

Milan Škulić*

DOKAZNI ZNAČAJ INFORMACIJA IZ KOMUNIKACIJE OSTVARENE APLIKACIJAMA/ MODIFIKOVANIM UREĐAJIMA ZA KRIPTOVANJE – KAO ŠTO SU SKY ECC I ENCHROCHAT

Apstrakt. U radu se izlaže jedan pogled na informacije i potencijalne dokaze iz komunikacije ostvarene korišćenjem uređaja i aplikacija za kriptovanje komunikacije. Posebno se objašnjava fenomen aplikacije *Sky ECC*, koja ne samo da se najviše komentariše u medijima već je aktuelna u brojnim aktuelnim krivičnim postupcima, posebno iz sfere organizovanog kriminaliteta, kako u Srbiji, tako i širom Evrope, ali i sveta uopšte.

Nakon analiziranja osnovnih dokaznih pravila u pozitivnom krivičnom procesnom zakonodavstvu Srbije, a koja bi načelno mogla imati značaj u oceni dokazne verodostojnosti informacija proisteklih iz komunikacije ostvarene posebnim aplikacijama za kriptovanje razgovora, u radu se objašnjavaju relevantni primeri iz uporedne sudske prakse mnogih evropskih država. Objasnjeni su i veoma aktuelni slučajevi ove vrste o kojima se rešavalo u Srbiji. Analizirana je i praksa Evropskog suda za ljudska prava, koja se tiče moguće povrede prava na privatnost usled presretanja komunikacija ostvarenih posebnim aplikacijama. Posebna pažnja je poklonjena mišljenju generalnog advokata koji postupa pred Sudom pravde Evropske unije u odnosu na brojna pitanja koja je tom sudu postavio Regionalni sud u Berlinu, a koja se tiču informacija proisteklih primenom evropskog istražnog naloga, koje su prethodno u Francuskoj pribavljene posebnim operativno-taktičkim načinima za prikupljanje podataka iz komunikacije kriptovane aplikacijom *EnchroChat*.

U zaključku se ističe da nema čudotvornog recepta koji će apsolutno rešiti sve dokazne probleme koji nastaju ili mogu nastati kada je reč o informacijama iz komunikacija ostvarenih posebnim aplikacijama za kriptovanje razgovora. Vreme u kojem će se realizovati i buduća sudska praksa (čije se osnovne konture već sada relativno jasno naziru), a pre svega stavovi najviših sudova konkretnih država, pa i stavovi srpskih sudova, pokazaće kakav je realan značaj, pa i stepen relevantnosti mnogih faktora, koji bi načelno mogli imati uticaj na dokaznu verodostojnost takvih informacija/dokaza. Naravno, takva sudska praksa, kao i inače praksa sudova u pravnom ambijentu pravne države koja se odlikuje vladavinom prava, mora nastati u zakonito i pravično sprovedenim krivičnim postupcima.

Ključne reči: dokazi, šifrovana/kriptovana komunikacija, *Sky ECC*, krivični postupak, uporedno pravo, Evropski sud za ljudska prava, Sud pravde Evropske unije

* Pravni fakultet Univerziteta u Beogradu, sudija Ustavnog suda, skulic@ius.bg.ac.rs

1. UVODNA RAZMATRANJA

„Bauk skaja (*Sky ECC*) kruži Evropom“, kada je reč o mnoštvu aktuelnih krivičnih postupaka čiji su predmet krivična dela iz sfere organizovanog kriminaliteta, kao i druga teška krivična dela najčešće (ne)posredno povezana sa organizovanim kriminalitetom, poput tzv. teške/visoke korupcije, teških ubistava i pokušaja takvih krivičnih dela i sl. Sama aplikacija/uređaj *Sky ECC* je, inače, najpoznatija u medijskom smislu, tj. sa stanovišta komentarisanja konkretnih krivičnih postupaka u sredstvima javnog informisanja, kada se uobičajeno piše/govori o tzv. *Sky* telefonima, iako inače nije suština u „telefonu“ (mada taj sistem podrazumeva i korišćenje posebno prilagođenih telefona), već u aplikaciji. To pitanje je, naravno, bitno i u nekim aktuelnim krivičnim postupcima u Srbiji, kao i u tzv. regionu, ali je sama ta najpoznatija aplikacija te vrste, samo jedna od nekoliko specifičnih aplikacija namenjenih tajnoj/zaštićenoj komunikaciji. Naime, to su, pre svega, aplikacije tipa *Anom*, *EncroChat*, *Sky ECC*, *Bylock* i *Exclu*, ali već je u praksi primećeno da se kreiraju i neke sasvim nove aplikacije te vrste, a sasvim je izvesno da će i u tom pogledu, kao i inače, „praksa“ i ubuduće pokazivati veliku inventivnost. Tehnologija uopšte, pa naravno i veoma ekspanzivna računarska tehnologija, već decenijama svojim rapidnim razvojem doprinosi uvođenju efikasnijih metoda suzbijanja kriminaliteta, ali ona, obrnuto, često daje i veliki doprinos i razvijanju novih formi izvršenja nekih krivičnih dela¹ i boljem realizovanju nekih vidova kriminaliteta, poput organizovanog kriminaliteta, razvijanjem „otpornosti“ učinilaca takvih krivičnih dela u odnosu na radnje koje se vrše radi otkrivanja, razjašnjavanja i dokazivanja tih oblika kriminalne aktivnosti, poput posebnih dokaznih radnji kao što je nadzor nad komunikacijom. Suština svih aplikacija za tajno/zaštićeno komuniciranje je u omogućavanju da na kriptovan način komuniciraju jedino korisnici iste „platforme“.

Posebno je interesantan slučaj kompanije *Sky Global*, koja je bila komunikaciona mreža i provajder telekomunikacionih usluga, osnovan 2008. godine u Vanuveru u Kanadi. Taj sistem je bio veoma ekspanzivan te se brzo razvio u najveću globalnu mrežu za kriptovanje poruka. Prodaja usluga ove kompanije je bila organizovana na „piramidalnom nivou“, organizovanjem mreže prodavaca i preprodavaca, do krajnjeg korisnika. Korišćenje ovog vida komunikacije je bilo veoma skupo. Cena se kretala od 1.400 do 2.500 evra mesečno za period od šest meseci, uz kupovinu i samog prilagođenog uređaja. Kako su taj sistem pretežno, ako ne i isključivo (što je *questio facti*), koristile kriminalne organizacije, a posebno one koje su imale transnacionalni karakter i pretežno bile usmerene na trgovinu drogom, kompanija koja ga je kreirala i koja je bila provajder tih veoma specifičnih telekomunikacionih usluga vremenom je primarno posmatrana kao osobeni „pomagač/saradnik na profitnoj osnovi“ tih organizacija,² iako je, naravno, sama kompanija uvek zvanično tvrdila da je njen osnovni motiv za tržišno plasiranje svog „proizvoda“ zaštita privatnosti kao jednog od osnovnih ljudskih prava. To je u krajnjoj liniji i izazvalo niz

1 Ž. Aleksić, M. Škulić (2020). *Kriminalistika*, 11. izmenjeno i dopunjeno izdanje, Beograd, p. 357.

2 <https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices>, 27. mart 2024.

policijskih/pravosudnih akcija u nekoliko zemalja početkom 2021. godine, kada je infrastruktura te kompanije i njenog sistema narušena, a sama kompanija prestaje sa radom u martu 2021. godine, kada je proizvođač telefona *BlackBerry* onemogućio da ona koristi njegov servis. Kasnije je i američki FBI zaplenio/blokirao *website* te kompanije.

Sistem *Sky ECC* kriptovanja, koji se danas najviše i spominje u brojnim aktuelnim krivičnim postupcima, kao i u medijima, originalno je razvijen na platformi mobilnog telefona *BlackBerry*, koji je i sam obezbeđivao specifičnu složenu kriptografiju, od koje i počinje skraćenica *ECC* (*elliptic-curve cryptography*). U posebne karakteristike te vrste komuniciranja koju je na *BlackBerry* platformi razvila kompanija *Sky Global* spadao je i veoma efikasan mehanizam „samouništenja“ poruke, nakon što istekne unapred definisan vremenski period. Naime, kompanija *Sky Global* je za potrebe tajnog/zaštićenog komuniciranja putem posebne aplikacije koristila modifikovane mobilne telefone, najčešće brendova *Nokia* i *BlackBerry*, ali i *Apple* računare, kao i sistem *Google*.

Telefoni koji su korišćeni za kriptovanu komunikaciju tehnologijom koju je razvio *Sky Global* bili bi tehnički modifikovani kako ugrađivanjem posebne aplikacije, te blokiranjem svih drugih, inače uobičajenih aplikacija, koje su postojale na telefonu samo vizuelno, ali nisu bile funkcionalne, tako i uklanjanjem kamera, mikrofona, kao i mogućnosti lociranja putem GPS-a. Svaki tako modifikovan i prilagođen telefon imao je i „dugme ubicu“, odnosno „dugme za samoubistvo informacija“. To, naravno, nije bilo realno „dugme“ u fizičkom obliku, već se svodilo na poseban mehanizam uništenja/nepovratnog brisanja svih informacija sadržanih u telefonu, onda kada bi korisnik aktivirao tzv. lozinku za hitno reagovanje u opasnim/ugrožavajućim situacijama („panic password“). Informacije bi bile uništavanje i ukoliko bi se više puta uzastopno pogrešnom lozinkom pokušalo aktiviranje telefona, ili čak nekada posle samo jedne pogrešno „ukucane“ lozinke. Najčešće je i sam „password“ bio „kamufliiran“, tako što bi se aktivirao ukucavanjem određene brojčane operacije u kalkulator na telefonu (koju je određivao sam korisnik uređaja i mogao periodično da je menja), ali se pritom, nije radilo o pravom kalkulatoru, niti se zaista sprovodila brojčana operacija, poput sabiranja, množenja i sl., već je to samo bio način za prikriveno aktiviranje aplikacije/telefona. Ukupno je bilo registrovano oko 171.000 *Sky ECC* uređaja, pretežno u Evropi, Severnoj Americi, na Srednjem istoku i u nekim južnoameričkim državama, najviše u Kolumbiji. Posebno je indikativno bilo postojanje velikog broja korisnika i njihovih komunikacija u regionima tipičnim za multinacionalne operacije transnacionalnog organizovanog kriminaliteta usmerenog na krijumčarenje opojnih droga, kao što su to bile velike luke, poput Roterdama, Antverpena itd.

