupštine UN.

3 Međunarodni pakt o građanskim i političkim pravima, 16. decembar 1966, Rezolucija 2200A (XXI) Generalne skupštine UN, stupio na snagu 23. marta 1976.

4 *Konvencija za zaštitu ljudskih prava i osnovnih sloboda, 4. novembar 1950, CETS br. 5, stupila na snagu 3. septembra 1953.*

5 Povelja Evropske unije o osnovnim pravima, 18. decembar 2000, OJEC 2012/C 326/02, stupila na snagu 1. decembra 2009.

6 OHCHR (bez datuma), Komitet za ljudska prava, dostupno na https://www.ohchr.org/en/treaty-bodies/ccpr.

7 Fakultativni protokol uz Međunarodni pakt o građanskim i političkim pravima, 16. decembar 1966, Rezolucija 2200A (XXI) Generalne skupštine UN, stupio na snagu 23. marta 1976.

8 Protokol 3 o Statutu Suda pravde Evropske unije, 16. decembar 2004, SL EU C 310/210.

9 Savet UN za ljudska prava, 15. mart 2006, Rezolucija 60/251 Generalne skupštine UN, kojom se zamenjuje Komisija UN za ljudska prava od 16. juna 2006.

u okviru njega, uključujući specijalne izvestioce, specijalne predstavnike, nezavisne eksperte i radne grupe.[10] Pored toga, Kancelarija visokog komesara UN za ljudska prava (OHCHR) unapređuje i štiti sva ljudska prava kroz istraživanje, obrazovanje, zagovaranje i pomoć vladama.

Poštovanje ljudskih prava i osnovnih sloboda je ključno i za sveobuhvatni koncept bezbednosti OEBS-a. Od potpisivanja Završnog akta iz Helsinkija 1975. godine, Konferencija za evropsku bezbednost i saradnju (KEBS), kasnije OEBS, je prikupila značajan korpus obaveza u oblasti ljudskih prava, demokratije, vladavine prava i nacionalnih manjina koje su usvojili različiti organi odlučivanja KEBS-a, a kasnije i OEBS-a.[11] Mnoge od ovih obaveza su relevantne za rad krivičnopravnih institucija, između ostalog i u kontekstu istraga i procesuiranja visokotehnološkog kriminala i drugih krivičnih dela koja uključuju elektronske dokaze. Iako, prema međunarodnom pravu, obaveze preuzete u okviru OEBS-a nemaju karakter pravno obavezujućih ugovora, one predstavljaju važne političke obaveze koje su konsenzusom usvojile sve države učesnice.

2.3 NACIONALNO ZAKONODAVSTVO I INSTITUCIJE ZA LJUDSKA PRAVA

Da bi bili delotvorni, međunarodni standardi ljudskih prava moraju biti sprovedeni i zaštićeni nacionalnim zakonodavstvom, politikom i praksom. Zakonodavci su prvenstveno oni čiji je zadatak da obezbede da nacionalni zakonodavni okvir odražava i uključuje međunarodne standarde ljudskih prava. Zaštita ljudskih prava je, po pravilu, sastavni deo ustava i drugih međusektorskih propisa ili propisa za konkretne sektore. Procesna prava su uglavnom ugrađena u zakone o krivičnom postupku kroz različite uslove i zaštitne mere.

Nacionalno zakonodavstvo o ljudskim pravima tumače nacionalni sudovi, uključujući – kada su u pitanju ustavne odredbe – ustavne sudove. Korpus domaće sudske prakse pruža važne smernice o tome kako domaće zakonodavstvo o ljudskim pravima treba primenjivati u praksi.

Nacionalna tela za ljudska prava (kao što su nacionalne institucije za ljudska prava ili zaštitnici građana) takođe imaju važnu funkciju u zaštiti ljudskih prava na nacionalnom nivou tako što daju savete i postupaju u pojedinačnim slučajevima kršenja. Pored toga, civilno društvo, uključujući nevladine organizacije (NVO) i medije, igra ključnu ulogu u podizanju svesti o ljudskim pravima, zagovaranju javnih interesa i promovisanju javnog nadzora poštovanja ljudskih prava.

10 Savet UN za ljudska prava (bez datuma), Posebni postupci Saveta za ljudska prava, dostupno na https://www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx.

11 Radi sveobuhvatnog pregleda, vidi Obaveze iz ljudske dimenzije OEBS/ODIHR: Tom 1 – Tematska kompilacija, 4. izdanje (Varšava, 2023); i OEBS/ODIHR, Obaveze iz ljudske dimenzije OEBS-a: Tom 2 – Hronološka kompilacija, 4. izdanje (Varšava, 2023).

3

Ljudska prava i istrage visokotehnološkog kriminala

3.1 ZAŠTO SU LJUDSKA PRAVA VAŽNA U KONTEKSTU ISTRAGA VISOKOTEHNOLOŠKOG KRIMINALA

Državni akteri, uključujući ministarstva i praktičare iz krivičnog pravosuđa, imaju prvenstvenu odgovornost da poštuju, štite i obezbede sprovođenje ljudskih prava. To uključuje obezbeđivanje praktičnog sprovođenja standarda ljudskih prava iz međunarodnih konvencija koje je država potpisala.. Obaveze država se primenjuju na sve aspekte krivičnopravnog reagovanja pravosuđa na visokotehnološki kriminal. To uključuje obezbeđivanje da domaće zakonodavstvo poštuje ljudska prava i da sadrži potrebne procesne garancije, što praktičare čini svesnim njihove odgovornosti za poštovanje ljudskih prava, praćenje njihovog sprovođenja u praksi i pružanje mogućnosti pojedincima da traže pomoć kada se njihova ljudska prava prekrše.

Pored toga što poštovanje ljudskih prava predstavlja odgovornost na osnovu međunarodnog prava, istrage visokotehnološkog kriminala i rad krivičnopravnih organa uopšte od njega imaju i jasne praktične koristi, kao što pokazuju sledeći primeri.

Prvo, poštovanje ljudskih prava je važno za obezbeđivanje neophodnih dokaza iz inostranstva i omogućavanje međunarodne saradnje kako između samih krivičnopravnih organa, tako i između krivičnopravnih organa i privatnih kompanija. Nepoštovanje standarda ljudskih prava može, na primer, biti razlog za odbijanje zahteva za međunarodnu pravnu pomoć. Za mnoge države, preduslov za zvanično pružanje pomoći je da država molilja garantuje pravično suđenje i da poštuje ljudska prava utvrđena međunarodnim i regionalnim instrumentima o ljudskim pravima. Privatne kompanije, uključujući velike provajdere kao što su Majkrosoft, Gugl ili Meta, takođe razmatraju stanje ljudskih prava u državi kada odlučuju o tome kako će odgovoriti na zahtev za čuvanje podataka ili njihovo deljenje za potrebe krivične istrage.[12]

Drugo, nepoštovanje ljudskih prava i procesnih garancija prilikom sprovođenja istrage može da dovede do toga da sud oceni dokaze kao nezakonite. Ovo je posebno relevantno u istragama visokotehnološkog kriminala, koje mogu da uključuju dokazne radnje koje narušavaju privatnost i oslanjaju se na nestabilne elektronske dokaze. Obezbeđivanje primene standarda ljudskih prava tokom cele istrage zato povećava verovatnoću da će doći do uspešne osude učinilaca.

Treće, krivičnopravni organi koji ne sprovode istrage visokotehnološkog kriminala u skladu sa standardima ljudskih prava mogu se naći u fokusu žalbenog postupka ili tužbe. Pojedinačni policijski službenici i rukovodioci, na primer, mogu se suočiti sa upravnim ili krivičnim sankcijama ako učestvuju u istragama za koje se utvrdi da su nezakonito vođene. To može da ima štetan uticaj na moral i ugled tih organa, kao i na verovatnoću da će učinioci krivičnih dela iz oblasti visokotehnološkog kriminala biti osuđeni.

Konačno, kršenja ljudskih prava tokom istraga visokotehnološkog kriminala mogu da dovedu do gubitka poverenja javnosti u krivičnopravne organe, što otežava postizanje saradnje koja je neophodna za efikasnu borbu protiv visokotehnološkog kriminala. Pored toga što podriva akcije usmerene na sprečavanje visokotehnološkog kriminala, nepoverenje može i da ima negativan uticaj na spremnost pripadnika javnosti da prijavljuju takva krivična dela ili da daju izjave u svojstvu svedoka. Poštovanje i zaštita ljudskih prava u kontekstu istraga visokotehnološkog kriminala je stoga

12 Vidi, npr., UNODC, Praktični vodič za zahteve za elektronske dokaze preko granica (Beč, 2021), str. 18, 37.

od ključnog značaja da bi se obezbedilo da napori u borbi protiv visokotehnološkog kriminala budu održivi, efikasni, a najzad i uspešni.

3.2 LJUDSKA PRAVA NA KOJA NAROČITO UTIČU ISTRAGE VISOKOTEHNOLOŠKOG KRIMINALA

Istrage visokotehnološkog kriminala mogu da utiču na uživanje brojnih ljudskih prava. Sledeća ljudska prava su posebno relevantna u kontekstu istraga visokotehnološkog kriminala:

- pravo na privatnost;
- pravo na pravično suđenje;
- pravo na slobodu izražavanja/govora;
- pravo na zaštitu imovine.

Kompletan tekst članova ICCPR-a i EKLJP u kojima se navode ova prava možete naći u prilogu 1.

Ostala prava na koja istrage visokotehnološkog kriminala mogu da direktno ili indirektno utiču uključuju: zabranu diskriminacije, slobodu veroispovesti ili uverenja, slobodu udruživanja, pravo na slobodu i prava deteta.

PRAVO NA PRIVATNOST

Pravo na privatnost je utvrđeno u članu 17 ICCPR i članu 8 EKLJP, gde se pominje kao pravo na poštovanje privatnog i porodičnog života. Pored obaveza na osnovu ovih instrumenata, države učesnice OEBS-a su se u Dokumentu iz Moskve 1991 godine obavezale na pravo na zaštitu privatnog i porodičnog života, prebivališta, prepiske i elektronskih komunikacija, kao i na sprečavanje neosnovanog upada u individualni prostor.[13]

Pravo na privatnost ima ključnu važnost u demokratskom društvu. Ono uključuje zaštitu privatnosti poruka, telefonskih poziva i elektronske pošte, kao i zaštitu od nezakonitog i nepotrebnog državnog nadzora. Da bi sprovele pravo na privatnost, države imaju kako pozitivnu (da štite ovo pravo), tako i negativnu obavezu (da se uzdrže od mešanja u ovo pravo). Pravo na privatnost takođe omogućava pojedincima da preduzimaju mere za zaštitu svog privatnog života, na primer tako što će koristiti tehnologije za povećanje privatnosti kao što su šifrovanje i virtuelne privatne mreže (VPN).

Važnost prava na privatnost leži u tome što se ono opisuje kao „pravo koje vodi ka drugim pravima“. Bez privatnosti, ugroženo je puno uživanje širokog spektra drugih prava, na primer, prava na izražavanje sopstvenog mišljenja, udruživanja sa drugima ili slobodnog učešća u javnom i političkom životu.[14]

13 OEBS/KEBS, Dokument iz Moskve iz 1991. godine, 3. oktobar 1991, KEBS/CHDM.49/Rev.1, st. 24; OEBS/KEBS, Dokument iz Kopenhagena iz 1990. godine, 27. jun 1990, KEBS/CHDC.43, st. 26, napomena 16.

14 OHCHR (2018), Univerzalna deklaracija o ljudskim pravima na 70: 30 članova na 30 članova - član 12, dostupno na: https://www.ohchr.org/en/press-releases/2018/11/universal-declaration-human-rights-70-30-articles-30-articles-article-12.

Zaštita podataka je važan deo prava na privatnost, što priznaju Komitet UN za ljudska prava[15] i ESLJP.[16] Izvestan broj međunarodnih i regionalnih instrumenata sadrži konkretna načela zaštite podataka koja treba poštovati kako bi se obezbedila puna usaglašenost sa pravom na privatnost.[17] Oni, na primer, uključuju načela prema kojima lični podaci koji se automatski obrađuju moraju biti:

- dobijeni i obrađeni na pravičan i zakonit način;
- čuvani za konkretno navedene i legitimne svrhe (ograničenje svrhe);
- adekvatni, relevantni i ne preterani (minimizacija podataka);
- čuvani ne duže nego što je neophodno (ograničeno zadržavanje podataka);
- zaštićeni od neovlašćenog pristupa.

Kao i kod mnogih prava, pravo na privatnost nije apsolutno i pod određenim okolnostima može biti ograničeno. Svako mešanje u ostvarivanje ovog prava mora biti **zasnovano na zakonu**, **nužno** u demokratskom društvu, kao na primer radi zaštite nacionalne bezbednosti ili javne bezbednosti ili sprečavanja nereda ili krivičnih dela, i **proporcionalno** (vidi i odeljak 3.3). Na primer, nadležni pravosudni organ može da dozvoli policiji da presreće komunikaciju nekog pojedinca ako ima razuman osnov da smatra da se ta osoba sprema da izvrši neko teško krivično delo.

PRAVO NA PRAVIČNO SUĐENJE

Pravo na pravično suđenje je jedan od ključnih elemenata zaštite ljudskih prava i služi kao procesno sredstvo za očuvanje vladavine prava.[18] I član 14 ICCPR-a i član 6 EKLJP postavljaju niz jasnih uslova koji zajedno čine pravo na pravično suđenje, uključujući i to da svako ko je optužen za krivično delo:[19]

- ima pravo na pravičnu i javnu raspravu pred nezavisnim i nepristrasnim sudom;
- smatra se nevinim sve dok se ne dokaže njegova krivica na osnovu zakona;
- treba da ima dovoljno vremena i mogućnosti za pripremu odbrane;
- treba da bude u stanju da se brani lično ili putem branioca koga sam izabere;
- treba da mu se sudi u razumnom roku bez neopravdanog odlaganja.

Pojedini elementi prava na pravično suđenje mogu pod određenim uslovima biti ograničeni. Drugi – kao što su pretpostavka nevinosti, pravo na raspravu pred nadležnim, nezavisnim i nepristrasnim sudom, kao i zahtev da suđenje u celini bude pravično – smatraju se apsolutnim i ne mogu

15 Vidi Komitet UN za ljudska prava, Opšti komentar br. 16 o čl. 17, Pravo na privatnost, 8. april 1988, U.N. Doc. HRI/GEN/1/Rev.1, str. 21-23, st. 10.

16 ESLJP, Vodič kroz član 8 Evropske konvencije o ljudskim pravima: Pravo na poštovanje privatnog i porodičnog života, doma i prepiske (Strazbur, 2022); Vidi i ESLJP (2023), Informativni list o zaštiti podataka o ličnosti, dostupno na https://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

17 Vidi, npr. Konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka, 28. januar 1981, CETS br.108; Povelju EU o osnovnim pravima, član 8 u kombinaciji sa Opštom uredbom EU o zaštiti podataka o ličnosti, 27. april 2016, Reg. (EU) 2016/679 o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i o slobodnom kretanju takvih podataka.

18 Vidi Komitet UN za ljudska prava, *Opšti komentar br. 32 o članu 14: Pravo na ravnopravnost pred sudovima i tribunalima i pravo na pravično suđenje*, 23. avgust 2007, UN Doc. CCPR/C/GC/32, st. 2.

