UDK: 343.983.2:004.056.55
doi: 10.5937/crimen2202154B
Originalni naučni rad
primljen / prihvaćen: 20.09.2022 / 19.10.2022

*Vanja Bajović**
Univerzitet u Beogradu, Pravni fakultet

ENCROCHAT I SKY ECC KOMUNIKACIJA KAO DOKAZ U KRIVIČNOM POSTUPKU

Apstrakt: U radu se razmatra problematika pravne prirode i dokaznog značaja podataka pribavljenih nadzorom i dekodiranjem kriptovanih komunikacionih platformi EncroChat i Sky ECC. Prvi deo rada bavi se načinom na koji je sproveden nadzor nad ovim platformama, pravnom uporištu takvih radnji, pravnom osnovu za dostavljanje pribavljenih podataka drugim državama, njihovoj oceni i daljoj upotrebi u krivičnom postupku. U drugom delu bavimo se pravnom prirodom pribavljenih podataka kroz dilemu da li se radilo o ciljanom nadzoru u krivičnom postupku ili masovnom nadzoru sprovedenom od strane obaveštajnih službi kao i praksom ESLJP vezanom za ova pitanja i zaštitu člana 8 EKLJP. Imajući u vidu da mnogi podaci vezani za otkrivanje i obelodanjivanje ovih platformi još uvek nisu dostupni javnosti, analiza je mahom rađena na osnovu raspoloživih izveštaja pojedinih organizacija i odluka donetih od strane sudova u Nemačkoj i Velikoj Britaniji.

Ključne reči: EncroChat, SkyEcc, ocena dokaza pribavljenih u inostranstvu, masovni nadzor.

UVOD

Razvoj digitalne tehnologije obesmišljava postojeće ustavne i zakonske odredbe koje još uvek govore o „nadzoru i zapleni pisama i drugih pošiljki" iako je svet već decenijama unazad sa pisama, razglednica i čestitki prešao na e-mailove i digitalne čestitke, sa fiksnih telefona na mobilne, sa SMS poruka na komunikacione platforme vezane za internet poput Viber-a, WhatsUp-a i Telegrama, a poslednjih godina se sve više govori i o kriptovanim odnosno šifrovanim uređajima koji garantuju tajnost i sigurnost komunikacije. Pod lupu javnosti ovi uređaji su dospeli nakon otkrića da kriminalci za svoju komunikaciju ne koriste „klasične metode" koje zakonici o krivičnim postupcima imaju u vidu, poput pisama, fiksnih ili mobilnih telefona, već koriste najnovija tehnička dostignuća poput kriptovanih komunikacionih platformi sa serverima u inostranstvu, stvarajući tako „problem" nadležnim organima da otkriju i dešifruju komunikaciju kao i da je podvedu pod neku od postojećih dokaznih radnji.

* Vanredni profesor, bajovic@ius.bg.ac.rs.

„Problem" je eskalirao i dospeo u centar pažnje mnogih evropskih država nakon „razbijanja" komunikacionih platformi EncroChat i SKY Ecc, što je svakako doprinelo otkrivanju (i sprečavanju) brojnih krivičnih dela od strane kriminalnih grupa, ostavljajući istovremeno brojna pitanja otvorenim, počevši od načina otkrivanja komunikacije, dostavljanja materijala drugim državama i njegovog korišćenja u krivičnim postupcima, osnovanosti i dopuštenosti tzv. „masovnog nadzora" koji ne pogađa samo „kriminalce" već i „obične građane" odnosno sve korisnike određenih komunikacionih platformi.

1. KAKO SU OTKRIVENI ENCROCHAT I SKY ECC?

EncroChat i Sky ECC su komunikacione platforme izgledom identične „pametnim" mobilnim telefonima koje pretplatnicima omogućavaju poverljivu komunikaciju koja se ne odvija preko klasičnih mobilnih operatera, već putem aplikacija za razmenu poruka zasnovanim na posebnom protokolu (tzv. OTR protokol ili *Off-the-Record Messaging*) koji obezbeđuje momentalno šifrovanje poruke i njenu transmisiju preko centralnih servera koji su se nalazili u inostranstvu odnosno, koliko je za sada poznato, u Francuskoj i Kanadi.

Samo posedovanje ovih uređaja nije bilo zabranjeno, oni su, na različitim internet stranama reklamirani uz garancije sigurne komunikacije bez mogućnosti prisluškivanja, a na web-strani kompanije Sky ECC čak je i nuđena nagrada od četiri miliona dolara onome ko bi uspeo da dekodira enkripciju ove mreže! Izgledom se ovi uređaji nisu razlikovali od klasičnih mobilnih telefona nove generacije, osim što nisu sadržali kameru, mikrofon i GPS, poruke su automatski brisane posle određenog vremena, a telefon je posedovao i posebno dugme na čiji pritisak bi se brisao celokupan sadržaj. Shodno tome, da je policija i zaplenila neki od ovih uređaja, klasičnim „uviđajem" ne bi mogla da pribavi bilo kakav podatak, jer sami telefoni nisu sadržali nikakav „škakljivi" materijal. Sa ovih telefona nije bilo moguće komunicirati sa „običnim" mobilnim telefonima, već je preduslov bio da lice sa kojim komunicirate takođe poseduje poseban EncroChat ili Sky uređaj. Anonimnost komunikacije se obezbeđivala automatskim šifrovanjem poruke koja se šalje, tako da se, i pod pretpostavkom njenog „hvatanja" tokom prenosa, ona bez koda za dešifrovanja ne može pročitati, dok se anonimnost korisnika obezbeđivala time što prilikom kupovine ili instalacije ovih uređaja korisnik ne ostavlja svoje lične podatke, a na „mreži" odnosno tokom komunikacije sa drugim korisnicima se koristio nadimak koji bi korisnik sam sebi dao.

Pod lupu francuske žandarmerije ovi telefoni su dospeli 2017. godine, kada je primećeno da veliki broj pripadnika „kriminalnog miljea" poseduje EncroChat uređaje i da kompanija posluje sa servera koji se nalaze u Francuskoj.[1] Francuska je 2019. godine otvorila slučaj pred Eurojust-om i u aprilu 2020. godine formiran

1 Europol/Eurojust joint press release (02. 07. 2020): "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe", https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, 21. avgust 2022.

je zajednički istražni tim Francuske i Holandije sa učešćem Europol-a.[2] Analizom zaplenjenih telefona je ustanovljeno da se komunikacija odvijala preko servera koji se nalazio u Francuskoj, pa je naredbom istražnog sudije u Lilu dozvoljen nadzor kompjuterskih podataka na serveru i terminalima povezanim sa tim serverom, kao i preusmeravanje tokova podataka (DNS preusmeravanje) sa datog servera.[3]

Naredba koju je izdao sud u Lilu odnosila se na vlasnika domena EncroChat kome se stavljalo na teret krivično delo krivičnog udruživanja u pripremi krivičnog dela, obezbeđivanju sredstava kriptologije, prenosu sredstava kriptologije i uvozu sredstava kriptologije. Pored toga, naredba je bila usmerena i prema samom serveru za dopisivanje (EncroChat) nakon čega su pribavljene sve poruke sa tog servera, pretpostavlja se svih korisnika ove aplikacije. Francusko pravo poznaje posebnu dokaznu radnju „upada u računarski sistem" po kojoj u postupcima za organizovani kriminal istražni sudija, nakon pribavljenog mišljenja javnog tužioca, može dozvoliti istražiteljima „unošenje tehničkog uređaja" kojim bi se obezbedio pristup, skladištenje i prenos podataka koji se nalaze u uređaju, i bez saglasnosti njegovog vlasnika (čl. 706–102–1 francuskog ZKP).[4] Tehnički gledano, „uređaji" mogu biti ubačeni neposredno, ako istražitelji imaju pristup mobilnom telefonu ili računaru osumnjičenog ili „na daljinu" odnosno putem raznih virusa ili trojanaca, što je, pretpostavlja se bio slučaj kod „razbijanja" EncroChat-a.

Za sada nije nedvosmisleno objašnjeno na koji način je pribavljen sadržaj sa ovih platformi, da li su poruke bile pribavljane u realnom vremenu, odnosno u trenutku odašiljanja ili primanja ili su već uskladištene poruke „skidane" sa servera i uređaja korisnika, a sporan je i osnov masovnog nadzora korisnika širom sveta[5], na osnovu naredbe istražnog sudije u Lilu. U vezi sa tim, nedavno je podneta i predstavka ESLJP, mada njegovu odluku ne treba očekivati u skorije vreme.[6] Poznato je da je nadzor nad mrežom EncroChat prestao u junu 2020. godine, nakon što je kompanija obavestila svoje korisnike da je „sistem probijen" savetujući im da ne ko-

2 Europol/Eurojust /2021/: "Third Report of the Observatory Function on Encryption", https://www.europol.europa.eu/cms/sites/default/files/documents/3rd_report_of_the_observatory_function_on_encryption-web.pdf, 21. avgust 2022.

3 Higher Regional Court Hamburg 2nd Criminal Senate, no. Ws 2/21 – 7 OBL 3/21 v. 29. 01. 2021., par. 8, https://www.landesrecht-hamburg.de/bsha/document/JURE210003021, 21. avgust 2022.

4 *Code de procedure penale*, 1958, Modifie par LOI n. 219-222 du 23 mars 2019. https://codes.droit.org/PDF/Code%20de%20proc%C3%A9dure%20p%C3%A9nale.pdf, 21. avgust 2022.

5 Po izveštaju Evropola, nadzirana je komunikacija „na hiljade korisnika širom sveta, dok iz odluke nemačkog suda proizilazi da je mera pogodila 32.477 korisnika u 121 državi, od čega je samo 380, u potpunosti ili povremeno bilo locirano na francuskoj teritoriji. Higher Regional Court Hamburg. *op. cit*. par. 8.

6 Predstavku su podnela dvojica britanskih državljana, koja tvrde da im je korišćenjem EncroChat komunikacije kao dokaza u postupku povređeno pravo na pravično suđenje iz člana 6., pravo na poštovanje privatnog života i prepiske iz čl. 8. kao i pravo na efikasno pravno sredstvo iz čl. 13. Konvencije (A. L. v. France, no. 44715/20 and E. J. v. France, no. 47930/21). Predstavka je dostavljena francuskoj vladi na odgovor 08. 12. 2021., ali ovaj odgovor ne treba očekivati brzo, imajući u vidu da Francuska još uvek nije odgovorila na podneske dostavljene 2017. godine, kojim se osporavaju odredbe Zakona o obaveštajnim delatnostima. ECHR, *Mass surveillance*, june 2022., p. 7.,: https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf, 21. avgust 2022.

riste više ove uređaje jer kompanija više ne može garantovati za bezbednost njihove komunikacije.[7]

Još više nedoumica i nepoznanica postoji u pogledu otkrivanja komunikacije koja se odvijala putem platforme Sky Ecc. Ovu aplikaciju lansirala je kanadska kompanija Sky Global, koja je zakonito poslovala u Kanadi, a uređaji su regularno reklamirani na internet strani kompanije, kao garanti „sigurne" i neprobojne komunikacije. Početkom marta 2021. godine Europol je izdao saopštenje da su istražni timovi Belgije, Francuske i Holandije uz podršku Europol-a i Eurojust-a, izvršili veliki broj pretresa i oduzimanja predmeta širom Belgije i Holandije i lišili slobode na stotine pripadnika organizovanih kriminalnih grupa, nakon što su uspeli da dešifruju komunikaciju koja se odvijala putem Sky Ecc platforme.[8] Preliminarna istraga je započeta još sredinom 2018. u Belgiji, nakon što je policija od osumnjičenog oduzela ovaj uređaj, a ustanovljeno je da veliki broj pojedinaca širom sveta koristi ovu aplikaciju, koja ima sopstvenu infrastrukturu sa sedištem u Kanadi i koristi kompjuterske servere locirane u Evropi.[9] „Napad" je navodno izveden po uzoru na razotkrivanje EncroChata koje je imalo dve faze. U prvoj fazi policija je presretala šifrovanu komunikaciju sa Sky Ecc mreže, a kompjuterski eksperti su radili na njenom dešifrovanju. Krajem 2020. godine holandska policija je uspela da dešifruje presretane poruke, a u drugoj fazi policija je bila u mogućnosti da uživo nadzire komunikaciju koja se odvijala preko ove platforme. Kompanija Sky Global je sa druge strane negirala ove tvrdnje ističući da je „sistem razbijen" tako što su na tržište kao „mamac" ubačeni lažni i nezaštićeni Sky telefoni, što bi aludiralo na neki vid prikrivenih aktivnosti u krivičnom postupku.[10] Procenjuje se da je sredinom februara 2021., policija nadzirala komunikaciju oko 70.000 korisnika Sky ECC uređaja,[11] što je maltene dvostruko veći broj u poređenju sa pretpostavljenim korisnicima EncroChat-a.