Kao i inače, često je „život inventivniji od prava“, a rapidan napredak tehnike i tehnologije, s jedne strane, redovno doprinosi uvođenju novih tehničko-tehnoloških metoda u funkciji efikasnijeg otkrivanja/razjašnjavanja/dokazivanja krivičnih dela, što predstavlja domen kriminalističke tehnike, kao najdinamičnijeg segmenta kriminalistike.³ Međutim, s druge strane, nekada omogućava i efikasnije vrše-

3 M. Škulić (2022). *Kriminalistika*, Beograd, p. 17.

nje određenih krivičnih dela, komuniciranje lica u tzv. kriminalnom podzemlju i sl. Inače, kada je reč o fenomenu korišćenja, a zatim „provaljivanja“ te vrste zaštićene komunikacije zahvaljujući korišćenju posebnih „uređaja“, odnosno specijalnih aplikacija namenjenih tajnoj/zaštićenoj komunikaciji, u našoj teoriji se već isticalo da „samo posedovanje ovih uređaja/aplikacija nije bilo zabranjeno, oni su, na različitim internet stranama reklamirani uz garancije sigurne komunikacije bez mogućnosti prisluškivanja, a na web-strani kompanije *Sky Global* čak je i velikodušno nuđena nagrada od četiri miliona dolara onome ko bi uspeo da dekodira enkripciju ove mreže“.⁴

Sada kada je (očigledno suprotno tvrdnjama iz reklame kompanije *Sky Global*) ipak došlo do sistematskog „provaljivanja“ komunikacija ostvarenih putem tih specifičnih uređaja/aplikacija, primećeno je da „kriminalno podzemlje“ najčešće i dalje koristi aplikacije i uređaje ove vrste, ali sada na način koji značajno otežava nadzor tako ostvarene komunikacije, bez obzira na to što za to, inače, već postoji odgovarajući „know how“. To se postiže kreiranjem potpuno novih i još naprednijih aplikacija/uređaja te vrste i novim načinom/novom taktikom korišćenja takvih aplikacija/uređaja. To podrazumeva da učesnici u komunikaciji koriste nekoliko aplikacija sukcesivno, tako da jednom šalju prvu poruku, a drugom primaju odgovor, pa zatim opet menjaju aplikacije za dalju komunikaciju itd. Takvim „ukrštenim“ i simultanim korišćenjem većeg broja aplikacija/uređaja za zaštićenu/šifrovanu komunikaciju značajno se otežava nadzor na do sada uobičajene načine, te se samim tim višestruko podiže stepen otpornosti takvog načina komuniciranja u odnosu na postojeće načine kontrole i „provaljivanja“ od strane nadležnih državnih organa, pre svega policije i drugih nadležnih službi pojedinih država koje su, zahvaljujući svojim veoma naprednim tehničkim mogućnostima, do sada povremeno uspevale da ostvare prodore u tu vrstu tajne komunikacije.

Osnovna funkcionalna karakteristika svih uređaja/aplikacija koje omogućavaju šifrovanu/zaštićenu komunikaciju jeste da su one isključivo i kreirane radi obezbeđivanja tajne i zaštićene komunikacije svojim korisnicima. To je osnovna, ako ne i jedina svrha njihovog postojanja. To praktično znači da je osnovna ideja prilikom stvaranja i korišćenja takvih uređaja/aplikacija bila obezbeđivanje da takav način komuniciranja bude maksimalno „imun“ i otporan u odnosu na inače uobičajene oblike „presretanja“ i nadzora komunikacija koje se ostvaruju raznovrsnim i klasičnim tehničkim sredstvima za razgovore na daljinu i prenošenje/primanje informacija, kao kada je reč o klasičnim razgovorima putem mobilne telefonije (što uključuje i razmenu poruka, tj. SMS-ova tom vrstom telefonije), a isto je i u pogledu danas u praksi znatno ređe fiksne telefonije, kao i kada je reč o komunikaciji putem interneta, što se pre svega tiče razmene mejlova.

Sušтина se, dakle, kada je reč o posebnim aplikacijama kao što je ona medijski daleko najpoznatija – *Sky ECC* (što podrazumeva i korišćenje posebno prilagođenih telefona), svodi na onemogućavanje da se komuniciranje takvim sredstvima nadzire/„presreće“ odgovarajućim posebnim dokaznim radnjama/specijalnim istražnim

4 V. Bajović (2022). EncroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku, *Crimen*, 2, p. 155.

tehnikama, koje predstavljaju prisluškivanje i snimanje razgovora i uopšte nadzor komunikacija tehničkim sredstvima na daljinu, čime se postiže obezbeđivanje dokaza primenom odgovarajućih specijalnih istražnih tehnika, poput posebnih dokaznih radnji prema pravilima srpskog krivičnog procesnog prava. Sve te aplikacije i uređaji te vrste su, naravno, tržišno plasirani, a firme koje su ih kreirale su redovno ostvarivale veliku dobit prodajom takve vrste usluga. Iako često, u praksi u vezi sa konkretnim krivičnim postupcima, pre svega krivičnoprocesni subjekti u funkciji odbrane objašnjavaju da je osnovna ideja razvijanja i tržišnog plasmana takvih aplikacija bila zaštita privatnosti, činjenica je da su u praksi takve vidove zaštićene komunikacije skoro isključivo, mada i to, naravno, predstavlja svojevrsni *questio facti* u svakom konkretnom slučaju, koristili okrivljeni za teška krivična dela, pretežno u sferi organizovanog kriminaliteta.

Dakle, u mnogim evropskim državama, kao i u samoj Srbiji, te u tzv. regionu, jedno od veoma aktuelnih pitanja je šifrovana/kriptovana komunikacija, odnosno pitanje dokazne verodostojnosti u krivičnom postupku tajne/šifrovane komunikacije ostvarene određenim tehničkim sredstvima, na temelju posebnih aplikacija za tajno/zaštićeno komuniciranje i dokaza/informacija proizišlih iz dešifrovanja tako ostvarene komunikacije. To pitanje je važno i sa stanovišta važećih nacionalnih krivičnoprocesno-dokaznih pravila i u kontekstu delovanja Evropske konvencije o ljudskim pravima i u vezi sa njom, donekle već postojeće, ali i očekivane prakse Evropskog suda za ljudska prava. Osim toga, u toj sferi je značajan i stav Suda pravde EU, koji se nedavno, iniciran zahtevom nadležnih nemačkih pravosudnih organa, ali samo na preliminarnom nivou i to aktivnostima generalnog advokata koji pred tim Sudom postupa, „oglasio“ i u odnosu na to pitanje. Tako je i za države u sastavu Evropske unije, koje taj stav, kao svojevrsno „imperativno tumačenje“, i formalno obavezuje, ali je taj intepretativni stav od značaja i za države koje su kao „kandidati“ u izvesnoj meri u „pravnoj orbiti“ EU.

U daljem tekstu će se izložiti jedan pogled na pitanje osnovnih dokaznih problema i procesnih reperkusija pojave u krivičnom postupku dokaza/informacija proizišlih iz (de)šifrovane komunikacije ostvarene korišćenjem posebnih aplikacija za tajno/zaštićeno/kriptovano komuniciranje, uz odgovarajuću analizu uporedno-pravnih primera/prakse. Osim toga, kao i inače kada je reč i o bilo kojoj drugoj vrsti informacije/dokaza u krivičnom postupku, neophodno je obratiti pažnju i na objašnjenje osnovnih zakonskih pravila koja se generalno i načelno tiču pravne valjanosti/zakovitosti dokaza. To će se, naravno, prikazati bez konačnog zaključka u pogledu definitivnog dokaznog značaja/definitivne dokazne verodostojnosti dokaza/informacija proizišlih iz oblika tajne/kriptovane komunikacije tehničkim sredstvima i korišćenjem posebnih aplikacija, a koja je dešifrovana na relevantne tehničke načine i u određenom pravnom ambijentu, što znači u skladu sa pravilima konkretne države/konkretnih država čiji su nadležni organi sprovodili konkretne dokazne radnje i pribavljali podatke o ostvarenoj tajnoj komunikaciji jer pravo na izvođenje takvog definitivnog zaključka pripada samo nadležnim sudovima u krivičnom postupku/aktuelnim krivičnim postupcima.

2. RELEVANTNE ODREDBE EVROPSKE KONVENCIJE O LJUDSKIM PRAVIMA I OSNOVNIM SLOBODAMA – KADA JE REČ O INFORMACIJAMA/DOKAZIMA PROIZIŠLIM IZ (DE)ŠIFROVANE KOMUNIKACIJE KRIPTOVANE POSEBNIM APLIKACIJAMA

Dokazni značaj informacija proizišlih iz (de)šifrovane komunikacije, što se tiče i načina pribavljanja/korišćenja tih informacija/dokaza i njihove veze sa drugim informacijama/dokazima, onda kada je reč o pravnim sistemima država koje su članice Saveta Evrope, imaju i određene odredbe Evropske konvencije o ljudskim pravima (EKLJP). To se pre svega tiče člana 5. EKLJP (pravo na slobodu i bezbednosti) te člana 6. EKLJP (pravo na pravično suđenje).⁵ U određenoj meri je relevantan i član 8. EKLJP (pravo na privatnost), što će se, ilustracijom prakse ESLJP koja se tiče tog prava u kontekstu korišćenja u krivičnom postupku informacija proizišlih iz (de)šifrovane komunikacije ostvarene posebnim uređajima/aplikacijama za zaštićeno/tajno komuniciranje putem kriptovanja, posebno objasniti u daljem tekstu.