19 ESLJP, *Vodič za član 6 Evropske konvencije za zaštitu ljudskih prava: Pravo na pravično suđenje* (krivični aspekt) (Strazbur, 2022).

se ograničiti ni pod kojim okolnostima.[20]

PRAVO NA SLOBODU IZRAŽAVANJA

Sloboda izražavanja, kako je navedeno u članu 19 ICCPR-a i članu 10 EKLJP, predstavlja jedan od suštinskih temelja demokratskog društva. Ona uključuje pravo na traženje, primanje i saopštavanje informacija i ideja putem bilo kog medija, bez obzira na granice i bez mešanja javnih vlasti. Važno je da se sloboda izražavanja ne odnosi samo na informacije i ideje koje se dobro prihvataju, već i na one koje mogu da uvrede ili uznemire.[21] Države učesnice OEBS-a su ponovo potvrdile da „svako ima pravo na slobodu izražavanja, uključujući i pravo na komunikaciju," i „slobodu da ima mišljenje i da prima i saopštava informacije i ideje bez mešanja javnih vlasti i bez obzira na granice".[22]

U ograničenim okolnostima mogu postojati izuzeci od slobode izražavanja, na primer da bi se zaštitila nacionalna bezbednost ili javni red ili da bi se sprečili neredi ili krivično delo. U sudskoj praksi se naglašava da se ti izuzeci moraju usko tumačiti. Time se izbegava prekomerno mešanje i tzv. odvraćajuće dejstvo (eng. *chilling effect*), gde pojedinci pribegavaju autocenzuri zbog straha od krivičnog postupka (vidi okvir 4).

Internet je otvorio nove mogućnosti za ostvarivanje prava na slobodu izražavanja kroz vrlo široko deljenje informacija dosad nezabeleženom brzinom. Zbog svoje dostupnosti i mogućnosti čuvanja i prenošenja velike količine informacija, internet igra važnu ulogu u omogućavanju boljeg pristupa javnosti vestima i lakšeg širenja informacija.[23] Ove prednosti su, međutim, praćene izvesnim opasnostima, a naročito onom da se nezakoniti govor, uključujući govor mržnje i govor koji podstiče diskriminaciju, neprijateljstvo ili nasilje, može proširiti kroz ceo svet za samo nekoliko sekundi i da često ostaje trajno dostupan na internetu.[24]

Kao i u svetu izvan interneta, države imaju dužnost da obezbede da sva ograničenja izražavanja na internetu budu **propisana zakonom, nužna i proporcionalna**.[25]

PRAVO NA ZAŠTITU IMOVINE

EKLJP navodi da fizička i pravna lica imaju pravo da poseduju imovinu koja je po zakonu njihova. To uključuje fizičke predmete koje neko poseduje, finansijska sredstva, kao što su ulozi u bankama i akcije, kao i intelektualnu svojinu.[26] Imovina obuhvata i virtuelnu imovinu, kao što su kriptovalute.

---

20 Vidi Komitet UN za ljudska prava, Opšti komentar br. 32 o članu 14: Pravo na ravnopravnost pred sudovima i tribunalima i pravo na pravično suđenje, 23. avgust 2007, UN Doc. CCPR/C/GC/32, st. 6, 19.

21 Odeljenje SE za izvršenje presuda Evropskog suda za ljudska prava, *Tematski informativni list: Sloboda izražavanja*,. april 2021, dostupno na https://rm.coe.int/thematic-factsheet-freedom-expression-eng/1680a235d0.

22 KEBS/OEBS, Dokument iz Kopenhagena iz 1990, 27. jun 1990, KEBS/CHDC.43, st. 9.1.

23 Vidi, npr. ESLJP, *Delfi AS protiv Estonije* [GC], 10. oktobar 2013, br. 64569/09, § 133; ESLJP, T*imes Newspapers Ltd (br. 1 i 2) protiv Ujedinjenog Kraljevstva*, 10. mart 2009, br. 3002/03 i 23676/03, § 27..

24 Vidi, npr. ESLJP, *Delfi AS protiv Estonije* [GC], 10. oktobar 2013, br. 64569/09, § 110; ESLJP, *Anen protiv Nemačke*, 20. septembar 2018, br. 3682/10, § 67.

25 OHCHR (bez datuma), Informativni list o slobodi mišljenja i izražavanja, dostupno na https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/Factsheet_1.pdf.

26 Odeljenje SE za izvršenje presuda Evropskog suda za ljudska prava, Tematski informativni list o zaštiti imovine, jun 2022, dostupno na https://rm.coe.int/thematic-factsheet-protection-of-property-eng/1680a6f07f.

Države ne mogu da liše fizička ili pravna lica imovine ako to nije u javnom interesu i ako ne podleže zakonom utvrđenim uslovima.

3.3 NAČELA ZAKONITOSTI, NUŽNOSTI I PROPORCIONALNOSTI

Većina ljudskih prava, uključujući pravo na privatnost i slobodu izražavanja, nije apsolutna i može se ograničiti pod određenim okolnostima. Dobro poznato načelo međunarodnog prava ljudskih prava je da svako takvo ograničenje prava mora biti propisano zakonom, nužno i proporcionalno.

Na osnovu načela **zakonitosti**, svaka mera koja ograničava neko pravo mora da ima osnov u nacionalnom zakonodavstvu. Ovaj zakonski osnov mora da bude dostupan onima na koje takva mera može da utiče i dovoljno jasan da na odgovarajući način obavesti pojedince o okolnostima i uslovima pod kojima organi javne vlasti imaju pravo da pribegnu merama koje utiču na njihova prava. Zakonodavstvo mora da sadrži adekvatne mere za zaštitu od proizvoljne primene i ne sme da omogući prekomerno diskreciono pravo službenicima kojima je poverena njegova primena.

Načelo **nužnosti** se sastoji od dva elementa. Prvo, svako ograničenje prava mora da **teži legitimnom cilju**. Kod nekih prava ovi legitimni ciljevi se bliže određuju. Na primer, EKLJP, između ostalog, dozvoljava ograničavanje prava na poštovanje privatnog i porodičnog života i na slobodu izražavanja u interesu nacionalne bezbednosti, javne bezbednosti ili radi sprečavanja nereda ili krivičnih dela. Drugo, ograničenje mora da bude u okvirima onoga što je **nužno za postizanje tog cilja**. Drugim rečima, ograničenje ne sme da bude preširoko niti da traje duže nego što je neophodno za postizanje cilja, odnosno mora biti usko definisano i ograničenog trajanja.

Načelo **proporcionalnosti** znači da svaka mera koja ugrožava neko pravo mora da bude srazmerna legitimnom cilju kojem se teži. Zbog toga je potrebno pokazati da manje restriktivne mere nisu bile dostupne, da je suština tog prava očuvana i da ograničenje prava nije diskriminatorno. Postojanje i delotvorna primena procesnih garancija predstavlja jedan od ključnih aspekata kod utvrđivanja da li je ograničenje prava srazmerno.

4

Procesna ovlašćenja specifična za visokotehnološki kriminal i mere zaštite ljudskih prava

4.1 SPECIFIČNOSTI ISTRAGA VISOKOTEHNOLOŠKOG KRIMINALA S

Istraživanje i uspešno procesuiranje visokotehnološkog kriminala i drugih krivičnih dela koja uključuju elektronske dokaze stavlja praktičare iz krivičnopravnih organa pred posebne izazove. Prvo, pošto za vršenje krivičnih dela iz oblasti visokotehnološkog kriminala nije neophodno fizičko prisustvo ili blizina žrtve, učinioci i žrtve se mogu nalaziti u različitim nacionalnim jurisdikcijama. Štaviše, može postojati i više učinilaca, a svaki od njih se može nalaziti u drugoj jurisdikciji.

Drugo, kriminalci sve više skrivaju svoje identitete tako što koriste servise kao što su Tor ili virtuelne privatne mreže (VPN), koje im omogućavaju da koriste resurse na internetu uz relativnu anonimnost. Oni takođe koriste različite alate za šifrovanje kako bi obezbedili svoje podatke i komunikaciju i sakrili svoje kriminalne aktivnosti. Operateri mobilnih mreža koriste tehnologije poput prevođenja mrežnih adresa, što otežava identifikaciju korisnika interneta prema adresama internet protokola (IP). Zbog svega navedenog pripisivanje krivičnih dela u internet prostoru postaje sve veći izazov.

Pored toga, većina dokaza krivičnih dela iz oblasti visokotehnološkog kriminala – pa čak i ključnih dokaza mnogih krivičnih dela izvršenih izvan interneta – nalazi se u obliku digitalnih podataka, koji su po svojoj prirodi nestabilni i mogu se lako izmeštati, menjati ili brisati. Takođe, podaci se često čuvaju u „klaudu“, na serverima koji se mogu nalaziti u jednoj ili više stranih jurisdikcija. Različiti privatni pružaoci usluga mogu imati pristup ili kontrolu nad digitalnim tragovima i elektronskim dokazima koji se odnose na krivično delo koje se istražuje.

To znači da istrage visokotehnološkog kriminala često zahtevaju intenzivnu međunarodnu saradnju – kako sa krivičnopravnim akterima iz drugih zemalja, tako i sa privatnim subjektima kao što su multinacionalni pružaoci usluga. Određene vrste visokotehnološkog kriminala, na primer ucenjivački softver (eng. *ransomware*) ili hakovanje poslovne elektronske pošte, takođe zahtevaju kombinaciju finansijskih i digitalnih istraga.

4.2 PROCESNA OVLAŠĆENJA I OVLAŠĆENJA ZA MEĐUNARODNU SARADNJU U POGLEDU VISOKOTEHNOLOŠKOG KRIMINALA

Specifičnosti istraga visokotehnološkog kriminala ili drugih krivičnih dela koja uključuju elektronske dokaze otvaraju niz pitanja kao što su:

- Ko koristi ili je koristio neku konkretnu (statičku ili dinamičku) IP adresu u nekom konkretnom trenutku?
- Ko koristi ili je koristio neku konkretnu adresu elektronske pošte ili nadimak na blogu ili na društvenoj mreži?

- Koji su uslovi da pružaoci usluga zadrže podatke o saobraćaju, uključujući dinamičke IP adrese, i pod kojim uslovima krivičnopravni akteri mogu da dobiju takve podatke?
- Kako dobiti podatke o korisničkom nalogu i/ili podatke o sadržaju od multinacionalnog pružaoca usluga čije je sedište u inostranstvu?
- Kako dobiti pristup, oduzeti i istražiti sadržaj elektronske komunikacije (npr., elektronske pošte ili aplikacije za razmenu poruka) ili podatke sa različitih elektronskih uređaja, uključujući i one koji su šifrovani?
- Kako pratiti šifrovanu komunikaciju (onlajn)?
- Kako otkriti i pratiti onlajn bogatstvo, transfere elektronskog novca i transakcije kriptovaluta?
- Kako oduzeti kriptovalute ili drugu virtuelnu imovinu?

Iako istrage visokotehnološkog kriminala slede ista procesna pravila kao i sve druge krivične istrage, u skladu sa relevantnim nacionalnim zakonodavstvom, odgovori na ova pitanja mogu, dodatno, zahtevati da istražitelji imaju pristup određenim procesnim ovlašćenjima.

Konvencija SE o visokotehnološkom kriminalu iz 2001. godine, poznata i kao Budimpeštanska konvencija, prvi je međunarodni ugovor o krivičnim delima izvršenim putem interneta i drugih računarskih mreža.[27] Otvorena je za ratifikaciju/pristup i državama koje nisu članice SE, a ratifikovao ju je veliki broj država u različitim regionima, uključujući i većinu država učesnica OEBS-a. Konvencija predviđa posebna ovlašćenja relevantna za prikupljanje i korišćenje elektronskih dokaza, kao i za međunarodnu saradnju u kontekstu istraga visokotehnološkog kriminala. Ova ovlašćenja se primenjuju kako na krivična dela koja zavise od visokih tehnologija, tako i na krivična dela koja omogućavaju visoke tehnologije, kao i na sva druga krivična dela koja uključuju elektronske dokaze.

U ovoj konvenciji se od država članica zahteva da u domaće zakonodavstvo uključe izvestan broj istražnih ovlašćenja za potrebe krivičnih istraga ili postupaka. To su:

- hitna zaštita sačuvanih računarskih podataka (član 16);
- hitna zaštita i delimično otkrivanje podataka o saobraćaju (član 17);
- izdavanje naredbe za predavanje računarskih podataka (član 18);
- pretraživanje i zaplena sačuvanih računarskih podataka (član 19);
- prikupljanje računarskih podataka u realnom vremenu (član 20);
- presretanje podataka iz sadržaja (član 21).

Konvencija takođe sadrži odredbe koje čine osnovu za međunarodnu saradnju u borbi protiv visokotehnološkog kriminala. One uključuju:

- slučajne informacije (član 26);
- hitnu zaštitu sačuvanih računarskih podataka (član 29);
- hitno otkrivanje zaštićenih podataka o saobraćaju (član 30);
- uzajamnu pomoć u odnosu na pristupanje sačuvanim računarskim podacima (član 31);

27 Konvencija o visokotehnološkom kriminalu, 23. novembar 2001, CETS br. 185, stupila na snagu 1. jula 2004.

- uzajamnu pomoć u prikupljanju podataka o saobraćaju u realnom vremenu (član 33);
- uzajamnu pomoć u presretanju podataka iz sadržaja (član 34).

Pored toga, potpisnice ove konvencije su u maju 2022 godine otvorile za potpisivanje Drugi dodatni protokol uz Budimpeštansku konvenciju. Njime se uvode novi postupci za unapređenje direktne saradnje sa pružaocima usluga i subjektima u drugim ugovornim stranama, kao i za unapređenje međunarodne saradnje između organa za otkrivanje uskladištenih računarskih podataka, uključujući saradnju u pogledu hitne međunarodne pomoći.[28]

Ova ovlašćenja daju praktičarima iz krivičnopravnih organa važne alate za uspešno otkrivanje, istraživanje i krivično gonjenje krivičnih dela izvršenih protiv ili korišćenjem računara. Međutim, njihova primena može da utiče na ljudska prava i osnovne slobode. Istražitelji koji koriste ova ovlašćenja odgovorni su da obezbede da sva ograničenja ljudskih prava budu zasnovana na zakonu, nužna i proporcionalna.

4.3 ZAŠTITNE MERE ZA LJUDSKA PRAVA KOJE SU SPECIFIČNE ZA VISOKOTEHNOLOŠKI KRIMINAL

Iako se odredbe međunarodnih i regionalnih standarda ljudskih prava primenjuju na sve krivične istrage, Konvencija SE o visokotehnološkom kriminalu nastoji da ih primeni posebno na istrage visokotehnološkog kriminala i drugih krivičnih dela koja uključuju elektronske dokaze. U članu 15 Konvencije se od svake strane zahteva da u domaćem pravu utvrdi određene uslove i zaštitne mere koje će se primenjivati prilikom korišćenja procesnih ovlašćenja iz Konvencije (vidi okvir 2).

Član 15 ne navodi detaljno ove zaštitne mere, već se, umesto toga, odnosi na obaveze država na osnovu EKLJP i ICCPR kao izvora zaštitnih mera. To omogućava ovoj odredbi da uzme u obzir značajne razlike koje postoje u različitim pravnim tradicijama u pogledu načina na koji se zaštitne mere primenjuju.

