UDK 343.14:004.056(497.5)
342.722:343.14(497.5)
Primljeno 6. studenoga 2023.
Izvorni znanstveni rad
DOI 10.54070/hljk.30.2.2

Dr. sc. Zoran Burić *
Dr. sc. Marc Engelhart **
Dr. sc. Ante Novokmet ***
Dr. sc. Sunčana Roksandić ****

UPOTREBLJIVOST REZULTATA MASOVNOG NADZORA KOMUNIKACIJA KAO DOKAZA U HRVATSKOM KAZNENOM POSTUPKU – SLUČAJ *SKY ECC*

U radu se analizira mogu li se i u kojoj mjeri informacije prikupljene kroz masovni nadzor komunikacija upotrijebiti kao dokaz u hrvatskom kaznenom postupku. Radi se o informacijama koje su prikupljene u Francuskoj kroz zajednički istražni rad francuskih, nizozemskih i belgijskih nadležnih tijela, uz pomoć i suradnju Europola i Eurojusta. Primarna specifičnost ovih informacija temelji se na činjenici da se ne radi o podacima koji su prikupljeni kroz ciljani nadzor unaprijed određenog broja osoba osumnjičenih za kriminalne aktivnosti, već o informacijama koje su prikupljene kroz nadzor svih korisnika određene komunikacijske mreže – Sky ECC – *koja je, temeljeći se na kriprografiji, jamčila svojim korisnicima popunu zaštitu privatnosti, bez mogućnosti njezina vanjskog nadzora, uključujući i od strane tijela kaznenog progona, te je bila na tržištu dostupna svakome tko ju je želio kupiti kroz registriranu zakonitu djelatnost. Pitanje zakonitosti dokaza razmatra se primarno kroz prizmu činjeničnih i pravnih okolnosti pribavljanja informacija u Francuskoj i njihova transfera u Hrvatsku. U odnosu na*

* Dr. sc. Zoran Burić, izvanredni profesor na Katedri za kazneno procesno pravo, Sveučilište u Zagrebu Pravni fakultet; zoran.buric@pravo.unizg.hr; https://orcid.org/0000-0001-5353-8478

** Dr. sc. Marc Englehart, odvjetnik i naslovni profesor, Sveučilište Ludwiga Maximiliana u Münchenu, Pravni fakultet; marcengelhart@googlemail.com; ORCID iD: https://orcid.org/0000-0001-8848- 5468

*** Dr. sc. Ante Novokmet, izvanredni profesor na Katedri kaznenopravnih znanosti, Sveučilište u Osijeku, Pravni fakultet Osijek; ante.novokmet@pravos.hr; https://orcid.org/0000-0001-8833-9751

**** Dr. sc. Sunčana Roksandić, izvanredna profesorica na Katedri za kazneno pravo Pravnog fakulteta Sveučilišta u Zagrebu, predstojnica Katedre za kazneno pravo; suncana.roksandic@pravo.unizg. hr; https://orcid.org/0000-0003-3523-6032

pravne okolnosti posebna je pažnja posvećena standardima koje vezano uz pribavljanje i transfer dokaza propisuje pravo EU-a.

Ključne riječi: Sky ECC, masovni nadzor komunikacija, dokazi pribavljeni u inozemstvu, nezakoniti dokazi u kaznenom postupku

1. UVOD

Sky ECC bila je aplikacija za sigurno dopisivanje,[1] koju je razvila kanadska kompanija *Sky Global* (Vancouver). Kao i sve ostale aplikacije za sigurno dopisivanje, bila je namijenjena svima zainteresiranima za maksimalnu sigurnost i privatnost.[2] U trenutku kada su istražitelji uspjeli razbiti zaštitu koju je aplikacija pružala i ostvariti nadzor nad komunikacijom korisnika, radilo se o najvećoj svjetskoj mreži korisnika kriptiranih uređaja. Da bi aplikacija to omogućila, trebalo ju je koristiti uz odgovarajući modificirani uređaj, a postojala je i licenca koja je omogućavala korištenje aplikacije za određeno vrijeme (3, 6 ili više mjeseci). Cijena licence bila je od 600 do 2200 eura. *Sky ECC* nije prva ni jedina aplikacija za sigurno dopisivanje. Radilo se o proizvodu koji je bio legalno proizveden i plasiran na tržište te je bio

[1] Ovaj se članak temelji, osim na istraživanju mjerodavne sudske prakse i stručnih i znanstvenih radova objavljenih u zadnjih godinu dana, na zajedničkom pravnom mišljenju autora, koje je zatražio branitelj Ljubo Pavasović Visković. Tijekom 2022. godine zatraženo je pravno mišljenje vezano uz (ne)dopustivost korištenja i (ne)zakonitost dokaza pribavljenih u inozemstvu kroz masovni nadzor komunikacija u hrvatskom kaznenom postupku. Ujedno je zatražena i analiza vezana uz uporabu aplikacija *Sky* i ANOM u poredbenom pravu s obzirom na snažno izraženi međunarodni element u izradi i korištenju obiju aplikacija i njihovo globalno korištenje, odnosno prosljeđivanje prikupljenih informacija u razne nacionalne države. Kako navedeni način prikupljanja i transferiranja informacija predstavlja novinu ne samo u RH nego i globalno, izv. prof. dr. sc. S. Roksandić, nakon identificiranja pravnog problema od strane odvjetnika Pavasovića, oformila je (nad)nacionalni tim stručnjaka u sastavu autora.

[2] Više o samoj aplikaciji i načinu pristupa raznih nacionalnih zakonodavstva, kao i prava EU-a, ovoj problematici v. Zimmermann, F., *Die Verwertbarkeit von Auslandsbeweisen im Lichte der EncroChat-Ermittlungen*, Zeitschrift für internationale Strafrechtswissenschaft (ZflStW), vol. 1, br. 2, 2022, str. 173–190, Sagittae, G., *On the lawfuness of the EncroChat and Sky ECC-operations,* New Journal of European Criminal Law 2023, vol. 14, br. 3, str. 273–293; Oerlemans, J.; Royer, S., *The future of dana driven investigations in light of the Sky ECC operation*, New Journal of European Criminal Law, 2023, vol. 0, br. 0, str. 1–25; Stoykova, R. (A.), *Enchrochat: The hacker with a warrant and fair trials?*, Forensic Science International: Digital Investigation, vol. 46, 2023; Bajović, V., *Encrochat i sky ecc komunikacija kao dokaz u krivičnom postupku*, CRIMEN, vol. XIII, br. 2, 2022, str. 154–179; Simović, M., Šikman, M., *Sadržaj šifrovane komunikacije (Ennercom, Encrochat, Sky.ecc, Anom, Exclu) kao dokaz u krivičnom postupku*, Pravo i pravda, vol. 21, br 1, str. 227–254; v. također Bachmaier, L., *Mutual Admissibility of Evidence and electronic Evidence in the EU*, Eucrim (2 11. 2023.).

zakonito dostupan svima onima koji su bili zainteresirani za takvu vrstu komunikacijske usluge.[3]

Interes za nadzor nad *Sky ECC*-jem pojavio se kod belgijskih nadležnih tijela nakon što su uvidjeli da su uređaji osumnjičenika zaplijenjeni tijekom njihovih akcija bili opremljeni tom aplikacijom. Prema podacima Europola tu je aplikaciju koristilo više od 170 000 ljudi diljem svijeta. Nakon što su došla do početnih saznanja da aplikaciju, između ostalih, koriste i pripadnici organiziranih kriminalnih skupina, belgijska nadležna tijela, u suradnji s francuskim i nizozemskim, i uz pomoć Europola i Eurojusta, krenula su u akciju masovnog nadzora nad komunikacijom više od 70 000 korisnika aplikacije. Pritom se nije radilo o ciljanom nadzoru samo onih korisnika u odnosu na koje je postojala sumnja da se bave kriminalnim aktivnostima, već o nadzoru svih osoba koje su u kritičnom periodu aplikaciju koristile. Kao dio početne operacije 9. ožujka 2021. u Belgiji i Nizozemskoj provedeno je više pretraga, brojne su osobe uhićene i zaplijenjena je značajna imovina.[4] Tehnički detalji o operaciji zasad su jedva poznati. Postoje neka izvješća – nepotvrđena – da vlasti namjerno stavljaju na tržište uređaje s manipuliranim verzijama izvornog softvera. Tvrtka je navodno prestala s radom 19. ožujka 2021. *Web*-stranicu preuzeo je FBI.[5] U ožujku 2021. Europol je objavio da je zajednički istražni tim sastavljen od belgijskih, francuskih i nizozemskih policijskih vlasti pratio razmjenu poruka više od 70 000 korisnika *Sky ECC*-ja i na sigurnom mjestu pohranio odgovarajući sadržaj presretnutih komunikacija.[6] Prema informacijama iz njemačkog kaznenog postupka francuski sud u Lilleu – isti kao i onaj u slučaju *EncroChat*[7] – odobrio je presretanje

[3] Sva komunikacija bila je zaštićena 512-bitnom eliptičnom zakrivljenom kriptografijom, za koju je tvrtka jamčila da pruža sigurnu komunikaciju, a sama aplikacija omogućava dodatnu sigurnost, kao što je šifrirani ulazak u aplikaciju, samouništavajuće poruke te tajna lozinka za samouništenje u slučaju kompromitacije korisnika aplikacije. Njome se upravljalo iz SAD-a i Kanade, uz korištenje računalnih poslužitelja u Europi. Više od 20 posto korisnika nalazilo se u Belgiji i Nizozemskoj. V. Cox, J., *Belgian Police Say They Decrypted Half a Billion 'Sky' Messages, Arrested 48 People*, 10. ožujka 2021., dostupno na: https://www.vice.com/en/article/7k9yjx/sky-ecc-decrypted-hacked-police-say-billion-messages.

[4] EUROPOL, New major interventions to block encrypted communications of criminal networks, dostupno na: https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks.

[5] V. poruku FBI-a na izvornoj stranici http:// Sky ECC.com/.

[6] EUROPOL, *ibid*.

[7] *EncroChat*, nizozemska tvrtka sa središnjim poslužiteljem u Roubaixu, bila je jedna od najvećih svjetskih kompanija koja je nudila kriptiranu komunikaciju. Oglašavala se na svojoj početnoj stranici, uz jamstvo anonimnosti. Kriptirani uređaji prodavali su se za oko 1000 € (i više), pri čemu je u tu cijenu bila uključena korisnička licenca u trajanju od 6 mjeseci. Tvrtka je imala više od 60 000 kupaca diljem svijeta. U mjeri u kojoj je javnosti poznato, uređaji su korišteni za nekriminalne, kao i za kriminalne aktivnosti. Šifrirani kontakt, osiguran

komunikacije s poslužitelja smještenog – kao i u slučaju *EncroChat* – u Roubaixu (Francuska).[8]

U SAD-u su J-F. Eap, glavni izvršni direktor *Sky Globala*, i T. Herdman, bivši distributer uređaja *Sky Globala*, uhićeni i optuženi za zavjeru za kršenje federalnog *Racketeer Influenced and Corrupt Organizations Act*.[9] Glavna je optužba da su svjesno i namjerno sudjelovali u zločinačkom pothvatu koji je omogućio transnacionalni uvoz i distribuciju narkotika prodajom i servisom kriptiranih komunikacijskih uređaja.[10]

Nakon zajedničke operacije opsežni set podataka nadležna francuska tijela kaznenog progona dostavila su pojedinim europskim zemljama. Količina prikupljenih podataka navodno je četiri puta veća od podataka prikupljenih u akciji *EncroChat*. Čini se da je svaka zemlja primila potpunu presretnutu komunikaciju kako bi mogla sama filtrirati relevantne podatke; ovo se razlikuje od slučaja *EncroChat*, gdje je svaka država primila informacije povezane s njezinim teritorijem. Zbog velike količine informacija npr. Udruga njemačkih sudaca očekivala je velik broj istraga i sudskih postupaka.[11] Svaki korisnik *Sky ECC*-jeve kriptirane komunikacijske platforme prilikom registracije na platformu dobivao je jedinstvenu oznaku (*userId*), odnosno PIN, koji ostaje nepromijenjen. Osim toga, svaki korisnik mogao je odabrati korisničko ime, koje se može promijeniti u bilo kojem trenutku, tako da jedna osoba može koristiti isti PIN s različitim korisničkim imenima. Dakle, radi identifikacije osoba iza određenih PIN kodova spisu francuskih vlasti priloženo je Izvješće o

putem unaprijed instalirane aplikacije, mogao se odvijati samo između korisnika. Funkcije na posebnom hardveru također su omogućile dotičnom korisniku da postavi individualne postavke za brisanje svoje poruke. Primjenom posebne lozinke cijeli fond podataka uređaja mogao se odmah izbrisati. Pored toga bili su predviđeni daljnji mehanizmi za sprječavanje manipulacije uređajima izvana. Pozadina istrage francuskih tijela kaznenog progona bilo je 7 tekućih istraga u Francuskoj protiv osumnjičenih trgovaca drogom, pri čemu su istražitelji pretpostavili da su koristili *EncroChat* uređaje za izvršenje svojih djela. Francuske su vlasti potom provele opću istragu zbog sumnje u formiranje zločinačke organizacije, kao i zbog navodnih kaznenih djela u vezi s prijenosom i uvozom uređaja za šifriranje (čl. 13. Décret br. 2007-663 od 2. svibnja 2007.). O međupovezanosti pravorijeka više država v. Ledwick Law: *Enchrochat: How France's Supreme Court Decicison affects the UK,* dostupno na: https://www.eldwicklaw.com/encrochat-uk-french-supreme-court-decision/ (22. 12. 2022.).

[8] V. izjavu o činjenicama u predmetu Oberlandesgericht (dalje: OLG) Celle, Beschluss v. 15. 11. 2021. – 2 HEs 24-30/21.