Kada je reč o pitanju zakonitosti/pravne valjanosti dokaza, od značaja je tradicionalni i davnašnji stav Evropskog suda za ljudska prava da se to pitanje načelno reguliše nacionalnim zakonodavstvom, tako da samo sud u krivičnom postupku koji se vodi u konkretnim državama članicama/strankama Evropske konvencije o ljudskim pravima može da oceni da li je postupak, posmatran u celini, vođen tako da se može smatrati *fair* procedurom (*Schenk v. Switzerland* §§ 45–46;⁶ kao i *Khan v the United Kingdom* § 34).⁷ ESLJP se do sada nije neposredno bavio pitanjem dokaznog kredibiliteta informacija proizišlih iz (de)šifrovane komunikacije ostvarene posebnim uređajima/aplikacijama za zaštićeno/tajno komuniciranje putem kriptovanja, u kontekstu prava na pravično suđenje, ali bi pitanje korišćenja takvih dokaza potencijalno moglo da bude predmet odlučivanja ESLJP i u kontekstu ocene po-

5 Na temelju uobičajenih prevoda tih odredaba Evropske konvencije o ljudskim pravima i osnovnim slobodama, kao i u vezi s tim, na osnovu formulacije sadržane u članu 32. stav 1. Ustava Republike Srbije, uobičajeno se govori o „pravu na pravičan krivični postupak/pravu na pravično suđenje“, u pogledu čega se, inače s pravom, ističe i da se u tom pogledu može govoriti i o pogrešnom prevodu na srpski jezik engleske sintagme *fair and public hearing*, gde se ne uzima u obzir da bi adekvatan prevod engleske reči „fair hearing/fair procedure“ pre bio pošten postupak/pošteno suđenje, nego pravičan postupak/pravično suđenje. Više o tome: K. Čavoški (2017). *O pravdi i pravičnosti*, Beograd, p. 249–250.

S druge strane, pravičnost, kako je formulisana u našem Ustavu, ali već i u članu 1. Zakonika o krivičnom postupku, postala je uobičajena, te čak predstavlja segment našeg pozitivnog relevantnog prava, iako nije sporno da, kada je reč o krivičnom postupku, svakako nije reč o „pravdi i pravičnosti u njihovom suštinskom smislu“, već je osnovna ideja da se krivični postupak ostvaruje uz poštovanje prava na odbranu, pretpostavke nevinosti i svih drugih osnovnih garancija jednog elementarnog „fair“ postupka, te da obe stranke u krivičnom postupku načelno imaju jednak procesni položaj, odnosno raspoložu približno jednakim procesnim sredstvima i mogućnostima, što je, inače, suština i načela „jednakosti oružja“ u krivičnoprocesnom smislu.

6 *Application no. 10862/84 – Judgment*, 12th July 1988. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-94249%22%5D%7D>, 30. mart 2024.

7 *Application no. 35394/97, Judgment*, 12th May 2000. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-108113%22%5D%7D>, 30. mart 2024.

štovanja garancija iz člana 6. EKLJP. U daljem tekstu će se objasniti jedan skorašnji takav slučaj protiv Turske, koji se suštinski ne može smatrati nekim načelnim stavom ESLJP jer se tu radi samo o zaključku ovog suda da činjenica da je okrivljeni posedovao konkretnu aplikaciju ne može biti jedini/ekskluzivni ili pretežni dokaz, dovoljan „sam po sebi“, za zaključak suda da je on samim tim i član terorističke organizacije/mreže.

Ni kada je reč o pravu na slobodu i bezbednost (član 5. EKLJP), nema još uvek stavova ESLJP, koji bi se ticali informacija/dokaza proizišlih iz (de)šifrovane komunikacije ostvarene posebnim uređajima/aplikacijama za zaštićeno/tajno komuniciranje putem kriptovanja, a u tom pogledu je, kao i inače, bitno imati na umu i neke ustaljene stavove ESLJP. Tako je posebno relevantan stav zauzet u slučaju *Simons v. Belgium*,⁸ shodno kojem pitanje zakonitosti i upotrebe dokaza nije nužno pitanje koje obavezno treba rešavati prilikom odlučivanja o pritvoru. Ovde je od značaja i stav ESLJP izražen u slučaju *Bykov v. Russia*,⁹ iz kojeg proizlazi da se prilikom odlučivanja o opravdanosti/obrazloženosti/valjanosti pritvora u konvencijskom smislu (što se, u osnovi, svodi i na ustavnopravni kriterijum), vodi računa o sledećim kumulativno formulisanim pitanjima: 1) priroda nezakonitosti u konvencijskom smislu, što znači sa stanovišta ocene da li je nastupila povreda nekog prava sadržanog u Konvenciji, 2) da li je kvalitet dokaza, s obzirom na okolnosti pod kojima su prabavljeni, takav da postoje dileme u pogledu pouzdanosti dokaza, 3) da li okrivljeni imao mogućnost osporavanja dokaza, kao i 4) kakav je značaj dokaza u konkretnom krivičnom postupku. Proveravanje ispunjenosti ovih pitanja, odnosno davanje odgovora na njih poznato je u praksi Evropskog suda za ljudska prava kao „Bykov test“, koji se inače, prema praksi samog ESLJP, koristi/mora koristiti i kada se radi o elektronskim/digitalnim dokazima (*Yüksel Yalçınkaya v. Türkiye* [GC] § 313).¹⁰

3. ZNAČAJ ZAKONITOSTI/PRAVNE VALJANOSTI DOKAZA U KRIVIČNOM POSTUPKU

Zakonik o krivičnom postupku ne sadrži pojam dokaza, iako se u mnogim njegovim odredbama spominju dokazi. Nije u pitanju nikakav poseban propust zakonodavca jer pojmovno određenje dokaza u suštini i ne treba da bude deo sadržine Zakonika o krivičnom postupku niti bilo kojeg drugog izvora krivičnog procesnog prava, već se u praksi, na temelju osnovnih teorijskih koncepcija, izgrađuje shvatanje o tome šta je dokaz u konkretnom slučaju i kakav je njegov dokazni kredibilitet, a pritom u odnosu na dokaze i druge dokazne pojmove važe i određena osnovna načela krivičnog postupka.¹¹ U našoj teoriji se opravdano ističe da dokazi proistekli iz *Sky*

8 <https://www.justiceinitiative.org/uploads/011e5634-375c-4d51-9135-055adc72058b/digests-arrest%20rights-european-court-human-rights-20130419.pdf>, 29. novembar 2023.

9 <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%222001-91704%22%5D%7D>, 29. novembar 2023.

10 <https://hudoc.echr.coe.int/fre#%7B%22tabview%22:%5B%22document%22%5D%7D%22%5D%7D>, 25. mart 2024.

11 Nikada se ranije u našim zakoni(ci)ma o krivičnom postupku nisu formalno definisali različiti procesno relevantni stepeni sumnje, kao što se to ni inače, po pravilu, ne čini u izvorima krivičnog procesnog prava drugih država, koje bi mogle da nam posluže kao uporednopravni primer.

ECC komunikacije, a isto je po logici stvari i kada je reč o informacijama/dokazima koji su proizašli iz drugih oblika zaštićene/tajne komunikacije ostvarene posebnim aplikacijama, predstavljaju (elektronske odnosno digitalne) isprave, pribavljene putem međunarodne pravne pomoći.¹² Slično tome se i u nemačkoj krivičnoprocesnoj teoriji konstatuje da su isprave u krivičnoprocesnom smislu „dokumenta, koja sadrže određene misli/značenja, koja se mogu pročitati“, a tu spadaju i elektronska dokumenta sve dok postoji mogućnost da se „pročitaju“, što znači dok je moguće uočiti njihovo odgovarajuće značenje.¹³ Sva opšta dokazna pravila, koja se odnose i na druge vrste dokaza u krivičnom postupku, moraju se, po logici stvari, primeniti i na takve dokaze, koji se mogu smatrati elektronskim ispravama.

Dokazi su podaci činjenične prirode, koji proizlaze iz krivičnoprocesnih radnji koje su preduzeli subjekti krivičnog postupka, na temelju kojih se izvode krivičnopravno relevantni zaključci u pogledu bitnih elemenata krivičnog dela, te izbora, odnosno mere konkretne krivične sankcije, kada su za to ispunjeni potrebni materijalni i procesni uslovi, ili se zahvaljujući tim podacima izvode krivičnopravno i krivičnoprocesno relevantni zaključci organa krivičnog postupka, a takvi zaključci suda se u procesnom smislu uobličavaju u odluci kojom se na zakonski regulisan način rešava predmet krivičnog postupka. Dokazivanje u krivičnom postupku tiče se odgovarajućeg predmeta dokazivanja (*thema probandi*). Predmet dokazivanja su *činjenice* koje su relevantne za donošenje sudske odluke o predmetu krivičnog postupka, bilo zbog toga što imaju direktan krivičnopravni značaj, kada se njima rešavaju pitanja krivičnog dela, te krivične sankcije, ako su ispunjeni potrebni uslovi za njeno izricanje, bilo zato što su značajne u krivičnoprocesnom smislu, kada se odnose na pitanja krivičnog gonjenja ili druga krivičnoprocesna pitanja. Predmet dokazivanja se u krivičnoprocesnoj literaturi tradicionalno označava kao „tema dokazivanja“ ili *predmet dokaza*, odnosno *thema probandi*, za koju se ističe da su to sve one „važne ili relevantne činjenice, od kojih zavisi pojedina sudska odluka u konkretnom krivičnopravnom sporu“.¹⁴

Dokazi i dokazivanje su u krivičnom postupku u funkciji utvrđivanja relevantnog činjeničnog stanja, a ni danas u vreme kada je, na prvi pogled, bitno promenjen način dokazivanja te modifikovan značaj i domet načela istine u krivičnom postupku, što je, naravno, prilično relativnog karaktera jer i prema pravilima važećeg Zakonika o krivičnom postupku, kao i decenijama ranije, postoji i žalbeni osnov koji se svodi na pogrešno ili nepotpuno utvrđeno činjenično stanje, ne gubi aktuelnost zapažanje naše tradicionalne krivičnoprocesne teorije o „posebnom zna-

Međutim, u važećem ZKP se definišu *tri procesno relevantna stepena sumnje* – osnovi sumnje, osnovana sumnja i opravdana sumnja, a tim se definicijama donekle, odnosno implicitno, definišu i dokazi, a naročito podela na neposredne i posredne dokaze, što inače nije karakteristično za savremene zakon(ik)e o krivičnom postupku, u kojima se to pitanje uglavnom prepušta sudskoj praksi, odnosno praksi organa krivičnog postupka, što se suštinski zasniva na delovanju načela slobodne ocene dokaza.