Nakon dekodiranja aplikacije i brojnih hapšenja širom Evrope, FBI je zaplenio Internet stranicu Sky Global, a SAD su izdale nalog za hapšenje osnivača i direktora kompanije, sa optužbama da su Sky uređaji prevashodno kreirani kako bi nadležnim organima onemogućili praćenje komunikacije pripadnika organizovanih kriminalnih grupa.[12] Kao odgovor na to, osnivač kompanije (*Jean Francois Eap*) je tvrdio da se našao na meti napada jer je osmislio uređaj koji je u stanju da zaštiti jedno

7 Hamilton, Fiona (02. 07. 2020). "Hundreds of arrests as police crack phone network used by crime bosses". *The Times*, https://www.thetimes.co.uk/article/hundreds-of-arrests-as-police-crack-phone-network-used-by-crime-bosses-h85qntqw3, 21. avgust 2022.

8 EUCRIM, *The European Criminal Law Associations' Forum*, 2021/1, p. 22., dostupno na: https://eucrim.eu/media/issue/pdf/eucrim_issue_2021-01.pdf, 21. avgust 2022.

9 Europol/Eurojust joint press release. *op. cit.*

10 NL Times (10. 03. 2012.): "Encrypted chat service Sky ECC denies being hacked by Dutch cops", https://nltimes.nl/2021/03/10/encrypted-chat-service-sky-ecc-denies-hacked-dutch-cops, 21. avgust 2022.

11 EUCRIM. *op. cit*., 2021/1, p. 22

12 US Department of Justice (12. 03. 2021.): "Sky Global Executive and Associate Indicted for Providing Encrypted Communication Devices to Help International Drug Traffickers Avoid Law Enforcement", https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices, 21. avgust 2022.

od osnovnih ljudskih prava-pravo na privatnost, štiteći građane od neopravdanog nadzora koji državne vlasti danas redovno sprovode.[13]

Shodno tome, još uvek ne postoje nedvosmisleni, javno dostupni podaci o načinu na koji je pribavljen sadržaj sa ovih platformi, što je od vitalnog značaja za upotrebu ovako pribavljenih sadržaja u krivičnom postupku.

2. PRIZNAVANJE I OCENA DOKAZA PRIBAVLJENIH U INOSTRANSTVU

Slučajevi EncroChat i Sky Ecc aktuelizovali su problematiku pribavljanja, prirode i ocene dokaza pribavljenih u inostranstvu. U vezi sa tim, postavlja se pitanje pravnog osnova za dostavljanje EncroChat i Sky komunikacije, njenog korišćenja u krivičnom postupku, ocene ovakvih dokaza od strane suda, kao i način i mogućnost njihovog izvođenja na glavnom pretresu.

2.1. Pribavljanje Sky ECC i EncroChat komunikacije kao dokaza

Prilikom odlučivanja o zakonitosti i prihvatljivosti dokaza mora se znati način njihovog pribavljanja, odnosno izvor dokaza, jer ZKP zabranjuje zasnivanje sudskih odluka na dokazima koji su sami po sebi ili prema načinu pribavljanja, u suprotnosti sa Ustavom, ZKP, drugim zakonima ili opšteprihvaćenim pravilima međunarodnog prava (čl. 16 st. 1. ZKP).[14]

Nadzor nad mrežom EncroChat sproveden je na osnovu naredbe suda i to „upadom u računarski sistem", a na osnovu člana 706–101–2 francuskog ZKP, a pretpostavlja se da je i Sky komunikacija pribavljena na sličan način. U vezi sa tim nameće se pitanje da li bi komunikacija koja se odvijala putem kriptovanih telefona u mnogim državama uopšte i mogla da bude otkrivena putem postojećih dokaznih radnji, da takvi dokazi nisu dostavljeni putem međunarodne pravne pomoći?

Prema podacima iz zajedničkog izveštaja Europol/Eurojust, svega nekolicina evropskih država ima posebnu regulativu koja reguliše tajno pristupanje šifrovanoj elektronskoj komunikaciji i njeno dekodiranje (*online* nadzor, upad u računarski sistem, korišćenje tehničkih sredstava za pristup digitalnim dokazima i sl.).[15] Ona se mahom svodi na tajno postavljanje posebnih softvera u uređaje, bilo a) „fizički"

13 „Sky Global tehnologija radi za dobrobit svih. Ona nije kreirana da bi sprečila policiju da nadgleda kriminalne grupe, već je kreirana kako bi sprečila nadzor i špijuniranje globalne zajednice. Optužnica protiv mene u SAD je još jedan primer vlasti koje pokušavaju da ućutkaju svakoga ko ustane protiv neopravdanog nadzora." Charlie Osborne (15. 03. 2021.): "Sky Global CEO indicted over encrypted chat drug trafficking, calls allegations an 'outrage'", https://www.zdnet.com/article/sky-global-ceo-indicted-over-encrypted-chat-drug-trafficking-claims-erosion-of-right-to-privacy/, 21. avgust 2022.

14 Zakonik o krivičnom postupku, „*Sl. glasnik* RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021-odluka US i 62/2021-odluka US.

15 To su Francuska, Nemačka, Holandija, Danska, Poljska, Švedska i Švajcarska. Pored toga i italijanski sudovi su u praksi prihvatili zakonitost korišćenja trojanskih softvera koji, nakon „ubacivanja" u uređaj omogućavaju pristup svim podacima koji se u njemu nalaze, kao i snimanje komunikacije. Vrhovni kasacioni sud je zauzeo stav da je primena ove mere moguća samo u

– ako nadležni organi imaju pristup uređaju ili b) na daljinu – ubacivanjem tzv. virusa ili trojanaca, koji zatim omogućavaju kopiranje celokupnog sadržaja sa uređaja i njeno prosleđivanje nadležnim organima. Međutim još uvek ne postoji opšti konsenzus od uvođenja ovih mera, prvenstveno usled bojazni od tzv. „masovnog nadzora".[16]

Naše pravo čak i ne reguliše posebno digitalne dokaze već ih podvodi pod isprave, propisujući da „računarski podatak koji je podoban ili određen da služi kao dokaz činjenice koja se utvrđuje u postupku predstavlja ispravu" (čl. 2 st. 1 t. 26 ZKP).[17] Prema odredbama ZKP dokazivanje ispravom se vrši čitanjem, gledanjem, slušanjem ili uvidom u sadržaj isprave na drugi način (čl. 138 st. 1). Imajući u vidu specifičnost računarskih podataka, u teoriji se osnovano navodi da se dokazivanje elektronskim dokazom vrši uvidom u njegov sadržaj na drugi način, a to se može preduzeti samo veštačenjem.[18]

Kako ZKP RS ne reguliše posebno digitalne dokaze i digitalne istrage, računarski podaci, odnosno elektronski zapisi odnosno isprave (u ovom digitalnom obliku) se, poput svih drugih dokaza pribavljaju nekom od zakonito propisanih dokaznih radnji.[19] S tim u vezi, ZKP posebno implicira da se oni mogu pribaviti oduzimanjem ili pretresanjem uređaja za automatsku obradu podataka (čl. 147 st. 3 i 152 st. 3 ZKP). Međutim, pod pretpostavkom da je naša policija oduzela Sky telefon i da je sud naredio njegovo pretresanje, ne bi pribavili ni jedan podatak imajući u vidu da su poruke automatski brisane nakon određenog vremena.[20] Internet provajderi i mobilni operateri su dužni da čuvaju komunikaciju godinu dana nakon od nje-

---

postupcima za najteža krivična dela, kao što su terorizam, organizovani kriminal i t. sl. Europol/ Eurojust /2021/. *op. cit.,* pp. 10-14.

16 Tako je Ustavni sud Austrije proglasio neustavnom odredbu ZKP kojom je predloženo uvođenje mere instaliranja posebnog programa (*Federal Trojan*) u računarski sistem, sa ciljem nadzora i snimanja kriptovanih poruka. U obrazloženju ove odluke je navedeno da je mera suprotna čl. 8 EKLJP jer „ne postoje garancije da je meru moguće ograničiti samo na otkrivanje i dokazivanje najtežih vidova kriminaliteta" već da se time nadležnim organima daje mogućnost da efektivno nadziru celokupnu *online* komunikaciju. Constitutional Court of Austria, AUT-2019-3-003, https://www.vfgh.gv.at/downloads/Bulletin_2019-3_AUT-2019-3-003_G_72-74_2019__ua.pdf, 16. avgust 2022.

17 U literaturi se osnovano upozorava na specifičnost računarskih podataka kao isprava pa se navodi da su veoma nepostojani, lako podležu izmenama i gubitku, mogu se umnožavati i kopirati bez ikakvih ograničenja, nevidljivi su za „nestručna" lica odnosno može ih protumačiti samo digitalni forenzičar itd. M. Pisarić /2016/: *Posebnosti dokazivanja dela visokotehnološkog krimi-nala*, doktorska disertacija odbranjena na Pravnom fakultetu Univerziteta u Beogradu, Beograd, pp. 95-100.

18 M. Pisarić /2020/: Prikupljanje elektronskih dokaza iz mobilnog telefona u praksi VKS Republike Srbije, *Kriminalistička teorija i praksa,* vol. 7, n° 2, p. 40.

19 U literaturi se osnovano navodi da su isprave samo „pismeni oblik" drugog dokaznog sredstva (V. Bayer /1989/: *Jugoslovensko krivično procesno pravo, knjiga druga, Pravo o činjenicama i njihovom utvrđivanju u krivičnom postupku*, Zagreb, p. 211.), odnosno izraz nekog drugog dokaznog sredstva koje se javlja u formi isprave (T. Vasiljević, M. Grubač /2011/: *Komentar Zakonika o krivičnom postupku*, Beograd, p. 299.).

20 Izuzetak bi predstavljala situacija da poruke nisu obrisane, kada bi mogle da budu fotografisane i korišćene kao dokaz i to kao uviđaj na pokretnoj stvari.

nog obavljanja,[21] ali u ovom slučaju komunikacija se nije odvijala putem domaćih mobilnih operatera ni internet provajdera. Mera tajnog nadzora komunikacije takođe bi u ovim slučajevima bila neproduktivna. Kao prvo bilo bi nemoguće izdati naredbu za primenu ove mere jer se Sky komunikacija odvijala preko SIM kartica stranih mobilnih operatera, a i pod pretpostavkom da je naređeno presretanje ove komunikacije, opet bi nadležni organi bili „u problemu" imajući u vidu da su poruke odmah nakon slanja bile šifrovane pa bi bez koda za dekodiranje bilo nemoguće prodreti u njihovu sadržinu. Računarsko pretraživanje podataka podrazumeva pretraživanje već obrađenih ličnih i drugih podataka i ono se po logici stvari vrši na serverima koji se nalaze na našoj teritoriji.

Shodno tome, predmetna komunikacija uopšte ne bi mogla da bude otkrivena dokaznim radnjama koje predviđa ne samo naše pravo, već i većina drugih evropskih zakonodavstava. U našem pravu dokaz pribavljen presecanjem Sky Ecc komunikacije predstavlja (elektronsku odnosno digitalnu) ispravu, pribavljenu putem međunarodne pravne pomoći, ali se opet kao prethodno nameće pitanje na koji način su ovakvi dokazi pribavljeni u zamoljenoj državi, pružaocu međunarodne pravne pomoći? U vezi sa tim, nije dovoljno reći da je dokaz pribavljen putem „međunarodne pravne pomoći", već je neophodno tačno ustanoviti izvor dokaza, odnosno način na koji je isprava/digitalni podatak pribavljena u toj stranoj državi kako bi se ispitala njena prihvatljivost kao dokaza u krivičnom postupku i pružila mogućnost njegovog izvođenja na glavnom pretresu.[22] Suprotnim postupanjem bi se faktički „ozakonili" i oni dokazi koji su u inostranstvu pribavljeni torturom, iznuđivanjem iskaza, narušavanjem nepovredivosti stana ili kršenjem drugih osnovnih prava pojedinca. Iako ESLJP u svojoj praksi ne analizira posebno (ne)zakonitost i prihvatljivost dokaza već njihovo izuzimanje ostavlja nacionalnim jurisdikcijama, ovaj Sud ispituje da li se upotrebom spornih dokaza dovode u pitanje prava zagarantovana EKLJP. U vezi sa tim je naglašeno da „pri utvrđivanju da li je postupak u celini bio pravičan, potrebno je posebno ispitati da li je podnosiocu predstavke data prilika da ospori autentičnost dokaza i da se protivi njihovoj upotrebi".[23] I kvalitet dokaza se mora uzeti u obzir, pod čime se podrazumeva da li okolnosti pod kojima je dokaz pribavljen bacaju sumnju na njegovu pouzdanost ili tačnost.[24] Stoga ne iznenađuje da su se nemački i britanski sudovi detaljno bavili pitanjem načina na koji je pribavljena EncroChat komunikacija, kao i osnova po kome je ona dostavljena ovim državama.