OKVIR 2 ČLAN 15 KONVENCIJE O VISOKOTEHNOLOŠKOM KRIMINALU - USLOVI I OGRANIČENJA

1. Svaka Strana ugovornica treba da obezbedi da uspostavljanje, sprovođenje i primena ovlašćenja i postupaka navedenih u ovom odeljku, podleže **uslovima i ograničenjima** predviđenim domaćim pravom, koje mora da omogući odgovarajuću zaštitu ljudskih prava i sloboda, uključujući i prava koja proizilaze iz obaveza koje je Strana ugovornica preuzela na osnovu Konvencije Saveta Evrope o zaštiti ljudskih prava i osnovnih sloboda iz 1950 godine, Međunarodnog pakta Ujedinjenih nacija o građanskim i političkim pravima iz 1966 godine i ostalih važećih međunarodnih dokumenata o ljudskim pravima, i koje će da **sadrži načelo proporcionalnosti**.

28 Drugi dodatni protokol uz Konvenciju o visokotehnološkom kriminalu o pojačanoj saradnji i otkrivanju elektronskih dokaza, 17. novembar 2021, CETS br. 224.

2. Ti uslovi i ograničenja mogu, u zavisnosti od vrste ovlašćenja ili postupaka o kojima se radi, između ostalog, da **obuhvate sudsku ili drugu vrstu nezavisne kontrole**, na osnovu kojih se **opravdava primena i ograničenje obima i trajanja tih ovlašćenja ili postupaka.**
3. U meri u kojoj je to u skladu sa javnim interesom, a naročito sa pravilnom primenom prava, svaka Strana ugovornica treba da razmotri posledice ovlašćenja i postupaka iz ovog odeljka **na prava, odgovornosti i opravdane interese trećih strana.**

U članu 15 se ističu sledeći uslovi i ograničenja:

- načelo proporcionalnosti;
- dostupnost sudske ili druge vrste nezavisne kontrole;
- potreba da se konkretno navede jasan osnov kojim se opravdava primena;
- ograničenje obima i trajanja ovlašćenja ili postupaka – u zavisnosti od vrste ovlašćenja ili postupaka o kojima se radi;
- potreba da se razmotre posledice ovlašćenja na prava, odgovornosti i opravdane interese trećih strana.

U praktičnom smislu, to znači da službenici koji istražuju optužbe o visokotehnološkom kriminalu moraju da budu svesni uticaja koji njihovi postupci imaju na prava utvrđena međunarodnim ugovorima o ljudskim pravima.

Načelo proporcionalnosti podrazumeva balansiranje različitih i konkurentnih istražnih mera u odnosu na neku konkretnu istragu visokotehnološkog kriminala. To znači da se mešanje u ljudska prava mora svesti na minimum i da istražitelji moraju da koriste najmanje intruzivna sredstva za postizanje svog cilja.

Takva ravnoteža je moguća samo ako u nacionalnom zakonodavstvu postoje različite – manje i više intruzivne – opcije. Na primer, postoje dva moguća načina za dobijanje pristupa podacima koje čuva pružalac usluga. Jedan je naredba za čuvanje i dostavljanje; druga je pretres i oduzimanje radi dobijanja podataka. Mehanizam naredbe za čuvanje i dostavljanje je generalno manje intruzivan od pretresa i oduzimanja, koji zahtevaju pristup većem skupu podataka i obično se sprovode na licu mesta. Istražitelji moraju da jasno obrazlože zašto koriste intruzivniju dokaznu radnju kada su im dostupne one koje su manje intruzivne.

U svakom slučaju, istražitelji moraju da sudu ili nezavisnom organu obezbede dovoljan osnov za davanje odobrenja za korišćenje intruzivnih dokaznih radnji. Sudski ili drugi nezavisni organi treba da, posle detaljne procene svakog pojedinačnog slučaja, dozvole korišćenje takvih ovlašćenja. U zavisnosti od težine krivičnog dela, nacionalno zakonodavstvo može da zahteva posebne uslove. Praktičari iz krivičnopravnih organa takođe moraju da obezbede da se intruzivna istražna ovlašćenja ne koriste duže nego što je apsolutno neophodno za efikasnu istragu predmeta.

Pored toga, Drugi dodatni protokol uz Budimpeštansku konvenciju[29] sadrži detaljan član 14 o

29 Ibid.na

zaštiti podataka o ličnosti. Ova odredba se primenjuje na nova procesna ovlašćenja predviđena Drugim dodatnim protokolom i utvrđuje obaveze potpisnica da obezbede da prilikom korišćenja ovih ovlašćenja budu podržani važni aspekti prava na privatnost i zaštitu podataka – kao što su svrha i korišćenje, kvalitet i integritet podataka, osetljivi podaci, zadržavanje podataka, automatizovano odlučivanje, bezbednost podataka i dalje deljenje podataka.

5

Primena mera zaštite ljudskih prava u istragama visokotehnološkog kriminala

U ovom poglavlju se istražuju elementi koje praktičari iz krivičnopravnih organa treba da uzmu u obzir kako bi obezbedili zaštitu ljudskih prava tokom istraga visokotehnološkog kriminala. Ono se u velikoj meri oslanja na smernice koje obezbeđuje sudska praksa ESLJP i SPEU. Ovo uputstvo je relevantno i za države koje nisu članice SE ili EU, jer pruža konkretne primere toga kako se poštovanje ljudskih prava može obezbediti u istragama visokotehnološkog kriminala. Nekoliko posebno važnih presuda ESLJP je detaljnije predstavljeno u prilogu 2.

5.1 PRAVO NA PRIVATNOST

Istrage visokotehnološkog kriminala i drugih krivičnih dela koja uključuju elektronske dokaze mogu da predstavljaju mešanje u pravo na privatnost kada:

- koriste podatke o ličnosti;
- uključuju zadržavanje i obradu podataka o pretplatniku, saobraćaju ili sadržaju;
- se mešaju u privatnost komunikacija, na primer prilikom presretanja poruka ili podataka o saobraćaju;
- uključuju tajni nadzor, kao što su tajne operacije radi hvatanja kriminalaca na onlajn tržištima (na darknet-u).

Postoji širok korpus sudske prakse ESLJP i SPEU u vezi sa sprovođenjem prava na privatnost.

OBIM I PRIMENA PRAVA NA PRIVATNOST U ISTRAGAMA VISOKOTEHNOLOŠKOG KRIMINALA

Sudska praksa ESLJP sadrži detaljna uputstva o obimu i primeni prava na privatnost u kontekstu istraga visokotehnološkog kriminala. Ovaj sud je u svojoj praksi široko definisao obim prava na privatni i porodični život, tako da ono obuhvata i:

- zaštitu ugleda pojedinca, klevetu (pozitivnu obavezu države u vezi sa obavezom pružaoca usluga);
- zaštitu podataka;
- prikupljanje datoteka ili podataka od strane bezbednosnih službi ili drugih državnih organa;
- policijski nadzor (uključujući i nadzor na internetu i darknet-u[30]);
- ovlašćenje policije da izvrši zaustavljanje i pretres;
- posete kućama, pretrese i oduzimanja;
- presretanje telekomunikacija u kontekstu krivičnih istraga;
- korespondenciju fizičkih lica, profesionalaca i preduzeća;
- tajni nadzor građana i organizacija;

30 Vidi još o praksi ESLJP u: SE, Priručnik za uzajamnu pravnu pomoć (Beograd, 2013), str. 101.

- zadržavanje podataka o pretplatnicima i saobraćaju.[31]

Sud je takođe podvukao da u pogledu prava na privatni i porodični život, države imaju i pozitivnu obavezu (da štite to pravo) i negativnu obavezu (da se uzdrže od mešanja u to pravo). Na primer, u predmetu K.U. *protiv Finske*, Sud je istakao pozitivnu obavezu države da efikasno istražuje krivična dela i da donosi odgovarajuće propise o izuzecima od obaveze pružalaca usluga da čuvaju poverljivost podatakal.[32] Sud je naglasio da, iako sloboda izražavanja i poverljivost komunikacije imaju nesumnjiv značaj, takve garancije ne mogu biti apsolutne. S obzirom na ozbiljnost ovog predmeta, Sud je smatrao da je država morala da uspostavi pravni okvir kojim bi se uspostavila ravnoteža u pogledu potrebe da se obezbedi zaštita poverljivosti internet usluga, spreče neredi ili kriminal i obezbedi zaštita prava i sloboda pojedinaca.[33]

Kao i sva mešanja u ljudska prava, ograničenja prava na privatnost moraju biti propisana zakonom, nužna i proporcionalna. Sudska praksa ESLJP-a daje uputstva o tome šta to znači u praksi. Slična načela važe i za odgovarajuću odredbu ICCPR-a (član 17).[34]

Što se tiče **zakonske osnove**, propisi koji odobravaju korišćenje ovlašćenja koja ometaju pravo na privatni život moraju biti dostupni onima na koje mogu da utiču i dovoljno jasni da „pojedincima daju odgovarajuću naznaku o okolnostima u kojima i uslovima pod kojima vlasti imaju pravo da koriste mere koje utiču na njihova prava na osnovu Konvencije."[35] TTo znači da različita procesna ovlašćenja koja stoje na raspolaganju istražiteljima (npr. odredbe o zahtevima za čuvanje ili dostavljanje podataka, omogućavanje prikupljanja podataka o saobraćaju u realnom vremenu ili traženje i oduzimanje računarskih podataka, predmeta ili dokumenata) moraju biti jasno definisana u nacionalnom zakonodavstvu.

Što se tiče **nužnosti i proporcionalnosti**, svako mešanje mora da ima legitiman cilj – u ovom slučaju, istragu nekog određenog krivičnog dela – i mora da bude ograničeno na ono što je nužno za postizanje tog cilja. To zahteva da se razmotri da li su dostupne neke manje restriktivne alternativne mere. Pored toga, propisi moraju da sadrže adekvatne mere zaštite od proizvoljne primene i ne smeju da daju prevelika diskreciona prava službenicima kojima je poverena njihova primena.

To znači da zakonodavstvo kojim se utvrđuju procesna ovlašćenja za korišćenje u istragama visokotehnološkog kriminala treba da:

- zahteva postojanje adekvatnih osnova za opravdavanje upotrebe pojedinačnih procesnih ovlašćenja;
- predviđa da ta mera podleže pravosudnoj ili drugoj nezavisnoj kontroli, a naročito kada uključuje posebno invazivne postupke, kao što je presretanje podataka o sadržaju;
- utvrdi rokove čuvanja podataka;
- izuzme (ili posebno zaštiti) privilegovane podatke iz obima naredbi za predavanje računarskih podataka kao i pretresa i oduzimanja.

---

31 ESLJP, Vodič kroz član 8 Evropske konvencije za zaštitu ljudskih prava: Pravo na poštovanje privatnog i porodičnog života, doma i prepiske (Strazbur, 2020); Vidi i: ESLJP (2023), Informativni list o zaštiti podataka o ličnosti, dostupno na https://www.echr.coe.int/Documents/FS_Data_ENG.pdf; ESLJP (2022), Informativni list o masovnom nadzoru, dostupno na https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf.

32 ESLJP, *K.U. protiv Finske*, 2. decembar 2008, br. 2872/02, § 49.

33 Ibid., §§ 48, 49.

34 Vidi Komitet UN za ljudska prava, CCPR Opšti komentar br. 16: član 17, Pravo na privatnost, 23. mart 1988, st. 4, 5.

35 ESLJP, *Fernandez Martinez protiv Španije* [GC], 12. jun 2014, br. 56030/07, § 117.

Primeri primene načela proporcionalnosti mogu se naći u predmetima ESLJP koji se odnose na presretanje podataka o sadržaju, što je najintruzivnije procesno ovlašćenje utvrđeno Konvencijom SE o visokotehnološkom kriminalu. U ESLJP se navodi da, naročito, zakonske odredbe koje regulišu presretanje komunikacija moraju da predvide adekvatne i efikasne garancije od proizvoljnosti i rizika od zloupotrebe svojstvenih svakom sistemu tajnog nadzora, i definišu se posebni uslovi i zaštitne mere za tajni nadzor komunikacija. (vidi odeljak „Tajni nadzor u istragama visokotehnološkog kriminala“ u tekstu dole).[36]

ZAŠTITA PODATAKA O LIČNOSTI U ISTRAGAMA VISOKOTEHNOLOŠKOG KRIMINALA

Drugi važan aspekt prava na privatnost tiče se prava na zaštitu podataka o ličnosti, koje je utvrđeno u nizu međunarodnih i regionalnih pravnih instrumenata (vidi okvir 3). Načela zaštite podataka moraju se uzeti u obzir prilikom regulisanja policijskih ovlašćenja i prilikom prikupljanja i obrade podataka o ličnosti u kontekstu krivičnih istraga. Ova načela uključuju:[37]

- **Zakonitost:** obrada podataka o ličnosti mora da bude zakonita, bilo uz saglasnost lica na koje se podaci odnose ili na osnovu drugog legitimnog osnova predviđenog propisima o zaštiti podataka.
- **Pravičnost:** obrada podataka o ličnosti treba da bude pravična, a lica na koja se podaci odnose moraju da budu obaveštena o tom riziku.
- **Transparentnost:** obrada podataka o ličnosti treba da bude transparentna. Lica na koja se podaci odnose treba da budu obaveštena o tome kako se njihovi podaci koriste.
- **Ograničenje svrhe:** svaka obrada podataka o ličnosti mora da se obavi sa konkretnom, jasno definisanom svrhom. Svaka dodatna obrada mora da bude u skladu sa prvobitnom svrhom.
- **Minimizacija podataka:** obrada podataka mora da bude ograničena na ono što je neophodno za ispunjavanje legitimne svrhe.
- **Tačnost podataka:** rukovaoci treba da obezbede tačnost i ažurnost podataka o ličnosti i moraju da preduzmu mere za brisanje ili ispravljanje netačnih podataka.
- **Ograničenje čuvanja:** podaci o ličnosti ne smeju se čuvati duže nego što je nužno i moraju se izbrisati ili anonimizirati čim više ne budu potrebni za svrhu za koju su prikupljeni.
- **Bezbednost podataka (integritet i poverljivost):** prilikom obrade podataka o ličnosti moraju se sprovesti odgovarajuće tehničke ili organizacione mere da bi se podaci zaštitili od slučajnog, neovlašćenog ili nezakonitog pristupa, korišćenja, izmene, otkrivanja, gubitka, uništenja ili oštećenja.
- **Odgovornost:** rukovaoci i obrađivači moraju da aktivno i stalno sprovode mere za unapređenje i osiguranje zaštite podataka i moraju da budu u stanju da pokažu usaglašenost sa odredbama o zaštiti podataka.

36 ESLJP, *Roman Zaharov protiv Rusije* [GC], 4. decembar 2015, br. 47143/06; ESLJP, Brejer protiv Nemačke, 30. januar 2020, br. 50001/12; uporedi i sa odlukama SPEU o zadržavanju podataka.