12 V. Bajović, p. 160.

13 W. Beulke, S. Swoboda (2020). *Strafprozessrecht*, 15. Neu bearbeitete Auflage, Heidelberg, p. 162.

14 B. Marković (1937). *Udžbenik sudskog krivičnog postupka Kraljevine Jugoslavije*, Beograd, p. 288. Inače, termin „spor“ se u našem savremenom krivičnom procesnom pravu praktično ne koristi jer je on više vezan za građanski postupak.

čaju i posebnim teškoćama utvrđivanja činjenica u krivičnom postupku“. Tako se ističe: „U krivičnom postupku, više no u bilo kom drugom, postoji opšti interes da se činjenice pravilno utvrde. Građanin ni u jednom postupku ne sme da trpi zbog nesposobnosti, površnosti ili neznanja suda, ali najmanje u krivičnom. Nije bez značaja da li će pojedinac koji je tužen u parničnom postupku, neopravdano biti odbijen od svog tužbenog traženja zbog netačno utvrđenog činjeničnog stanja, ali je nesumnjivo većeg opšteg i individualnog značaja da li će pojedinac zbog netačno utvrđenog činjeničnog stanja biti neopravdano osuđen na kaznu za krivično delo, odnosno iz tog razloga biti neopravdano oslobođen.“¹⁵

Da bi dokazi mogli da posluže bilo kao osnova za bilo koji procesno relevantan stepen sumnje u krivičnom postupku, bilo kao temelj za odluku suda o predmetu krivičnog postupka, oni moraju biti pravno valjani, odnosno zakoniti sa stanovišta načina njihovog pribavljanja, obezbeđivanja, ocenjivanja i uopšte procesnog vrednovanja.¹⁶ U savremenom krivičnom procesnom pravu pravne države zasnovane na vladavini prava, veliki je značaj dokaznih zabrana koje predstavljaju pravila po kojima se, *s jedne strane*, određena dokazna sredstva načelno isključuju od upotrebe u krivičnom postupku, te se neki izvori dokaza iz određenih razloga, koji se svode bilo na njihovu neetičnost, striktnu zakonsku zabranjenost, odnosno njihov kriminalni karakter (na primer, tortura, narkoanaliza itd.), bilo na njihovu nedovoljno potvrđenu pouzdanost (na primer, poligraf, odnosno tzv. detektor laži, hipnoza itd.), ne mogu koristiti za utvrđivanje činjenica u krivičnom postupku, niti se na njima može zasnivati odluka suda kojom se rešava predmet krivičnog postupka.

Dokazne zabrane se odnose i na određene načine izvođenja dokaza i na odgovarajuće vrednovanje dokaza u krivičnom postupku.¹⁷ Smatra se da je primena određenih metoda i načina ispitivanja zabranjena u odnosu na okrivljenog jer mada je „cilj krivičnog postupka utvrđivanje istine“, njemu se ne sme težiti po svaku cenu, jer krivični postupak, osim toga, mora da bude pravičan, korektan i pošteno vođen.¹⁸ U teoriji je veoma uticajno i učenje o paralelnom postojanju dokaznih zabrana i dokaznih pravila, mada su to, u stvari, pre svega dokazna pravila, a deo tih pravila sadrži i odgovarajuće dokazne zabrane, tj. odnosi se na njih.¹⁹ Smisao i osnovna svrha postojanja zabranjenih metoda/načina izvođenja dokaza je da bi „razjašnjavanje krivičnih dela bez postojanja bilo kakvih granica u tome, proizvelo opasnost uništenja mnogih društvenih i ličnih vrednosti“.²⁰

Prva grupa dokaznih zabrana su istovremeno zabrane *apsolutnog karaktera* jer određene metode nikada ne mogu biti legalna dokazna sredstva. Tako se, na primer, ni pod kojim uslovima iskaz dobijen mučenjem ne može dokazno koristiti, a osim

15 T. Vasiljević (1981). *Sistem krivičnog procesnog prava SFRJ*, Beograd, p. 293.

16 Z. Stojanović, M. Škulić, V. Delibašić (2018). *Osnovi krivičnog prava, Knjiga II – Krivično procesno pravo – Krivični postupak kroz praktičnu primenu*, Beograd, p. 151–152.

17 G. Ulsamer (hrsg.) (1996). *Lexikon des Rechts – Strafrecht – Strafverfahrensrecht*, 2. überarbeitete und erweiterte Auflage, p. 179.

18 H. Walder (1965). *Die Vernehmung des Beschuldigten*, Hamburg, p. 147.

19 Više o „dokaznim zabranama i dokaznim pravilima“: S. Kaiser (1999). *Die Drei-Stufen-Theorie zur Bestimmung von Beweisverboten im Strafprozeß*, Frankfurt, Berlin, p. 21–23.

20 C. Roxin, B. Schüneman (2017). *Strafverfahrensrecht*, 29. Auflage, München, p. 172.

toga, lice koje je primenilo torturu, odnosno iznuđivalo iskaz, moralo bi i krivično da odgovara. Zabranjeno je i kažnjivo svako nasilje nad licem lišenim slobode i licem kome je sloboda ograničena, kao i svako iznuđivanje priznanja ili kakve druge izjave od okrivljenog ili drugog lica koje učestvuje u postupku.

Druga grupa dokaznih zabrana su zabrane *relativnog karaktera* jer su to inače dopuštena i zakonska dokazna sredstva, ali se dokazi njima ostvareni ne smatraju podobnim za korišćenje u krivičnom postupku, te se u dokaznom smislu potpuno procesno isključuju, jer su prilikom njihovog izvođenja, odnosno pribavljanja, napravljene određene teške greške, bilo da su one plod nemarnog, odnosno nestručnog rada, ili su čak proizašle iz nekih zloupotreba subjekata postupka. To bi, na primer, bilo kada bi se okrivljeni u nekom od slučajeva obavezne stručne odbrane saslušao bez prisustva branioca i u takvom slučaju njegov iskaz ne bi imao nikakav dokazni kredibilitet u krivičnom postupku.

Smatra se da u nauci krivičnog procesnog prava ne postoji sasvim jedinstvena terminologija dokaznih zabrana. Pod opštim pojmom dokaznih zabrana treba podrazumevati sve pravne norme, koje sadrže ograničenja za izvođenje određenih dokaza u krivičnom postupku, a one mogu da se podele na *dve osnovne grupe*: 1) *zabrana korišćenja* određenih dokaza i dokaznih sredstava, te 2) *zabrana vrednovanja* određenih dokaza, odnosno zabrana korišćenja rezultata nekih dokaznih sredstava.²¹ Na primer, mučenje kao zabranjena metoda ili korišćenje nekih hemijskih sredstava kojima se deluje na volju lica koje se saslušava, odnosno ispituje, spadaju u zabranjena dokazna sredstva, te su i dokazi pribavljeni takvim dokaznim sredstvima zabranjeni, ali je istovremeno, po logici stvari, ako bi se takav dokaz nekom omaškom ipak zadržao u spisima, zabranjeno njegovo vrednovanje, odnosno na njemu se ne može zasnivati sudska odluka. To znači da prva grupa dokaznih zabrana, prema prethodno izloženoj podeli (Roxin), istovremeno ima i karakteristike druge grupe dokaznih zabrana, tako da je upotreba tih dokaznih sredstava i dokaza zabranjena, ali ako su oni iz nekog razloga ipak upotrebljeni, zabranjeno je njihovo vrednovanje. Kod ove grupe dokaznih zabrana praktično postoji kumulativna *zabrana korišćenja i vrednovanja*.

Za drugu grupu dokaza je karakteristično da se oni mogu načelno upotrebljavati, ali u određenim slučajevima se *ne mogu vrednovati*, odnosno na njima se ne može zasnivati sudska odluka. Na primer, iskaz okrivljenog (izvor dokaza) je dokaz koji se dobija saslušanjem okrivljenog, koje služi kao dokazno sredstvo, ali ako su tokom saslušanja napravljene određene greške, na primer, ako je okrivljeni protivno odredbama ZKP saslušan bez prisustva branioca, onda se na tako dobijenom iskazu ne može zasnivati sudska odluka, to jest taj se iskaz ne može dokazno vrednovati. Takođe, poseban slučaj zabrane vrednovanja određenih dokaza je postupanje prema pravilima dokazne koncepcije o „plodovima otrovnog drveta“.

Zakonikom o krivičnom postupku je propisano da se sudske odluke ne mogu zasnivati na *pravno nevaljanim dokazima*, gde spadaju dokazi koji su, neposredno ili posredno, sami po sebi ili prema načinu pribavljanja u suprotnosti sa sledećim opštim izvorima prava: 1) Ustavom, 2) Zakonikom o krivičnom postupku, 3) dru-

21 Više o tome: C. Roxin (1998). *Strafverfahrensrecht*, 25. Auflage, München, p. 180.

gim zakonom ili 4) opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima.