---

21 Po članu 128. Zakona o elektronskim komunikacijama („*Sl. glasnik RS*", br. 44/2010, 60/2013– odluka US, 62/2014 i 95/2018– dr. zakon), svaki operater, odnosno telekomunikacioni ili internet provajder dužan je da čuva podatke o komunikaciji godinu dana po obavljenoj komunikaciji i da ih učini dostupnim nadležnim organima.

22 Osnovano se ističe da „upotreba dokaznog materijala pribavljenog u drugoj državi otvara brojne dileme u oblasti dokaznog prava. Neke dokazne radnje preduzete na taj način teško se slažu sa procesnim načelom neposrednosti koje zahteva da se dokazi izvode neposredno pred sudom koji će izreći presudu, tj. pred domaćim sudom". M. Grubač, G. Ilić, M. Majić /2009/: *Komentar Zakona o međunarodnoj pravnoj pomoći u krivičnim stvarima*, Službeni glasnik, Beograd, p. 169, par. 8.

23 *Dragojevic v. Croatia*, App. No. 68955/11, 15. 01. 2015., par. 129.

24 *Jalloh v. Germany*, App. No. 54810/00, 11. 07. 2006., par. 96, *Khan v. the United Kingdom*, App. No. 35394/97, 12. 05. 2000., par. 35 i 37, *Allan v. the United Kingdom*, App. No 48539/99, 05. 02. 2003., par. 43

2.2. Ocena i prihvatljivost dokaza pribavljenih u inostranstvu

Različite države imaju različita dokazna pravila, što aktuelizuje pitanje ocene i prihvatljivosti dokaza pribavljenih u inostranstvu. Najjednostavnije rečeno, pitanje je da li je domaći sudija uopšte ovlašćen da ocenjuje zakonitost tako pribavljenih dokaza? U vezi sa tim, zakoni i međunarodne konvencije se retko izjašnjavaju, a pravna teorija daje nekoliko mogućih odgovora.

Pojedini autori prave podelu na test neutralnosti i test dvostruke prihvatljivosti.[25] Test „neutralnosti" podrazumeva da se strani dokaz ocenjuje kao da nije pribavljen u inostranstvu već se njegova valjanost ispituje isključivo kroz norme domaćeg prava. U tom smislu ako dokaz zadovoljava kriterijume prihvatljivosti koje propisuje pravo države molilje, on će biti prihvatljiv čak i ako bi bio nezakonit u državi u kojoj je pribavljen i obrnuto. Sa druge strane test „dvostruke prihvatljivosti" podrazumeva ocenu prihvatljivosti dokaza i po kriterijumima zamoljene države kao i države molilje. U tom smislu dokaz mora biti zakonit i po pravu države u kojoj je pribavljen i po pravu države u kojoj se koristi.

Navedena podela zanemaruje različitosti u pogledu dokaznih radnji različitih država, jer polazi od pretpostavke da dokazna radnja kojom je dokaz pribavljen mora postojati i u pravu države u kojoj se dokaz koristi, da bi se uopšte ispitala njena zakonitost. Tako primera radi, ako u pravu države molilje branilac mora prisustvovati saslušanju okrivljenog, dok u pravu zamoljene države to nije slučaj, primenom ovih kriterijuma bi se moglo odrediti da li će iskaz okrivljenog dat bez prisustva branioca u zamoljenoj državi biti prihvatljiv u državi molilji. Problem nastaje kad pravo države molilje uopšte ne poznaje dokaznu radnju kojom je dokaz pribavljen u zamoljenoj državi (primera radi presecanje Sky ECC ili EncroChat komunikacije), kada su navedene teorije faktički neprimenjive.

Zbog toga drugi autori navode više mogućih varijanti kod ocene prihvatljivosti dokaza pribavljenih u drugoj državi i dostavljenih putem međunarodne pravne pomoći.[26]

Prva varijanta je da domaći sudija uopšte nema ovlašćenje da se upušta u zakonitost dokaza pribavljenih u inostranstvu, već polazi od pretpostavke zakonitosti njihovog pribavljanja. Ova varijanta prihvaćena je u okviru država članica EU i to kroz evropske naloge za istragu, ali joj se zamera da nekontrolisano prihvatanje stranih dokaza predstavlja uvoz „potencijalno opasnih proizvoda" te da različitost jezika i proceduralnih pravila nameće zabrinutost u pogledu zaštite ljudskih prava u oblasti slobode, bezbednosti i pravosuđa unutar EU.[27] Veruje se da su njome najviše ugrožena prava odbrane jer se princip pravičnosti postupka žrtvuje zarad njegove efikasnosti.[28]

25 M. Mrela /2000/: Pravna valjanost dokaza pribavljenih u inozemstvu, *Hrvatski ljetopis za kazneno pravo i praksu* (Zagreb), vol. 7, n° 1, pp. 100-104.

26 K. Šugman Stubbs /2014/: Ocjena dokaza pribavljenih u inozemstvu: teorijski problemi i slovenska sudska praksa, *Hrvatski ljetopis za kazneno pravo i praksu* (Zagreb), vol. 21, n° 1, pp. 114-115.

27 S. Ruggeri /2012/: Investigative Powers Affecting Fundamental Rights and Principles for a Fair Transnational Procedure in Criminal Matters. A Proposal of Mutual Integration in the Multicultural EU Area, *CRIMEN* (III), n° 2, p. 148.

28 H. Satzger /2019/: Is mutual recognition a viable general path for cooperation?, *New Journal of European Criminal Law*, Vol 10(I), p. 53.

Druga mogućnost je da se procenjuje zakonitost dokaza pribavljenih u inostranstvu a samim tim i njihova validnost u unutrašnjem pravu, ali i ovde se postavlja pitanje po kojim merilima.

a) Moguće je najpre da sudija procenjuje zakonitost dokaza po pravu države u kojoj su pribavljeni (*locus regit actum*). U tom slučaju dokaz je prihvatljiv ako sud nađe da je u državi u kojoj je pribavljen, dokaz pribavljen u skladu sa zakonskim merilima, bez obzira na to da li je ista dokazna radnja predviđena i unutrašnjim zakonodavstvom i da li se u unutrašnjem pravu izvodi pod istim uslovima i na isti način. Za razliku od automatskog preuzimanja dokaza (prva varijanta), ovde sudija ispituje način na koji su dokazi pribavljeni u inostranstvu kako bi ispitao njihovu zakonitost.
b) Moguće je i da se dokazi pribavljeni u inostranstvu ocenjuju u skladu sa unutrašnjim propisima, što bi značilo da se ceni da li bi dokaz bio prihvatljiv po pravu one države u kojoj se koristi. Ovo opet nameće problem (ne) istovetnosti svih dokaznih radnji na međunarodnom nivou i teškoća da se zakonitost dokaza pribavljenog dokaznom radnjom koju domaći zakon uopšte ne predviđa, kasnije procenjuje po unutrašnjim propisima.
c) Moguća je i kombinacija ovih pristupa po kojoj bi sudija najpre ocenjivao da li je dokaz zakonito pribavljen u stranoj državi, a zatim da li bi tako pribavljen dokaz bio „valjan" po unutrašnjim propisima (pomenuti test „dvostruke prihvatljivosti"). Na kraju, postoji mogućnost uspostavljanja nekih zajedničkih standarda za sprovođenje dokaznih radnji i istražnih aktivnosti na „širem planu", što je još uvek utopijska zamisao.

Naš Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima (ZMPPKS)[29] predviđa da se radnje „male" međunarodne pomoći sprovode prema domaćim propisima (čl. 90), dakle u skladu sa principom *locus regit actum*, ali ne govori ništa o prihvatljivosti dokaznih i drugih procesnih radnji preduzetih u inostranstvu, na zahtev našeg suda. U teoriji se opravdano ističe da domaća država treba da prizna dejstvo procesnopravnoj radnji koju je strani pravosudni organ preuzeo u skladu sa svojim pravom, ali pod uslovom da to „nije u suprotnosti sa načelima njenog pravnog sistema i opšteprihvaćenim pravilima međunarodnog prava".[30] Dakle za razliku od sistema uzajamnog priznanja zastupljenog u okviru EU kroz evropske naloge za istragu, po kome se sadržina odluke uopšte ne ispituje već je dovoljno da ju je doneo nadležni organ države članice, međunarodna saradnja u krivičnim stvarima podrazumeva i određeno ispitivanje odluke u smislu njene usklađenosti sa unutrašnjim pravnim poretkom.[31] Tako primera radi dok se presude donete u okviru država članica EU u drugim državama članicama EU izvršavaju po automatizmu, u našem pravu moraju da prođu poseban postupak priznanja u kome se zamolnica pod određenim uslovima može i odbiti (čl. 63 ZMPPKS). Analogno tome i dokaze pribavljene u inostranstvu ne treba priznavati po automatizmu, dok se prethodno

29 Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima, „*Sl. glasnik RS*", br. 20/2009.

30 M. Grubač, G. Ilić, M. Majić. *op. cit.,* p. 181., par. 3.

31 O razlikama ova dva sistema: S. Ruggeri. *op. cit.,* pp. 147–169.

ne oceni zakonitost njihovog pribavljanja u zamoljenoj državi kao i prihvatljivost tako pribavljenih dokaza shodno članu 16 ZKP.

Ovo pitanje je od manjeg značaja na teritoriji država članica EU, imajući u vidu važenje Evropskih naloga za istragu. Reč je o sudskoj odluci koju izdaju ili odobravaju pravosudni organi države članice EU, radi izvršenja jedne ili nekoliko posebnih istražnih mera u drugoj državi članici, a radi pribavljanja dokaza. Ovaj nalog se može izdati i za pribavljanje dokaza koji se već nalaze u posedu nadležnih organa zamoljene države, što je upravo bio slučaj sa podacima pribavljenim sa servera EncroChat. Evropski nalog za istragu temelji se na načelu uzajamnog priznanja, koje nalaže prihvatanje odluka koje potiču iz drugih država članica.[32]

U vezi sa tim, Regionalni sud u Hamburgu je istakao da: „Nemačke vlasti ne mogu dovoditi u pitanje zakonitost dokaza pribavljenih u drugoj državi s obzirom da bi preispitivanje i ispravljanje strane sudske odluke dovelo u pitanje poštovanje njenog suvereniteta ili princip uzajamnog priznanja zastupljen unutar Evropske Unije... Na osnovu raspoloživih činjenica može se pretpostaviti da su dokazi u Francuskoj pribavljeni zakonito, u skladu sa unutrašnjom regulativom, postojala je naredba suda za sprovođenje dokazne radnje, a predmet istrage je bilo krivično delo u pogledu koga je, shodno francuskom krivičnom postupku, bilo moguće odrediti nadzor telekomunikacija." Takođe je naglašeno da se „ne može očekivati potpuna podudarnost dokaznih radnji sa nemačkim pravom, imajući u vidu razlike pravnih sistema u okviru država članica EU, ali da su principi poverenja i uzajamnog priznanja koji važe u okviru EU, zasnovani na poverenju u pravni sistem duge države članice, odnosno može se pretpostaviti da i druge članice EU poštuju fundamentalna prava zagarantovana njenom poveljom".[33] Međutim, nemački sud je ipak naglasio da se mere, odnosno dokazne radnje na osnovu kojih su dokazi pribavljeni u Francuskoj mogu primeniti i po nemačkom ZKP, te da će se u skladu sa tim pravilima i izvoditi na glavnom pretresu, praveći analogiju sa merom *online* pretresa (tajnog daljinskog pretraživanja informaciono-tehnoloških sistema) regulisanom članom 100b nemačkog ZKP.[34]

Osnovno pitanje i pred apelacionim sudom u Londonu bilo je pitanje načina na koji su dokazi pribavljeni, a u cilju ispitivanja da li bi dokazi pribavljeni na taj način u Velikoj Britaniji bili dozvoljeni. Shodno tome, britanski sud je cenio zakonitost dokazne radnje po unutrašnjim propisima, a „koplja su se lomila" oko dileme da li su dokazi pribavljeni presretanjem odnosno nadzorom komunikacije,[35] ili je pak

32 O ovom opširnije: M. Matić Bošković /2022/: *Krivično procesno pravo EU*, Institut za kriminološka i sociološka istraživanja, Beograd, pp. 37-51.