[9] United States Attorney's Office Southern District of California, *Sky Global Executive and Associate Indicted for Providing Encrypted Communication Devices to Help International Drug Traffickers Avoid Law Enforcement*, dostupno na: https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices (12. 3 2021.).

[10] *Ibid*.

[11] Süddeutsche Zeitung, 15. studenog 2021., *Richter: Polizei soll Millionen Krypto-Handys-Chats kriegen*,

identifikaciji kako bi se omogućila identifikacija pojedinih osoba koje su koristile mrežu *Sky ECC* za kriptiranu komunikaciju pod određenim PIN kodom.

U RH postoji niz slučajeva vezanih uz *Sky ECC*. U više kaznenih predmeta USKOK je, na temelju kaznene prijave PNUSKOK-a i rezultata dokaznih radnji pribavljenih putem pravosudne suradnje s više država, Eurojustom i Europolom, pokrenuo istragu koristeći pritom informacije i podatke pribavljene putem europskog istražnog naloga.[12] Radi se o informacijama i podacima koji su prikupljeni na temelju presretanja, prikupljanja i snimanja računalnih podataka te tehničkog snimanja i tajnog nadzora nad platformom i serverom *Sky ECC*.

Cilj je ovog rada istražiti predstavljaju li informacije koje su nadležna hrvatska tijela pribavila putem pravosudne suradnje u kaznenim stvarima zakonite dokaze u postupcima pred hrvatskim sudovima ili postoje razlozi zbog kojih ih valja smatrati nezakonitim dokazima.[13] Drugim riječima, mogu li se na njima temeljiti sudski nalozi za poduzimanje dokaznih radnji i rješenja o oduzimanju slobode te druge sudske odluke, kao što su rješenje o potvrđivanju optužnice i presuda.[14] U tom se smislu najprije analiziraju zakonitost tajnog

[12] V. ne samo za Hrvatsku nego i za Srbiju, Bosnu i Hercegovinu te Crnu Goru: Jakelić, Jovanović (Vijesti), Brkić – Čekić (Oslobođenje), Jeremić (Danas), *Kako je policija hakiranjem aplikacije Sky razbila kriminalnu scenu u Hrvatskoj, BiH, Srbiji i Crnoj Gori*, Večernji list, 6. studenog 2022. Dostupno na: https://www.vecernji.hr/vijesti/kako-je-policija-hakiranjem-aplikacije-sky-razbila-kriminalnu-scenu-u-hrvatskoj-bih-srbiji-i-crnoj-gori-1631400.

[13] Osim u slučaju *SkyECC* ta se pitanja postavljaju i za slučajeve aplikacija *EncroChat* i ANOM. U slučajevima *EncroChat* i *Sky ECC* podatke su prikupljali strana policijska i državna tijela. U slučajevima *EnchoChat* i *Sky ECC* riječ je prvenstveno o francuskim vlastima (*Sky ECC* u suradnji s belgijskim i nizozemskim vlastima). Predmeti otvaraju i najmanje tri aspekta: namjerno zaobilaženje hrvatskih proceduralnih standarda, opasnost od *patchwork* pristupa i dozvoljenost tajnog (masovnog) elektroničkog nadzora. Osim namjernog zaobilaženja nacionalnih kongentnih pravnih standarda ostaje situacija da nacionalne vlasti namjerno iskorištavaju miješanje pravila postupanja iz različitih sustava kaznenih postupaka. Ovaj problem postaje očit kada miješanje različite procesne norme stvara situaciju u kojoj su posebno smanjena prava obrane jer se primjenjuju pravila različitih pravnih sustava s različitim mehanizmima zaštite. Npr. Gleß, S., *Zum Prinzip der gegenseitigen Anerkennung,* Zeitschrift für Internationale Strafrechtsdogmatik (ZStW), vol. 116, 2004, str. 354–356, str. 352 (365 f.); Satzger, H., *Gefahren für eine effektive Verteidigung im geplanten europäischen Verfahrensrecht – eine kritische Würdigung des Grünbuchs zum strafrechtlichen Schutz der finanziellen Interessen der Europäischen Gemeinschaften und zur Schaffung einer europäischen Staatsanwaltschaft* (StV), vol. 23, 2003, str. 137, 140 f.; Schünemann, Ein Gespenst geht um in Europa – Brüsseler „Strafrechtspflege" intra muros, Goltdammers Archiv, vol. 151, 2002, str. 501–516; Schuster, Frank P., *Verwertbarkeit von Beweismitteln bei grenzüberschreitender Strafverfolgung*, Zeitschrift für internationale Strafrechtsdogmatik, vol. 11, br. 8, 2016, str. 572 f., Zimmermann, F., *op. cit.* u bilj. 2, str. 173, 185.

[14] I provedena istraživanja pokazuju da unatoč načelnoj naklonosti dokazima iz inozemstva države članice još uvijek žele imati mogućnost odbiti koristiti neki dokaz ako je prikupljanje takva dokaza bilo u suprotnosti s temeljnim načelima njihova pravnog poretka. Vermeulen,

nadzora u državama u kojima je proveden te zakonitost transfera tako prikupljenih stranih dokaza u Republiku Hrvatsku. Potom se daje osvrt na mogućnost zakonitog korištenja tih dokaza u postupcima pred hrvatskim sudovima s obzirom na dva ključna aspekta: 1. odstupa li način na koji su pribavljeni ti dokazi suštinski u većoj mjeri od temeljnih načela domaćeg kaznenog zakonodavstva, i 2. na koji se način uporaba tako pribavljenog dokaza u kaznenom postupku odražava na prava obrane i pravičnost postupka.[15]

Osim pitanja koja su predmet ovog članka, postavlja se i pitanje povrede prava na privatnost, prava na pravično suđenje (čl. 6. EKLJP-a) i prava na učinkovitu pravnu zaštitu, uključivo i mogućnost okrivljenika da dobije učinkovitu sudsku zaštitu u prekograničnim predmetima.

Pitanje koje se dakle također postavlja jest jesu li mjere nadzora u predmetima koje se tiču presretanja i dekodiranja aplikacija *EncroChat*, *ANOM*[16] i *Sky*

G. *et al*. EU *Cross Border Gathering and Use of Evidence in Criminal Matters. Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence?* Maklu, 2010, str. 150–151.

[15] Potrebno je napomenuti da vezano uz informacije koje su pribavljene masovnim nadzorom komunikacija postoji cijeli niz drugih pitanja u kontekstu upotrebljivosti rezultata tih radnji kao dokaza u kaznenom postupku, a koja se ne obrađuju u ovom radu. Pitanje vjerodostojnosti tih informacija kao dokaza, koje je vezano uz način na koji su iz ukupne količine pribavljenih informacija izdvojene baš one za koje je zaključeno da su kaznenopravno relevantne. Pitanje sukladnosti prikupljanja, analize, transfera i uporabe ovih informacija iz aspekta prava na zaštitu privatnosti, posebice zaštitu osobnih podataka, v. Oerlemans, J.; Royer, S., *The future of data driven investigations in light of the Sky ECC operation*, New Journal of European Criminal Law, vol. 0: Ahead of Print, 2023, str. 1–25.

[16] Godine 2018. uhićen je V. Ramos, koji je bio osnivač i izvršni direktor kriptiranog *messengera Phantom Secure*, koji su koristile organizirane kriminalne skupine. Nakon toga FBI je razvio ANOM u suradnji s povjerljivim hakerom, koji je prethodno radio na *PS* (kao i na *Sky Global*) i dobio oprost za svoje sudjelovanje. FBI je pokrenuo operaciju Trojanski štit, koja je uključivala distribuciju navodno sigurne aplikacije diljem svijeta uz pomoć hakera i, između ostalog, australskih tijela kaznenog progona. Prodan je u više od 90 zemalja, a najviše se koristio u Njemačkoj, Nizozemskoj, Španjolskoj, Australiji i Srbiji. Više od 20 milijuna poruka na više od 11 800 uređaja bilo je presretnuto. "Pretplata" za korištenje iznosila je u Europi otprilike 1000–1500 eura za 6 mj. korištenja. FBI se u ljeto 2019. godine obratio nepoznatoj trećoj (europskoj) zemlji, koja je postavila vlastiti poslužitelj i omogućila FBI-u da prima nove podatke s poslužitelja ANOM-a putem sudskog naloga svakog ponedjeljka, srijede i petka u okviru međunarodne pravne pomoći. Prvim sudskim nalogom FBI je bio ovlašten primati podatke od 7. 10. 2019. do 7. 1. 2020. i na temelju dodatnog sudskog naloga do 7. 6. 2021. Primljeno je više od 20 milijuna poruka s oko 12 000 uređaja u više od 100 država. U to vrijeme sam FBI nije imao pristup podacima ANOM-a, barem službeno. Softver na kripto telefonima bio je programiran tako da se kopija svake poslane poruke potajno šalje na poslužitelj izvan SAD-a (poslužitelj u nepoznatoj trećoj zemlji), gdje je prvo dešifrirana, a zatim ponovno šifrirana FBI-evim kodom i proslijeđena na sljedeći poslužitelj. Poruke korisnika koji su bili u SAD-u automatski su filtrirane (jer bi inače nadzor vlastitih građana bio nedopustiv). Ostale zemlje, iako su bile uključene u tekuću operaciju, bile su obaviještene u prilično kasnoj fazi

ECC kršile opseg zaštite iz čl. 8. EKLJP-a te čl. 7. Povelje EU-a. Glavno pitanje u vezi s tim jest jesu li mjere nadzora od strane istražnih tijela predstavljale legitimno ograničenje prava na privatnost. U svakom slučaju, čini se da bez detalja o tehničkoj provedbi pojedinih operacija nije moguće prosuditi zakonitost izvorne mjere, utvrditi opseg i učinkovitost potrebnih prethodnih sudskih kontrola, odrediti mjere za zaštitu privatnih podataka. Nužno je utvrditi je li takvim privatnim podacima pristupljeno nezakonito i prenose li se prikupljeni podaci stvarno bez ikakvih smetnji (kako bi se isključila mogućnost manipulacije, uključujući i izostavljanje relevantnih podataka u korist okrivljenika).

2. PRIKUPLJANJE INFORMACIJA MASOVNIM NADZOROM KOMUNIKACIJA U INOZEMSTVU

2.1. Masovni nadzor komunikacija i europski pravni standardi

Polazišna osnova za razmatranje pravnih posljedica upotrebljivosti provedenih radnji u hrvatskim predmetima koji se temelje na informacijama i podacima pribavljenim putem *Sky ECC*-ja jest kontekst u kojem su prikupljene. Taj su kontekst operativne (prikrivene) radnje i mjere koje po naravi stvari značajno ograničavaju temeljna ustavna prava i slobode građana.[17] Na delikatnost određivanja posebnih dokaznih radnji, zbog toga što se njihovom primjenom zadire u ustavna prava i slobode građana, upućuje i judikatura ESLJP-a, koja je nastala povodom tužbi pojedinaca zbog povreda prava na slobodu, prava na pravičan postupak i prava na zaštitu privatnosti (čl. 5., 6. i 8. EKLJP-a). Ista je postavila određene postulate za dopustivost posega državnih vlasti u temeljna prava i slobode građana: a) poseg mora biti poduzet na temelju norme zakonskog ranga, b) poseg mora biti poduzet s legitimnim ciljem,[18] c) poseg mora

operacije. (Glavne informacije navedene u ovom dijelu proizlaze iz odgovora na parlamentarni zahtjev savezne vlade u Njemačkoj. ANOM dodatno postavlja pitanja granica dopustivost radnji agenata provokatora, koje prelaze opseg ovog rada. V. Bundestag, -Drucksache 20/1249; v. također Klaubert, D., Organisierte Kriminalität in der Falle, FAZ online, dostupno na: https://www.faz.net/aktuell/gesellschaft/kriminalitaet/kryptodienst-anom-organisierte-kriminalitaet-in-der-falle-17741919.html?premium (27. 10. 2023.). Detaljnije informacije mogu se pronaći u javno objavljenoj optužnici od 28. svibnja 2021. u predmetu *USA v. Ayik et al*., US District Court, Southern District of California, predmet br. '21 CR1623 JLS.).

[17] Ljubanović, V., Novokmet, A., Tomičić, Z., *Kazneno procesno pravo*, Grafika, Osijek, 2020, str. 181–182.

[18] Prema čl. 8. st. 2. EKLJP-a legitimni su ciljevi ograničenja prava na zaštitu osobnosti, državna sigurnost, javni red i mir, gospodarska dobrobit zemlje, sprečavanje nereda i zločina, zaštita zdravlja ili morala, zaštita prava i slobode drugih ljudi.

prema težini biti razmjeran legitimnom cilju,[19] d) poseg mora biti nužan u demokratskom društvu, e) poseg mora biti poduzet na način čiji dokazni rezultati ne narušavaju „pravičnost postupanja" državnih vlasti prema osumnjičeniku ili okrivljeniku u konkretnom slučaju.[20]

Odluka tijela kaznenog progona u predmetima *Sky ECC* i ANOM da provedu generalni nadzor nad cjelokupnom mobilnom mrežom i da preusmjere kompletnu komunikaciju na sigurni poslužitelj koji će poslužiti za dekriptiranje podataka otvara niz problema ne samo iz aspekta toga što je tim činom kompromitirana kompletna digitalna komunikacijska infrastruktura nego i iz perspektive zaštite ljudskih prava, posebno u pogledu zaštite privatnosti i pretpostavke nedužnosti.[21] U slučaju *Sky ECC* zajednički istražni tim (JIT), koji je uključivao francuska, nizozemska i belgijska tijela kaznenog progona, nije se koncentrirao samo na dekriptiranje sadržaja komunikacije osoba za koje su prethodno utvrdili postojanje određenog stupnja vjerojatnosti sumnje da su počinitelji kaznenog djela nego su odlučili dekriptirati cijelu telefonsku mrežu pretpostavljajući da su svi korisnici *Sky ECC* bili kriminalno povezani.[22] Stoga se kao ključno pokazuje pitanje je li takav vid masovnog presretanja, premda možda određen i proveden na temelju norme zakonskog ranga, doista bio poduzet s legitimnim ciljem, je li prema težini bio razmjeran legitimnom cilju, je li bio nužan u demokratskom društvu i jesu li pri takvu postupanju prikupljeni dokazi pribavljeni na način da ne narušavaju „pravičnost postupanja" državnih vlasti prema osumnjičeniku ili okrivljeniku u konkretnom slučaju. Ujedno, poznato je da su aplikaciju *Sky ECC*, koja je legalno stavljena na tržište, koristile i osobe izvan okruženja organiziranog kriminaliteta.