37 Agencija EU za osnovna prava i SE, Priručnik o evropskom zakonodavstvu o zaštiti podataka (Luksemburg, 2018).

OKVIR 3 MEĐUNARODNI I REGIONALNI PRAVNI INSTRUMENTI O ZAŠTITI PODATAKA O LIČNOSTI

- **Konvencija SE o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti** od 28. januara 1981. godine, br. 108 (stupila na snagu 1985).
- **Dodatni protokol uz Konvenciju SE o zaštiti lica u odnosu na automatsku obradu podataka o ličnosti** od 10. oktobra 2018. godine, br. 223 (još nije stupio na snagu).
- **Opšta uredba EU o zaštiti podataka:** Uredba (EU) 2016/679 Evropskog parlamenta i saveta od 27. aprila 2016. godine o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i o slobodnom kretanju takvih podataka i o stavljanju direktive 95/46/EZ van snage (stupila na snagu 2018).
- **Policijska direktiva EU:** Direktiva (EU) 2016/680 Evropskog parlamenta i saveta od 27. aprila 2016. godine o zaštiti fizičkih lica u vezi sa obradom podataka od strane nadležnih tela u svrhe sprečavanja, istrage, otkrivanja ili gonjenja za krivična dela ili izvršenja krivičnih sankcija i o slobodnom kretanju takvih podataka, te o stavljanju van snage Okvirne odluke Saveta 2008/977/JHA (stupila na snagu 2018).

ESLJP je već ispitao širok spektar mešanja u pravo na privatni život na osnovu člana 8 EKLJP koja proističu iz čuvanja, obrade i korišćenja podataka o ličnosti. Ona uključuju: korišćenje GPS praćenja u krivičnim istragama;[38] otkrivanje identifikacionih podataka organima za sprovođenje zakona od strane pružalaca telekomunikacionih usluga;[39] neograničeno zadržavanje otisaka prstiju, uzoraka ćelija i DNK profila posle krivičnog postupka;[40] tzv. merenje ili prikupljanje podataka o korišćenju ili saobraćaju;[41] i skladištenje podataka o korisnicima pripejd SIM kartica.[42]

U predmetu *Marper protiv Ujedinjenog Kraljevstva*, ESLJP je jasno naveo da i samo čuvanje podataka koji se odnose na privatni život nekog lica predstavlja mešanje u pravo na privatnost iz člana 8 EKLJP. Sud smatra da je zaštita podataka o ličnosti od ključnog značaja za uživanje prava na poštovanje privatnog i porodičnog života. Domaći zakon treba da obezbedi odgovarajuće zaštitne mere, naročito kada je u pitanju automatska obrada podataka o ličnosti. Konkretno, domaći zakon treba da obezbedi da su takvi podaci relevantni, da nisu preterani u pogledu svrha zbog kojih se čuvaju, kao i da se čuvaju u obliku koji dozvoljava identifikaciju lica na koja se podaci odnose najduže toliko koliko je neophodno za svrhu za koju se ti podaci čuvaju. On takođe mora da pruži adekvatne garancije da su zadržani podaci o ličnosti efikasno zaštićeni od zloupotrebe.

38 ESLJP, *Uzun protiv Nemačke*, 2. septembar 2010, br. 35623/05; ESLJP, Ben Faiza protiv Francuske, 8. februar 2018, br. 31446/12.

39 ESLJP, *K.U. protiv Finske*, 2. decembar 2008, br. 2872/02; ESLJP, Benedik protiv Slovenije, 24. april 2018, br. 62357/14.

40 ESLJP, *S. i Marper protiv Ujedinjenog Kraljevstva* [GC], 4. decembar 2008, 30562/04 i 30566/0.

41 ESLJP, *Maloun protiv Ujedinjenog Kraljevstva*, 2. avgust 1984, br. 8691/79; ESLJP, Kopland protiv Ujedinjenog Kraljevstva, 3. april 2007, br. 62617/00.

42 ESLJP, *Brejer protiv Nemačke*, 30. januar 2020, br. 50001/12.

ZADRŽAVANJE I PRISTUP PODACIMA O PRETPLATNIKU ILI SAOBRAĆAJU

Jedno od pitanja koja se direktno odnose na zaštitu podataka o ličnosti je zadržavanje podataka. I ESLJP i SPEU su se bavili ovim pitanjem u brojnim predmetima. U predmetu Benedik protiv Slovenije, ESLJP je utvrdio kršenje člana 8 EKLJP u vezi sa nedovoljnom jasnoćom slovenačkog ustavnog okvira o zakonskim uslovima za pristup podacima o pretplatnicima koji se odnose na (dinamičke) IP adrese. Sud je našao da korisnici instalacija za pristup internetu legitimno očekuju privatnost, čak i ako svesno otkriju svoju IP adresu javnosti.

U predmetu Brejer protiv Nemačke, sud je ustanovio da nije prekršen član 8 EKLJP, jer su uslovi i zaštitne mere iz nemačkog zakonodavstva koje reguliše obavezu pružalaca usluga da čuvaju podatke o ličnosti korisnika pripejd SIM kartica za mobilni telefon i uslove pod kojima se ti podaci, na zahtev, stavljaju na raspolaganje organima vlasti bili jasni i proporcionalni. Prilikom odlučivanja u ovom predmetu, sud je istakao ključni značaj prava na privatnost i potrebe za snažnim zaštitnim merama koje će sprečiti korišćenje podataka o ličnosti suprotno članu 8.

Konkretno, sud je utvrdio da je prikupljanje imena i adresa podnosilaca predstavki kao korisnika pripejd SIM kartica predstavljalo ograničeno mešanje u njihova prava. Predmetni zakon je sadržavao dodatne zaštitne mere, a ljudi su se mogli obratiti i nezavisnim telima za nadzor nad podacima radi preispitivanja zahteva organa vlasti za dobijanje podataka i tražiti pravni lek ako je potrebno. Zbog toga, u ovom slučaju, Nemačka prilikom primene tog zakona nije prekoračila granice svog diskrecionog prava („granicu slobodne procene") i prikupljanjem podataka nije narušila prava podnosilaca predstavke.

EU je 2006. godine usvojila takozvanu Direktivu o zadržavanju podataka, koja reguliše zadržavanje određenih vrsta podataka o saobraćaju koji se odnose na korišćenje telekomunikacionih mreža (telefonske podatke, podatke sa mobilnih telefona i podatke sa interneta) za krivičnopravne potrebe.[43] Podaci o saobraćaju odražavaju aktivnosti korisnika na mreži i, između ostalog, omogućavaju organima za sprovođenje zakona da vide odakle dolaze i kome su upućeni telefonski pozivi u okviru mreže, podatke o lokaciji (u mobilnoj mreži), kao i IP adrese korisnika usluga pristupa internetu. Konkretno u vezi sa visokotehnološkim kriminalom, važno je napomenuti da ova direktiva nije zahtevala zadržavanje podataka o posećenim internet stranicama ili drugih podataka koji se odnose na korišćenje interneta, već je bila ograničena na zadržavanje veze između IP adrese i pretplatničkih podataka korisnika.

SPEU je 2014. godine proglasio Direktivu o zadržavanju podataka nespojivom sa članovima 7 i 8 Povelje EU o osnovnim pravima (poštovanje privatnog i porodičnog života i zaštita podataka o ličnosti) i zato nevažećom.[44] Sud je presudio da je zadržavanje podataka o saobraćaju predviđeno Direktivom nespojivo sa pravom na privatnost zbog svoje uopštene prirode (zahtevalo je čuvanje podataka korisnika koji nisu osumnjičeni ni za kakvo krivično delo), nedostatka mera zaštite od nezakonitog pristupa i korišćenja tih podataka, kao i nedostatka ograničenja svrhe (koristili bi se za teška krivična dela, ali ovaj pojam nije bio jasno definisan u Direktivi).

43 Direktiva 2006/24/EZ Evropskog parlamenta i Saveta o zadržavanju podataka dobijenih ili obrađenih u vezi s pružanjem javno dostupnih elektronskih komunikacijskih usluga ili javnih komunikacijskih mreža i o izmeni Direktive 2002/58/EZ, 13. april 2006, SLEU L 105/54.

44 SPEU, *Digital Rights Ireland Ltd protiv ministra za komunikacije, morskih i prirodnih resursa i drugih i Karntner Landesregierung i drugih* [GC], 8. april 2014, spojeni C-293/12 i C-594/12.

SPEU je dodatno razjasnio svoj stav u nekoliko narednih predmeta u vezi sa nacionalnim zakonodavstvom u državama članicama EU, koji su se zasnivali na Direktivi o zadržavanju podataka.[45] Sud je našao da ovi nacionalni pravni okviri krše prava na privatnost i zaštitu podataka jer zahtevaju opšte i neselektivno zadržavanje podataka o saobraćaju i lokaciji. Razjasnio je da je takvo zadržavanje podataka dozvoljeno samo ako je prisutna ili se može predvideti ozbiljna pretnja po nacionalnu bezbednost i ako zadržavanje podataka podleže sudskoj ili drugoj nezavisnoj kontroli i traje samo u ograničenom vremenskom periodu. Sud je takođe naveo da pravo EU ne isključuje nacionalno zakonodavstvo koje predviđa ciljano zadržavanje podataka o saobraćaju i lokaciji za potrebe zaštite nacionalne bezbednosti, borbe protiv teškog kriminala i sprečavanja ozbiljnih pretnji po javnu bezbednost, pod uslovom da postoje određene mere zaštite.[46]

Istovremeno, Sud je pojasnio da pravo EU dozvoljava opšte i neselektivno zadržavanje pretplatničkih podataka, odnosno podataka o IP adresama i podataka koji se odnose na građanski identitet korisnika, za iste svrhe.[47] Smatralo se da potreba za procesuiranjem (visokotehnološkog) kriminala i identifikovanjem zlonamernih korisnika na internetu preteže nad mešanjem u pravo na privatnost do koga dovodi zadržavanje ograničenih podataka na izvornim IP adresama korisnika interneta. To je utrlo put zakonodavnim merama koje predviđaju preventivno zadržavanje IP adresa u cilju borbe protiv kriminala i zaštite javne bezbednosti. Bez ovih podataka, korišćenje interneta bi moglo da postane potpuno anonimno, sa značajnim posledicama po istrage i krivično gonjenje (visokotehnološkog) kriminala.

TAJNI NADZOR U ISTRAGAMA VISOKOTEHNOLOŠKOG KRIMINALA

Različite otvorene i prikrivene metode za prikupljanje informacija se u različitoj meri mešaju u pravo na privatnost. Neke od ovih metoda, kao što je korišćenje posebnih i drugih tajnih dokaznih radnji, uključujući nadzor privatnih prostorija ili domova, presretanje komunikacije, korišćenje prikrivenih islednika i doušnika, kao i pristup bankovnim računima i drugim poverljivim informacijama, detaljnije su istražene u OEBS-ovom priručniku *Ljudska prava u antiterorističkim istragama*.[48]

Za razliku od ciljanog nadzora, koji se obično zasniva na prethodnoj sumnji i podleže dobijanju odobrenja od suda ili izvršnih organa, programi masovnog nadzora ne dozvoljavaju individualizovanu procenu proporcionalnosti od slučaja do slučaja pre nego što se takve mere preduzmu. Kao takvi, oni rizikuju da naruše samu suštinu prava na privatnost. Informacije prikupljene za obaveštajne potrebe ponekad se koriste i kao dokaz u krivičnim postupcima. Međutim, prvobitna svrha prikupljanja takvih informacija se razlikuje od svrhe procesuiranja visokotehnološkog kriminala ili drugih krivičnih dela koja uključuju elektronske dokaze, a na njihovo prikupljanje se često prime-

45 SPEU, *Digital Rights Ireland Ltd protiv ministra za komunikacije, morskih i prirodnih resursa i drugih* i Karntner Landesregierung i drugih [GC], 8. april 2014, spojeni C-293/12 i C-594/12; SPEU, *Tele2 Sverige AB protiv Post- och telestyrelsen i Državni sekretar za unutrašnje poslove protiv Toma Votsona i drugih* [GC], 21. decembar 2016, spojen C-203/15 i C-698/15; SPEU, *Privacy International protiv državnog sekretara za inostrane poslove i poslove Komonvelta i drugih* [GC], 6. oktobar 2020, C-623/17; SPEU, *La Quadrature du Net i drugi protiv premijera i drugih* [GC], 6. oktobar 2020, spojen C-511/18, C-512/18 i C-520/18; SPEU, SpaceNet i Telekom Deutschland GmbH [GC], 27. oktobar 2022, spojen C-793/19 i C-794/19.

46 SPEU, *SpaceNet i Telekom Deutschland GmbH* [GC], 27. oktobar 2022, spojen C-793/19 i C-794/19.

47 CJEU, *La Quadrature du Net and Others v Premier ministre and Others* [GC], 6 October 2020, Joined C-511/18, C-512/18 and C-520/18; CJEU, *SpaceNet and Telekom Deutschland GmbH* [GC], 27 October 2022, Joined C-793/19 and C-794/19.

48 Vidi i OEBS/ODIHR, Ljudska prava u antiterorističkim istragama: Praktični priručnik za policijske službenike (Varšava, 2013).

njuju i različita pravna pravila i uslovi. Zbog toga je očigledno potreban oprez kada se takve informacije koriste u krivičnom postupku. Korišćenje nezakonito prikupljenih obaveštajnih podataka u krivičnom postupku u suprotnosti je sa ljudskim pravima.

ESLJP je našao da je član 8 EKLJP prekršen u nekoliko predmeta koji se odnose na režime tajnog nadzora, uključujući i masovno presretanje komunikacija i razmenu obaveštajnih podataka, kao što su, na primer, *Roman Zaharov protiv Rusije*,[49] *Sabo i Viši protiv Mađarske*,[50] *Big Brother Watch i drugi protiv Ujedinjenog Kraljevstva*.[51] TPresuda u predmetu Viši protiv Mađarske je jasno pokazala da je sudska kontrola nad tajnim nadzorom izuzetno važna. Nezavisno sudsko telo treba da nadzire upotrebu ove mere; telo koji je direktno povezano sa izvršnim organima (u ovom slučaju ministrom unutrašnjih poslova) ne ispunjava ovaj uslov. U presudi je takođe naglašeno pitanje obima mera nadzora, a zaštitne mere koje su predviđene u zakonodavstvu smatraju se nedovoljno preciznim, delotvornim i sveobuhvatnim u pogledu naređivanja, izvršenja i potencijalnog ispravljanja takvih mera.

U predmetu *Big Brother Watch i drugi protiv Ujedinjenog Kraljevstva*, sud je naveo da se kod svakog režima masovnog presretanja moraju primeniti „potpune zaštitne mere“ na domaćem nivou, što znači da: procenu nužnosti i proporcionalnosti preduzetih mera treba napraviti u svakoj fazi procesa; za masovno presretanje se mora dobiti nezavisno odobrenje na samom početku, kada se definišu objekat i obim ove operacije; i ta operacija treba da bude predmet nadzora i nezavisne ex post facto kontrole.[52]

U povezanom predmetu *Centrum För Rättvisa protiv Švedske*, sud je istakao nedostatke u domaćem pravnom okviru koji nisu u dovoljnoj meri nadomešteni drugim zaštitnim merama.[53] To su, između ostalog, bili: odsustvo jasnog pravila o uništavanju presretnutog materijala koji ne sadrži podatke o ličnosti; odsustvo obaveze da se privatnost pojedinaca uzme u obzir prilikom odlučivanja da li će se obaveštajni materijal preneti stranim partnerima; i odsustvo delotvorne *ex post facto* kontrole, kao što je mogućnost da u odgovoru na upite u vezi sa masovnim presretanjem komunikacija, pripadnici javnosti dobiju obrazložene odluke.