33 Higher Regional Court Hamburg. *op. cit.,* para. 77-88.

34 „Pretpostavka da je postupak sproveden u skladu sa pravom je potkrepljena i činjenicom da se mere primenjen u Francuskoj takođe mogu primeniti i u Nemačkoj, a u skladu sa čl. 100a i 100b ZKP". *ibid*, par. 93.

35 Po prihvaćenoj definiciji, presretanje predstavlja pribavljanje sadržaja komunikacije poslate telekomunikacionim sistemima ili poštanskim uslugama, od strane lica koje nije ni pošiljalac ni primalac poruke. Tipičan primer presretanja komunikacije je nadzor ili snimanje telefonskih razgovora, ali britanski zakon navodi i druge vidove presretanja, kao što je slanje kopije poruke licu kome nije namenjena odnosno upoznavanje sa sadržinom komunikacije u trenutku u kome

pribavljana uskladištena komunikacija sa servera i mobilnih uređaja. Sporno je bilo da li su poruke bile pribavljane u realnom vremenu, odnosno u trenutku slanja ili primanja ili su već uskladištene poruke „skidane" sa servera i uređaja korisnika. U zajedničkom izveštaju Europol/Eurojust je navedeno da su nadležni organi bili u mogućnosti da čitaju poruke u „realnom vremenu"[36], ali u tom slučaju bi pribavljen materijal bio neprihvatljiv u postupku pred britanskim sudovima. Britanski zakon (*Investigatory Powers Act*) ne dozvoljava korišćenje u dokaznom postupku materijala pribavljenog „presretanjem" komunikacije odnosno nadzorom telefonskih razgovora i drugih sredstava komunikacije u „realnom vremenu".[37] [38]

Nakon veštačenja rada platforme EncroChat od strane britanskih stručnjaka, ustanovljeno je da je francuska žandarmerija, po naredbi suda, zapravo ubacila virus („implant") u EncroChat uređaje, tako što je svim korisnicima poslala poruku da je neophodno ažuriranje softvera. Nakon što bi pristupili ažuriranju, virus je bivao instaliran u sistem i omogućavao je da se žandarmeriji prenesu svi podaci koji se nalaze na uređaju, a koji su zatim prosleđivani i Europol-u i policijama širom Evrope. Virus je prikupljao i druge podatke i to poruke u trenutku kucanja kao i prilikom prijema, što je omogućavalo njihovo čitanje i pre nego što bi bile poslate odnosno šifrovane, što je *de facto* uporedivo sa situacijom kada neko stoji iznad vašeg telefona i neposredno čita poruke koje kucate ili primate.

> „Vrlo je jasno i bez bilo kakvih kontroverzi, da je efekat virusa bio da dovede do eksfiltracije poruka sa uređaja; poruke nisu preuzimane nakon slanja sa uređaja pošiljaoca niti pre prijema na uređaj primaoca. Ovaj zaključak je potkrepljen činjenicom da u vreme preuzimanja poruke nisu bile šifrovane, odnosno da su pribavljane pre šifrovanja sa uređaja sa koga su slate ili nakon dešifrovanja na prijemnom uređaju."[39]

Za očekivati je da se naši sudovi ubrzo nađu pred istom dilemom, koja je utoliko veća jer je način pribavljanja Sky komunikacije još uvek „pod velom tajne". Ana-

---

se ona odvija, bilo kog lica koje nije pošiljalac ili primalac komunikacionog sadržaja. UK Government, *Intercept as Evidence* (2014.) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/388111/InterceptAsEvidence.pdf, 17. avgust 2022.

36 Europol/Eurojust /2021/. *op. cit.,* p. 37.

37 Član 56 ovog zakona zabranjuje korišćenje sadržaja presretnute komunikacije ili podataka iz te komunikacije kao dokaza u krivičnom postupku, a stav 5 istog člana presretnutu komunikaciju definiše kao onu komunikaciju koja je pribavljena tokom njenog prenosa putem poštanske službe ili telekomunikacionih sistema. https://www.legislation.gov.uk/ukpga/2016/25/section/4/enacted, 17. avgust 2022.

38 S tim u vezi, interesantno je napomenuti da je sud u Hamburgu, prilikom odlučivanja o prihvatljivosti ovih dokaza razmotrio obe varijante, upoređujući ih sa merama koje predviđa nemački ZKP i nalazeći da bi, u oba slučaja dokazi bili prihvatljivi u okviru dokazne radnje predviđene članom 100b nemačkog ZKP." Ako je zlonamerni softver instaliran u mobilni uređaj osumnjičenog, to je dozvoljeno u skladu sa članom 100b (3) par. 1 StPO. Ako su poruke pribavljene preusmeravanjem tokova komunikacije sa servera, to bi bilo dozvoljeno u skladu sa članom 100b (3) par. 2 StPO, imajući u vidu da je okrivljeni koristio informaciono-tehnološki sistem operatera EncroChat, a pristup isključivo mobilnom telefonu okrivljenog ne bi doveo do pribavljanja podataka". Higher Regional Court Hamburg. *op. cit.,* para. 68.

39 Royal Courts of Justice Strand, London, WC2A 2LL, R v A and others [2021] EW CA Crim 128, 05. 02. 2021., par. 149., https://www.judiciary.uk/wp-content/uploads/2021/02/A-v-R.pdf, 17. avgust 2022.

logija sa pribavljanjem dokaza u slučaju EncroChat je neprimenjiva jer, za razliku od kompanije EncroChat koja nije imala zvanično sedište ni ovlašćene predstavnike, kompanija Sky Global je zakonito poslovala u Kanadi gde su se i nalazili glavni serveri, a pribavljanje dokaza na teritoriji Kanade nije bilo moguće bez njenog odobrenja. Pored toga, činjenica da je protiv vlasnika kompanije Sky Global postupak pokrenut u SAD govori u prilog činjenice da se naredba francuskog suda nije mogla odnositi na njega. Na kraju, ova analogija ni našim sudovima ne bi išla u prilog, jer je pravljenje i unošenje računarskih virusa krivično delo predviđeno članom 300 KZ, pa bi upotreba ovog dokaza bila zabranjena.[40] Za razliku od krivičnog dela iz člana 302 KZ koje inkriminiše samo ***neovlašćeni*** pristup zaštićenom računaru, računarskoj mreži ili elektronskoj obradi podataka, naše pravo ne ostavlja mogućnost da pravljenje i unošenje računarskih virusa iz čl. 300 bude ovlašćeno. To je i razumljivo imajući u vidu da pre 20-tak godina, u vreme unošenja ovih inkriminacija nije moglo ni da se pretpostavi da će se i državni organi služiti „hakovanjem" i unošenjem računarskih virusa, kao jedinim načinom za pristup određenim podacima i komunikaciji osumnjičenih.

3. PRENOS I PRAVNA PRIRODA PRIBAVLJENIH PODATAKA

3.1. Prenos podataka pribavljenih presecanjem EncroChat i Sky Ecc komunikacije drugim državama

Podaci pribavljeni presecanjem EncroChat i Sky ECC komunikacije dostavljeni su drugim državama putem međunarodne pravne pomoći odnosno, državama članicama EU, putem evropskih naloga za istragu. Klasična „mala" međunarodna pravna pomoć podrazumeva da je na teritoriji određene države pokrenuta istraga, a da se pojedini dokazi nalaze van njene teritorije, te je neophodno obratiti se zamolnicom drugoj državi koja bi onda sprovela te dokazne radnje u skladu sa svojim propisima. ZMPPKS kao i istoimena Konvencija[41] govore o „obavljanju istražnih radnji2 u državi molilji na zahtev zamoljene države, što bi podrazumevalo da je naša država „zamolila" Francusku da ispita određene svedoke, izvrši nadzor telekomunikacija ili obavi drugu dokaznu radnju. Međutim, u slučajevima vezanim za EncroChat i Sky Ecc, imamo situaciju da su istražni organi Holandije, Belgije i Francuske, vodeći zajedničku istragu na svojim teritorijama pribavili „uzgredne" dokaze, odnosno „slučajne nalaze" koji ukazuju na kriminalne aktivnosti na teritorijama drugih država i od strane državljana tih drugih država. Te „druge države" bi

40 Radilo bi se o izvoru dokaza koji ima „kriminalni karakter" i čija je upotreba zabranjena. „Neki izvori dokaza se, iz određenih razloga koji se svode bilo na njihovu neetičnost, striktnu zakonsku zabranjenost odnosno kriminalni karakter (na primer tortura, narkoanaliza itd.) ne mogu koristiti za utvrđivanje činjenica u krivičnom postupku niti se na njima može zasnovati odluka suda". M. Škulić, G. Ilić, Marina Matić Bošković (eds.) /2015/: *Unapređenje Zakonika o krivičnom postupku – de lege ferenda predlozi*, OEBS, Beograd, p. 66.

41 Zakon o potvrđivanju evropske konvencija o međunarodnoj pravnoj pomoći u krivičnim stvarima, „*Sl. list SRJ– Međunarodni ugovor*i", br. 10/2001.

pokretale istrage protiv ovih lica tek nakon što im je Francuska dostavila pribavljene podatke, dakle na osnovu ove specifične krivične prijave koja je u sebi sadržala ključni dokazni materijal.

Prilikom odlučivanja o prihvatljivosti dokaza pribavljenih presecanjem EncroChat komunikacije, nemački i britanski sudovi posebno su se bavili i pitanjem da li je došlo do povrede zakona prilikom prenosa ovih podataka od strane Francuske. U dva odvojena slučaja Viši regionalni sud u Bremenu (u decembru 2020.) i viši regionalni sud u Hamburgu (u januaru 2021.) su u svojim odlukama potvrdili zakonitost ovog prenosa pozivanjem na pojednostavljenu razmenu informacija i obaveštajnih podataka.[42] Kako su podaci najpre dostavljeni Kancelariji Federalne krivične policije u skladu sa Evropskim istražnim nalogom, reč je o spontanoj razmeni podataka u skladu sa članom 7(1) Okvirne odluke Saveta o pojednostavljenoj razmeni informacija i obaveštajnih podataka između nadležnih organa država članica EU.[43] U skladu sa ovom odlukom nadležni državni organi države članice će, i bez prethodnog zahteva dostaviti informacije i obaveštajne podatke drugoj državi članici, kada postoje opravdani razlozi da se veruje da će ove informacije doprineti otkrivanju, sprečavanju ili sprovođenju istraga o krivičnim delima.[44] Britanske vlasti su takođe izdale evropski nalog za istragu,[45] na osnovu koga je nadležnim britanskim organima dozvoljen pristup podacima pribavljenim od strane francuskih vlasti. Ovim nalogom nije zahtevana „pomoć" u pogledu sprovođenja određene dokazne radnje, već su tražene informacije koje su francuske vlasti već pribavile.[46]

Suprotno tome, državama van sistema evropskih istražnih naloga, ovi podaci se dostavljaju po sistemu međunarodne pravne pomoći. Konvencija o međunarodnoj pravnoj pomoći u krivičnim stvarima doneta je 1959. godine, u vreme kada kompjuteri još nisu ni postojali, posedovanje televizora ili fiksnih telefona bilo je stvar prestiža, pa su i mnoge dokazne radnje kojima se danas uglavnom pribavljaju dokazi bile ne samo mimo domašaja ove Konvencije već u domenu naučne fantastike. Konvencija je „modernizovana" 2001. godine donošenjem II dodatnog protokola, kojim je između ostalog predviđeno saslušanje putem video konferencijske veze, praćenje lica na teritoriji više država, kontrolisana isporuka, tajne istrage, formiranje zajedničkih istražnih timova, kao i mogućnost dostavljanja informacija prikupljenih tokom istrage u jednoj strani ugovornici nadležnim organima druge strane ugovornice i bez prethodno upućenog zahteva.