Na neka od ovih pitanja nedavno je prve odgovore dao ESLJP u predmetu *Big Brother Watch and Others v. UK*.[23] Predmet se odnosio na pritužbe od strane novinara i organizacija za ljudska prava u vezi s tri različita nadzora: (1) masovno presretanje komunikacija; (2) primitak presretnute komunikacije od stranih vlada i obavještajnih agencija; (3) pribavljanje komunikacijskih podatka od pružatelja komunikacijskih usluga.

[19] To znači da poseg ne smije premašiti ono što je nužno potrebno; ako se legitimni cilj može postići blažim posegom, onda teži poseg nije dopušten jer nije razmjeran. Usp. Chantal, J., *Judicial Control of Foreign Evidence in Comparative Perspective*, 2005, str. 98–99.

[20] Taj uvjet navodi Krapac na temelju slučaja Francisco Teixeira de Castro protiv Portugala. V. Krapac, D. *Pogled na neke važnije odredbe novog hrvatskog kaznenog zakonodavstva o organiziranom kriminalitetu i pitanja njihove praktične primjene*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 5, br. 2, 1998, str. 528 i d.

[21] V. osobito Watt, E., *The right to privacy and the future of mass surveillance*, The International Journal of Human Rights, vol. 21, br. 7, 2017, str. 773–799.

[22] Usp. Pisarić, M., *Encryption as a challenge for European law enforcement agencies*, Australasian Policing, vol. 10, br. 1, 2021, str. 611–615.

[23] *Big Brother Watch and Others v. the United Kingdom*, zahtjevi br. 58170/13, 62322/14 i 24960/15, 25. svibnja 2021.

Veliko vijeće donijelo je oglednu presudu o uvjetima i pretpostavkama koje moraju biti ispunjene da bi se masovno presretanje smatralo usklađenim s konvencijskim standardima.[24] Određena jasna jamstva moraju postojati. Sud je prepoznao razliku između nadzora pojedinačnih komunikacija i masovnog presretanja komunikacija korištenjem metapodataka te je odredio niz proceduralnih jamstava koja se moraju poštivati u početnoj, središnjoj i završnoj fazi nadzora prikupljenih podataka. Naglasio je da takav sistem mora biti podložan „*end-to-end* zaštitnim mjerama"; na nacionalnoj razini u svakoj fazi postupka treba procijeniti neophodnost i proporcionalnost mjera koje se poduzimaju; da bi masovno presretanje trebalo na početku biti predmet nezavisnog odobrenja, kada su definirani cilj i opseg operacije; i da operacija treba biti predmetom kontrole tijekom provođenja i *ex post facto* nadzora. ESLJP je odredio osam kriterija kao osnovu na temelju koje se procjenjuje zakonitost, osnovanost i svrhovitost provođenja mjera masovnog presretanja telekomunikacija: a) razlozi pod kojima se može dopustiti masovno presretanje; b) okolnosti u kojima se komunikacija pojedinca može presresti; c) postupak koji treba prethoditi davanju odobrenja za presretanje; d) postupci koje treba slijediti za odabir, provjeru i korištenje presretnute komunikacije; e) mjere opreza koje je potrebno poduzeti prilikom dostavljanja presretnute komunikacije trećim osobama; f) ograničenje trajanja presretanja, pohranjivanje presretnutog materijala i okolnosti u kojima se takav materijal mora izbrisati i uništiti;[25] g) postupci i modaliteti za nadzor od strane neovisnog tijela nad poštivanjem gore navedenih zaštitnih mjera i njegove ovlasti u slučaju utvrđenih pogrešaka u postupanju; h) neovisna *ex post facto* kontrola postupanja i ovlasti povjerenih nadzornom tijelu u rješavanju slučajeva nepoštivanja zaštitnih mjera (§ 361.).[26]

Valja istaknuti kako će za sve nacionalne predmete koje uključuju dekripciju *Sky ECC*-jevih uređaja biti od velike važnosti ishod predmeta pred ESLJP-om *A. L. v. Francuske* i *E. J. v. Francuske*.[27] Ti se predmeti posebno odnose

[24] Schaar, P., *ECHR: Mass surveillance by British secret service violated European Convention on Human Rights*, u: T. Kahler (ur.), Turning Point in Data Protection Law, Nomos, str. 63–66.

[25] Što se tiče korištenja umjetne inteligencije u navedenim postupcima, ona bi trebala biti dopuštena u skladu s propisanim pravilima. V. i Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy artificial intelligence and its use by law enforcement authorities: where do we stand*, u: Vrcek, N, *et al*. (ur.), 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Croatian Society for Information, Communication and Electronic Technology – MIPRO, 2022, str. 1395–1402.

[26] Usp. Vincent, S., *Preventing the Police State: International Human Rights Laws Concerning Systematic Government Access to Communications Held or Transmitted by the Private Sector*, u: Cate, F. H; Dempsey, J. X. (ur.), Bulk Collection: Systematic Government Access to Private-Sector Dana, New York, 2017, 355–380.

[27] *A. L. protiv Francuske*, zahtjev br. 44715/20, i *E. J. protiv Francuske*, zahtjev br. 47930/21.

na infiltraciju francuskih vlasti u šifriranu komunikacijsku mrežu *EncroChat* i snimanje, kopiranje i analizu podataka pohranjenih i razmijenjenih s uređajima povezanima na tu mrežu. ESLJP je obavijestio francusku vladu o zahtjevima i postavio pitanja strankama prema čl. 6. st. 1., čl. 8., čl. 13., čl. 34. i čl. 35. EKLJP-a. Naravno, rješenja nacionalnih predmeta ovisit će i o nacionalnom zakonodavstvu i reguliranosti takva načina nadzora u kaznenom postupku te o regulaciji ovlasti tzv. dozvoljenog policijskog hakiranja.[28]

2.2. Normativna podloga masovnog nadzora komunikacija u inozemstvu

Kad se primijene spomenuti konvencijski standardi na slučaj *Sky ECC*, može se utvrditi da je provođenje masovnog presretanja komunikacija bilo utemeljeno na članku 706-102-1 francuskog Zakona o kaznenom postupku. Konkretno, navedena je odredba propisana u okviru Poglavlja 4: Posebni postupci, Naslov XXV: Posebni postupci koji se primjenjuju na kaznena djela organiziranog kriminaliteta, Poglavlje II: Postupak (članci 706-80 do 706-106), Odjeljak 6: Druge posebne istražne tehnike, Stavak 4: Snimanje računalnih podataka (članci 706-102-1 do 706-102-5).[29] Kako je francuski ZKP očito dozvolio tajno masovno presretanje komunikacije, zahtjev za postojanjem „a) razloga pod kojima se može dopustiti masovno presretanje" podrazumijeva da domaće pravo mora biti ne samo dostupno, a njegova primjena predvidljiva, nego i da se njime mora osigurati da se mjere tajnog nadzora primjenjuju samo kada je to „neophodno u demokratskom društvu", konkretno tako što će u njemu biti propisane odgovarajuće i djelotvorne mjere zaštite i garancije

[28] U tome prednjači npr. Nizozemska. Zakon *Wet Computercriminaliteit III*, koji je na snazi od ožujka 2019. godine (v. https://www.simmons-simmons.com/en/publications/ck0bi-70lg7kew0b94qi4inld1/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force (27. 10. 2023.), ima za cilj poboljšati učinkovitost u borbi protiv kibernetičkog kriminala i u tu svrhu mijenja različite odredbe nizozemskog Kaznenog zakona i Nizozemskog zakona o kaznenom postupku. Ovaj je zakon stvoren kako bi se uhvatio u koštac s brzim razvojem tehnologije, interneta i kibernetičkog kriminala nastavljajući regulaciju koja je prvi put postavljena u Zakonu o računalnom kriminalu I iz 1993. i konsolidirana u Zakonu o računalnom kriminalu II iz 2006. Zakon regulira i „ovlast hakiranja", moć da se sadržaj učini nedostupnim, kriminalizaciju prikupljanja i nuđenja internetskih (ukradenih) podataka i (proširenu) kriminalizaciju internetske komercijalne prijevare te *groominga*. Da se radi o iznimno važnom pitanju, vidljivo je i iz Izvještaja Europskog parlamenta iz 2017. godine, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, dostupno na: https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf. (27. 10. 2023.).

[29] Usp. Vullierme, L. N., *Data Protection in the Internet: French report*, u: D. M. Vicente, S. de Vasconcelos Casimiro, Data Protection in the Internet, Springer, 2019, str. 174.

od zloupotreba. Domaći je zakon ispunio navedene pretpostavke propisujući da sudac sloboda i pritvora može na prijedlog državnog odvjetnika ili sam sudac istrage nakon konzultacija s državnim odvjetnikom (članak 706-95-12) odrediti primjenu posebnih istražnih tehnika, a među njima snimanje računalnih podataka (članak 706-102-1), i to pisanim i obrazloženim nalogom, s upućivanjem na činjenične i pravne elemente koji opravdavaju da su takvi postupci potrebni (članak 706-95-13) za taksativno navedeni krug kaznenih djela iz članka 706-73 i 706-73-1. U pogledu „b) okolnosti u kojima se komunikacija pojedinca može presresti" zakonska je odredba prilično široka i omogućava postavljanje tehničkog uređaja čija je svrha omogućiti bez pristanka pristup, bilo gdje, računalnim podacima, njihovo snimanje, pohranjivanje i prijenos, kao i da se pohranjuju u računalni sustav (članak 706-102-1). Iz navedenog je vidljivo da se ne traže niti jasno opisuju osobe ni predmet presretanja ili skup uređaja u odnosu na koje će se presretanje provesti. U nedostatku bilo kakva ograničenja broja komunikacija koje su mogle biti presretnute čini se da su presretnuti svi paketi komunikacija koji su tekli preko platforme *Sky ECC* dok je nalog bio na snazi. Jasno je da u konkretnom slučaju presretanje komunikacije nije bilo određeno prema osobi ili skupini osoba, nego prema cjelokupnoj platformi koja je pružala usluge sigurne komunikacije. „c) Postupak koji treba prethoditi davanju odobrenja" proveden je pred sucem istrage, koji je pisanim i obrazloženim nalogom odredio provođenje predloženih mjera. Odluka kojom se odobrava primjena tih mjera morala je sadržavati kazneno djelo zbog kojeg se primjenjuju takve mjere, točnu lokaciju ili detaljan opis sustava automatizirane obrade podataka, kao i trajanje mjera (članak 706-102-3). Kako je riječ o mjerama koje podrazumijevaju visokotehnološko znanje i sposobnosti za dekriptiranje podataka, tada je u okviru zahtjeva koji se odnose na „d) postupak koji treba slijediti za odabir, provjeru i korištenje presretnute komunikacije" u članku 706-102-1 propisano da će državni odvjetnik ili sudac istrage imenovati bilo koju fizičku ili pravnu osobu ovlaštenu i upisanu na jednu od lista iz čl. 157. radi obavljanja tehničkih poslova kojima se omogućuje realizacija naloženih istražnih mjera. Očito je intencija zakonodavca bila da se angažmanom stručne osobe tako presretnut materijal može odabrati, ispitati, koristiti i pohraniti kako bi se očuvala objektivnost provedenog postupka. Kada je riječ o „e) mjerama opreza koje je potrebno poduzeti prilikom dostavljanja presretnute komunikacije trećim osobama", domaći zakon ne propisuje na koji bi se način presretnuti materijal sačuvao od kasnije manipulacije. U domaćem pravu nije propisan siguran način dostavljanja stranom obavještajnom partneru, državi ili međunarodnoj organizaciji prikupljenih podataka. Dokumentacija iz predmeta *Sky ECC* dostavljena je širokom krugu obavještajnih partnera i drugih država, a prethodno nije utvrđeno da obavještajni partner, odnosno država, pri rukovanju prikupljenim materijalom ima uspostavljene zaštitne mjere koje mogu spriječiti zlouporabu i nerazmjerno uplitanje, a posebice omogućiti si-

gurno skladištenje materijala i ograničiti njegovo daljnje objavljivanje. Zahtjev za „f) ograničenje trajanja presretanja, pohranjivanja presretnutog materijala i okolnosti u kojima se takav materijal mora izbrisati i uništiti" proveden je na način da je u općim odredbama definiran najdulji rok primjene posebnih istražnih tehnika za kaznena djela počinjena u sastavu kriminalne organizacije. Posebne istražne tehnike odvijaju se pod ovlasti i kontrolom suca koji ih je odredio i koji u svakom trenutku može naložiti njihov prekid. Ako sudac smatra da radnje nisu provedene u skladu s donesenim nalogom ili da nisu poštivane važeće odredbe zakona, obrazloženim nalogom naložit će uništavanje zapisnika i napravljenih snimaka. Trajanje ove istražne metode ograničeno je općom odredbom da tijekom preliminarnih istraživanja (izvida) ova mjera može po odluci „suca za slobodu i pritvor" trajati mjesec dana i može se produljiti za još mjesec dana, dok tijekom formalne istrage sudac istrage može odrediti ovu mjeru najviše četiri mjeseca i može se produljiti pod istim uvjetima za još četiri mjeseca (706-95-16 i 706-95-12). Snimke i podaci prikupljeni tijekom posebnih istražnih radnji uništavaju se po nalogu državnog odvjetnika istekom roka zastare javnog djelovanja i o tome se sastavlja zapisnik (706-95-19). Kad je riječ o „g) postupcima i modalitetu nadzora od strane neovisnog tijela nad poštivanjem zaštitnih mjera i njegovoj ovlasti u slučaju utvrđenih pogrešaka u postupanju" i „h) neovisnoj *ex post facto* kontroli postupanja i ovlasti povjerenih nadzornom tijelu u rješavanju slučajeva nepoštivanja zaštitnih mjera", potrebno je istaknuti da francuski ZKP propisuje da se posebne istražne tehnike određuju i odvijaju pod isključivim ovlaštenjem i kontrolom suca koji ih je odredio. Taj sudac može u svakom trenutku naložiti prekid provođenja radnji (706-95-14). Budući da posebne istražne tehnike određuje sudac i da zadržava permanentnu internu kontrolu nad njihovim provođenjem, može se konstatirati da je osiguran najviši stupanj neovisne kontrole nad određivanjem i provođenjem naloženih radnji.