Ovi predmeti pružaju jasna uputstva o nekim zaštitnim merama koje su potrebne u kontekstu tajnog nadzora komunikacija. ESLJP je naveo da očekuje da postoji režim nezavisnog nadzora nad upotrebom takvih prikrivenih i intruzivnih ovlašćenja, i da što je nezavisnije telo za davanje odobrenja ili kontrolu, veća je verovatnoća da će režim odobravanja i kontrole biti odgovarajući. Zaista, u predmetu *Klas protiv Nemačke*, ESLJP je primetio da sudska kontrola postupka odobravanja pruža „najbolje garancije nezavisnog, nepristrasnog i pravilnog postupka.”[54] Korišćenje specijalizovanih poverenika i tribunala na nacionalnom nivou takođe može da zadovolji uslove iz člana 8 EKLJP.

49 ESLJP, *Roman Zaharov protiv Rusije* [GC], 4. decembar 2015, No. 47143/06.

50 ESLJP, *Sabo i Viši protiv Mađarske*, 12, januar 2016, No. 37138/14.

51 ESLJP, *Big Brother Watch i drugi protiv Ujedinjenog Kraljevstva* [GC], 25. maj 2021, br. 58170/13, 62322/14 i 24960/15.

52 Ibid.na

53 ESLJP, *Centrum För Rättvisa protiv Švedske* [GC], 25. maj 2021, br. 35252/08.

54 ESLJP, *Klas i drugi protiv Nemačke*, 6. septembar 1978, br. 5029/71.

5.2 PRAVO NA PRAVIČNO SUĐENJE

Istrage visokotehnološkog kriminala obuhvataju niz procesa koji se odnose na glavne elemente prava na pravično suđenje, uključujući:

- pristup podacima koji se čuvaju na elektronskim uređajima;
- održavanje integriteta oduzetih elektronskih dokaza u kontekstu pretresa, oduzimanja i upravljanja elektronskim podacima;
- pristup dokazima i uvid u njih od strane okrivljenog u vezi sa oduzetim elektronskim dokazima;
- izuzimanje ili ograničenja pretraga privilegovane komunikacije i informacija (kao što je komunikacija sa advokatima, medicinska evidencija, ili komunikacija između novinara i njihovih izvora).

Pretpostavka nevinosti je usko povezana sa pravom lica da ne inkriminišu sama sebe i sa pravom na odbranu ćutanjem.[55] Pravo na odbranu ćutanjem je naročito važno u kontekstu pretresa i istraživanja elektronskih podataka. Iako u nacionalnom zakonodavstvu mogu da se izreknu (upravne) sankcije svedoku koji nije voljan da pruži informacije, kao što je lozinka za pristup računaru tokom pretresa elektronskih uređaja, sankcionisanje osumnjičenog bi bilo problematično, jer se osumnjičeni može pozvati na svoje pravo na odbranu ćutanjem. Zato je važno da osumnjičeni bude obavešten o svojim pravima pre nego što se od njega zatraži da dobrovoljno unese lozinku ili šifru za pristup u računar ili drugi elektronski uređaj.[56]

Uređaj za skladištenje, kao što je interni ili eksterni računarski disk, USB ili mobilni uređaj, može da sadrži ogromnu količinu podataka koji se ne mogu pretražiti tokom pretresa stana. Zato se on često mora oduzeti i pregledati u kasnijoj fazi.[57] Domaće zakonodavstvo, uključujući konkretna pravila o pretresu i oduzimanju (ili preciznije: pristupu i kopiranju[58]) elektronskih dokaza, mora da garantuje da će pravo na delotvornu odbranu i materijalni dokazi biti jednako očuvani. Relevantne procesne odredbe uključuju: obavezu oduzimanja elektronskog uređaja i izrade tačne kopije; obavezu obaveštavanja i pozivanja osumnjičenog i njegovog branioca na pretragu oduzetog elektronskog uređaja; i obavezu davanja oduzetih dokaza na uvid odbrani. Uvođenje takvih procesnih zaštitnih mera pomaže da se obezbedi sprovođenje u praksi načela jednakosti stranaka i stranačkog postupka, koji predstavljaju važne komponente pravičnog suđenja.

Veliki obim podataka koji su uključeni u neke istrage takođe predstavlja izazov u pogledu obelodanjivanja. Važna zaštitna mera je da se odbrani obezbedi mogućnost da učestvuje u utvrđivanju kriterijuma koji se koriste za određivanje podataka koji mogu biti relevantni za obelodanjivanje.[59] To je naročito važno u slučajevima koji uključuju podatke koji se čuvaju na internetu. Pored toga, svako nedozvoljavanje odbrani da dalje pretražuje identifikovane ili označene podatke iz predmeta (npr. podatke koji su dobijeni prilikom pretresa) otvara pitanje obezbeđivanja adekvatnih uslova za pri-

55 ESLJP, Vodič za član 6 Evropske konvencije za zaštitu ljudskih prava: Pravo na pravično suđenje (krivični aspekt) (Strazbur, 2022), para 197 i 373.

56 Konvencija o visokotehnološkom kriminalu, 23. novembar 2001, CETS br. 185, član 32(b).

57 SE, Eksplanatorni izveštaj uz Konvenciju o visokotehnološkom kriminalu (Budimpešta, 2001), § 187.

58 Ibid. §§ 137, 191 i 197.

59 ESLJP, *Sigurdur Einarson i drugi protiv Islanda*, 4. jun 2019, br. 39757/15, § 90; Vidi i ESLJP, Rook protiv Nemačke, 25. jul 2019, br. 1586/15, §§ 67, 72.

premu odbrane.[60] Kad god je moguće, odbrana treba da bude obaveštena o kriterijumima za pretragu velikih skupova podataka, treba da joj se omogući jednak pristup i treba da ima svaku priliku za pretraživanje skupova podataka radi pronalaženja relevantnih (oslobađajućih) podataka. Privilegovanu prirodu komunikacije između branilaca i njihovih klijenata treba poštovati i prilikom pretraživanja elektronskih dokaza.

Ukratko, pravo na pravično suđenje zahteva pravičan i uravnotežen postupak, naročito kada se elektronski dokazi pretražuju u odnosu na kriterijume koje identifikuju krivičnopravni organi. Isključivanje odbrane iz ovog procesa nije prihvatljivo, a treba obezbediti odgovarajuće zaštitne mere i mogućnosti za pronalaženje oslobađajućih dokaza.

Konačno, pojam „suda obrazovanog na osnovu zakona“, zajedno sa pojmovima „nezavisnosti“ i „nepristrasnosti“ suda, čine deo „institucionalnih uslova“ iz člana 6 EKLJP. U sudskoj praksi ESLJP postoji vrlo tesna međusobna veza između ovih pojmova.[61] Iako oni, kao različite garancije pravičnog suđenja, služe konkretnim ciljevima, postoji zajednička nit koja se provlači kroz te institucionalne uslove, a to je da su vođeni ciljem podržavanja osnovnih načela vladavine prava i podele vlasti.[62]

U predmetu *Sabo i Viši protiv Mađarske*, ESLJP je ponovio vezu između nezavisnosti sudskog nadzornog organa i prava na pravično suđenje.[63] Slično tome, SPEU je u svojoj sudskoj praksi identifikovao nadzor nad mehanizmima zadržavanja podataka kao važnu zaštitnu meru.

5.3 PRAVO NA SLOBODU IZRAŽAVANJA

ESLJP je više puta priznao da internet sadržaj koji kreiraju korisnici predstavlja platformu za ostvarivanje slobode izražavanja bez presedana.[64] Sud je, međutim, takođe podvukao opasnosti od nelegalnih sadržaja na internetu, uključujući dečju pornografiju, govor mržnje i govor koji podstiče nasilje.[65]

Istrage visokotehnološkog kriminala mogu da direktno ili indirektno utiču na pravo na slobodu izražavanja:

- do direktnog mešanja u pravo na slobodu izražavanja dolazi kada se blokiraju ili uklone internet stranice i sadržaj postane nedostupan zbog njegove nezakonite prirode (npr. dečija pornografija, onlajn tržišta nelegalnom robom i uslugama, govor mržnje);
- do indirektnog ometanja slobode govora može doći ako se na pružaoce usluga ili korisnike interneta vrši pritisak da cenzurišu sadržaj pod pretnjom sankcijama ili krivičnim postupkom.

60 ESLJP, *Sigurdur Einarson i drugi protiv Islanda*, 4. jun 2019, br. 39757/15, § 91; Vidi i: SE, Eksplanatorni izveštaj uz Konvenciju o visokotehnološkom kriminalu (Budimpešta, 2001), § 179.

61 ESLJP, Gudmundur Andri Astradson protiv Islanda [GC], 1. decembar 2020, br. 26374/18, § 218.

62 Ibid., §§ 218, 232, 233; Vidi i: SE, Eksplanatorni izveštaj uz Konvenciju o visokotehnološkom kriminalu (Budimpešta, 2001), § 70.

63 ESLJP, *Sabo i Viši protiv Mađarske*, 12. januar 2016, br. 37138/14.

64 Vidi ESLJP, Vodič za član 10 Evropske konvencije za zaštitu ljudskih prava, Sloboda izražavanja (Strazbur, 2022), §§ 588-632.

65 ESLJP, Delfi AS protiv Estonije [GC], 10. oktobar 2013, br. 64569/09, § 110; ESLJP, *Anen protiv Nemačke*, 20. septembar 2018, br. 3682/10, § 67.

Pored toga, istražitelji moraju da naprave ravnotežu između zaštite ličnih prava (npr. klevete) i potrebe za očuvanjem javne bezbednosti, sa jedne strane, i obaveze da obezbede slobodu govora, sa druge.

BLOKIRANJE PRISTUPA INTERNETU

Međunarodna tela za ljudska prava su više puta naglašavala da je blokiranje čitavih internet stranica, IP adresa, portova ili mrežnih protokola po nalogu države ekstreman potez koji je dozvoljen samo kao krajnja mera i ako se poštuju minimalne garancije pravičnog sudskog postupka.[66] Mere blokiranja internet stranica mogu biti u skladu sa međunarodnim standardima slobode izražavanja samo ako su predviđene zakonom i nužne i proporcionalne zaštiti legitimnih ciljeva.[67]

ESLJP je u svojoj praksi podvukao da blokiranje pristupa internetu može biti u direktnom sukobu sa stavom 1 člana 10 EKLJP, koji garantuje slobodu izražavanja „bez obzira na granice".[68] Predmet *Bulgakov protiv Rusije* odnosio se na blokiranje čitave internet stranice na osnovu naredbe suda zbog prisustva nelegalnog materijala (čak i pošto je taj materijal uklonjen). ESLJP je u svojoj presudi utvrdio da nije postojao zakonski osnov za naredbu za blokiranje, jer zakon na kojem se zasnivala naredba nije dozvoljavao organima vlasti da blokiraju pristup čitavoj internet stranici. Sud je takođe naveo da se njegov nalaz o nezakonitosti posebno odnosi na dalje blokiranje internet stranice nakon što je zabranjeni materijal uklonjen.

U posebnom predmetu, *Čengiz i drugi protiv Turske*, u vezi sa blokiranjem sajta za hosting video snimaka Jutjub, ESLJP je odlučio da podnosioci predstavke, koji su bili korisnici sajta, mogu legitimno da tvrde da je ta mera uticala na njihovo pravo da primaju i saopštavaju informacije ili ideje. S obzirom na jedinstvene karakteristike ove platforme, njenu dostupnost i, pre svega, njen potencijalni uticaj, kao i na to da podnosiocima predstavke nisu bile dostupne nikakve alternative, sud je utvrdio da je blokiranje narušilo njihovu slobodu izražavanja.[69]

ODGOVORNOST ZA ONLAJN SADRŽAJ

Iako je priznao važne koristi interneta za ostvarivanje slobode izražavanja, ESLJP smatra da, u principu, odgovornost za klevetu ili druge vrste nezakonitog govora mora biti zadržana i da predstavlja delotvoran pravni lek za kršenja prava ličnosti.[70]

Procenjujući da li vlasnik informativnog internet portala ima obavezu da ukloni komentare koje je objavila treća strana, u predmetu *Delfi AS protiv Estonije* sud je identifikovao četiri aspekta

66 Vidi UN OEBS predstavnik za slobodu medija i drugi, Zajednička deklaracija o slobodi izražavanja i "lažnim vestima", dezinformacijama i propagandi, 3. mart 2017, FOM.GAL/3/17

67 Vidi, npr. OEBS, Međunarodni standardi i komparativni pristupi slobodi izražavanja i blokiranju terorističkog i "ekstremističkog" sadržaja na internetu (Beč, 2018), st. 47; Vidi i: OEBS/ODIHR, Komentari na određene pravne akte koji regulišu masovnu komunikaciju, informacione tehnologije i korišćenje interneta u Uzbekistanu (Varšava, 2019), st. 86-89.

68 ESLJP, *Ahmet Jildrim protiv Turske*, 18. decembar 2012, br. 3111/10, § 67.

69 ESLJP, *Čengiz i drugi protiv Turske*, 1. decembar 2015, br. 48226/10 i 14027/11, §§ 52, 53, 55; Vidi i: ESLJP, *Ahmet Jildrim protiv Turske*, 18. decembar 2012, br. 3111/10, §§ 49, 55 o sličnom predmetu koji se odnosi na pristup internet stranici na hosting servisu Gugl sajts.

70 ESLJP, *Delfi AS protiv Estonije* [GC], 10. oktobar 2013, br. 64569/09, § 110.

relevantna za utvrđivanje odgovornosti pružalaca usluga za sadržaj na njihovim platformama:[71]

- kontekst komentara;
- mere koje je kompanija podnosilac predstavke primenila da bi sprečila ili uklonila klevetničke komentare;
- odgovornost stvarnih autora komentara u odnosu na odgovornost kompanije podnosioca predstavke;
- posledice domaćih sudskih postupaka po kompaniju podnosioca predstavke.

Razmotrivši ove aspekte, sud je naveo da, ako je praćen delotvornim postupcima koji omogućavaju brzu reakciju, sistem prijavljivanja i uklanjanja sadržaja može da obezbedi dovoljno uravnotežen pristup pravima trećih lica.[72] Pružaoci usluga se zato mogu osloniti na takav sistem bez direktne odgovornosti za sadržaj koji stvara korisnik, kao što su klevetnički komentari.[73] Međutim, sud je takođe podvukao da u slučajevima kao što je *Delfi AS protiv Estonije*, gde su komentari korisnika (trećih lica) u obliku govora mržnje i direktnih pretnji fizičkom integritetu fizičkih lica, pravima i interesima drugih lica, kao i društvu u celini, mogu da daju državama pravo da pozovu na odgovornost novinske internet portale ako bez odlaganja ne preduzmu mere za uklanjanje očigledno nezakonitih komentara, čak i bez obaveštenja od strane navodne žrtve ili trećih lica.

OKVIR **4** ODVRAĆAJUĆE DEJSTVO SLOBODE IZRAŽAVANJA

Ako se internet stranica sa video snimcima, na primer, suoči sa nejasnim propisima, može preterano da cenzuriše korisnike kako bi sprečila probleme sa državnim organima. Ovo dejstvo, koje se često naziva odvraćajućim dejstvom (eng. *chilling effect*), može se sprečiti postojanjem jasnih pravila, kao i mehanizama koji ograničavaju odgovornost pružalaca usluga u slučajevima kada se na njihovim platformama nalazi potencijalno nezakonit sadržaj bez njihovog znanja ili dozvole. Do efekta odvraćanja u pogledu slobode izražavanja može doći i ako ljudi primenjuju autocenzuru zbog nadzora ili iz straha da će biti predmet pogrešne sumnje. Ovo je, pak, često rezultat nejasnih ili proizvoljnih normi.