Konačno, za savremene krivične postupke karakteristično je i važenje dokazne koncepcije o „plodovima otrovnog drveta“, odnosno „plodovima otrovne vočke“ – *Fruit of the poisonous tree doctrine – die Früchte des vergifteten Baumes*.²² Ta teorija je inače veoma uticajna u anglo-američkom krivičnom procesnom pravu,²³ gde se dođuše mnogo više vezuje za koncepciju o pravnoj nevaljanosti dokaza do kojih se došlo nakon ispitivanja osumnjičenog koje nije obavljeno u skladu sa zakonskim i ustavnopravnim propisima – poznati slučaj „Miranda“.²⁴ U našem krivičnom procesnom zakonodavstvu dugo nije na izričit način regulisano pitanje dokaza koji su inače valjani, ali se do njih došlo zahvaljujući podacima koji su prethodno pribavljeni na nezakonit način. Prema pravilima dokazne koncepcije o „plodovima otrovnog drveta“, ni takvi dokazi ne bi bili zakoniti, iako oni sami po sebi to jesu, zato što je način njihovog pribavljanja bio nelegalan. To pitanje se u našem krivičnom procesnom ambijentu i u periodu postojanja pravne praznine u odnosu na problematiku kojom se bavi ta veoma uticajna dokazna koncepcija i inače moglo rešavati prema opštem tradicionalnom pravnom pravilu da ono što je od početka ništavo ne može u daljem postupku da se osnaži, slično kao što, na primer, u građanskom pravu važi poznato pravilo – „što se grbo rodi, ni vreme ne ispravi“. Slično tome, moglo bi se poći od stava da se upotrebom pravno nevaljanih radnji ne mogu pribavljati pravno valjani dokazi, odnosno važeći dokazi koji imaju potreban stepen dokaznog kredibiliteta, ali to u našim izvorima krivičnog procesnog prava doskora nije bilo striktno određeno, pa se rešenje tog pitanja moralo prepuštati sudskoj praksi.

Međutim, u našoj teoriji postoji i stav prema kome ni naše „doskorašnje“ zakonodavstvo (ZKP iz 2001) nije prihvatilo dokaznu teoriju „plodova otrovnog drveta“, što se ilustruje nekim primerima koji se odnose na pribavljanje inače zakonitih dokaza, ali do kojih se došlo nekom prethodnom nezakonitom radnjom. Kada, na primer, osumnjičeni za krivično delo ubistva prizna pod prinudom da je izvršio krivično delo, pa na osnovu tog priznanja policija pronade leš, tada se prema koncepciji „plodova otrovnog drveta“ smatra da „za sud ne postoji ni priznanje ni leš“. Međutim, u našoj teoriji se ističe da takav stav predstavlja čistunstvo koje je očigledno preterano, te kao takvo nije prihvatljivo za naše krivično procesno pravo.²⁵ Da li se ovde uopšte radi o nekakvom „čistunstvu“ u odnosu na dokaze ili se pitanje mora posmatrati u okvirima rešenja pozitivnog Zakonika o krivičnom postupku? Prethodno citirani autor se poziva na jedan rad iz naše starije literature koji se odnosi na ranije važeći Zakon o krivičnom postupku,²⁶ koji zaista nije sadržavao norme čije bi se dejstvo svodilo na zabranu upotrebe dokaza koji su sami po sebi ili *prema*

22 Više o tome: K. Schaefer (1976). *Strafprozessrecht – Eine Einführung*, Berlin, New York, p. 271.

23 M. Škulić (2023). *Osnovi krivičnog prava Sjedinjenih Američkih Država*, 2. izmenjeno i dopunjeno izdanje, Beograd.

24 J. M. Scheb (1999). *Criminal Law and Procedure*, Belmont, Bonn, Boston, Washington, p. 427.

25 M. Grubač (2002). *Krivično procesno pravo – Uvod i opšti deo*, 2. izmenjeno i dopunjeno izdanje, Beograd, p. 296.

26 M. Damaška (1960). Procesne posledice upotrebe dokaza dobivenih na nedozvoljen način, *Naša zakonitost*, 3–6, p. 220.

načinu pribavljanja pravno nevaljani. Međutim, čini se da je potom, nakon većih promena naše krivične procedure, taj problem bio rešen na bitno drugačiji način, tako da se više nije postavljalo pitanje tumačenja da li bi isključenje dokaza koji su sami po sebi dokazno valjani, ali se do njih došlo na način koji je zabranjen ili nije u dokaznom smislu dozvoljen, *već je to pitanje bilo striktno rešeno samim Zakonikom o krivičnom postupku.*

Osnov za stav da je naš zakonodavac ipak prihvatao teoriju o „voću otrovnog drveta“ ili koncepciju o „plodovima otrovne voćke“ može se naći u nekadašnjim opštim odredbama Zakonika o krivičnom postupku. Odredbom člana 18. stav 2. ZKP iz 2001. godine bilo je predviđeno da se sudske odluke ne mogu zasnivati na dokazima koji su sami po sebi ili prema načinu pribavljanja u suprotnosti sa odredbama tog zakonika, drugog zakona, ustava ili međunarodnog prava. Na taj je način bio utvrđen funkcionalni pojam nelegalnog dokaza, koji je definisan kao *zabranjeni osnov* za donošenje sudskih odluka. Pojam nezakonitog dokaza se određivao funkcionalno, i to u dva smisla: *prvo* – s obzirom na kvalitet i poreklo njegove dokazne nekredibilitnosti, kada su postojale dve situacije; 1) ako je takav dokaz *sam po sebi* bio suprotan sa odgovarajućim pravilima i 2) ukoliko je suprotnost tog dokaza u odnosu na odgovarajuća pravila proizlazila *iz načina* na koji je pribavljen; *drugo* – s obzirom na suprotnost u odnosu na pravila sadržana u nekoliko alternativno navedenih izvora prava, tako da je dokaz sam po sebi, ili prema načinu pribavljanja, mogao da bude u suprotnosti sa odredbama: 1) Zakonika o krivičnom postupku, 2) drugog zakona, 3) ustava, 4) međunarodnog prava.

Iz toga proizlazi da je naš ZKP iz 2001. godine sadržavao dve osnovne vrste nezakonitih, odnosno pravno nevaljanih dokaza: 1) *direktno pravno nevaljani dokazi*, a to su oni dokazi koji su sami po sebi bili nezakoniti, odnosno suprotni određenim krivičnoprocesnim, drugim zakonskim, ustavnim ili međunarodnopravnim pravilima, te 2) *indirektno pravno nevaljani dokazi*, a to su oni dokazi koji sami po sebi nisu smatrani nezakonitim, odnosno pravno nevaljanim, ali je način njihovog pribavljanja bio suprotan određenim pravilima sadržanim u ZKP, drugom zakonu, ustavu ili međunarodnom pravu.

Zatim je, novelama našeg krivičnog postupka 2009. godine (u odnosu na ZKP iz 2001. godine), uvedeno pravilo da se sudske odluke ne mogu zasnivati na *pravno nevaljanim dokazima*, u koje spadaju oni dokazi koji su sami po sebi ili prema načinu pribavljanja u suprotnosti sa Ustavom ili potvrđenim međunarodnim ugovorom ili su Zakonikom o krivičnom postupku, odnosno drugim zakonom, izričito zabranjeni (član 18. stav 2. ZKP iz 2001). Suština te zakonske novele se sastojala u tome što se više nije radilo o zabrani korišćenja i onih dokaza koji su po načinu pribavljanja *suprotni* zakonskim odredbama, već se zahtevalo da su u pitanju dokazi koji su zakonskim odredbama, kako onim sadržanim u ZKP, tako i odredbama drugih zakona, *izričito zabranjeni*. Time se (što bi moglo biti predmet argumentovane kritike), praktično, u određenoj meri sužavalo dejstvo poznate dokazne koncepcije o „plodovima otrovnog drveta“.

Pozitivni Zakonik o krivičnom postupku Srbije se u suštini „vraća“ na rešenje koje je već bilo sadržano u Zakoniku iz 2001. godine, tako da se, kao što je već

navedeno, sudske odluke ne mogu zasnivati na *pravno nevaljanim dokazima*, u koje spadaju dokazi koji su, neposredno ili posredno, sami po sebi ili prema načinu pribavljanja, u suprotnosti sa sledećim opštim izvorima prava: 1) Ustavom, 2) Zakonikom o krivičnom postupku, 3) drugim zakonom ili 4) opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima. To znači da postoje *dve vrste pravno nevaljanih dokaza*: 1) *direktno* pravno nevaljani dokazi, u koje spadaju dokazi koji su pribavljeni neposredno suprotno Ustavu, Zakoniku o krivičnom postupku, drugom zakonu ili opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima, kao i 2) *indirektno* pravno nevaljani dokazi – dokazi koji bi sami po sebi bili pravno valjani, ali se smatraju pravno nevaljanim jer način njihovog pribavljanja nije bio pravno valjan.²⁷ Iz toga proizlazi da je naš zakonodavac prihvatio dokaznu koncepciju o „plodovima otrovnog drveta“. U striktnom smislu onaj „dokaz“ koji je nevaljan bilo direktno (sam po sebi), bilo indirektno (prema načinu pribavljanja), u formalnom smislu uopšte i nije dokaz.

Pitanje zakonitosti/pravne valjanosti dokaza je u krivičnom postupku Srbije značajno u svim stadijumima krivičnog postupka, što proizlazi iz toga što je za svaki procesni stadijum neophodno postojanje određenog procesno relevantnog stepena sumnje, poput osnova sumnje za predistražni postupak i istragu te opravdane sumnje za optuženje. I kada prvostepeni sud donese presudu, on mora biti uveren da je ona zasnovana na zakonitim/pravno valjanim dokazima, što potom može biti predmet ocene i u postupku po pravnim lekovima. Tako je jer se pritom svaki procesno relevantan stepen sumnje, kao i izvesnost koju sud stekne nakon izvođenja dokaznog postupka u skladu sa opštim dokaznim pravilima, poput onih sadržanih u načelima slobodne ocene dokaza i slobodnog uverenja suda, ali i principa *in dubio pro reo*, temelji na određenim dokazima koji moraju biti zakoniti/pravno valjani.