2.3. Posebni zahtjevi iz pozicije prava EU-a (Direktiva 2014/41/EU)

U odnosu na *SkyECC*, budući da je nadzor provođen ne samo nad osobama koje su bile locirane u Francuskoj već i nad osobama koje su se u trenutku nadzora nalazile na teritoriju drugih država članica, pa i Hrvatske, za pitanje zakonitosti nadzora relevantna je ne samo pozicija francuskoga prava već i pozicija prava Europske unije.

U odnosu na pravo EU-a temeljni pravni izvor koji regulira pitanja transnacionalnog nadzora jest Direktiva 2014/41/EU. Prema čl. 31. Direktive, kada nadležno tijelo jedne države članice („država članica koja presreće") odobri presretanje telekomunikacija u svrhu izvršavanja istražne mjere, a adresa subjekta presretanja za komunikaciju navedena u nalogu za presretanje koristi se na državnom području druge države članice („obaviještena država članica"),

čija tehnička pomoć nije potrebna za izvršenje presretanja, država članica koja presreće obavješćuje nadležno tijelo obaviještene države članice o presretanju.[30] Koji je smisao takva obavještavanja, jasno proizlazi iz odredbe čl. 42.an st. 3. Zakona o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije. Prema toj odredbi, nakon što je o takvu nadzoru subjekta koji se nalazi u Hrvatskoj obaviješten Županijski sud u Zagrebu kao domaće tijelo nadležno za zaprimanje obavijesti o nadzoru, taj sud dužan je bez odgode, a najkasnije u roku od 96 sati od primitka obavijesti, obavijestiti nadležno tijelo države članice koja nadzire da se nadzor ne može izvršiti ili da se prekida, odnosno da se sav prethodno nadzirani materijal dok se subjekt nadzora nalazio na državnom području Republike Hrvatske ne može upotrijebiti kao dokaz u kaznenom postupku. Iz te je odredbe vidljivo da je smisao obavještavanja da se nadležnom hrvatskom tijelu dade prilika da iskontrolira provodi li se nadzor u skladu s onim što je iz aspekta temeljnih načela hrvatskog pravnog poretka prihvatljivo. Nastavno, propisani rok od 96 sati upravo služi navedenoj svrsi. Koliko je iz informacija predmeta poznato, nadležno tijelo Republike Hrvatske nije bilo obaviješteno o tome da su nadzoru podvrgnuti i subjekti koji su se u trenutku nadzora nalazili na teritoriju Republike Hrvatske, čime ne samo što je postupljeno protivno čl. 31. Direktive već je i domaće nadležno tijelo onemogućeno u obavljanju svoje Zakonom o pravosudnoj suradnji dodijeljene zadaće.

Njemačka iskustva pokazuju da se njihovi sudovi do sada nisu pozivali na kršenje Direktive o EIN-u kao argument za neprihvatljivost dokaza, već su zauzimali stav da pravila ili uopće nisu primjenjiva ili – čak i ako jesu – ne predviđaju zabranu korištenja pribavljenih dokaza.[31] Savezni sud posebno se osvrnuo na čl. 31. Direktive 2014/41/EU i pokrenuo nekoliko pitanja u vezi s tim: je li čl. 31. namijenjen zaštiti pojedinaca, je li nadzor telekomunikacija uopće obuhvaćen (ili se čl. 31. bavi drugim aspektima), štiti li čl. 31. pojedinca samo od upotrebe dokaza u državi koja provodi istragu (jer njegova država nije bila obaviještena), a ne – kao u ovom slučaju – od upotrebe u državi primateljici dokaza (ovdje: Njemačka).[32] Sud nije odlučivao o ovim pitanjima, ali je ustvrdio da čak i ako čl. 31. predviđa mehanizam zaštite pojedinca za presretanje komunikacije u Njemačkoj, interesi države za kaznenim progonom

[30] Guerra, J., Janssens Ch., *Legal and Practical Challenges in the Application of the European Investigation Order*, Eucrim, br. 1, 2019, str. 51.

[31] V. u predmetu *EncroChat*: OLG Schleswig-Holstein, odluka od 29. 4. 2021. – 2 Ws 47/21, par. 25., i OLG Celle, odluka od 12. 8. 2021. – 2 Ws 250/21, par. 37., odbacuju zabranu dokaza budući da europsko pravo izričito ne predviđa takvu posljedicu; OLG Hamburg, Beschluss v. 29. 1. 2021. – 1 Ws 2/21, Rn. 105, i OLG Karlsruhe, odluka od 10. 11. 2021. – 2 Ws 261/21, par. 33., naglašavaju aspekt zaštite državnog suvereniteta, KG Berlin, Beschluss v. 30. 8. 2021. – 2 Ws 93/21, par. 52., obveza prvenstveno omogućuje državama članicama da jamče tajnost komunikacije.

[32] Bundesgerichtshof (dalje: BGH), odluka od 2. 3. 2022. – 5 StR 457/21, para. 39.–45.

prevladali bi nad kršenjem prava pojedinca i dopustili korištenje informacija u kaznenom postupku.[33] Ipak, ovaj je zaključak više nego dvojben. Budući da neobavještavanje u potpunosti onemogućuje poduzimanje bilo kakvih mjera od strane pogođene države članice (osobito mjera za zaštitu vlastitih građana u istragama stranih tijela kaznenog progona), to se može smatrati ozbiljnim kršenjem temeljnih načela domaćeg pravnog poretka.[34] Budući da bi ova obavijest bila jedini način na koji su pogođene zemlje mogle imati bilo kakav utjecaj na istragu i nastojanje da se zajamči poštivanje temeljnih prava osoba koje su nadzirane, kršenje obveze obavještavanja treba smatrati značajnim propustom i solidnom osnovom za zabranu korištenja tako pribavljenih dokaza u nacionalnim postupcima. Što je veći dio opsega čl. 31. osporavan (i tumačen na prilično restriktivan način, npr. na sudovima u Njemačkoj), to se više može očekivati da će posljednju riječ morati zauzeti Sud EU-a.

Što se tiče suda EU-a, dana 26. listopada 2023. nezavisna odvjetnica Ćapeta iznijela je svoje mišljenje sudu sa sljedećim zaključcima:[35]

(1.) Kada je temeljnu mjeru u državi izvršenja odobrio sudac, europski istražni nalog (EIN) za prijenos takvih dokaza ne mora izdati sudac, čak i ako bi prema zakonu države izdavateljice predmetno prikupljanje dokaza morao odrediti sudac. Činjenica da je presretanje obavljeno na državnom području druge države članice ne utječe na određivanje tijela koje je izdalo EIN. Pravo EU-a ne zahtijeva da europski istražni nalog za prijenos postojećih dokaza prikupljenih presretanjem telekomunikacija izda sud ako nacionalno pravo predviđa da državni odvjetnik može narediti takav prijenos u sličnom domaćem slučaju.

(2.) Procjena nužnosti i razmjernosti EIN-a kojim se traži prijenos postojećih dokaza stvar je tijela koje ga je izdalo, uz mogućnost revizije od strane nadležnog nacionalnog suda. Takva procjena mora uzeti u obzir da pristup nacionalnog tijela presretnutim komunikacijskim podacima predstavlja ozbiljno miješanje u privatne živote dotičnih osoba. To miješanje mora biti uravnoteženo ozbiljnim interesom javnosti za istragu i procesuiranje kaznenih djela.

(3.) Kada se EIN izdaje za prijenos dokaza koji su već u posjedu druge države, pozivanje na sličan domaći slučaj prema čl. 6. st. 1. t. (b) Direktive 2014/41/EU Europskog parlamenta i Vijeća od 3. travnja 2014. u vezi s europskim istražnim nalogom u kaznenim stvarima zahtijeva od tijela koje ga izdaje da utvrdi dopušta li i pod kojim uvjetima relevantno nacionalno pravo prijenos dokaza prikupljenih presretanjem komunikacije

[33] BGH, odluka od 2. 3. 2022. – 5 StR 457/21, para. 44.–45.

[34] Tako i Zimmermann, *op. cit*. u bilj. 2 , str. 173, 178 s obzirom na njemački pravni sustav.

[35] *Mišljenje nezavisne odvjetnice Ćapete*, 26. listopad 2023., Case C-670/22 (Staatsanwaltschaft Berlin v. M.N.), ECLI:EU:C:2023:817.

između domaćih kaznenih postupaka. Prilikom odlučivanja može li izdati europski istražni nalog za prijenos postojećih dokaza tijelo koje ga je izdalo ne može ocijeniti zakonitost temeljnog prikupljanja dokaza u državi izvršiteljici čiji prijenos zahtijeva europskim istražnim nalogom. Činjenica da su temeljne mjere poduzete na teritoriju države izdavateljice ili da su bile u interesu te države ne utječe na prethodni odgovor.

(4.) Država članica koja tijekom svoje jednostrane kaznene istrage ili postupka presreće telekomunikacije na teritoriju druge države članice mora tu drugu državu obavijestiti o presretanju. Ta se obavijest može podnijeti bilo kojem tijelu koje država članica koja presreće smatra prikladnim jer ta država ne može znati koje je tijelo nadležno u sličnom domaćem slučaju.

Čl. 31. Direktive 2014/41 ima za cilj zaštititi pojedinačne dotične telekomunikacijske korisnike i suverenitet države članice o kojoj je riječ.

(5.) Pravo EU-a, u ovoj fazi razvoja, ne uređuje dopuštenost dokaza prikupljenih EIN-om koji je izdan suprotno zahtjevima Direktive 2014/41. Dopuštenost dokaza pitanje je nacionalnog prava, koje, međutim, mora biti u skladu sa zahtjevima prava na obranu iz čl. 47. i 48. Povelje o temeljnim pravima Europske unije.

Što se tiče prava na pravično suđenje, ovdje ističemo kako organizacija *Fair Trials* pozdravlja odluku talijanskog Vrhovnog suda iz 2022. godine, koji je tražio od tužitelja i policije podatke o tome kako su prikupljane poruke s aplikacije *Sky ECC* jer bi izostanak te odluke mogao imati ozbiljne posljedice za pravo na pravično suđenje.[36]

3. TRANSFER DOKAZA U REPUBLIKU HRVATSKU

3.1. Mjerodavno pravo – bilateralni/međunarodni ugovor/pravo EU-a i provedba u domaćem pravnom sustavu

Sljedeće pitanje na koje je potrebno odgovoriti jest jesu li informacije pribavljene masovnim nadzorom komunikacija, koje će se koristiti kao dokazi u kaznenom postupku, transferirane u Republiku Hrvatsku na zakonit način. Pritom su primarno relevantne odredbe tri pravna izvora prava Europske unije:

1. Konvencija utvrđena od strane Vijeća u skladu s čl. 34. Ugovora o EU-u o uzajamnoj pravnoj pomoći u kaznenim stvarima među državama članicama EU-a (OJ C 197 od 12. 7. 2000., str. 3)

[36] Fair Trials, *Fair Trials welcomes Italian Supreme Court ruling on SkyECC evidence,* 6. listopada 2022. Dostupno na: https://www.fairtrials.org/articles/news/fair-trials-welcomes-italian-supreme-court-ruling-on-sky-ecc-evidence/.

2. Okvirna odluka Vijeća 2006/960/PUP od 18. prosinca 2006. o pojednostavljenju razmjene informacija i obavještajnih podataka između tijela zaduženih za izvršavanje zakona u državama članicama Europske unije i
3. Direktiva 2014/41/EU Europskog parlamenta i Vijeća od 3. travnja 2014. o europskom istražnom nalogu u kaznenim stvarima.

Oba su potonja propisa EU-a transponirana u hrvatski pravni sustav kroz odredbe hrvatskih zakona, i to:

1. Zakona o pojednostavljenju razmjene podataka između tijela država članica EU-a nadležnih za provedbu zakona[37] i
2. Zakona o pravosudnoj suradnji u kaznenim stvarima s državama članicama EU-a.[38]

Razlika između tih dvaju zakona jest u tome što prvi omogućava spontanu razmjenu informacija, a drugi ciljano pribavljanje i razmjenu dokaza. U konkretnom predmetu oba su od važnosti jer je u njemu inicijalno došlo do spontane razmjene informacije, nakon čega su hrvatska nadležna tijela korištenjem europskog istražnog naloga zapravo dobila dopuštenje da neke od razmijenjenih informacija (one koje su bile od interesa za hrvatska nadležna tijela) koriste kao dokaze u kaznenim postupcima u Republici Hrvatskoj.