URAVNOTEŽENJE PRAVA NA SLOBODU IZRAŽAVANJA, PRIVATNOSTI I PREVENCIJE KRIMINALA

ESLJP se takođe bavio potrebom nalaženja ravnoteže između prava na slobodu izražavanja i privatnosti, s jedne strane, i odgovornosti država za sprečavanje i istraživanje krivičnih dela, sa druge. U predmetu *K.U. protiv Finske*, sud je smatrao da je nespojivo sa članom 8 EKLJP da pružalac usluga nema obavezu da otkrije identitet lica koje se traži zbog postavljanja nemoralnog

71 ESLJP, *Delfi AS protiv Estonije* [GC], 10. oktobar 2013, br. 64569/09, §§ 142-143; Vidi I: ESLJP, Magyar Tartalomszolgaltatok Egyesulete i Index.hu Zrt protiv Mađarske, 2. februar 2016, br. 22947/13, §§ 60 et seq.

72 ESLJP, *Delfi AS protiv Estonije* [GC], 10. oktobar 2013, br. 64569/09, § 159.

73 ESLJP, *Magyar Tartalomszolgaltatok Egyesulete i Index.hu Zrt protiv Mađarske*, 2. februar 2016, br. 22947/13, § 91; Vidi i: ESLJP, *Rolf Anders Daniel Pihl protiv Švedske*, 7. februar 2017, br. 74742/14, § 32; ESLJP, *Tamiz protiv Ujedinjenog Kraljevstva*, 19. septembra 2017, br. 3877/14, § 84; ESLJP, *Hoines protiv Norveške*, 19. mart 2019, br. 43624/14, §§ 73-74 u vezi sa važnošću blagovremene reakcije posle obaveštenja o nezakonitosti sadržaja.

oglasa o maloletniku na internet sajtu za upoznavanje, pozivajući se u ovom kontekstu na moguću pretnju fizičkoj i psihičkoj dobrobiti maloletnika i na osetljivost zbog njegove mladosti.[74] Sud je naglasio da, iako sloboda izražavanja i poverljivost komunikacije imaju nesumnjiv značaj i korisnici interneta moraju imati garanciju da će njihova sopstvena privatnost i sloboda izražavanja biti poštovani, takva garancija ne može biti apsolutna. Ona povremeno mora da propusti druge legitimne imperative, kao što su sprečavanje nereda ili kriminala, ili zaštita prava i sloboda drugih.[75]

Ukratko, sloboda izražavanja može biti ograničena samo na osnovu zakona. Zakonodavstvo treba da definiše precizna pravila i uslove za blokiranje i uklanjanje internet stranica ili sadržaja i da ograniči odgovornost pružalaca usluga za sadržaj koji stvaraju korisnici. Kada policija predloži neku meru u vezi sa nelegalnim sadržajem na internetu, a sud razmatra njeno odobravanje, on treba da detaljno proceni njen uticaj na slobodu izražavanja da bi se izbeglo preterano mešanje. Mora se uspostaviti ravnoteža, naročito u pogledu slobode medija i u slučajevima klevete ili govora mržnje, gde granice između navodno nezakonitog sadržaja i izražavanja mišljenja, kritike ili političkih stavova nisu uvek jasne. Odvraćajući efekat koji cenzura ima na društvo je još jedan važan aspekt (vidi okvir 4). Blokiranje internet stranica treba da bude strogo ograničeno na kriminalni sadržaj i ne treba da utiče na sadržaj koji nije nezakonit.

5.4 PRAVO NA ZAŠTITU IMOVINE

Istrage visokotehnološkog kriminala često uključuju virtuelnu imovinu, koja se može oduzeti privremeno, kao dokaz krivičnog dela, i/ili trajno, kao imovinska korist stečena izvršenjem krivičnog dela. Najčešća virtuelna imovina u ovom kontekstu su kriptovalute, koje se često koriste kao sredstvo plaćanja ilegalne robe koja se nudi na tržištima darknet-a ili za otkup u slučajevima ucenjivačkog softvera. Kriptovalute imaju tržišnu vrednost i zato se mogu smatrati „imovinom“ prema međunarodnim standardima.

Upotreba kriptovaluta ili druge virtuelne imovine nije sama po sebi nelegalna, iako u mnogim zemljama nije regulisana. Standardi za borbu protiv pranja novca Radne grupe za finansijsku akciju (FATF), međutim, zahtevaju regulisanje određenih aspekata kriptovaluta, a sve veći broj zemalja primenjuje pravila za pružaoce usluga kriptovaluta, na primer u vezi sa generisanjem novčanika, skladištenjem, menjanjem za dekretnu valutu ili druge kriptovalute ili virtuelnu imovinu.

ESLJP generalno smatra da privremeno i trajno oduzimanje predstavljaju kontrolu nad korišćenjem imovine, koju treba razmatrati na osnovu člana 1 (2) Protokola br. 1 uz EKLJP. Sud je ispitao različite mere koje su preduzete u cilju borbe protiv nezakonitog bogaćenja sticanjem imovinske koristi. Države imaju široka diskreciona ovlašćenja u sprovođenju politika za borbu protiv kriminala, uključujući i putem trajnog oduzimanja:

- imovine za koju se smatra da ima nezakonito poreklo;[76]

74 ESLJP, *K.U. protiv Finske*, 2. decembar 2008, br. 2872/02, § 41.

75 Ibid., § 49.

76 ESLJP, *Raimondo protiv Italije*, 22. februar 1994, br. 12954/87; *Riela i drugi protiv Italije*, 4. septembar 2001, br. 52439/99; ESLJP, *Arkuri i drugi protiv Italije*, 5. jul 2001, br. 52024/99; ESLJP, *Gogitidze i drugi protiv Gruzije*, 12. maj 2015, br. 36862/05 u vezi sa konfiskacijom sprovedenom u građanskom postupku; ESLJP, *Balsamo protiv San Marina*, 8. oktobar 2019, br. 20319/17 i 21414/17 u vezi sa postupkom za pranje novca.

- imovine koja je kupljena nezakonitim sredstvima;[77]
- imovinske koristi stečene krivičnim delom;[78]
- imovine koja je bila predmet krivičnog dela;[79]
- imovine koja je služila ili je trebalo da služi za izvršenje krivičnog dela.[80]

Koliko policija može da oduzme privremeno, a koliko sud može da oduzme trajno zavisi od nacionalnog režima oduzimanja, koji se može primeniti i na virtuelnu imovinu u pojedinačnom krivičnom predmetu.

ESLJP je razmatrao nekoliko predmeta koji se odnose na proporcionalnost i pravično suđenje u postupcima za oduzimanje imovine. U predmetu *Todorov i drugi protiv Bugarske*,[81] sud je utvrdio da je u četiri od sedam predstavki došlo do povrede člana 1 Protokola 1 uz EKLJP. Domaći sudovi nisu uspeli da utvrde vezu između oduzete robe i kriminalnih aktivnosti, ili između vrednosti imovine i razlike između prihoda i rashoda. Zbog toga je naredba za oduzimanje bila neproporcionalna.

U predmetu *Balsamo protiv San Marina*,[82] sud je potvrdio da su mere konfiskacije bile srazmerne, čak i bez osuđujuće presude kojom bi se utvrdila krivica okrivljenih i mada su takođe izrečene deci zbog kriminalne prošlosti njihovog oca. Za test proporcionalnosti smatralo se dovoljnim da pored velike verovatnoće da je poreklo imovine nezakonito, postoji i nemogućnost vlasnika da dokaže suprotno.

Predmet *Gogitidze i drugi protiv Gruzije*[83] odnosio se na meru oduzimanja imovine koja je pripadala bivšem zameniku ministra unutrašnjih poslova, koju je izrekao sud. ESLJP je utvrdio da je postignuta pravična ravnoteža između sredstava upotrebljenih za oduzimanje imovine podnosilaca predstavke i opšteg interesa u borbi protiv korupcije u javnoj službi. Podnosiocima predstavke nije uskraćena razumna prilika da iznesu svoj slučaj, a zaključci domaćih sudova nisu bili proizvoljni.

77 ESLJP, *Milorad Ulemek protiv Srbije*, 2. februar 2021, br. 41680/13.

78 ESLJP, *Filips protiv Ujedinjenog Kraljevstva*, 5. jul 2001, br. 41087/98; ESLJP, *Velč protiv Ujedinjenog Kraljevstva*, 9. februar 1995, br. 17440/90; ESLJP, Silikiene protiv Litvanije, 10. april 2012, br. 20496/02; ESLJP, *Gogitidze i drugi protiv Gruzije*, 12. maj 2015, br. 36862/05.

79 ESLJP, *Agosi protiv Ujedinjenog Kraljevstva*, 24. oktobar 1986, br. 9118/80.

80 ESLJP, *Andonoski protiv Bivše Jugoslovenske Republike Makedonije*, 17. septembra 2015, br. 14464/11; ESLJP, Todorov i drugi protiv Bugarske, 13. jul 2021, br. 50705/11 i 6 drugih.

81 *Todorov i drugi protiv Bugarske*, 13. jul 2021, br. 50705/11 i 6 drugih.

82 *Balsamo protiv San Marina*, 8. oktobar 2019, br. 20319/17 i 21414/17.

83 ESLJP, *Gogitidze i drugi protiv Gruzije*, 12. maj 2015, br. 36862/05.

6

Zaključak

Poštovanje ljudskih prava i vladavine prava je važan aspekt svakog demokratskog društva, a može da bude i uslov za zakonitost dokaza i pravičnost krivičnog postupka. To takođe utiče na poverenje koje građani imaju u javne institucije i u mnogim slučajevima predstavlja preduslov za obezbeđivanje međunarodne saradnje koja je ključna za efikasne istrage visokotehnološkog kriminala. Zato je važno da praktičari iz krivičnopravnih organa znaju i razumeju standarde ljudskih prava koji se primenjuju na različite faze i procese istrage visokotehnološkog kriminala.

Tokom istraga visokotehnološkog kriminala može se uticati na mnoga ljudska prava, uključujući i pravo na privatnost, pravično suđenje, slobodu izražavanja i zaštitu imovine. Svako mešanje u ljudska prava kod kojih su dozvoljena ograničenja tokom istraga o visokotehnološkom kriminalu mora biti **zasnovano na zakonu**, **nužno i proporcionalno**, i mora da teži **legitimnom cilju**, kao što je zaštita ljudskih prava žrtava ili drugih interesa društva.

Međunarodni i regionalni standardi ljudskih prava, kao i praksa međunarodnih sudova poput ESLJP, daju važna uputstva državama o tome kako da u praksi primene svoje obaveze u oblasti ljudskih prava u vezi sa istragama visokotehnološkog kriminala. To uključuje uspostavljanje domaćeg zakonodavstva koje će regulisati upotrebu istražnih ovlašćenja u skladu sa međunarodnim standardima i merama zaštite ljudskih prava, kao i obezbeđivanje da praktičari imaju znanje i veštine neophodne za održavanje ovih standarda tokom istraga o visokotehnološkom kriminalu.

7

Prilozi

PRILOG 1 RELEVANTNI ČLANOVI ICCPR I EKLJP

PRILOG 2 IZABRANA SUDSKA PRAKSA ESLJP

PRILOG 1 RELEVANTNI ČLANOVI ICCPR I EKLJP

PRAVO NA POŠTOVANJE PRIVATNOG I PORODIČNOG ŽIVOTA

Član 17 ICCPR

1. Niko ne može biti predmet samovoljnih ili nezakonitih mešanja u njegov privatni život, porodicu, stan ili prepisku, niti nezakonitih povreda nanesenih njegovoj časti ili ugledu.
2. Svako lice ima pravo na zaštitu zakona protiv ovakvih mešanja ili povreda.

Član 8 ICCPR

1. Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske.
2. Javne vlasti neće se mešati u vršenje ovog prava osim ako to je to u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih.

PRAVO NA PRAVIČNO SUĐENJE

Član 14 ICCPR

1. Svi su jednaki pred sudovima i tribunalima. Svako lice ima pravo da njegov slučaj bude raspravljan pravično i javno pred nadležnim, nezavisnim i nepristrasnim sudom, ustanovljenim na osnovu zakona koji odlučuje o osnovanosti svake optužbe podignute protiv njega u krivičnim stvarima ili o osporavanju njegovih građanskih prava i obaveza. Može se narediti isključivanje javnosti za vreme trajanja cele rasprave ili jednog dela u interesu morala, javnog reda ili nacionalne bezbednosti u demokratskom društvu, ili ako to interes privatnog života stranaka zahteva, ili još ako to sud smatra apsolutno potrebnim iz razloga posebnih okolnosti slučaja kada bi javnost štetila interesima pravde, ipak, svaka presuda doneta u krivičnim ili građanskim stvarima biće javna, osim ako interes maloletnika zahteva da se postupa drukčije ili ako se rasprava odnosi na bračne sporove ili na starateljstvo dece.
2. Za svako lice koje je optuženo za krivično delo pretpostavlja se da je nevino dok njegova krivica ne bude zakonski ustanovljena.
3. Svako lice koje je optuženo za krivično delo ima, uz potpunu ravnopravnost, prava na sledeće garancije:
   a. da bude obavešteno detaljno, u najkraćem roku, i na jeziku koji razume, o prirodi i razlozima optužbe koja je podignuta protiv njega;
   b. da raspolaže potrebnim vremenom i olakšicama u vezi sa pripremanjem svoje odbrane i da opšti sa braniocem koga ono bude izabralo;
   c. da mu bude suđeno bez velikog zakašnjenja;
   d. da prisustvuje raspravi i da se sam brani ili da ima branioca koga je izabralo; ako nema branioca, da bude obavešteno o svom pravu da ga ima i, svaki put kad to zahtevaju interesi pravde, da mu se dodeli branilac po službenoj dužnosti besplatno, ako nema

mogućnosti da ga nagradi;

e. da sasluša ili da predloži da drugi saslušaju svedoke koji terete optuženog i da izdejstvuje dolazak i saslušanje svedoka odbrane pod istim uslovima kao i svedoka optužbe;

f. da dobije besplatno pomoć tumača ako ne razume ili ne govori jezik na kojem se vodi rasprava;

g. da ne bude prinuđeno da svedoči protiv samoga sebe ili da prizna krivicu.

4. Postupak koji se vodi protiv maloletnih lica vodiće računa o njihovim godinama i o interesu njihovog prevaspitavanja.

5. Svako lice oglašeno krivim za počinjeno krivično delo ima pravo da zatraži da, shodno zakonu, viši sud ispita odluku o krivici i presudi.

6. Ako konačno izrečena krivična presuda bude kasnije poništena ili ako je dato pomilovanje zbog toga što nova ili naknadno otkrivena činjenica dokazuje da se radilo o sudskoj grešci, lice koje je izdržalo kaznu na osnovu ove osude biće obeštećeno shodno zakonu, ukoliko se ne dokaže da je ono u potpunosti ili delimično krivo za neblagovremeno otkrivanje nepoznate činjenice.

7. Niko ne može biti gonjen ili kažnjen zbog krivičnog dela u vezi kojeg je već bio oslobođen krivice ili osuđen pravnosnažnom presudom prema zakonu i krivičnom postupku svake zemlje.

Član 6 EKLJP

1. Svako, tokom odlučivanja o njegovim građanskim pravima i obavezama ili o krivičnoj optužbi protiv njega, ima pravo na pravičnu i javnu raspravu u razumnom roku pred nezavisnim i nepristrasnim sudom, obrazovanim na osnovu zakona. Presuda se izriče javno, ali se štampa i javnost mogu isključiti s celog ili s dela suđenja u interesu morala, javnog reda ili nacionalne bezbednosti u demokratskom društvu, kada to zahtevaju interesi maloletnika ili zaštita privatnog života stranaka, ili u meri koja je, po mišljenju suda, nužno potrebna u posebnim okolnostima kada bi javnost mogla da naškodi interesima pravde.