Dostavljanje informacija o Sky Ecc komunikaciji od strane Francuske i bez prethodno upućenog zahteva Srbije, može imati uporište u članu 11. st. 1. ovog Protokola koji predviđa da „nadležni organi jedne strane ugovornice mogu, ne dirajući u sopstvene istrage ili postupke i bez prethodno upućenog zahteva, dostaviti nadležnim organima druge strane ugovornice ***informacije*** do kojih su došli u okviru sopstvenih istraga, ukoliko smatraju da bi takve informacije pomogle njihovom

42 EUCRIM /2021/. *op. cit.,* p. 23.

43 Framework Decision 2006/960/JI od 18. 12. 2006.

44 Higher Regional Court Hamburg. *op. cit.,* par. 108 i 109.

45 Velika Britanija je zvanično napustila EU 31. 01. 2020. i od tog datuma nije više u sistemu evropskih istražnih naloga, što ne dovodi u pitanje validnost naloga izdatih pre tog datuma.

46 Royal Courts of Justice Strand, London. *op. cit*., par. 33.

primaocu u pokretanju ili sprovođenju istrage ili postupka, ili bi mogle dovesti do upućivanja zahteva od strane te države, shodno odredbama ove Konvencije ili njenih dodatnih protokola."[47]

Ovde dakle nije reč o dokazima već o „informacijama". Ako država smatra da bi informacije mogle da imaju dokazni značaj, dužna je da se državi koja ih je dostavila obrati formalnim, zamolnim putem u cilju pribavljanja određenog dokaza. Ali opet se kao prethodno nameće pitanje načina pribavljanja tih informacija, odnosno da li su one regularno pribavljene u krivičnom postupku, kada mogu imati dokazni značaj, ili su pribavljene od strane obaveštajnih službi i dostavljene kao obaveštajni podaci na osnovu kojih se „skreće pažnja" nadležnim organima na krivična dela koja se vrše na njenoj teritoriji, kako bi država „reagovala" pokretanjem krivičnog postupka i pribavljanjem validnih dokaza? Da li se ovde radilo o ciljanom nadzoru komunikacija u krivičnom postupku ili o masovnom nadzoru koji po pravilu vrše obaveštajne službe? Francuska je jedna od sedam evropskih država koja zvanično dozvoljava masovni nadzor komunikacija preko optičkih kabala[48], ali je problem što se ovaj nadzor ne sprovodi prema odredbama ZKP već prema Zakonu o obaveštajnim delatnostima pa je dokazni karakter ovako pribavljenih podataka upitan. Čak i ako pretpostavimo da je nadzor inicijalno određen kao ciljani nadzor prema odredbama ZKP, on je nesumnjivo imao masovni karakter imajući u vidu broj lica čija je komunikacija nadzirana a koja se nisu nalazila pod teritorijalnom jurisdikcijom francuskog suda koji je izdao naredbu.

3.2. Dokazi ili obaveštajni podaci – ciljani ili masovni nadzor?

Kod pribavljanja Sky komunikacije, ako iz gore navedenih razloga, izuzmemo analogiju sa „razbijanjem2 EncroChat-a i primenu člana 706–102–1 ZKP, u obzir dolazi primena člana 100. Francuskog ZKP koji reguliše presretanje elektronske komunikacije i predviđa da istražni sudija može, u postupcima za krivična dela i prekršaje za koje se može izreći kazna teža od tri godine zatvora, narediti presretanje, snimanje i transkripciju prepiske poslate putem elektronskih komunikacija.

Ali, u tom slučaju, kao veliki problem nameće se problem nadzora stranih državljana, na stranoj teritoriji, bez znanja i odobrenja te strane države. Drugim rečima, diskutabilno je po kom osnovu je vršen nadzor van teritorijalne nadležnosti Francuske, odnosno po kom osnovu je bilo moguće nadzirati komunikaciju lica koja se ne nalaze na Francuskoj teritoriji, nisu izvršili krivično delo na Francuskoj teritoriji niti protiv njenog državljanina, te je jedina „spona" koja ih povezuje sa Francuskom server preko koga se odvijala komunikacija a koji se nalazio na francuskoj teritoriji, i to opet pod pretpostavkom da se sva komunikacija odvijala preko tog servera, a ne preko glavnog servera koji se nalazio u Kanadi?

47 U konkretnom slučaju dolazi u obzir i primena čl. 26 Konvencije o VTK koji reguliše razmenu slučajnih informacija. Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, „*Sl. glasnik RS*", br. 19/2009.

48 Pored Francuske, u ovoj grupi se još nalaze Finska, Nemačka, Holandija, Švedska i Velika Britanija, a u Norveškoj je zakon o masovnom presretanju u proceduri. ECHR, *Big Brother Watch and others v. the United Kingdom,* App. Nos. 58170/13, 62322/14 and 24960/15, 25. 05. 2021., par. 242-244.

U vezi sa tim, član 100–8 francuskog ZKP predviđa:

> Ako se presretanje elektronske prepiske odnosi na komunikaciju koja se odvija na teritoriji članici Evropske Unije, a ne sprovodi se u kontekstu sprovođenja evropskog istražnog naloga, istražni sudija će obavestiti o tome nadležne organe te države ako se osumnjičeni nalazi na njenoj teritoriji.
>
> Takvo obaveštenje se šalje ili pre presretanja ako se utvrdi da se osumnjičeni nalazi li da će se naći na teritoriji te države, ili u toku presretanja ili nakon njegovog izvršenja, čim se utvrdi da je to lice na teritoriji te države, ili da se nalazilo na njenoj teritoriji.
>
> Na zahtev nadležnog organa države članice, opravdanog činjenicom da takvo presretanje nije moglo biti odobreno po zakonu te države, presretanje ne može biti izvršeno ili se mora prekinuti a podaci koji su pribavljeni dok se osumnjičeni nalazio na njenoj teritoriji ne mogu da se koriste u postupku i moraju biti uklonjeni ili se mogu koristiti samo pod uslovima koje je naveo organ te države.

Problem je što ovaj član ima u vidu samo države članice EU i nadzor njihovih državljana, što se pravda supranacionalnim karakterom prava EU i načelom uzajamnog priznanja, polazeći od toga da francuski organi, ni u kom slučaju ne mogu da u krivičnom postupku nadziru komunikaciju koja se odvija van granica EU. U tom slučaju se dokazi prikupljaju putem međunarodne pravne pomoći, odnosno od strane države bi trebalo zamolnim putem zahtevati da preduzme dokaznu radnju na svojoj teritoriji.[49]

Ne isključujemo mogućnost ni da je sva ova komunikacija pribavljena na osnovu *Zakona o obaveštajnim delatnostima* iz 2015. godine, koji između ostalog dozvoljava „eksploataciju kompjuterske mreže" ili kompjutersko hakovanje kao način pribavljanja obaveštajnih podataka.[50] Ovaj zakon je usvojen 24.07.2015, kao odgovor na napad na *Charlie Hebdo* u Parizu 2015. godine i dozvoljava krajnje invanzivne mere nadzora poput „crnih kutija" koje skeniraju celokupan Internet sadržaj kako bi otkrili „sumnjive" URLs (član 13), ili obaveze privatnih kompanija da sarađuju sa vlastima prilikom hakovanja šifrovanih poruka (čl. 10). Po članu 853–2 ovog zakona, dozvoljen je: a) Pristup, prikupljanje, zadržavanje i prenošenje kompjuterskih podataka koji su sačuvani u kompjuterskom sistemu i b) Pristup, prikupljanje, zadržavanje i prenošenje kompjuterskih podataka, na način na koji su prikazani na ekranu korisnika, kako su uneti putem tastature ili kako su primljeni na drugom uređaju. Razlozi zbog kojih obaveštajne agencije mogu sprovoditi nadzor su brojni i svode se na razloge nacionalne bezbednosti, teritorijalnog integriteta, odbrane; inte-

---

49 U nemačkoj teoriji se osnovano ističe da „teritorijalni princip, koji između ostalog podrazumeva i pravo svake države da suvereno odlučuje da li će dozvoliti prikupljanje dokaza i sprovođenje istraga na njenoj teritoriji, ne može biti poništen zbog novih sredstava komunikacije kao što je Internet. Takvi dokazi mogu biti pribavljeni samo uz saglasnost dotične države, a u suprotnom su nezakoniti i neprihvatljivi." N. Seitz /2004/: Transborder Search: A New Perspective in Law Enforcement?, *International Journal of Communications Law & Policy*, Issue 9, Autumn 2004, p. 8.

50 U vezi sa tim i ESLJP je naglasio da masovni nadzor mahom obuhvata komunikaciju koja se odvija van državnih granica, kada je interes države da nadzire komunikaciju osoba koje se nalaze van njene teritorijalne nadležnosti, što nije moguće ostvariti ciljanim nadzorom. *Big Brother Watch*, par. 344.

rese spoljne politike, primene evropskih i međunarodnih obaveza Francuske i sprečavanja svih oblika stranog uticaja; glavne ekonomske, industrijske i naučne interese Francuske; prevenciju terorizma, prevenciju organizovanog kriminaliteta, prevenciju širenja oružja za masovno uništenje.[51] Zakon takođe pruža imunitet pripadniku obaveštajne agencije koji izvrši krivično delo pristupajući kompjuterskom sistemu koji se nalazi u inostranstvu. Imajući u vidu invanzivnost mera koje predviđa i širok opseg primene[52], Zakon o obaveštajnim delatnostima je vrlo brzo naišao na snažne kritike što je rezultiralo podnošenjem predstavke ESLJP za ocenu usklađenosti njegovih odredbi sa osnovnim zahtevima EKLJP.[53]

Problem bi u tom slučaju nastao jer je diskutabilno da li se obaveštajni podaci, nastali mimo krivičnog postupka, mogu koristiti kao dokaz u krivičnom postupku.[54] U preporuci Generalne Skupštine Saveta Evrope o kontroli obaveštajnih službi je navedeno da obaveštajne službe ne bi trebalo da imaju bilo kakvu nadležnost u borbi protiv kriminala, osim ako se ne radi o pretnjama po nacionalnu bezbednost.[55] U tom smislu, britanska regulativa o istražnim ovlašćenjima (*the Regulation of Investigatory Powers Act* 2000-RIPA), koja je bila predmet osporavanja pred ESLJP u predmetu *Big Brother*, izričito predviđa da se podaci pribavljeni masovnim nadzorom ne mogu koristiti kao dokaz u krivičnom postupku, ali da na osnovu tako pribavljenih informacija nadležni organi mogu da reaguju pokretanjem krivičnog postupka.

51 F. Tréguer /2021/: Overview of France's Intelligence Legal Framework, [Research Report] CERI Paris. https://halshs.archives-ouvertes.fr/halshs-01399548/document, 21. avgust 2022.

52 F. Tréguer /2022/: Major oversight gaps in the French intelligence legal framework, https://aboutintel.eu/major-oversight-gaps-in-the-french-intelligence-legal-framework/, 21. avgust 2022.

53 Predstavku je podnelo nekolicina advokata i novinara i ona je dostavljena francuskoj vladi na odgovor 26. 04. 2017. godine (ECHR, Association confraternelle de la presse judiciaire v. France et 11 autres requetes). Slična predstavka podneta je i u Follorou v. France (no. 30635/17) i Johannes v. France (no. 30636/17), što je francuskoj vladi dostavljeno na odgovor 04. 07. 2017. ECHR, *Mass surveillance. op. cit.,* 21. avgust 2022.