3.2. Spontana razmjena informacija

Pravila za spontani prijenos informacija prilično su ograničena. Naime, čl. 7. Konvencije EU-a o uzajamnoj pravnoj pomoći u kaznenim stvarima iz 2000. dopušta prijenos informacija među državama članicama EU-a bez postojanja prethodnog zahtjeva. Iako je tim člankom prvi put uređena ustaljena praksa,[39] čl. 7. ne propisuje uvjete pod kojima se takve informacije mogu razmjenjivati, osim da se informacije moraju odnositi na kaznena djela (u smislu čl. 3. Konvencije) i da tijela koja daju informacije mogu postaviti neke uvjete za korištenje informacija od strane države primateljice. Slijedom toga čl. 7. Konvencije može se smatrati prvim valjanim temeljom za prijenos informacija bez prethodnog i formalnog zahtjeva; sukladno rečenom na temelju tako dobivenih informacija nacionalna tijela mogu dalje upućivati službene zahtjeve za pružanjem daljnje pravne pomoći.[40]

[37] Zakon o pojednostavljenju razmjene podataka između tijela država članica Europske unije nadležnih za provedbu zakona, Narodne novine br. 56/15.

[38] Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije, Narodne novine br. 91/10, 81/13, 124/13, 26/15, 102/17, 68/18, 70/19, 141/20.

[39] V. Gleß, S.; Wahl, T. u Schomburg/Lagodny, *Art. 7 EU-RhÜbk*, st. 1.: „Čl. 7 … otvara nove temelje. Norma legalizira uobičajenu praksu, koja je dugo postojala samo u transnacionalnoj sivoj zoni."

[40] Pauli, G., *Zur Verwertbarkeit der Erkenntnisse ausländischer Ermittlungsbehörden - EncroChat*, Neue Zeitschrift für Strafrecht, vol. 41, br. 3, 2021, str. 146 i 147.

Više pravila sadrži Okvirna odluka 2006/960/JHA o pojednostavljenju razmjene informacija i obavještajnih podataka, koja je, dakle, relevantna osnova za spontani prijenos informacija između tijela zaduženih za izvršavanje zakona u državama članicama Europske unije. Međutim, navedena pravila nisu primarno namijenjena na prijenos dokaza iz jedne države u drugu jer njezin čl. 1.(2.) navodi da Okvirna odluka ne utječe na tradicionalne instrumente uzajamne pomoći i uzajamnog priznavanja. Ali budući da se Okvirna odluka bavi informacijama i obavještajnim podacima relevantnim za kaznene postupke, ona ima sličan cilj kao i propisi o međunarodnoj pomoći. Prema čl. 7.(1.) tijela kaznenog progona mogu dijeliti informacije s tijelima drugih država članica, a da se to od njih prethodno ne zatraži, „ako postoji činjenična osnova koja upućuje na to da bi te informacije i obavještajni podaci mogli pomoći u otkrivanju, sprečavanju ili provođenju istrage o kaznenim djelima“ (odnosi se na kaznena djela navedena u čl. 2. st. 2. Okvirne odluke o europskom uhidbenom nalogu 2002/584/JHA).[41] Ova formulacija čl. 7 “određena kaznena djela” itekako upućuje na to da je treba čitati na način da je u ovoj konstelaciji nužna konkretna sumnja u vezi s konkretnim kaznenim djelom.

Uz ogradu da okolnosti *spontane razmjene informacija* nisu do kraja razjašnjene, čini se da su nadležna tijela koja su okupljena u zajednički istražni tim, uz posredovanje Europola, sve informacije koje su prikupljene kroz masovni nadzor korisnika aplikacije *Sky ECC*, bez njihova prethodnoga filtriranja, proslijedile hrvatskim nadležnim tijelima. Slanje integralnog paketa presretnutih informacija, bez njihova prethodnoga filtriranja (slanje samo onoga što može biti od interesa za hrvatska nadležna tijela u kontekstu istraživanja konkretnih kaznenih djela), protivno je odredbama čl. 7. st. 2. Okvirne odluke 2006/960. Navedene odredbe upućuju na ograničenu razmjenu filtriranih informacija, odnosno onih „koje se smatraju relevantnim i potrebnim za uspješno otkrivanje, sprečavanje ili provedbu istrage o zločinu ili kriminalnoj radnji o kojoj je riječ“. Ako je u konkretnom predmetu zaista postupljeno na ovakav način, takvo postupanje predstavlja *povredu prava EU-a*, odnosno postupanje protivno odredbi čl. 7. st. 2. Okvirne odluke 2006/960. Svakako je u konkretnom postupku *potrebno do kraja razjasniti je li, pod kojim okolnostima i u kojem opsegu došlo do spontane razmjene informacija s hrvatskim tijelima nadležnim za provedbu zakona*, da bi se na temelju tako utvrđenih činjenica moglo zaključiti je li takvim postupanjem došlo do povrede prava EU-a.

[41] Vidi: Zimmermann, *op. cit.* u bilj. 2 , str. 173, 183.

3.3. Odnos zatražene i provedene istražne (dokazne) radnje

U predmetu *Sky ECC* riječ je o dokazima koje je pribavilo pravosudno tijelo države članice EU-a, konkretno Francuske. Sukladno rečenom pored procjene zakonitosti prikupljenog dokaza, koja je provedena prvenstveno sagledavanjem normi domaćeg (francuskog) prava, transfer dokaza i pitanje dopustivosti korištenja prikupljenog inozemnog dokaza u Republici Hrvatskoj valja promatrati kroz prizmu Zakona o pravosudnoj suradnji u kaznenim stvarima (ZPSKS) i EIN-a. Riječ je o instrumentu pravosudne suradnje utemeljenom na načelu uzajamnog priznanja.[42] Važna sadržajna specifičnost EIN-a leži u činjenici što se EIN usredotočuje na istražne radnje koje treba poduzeti, a ne na dokaz koji treba pribaviti.[43] Zbog toga je i prihvaćeno shvaćanje da o istražnoj mjeri koju treba koristiti odlučuje tijelo izdavatelj na temelju podataka kojima raspolaže o dotičnoj istrazi (Recital 10). EIN bi trebalo izabrati ako se provođenje istražne mjere čini proporcionalnim, primjerenim i primjenjivim na konkretan slučaj. Tijelo izdavatelj trebalo bi stoga utvrditi jesu li traženi dokazi nužni i proporcionalni svrsi postupka, je li izabrana istražna mjera nužna i proporcionalna za pribavljanje dotičnih dokaza i bi li u pribavljanje tih dokaza trebalo izdavanjem EIN-a uključiti drugu državu članicu (Recital 11).[44] Sukladno rečenom čl. 42.c ZPSKS-a propisuje da će nadležno pravosudno tijelo izdati europski istražni nalog ako su ispunjene sljedeće pretpostavke: 1. izdavanje europskog istražnog naloga nužno je i razmjerno svrsi postupaka iz čl. 2. t. 9. ZPSKS-a, 2. dokazna radnja ili radnje navedene u europskom istražnom nalogu mogu biti određene u tom postupku. Prema rečenom europski istražni nalog može se izdati u svrhu provođenja svih dokaznih radnji propisanih Zakonom o kaznenom postupku na području druge države članice Europske unije, uz poštovanje načela razmjernosti (dokazna radnja zatražena europskim istražnim nalogom mora biti razmjerna svrsi koja se njome želi postići) i postojanje pretpostavki propisanih Zakonom o kaznenom postupku (dokazne radnje zatražene europskim istražnim nalogom mogu biti provedene u domaćem postupku).[45]

U navedenom slučaju razvidno je da je do izdavanja europskog istražnog naloga od strane hrvatskog pravosudnog tijela došlo tek *ex post*, nakon što su

[42] Suominen, A., *The principle of Mutual Recognition in Cooperation in Criminal Matters*, Larcier Intersentia, 2011, str. 20–22.

[43] Šugman Stubbs, Katja, *Ocjena dokaza pribavljenih u inozemstvu: teorijski problemi i slovenska sudska praksa*, Hrvatski ljetopis za kaznene znanosti i praksu, vol. 21, br. 1, 2014, str 119.

[44] Usp. Rafaraci, T., *General Considerations on the European Investigation Order*, u: S. Ruggeri (ur.), Transnational Evidence and Multicultural Inquiries in Europe, Springer, 2014, str. 41.

[45] Hržina D., *Novela Zakona o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije*, Pravosudna akademija, 2018, str. 19.

već dokazne radnje provedene sukladno pravu države izvršiteljice. To, dakako, nije razlog koji bi državu izdavateljicu prekludirao u izdavanju europskog istražnog naloga budući da se EIN također može izdati za pribavljanje dokaza koji su već u posjedu nadležnih tijela države izvršiteljice (čl. 1. st. 1. EIN-a).[46] Međutim, iz ovog aspekta sporna je okolnost što je hrvatsko pravosudno tijelo zahtijevalo pribavljanje dokaza koji se po hrvatskom pravu uopće ne bi mogao pribaviti. Naime, usporedive posebne dokazne radnje u hrvatskom Zakonu o kaznenom postupku jesu: 1) nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu (čl. 332. st. 1. t. 1.) i presretanje, prikupljanje i snimanje računalnih podataka (čl. 332. st. 1. t. 2.). No unatoč tome što su te radnje u procesnom (provedbenom) smislu praktično identične provedenim dokaznim radnjama u Francuskoj, sličnost uopće ne postoji kad se sagledaju ključne materijalnopravne pretpostavke koje predstavljaju minimalni legitimacijski uvjet koji u svakom slučaju mora biti ispunjen za primjenu navedenih mjera, koje po svojem opsegu predstavljaju teški zahvat u temeljno pravo na nepovredivost osobnog i obiteljskog života (čl. 35. st. 1. Ustav RH) i na nepovredivost slobode i tajnosti dopisivanja i svih drugih općenja (čl. 36. st. 1. Ustav RH). U Hrvatskoj su materijalnopravne pretpostavke za primjenu posebnih dokaznih radnji propisane kao postojanje osnova sumnje da je neka osoba sama počinila ili zajedno s drugim osobama sudjelovala u kaznenom djelu (čl. 332. st. 1. ZKP-a), da se radi o kaznenom djelu iz kataloga kaznenih djela iz čl. 334. ZKP-a i da je ta mjera nužna za uspješno vođenje izvida kaznenih djela (čl. 332. st. 1. i čl. 334. ZKP-a).[47] U nalogu se navode raspoloživi podaci o osobi protiv koje se mjere primjenjuju, činjenice iz kojih proizlazi potreba njihova poduzimanja i rok njihova trajanja, koji mora biti primjeren ostvarenju njezina cilja, kao i način, opseg i mjesto provođenja radnje (čl. 332. st. 1., čl. 335. st. 1. ZKP-a). Sukladno rečenom nedvojbeno je da je Zakon izrijekom odredio da se posebne dokazne radnje mogu odrediti samo protiv konkretne osobe u odnosu na koju postoje osnove sumnje da je počinila kazneno djelo. To znači da je primjena posebnih dokaznih radnji dopuštena samo kad postoji određena sumnja (vjerojatnost) da je određena osoba počinila kazneno djelo.[48] Taj određeni stupanj sumnje određen je kriterijem „osnove sumnje da je određena osoba počinila kazneno djelo“ i predstavlja **pravni standard** koji se tumači u prav-

[46] Belfiore, R., *The European Investigation Order in Criminal Matters: Developments in Evidence-gathering across the EU*, European Criminal Law Review, br. 3, 2015, str. 315.

[47] Ljubanović, Novokmet, Tomičić, *op. cit*. u bilj. 16, str. 183–188.

[48] Krapac D., *Institucije*, 2014, 320. Detaljno za regulaciju pristupa telekomunikacijskim podacima u kaznenom postupku za RH v. Jurić, M.; Roksandić, S., *Access to Telecommunication Data in Criminal Justice (Croatia)*, u: Sieber, U.; von zur Muehlen, N ; Tropina, T. (ur.), drugo izmijenjeno i dopunjeno izdanje, Berlin, Duckner & Humblot 2021, str. 377–418, Za komparativni pristup v. vol. 1 i 2.

nom, a ne u spoznajnom smislu.[49] To znači da taj stupanj vjerojatnosti mora: 1. prethoditi određivanju mjere – to znači da se posebne dokazne radnje ne mogu određivati radi naknadnog provjeravanja postoji li ta vjerojatnost ili ne, odnosno radi toga da se tek prikupljaju podaci na temelju kojih bi se ta vjerojatnost tek mogla pojaviti, 2. konkretno upućivati na to da je određena osoba počinila određeno kazneno djelo – to znači da navedene činjenice ne smiju proizlaziti iz paušalnog nagađanja, kalkulacija, spekuliranja i sl.,[50] 3. konkretno upućivati na to da ponašanje neke osobe predstavlja napad na specifična pravna dobra koji je propisima kaznenog prava inkriminiran kao kazneno djelo, 4. biti moguće jasno izraziti, artikulirati na logičan i za sve sudionike postupka uvjerljiv način – artikulabilna vjerojatnost jest ona koja proizlazi iz objektivno provjerljivih podataka i obavijesti (dokaza) o činjenicama povezanim s kaznenim djelom i počiniteljem i mora se moći izraziti u obrazloženju pisanog naloga kojim se određuju posebne dokazne radnje.[51] U navedenom slučaju, kako je rečeno, posebne dokazne radnje provedene su na način da je njima bio zahvaćen širok krug unaprijed neodređenih osoba, iz čega proizlazi da nisu bile poduzete s ciljem da se pronađu i utvrde konkretni dokazi protiv određene osobe koji bi bili važni za kazneni postupak. Naprotiv, navedene su radnje bile provedene isključivo protiv velikog broja osoba pod eventualnom sumnjom da je „netko nešto počinio", bez jasno određene svrhe provođenja posebnih dokaznih radnji, iz čega proizlazi da, sukladno hrvatskom pravu, provedene radnje i mjere nisu bile utemeljene na normi zakonskog ranga niti su bile razmjerne i uravnotežene.