2. Svako ko je optužen za krivično delo smatraće se nevinim sve dok se ne dokaže njegova krivica na osnovu zakona.

3. Svako ko je optužen za krivično delo ima sledeća minimalna prava:

a. da u najkraćem mogućem roku, podrobno i na jeziku koji razume, bude obavešten o prirodi i razlozima za optužbu protiv njega;

b. da ima dovoljno vremena i mogućnosti za pripremanje odbrane;

c. da se brani lično ili putem branioca koga sam izabere ili, ako nema dovoljno sredstava da plati pravnu pomoć, da ovu pomoć dobije besplatno kada interesi pravde to zahtevaju;

d. da ispituje svedoke protiv sebe ili da postigne da se oni ispitaju i da se obezbedi prisustvo i saslušanje svedoka u njegovu korist pod istim uslovima koji važe za one koji svedoče protiv njega;

e. da dobije besplatnu pomoć prevodioca ako ne razume ili ne govori jezik koji se upotrebljava na sudu.

SLOBODA IZRAŽAVANJA

Član 19 ICCPR

1. Niko ne može biti uznemiravan zbog svojih mišljenja.
2. Svako lice ima pravo na slobodu izražavanja; ovo pravo bez obzira na granice, podrazumeva slobodu iznalaženja, primanja i širenja informacija i ideja svih vrsta, u usmenom, pismenom, štampanom ili umetničkom obliku, ili na bilo koji način po slobodnom izboru.
3. Ostvarivanje sloboda predviđenih u tački 2. ovog člana obuhvata posebne dužnosti i odgovornosti. Sledstveno tome, ono može biti podvrgnuto izvesnim ograničenjima koja moraju, međutim, biti izričito određena zakonom, a potrebna su iz razloga:
   a. poštovanja prava ili ugleda drugih lica;
   b. zaštite državne bezbednosti, javnog reda, javnog zdravlja i morala.

Član 10 EKLJP

1. Svako ima pravo na slobodu izražavanja. Ovo pravo uključuje slobodu posedovanja sopstvenog mišljenja, primanje i saopštavanja informacija i ideja bez mešanja javne vlasti i bez obzira na granice. Ovaj član ne sprečava države da zahtevaju dozvole za rad televizijskih, radio i bioskopskih preduzeća.
2. Pošto korišćenje ovih sloboda povlači za sobom dužnosti i odgovornosti, ono se može podvrgnuti formalnostima, uslovima, ograničenjima ili kaznama propisanim zakonom i neophodnim u demokratskom društvu u interesu nacionalne bezbednosti, teritorijalnog integriteta ili javne bezbednosti, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, zaštite ugleda ili prava drugih, sprečavanja otkrivanja obaveštenja dobijenih u poverenju, ili radi očuvanja autoriteta i nepristrasnosti sudstva.

PRAVO NA ZAŠTITU IMOVINE

Član 1 Protokola 1 uz EKLJP

1. Svako fizičko i pravno lice ima pravo na neometano uživanje svoje imovine. Niko ne može biti lišen svoje imovine, osim u javnom interesu i pod uslovima predviđenim zakonom i opštim načelima međunarodnog prava.
2. Prethodne odredbe, međutim, ni na koji način ne utiču na pravo države da primenjuje zakone koje smatra potrebnim da bi regulisala korišćenje imovine u skladu s opštim interesima ili da bi obezbedila naplatu poreza ili drugih dažbina ili kazni.

PRILOG 2 IZABRANA SUDSKA PRAKSA ESLJP

Benedik protiv Slovenije[84]

Ovaj predmet se odnosio na povredu prava na poštovanje privatnog života iz člana 8 EKLJP. Slovenačka policija je 2006. godine dobila informaciju od švajcarske policije o razmeni datoteka koje sadrže dečju pornografiju preko *peer-to-peer* internet stranice za razmenu datoteka. Među IP adresama koje je evidentirala švajcarska policija bila je i izvesna dinamička IP adresa u Sloveniji. U avgustu 2006. godine, slovenačka policija je, bez sudske naredbe, zatražila od slovenačkog pružaoca internet usluga (ISP) da obelodani podatke o korisniku kome je u dato vreme dodeljena ta dinamička IP adresa. Zahtev se zasnivao na odredbi Zakona o krivičnom postupku koja je omogućavala policiji da od pružaoca usluga elektronskih komunikacija zatraži podatke o korisniku određenog sredstva elektronske komunikacije čiji podaci nisu dostupni u odgovarajućem imeniku.

ISP je obezbedio ime i adresu pretplatnika koji se povezuje sa tom IP adresom. Nakon toga, u decembru 2006. godine, sud je izdao naredbu kojom se od ISP-a zahteva da otkrije i podatke o ličnosti i podatke o saobraćaju pretplatnika koji se povezuje sa tom IP adresom. Na osnovu dobijenih podataka, okružni sud je u januaru 2007. godine naredio pretres porodične kuće podnosioca predstavke. Tokom pretresa, oduzeti su računari sa pornografskim materijalom koji uključuje maloletnike.

U decembru 2008. godine, podnosilac predstavke je proglašen krivim za krivično delo prikazivanje, proizvodnja, posedovanje i distribucija pornografskog materijala. Osuđen je na uslovnu kaznu zatvora od osam meseci, sa rokom provere od dve godine. U novembru 2009. godine, u žalbenom postupku, Viši sud u Ljubljani je preinačio uslovnu kaznu podnosioca predstavke u zatvorsku kaznu od šest meseci.

Podnosilac predstavke je bezuspešno tražio pravni lek pred domaćim sudovima, tvrdeći da se privatnost prepiske i drugih sredstava komunikacije može suspendovati samo na osnovu naredbe suda i da zato bilo kakve nezakonito dobijene informacije treba izuzeti kao dokaz. Pritužba podnosioca predstavke odnosila se na prvi zahtev policije od ISP-a za identifikaciju korisnika IP adrese na osnovu Zakona o krivičnom postupku.

S tim u vezi, Ustavni sud je u februaru 2014. godine zaključio da su Ustavom zaštićeni i podaci o saobraćaju, odnosno svi podaci koji se obrađuju radi prenosa komunikacija u mreži za elektronsku komunikaciju. Sud je smatrao da su IP adrese uključene u takve podatke o saobraćaju i da bi inače bila potrebna naredba suda. Međutim, podnosilac predstavke, koji ni na koji način nije sakrio IP adresu preko koje je pristupio internetu, svesno se izložio javnosti i tako odrekao legitimnog očekivanja privatnosti. Usled toga, iako su podaci koji se odnose na identitet korisnika IP adrese u načelu zaštićeni Ustavom u okviru privatnosti komunikacije, Ustavni sud je odlučio da u slučaju podnosioca predstavke nije bila potrebna naredba suda za njihovo objavljivanje.

Kada je predmet iznesen pred ESLJP, Sud je zaključio da su zahtev policije upućen ISP-u i korišćenje informacija o pretplatniku koji su doveli do identifikacije podnosioca predstavke

84 ESLJP, *Benedik protiv Slovenije*, 24. april 2018, br. 62357/14; rezimirana u: ESLJP, Obaveštenje o praksi suda 217.

predstavljali mešanje u njegova prava na osnovu člana 8 EKLJP. Sud je primetio da su policijske mere imale osnov u domaćem zakonu. Kako relevantno zakonodavstvo nije bilo dosledno u pogledu stepena zaštite interesa privatnosti podnosioca predstavke, sud se oslonio na tumačenje Ustavnog suda, prema kojem je za obelodanjivanje informacija o pretplatniku povezanih sa određenom dinamičkom IP adresom u principu bila potrebna naredba suda, pošto su podaci o saobraćaju zaštićeni na osnovu Ustava. Što se tiče stava Ustavnog suda da se podnosilac predstavke u konkretnom slučaju odrekao legitimnog očekivanja privatnosti pošto ni na koji način nije sakrio IP adresu preko koje je pristupio internetu, ESLJP je ustanovio da to nije u skladu sa obimom prava na privatnost na osnovu EKLJP. Dakle, u ovom slučaju je bila neophodna naredba suda i ništa u domaćem zakonu nije sprečavalo policiju da je dobije.

ESLJP je ustanovio da zakonodavstvo, odnosno relevantne odredbe Zakona o krivičnom postupku (koje nisu sadržavale konkretna pravila u pogledu povezanosti između dinamičke IP adrese i podataka o pretplatniku), Zakona o elektronskim komunikacijama (koje su posebno regulisale tajnost i poverljivost elektronskih komunikacija) i Ustava (koji zahteva naredbu suda za bilo kakvo mešanje u privatnost komunikacije), nije dosledno u pogledu nivoa zaštite koji se obezbeđuje interesu privatnosti podnosioca predstavke.

U tom kontekstu, Sud je takođe primetio da u relevantno vreme nije postojao propis koji bi precizirao uslove za čuvanje podataka dobijenih na osnovu Zakona o krivičnom postupku i da postupak za pristupanje takvim podacima i njihovo prenošenje nije sadržavao mere zaštite od zloupotrebe od strane državnih službenika. U to vreme nije postojao nezavisni nadzor nad korišćenjem policijskih ovlašćenja u vezi sa dobijanjem informacija od ISP-a.

ESLJP je zato zaključio da zakon na kojem se zasniva osporena mera i način na koji su je primenili domaći sudovi nisu bili jasni i nisu ponudili dovoljne mere zaštite od proizvoljnog mešanja u član 8 EKLJP. Sud je ustanovio da mešanje u pravo podnosioca predstavke na poštovanje njegovog privatnog života nije bilo „u skladu sa zakonom“, kako se zahteva u članu 8 (2) Konvencije.

Nakon presude, slovenačka policija i tužioci su odmah promenili svoju praksu. Godine 2019. usvojene su izmene i dopune Zakona o krivičnom postupku da bi se preciziralo da se podaci o pretplatnicima mogu dobiti bez naredbe suda samo ako se ne analiziraju podaci o saobraćaju. U praksi to znači da je za pristup podacima o korisniku konkretne dinamičke IP adrese potrebna naredba suda. To nije slučaj kada su podaci o pretplatnicima uključeni u ugovor sa pružaocem usluga, na primer za broj mobilnog telefona ili statičku IP adresu.

U junu 2018. godine, gospodin Benedik je Vrhovnom sudu podneo zahtev za zaštitu zakonitosti, a u junu 2020. godine, Vrhovni sud je usvojio zahtev za zaštitu zakonitosti podnosioca predstavke, poništio pravnosnažnu presudu i vratio predmet Okružnom sudu u Kranju na ponovno suđenje. Okružni sud u Kranju je u maju 2021. godine obustavio krivični postupak protiv gospodina Benedika nakon što je Okružno tužilaštvo u Kranju povuklo optužnicu.

U zaključku, treba istaći da naredba suda za dobijanje podataka o korisniku (dinamičke) IP adrese kao uslov proizilazi iz slovenačkog Ustava i prakse slovenačkog Ustavnog suda i ne predstavlja međunarodni standard. Ovaj predmet takođe pokazuje važnost prava poštovanja privatnog života i dovoljne pravne jasnoće i adekvatne prakse prilikom mešanja u ljudska prava. Zbog povrede EKLJP u ovom predmetu, elektronski dokazi su izuzeti i obnovljeni krivični postupak je obustavljen.

Brejer protiv Nemačke[85]

Na osnovu izmena i dopuna nemačkog Zakona o telekomunikacijama iz 2004. godine, telekomunikacione kompanije su imale obavezu da prikupljaju i čuvaju lične podatke svih svojih korisnika, uključujući i korisnike pripejd SIM kartica, čak i kada to nije neophodno za potrebe izdavanja računa ili iz drugih ugovornih razloga, kao i da ih na zahtev učine dostupnim organima vlasti. Korisnici su kod pružalaca usluga morali da registruju lične podatke kao što su ime i adresa, brojevi telefona i datum rođenja. Oni su se žalili na to što se čuvaju njihovi lični podaci kao korisnika pripejd SIM kartica.

ESLJP je smatrao da nije došlo do povrede člana 8 EKLJP (pravo na poštovanje privatnog života). Sud je utvrdio da, u celini, Nemačka nije prekoračila granice svog diskrecionog prava („polja slobodne procene“) prilikom izbora sredstava za postizanje legitimnih ciljeva zaštite nacionalne bezbednosti i borbe protiv kriminala, kao i da je čuvanje podataka o ličnosti podnosilaca predstavke bilo proporcionalno i „neophodno u demokratskom društvu“. Dakle, nije došlo do povrede Konvencije.

Sud naročito smatra da prikupljanje imena i adresa podnosilaca predstavke kao korisnika pripejd SIM kartica predstavlja ograničeno mešanje u njihova prava. On je, međutim, primetio da taj zakon ima dodatne zaštitne mere i da se ljudi takođe mogu obratiti nezavisnim telima za nadzor nad podacima kako bi pregledali zahteve organa vlasti u pogledu podataka i po potrebi tražili pravni lek.

Što se tiče korišćenja uskladištenih podataka, te podatke mogu tražiti različiti javni organi bez naredbe suda ili obaveštavanja tih lica. Zahtevi za prikupljanje podataka mogu da pod određenim uslovima budu automatizovani i da za rezultat imaju liste koje se zasnivaju na pukoj sličnosti (upiti o delimičnim podacima) imena ili brojeva. Takvi zahtevi za informacijama bili su dozvoljeni kada se to smatralo neophodnim „za krivično gonjenje krivičnih dela i upravnih prekršaja, za otklanjanje opasnosti i za obavljanje obaveštajnih zadataka“.

Sud je naročito razmotrio dva glavna aspekta. Prvo, da li je mešanje bilo neophodno u demokratskom društvu i proporcionalno, uključujući i pitanje predvidljivosti i dovoljno detaljnih relevantnih odredbi. Sud je priznao da je to skladištenje, sa opšte tačke gledišta, prikladan odgovor na promene u ponašanju u pogledu komunikacije i u sredstvima telekomunikacije:

- Prethodna registracija pretplatnika mobilne telefonije u velikoj meri je pojednostavila i ubrzala istrage službi za sprovođenje zakona, i na taj način bi mogla da doprinese efikasnom sprovođenju zakona i sprečavanju nereda ili kriminala.
- Postojanje mogućnosti zaobilaženja zakonskih obaveza ne može biti razlog da se dovede u pitanje njihova ukupna korisnost i delotvornost.
- Pored nepostojanja konsenzusa, određeno polje slobodne procene opravdava i činjenica da su u pitanju zabrinutosti u pogledu nacionalne bezbednosti.

Drugi aspekt kojim se sud bavio odnosio se na pitanje da li je mešanje u pravo na privatni život bilo proporcionalno. Za razliku od predmeta koje je Sud prethodno ispitao, ovo skladištenje podataka nije uključivalo nikakve vrlo lične podatke niti je dozvoljavalo izradu profila ličnosti

85 ESLJP, *Brejer protiv Nemačke*, 30. januar 2020, br. 50001/12; rezimirana u: ESLJP, Obaveštenje o praksi suda 236.

ili praćenje kretanja pretplatnika. Štaviše, nisu bili skladišteni nikakvi podaci o pojedinačnim događajima u pogledu komunikacije. Iako nije bilo trivijalno, mešanje je zato bilo prilično ograničene prirode.