U tom smislu i prethodno objašnjeni stav ESLJP zauzet u slučaju *Simons v. Belgium*,²⁸ shodno kojem pitanje zakonitosti i upotrebe dokaza nije nužno pitanje o kojem treba odlučiti priilikom odlučivanja o pritvoru, ima u osnovi sasvim relativan značaj za srpsko krivično procesno pravo. Naime, osnovni uslov za određivanje pritvora je postojanje osnovane sumnje da je okrivljeni učinio krivično delo, pritom uz postojanje i nekog/jednog ili više od opciono propisanih posebnih pritvorskih/osnova razloga, a osnovana sumnja mora proizlaziti iz određenih dokaza odgovarajućeg dokaznog kredibiliteta. Ti dokazi moraju biti zakoniti/pravno valjani, što znači da se pitanjem zakonitosti/pravne valjanosti dokaza krivični sud mora baviti i kada je reč o dokazima iz kojih proizlazi osnovana sumnja kao osnovni uslov za određivanje pritvora.

Konačno, ovde treba imati u vidu i da važeći Zakonik o krivičnom postupku Srbije pravno nevaljan dokaz, odnosno dokaz koji je, inače, zakonskim pravilima isključen kao dokaz, svrstava među relativno bitne povrede odredaba krivič-

27 M. Škulić (2022). *Krivično procesno pravo*, 13. izdanje, Beograd, p. 195.

28 <https://www.justiceinitiative.org/uploads/011e5634-375c-4d51-9135-055adc72058b/digests-arrest%20rights-european-court-human-rights-20130419.pdf>, 29. novembar 2023.

nog postupka,²⁹ kada se radi o žalbenim osnovima.³⁰ Naime, postoji bitna povreda odredaba krivičnog postupka onda kada se presuda zasniva na dokazu na kome se prema odredbama Zakonika o krivičnom postupku ne može zasnivati, osim ako je, s obzirom na druge dokaze, očigledno da bi i bez tog dokaza bila doneta ista presuda.

4. ZAJEDNIČKI EVROPSKI ISTRAŽNI TIMOVI, EVROPOL, EVRODŽAST I EVROPSKI ISTRAŽNI NALOG U KONTEKSTU NADZORA I DEŠIFROVANJA KOMUNIKACIJE KRIPTOVANE POSEBNIM APLIKACIJAMA/UREĐAJIMA

Kada je u pitanju međunarodna pravna pomoć u krivičnim stvarima, zemlje članice Evropske unije imaju dva režima, jedan koji važi u odnosu na zemlje članice i drugi koji važi u odnosu na treće zemlje.³¹ Evropol i Evrodžast su primarno svrstani u prvi režim, ali oni redovno ili po potrebi ostvaruju i određene oblike saradnje sa nadležnim organima država koje nisu članice EU, dok su zajednički evropski istražni timovi i evropski istražni nalog isključivo mehanizmi uzajamne krivičnopravne saradnje samih država članica EU.

Evropski istražni nalog u najvećem delu predstavlja značajno unapređenje i činj enje efikasnijim nekih već ranije postojećih mehanizama sadržanih u evropskom nalogu za dostavljanje dokaza, koji je njegova preteča, ali se njime uvode i neki ranije potpuno nepostojeći oblici i nove forme dokazne saradnje između država članica EU.³² Evropski nalog za dostavljanje dokaza bio je samo prva faza u procesu racionalne supstitucije decenijama postojećeg sistema klasične uzajamne krivičnopravne pomoći u dokaznoj materiji na nivou Evropske unije. Drugu fazu u tom prilično dugotrajnom procesu predstavlja evropski istražni nalog, koji je usvojen u formi Direktive broj 2014/41/EU, u aprilu 2014. godine, a čije su relevantne odredbe, u skladu sa članom 36. te direktive, države članice EU dužne da unesu u domaće zakonodavstvo do 22. maja 2017. godine. Na operativnom nivou policije država članica EU u nekim slučajevima formiraju zajedničke istražne timove, a saradnja pravosudnih istražnih organa, bilo javnih/državnih tužilaca u državama koje imaju javnotužilačku/državnotužilačku istragu, bilo istražnih sudija u državama koje poznaju sistem sudske istrage, odvija se posredstvom i u okviru Evrodžasta.³³ Svi ovi oblici uzajamne krivičnopravne saradnje imali su odgovarajuću ulogu i u slučajevima informacija/dokaza proizišlih iz tajne/šifrovane komunikacije ostvarene određenim tehničkim sredstvima, na temelju posebnih aplikacija za tajno/zaštićeno komuniciranje.

29 Za relativno bitne povrede odredaba krivičnog postupka karakteristično je da kod njih kumulativno moraju da postoje: a) određena povreda zakonske odredbe i b) odgovarajuća *posledica* koja iz te povrede proizlazi.

30 M. Škulić, T. Bugarski (2015). *Krivično procesno pravo*, Novi Sad, p. 501.

31 Z. Stojanović (2018). *Međunarodno krivično pravo*, 12. izdanje, Beograd, p. 180.

32 M. Škulić (2022). *Međunarodno krivično pravo*, Beograd, p. 539.

33 M. Fletcher, R. Löf, B. Gilmore (2008). *Eu Criminal Law and Justice*, Cheltenham, Northampton, p. 65.

Evropski istražni nalog omogućava sprovođenje određenih elemenata istrage u jednoj državi članici EU, što podrazumeva i preduzimanje neophodnih dokaznih radnji za potrebe ostvarenja svrhe krivičnog postupka koji se vodi u drugoj državi EU. Za razliku od evropskog naloga za dostavljanje dokaza, koji je u suštini sveden na jednostavno „transferisanje“ predmeta, spisa i uopšte podataka koji mogu imati dokazni značaj jedne države članice EU drugoj državi u sastavu EU, evropski istražni nalog ima znatno širi domet, a pomoć koju nadležni organi jedne države članice EU, na osnovu tog naloga, pružaju nadležnim organima druge države u sastavu EU znatno je šira i kompleksnija. Što je posebno značajno, ona proizlazi iz aktivnog istražnog (dokaznog) delovanja, tako da u praksi ima daleko veći dokazni potencijal.

Evropski istražni nalog može se izdati u odnosu na krivični postupak koji pokreće pravosudni organ ili koji se može pokrenuti pred tim organom u vezi sa krivičnim delom prema pravu države izdavanja, kao i u odnosu na druge postupke, pa i neke upravne postupke. Evropski istražni nalog se izdaje na standardizovanom obrascu koji sadrži sledeće obavezne elemente: 1) podatke o organu države izdavanja, 2) predmet evropskog istražnog naloga i razloge za njegovo izdavanje, 3) potrebne informacije koje se odnose na okrivljenog ako je on poznat, 4) opis krivičnog dela koje je predmet istrage ili postupka i važeće odredbe krivičnog prava države izdavanja i 5) opis zatražene istražne mere ili više mera, uz navođenje dokaza koje treba pribaviti konkretnim dokaznim radnjama. Evropskim istražnim nalogom se može zahtevati/dobiti čitav niz istražnih mera i dokaza iz njih proizišlih; moguće je održavanje video-telefonskih konferencijskih veza, pribavljanje informacija o bankovnim računima, nadzor nad telekomunikacijama pojedinih lica/okrivljenih itd.³⁴

Evropski istražni nalog će se izdati samo ako su kumulativno ispunjena dva uslova: 1) njegovo izdavanje mora biti nužno i srazmerno svrsi postupka, što znači da evropski istražni nalog nije namenjen istragama krivičnih dela malog/manjeg značaja, te ipak predstavlja svojevrsni dokazni *ultima ratio*, kao i 2) neophodno je da dokazna radnja ili radnje navedene u evropskom istražnom nalogu mogu biti određene u sličnom domaćem krivičnom postupku.³⁵ Izvršenje evropskog istražnog naloga može biti odbijeno ako postoji neki od više opciono propisanih uslova: 1) ukoliko prema pravilima domaćeg prava postoji imunitet ili druga trajna procesna smetnja koja onemogućava izvršenje evropskog istražnog naloga ili se on ne može sprovesti zbog pravila o utvrđivanju i ograničenju krivične odgovornosti u odnosu na slobodu štampe i slobodu izražavanja u drugim medijima, 2) ako bi izvršenje evropskog istražnog naloga štetilo bitnim interesima nacionalne bezbednosti, dovelo u opasnost izvor informacija ili podrazumevalo korišćenje poverljivih informacija koje se odnose na određene obaveštajne aktivnosti, 3) ukoliko dokazna radnja ne bi bila primenjiva u sličnom domaćem slučaju prema domaćem pravu, 4) ako bi izvršenje evropskog istražnog naloga bilo u suprotnosti sa načelom *ne bis in idem*, 5) ako nije ispunjen uslov dvostruke kažnjivosti itd. Evropski istražni nalog izvršava

34 K. Ambos (2018). *Internationales Strafrecht – Strafanwendungsrecht, Völkerstrafrecht, Europäisches Strafrecht, Rechtshilfe*, 5. Auflage, München, p. 667.

35 M. Škulić (2022). *Međunarodno krivično pravo – prostorno važenje krivičnog prava, krivično pravo međunarodnog porekla, međunarodna krivičnopravna pomoć, začeci krivičnog prava EU*, Beograd, p. 769.

se na isti način i pod jednakim uslovima kao da je konkretnu dokaznu radnju na koju je usmeren nalog odredio nadležni domaći organ i izvršava se po postupku koji je organ države izdavanja izričito naveo u nalogu, osim ako je taj postupak u suprotnosti sa osnovnim načelima domaćeg pravnog poretka. Evropski istražni nalog se može odnositi na raznovrsne opšte i posebne dokazne radnje i specijalne istražne tehnike (elementi tzv. prikrivene istrage), među kojima poseban značaj ima nadzor nad elektronskim komunikacijama osumnjičenog. Taj nalog se sprovodi prema načelu hitnosti, a propisani su i odgovarajući rokovi, doduše, po logici stvari, instrukтивne prirode, za postupanje i dostavljanje pribavljenih dokaza.