Kad se uzme u obzir sve navedeno, mogu se izvesti određene usporedbe s posebnim dokaznim radnjama provedenim u predmetima *Sky ECC* i ANOM, barem kolike su poznate. Sličnosti s provedenom posebnom dokaznom radnjom u predmetu *Sky ECC* ogledaju se u okolnosti da i jedna i druga predstavljaju posebne istražne tehnike u otkrivanju i pronalaženju počinitelja kaznenog djela, pa je zakonodavac u oba slučaja odredio taksativno nabrojana kaznena djela za koja se takva mjera može odrediti i provesti, da je utvrđivanje pretpostavki za određivanje tih mjera i nalaganje njihova provođenja stavljeno u isključivu nadležnost suda, da ih u oba slučaja izvršavaju posebno osposobljeni policijski službenici te da su ograničene vremenskim periodom u kojem se mogu poduzimati. Konačno, provedene posebne dokazne radnje u okviru *Sky ECC* mogu se usporediti s hrvatskim posebnim dokaznim radnjama kao što su nadzor i tehničko snimanje telefonskih razgovora i drugih komunikacija na daljinu te presretanje, prikupljanje i snimanje računalnih podataka.

[49] *Ibid*.
[50] *Ibid*.
[51] *Ibid*., 321.

Ipak, ključna fundamentalna razlika ogleda se u činjenici da hrvatski pravni poredak uopće ne poznaje „masovno presretanje" komunikacije na način da bi se takve radnje mogle u Hrvatskoj odrediti protiv „nepoznatog" počinitelja. Francuski pravni sustav tu je otišao korak dalje i u svojem je zakonodavstvu predvidio upravo mogućnost masovnog presretanja. U tom je dijelu francuski zakonodavac očito bio inspiriran shvaćanjem ESLJP-a u predmetu *Big Brother Watch and Others v. UK*, u kojem su definirane odrednice minimalnih europskih standarda koji moraju biti zadovoljeni da bi tako teški zahvati u pravo i slobodu pojedinca bili prihvatljivi u demokratskom društvu. Međutim, hrvatski pravni poredak ni na koji način ne dopušta takvo korištenje posebnih dokaznih radnji koje bi bile upravljene prema neodređenom broju osoba, nego inzistira na tome da se posebne dokazne radnje mogu i smiju odrediti samo protiv poznate osobe.

3.4. Uvoz ranije izvedenih dokaza i pravilo *forum regit actum*

Europski istražni nalog idejno je zamišljen kao instrument koji će učvrstiti načelo uzajamnog povjerenja i dovesti do slobodnog protoka dokaza, što bi značilo da bi svaki dokaz, zakonito pribavljen u jednoj državi, trebao automatski biti prihvaćen u drugoj državi.[52] Ipak, ta se ideja nije ostvarila u čistoj procesnoj formi, nego je danas prihvaćen svojevrsni slobodan protok naloga za poduzimanje istražne radnje.[53] Za razliku od tradicionalnog pravila *locus regit actum*, prihvaćenog u klasičnoj međunarodnoj suradnji u kaznenim stvarima, Europska unija problem ocjene dopuštenosti dokaza pribavljenih u inozemstvu pokušala je razriješiti primjenom pravila *forum regit actum*.[54] Dakle, u postupanju na temelju europskog istražnog naloga država izvršiteljica trebala bi postupati po pravu države tražiteljice i poduzeti zatraženu istražnu radnju sukladno pravu države tražiteljice ako takvo postupanje ne bi bilo u suprotnosti s temeljnim načelima domaćeg pravosudnog sustava.[55] Time se barem načelno otklanja problem dopustivosti primjene dokaza pribavljenih u inozemstvu za potrebe domaćeg kaznenog postupka.

Međutim, u predmetu *Sky ECC* kronologija događaja pokazuje da je došlo do svojevrsne inverzije u postupanju. Odnosno, istražna radnja već je ranije poduzeta u stranoj državi za potrebe domaćeg kaznenog postupka, a o njoj su

[52] Šugman Stubbs, K., *op. cit.* u bilj. 43, str. 120.

[53] *Ibid.*

[54] Usp. Karsai, K., *Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters*, Hungarian Journal of Legal Studies, vol. 60, br. 2, 2019, str. 162–163.

[55] Kusak M., *Mutual admissibility of evidence and the European investigation order: aspirations lost in reality*, ERA Forum, vol. 19, 2019, str. 391–400.

obaviještena hrvatska pravosudna tijela, koja su naknadno zatražila dostavljanje rezultata već provedenih dokaznih radnji izdavanjem europskog istražnog naloga. Dakako, takvo traženje hrvatskih pravosudnih tijela bilo je apsolutno legitimno jer i sama Direktiva 2014/41/EU u čl. 1. st. 1. izrijekom propisuje mogućnost pribavljanja dokaza koji su već u posjedu nadležnih tijela države izvršiteljice. No sukladno čl. 6. st. 1. i 2. Direktive tijelo izdavatelj, dakle hrvatsko pravosudno tijelo, bilo je dužno u konkretnom slučaju provjeriti je li izdavanje EIN-a potrebno i proporcionalno svrsi postupka iz čl. 4. uzimajući u obzir prava osumnjičenika ili okrivljenika i jesu li istražne mjere navedene u EIN-u mogle biti određene u sličnom domaćem slučaju.[56] Očito je da su u hrvatskom pravnom poretku materijalne pretpostavke za provođenje usporedive posebne dokazne radnje propisane u strožem režimu i da kvaliteta pravne norme pruža jaču zaštitu građaninu od neopravdanog upliva državnih represivnih vlasti u njegova prava i slobode. Dok je načelna zamisao da u kontekstu europskog istražnog naloga država tražiteljica, sukladno pravilu *forum regit actum*, „izvozi" svoju pravnu normu u strani pravni poredak, a potom, nakon što je radnja poduzeta, „unosi" u svoj pravni poredak njezin zakoniti rezultat i na taj način dovodi do ostvarenja ideje uzajamnog povjerenja, očito je da se u navedenom slučaju dogodio potpuno inverzni pristup, u kojem hrvatska pravosudna tijela „uvoze" rezultat poduzete radnje iz stranog pravnog poretka u domaći pravni poredak, a da prethodno nisu izvršila nužnu procjenu bi li tako provedene radnje uopće mogle biti određene i provedene u sličnom domaćem slučaju.

Kad se uzme u obzir sve navedeno, jasno je da je u ovom slučaju došlo je do automatskog uvoza rezultata dokazne radnje poduzete u stranoj zemlji, pri čemu nisu učinjene nužne provjere dopustivosti korištenja tako pribavljenih dokaza u hrvatskom kaznenopravnom kontekstu. Prethodnu procjenu dopustivosti trebalo je provesti pravosudno tijelo države izdavateljice (hrvatsko pravosudno tijelo) prije nego što je izdalo europski istražni nalog kako bi se ocijenila materijalnopravna i formalnopravna usklađenost rezultata već provedene istražne radnje u stranoj zemlji. Bit je europskog istražnog naloga u tome da država izdavateljica odredi uvjete i način pod kojima se dokazi u inozemstvu trebaju pribaviti te da država izvršiteljica postupi po takvu nalogu, osim ako smatra da je izvršenje takve radnje i mjere sadržajno protivno temeljnim načelima njezina pravnog poretka.[57] Analiza usklađenosti usporedive domaće pravne norme u Francuskoj i Hrvatskoj pokazala je da hrvatski pravni pore-

[56] Usp. Allegreza, S., *Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality*, u: S. Ruggeri (ur.), Transnational Evidence and Multicultural Inquiries in Europe, Springer, 2014, str. 62–63.

[57] Daniele, M., *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, New Journal of European Criminal Law, vol. 6, br. 2, 2015, str. 184.

dak postavlja veće zahtjeve pred državna represivna tijela i, posljedično, veću kvalitetu poduzete radnje nego što je to slučaj u Francuskoj. S druge strane, ne postoje zajednički europski minimalni standardi na temelju kojih bi se mogao odrediti donji minimum kvalitete koji mora zadovoljiti dokaz pribavljen u inozemstvu da bi ga se moglo smatrati dopustivim u državi izdavateljici.[58] Stoga je zadatak na domaćem sudu da odluči o dopustivosti izvođenja tako pribavljenog dokaza ocjenom težine procesne povrede i njezina značaja za zaštićene pravne vrijednosti u hrvatskom kaznenom postupku.

3.5. Usklađenost stvarno provedene istražne radnje s čl. 30. Direktive 2014/41/EU

Direktiva 2014/41/EU o europskom istražnom nalogu sadrži posebne odredbe za provođenje određenih istražnih mjera, među kojima je u čl. 30. propisana i mjera presretanje telekomunikacija uz tehničku pomoć druge države članice, a pomnije ju razrađuje čl. 42.al ZPSKS-a. Tako je u čl. 30. Direktive 2014/41/EU propisano da se EIN može izdati za presretanje telekomunikacija u državi članici iz koje je potrebna tehnička pomoć. Ta je odredba detaljnije razrađena čl. 42.al ZPSKS-a na način da nadležno županijsko državno odvjetništvo, nakon što pribavi odluku suca istrage, može u skladu s domaćim pravom izdati europski istražni nalog za presretanje računalnih podataka, nadzor i tehničko snimanje telefonskih razgovora i drugih telekomunikacija na daljinu te provjeru uspostavljanja telekomunikacijskih kontakata u državi članici od koje je potrebno osigurati tehničku pomoć. Poanta je navedenih odredbi u tome da opisane posebne dokazne radnje u državi izdavateljici određuje sudac istrage pisanim obrazloženim nalogom na pisani obrazloženi zahtjev državnog odvjetnika (čl. 332. st. 1. ZKP-a). Pritom se kao garancija zakonitosti i razmjernosti naložene mjere u europskom istražnom nalogu moraju navesti: a) podaci potrebni u svrhu identifikacije subjekta nadzora; b) traženo trajanje nadzora i c) dostatni tehnički podaci, posebno identifikacijska oznaka uređaja, kako bi se osiguralo da se europski istražni nalog može izvršiti (čl. 30. st. 3. Direktiva 2014/41/EU, čl. 42.al st. 3. ZPSKS-a), a mora se navesti i razlog zbog kojeg je naložena dokazna radnja važna za domaći kazneni postupak (čl. 30. st. 4. Direktive 2014/41/EU, čl. 42.al st. 4. ZPSKS-a). Konačno, država izvršiteljica može odbiti europski istražni nalog kada smatra da istražna mjera ne bi bila odobrena u sličnom domaćem slučaju, odnosno svoju suglasnost može uvjetovati ispunjenjem bilo kojih uvjeta koji bi se trebali ispuniti u sličnom doma-

[58] Bachmaier W., L., *European investigation order for obtaining evidence in the criminal proceedings Study of the proposal for a European directive*, Zeitschrift für Internationale Strafrechtsdogmatik, vol. 5, br. 9, 2010, str. 587–588.

ćem slučaju (čl. 30. st. 5. Direktive 2014/41/EU). Iz izričaja navedenih odredbi potpuno je jasno da primat u nalaganju posebne dokazne radnje u kontekstu europskog istražnog naloga ima država izdavateljica i da EIN primarno služi u kontekstu tehničke pomoći državi izdavateljici da provede istražnu radnju na području druge države članice EU-a iz razloga jer se subjekt nad kojim se provodi takva posebna dokazna radnja nalazi na državnom području dotične strane zemlje.[59] Pritom je indikativno da Direktiva, ali i ZPSKS, jasno propisuju određene kriterije nadzora nad zakonitošću i razmjernosti određene mjere, iz čega proizlazi da država izvršiteljica može odbiti EIN ako utvrdi da istražna mjera ne bi bila odobrena u sličnom domaćem slučaju.

Budući da je u predmetu *Sky ECC* dokaze pribavljao zajednički istražni tim u sastavu Francuska, Belgija i Nizozemska, očito je da su te zemlje za svoje potrebe pribavljale dokaze primjenom posebnih dokaznih radnji koje se mogu opravdati u navedena tri pravosudna sustava. Sasvim je onda legitimno da se u tim državama prikupljeni dokazi mogu i trebaju koristiti kao dokaz u kaznenom postupku. No kad je u pitanju Republika Hrvatska, onda valja uočiti da Republika Hrvatska ne samo što nije bila dio zajedničkog istražnog tima nego nije ni inicirala prikupljanje dokaza u akciji *Sky ECC* u inozemstvu. Stoga je nedvojbeno da spontano uvoženje već izvedenih dokaza u inozemstvu ne može biti opravdano samo formom europskog istražnog naloga, nego mora biti prihvatljivo i iz aspekta norme domaćeg zakona prema kojoj bi takva radnja poduzeta u inozemstvu pod istim uvjetima bila vjerodostojna i u domaćem pravnom krugu. Ako bi se taj čvrsti stav napustio i ako bi se slijepo podržavala dopustivost korištenja inozemnog dokaza kao zakonitog unatoč tome što ne bi ispunjavao potrebne materijalne ili procesne pretpostavke, to bi dovelo do izvrtanja biti uzajamnog priznavanja u kaznenim stvarima. Potencijalno bi se otvorila praksa tzv. *forum shoppinga*, tj. da tijela kaznenog progona svjesno poduzimaju neku dokaznu radnju u državi članici EU-a koja ima značajno niže postavljen prag zaštite temeljnih prava pojedinaca, svjesna da će rezultate tako pribavljenih radnji biti prisiljena prihvatiti država članica EU-a u kojoj se takva dokazna radnja inače ne bi mogla provesti zbog viših standarda zaštite građana od represivne moći državne vlasti. Očito je da u takvoj situaciji sud u domaćem pravnom poretku mora provesti evaluaciju dopustivosti tako prikupljenog dokaza i ocijeniti mogućnost njegove upotrebe u skladu s domaćim pravilima koja rješavaju pitanje zakonitosti dokaza.[60]

[59] Arasi, S., *The EIO Proposal and the Rules on Interception of Telecommunications*, u: S. Ruggeri (ur.), Transnational Evidence and Multicultural Inquiries in Europe, Springer, 2014, str. 130.