Što se tiče zaštitnih mera u vezi sa registracijom i skladištenjem podataka kao takvih, sud je primetio da:

- Podnosioci predstavke nisu tvrdili da je ovo skladištenje podlegalo bilo kakvim tehničkim nesigurnostima.
- Trajanje skladištenja je ograničeno na kalendarsku godinu posle godine u kojoj se ugovorni odnos završio; to nije izgledalo preterano, s obzirom na to da bi istrage o krivičnim delima mogle da potraju neko vreme i da traju i posle prestanka ugovornog odnosa.
- Sačuvani podaci bili su ograničeni na informacije koje su neophodne za jasnu identifikaciju relevantnog pretplatnika.
- Zahtevi za automatizovano prikupljanje podataka su, prema Zakonu o telekomunikacijama, ograničeni na konkretne organe za sprovođenje zakona i nacionalnu bezbednost. Zahtevi za manuelno prikupljanje podataka, s druge strane, nisu izričito navedeni, već se određuju na osnovu zadataka organa vlasti (npr. sprečavanje opasnosti, gonjenje krivičnih dela, sprovođenje propisa). Ovaj nivo detalja je adekvatan, bez obzira na nedostatak izričitog nabrajanja nadležnih organa.

Savezni ustavni sud Nemačke je takođe razmatrao pitanje da li postoje dovoljne zaštitne mere za mogući budući pristup sačuvanim podacima i njihovo korišćenje, naročito u pogledu sledećih aspekata:

- Nadležnost za upućivanje zahteva za pristup podacima: činjenica da postojeći zakon predviđa da se informacije mogu davati samo u meri u kojoj je to neophodno za obavljanje dužnosti već stvara objektivno ograničavajući faktor. To znači da je prikupljanje dozvoljeno samo kada se informacije koje su stvarno potrebne za obavljanje dužnosti ne mogu dobiti lakše, već jednako efikasno na drugačiji način. Zbog toga van ustavnog nivoa ne postoji zahtev da ovlašćeni organi budu izričito navedeni u zakonu.
- Svrha zahteva za pristup podacima: organi koji upućuju zahtev su morali da imaju dodatni pravni osnov za prikupljanje podataka (analogija sa sistemom dvokrilnih vrata[86]).
- Obim zahteva za pristup podacima: prikupljanje je bilo ograničeno na nužne podatke, sa opštom obavezom brisanja bez nepotrebnog odlaganja svih podataka koji organu koji je podneo zahtev nisu potrebni. Pored toga, uslov „nužnosti“ nije bio sadržan samo u posebnim zakonskim odredbama koje su predmet ove žalbe, već i nemačkom i evropskom zakonu o zaštiti podataka.
- Kontrola i nadzor zahteva za pristup podacima: iako je odgovornost za zakonitost zahteva za pristup podacima na samim službama za prikupljanje, Savezna agencija za mreže se smatra nadležnom za nezavisno ispitivanje zakonitosti prenosa podataka kada uviđa razloge za to. Prema opštim pravilima se takođe može tražiti i pravna zaštita od prikupljanja informacija. S obzirom na te puteve kontrole, neobaveštavanje o postupku prikupljanja nije predstavljalo problem na osnovu Konvencije.

86 Razmena podataka se odvija kroz zadiranja prikupljanja i prenosa, koji se podudaraju i od kojih svaki zahteva nezavisan pravni osnov. Figurativno govoreći, zakonodavac mora ne samo da otvori krilo za prenos podataka, već i krilo za njihovo prikupljanje. Samo oba pravna osnova zajedno, koji moraju da zajedno funkcionišu kao dvokrilna vrata, daju ovlašćenje za razmenu podataka o ličnosti.

ESLJP je potvrdio odluku nemačkog Saveznog ustavnog suda da nije došlo do kršenja ljudskih prava i naglasio važnost zakonskih ograničenja i zaštitnih mera u okviru nacionalnog polja slobodne procene kako bi se zadovoljila načela proporcionalnosti i nužnosti u demokratskom društvu. Konkretno, našao je da je zakonska obaveza pružalaca usluga da čuvaju podatke o ličnosti korisnika pripejd SIM kartica za mobilne telefone i da ih na zahtev učine dostupnim organima vlasti srazmerna legitimnim ciljevima zaštite nacionalne bezbednosti i borbe protiv kriminala, kao i da je prikupljanje podataka od strane organa vlasti bilo praćeno adekvatnim zaštitnim merama.

Roman Zakharov v. Russia[87]

Podnosilac predstavke, koji je bio glavni i odgovorni urednik izdavačke kuće, pokrenuo je sudski postupak protiv tri operatera mobilnih mreža, tvrdeći da je došlo do mešanja u njegovo pravo na privatnost telefonskih komunikacija. Tvrdio je da su, shodno relevantnom domaćem zakonu, operateri mobilnih mreža instalirali opremu koja je omogućila Federalnoj službi bezbednosti presretanje svih telefonskih komunikacija bez prethodnog sudskog odobrenja. Tražio je da sud izda naredbu za uklanjanje opreme i da se pristup telekomunikacijama obezbedi samo ovlašćenim licima.

Domaći sudovi su odbili tužbeni zahtev podnosioca predstavke i našli da nije dokazao da su njegovi telefonski razgovori bili presretnuti ili da su operateri mobilnih mreža preneli zaštićene informacije neovlašćenim licima. Domaći sudovi su takođe našli da mu instaliranje opreme o kojoj je govorio samo po sebi nije narušilo privatnost komunikacije.

ESLJP je našao da je postojanje spornog zakona o presretanju mobilnih telefonskih komunikacija samo po sebi predstavljalo mešanje u ostvarivanje prava podnosioca predstavke na osnovu člana 8. Sud je razmotrio više aspekata mešanja u član 8:

- **Zakonitost:** presretanje mobilnih telefonskih komunikacija imalo je osnovu u domaćem zakonu i težilo je ostvarivanju legitimnih ciljeva zaštite nacionalne bezbednosti i javnog reda i mira, sprečavanja kriminala i zaštite ekonomske dobrobiti zemlje.
- **Dostupnost:** zakonske odredbe su zvanično objavljene i bile su dostupne javnosti.
- **Obim primene mera tajnog nadzora:** priroda krivičnih dela koja bi mogla da daju povod za izdavanje naredbe za presretanje bila je dovoljno jasna. Međutim, obim je bio preširok i presretanje se moglo narediti i za lica koja nisu osumnjičena ili optužena.
- **Trajanje mera tajnog nadzora:** zakon je sadržavao jasna pravila o trajanju i produženju mere presretanja, ali ne i o njenom prekidu.
- **Postupci** za, između ostalog, čuvanje i uništavanje presretnutih podataka: automatsko čuvanje u trajanju od šest meseci očigledno nerelevantnih podataka ne može se smatrati opravdanim prema članu 8.
- **Odobravanje presretanja:** presretanje je morao da odobri sud, ali ruske sudije nisu dobile uputstvo da provere postojanje „razumne sumnje“ protiv tog lica ili da primene testove „nužnosti“ i „proporcionalnosti“. Zakon nije sadržavao nikakve uslove u pogledu sadržaja zahteva ili odobrenja za presretanje. U nekim naredbama nije pominjano konkretno lice ili broj telefona,

87 ESLJP, *Roman Zaharov protiv Rusije*, 4. decembar 2015, br. 47143/06; rezimirana u: ESLJP, Obaveštenje o praksi suda 191.

niti trajanje nadzora. Prema domaćem zakonu nije postojala obaveza da se sudsko odobrenje pokaže pružaocu komunikacionih usluga pre dobijanja pristupa komunikacijama.

- **Nadzor:** nadzorni organ nije mogao da otkrije presretanja koja su izvršena bez propisnog odobrenja suda, što, zajedno sa tehničkom sposobnošću organa za sprovođenje zakona da direktno presretnu komunikaciju, čini aranžmane nadzora neefikasnim. Tužilački nadzor je bio ograničen.
- **Obaveštavanje o presretanju i dostupni pravni lekovi:** lica čija je komunikacija presretnuta nisu obaveštena.

Pravni lekovi na koje se poziva Vlada stajali su na raspolaganju samo licima koja poseduju informacije o presretanju njihove komunikacije. Njihova delotvornost je narušena zbog nepostojanja obaveze obaveštavanja lica čija je komunikacija presretnuta ili adekvatne mogućnosti traženja i dobijanja informacija o presretanju od organa vlasti. Shodno tome, ruski zakon nije predviđao delotvoran pravni lek protiv mera tajnog nadzora u slučajevima kada nije pokrenut krivični postupak protiv lica čija je komunikacija presretnuta.

Kao takve, odredbe domaćih zakona koje regulišu presretanje komunikacija ne pružaju adekvatne i delotvorne garancije zaštite od proizvoljnosti i rizika zloupotrebe. Domaći zakon ne ispunjava zahtev „kvaliteta zakona“ i nije u stanju da svede „mešanje“ na ono što je „nužno u demokratskom društvu“. Svojom presudom, ESLJP je postavio precizne standarde i test usaglašenosti za zakonodavstvo u slučaju masovnog nadzora.

K.U. protiv Finske[88]

U ovom predmetu, ESLJP je raspravljao o pozitivnim obavezama država članica u pogledu delotvorne zaštite privatnog života (privatnosti) i upotrebe podataka o komunikaciji u predmetima koji se odnose na elektronske dokaze i visokotehnološki kriminal. U ovom predmetu se radilo o dvanaestogodišnjem dečaku iz Finske čiji su podaci podeljeni protiv njegove volje na internet stranici za upoznavanje i koga je kontaktirala odrasla osoba. Jasno je da je takav (seksualni) kontakt u to vreme bio protivzakonit, pogotovo što je učinilac ostao anoniman.

Kada su finske vlasti pokušale da procesuiraju ovaj predmet, nisu mogle da dobiju podatke o učiniocu od pružaoca usluga internet stranice za upoznavanje. Pružalac usluga, na osnovu finskih propisa, nije mogao da otkrije identitet korisnika na zahtev policije. Sud je to ocenio i našao da finski zakonodavac nije preduzeo dovoljne mere da reši takvu situaciju.

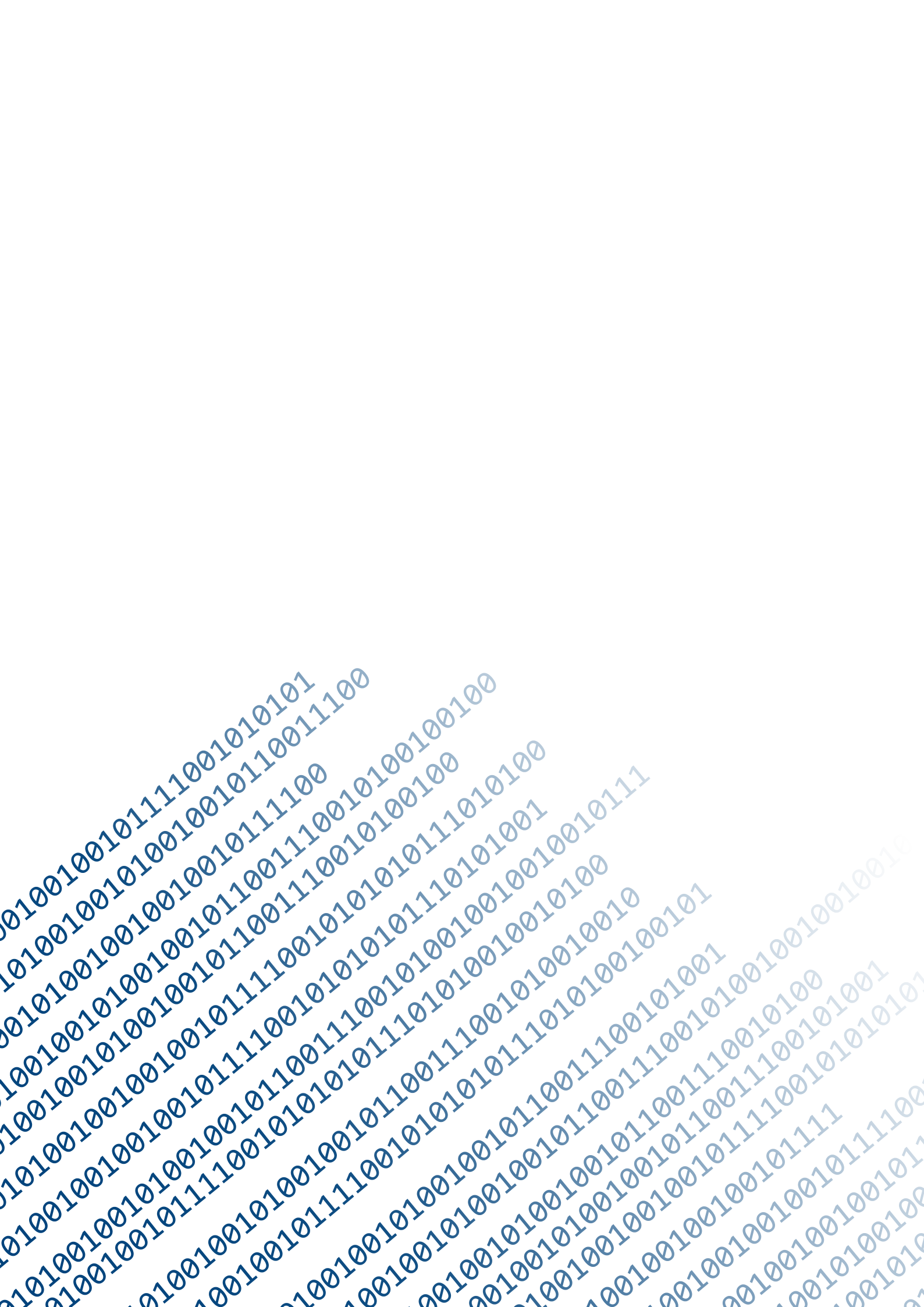
Presuda je glasila: „Sud smatra da je praktična i delotvorna zaštita podnosioca predstavke zahtevala da se preduzmu delotvorni koraci u cilju identifikacije i krivičnog gonjenja učinioca, tj. lica koje je postavilo oglas. U predmetnom slučaju, takva zaštita nije pružena. Delotvorna istraga nikada ne bi mogla da se pokrene zbog pretežnog zahteva poverljivosti.

Iako su sloboda izražavanja i poverljivost komunikacija prvenstvene brige i korisnici telekomunikacionih i internet usluga moraju imati garanciju da će njihova privatnost i sloboda izražavanja biti poštovani, takva garancija ne može biti apsolutna i mora povremeno da popusti pred drugim

88 ECtHR, *K.U. v. Finland*, 2 December 2008, No. 2872/02; summarized in: ECtHR, Information Note on the Court's caselaw 114.

legitimnim imperativima, kao što su kao sprečavanje nereda ili krivičnih dela, ili zaštita prava i sloboda drugih."

Sud je zato zaključio da u predmetu K.U. nije moglo da se delotvorno postupa u okviru postojećeg pravnog okvira, što je dovelo do povrede pozitivne dužnosti države da zaštiti K.U. od ovakvog ponašanja. Država nije uspela da zaštiti pravo K.U. na poštovanje privatnog života tako što je obavezi poverljivosti dala prednost nad njegovom fizičkom i moralnom dobrobiti.



OEBS
Organizacija za evropsku
bezbednost i saradnju