Policije država u sastavu EU međusobnu saradnju ostvaruju kako bilateralno i neposredno, tako i u okviru Evropola, čije su članice, a putem Evropola je pod određenim uslovima moguće ostvariti saradnju i sa državama koje nisu članice EU. Poseban oblik saradnje iz koje je u konkretnim situacijama i proizišlo dešifrovanje tajne komunikacije tehničkim sredstvima korišćenjem posebnih aplikacija/uređaja predstavlja i formiranje zajedničkih istražnih timova više evropskih policija, što se, takođe, može realizovati i neposrednom policijskom saradnjom i posredstvom Evropola, isto kao što se i informacije/dokazi proizišli iz delovanja takvih istražnih timova, kao i realizovanjem evropskog istražnog naloga, mogu plasirati drugim policijama u EU, ali i van EU, kako klasičnim mehanizmima međunarodne krivično-pravne pomoći, tako i posredstvom samog Evropola.³⁶ Osnovne funkcije Evropola su: 1) informativna i 2) analitička. Informativna funkcija Evropola se ostvaruje stvaranjem centralnog punkta u koji se slivaju sve relevantne informacije, dok se njegova analitička funkcija tiče proučavanja uslova i drugih bitnih elemenata koji se odnose na fenomenologiju i etiologiju kriminaliteta, pre svega u odnosu na EU.³⁷

Evropol nije jedinstvena policijska služba sa izvršnim zadacima, već samo informativno i analitički podržava nacionalne policije u okviru EU u suprotstavljanju teškom kriminalitetu sa elementima inostranosti, koji se odnosi na sledeće kategorije: nelegalna trgovina drogom, nelegalna trgovina radioaktivnim i nuklearnim materijalima, krivična dela protiv ustavnog uređenja, trgovina ljudima, pranje novca, organizovani kriminalitet, terorizam, falsifikovanje novca, zloupotrebe kreditnih kartica, a u vezi sa tim nabrojanim krivičnim delima, organizuju se i potrage za učinocima koji se nalaze u bekstvu.³⁸ Istovremeno sa ukidanjem čvrstih granica između država EU, omogućeno je da policija jedne države pod određenim uslovima može da deluje i na teritoriji druge države u okviru EU, bez nekih posebnih formalnosti.³⁹ To je prvenstveno moguće ukoliko je na teritoriji svoje države započela poteru za učinocima krivičnih dela, koja se brzo mora nastaviti na teritoriji druge države EU. Interno, ali i posebno putem informativnog sistema Evropola, nadležna

36 Inače, sama Organizacija Evropske policije (*Evropol*, na engl. skraćeno *Europol – European Police Office*), nastala je sporazumom iz Maastrichta od 26. jula 1995, a počela je da radi 1. jula 1999. godine.

37 M. Škulić (2022). *Međunarodno krivično pravo*, Beograd, p. 539.

38 W. Brodag (2001). *Kriminalistik – Grundlagen der Verbrechensbekämpfung*, Stuttgart, München, p. 42–43.

39 Više o tome: M. Škulić (2012). Začeci evropskog krivičnog procesnog prava, *Zbornik škole prava Evropske unije*, III sesija, Podgorica, p. 77.

policija se u najkraćem roku obaveštava o preduzetoj akciji, a uvek se teži koordinaciji i saradnji u njenoj realizaciji. Takve mogućnosti predstavljaju početak stvaranja jedinstvene evropske policije, što je od kraja devedesetih godina segment ukupnih napora EU da stvori jedinstven pravni sistem.⁴⁰ Sedište Evropola je u Hagu u Holandiji, a njegovi osnovni zadaci su: ubrzanje razmene informacija između nacionalnih evropskih policija, pripremanje preventivnih analiza kojima se podržavaju aktivnosti država članica EU, pravljenje određenih stratejskih analiza, podržavanje delovanja nacionalnih policija, razvijanje savetodavnih funkcija i edukacije policijskih službenika itd.⁴¹

Informacije/dokazi potekli/proistekli iz šifrovane komunikacije tehničkim sredstvima, do kojih su došli zajednički istražni timovi određenih evropskih policija (Holandije, Belgije i Francuske), kao u nekim situacijama francuska policija, a drugim policije u EU, ali i policije određenih država van EU i uopšte, pravosudnim organima drugih država se dostavljaju prvo na operativnom nivou putem Evropola, a kasnije i na temelju procesnopravnih mehanizama iz domena međunarodne krivičnopravne pomoći. U daljem tekstu će se posebno objasniti koje su dileme s tim u vezi, a pre svega sa stanovišta razjašnjavanja prigovora odbrane u pogledu zakonitosti dokaza do kojih se došlo na takav način delovanjem zajedničkih istražnih timova i stranih policijskih i pravosudnih organa. To je povezano i sa nekim aspektima evropskog istražnog naloga, koji su u jednom trenutku nastali u Nemačkoj, kada se jedan regionalni/zemaljski sud te države obratio Sudu pravde EU radi razjašnjavanja određenih pitanja koja su se smatrala/mogla smatrati spornim.

5. ANALIZA PRIMERA IZ UPOREDNOPRAVNE SUDSKE/PRAVOSUDNE PRAKSE KOJI SE TIČU (DE)ŠIFROVANE KOMUNIKACIJE OSTVARENE APLIKACIJAMA/UREĐAJIMA ZA TAJNO/ZAŠTIĆENO KOMUNICIRANJE

Pitanje dokazne verodostojnosti i dokaznog značaja informacija pribavljenih dešifrovanjem na odgovarajuće tehničke načine komunikacije ostvarene posebnim aplikacijama/uređajima za tajno/zaštićeno komuniciranje, veoma aktuelno širom Evrope, predstavlja i složen dokazni problem, što neposredno proizlazi i iz činjenice da su konkretni podaci pribavljeni mehanizmima međunarodnopravne saradnje – pre svega na nivou EU, kako *inicijalno* (zajednički istražni timovi, uloga Evropola i Evrodžasta, kao i evropski istražni nalog), tako i klasičnim mehanizmom korišćenja *zamolnica*, zahvaljujući čemu se međunarodna pravna pomoć pruža/dobija i unutar EU i u odnosu na države koje nisu članice EU. Zbog toga je i uporednopravna praksa u Evropi još uvek relativno oskudna, pa donekle i kolebljiva.

S druge strane, realno je očekivati i da će se ta praksa na uporednopravnom nivou, nakon skorašnje odluke Suda pravde EU, dobiti odgovarajući „stimulans“, pa

40 W. Beulke (2000). *Strafprozessrecht*, Heidelberg, p. 5–7.

41 W. D. Brodag, p. 43.

i „putokaz“, u odnosu na osnovni pravac rezonovanja o nekim potencijalno spornim pitanjima, koja su od ključnog značaja za načelnu ocenu dokaznog kredibiliteta dokaza i informacija pribavljenih dešifrovanjem na odgovarajuće tehničke načine komunikacije ostvarene posebnih aplikacijama za tajno/zaštićeno komuniciranje.

5.1. Holandija

Praksa holandskih sudova sa informacijama/dokazima proizišlim iz dešifrovane kriptovane komunikacije, ostvarene korišćenjem posebnih aplikacija/uređaja, utemeljena je primarno na načelnom stavu Vrhovnog suda Holandije, interpretativnog karaktera, koji se tiče (de)šifrovane komunikacije ostvarene putem aplikacije *EncroChat* za tajno/zaštićeno komuniciranje.⁴² Prema tom načelnom stavu Vrhovnog suda Holandije, „skinute“/dešifrovane poruke ove vrste (proizišle iz aplikacije *EncroChat*) mogu da se pod određenim uslovima koriste kao dokazi u krivičnim postupcima koji se vode u Holandiji.

Holandski sudovi su svoj stav o dokaznoj verodostojnosti informacija sadržanih u komunikaciji ostvorenoj aplikacijama/uređajima za tajno/zaštićeno komuniciranje *Sky ECC/EncroChat* zasnovali na načelnom stavu da su takve informacije proistekle iz regularnih mehanizama međunarodne krivičnopravne saradnje između Holandije i druge države u čiji pravni sistem nadležni holandski organi načelno „imaju poverenje“. Konkretno, reč je o Francuskoj, ali je Holandski vrhovni sud u tom slučaju svoj stav generalno utemeljio na „opštem principu međudržavnog poverenja“, smatrajući da se taj „princip zasniva na opštem poverenju u pravni sistem druge države i posebno navodeći da je to, kada se radi o konkretnim dokazima, slučaj između Holandije i Francuske“, tako da stoga, „holandski sudovi mogu očekivati da su francuske vlasti istrage sprovele zakonito i da su rezultati pouzdani“.⁴³

Dakle, u krivičnim postupcima u Holandiji se, kada je reč o dokazima proisteklim iz (de)šifrovane komunikacije ostvarene korišćenjem posebnih aplikacija/uređaja za tajno/zaštićeno komuniciranje, do kojih se došlo tako što su dobijeni od nadležnih francuskih organa primenom mehanizama međunarodne pravne pomoći u krivičnim stvarima, načelno polazi od postojanja dve pretpostavke, koje proizlaze iz principa opšteg međudržavnog poverenja: 1) pretpostavlja se da su francuski nadležni organi dokaze pribavili na zakonit način i 2) pretpostavlja se da su takvi dokazi pouzdani.