[60] V. Kuczyńska, H., *Admissibility of evidence obtained as a result of issuing an European investigation order in a Polish criminal trial*, Review of european and comparative law, vol. XLVI, br. 3, 2021, str. 67–92.

4. ZAKONITOST DOKAZA U POSTUPKU PRED HRVATSKIM SUDOVIMA

U hrvatskom pravu ne postoje posebna pravila koja bi regulirala pitanje zakonitosti (dopustivosti) dokaza pribavljenih putem pravosudne suradnje u kaznenim stvarima s državama članicama EU-a. Takva pravila ne postoje ni u pravu EU-a. Načelo uzajamnog priznanja ne odnosi se na dokaze. U tom smislu ne postoji načelo o uzajamnom priznanju ili o uzajamnoj dopustivosti dokaza.[61] Razlog je to što su pravila o pribavljanju dokaza između država članica EU-a još uvijek značajno različita, na što upućuje i ovaj predmet, kroz koji postaje jasno da između država članica ne postoji neki zajednički pristup prema pitanju masovnog nadzora komunikacija. Najdalje je u regulaciji pitanja uzajamne dopustivosti dokaza otišla Uredba Vijeća (EU) 2017/1939 od 12. listopada 2017. o provedbi pojačane suradnje u vezi s osnivanjem Ureda europskog javnog tužitelja (EPPO), koja u čl. 37. propisuje da dokazi koje su tužitelji EPPO-a ili tuženik predložili sudu ne smiju biti odbačeni kao nedopušteni samo zbog toga što su ti dokazi prikupljeni u drugoj državi članici ili u skladu s pravom druge države članice (st. 1.) te da se njezinim pravilima ne utječe na ovlast suda pred kojim se vodi postupak da slobodno ocjenjuje dokaze koje su predložili tuženik ili tužitelji EPPO-a (st. 2.). Dakle, ne radi se o pravilu o uzajamnoj dopustivosti dokaza, već o pravilu koje zabranjuje sudu da dokaz iz inozemstva proglašava nedopuštenim (nezakonitim) samo zbog toga što je prikupljen po drugačijim postupovnim pravilima. Europska je unija, doduše, temeljnim ugovorima ovlaštena regulirati i pitanje uzajamne dopustivosti dokaza. Odredbom čl. 82. st. 2. (a) Ugovora o funkcioniranju Europske unije određeno je da Unija može direktivama, usvajanjem zajedničkih minimalnih pravila, regulirati i pitanje uzajamne dopustivosti dokaza između država članica. Ta zakonodavna ovlast Europske unije još uvijek nije iskorištena. Budući da takva zajednička minimalna pravila ne postoje, razumnim se čini u odnosu na dokaze pribavljene u kontekstu pravosudne suradnje u kaznenim stvarima između država članica Europske unije, odnosno dokaze pribavljene putem europskog istražnog naloga, koristiti iste standarde za ocjenu njihove zakonitosti (dopustivosti) koji se primjenjuju i na druge dokaze pribavljene iz inozemstva. Ti bi se standardi u kontekstu dokaza pribavljenih putem europskog istražnog naloga trebali nadopuniti onime na što nadležna tijela država članica obvezuje Direktiva. Dvije su odredbe Direktive u kontekstu dopustivosti dokaza relevantne: čl. 1. st. 4., koji propisuje obvezu poštovanja temeljnih prava i pravnih

[61] Ispravno Đurđević naglašava da je pretpostavka izjednačavanja učinaka stranih i vlastitih sudskih odluka u nacionalnom kaznenopravnom poretku uspostavljanje zajedničkih minimalnih procesnih standarda. Đurđević, Z. *Lisabonski ugovor: prekretnica u razvoju kaznenog prava u Europi*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 15, br. 2, 2008, str. 1090.

načela sadržanih u čl. 6. UEU-a, uključujući i prava na obranu osoba koje podliježu kaznenom postupku, te čl. 14. st. 7., druga rečenica, koja glasi: Ne dovodeći u pitanje nacionalna postupovna pravila, države članice osiguravaju da se u kaznenom postupku u državi izdavateljici, pri procjeni dokaza pribavljenih putem EIN-a, poštuju prava obrane i pravičnost postupka. Vidimo da je u pravu EU-a, u kontekstu dopustivosti dokaza koji su pribavljeni putem pravosudne suradnje u kaznenim stvarima, poseban naglasak stavljan na potrebu poštivanja prava obrane i prava na pravičan postupak.

Općenito, u odnosu na pitanje zakonitosti dokaza pribavljenih u inozemstvu, čini se da naša sudska praksa čvrsto stoji na stajalištu da se u odnosu na te dokaze primjenjuju nešto labavija pravila o zakonitosti negoli u odnosu na domaće dokaze. Takvo stajalište posljedica je shvaćanja da se pribavljanje dokaza u inozemstvu događa u kontekstu pravila koja su manje ili više različita od naših domaćih procesnih pravila.[62] Ima i stajališta prema kojima odredba hrvatskoga prava o nezakonitim dokazima, danas čl. 10. ZKP-a, treba biti polazišna točka za davanje odgovora na pitanje može li se dokaz pribavljen u inozemstvu, po odredbama stranoga prava, smatrati kod nas zakonitim dokazom.[63] Temeljni je pristup Vrhovnog suda Republike Hrvatske da će dokaz pribavljen sukladno drugačijim dokaznim pravilima još uvijek biti zakonit „ako način njegova pribavljanja nije protivan Ustavu i javnom poretku Republike Hrvatske“, odnosno ako se ti dokazi „ne protive temeljnim ili beziznimnim načelima domaćeg zakonodavstva“.[64] Jednako tako, ako su dokazi pribavljeni kroz radnje „koje su prema propisima domaćeg zakonodavstva uvijek pravno nevaljane, iste treba izdvojiti iz spisa predmeta sukladno odredbi čl. 78. ZKP“. Svi navedeni pravni standardi proklamirani su u rješenju Vrhovnog suda Republike Hrvatske od 31. listopada 2001., I Kž-725/01-4. U toj odluci sud je potvrdio rješenje prvostupanjskog suda kojim je iz spisa predmeta izdvojen kao nezakonit dokaz zapisnik o saslušanju svjedoka pri Carinskom uredu u Münchenu te zapisnik o njegovu ispitivanju pred državnim odvjetnikom. Od-

[62] Mrčela, M., *Pravna valjanost dokaza pribavljenih u inozemstvu*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 7, br. 1, 2000, str. 104. Slično i Tripalo, D. Priznanje dokaza izvedenih pred pravosudnim tijelima strane države, dostupno na: https://www.vsrh.hr/kazneno-pravo-drazen-tripalo-mag-iur.aspx (27. 10 2023.).

[63] Tako *Tripalo* u ranije citiranom radu, str. 10.

[64] Slično i *Mrčela*, ibid.: „[A]ko pravo države moliteljice za određeni dokaz traži stogu beziznimnu formu, onda se dokaz koji je pribavljen u inozemstvu po pravu zamoljene države, iako po tom stranom pravu pravo valjan, ne bi mogao koristiti u postupku pred sudom države moliteljice jer po njezinom pravu takav dokaz uvijek nije pravno valjan“, str. 104. Tako ovaj autor zaključuje da se i saslušanje svjedoka pred policijom može prihvatiti kao zakonit dokaz, iako naš ZKP redarstvenim vlastima brani ispitivanje građana u svojstvu svjedoka, ali to pravilo ima iznimke (prepoznavanje koje su obavile redarstvene vlasti po nalogu državnog odvjetnika i sastavile zapisnik o toj radnji).

luka prvostupanjskog suda potvrđena je u dijelu u kojem zapisnik o ispitivanju svjedoka prikrivenog istražitelja pri Uredu carinske policije u Münchenu nije izdvojen iz spisa predmeta kao nezakonit dokaz, i to zato što „činjenica da je zapisnik sačinjen u Uredu carinske policije, prema stajalištu ovog suda, suštinski ne odstupa u tolikoj mjeri od temeljnih načela domaćeg kaznenog zakonodavstva da bi se anulirala valjanost dokaza u predmetnom kaznenom postupku". Zaključno bismo mogli kazati da je Vrhovni sud u ovom rješenju odluku o (ne)zakonitosti dokaza pribavljenih u inozemstvu sveo na pitanje **odstupa** li način pribavljanja dokaza u inozemstvu „**suštinski (…) u većoj mjeri od temeljnih načela domaćeg kaznenog zakonodavstva**".

U osnovi iste standarde Vrhovni sud preuzeo je i onda kada ispituje zakonitost dokaza pribavljenih u kontekstu pravosudne suradnje u kaznenim stvarima kada se radi o državama članicama Europske unije. Tako je u svojem rješenju od 17. prosinca 2020., I Kž-Us 120/2020-4, Vrhovni sud ispitivao je li načinom na koji je dokaz pribavljen u Rumunjskoj došlo do povrede prava na obranu te je li način pribavljanja dokaza „u suprotnosti s temeljnim načelima domaćeg kaznenog zakonodavstva".[65]

Na temelju provedene analize, koja je obuhvatila praksu naših sudova, ali i važeće odredbe prava Europske unije, zaključno bismo mogli kazati da je prilikom odlučivanja o zakonitosti (dopustivosti) dokaza pribavljenih putem pravosudne suradnje u kaznenim stvarima s državama članicama Europske unije nadležni sud dužan ocijeniti:

1. odstupa li način na koji su pribavljeni ti dokazi suštinski u većoj mjeri od temeljnih načela domaćeg kaznenog zakonodavstva i
2. na koji se način uporaba tako pribavljenog dokaza u kaznenom postupku odražava na prava obrane i pravičnost postupka.

Prilikom analiziranja načina na koji je dokaz pribavljen u inozemstvu (u okviru 1. dijela dvodijelnog testa) nadležni sud dužan je ispitati način na koji je dokaz pribavljen. Bez poznavanja činjenične i pravne osnove prikupljanja dokaza nemoguće je donijeti zaključak o tome odstupa li način pribavljanja dokaza suštinski od temeljnih načela domaćeg kaznenog zakonodavstva. Pored toga, deficit u poznavanju činjeničnog i pravnog okvira unutar kojega je neki dokaz prikupljen u inozemstvu predstavlja i ograničenje prava obrane. Obrana ima stvarnu mogućnost osporiti zakonitost određenog dokaza jedino ako su

[65] U ovom je predmetu putem europskog istražnog naloga zatraženo ispitivanje okrivljenika u Rumunjskoj. Hrvatska su nadležna tijela zatražila da se ispitivanje provede sukladno pravilima hrvatskoga prava, uključujući i audio-videosnimanje ispitivanja. Snimka ispitivanja u Rumunjskoj nije izrađena te je zbog toga obrana tvrdila da se radi o nezakonitom dokazu. Vrhovni je sud zaključio da zapisnik o ispitivanju okrivljenika nije nezakonit dokaz jer je prilikom ispitivanja bilo osigurano pravo na branitelja, a izostanak snimke ispitivanja nije u suprotnosti s temeljnim načelima domaćeg kaznenog zakonodavstva.

poznate činjenične i pravne okolnosti u okviru kojih je dokaz prikupljen. Što je način prikupljana dokaza više prekriven velom tajne, prava obrane značajnije su ograničena.

U odnosu na pitanje pravičnosti postupka temeljni je kriterij kroz koji se preispituje njegovo ostvarenje u kontekstu uporabe inozemnog dokaza: dovodi li način na koji je pribavljen određeni dokaz u sumnju njegovu vjerodostojnost, je li obrani tijekom postupka dana stvarna mogućnost da osporava uporabu određenog dokaza i, konačno, kolika je važnost tog dokaza za konkretni postupak, radi li se o jedinom ili odlučujućem dokazu, ili postoje i podupirući dokazi.

5. ZAKLJUČAK

Ključna okolnost vezano uz pitanje mogu li se informacije koje su prikupljene kroz tajni nadzor platforme *Sky ECC* koristiti kao dokaz u kaznenom postupku u Hrvatskoj jest činjenica da se u tim slučajevima radilo o masovnom nadzoru (*bulk interception*) svih korisnika aplikacije, unaprijed neodređenih osoba u odnosu na koje nije postojala osnova sumnje da su počinile kazneno djelo ili da su sudjelovale u njegovu počinjenju. To znači da su te informacije prikupljene na način koji hrvatsko pravo ne dopušta. Ipak, sama ta činjenica, iako značajna, nije nužno i dovoljna da bi se donio zaključak o tome jesu li na taj način prikupljene informacije nezakonit dokaz u hrvatskom kaznenom postupku, iako je prema predmetu ESLJP-a *Big Brother* od velike važnosti kako nacionalno pravo regulira takvo prikupljanje podataka. Da bi nadležni sud dao odgovor na to pitanje, treba razmotriti sljedeće okolnosti i primijeniti sljedeće pravne standarde:

1. Istražiti činjenične i pravne okolnosti pod kojima je došlo do prikupljanja dokaza u Francuskoj.[66] Bez uvida u te okolnosti nemoguće je donijeti valjan zaključak o mjeri u kojoj način pribavljanja dokaza suštinski odstupa od temeljnih načela hrvatskog pravnog poretka. Propust da se te okolnosti utvrde treba cijeniti u korist obrane. Bilo koji informacijski deficit vezano uz činjenične i pravne okolnosti prikupljanja dokaza predstavlja istodobno ograničenje prava obrane. Što je deficit takvih informacija veći, veće je i ograničenje prava obrane; istodobno isto pruža

[66] V. npr. i recentne presude u Italiji i Srbiji. Kako ističe Đorđević, „Napetost raste odlukom Apelacionog suda u Beogradu iz avgusta 2023. godine da ukine presudu u Stolićevom slučaju i vrati je nazad prvostepenom sudu na ponovno razmatranje. Razlog je zakonitost nadzora Sky ECC komunikacije." Đorđević, S. *Neizvesna budućnost Sky ECC prepiske u sudskim postupcima*, 5. studenog 2023., dostupno na: https://autonomija.info/neizvesna-buducnost-sky-ecc-prepiske-u-sudskim-postupcima/. (12. 11. 2023.).

nemogućnost ispitivanja zakonitosti prikupljanja dokaza i odobravanja posebnih dokaznih radnji.