54 Tako član 15v Zakona o BIA („*Sl. glasnik RS*", br. 42/2002, 111/2009, 65/2014-odluka US, 66/2014 i 36/2018) predviđa da ako je prilikom primene posebnih mera prikupljen materijal o krivičnom delu u odnosu na koje se mogu odrediti posebne dokazne radnje, takav materijal se dostavlja nadležnom javnom tužilaštvu i sa njime se postupa u skladu sa odredbama koje regulišu krivični postupak. Na osnovu dostavljenog materijala tužilac bi mogao da inicira pokretanje krivičnog postupka i primenu neke od posebnih dokaznih radnji koja bi se sprovela u skladu sa ZKP i imala dokazni značaj, imajući u vidu da se po članu 15 stav 1 ZKP dokazi prikupljaju i izvode u skladu sa tim zakonom. Zakon o VBA i VOA *(„Sl. glasnik RS*", br. 88/2009, 55/2012-odluka US i 17/2013) je u tom smislu mnogo jasniji jer izričito predviđa da se podaci prikupljeni primenom posebnih postupaka i mera u preventivne svrhe ne mogu koristiti kao dokaz u krivičnom postupku (čl. 11 st. 2.), a ako prikupljeni podaci ukazuju da se priprema ili da je izvršeno krivično delo koje se goni po službenoj dužnosti, VBA o tome obaveštava nadležno javno tužilaštvo (čl. 18 st. 1). VBA tužilaštvu može predložiti primenu tajnog nadzora komunikacije ili neke druge dokazne radnje pod uslovima i na način propisan ZKP (čl. 18 st. 3). O tome: V. Bajović /2022/: Tajni nadzor od strane policije i službi bezbednosti – in: *Kaznena reakcija u Srbiji-XII deo* (Ignjatović Đ., ed), Univerzitet u Beogradu-Pravni fakultet, Beograd, pp. 239-240.

55 Recommendation 1402 (1999) of the Parliamentary Assembly of the Council of Europe on the control of internal security services in Council of Europe member states, Guideline A (ii)., http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16689&lang=en, 21. avgust 2022.

Razlozi određivanja različitih vrsta nadzora su drugačiji. Ciljani nadzor se koristi u krivičnom postupku, dok se masovni nadzor mahom koristi od strane obaveštajnih službi, u cilju prikupljanja obaveštajnih podataka.[56] Međutim ESLJP ističe da se i masovni nadzor može koristiti u cilju otkrivanja i sprečavanja određenih krivičnih dela, sajber ili terorističkih napada i sl., kao i da se može koristiti i u cilju praćenja komunikacije određenih lica, iako se primarno ne određuje sa tim ciljem. Ali kada to i jeste slučaj, „ne nadziru se uređaji tih pojedinaca već se pojedinci 'ciljaju' primenom jakih selektora na komunikacije koje se već prate od strane obaveštajnih službi".[57] U praksi bi to primera radi značilo da obaveštajne službe nadziru celokupnu komunikaciju sa određenih servera, a da u milionima poruka koje tako pribavljaju posebno nadziru komunikaciju „sumnjivih" pojedinaca preko njihove e-mail adrese, IP adrese, broja uređaja koji koriste i sl. Pored toga, ESLJP posebno naglašava da masovni nadzor mahom obuhvata komunikaciju koja se odvija van državnih granica, jer je u mnogim slučajevima interes države da nadzire komunikaciju osoba koje se nalaze van njene teritorijalne nadležnosti, što nije moguće ostvariti ciljanim nadzorom. [58] Iz ovoga proizilazi da Francuska ciljanim nadzorom nije mogla da nadzire lica van svoje teritorije, već da je to bilo moguće samo masovnim nadzorom od strane obaveštajnih službi.

Prema raspoloživim podacima, nadzor nad EncroChat platformom je inicijalno određen u krivičnom postupku pokrenutom protiv predstavnika ove kompanije, ali je za posledicu imao pribavljanje komunikacije na hiljade korisnika ove mreže, širom sveta, što je kasnije iniciralo pokretanje mnogih krivičnih postupaka. Sam način sprovođenja „operacije" više podseća na masovni nego na ciljani nadzor imajući u vidu da su meta napada bili nosioci komunikacije (svi EncroChat i Sky Ecc telefoni), a ne pojedinačni uređaji sa kojih se odvijala komunikacija, odnosno tačno određeni uređaji određenih korisnika. U vezi sa tim, ESLJP je, kao jednu od karakteristika masovnog nadzora navodi to da „naredba za nadzor komunikacije ne imenuje niti opisuje predmet nadzora, niti određuje broj spoljnih komunikacija koje mogu biti presretane". Drugim rečima, ovde su meta nosioci komunikacije (prim. aut. celokupna EncroChat i Sky Ecc platforma), a ne uređaji sa kojih se odvija komunikacija ili pošiljaoci i primaoci komunikacije (prim. aut. tačno ciljani korisnici).[59]

ESLJP načelno ne zabranjuje masovni nadzor, u cilju zaštite nacionalne bezbednosti i drugih vitalnih interesa, ali primena ovog nadzora mora da bude regulisana tako da se poštuju mere zaštite.[60] Kritikujući ovo viđenje, sudije Lemmens, Veha-

56 *Big Brother Watch*, par. 332.

57 *Big Brother Watch,* par. 345-346

58 *Big Brother Watch,* par. 344.

59 „U nedostatku bilo kakvog ograničenja broja komunikacija koje se mogu presretati, čini se da su svi paketi komunikacija koji teku preko određenih nosilaca predmet nadzora". *Big Brother Watch,* par. 372.

60 „Imajući u vidu da mere tajnog nadzora određene u cilju odbrane nacionalne bezbednosti i drugih vitalnih interesa mogu ugroziti ili čak i uništiti demokratske vrednosti pod plaštom njihove odbrane, Sud mora da proveri da li postoje adekvatne i efikasne garancije protiv zloupotreba, kao i da li je „mešanje" nadležnih organa u prava zagarantovana članom 8 EKLJP zadržano na onome što je „neophodno u demokratskom društvu". *Roman Zakharov v. Russia*, App. No. 47143/06, 04. 12. 2015., par. 232, *Big Brother Watch*, 339.

bović i Bošnjak su u svom izdvojenom mišljenju u predmetu Big Brother vizionarski upozorile da bi, „u ne tako dalekoj budućnosti istraga kriminala mogla da pređe sa ciljanog nadzora na masovno presretanje podataka“[61], dok je sudija de Albuquerque naglasio da danas masovni nadzor postaje „rupa u zakonu kojom se izbegava zaštita pojedinačnih prava“.[62]

4. TAJNI NADZOR KOMUNIKACIJA U PRAKSI ESLJP

U dosadašnjoj praksi Sud u Strazburu je razvio nekoliko kriterijuma odnosno mera zaštite prilikom tajnog nadzora komunikacija, koji moraju biti regulisana unutrašnjim pravom kako bi se izbegle zloupotrebe.[63] U tom smislu ESLJP ispituje da li domaće zakonsko rešenje na osnovu koga je određen tajni nadzor jasno definiše:

1) prirodu i vrstu krivičnih dela u pogledu kojih je određen nadzor;
2) kategoriju lica čija komunikacija može biti nadzirana;
3) trajanje nadzora;
4) postupak za, pristup, ispitivanje, korišćenje i čuvanje pribavljenih podataka
5) mere predostrožnosti koje treba preduzeti prilikom prenošenja podataka drugim subjektima
6) okolnosti pod kojima pribavljeni podaci mogu ili moraju biti izbrisani ili uništeni.

U skorijoj praksi, ovi kriterijumi su dodatno prošireni zahtevima za:

7) kontrolom primene tajnog nadzora od strane nezavisnog tela;
8) obaveštavanjem lica koja su bila pod nadzorom;
9) postojanjem efikasnog pravna sredstva kojim bi se osporavala osnovanost nadzora

Kada se radi o masovnom nadzoru ESLJP odstupa od prva dva kriterijuma navodeći da ove mere preciziranja vrste krivičnog dela i kategorije lica obuhvaćenih nadzorom nisu primenjive, već umesto toga „imperativom“ smatra da države, kada primenjuju ovaj režim, unutrašnjim pravom moraju urediti detaljna pravila kada pod kojima nadležni organi mogu pribeći ovoj meri.[64]

Primena ovih kriterijuma u slučajevima EncroChat i Sky ECC je neprimenjiva dok se jasno ne utvrdi zakonski osnov po kome je nadzor vršen, kako bi se onda ispitalo postojanje osnova za vršenje nadzora, preciziranje njegovog trajanja u zako-

61 Big Brother Watch and others v. the United Kingdom, *Joint Partly Concurring Opinion of Judges Lemmens, Vehabović and Bošnjak,* par. 29.

62 Big Brother Watch and others v. the United Kingdom, *Partly Concurring and Partly Dissenting Opinion of Judge Pinto de Albuquerque,* par. 11.

63 *Kruslin* v. France, 24.04.1990., par. 35; *Weber and Saravia v. Germany*, app. no. 54934/00, par. 95; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, app. no. 62540/00, 28. 06. 2007., par. 76., *Big Brother Watch*, par. 335, *Roman Zakharov*, par. 231.

64 „Unutrašnjim pravom treba jasno propisati osnov zbog koga može biti određen masovni nadzor i okolnosti pod kojima lična komunikacija može biti predmet nadzora.“ *Big Brother Watch*, par. 348.

nu/naredbi, postupak za pristup, ispitivanje, korišćenje i čuvanje pribavljenih podataka, postupak brisanja/uništavanja pribavljenih podataka itd.

U svakom slučaju masovnost „slučajnih nalaza" u postupcima inicijalno pokrenutim protiv predstavnika kompanija daje osnova za primedbu istaknutu u slučaju Zakharov protiv Rusije. Kritikujući ruski Zakon o operativno-istražnim radnjama po kome se u naredbi kojom se odobrava nadzor ne mora jasno navesti osoba čije se komunikacije nadziru i trajanje mere, ESLJP je naveo da se time daju veoma široka diskreciona ovlašćenja organima za sprovođenje zakona da odluče koje komunikacije će nadzirati i koliko dugo. „Kao rezultat toga, sudovi ponekad izdaju odobrenja za nadzor u kojima se ne navodi određena osoba niti broj telefona koji će se prisluškivati, nego se odobrava nadzor svih komunikacija u području u kojem je izvršeno krivično delo".[65]

Pored toga, posebno je sporno i postojanje delotvornog pravnog sredstva u ovim slučajevima. Pravo na efikasno pravno sredstvo predviđeno je članom 13 EKLJP i predviđa da „svako čija su prava i slobode, priznata ovom Konvencijom narušena ima pravo na pravni lek pred nacionalnim vlastima, čak i onda kada su povredu ovih prava i sloboda učinila lica u vršenju svoje službene dužnosti." U vezi sa tim, ESLJP je posebno naglašavao da efikasno pravno sredstvo treba da bude obezbeđeno svakome ko veruje da je njegova komunikacija bila pod nadzorom, a u cilju ispitivanja zakonitosti samog nadzora ili usaglašenost nadzora sa Konvencijom.[66]

Kriterijum postojanja delotvornog pravnog sredstva neraskidivo je povezan sa zahtevom da lice bude obavešteno od nadzoru, jer po logici stvari, lice mora biti obavešteno o tome da je bilo pod nadzorom, da bi uložilo pravno sredstvo. „Nedostatak obaveštavanja lica o tome da je bilo pod nadzorom lišava pojedinca prilike da traži naknadu za nezakonito mešanje u njegova prava iz člana 8, a propisane pravne lekove čini teorijskim i iluzornim a ne praktičnim i delotvornim... U tom slučaju, pojedinac i ne može znati da je bio pod nadzorom osim ako se protiv njega ne pokrene krivični postupak ili ne dođe do 'curenja' podataka".[67] Međutim, u slučajevima masovnog nadzora, kod koga je obaveštavanje svakog lica o nadzoru faktički neizvodljivo, ESLJP smatra da mogućnost podnošenja pravnog leka ne treba vezivati za prethodno obaveštavanje lica o tome, već pravo na podnošenje pravnog leka treba da ima svako ko sumnja da je njegova komunikacija bila predmet nadzora. Tako primera radi, u Velikoj Britaniji svaka osoba koja sumnja da je bila pod nadzorom može se obratiti posebnom telu (*Investigatory Powers Tribunal*), čija nadležnost ne zavisi od prethodnog obaveštavanja lica da je bilo podvrgnuto merama.[68] ESLJP je i u vezi sa tim naglasio da se masovni nadzor mahom koristi u cilju prikupljanja stranih obaveštajnih podataka, da je usmeren prema licima koja se nalaze u ino-

65 *Roman Zakharov,* par. 265

66 *Big Brother Watch*, par. 357

67 *Roman Zakharov,* par. 288,289.