2. Prilikom ocjenjivanja okolnosti u kojima je došlo do prikupljanja dokaza potrebno je uzeti u obzir činjenicu da je postupljeno protivno odredbama prava EU-a (čl. 31. Direktive 2014/41) i protivno hrvatskom pravu (čl. 42.an st. 3. Zakona o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije). Domaće nadležno tijelo onemogućeno je u obavljanju svoje Zakonom o pravosudnoj suradnji dodijeljene jamstvene zadaće.
3. Prilikom ocjenjivanja načina na koji je proveden transfer dokaza potrebno je utvrditi je li inicijalno došlo do spontane razmjene informacija između tijela koja su zadužena za provedbu zakona i je li ta spontana razmjena informacija provedena u skladu s odredbama prava EU-a (čl. 7. st. 2. Okvirne odluke 2006/960).
4. Prilikom ocjenjivanja načina na koji je proveden transfer dokaza potrebno je utvrditi je li postupljeno u skladu s čl. 6. st. 1. (b) Direktive 2014/41, odnosno u skladu s odredbom čl. 42.c Zakona o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije. Uputno je da se vezano uz tumačenje čl. 6. st. 1. (b) Direktive 2014/41 nadležni domaći sud prethodnim pitanjem obrati Sudu Europske unije.
5. Prilikom davanja odgovora na pitanje radi li se o zakonitim dokazima u hrvatskom postupku u kontekstu svih okolnosti prikupljanja i transfera dokaza potrebno je ocijeniti odstupa li način prikupljanja dokaza suštinski od temeljnih načela hrvatskog kaznenog zakonodavstva te na koji se način uporaba tih dokaza odražava na prava obrane i na pravičnost postupka.

Ujedno je potrebno u predmetima koji uključuju aplikacije poput *Sky ECC* svakako i utvrditi (6.) kada je masovni nadzor svih korisnika aplikacije, tj. unaprijed neodređenih osoba u odnosu na koje nije postojala osnova sumnje da su počinile kazneno djelo ili da su sudjelovale u njegovu počinjenju, dopušten po hrvatskom pravu i za koje postupke. Potrebno je razlikovati i prikupljanje podataka obavještajnih zajednica i prikupljanje za potrebe vođenja kaznenog postupka, poglavito pravila o provođenju zakonom propisanih posebnih dokaznih radnji. Čini se da masovno prikupljanje podataka takvu razliku, koja mora biti jasna, čini upitnom, što otvara dodatna pravna pitanja, poglavito vezana uz zaštitu ljudskih prava.

LITERATURA

1. Allegreza, S., Collecting Criminal Evidence Across the European Union: The European Investigation Order Between Flexibility and Proportionality, u: S. Ruggeri (ur.), *Transnational Evidence and Multicultural Inquiries in Europe*, Springer, 2014, str. 51–67.
2. Arasi, S., The EIO Proposal and the Rules on Interception of Telecommunications, u: Ruggeri S. (ur.), *Transnational Evidence and Multicultural Inquiries in Europe*, Springer, 2014, str. 127–137.
3. Bachmaier Winter, L., *Mutual Admissibility of Evidence and electronic Evidence in the EU*, Eucrim, 2. studenog 2023., dostupno na: https://eucrim.eu/articles/mutual-admissibility-of-evidence-and-electronic-evidence-in-the-eu/ (5.11.2023.).
4. Bachmaier Winter, L., *European investigation order for obtaining evidence in the criminal proceedings Study of the proposal for a European directive*, Zeitschrift für Internationale Strafrechtsdogmatik, vol. 5, br. 9, 2010, str. 580–589.
5. Bajović, V., *EncroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku*, CRIMEN, vol. XIII, br. 2, 2022, str. 154–179.
6. Belfiore, R., *The European Investigation Order in Criminal Matters: Developments in Evidence-gathering across the EU*, European Criminal Law Review, vol. 5, br. 3, 2015, str. 312–324.
7. Daniele, M., *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, New Journal of European Criminal Law, vol. 6, br. 2, 2015, str. 179–194.
8. Đurđević, Z., *Lisabonski ugovor: prekretnica u razvoju kaznenog prava u Europi*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 15, br. 2, 2008, str. 1077–1127.
9. Gleß, S., Wahl, T:, Art. 7 EU-RhÜbk, u: Schomburg W., Lagodny O. (ur.), *Internationale Rechtshilfe in Strafsachen*, 6. potpuno prerađeno izdanje, C. H. Beck, 2020.
10. Gleß, S., *Zum Prinzip der gegenseitigen Anerkennung,* Zeitschrift für Internationale Strafrechtsdogmatik (ZStW), vol. 116, br. 2, 2004, str. 354–356.
11. Guerra, J., Janssens C., *Legal and Practical Challenges in the Application of the European Investigation Order*, Eucrim, br. 1, 2019, str. 46–53.
12. Hržina, D., *Novela Zakona o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije*, Pravosudna akademija, 2018.
13. Joubert, C., *Judicial Control of Foreign Evidence in Comparative Perspective*, Rozenberg Publishers, 2005.
14. Jurić, M.; Roksandić, S., *Access to Telecommunication Data in Criminal Justice (Croatia*), Access to Telecommunication Data in Criminal Justice A Comparative Legal Analysis, drugo izmijenjeno i dopunjeno izdanje, u: Sieber, U.; Von zur Muehlen, N.; Tropina, T. (ur.), Berlin, Duckner & Humblot, 2021, str. 377–418.
15. Karsai, K., *Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters*, Hungarian Journal of Legal Studies, vol. 60, br. 2, 2019, str. 155–172.
16. Krapac D., *Kazneno procesno pravo, knjiga prva: Institucije*, Narodne novine, Zagreb, 2014.
17. Krapac, D., *Pogled na neke važnije odredbe novog hrvatskog kaznenog zakonodavstva o organiziranom kriminalitetu i pitanja njihove praktične primjene*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 5, br. 2, 1998, str. 511-543
18. Kuczyńska, H., *Admissibility of evidence obtained as a result of issuing an European investigation order in a Polish criminal trial*, Review of European and comparative law, vol. XLVI, br. 3, 2021, str. 67–92.
19. Kusak, M., *Mutual admissibility of evidence and the European investigation order: aspirations lost in reality*, ERA Forum, vol. 19, 2019, str. 391–400.
20. Ljubanović, V., Novokmet, A., Tomičić, Z., *Kazneno procesno pravo*, Grafika, Osijek, 2020.

21. Mrčela, M., *Pravna valjanost dokaza pribavljenih u inozemstvu*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 7, br. 1, 2000, str. 83–108.
22. Oerlemans, J. J.; Royer, S., *The future of data driven investigations in light of the Sky ECC operation*, New Journal of European Criminal Law, Volume 0: Ahead of Print, 2023, str. 1–25.
23. Pauli, G., *Zur Verwertbarkeit der Erkenntnisse ausländischer Ermittlungsbehörden – EncroChat*, Neue Zeitschrift für Strafrecht, vol. 41, br. 3, 2021, 146-149.
24. Pisarić, M., *Encryption as a challenge for European law enforcement agencies*, Australasian Policing, vol. 13, br. 1, 2021, str. 611–619.
25. Rafaraci, T., General Considerations on the European Investigation Order, u: S. Ruggeri (ur.), *Transnational Evidence and Multicultural Inquiries in Europe*, Springer, 2014, str. 37–44.
26. Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy artificial intelligence and its use by law enforcement authorities: where do we stand*, u:Vrcek, N, *et al*. (ur.), 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Croatian Society for Information, Communication and Electronic Technology – MIPRO, 2022, str. 1395–1402.
27. Sagittae, G., *On the lawfuness of the EncroChat and Sky ECC-operations,* New Journal of European Criminal Law, vol. 14, br. 3, 2023, str. 273–293.
28. Satzger, H., *Gefahren für eine effektive Verteidigung im geplanten europäischen Verfahrensrecht – eine kritische Würdigung des Grünbuchs zum strafrechtlichen Schutz der finanziellen Interessen der Europäischen Gemeinschaften und zur Schaffung einer europäischen Staatsanwaltschaft*, Strafverteidiger, vol. 23, 2003, str. 137–149.
29. Schaar, P., *ECHR: Mass surveillance by British secret service violated European Convention on Human Rights*, u: Kahler, Thomas (ur.), Turning Point in Data Protection Law, Nomos, 2000, str. 63–66.
30. Schuster, Frank Peter, *Verwertbarkeit von Beweismitteln bei grenzüberschreitender Strafverfolgung*, Zeitschrift für internationale Strafrechtsdogmatik, vol. 11, br. 8, 2016, 564–573.
31. Schünemann B., *Ein Gespenst geht um in Europa – Brüsseler „Strafrechtspflege" intra muros*, Goltdammers Archiv, vol. 151, 2002, 501–516.
32. Simović, M., Šikman, M., *Sadržaj šifrovane komunikacije (Ennercom, Encrochat, Sky ECC, Anom, Exclu) kao dokaz u krivičnom postupku*, Pravo i pravda, vol. 21, br. 1, str. 227–254.
33. Stoykova, R. (Adi), *Enchrochat: The hacker with a warrant and fair trials?*, Forensic Science International: Digital Investigation, vol 46, 2023, 301602, str. 1-14.
34. Suominen, A., *The principle of Mutual Recognition in Cooperation in Criminal Matters*, Larcier Intersentia, 2011.
35. Šugman Stubbs, K., *Ocjena dokaza pribavljenih u inozemstvu: teorijski problemi i slovenska sudska praksa*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 21, br. 1, 2014, str. 111–133.
36. Tripalo, D., *Priznanje dokaza izvedenih pred pravosudnim tijelima strane države*, dostupno na: https://www.vsrh.hr/kazneno-pravo-drazen-tripalo-mag-iur.aspx (27. 10. 2023.).
37. Vermeulen, G., De Bondt, W., Van Damme, Y., *EU Cross Border Gathering and Use of Evidence in Criminal Matters. Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence?* Maklu, Antwerpen-Apeldoorn-Portland, 2010.
38. Vincent, S., Preventing the Police State: International Human Rights Laws Concerning Systematic Government Access to Communications Held or Transmitted by the Private Sector, u: Cate, F. H.; Dempsey, J. X. (ur.), *Bulk Collection: Systematic Government Access to Private-Sector Data*, New York, 2017, str. 355–380.
39. Vullierme, L. N., Data Protection in the Internet: French report, u: Vicente, D.M.; de Vasconcelos Casimiro, S. (ur.), *Data Protection in the Internet*, Springer, 2019. str. 159-181.

40. Watt, Elisa, *The right to privacy and the future of mass surveillance,* The International Journal of Human Rights, vol. 21. br. 7, 2017, str. 773–799.
41. Zimmermann, Frank, *Die Verwertbarkeit von Auslandsbeweisen im Lichte der Encro-Chat-Ermittlungen*, Zeitschrift für internationale Strafrechtswissenschaft (ZfIStW), vol. 1, br. 2, 2022, str. 173–190.

Summary

Zoran Burić, PhD [*]
Marc Engelhart, PhD [**]
Ante Novokmet, PhD [***]
Sunčana Roksandić, PhD [****]

THE ADMISSIBILITY OF THE RESULTS OF MASS SURVEILLANCE OF COMMUNICATION AS EVIDENCE IN CROATIAN CRIMINAL PROCEDURE: THE SKY ECC CASE

The paper analyses whether and to what extent information collected through mass surveillance of communications can be used as evidence in Croatian criminal proceedings. It concerns information collected in France through the joint investigative teams of the French, Dutch and Belgian authorities, with the help and cooperation of Europol and Eurojust. The primary specificity of this information is based on the fact that it does not reflect data collected through targeted surveillance of a predetermined number of persons suspected of criminal activities, but about data collected through the surveillance of all users of a certain communication network – Sky ECC – which, based on cryptography, guaranteed its users complete privacy protection without the possibility of its external supervision, including by law enforcement authorities. In addition, the network was available on the market to anyone who wanted to buy it through a registered legal activity. The question of the legality of the evidence is considered primarily through the prism of the factual and legal circumstances of obtaining information in France and its transfer to Croatia. In relation to the legal circumstances, special attention is paid to the standards prescribed by EU law regarding the acquisition and transfer of evidence.

Keywords: Sky ECC, mass surveillance of communications, evidence obtained abroad, illegal evidence in criminal proceedings

[*] Zoran Burić, PhD, Associate Professor in the Department for Criminal Procedure, University of Zagreb Faculty of Law; zoran.buric@pravo.unizg.hr; https://orcid.org/0000-0001-5353-8478

[**] Dr. sc. Marc Englehart, odvjetnik i naslovni profesor, Sveučilište Ludwiga Maximiliana u Münchenu, Pravni fakultet; marcengelhart@googlemail.com; ORCID iD: https://orcid.org/0000-0001-8848- 5468

[***] Ante Novokmet, PhD, Associate Professor in the Department for Criminal Procedure, Faculty of Law, University Josip Juraj Strossmayer in Osijek; ante.novokmet@pravos.hr; https://orcid.org/0000-0001-8833-9751

[****] Sunčana Roksandić, PhD, Associate Professor in the Department for Criminal law, University of Zagreb Faculty of Law, Head of Department of Criminal Law; suncana.roksandic@pravo.hr; https://orcid.org/0000-0003-3523-6032