68 U predmetu *Kennedy v. the United Kingdom* (ECHR 18 May 2010.), ESLJP je utvrdio da neobaveštavanjem lica o merama nadzora kojima je bilo podvrgnuto nije došlo do povrede člana 8 i člana 13 EKLKP, jer u Velikoj Britaniji svako lice koje sumnja da je bilo pod nadzorom ima mogućnost da se obrati nezavisnom telu kako bi se ispitala osnovanost ovih sumnji.

stranstvu te da je verovatnoća obaveštavanja u takvim slučajevima mnogo manja.[69] Nedavno legitimisanje masovnog nadzora od strane ESLJP vodi zahtevu da se u svim državama osnuju nezavisna tela, poput onog u Velikoj Britaniji, koja bi na zahtev bilo kog pojedinca ispitala da li je njegova komunikacija bila pod nadzorom i da li je takav nadzor bio osnovan. Čini se da je većini korisnika Sky ECC i EncroChat uređaja koji, po logici stvari, ne moraju biti isključivo iz kriminalnog miljea, ovo pravo uskraćeno, jer većina država mogućnost sudske zaštite u ovim slučajevima vezuje za jasna saznanja lica da je bilo pod merama. Primera radi po našem ZKP sudija za prethodni postupak prema članu 162 st. 2. samo može (ali i ne mora) obavestiti lice da je prema njemu primenjena neka od posebnih dokaznih radnji, ali se ta mogućnost u praksi maltene i ne sprovodi, te sa tim u vezi stoji primedba istaknuta u predmetu Zakharov da lice i ne može znati da je bilo pod merama osim ako se protiv njega ne pokrene krivični postupak. Kako se podaci o ovim merama mahom vode kao tajni podaci, ni obraćanje Povereniku za informacije od javnog značaja ne bi urodilo plodom. Na taj način se u ovakvim slučajevima obesmišljava pravo na delotvorno pravno sredstvo, predviđeno članom 36 st. 2 Ustava RS i članom 13 EKLJP. Čak i pod pretpostavkom da lice zna odnosno čvrsto veruje da je bilo pod nadzorom jer je koristilo Sky telefon, Ustav RS ovo pravo vezuje za ***odluku*** kojom se odlučuje o nečijem pravu, obavezi ili na zakonu zasnovanom interesu, a odluka o nadzoru je u ovom slučaju doneta u inostranstvu, dakle van domašaja naših sudova.

5. MASOVNI NADZOR I PRAVO NA PRIVATNOST

Član 8 EKLJP svakome garantuje pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske. Takođe propisuje da se javne vlasti neće mešati u vršenje ovog prava, sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih. Isto tako i Ustav RS garantuje nepovredivost tajnosti pisama i drugih sredstava komuniciranja, dozvoljavajući odstupanja samo na određeno vreme, na osnovu odluke suda, na način predviđen zakonom i to u slučaju da su odstupanja neophodna radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije (čl. 41 Ustava RS).

Nesporno je da je otkrivanje i presecanje komunikacionih platformi EncroChat i Sky ECC doprinelo otkrivanju i sprečavanju mnogih krivičnih dela, što u skladu sa stavom 2 člana 8 EKLJP čini opravdanim zadiranje javnih vlasti u pravo pojedinaca na nepovredivost komunikacije. Jasno je i da su merama nadzora ostvareni legitimni ciljevi zaštite nacionalne i javne bezbednosti, sprečavanja nereda i kriminala, prava i sloboda drugih. Ono što je diskutabilno je da li je ovo „zadiranje" obavljeno u skladu sa zakonom i zahtevima koje je ESLJP postavio u svojoj dosadašnjoj praksi,

69 „Verovatnoća da će lice biti obavešteno o tome da je bilo pod nadzorom je mnogo manja u slučajevima masovnog nadzora imajući u vidu da se ovaj vid nadzora koristi za prikupljanje stranih obaveštajnih podataka i da će u najvećem broju slučajeva biti usmeren na komunikaciju osoba koje se nalaze van teritorijalne jurisdikcije države koja vrši nadzor". *Big Brother Watch*, par. 358.

posebno imajući u vidu da primenjenim merama nije samo presecana komunikacija „kriminalaca" već svih korisnika EncroChat i Sky ECC telefona.

Komunikacione platforme Sky ECC i EncroChat su imale na hiljade korisnika širom sveta, od kojih po logici stvari, nisu svi bili iz „iz kriminalnog miljea". Kriptovani uređaji sami po sebi nisu bili zabranjeni, što znači da je njihovo posedovanje i korišćenje bilo legalno. Iz odluke nemačkog suda proizilazi da je mera nadzora nad EncroChat aplikacijom pogodila 32.477 korisnika u 121 državi, od čega je 380 u potpunosti ili povremeno bilo locirano na francuskoj teritoriji. Po tvrdnjama francuskih vlasti, najmanje 242 osobe locirane na francuskoj teritoriji, tačnije 60% je koristilo šifrovanu komunikaciju za kriminalne delatnosti.[70] Merama nadzora nisu pribavljani podaci samo određenih lica, na koja bi se naredba odnosila, nego su nadležni organi dobili pristup komunikaciji i podacima svih njenih korisnika, odnosno celokupnoj komunikaciji koja se odvijala preko ovih platformi. Analogna situacija bi primera radi postojala kada bi nadležni organi nadzirali celokupnu komunikaciju koja se odvija preko Viber-a ili Whats Up-a. Ovakav vid nadzora doveo je u pitanje i onu komunikaciju koja uživa posebnu zaštitu. Primera radi, nije nezamislivo da su i advokati koristili ove telefone u komunikaciji sa svojim klijentima, ili da su ih koristili novinari ili političari u cilju razmene poverljivih informacija. Pored toga, otvara se i pitanje zaštite privatnosti korisnika „običnih" mobilnih telefona, koji su po pravilu daleko manje zaštićeni od EncroChat ili Sky Ecc uređaja, a koji takođe sadrže pojedincu značajne podatke – lična dokumenta i kartice, bankovne račune, privatne fotografije i sl.

Regionalni sud u Berlinu je dokaze pribavljene presretanjem EncroChat komunikacije proglasio nezakonitim upravo po ovom osnovu ističući da je ova mera predstavljala značajan atak na pravo na privatnost i da je nadzor nad 30.000 EncroChat korisnika inkompatibilan zahtevu za proporcionalnošću mere.[71] Ova odluka je kasnije ukinuta od strane apelacionog suda, a ostaje da se vidi stav Suda u Strazburu po svim ovim pitanjima.

Dvojica britanska državljanina protiv kojih je EncroChat komunikacija prihvaćena kao dokaz pred britanskim sudovima podnela su predstavku ESLJP kojom osporavaju pravo na pravično suđenje iz člana 6, pravo na poštovanje privatnog života i prepiska iz čl. 8, kao i pravo na efikasno pravno sredstvo iz čl. 13 Konvencije.[72] Predstavka je dostavljena francuskoj vladi na odgovor 08.12.2021., i od nje se, između ostalog zahteva da dostavi sledeće informacije:

a) Koliko je uređaja pogođeno spornim hvatanjem podataka?
b) Kakva je priroda podataka koji su prikupljeni na ovaj način, da li se radi o dokazima ili o obaveštajnim podacima?

---

70 Higher Regional Court Hamburg. *op. cit*. par. 8.

71 B. Goodwin /2021/: *Berlin court finds EncroChat intercept evidence cannot be used in criminal trials,* dostupno na: https://www.computerweekly.com/news/252503524/Berlin-court-finds-EncroChat-intercept-evidence-cannot-be-used-in-criminal-trials, 18. avgust 2022.

72 *A.L. v. France* (no. 44715/20) and *E.J. v. France* (no. 47930/21), francuskoj vladi dostavljeno na odgovor 08. 12. 2021. ECHR, *Mass surveillance*. *op. cit.,* p. 7.

c) Da li je i po kom osnovu Francuska bila nadležna da nadzire komunikaciju na teritoriji drugih država bez njihovog znanja?
d) Da li je nedvosmisleno utvrđeno da su podnosioci predstavke zapravo bili korisnici EncroChat-a na osnovu nadimaka koje su koristili?
e) Koje zaštitne mere su obezbeđene i sprovedene u fazi pribavljanja podataka, prenošenja podataka drugim subjektima i njihovog uništavanja?
f) Da li lica koja sumnjaju da im je komunikacija bila nadzirana imaju pravo pristupa takvim podacima i da li je postojao mehanizam njihovog obaveštavanja o primenjenoj meri?
g) Da li ta lica imaju pristup nezavisnom telu ili sudu u cilju ispitivanja zakonitosti mere?

Ovi odgovori su od suštinskog značaja za dalju sudbinu ovih dokaza. Iako po shvatanju ESLJP utvrđena povreda člana 8 Konvencije ne utiče na odluku domaćeg suda kojom je podnosilac predstavke oglašen krivim (već jedino okrivljenom pruža naknadu nematerijalne štete)[73], na odluku domaćeg suda će uticati povreda člana 6 Konvencije, u slučaju da je korišćenjem nezakonitog dokaza dovedeno u pitanje pravo na pravično suđenje. „Pravičnost postupka" nalaže da se jasno precizira na koji način i po kom osnovu su ovi dokazi pribavljeni i da se odgovori na mnoga druga pitanja, kako bi se omogućilo prihvatanje i izvođenje ovih dokaza na glavnom pretresu. U tom smislu ESLJP naglašava da u krivičnom postupku svi dokazi po pravilu moraju biti izvedeni na glavnom pretresu u prisustvu optuženog koji mora imati mogućnost da ih podvrgne kritici, jer je načelo neposrednosti važna garancija pravičnosti postupka.[74] Međutim, odgovor Francuske ne treba očekivati brzo, imajući u vidu da se još uvek čeka njen odgovor na podneske dostavljene 2017. godine, kojim se osporavaju odredbe Zakona o obaveštajnim delatnostima.

ZAKLJUČNA RAZMATRANJA

Razvoj tehnologije i novi vidovi kriminaliteta nalažu redefinisanje postojećih pravnih okvira, kako na unutrašnjem tako i na međunarodnom nivou, a slučajevi „razbijanja" EncroChat i Sky Ecc platformi istakli su ove probleme u prvi plan, bacajući sudove pred onu dilemu koju je Herbert Packer postavio još šezdesetih godina prošlog veka, da li prednost dati zaštiti od kriminaliteta ili zaštiti prava građana.

---

73 Sa tim u vezi, ESLJP još od predmeta Schnek v. Switzerland iz 1988. godine (App. No. 10862/84, 12. 07. 1988.), stoji na stanovištu da korišćenje nezakonitog ne čini postupak nepravičnim, pod uslovom da sporni snimak *nije jedini dokaz* na kome se zasniva osuda, odnosno, Sud kumulativno ispituje: a) da li je osuda zasnovana jedino ili bar u pretežnom delu na dokazu pribavljenom kršenjem člana 8, b) da li je okrivljeni imao prilike da osporava autentičnost i korišćenje spornog dokaza i c) da li okolnosti njegovog pribavljanja bacaju sumnju na njegovu tačnost ili pouzdanost odnosno da li u slučajevima smanjene pouzdanosti ima drugih dokaza koji ga potkrepljuju. Više o tome: B. Stanković /2022/: *Nezakoniti dokazi u krivičnom postupku*, doktorska disertacija odbranjena na Pravnom fakultetu Univerziteta u Beogradu, Beograd, pp. 94-97.

74 *Pitkanen v. Finland*, App. No 30508/96, 09. 03. 2004., par. 57-58.

Dok je zaštita prava građana dugi niz godina odnosila prevagu, vođena maksimama da se „demokratičnost jednog društva meri po odredbama njenog krivičnog postupka" i da je „bolje da stotinu krivih izbegne kaznu nego da jedan nevin bude osuđen", čini se da u eri informacionih tehnologija preteže drugi model koji ozakonjuje do skora nezamislive koncepte poput masovnog nadzora komunikacija uz derogiranje teritorijalne suverenosti, pa se čini da je najpoznatiji „uzbunjivač" današnjice Džulijen Asanž bio u pravu kada je tvrdio da je Internet najveća, ikada osmišljena špijunska mašinerija svih vremena.

Nesumnjivo da je presecanje i dekodiranje EncroChat i Sky Ecc platformi doprinelo otkrivanju i sprečavanju brojnih krivičnih dela, kao i pribavljanju mnogih materijalnih dokaza, ali je upitna pravna priroda i dokazni značaj ovako pribavljene komunikacije. Da bi ovi podaci mogli da se koriste kao dokaz, oni moraju biti zakonito pribavljeni u krivičnom postupku, te bi u vezi sa tim bilo neophodno nedvosmisleno utvrditi osnov i način njihovog pribavljanja, validnost, opseg i trajanje naredbe, prirodu i vrstu krivičnih dela u pogledu kojih je određen nadzor i druge garante zakonitog postupanja prilikom sprovođenja ove mere. Zatim je neophodno utvrditi po kom osnovu su strane države, tzv. ciljanim nadzorom u krivičnom postupku prikupljale dokaze van svojih teritorijalnih jurisdikcija, bez znanja i saglasnosti drugih država. Podvođenje ovako pribavljenih podataka pod „slučajne nalaze" bi u budućnosti dalo legitimitet svim moćnijim državama koje raspolažu najmodernijom tehnologijom, da vrše nekontrolisani nadzor nad svakim pojedincem na svetu i prikupljaju dokaze u svakoj državi, u potpunosti obesmišljavajući kontrolnu ulogu domaćih sudova u takvim situacijama.

Situacija je „pravno" čistija ako se ovako pribavljenom materijalu da karakter „obaveštajnih podataka" kojima se nadležnim organima u drugim državama „skretala pažnja" na kriminalne aktivnosti na njihovoj teritoriji i omogućavalo im se da prikupe validne dokaze nakon toga, ali se i u tom slučaju aktuelizuje pitanje masovnog nadzora koji postaje „rupa u zakonu kojom se izbegava zaštita pojedinačnih prava".

Dok se „dilema ne reši" na širem planu, sudovima ostaje da se od slučaja do slučaja bave ovim pitanjima pod okvirima koja im domaći zakoni nalažu. Pored otkrivanja i sprečavanja brojnih krivičnih dela, čini se da su slučajevi EncroChat i Sky Ecc najviše doprineli ukazivanju na neophodnost „modernizovanja" zakonskih odredbi, u smislu uvažavanja činjenice da se krivična dela danas između ostalog otkrivaju i ubacivanjem „virusa" u kompjuterski sistem, posebno regulisanje pribavljanja elektronskih dokaza i uvođenje novih dokaznih radnji poput online ili digitalnog nadzora, posebno regulisanje veštačenja elektronskih uređaja i elektronskih podataka, revidiranje postojećeg mehanizma pravne pomoći u krivičnim stvarima itd.

Na kraju, ako pođemo od davno izrečene konstatacije B. Frenklina da „društvo koje je spremno da se odrekne malo slobode zarad malo bezbednosti ne zaslužuje ni slobodu ni bezbednost", dolazimo do zaključka da je savremeno doba informacionih tehnologija doba u kome nema ni slobode ni bezbednosti.

LITERATURA

Bajović V. /2022/: Tajni nadzor od strane policije i službi bezbednosti – in: *Kaznena reakcija u Srbiji-XII deo* (Ignjatović Đ., ed.), Univerzitet u Beogradu-Pravni fakultet, Beograd.

Bayer V. /1989/: *Jugoslovensko krivično procesno pravo, knjiga druga, Pravo o činjenicama i njihovom utvrđivanju u krivičnom postupku*, Zagreb.

ECHR /2022/: *Mass surveillance.* https://www.echr.coe.int/documents/fs_mass_surveillance_eng.pdf, 21. avgust 2022.

EUCRIM /2021/: *The European Criminal Law Associations' Forum*, 1/2021 https://eucrim.eu/media/issue/pdf/eucrim_issue_2021-01.pdf, 21. avgust 2022.

Europol/Eurojust joint press release /2020/: "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe", https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe 21. avgust 2022.

Europol/Eurojust /2021/: "Third Report of the Observatory Function on Encryption", https://www.europol.europa.eu/cms/sites/default/files/documents/3rd_report_of_the_observatory_function_on_encryption-web.pdf, 21. avgust 2022.

Goodwin B. /2021/: *Berlin court finds EncroChat intercept evidence cannot be used in criminal trials,* https://www.computerweekly.com/news/252503524/Berlin-court-finds-EncroChat-intercept-evidence-cannot-be-used-in-criminal-trials, 18. avgust 2022.

Grubač M., Ilić G., Majić M. /2009/: *Komentar Zakona o međunarodnoj pravnoj pomoći u krivičnim stvarima*, Službeni glasnik, Beograd.

Hamilton F. /2020/: "Hundreds of arrests as police crack phone network used by crime bosses". *The Times*. https://www.thetimes.co.uk/article/hundreds-of-arrests-as-police-crack-phone-network-used-by-crime-bosses-h85qntqw3, 21. avgust 2022.

Matić Bošković M. /2022/: *Krivično procesno pravo EU*, Institut za kriminološka i sociološka istraživanja, Beograd.

Mrela M. /2000/: Pravna valjanost dokaza pribavljenih u inozemstvu, *Hrvatski ljetopis za kazneno pravo i praksu* (Zagreb), vol. 7, n° 1.

Osborne C. /2021/: https://www.zdnet.com/article/sky-global-ceo-indicted-over-encrypted-chat-drug-trafficking-claims-erosion-of-right-to-privacy/, 21. avgust 2022.

Pisarić M. /2016/: *Posebnosti dokazivanja dela visokotehnološkog kriminala*, doktorska disertacija odbranjena na Pravnom fakultetu Univerziteta u Beogradu, Beograd

Pisarić M. /2020/: Prikupljanje elektronskih dokaza iz mobilnog telefona u praksi VKS Republike Srbije, *Kriminalistička teorija i praksa,* vol. 7, n° 2.

Ruggeri S. /2012/: Investigative Powers Affecting Fundamental Rights and Principles for a Fair Transnational Procedure in Criminal Matters. A Proposal of Mutual Integration in the Multicultural EU Area, *CRIMEN* (III), n° 2.

Satzger H. /2019/: Is mutual recognition a viable general path for cooperation?, *New Journal of European Criminal Law*, Vol 10(I).

Seitz N. /2004/: Transborder Search: A New Perspective in Law Enforcement?, *International Journal of Communications Law & Policy*, n° 9.

Stanković B. /2022/: *Nezakoniti dokazi u krivičnom postupku*, doktorska disertacija odbranjena na Pravnom fakultetu Univerziteta u Beogradu, Beograd.

Škulić M, Ilić G., Matić Bošković M. /2015/: *Unapređenje Zakonika o krivičnom postupku– de lege ferenda predlozi*, OEBS, Beograd.

Šugman Stubbs K. /2014/: Ocjena dokaza pribavljenih u inozemstvu: teorijski problemi i slovenska sudska praksa, *Hrvatski ljetopis za kazneno pravo i praksu* (Zagreb), vol. 21, n° 1.

Tréguer F. /2021/: Overview of France's Intelligence Legal Framework. [Research Report] CERI Paris. https://halshs.archives-ouvertes.fr/halshs-01399548/document, 21. avgust 2022.

Tréguer F. /2022/: Major oversight gaps in the French intelligence legal framework, https://aboutintel.eu/major-oversight-gaps-in-the-french-intelligence-legal-framework/, 21. avgust 2022.

Vasiljević T., Grubač M. /2011/: *Komentar Zakonika o krivičnom postupku*, Beograd.

UK Government /2014/: *Intercept as Evidence,* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/388111/InterceptAsEvidence.pdf, 17. avgust 2022.

US Department of Justice /2021/: "Sky Global Executive and Associate Indicted for Providing Encrypted Communication Devices to Help International Drug Traffickers Avoid Law Enforcement", https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices, 21. avgust 2022.

PRAVNI IZVORI I SUDSKE ODLUKE

Code de procedure penale, 1958, Modifie par LOI n.219–222 du 23 mars. 2019. https://codes.droit.org/PDF/Code%20de%20proc%C3%A9dure%20p%C3%A9nale.pdf, 21. avgust 2022.

Constitutional Court of Austria, AUT-2019–3–003, https://www.vfgh.gv.at/downloads/Bulletin_2019–3_AUT-2019–3–003_G_72–74_2019__ua.pdf, 16. avgust 2022.

ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, App. no. 62540/00, 28. 06. 2007.

ECtHR, *Allan v. the United Kingdom*, App. No 48539/99, 05. 02. 2003.

ECtHR, *Big Brother Watch and others v. the United Kingdom,* App. no. 58170/13, 62322/14 and 24960/15, 25. 05. 2021.

ECtHR, *Dragojevic v. Croatia*, App. No. 68955/11, 15. 01. 2015.

ECtHR, *Jalloh v. Germany*, App. No. 54810/00, 11. 07. 2006.

ECtHR, *Khan v. the United Kingdom*, ECtHR, No. 35394/97, 12. 05. 2000.

ECtHR, *Kennedy v. the United Kingdom,* 18. 05. 2010.

ECtHR, *Pitkanen v. Finland*, App. No 30508/96, 09. 03. 2004.

ECtHR, *Roman Zakharov v. Russia*, App. No. 47143/06, 04. 12. 2015.

ECtHR, Schnek v. Switzerland, App. No. 10862/84, 12. 07. 1988.

Higher Regional Court Hamburg 2nd Criminal Senate, br. Ws 2/21– 7 OBL 3/21 v. 29. 01. 2021., par. 8, https://www.landesrecht-hamburg.de/bsha/document/JURE210003021, 21. avgust 2022.

Royal Courts of Justice Strand, London, WC2A 2LL, R v A and others [2021] EW CA Crim 128, 05. 02. 2021., par. 149., https://www.judiciary.uk/wp-content/uploads/2021/02/A-v-R.pdf, 17. avgust 2022.

Zakon o elektronskim komunikacijama („*Sl. glasnik RS*", br. 44/2010, 60/2013– odluka US, 62/2014 i 95/2018– dr. zakon.

Zakonik o krivičnom postupku, „*Sl. glasnik* RS", br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021-odluka US i 62/2021-odluka US

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima, „*Sl. glasnik RS*", br. 20/2009.

Zakon o potvrđivanju Evropske konvencija o međunarodnoj pravnoj pomoći u krivičnim stvarima, „*Sl. list SRJ– Međunarodni ugovo*ri", br. 10/2001.

Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu, „*Sl. glasnik RS*", br. 19/2009.

*Vanja Bajović**
University of Belgrade, Faculty of Law

EVIDENCE FROM THE ENCROCHAT AND SKY ECC ENCRYPTED PHONES

SUMMARY

Technological development and new forms of crime require redefinition of existing legal frameworks at domestic and international level. EncroChat and SkyEcc cases highlighted these problems, throwing the courts before the old Packer's dilemma, whether to give priority to crime control or due process model. While the protection of citizens' rights prevailed for many years, guided by the maxims that "the democracy of a society is measured by the provisions of its criminal procedure" and that "it is better 100 guilty persons to escape than that one innocent person suffer" it seems that in the era of information technologies, another model prevails, legitimizing almost unimaginable concepts such as mass surveillance of communications with derogation of the principle of territorial sovereignty.

The "problem" escalated and came to the attention of many European countries after the "breaking" of the communication platforms EncroChat and SKY Ecc, which certainly contributed to the detection (and prevention) of numerous criminal acts by criminal groups, while at the same time opened many questions, starting from the method of discovering communication, delivering material to other countries and using it in criminal proceedings, the validity and admissibility of the so-called of "mass surveillance" that affects not only "criminals" but also "ordinary citizens", i.e. all users of certain communication platforms.

The first part of the paper deals with the issues how these networks were break down, the legal basis for such actions, the legal basis for providing the obtained data to other countries, their evaluation and further use in criminal proceedings. As different countries have different procedural rules, the question is whether a domestic judge is authorized to evaluate the legality of evidence obtained abroad and according to what criteria? In this regard, a distinction is made between EU member states where European investigative orders and the principle of mutual recognition apply and other countries in the system of mutual legal assistance in criminal matters.

In the second part, we deal with the legal nature of the obtained data through the dilemma of whether it was targeted surveillance in criminal proceedings, or mass surveillance carried out by the intelligence services, as well as the ECtHR's practice related to these issues.

Bearing in mind that these investigations are still under the "veil of silence", the study was based on Europol/Eurojust data and few publicly available decisions of courts in Germany and the United Kingdom about the admissibility of these evidence.

Key words: EncroChat, SkyEcc, evaluation of evidence obtained abroad, mass surveillance.

* Associate Professor, bajovic@ius.bg.ac.rs .