Naravno, samim tim što se u odluci Vrhovnog suda Holandije „govori/piše“ o pretpostavkama, jasno je da se može dokazivati suprotno, a teret takvog dokazivanja, po logici stvari, pada na one subjekte kojima je to u interesu, a to su okrivljeni i njegov branilac. Međutim, kao što će se objasniti u daljem tekstu, i od suda se očekuje da pokloni pažnju tim pitanjima, ali samo ako postoje dokazi koji potenci-

42 Naime, Vrhovni sud Holandije je 13. juna 2023. godine doneo svoju interpretativnu odluku na zahtev više nižih sudova koji se ticao zauzimanja stava o nizu relevantnih pitanja proisteklih iz korišćenja komunikacije ostvarene *EncroChat* i *Sky ECC* aplikacijama, važnih za aktuelne krivične postupke.

43 Odluka Vrhovnog suda Holandije (*Hoge Raad*) od 13. juna 2023, ECLI:NL:HR:2023:913. <https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:HR:2023:913>, 21. januar 2024.

jalno dovode u pitanje opšte pretpostavke da su takvi dokazi pribavljeni na zakonit način te da su pouzdani. To se još i dodatno konkretizuje u interpretativnoj odluci Vrhovnog suda Holandije u kojoj se navodi da se može poći od pretpostavke da su rezultati istrage sprovedene u drugoj članici EU pouzdani, što znači da se takvi dokazi načelno smatraju pretpostavljeno verodostojnima, ali da ukoliko postoje konkretne informacije/dokazi koji pokazuju da to nije slučaj, sud ima obavezu da ispita pouzdanost tih dokaznih „rezultata“ istrage sprovedene u drugoj državi. Ovde se Vrhovni sud Holandije bavio i načelom „jednakosti oružja“, kao važnim aspektom opšteg krivičnog procesnog načela pravičnog krivičnog postupka, odnosno „jednakošću oružja“ kao segmentom prava na pravično suđenje.⁴⁴ Name, u svojoj odluci se pozvao i na relevantne stavove ESLJP iz kojih proizlazi da pravo odbrane da joj se učine dostupnim svi dokazi kojima raspolaže optužba nije apsolutno, te da to pravo može biti limitirano ako je to neophodno radi zaštite važnog javnog interesa, poput neotkrivanja istražnih metoda koje koristi policija, pri čemu takvo limitiranje mora biti apsolutno neophodno, a i tada se odbrani moraju obezbediti sve procesne garancije koje omogućavaju da postupak bude pravičan.

Inače, u krivičnim postupcima u Holandiji (a bilo je do sada više od 200), u kojima se kao potencijalni dokaz pojavljivala komunikacija proistekla iz (de)šifrovane komunikacije ostvarene korišćenjem posebnih aplikacija/uređaja za tajno/zaštićeno komuniciranje, odlučivalo se o nizu prigovora odbrane koja se ticala takve vrste dokaza, a o čemu je potom svoj autoritativan stav izneo Vrhovni sud Holandije. Naime, odbrana okrivljenih je u tim postupcima redovno zahtevala pristup podacima do kojih se došlo operacijom „hakovanja“ aplikacije *EncroChat*, kako bi na takav način mogla da ostvari sledeće ciljeve: 1) da proveriti integritet podataka, 2) da proveriti pouzdanost podataka, naročito stoga što su korisnici aplikacija koristili pseudonime, i 3) da ustanovi da li postoje i dokazi koji idu u prilog odbrani, poput tzv. ekskulpirajućih dokaza.⁴⁵

Odbrani, tj. braniocima okrivljenih je u krivičnim postupcima u Holandiji u kojima su se pojavljivali/koristili dokazi proistekli ih dešifrovane tajne komunikacije korišćenjem aplikacije *EncroChat*, bio obezbeđen pristup tim podacima te omogućeno pretraživanje svih podataka koji se tiču okrivljenog kojeg brane konkretni branioci. To je svojom (u prethodnom tekstu već pomenutom) odlukom afirmisao i Vrhovni sud Holandije, smatrajući da je takva praksa potpuno usklađena sa zakonom.⁴⁶ Sam pristup podacima ostvaruje se u prostorijama Forenzičkog instituta Holandije, a odbrana ima pravo da koristi isti softver za analizu podataka koji upotrebljava i holandska policija. Osim toga, branioci okrivljenih mogu da podnošenjem posebnog zahteva dobiju sve podatke koji se tiču njihovih branjenika i u *Excel* formatu. Posebno je značajno to što su holandski sudovi braniocima okrivljenih

44 Više o tome: I. Miljuš (2022). *Načelo jednakosti „oružja“ u krivičnom postupku*, Beograd, p. 216–217.

45 J. J. Oerlemans, D. A. G. van Toor (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective, *European Journal of Crime, Criminal Law and Criminal Justice*, no 30, Online Publication Date: 27 Dec 2022. https://brill.com/view/journals/eccl/30/3-4/article-p309_006.xml?language=en, 22. januar 2024.

46 J. J. Oerlemans, D. A. G. van Toor.

redovno davali i podatke o načinu na koji je u Francuskoj sprovedena „operacija“ dešifrovanja tajne komunikacije ostvarene putem posebnih aplikacija (pre svega aplikacije *EncroChat*), što je potom prosleđeno i holandskim nadležnim organima.⁴⁷

5.2. Francuska

Nadležni francuski organi su uspeli da „probiju“ zaštićeni sistem komuniciranja korišćenjem posebnih aplikacija za tajno/zaštićeno komuniciranje, pre svega aplikacije i uređaja *Sky ECC* (prilagođenih mobilnih telefona) za korišćenje te aplikacije. Sam tehničko-tehnološki način na koji su to uspele nadležne službe u Francuskoj, nekada samostalno, a nekada delovanjem zajedničkih istražnih timova sa nadležnim holandskim i belgijskim organima, smatra se tajnom i on se ne otkriva. Firma koja je kreirala *Sky ECC* i na profitnoj osnovi servisirala njeno održavanje tvrdila je da je to postignuto specifičnim „hakovanjem“ aplikacije, što znači ubacivanjem vrste „kompjuterskog virusa“, odnosno „trojanskog konja“ („trojanca“),⁴⁸ što nikada nije definitivno zvanično razjašnjeno, ali je inače i takav način delovanja moguć prema pravilima francuskog zakonodavstva.

Francuski Zakonik o krivičnom postupku⁴⁹ poznaje posebnu dokaznu radnju „infiltracije u računarski sistem“,⁵⁰ što se svodi na „unošenje tehničkog uređaja“ u kompjuterski sistem, koji omogućava uvid u informacije pohranjene u sistemu, komunikaciju koja se ostvaruje i prenos podataka, a to sve se čini bez saglasnosti vlasnika/korisnika sistema. To se u tehničkom smislu može postići „mehanički“, kada u konkretnom slučaju postoji taktička mogućnost potrebnog fizičkog kontakta sa računarom/mobilnim telefonom, i „daljinski“, slanjem poruka koje sadrže takve

47 J. J. Oerlemans, D. A. G. van Toor.

48 Unošenjem posebnog virusa koji se uobičajeno zove „trojanski konj“ ili „trojanac“ vrše se inače i određeni oblici kompjuterskog kriminaliteta. Takva aktivnost se sastoji u neprimetnom modifikovanju samog kompjuterskog programa ili modaliteta njegovog korišćenja. Ovaj metod se i naziva „trojanskim konjem“ jer se zasniva na prikričenom ubacivanju novih naredbi u postojeće programe, s tim da se njihovo izvršenje odlaže za neki duži period, od nekoliko dana, nedelja ili čak meseci. Takve instrukcije, ubačene u softver, poput svojevrsnog „kukavičjeg jajeta“, veoma je teško otkriti jer su zamaskirane u velikom broju postojećih programskih linija. Ukoliko bi se one i otkrile, bilo bi izuzetno teško identifikovati njihovog autora.

Osim toga, instrukcija ubačena metodom „trojanskog konja“ tako je programirana da se nakon izvršenja naredbe (npr. odašiljanja informacija drugom korisniku) ona sama briše, pa se na takav način eliminišu svi tragovi njenog prisustva i delovanja u memoriji/bazama informacija kompjutera, odnosno u računarskim mrežama. Više o tome: Ž. Aleksić, M. Škulić, p. 388–389.

49 Postoji čitav niz mogućnosti koje se primarno tiču (za)dobijanja digitalnih dokaza korišćenjem same kompjuterske tehnologije za nadzor nad informacijama pohranjenim u računarskoj memoriji, podacima koji su predmet komunikacije preko računarskih mreža, snimanje i transfer takvih podataka i sl. Kako je reč o relativno novim tehnologijama, takve dokazne mogućnosti ne predstavljaju neko tradicionalno rešenje francuskog krivičnog postupka, već su one u ZKP uvedene relativno skorašnjim novelama od 5. marta 2007. i 14. marta 2011. godine. Konkretno, mogućnost dobijanja informacija iz računara/računarske mreže daljinskim putem, zahvaljujući korišćenju posebnih „tehničkih uređaja“, zakonski je oživotvorena novelom od 14. marta 2011. O. Gutkes, *Digital Evidence in Criminal Law*. https://www.ecba.org/extdocserv/conferences/tallinn2012/recdev_france.pdf, 6. april 2024.

50 *Ibidem*.

„tehničke mehanizme“, koji su u stvari posebna vrsta kompjuterskih virusa, najčešće poznatih kao „trojanci“ ili „trojanski konji“.

Naime, prema pravilima iz člana 706–102–1 Zakonika o krivičnom postupku Francuske, istražni sudija u istrazi organizovanog kriminaliteta može, nakon pribavljanja mišljenja javnog tužioca, da dozvoli istražiteljima da ugrade tehnički uređaj kako bi se pristupilo podacima, oni snimili, pohranili i transferisali bez saglasnosti lica kojem takvi podaci pripadaju. Samom zakonskom odredbom je potom precizirano i da se „tehnički uređaj“ može postaviti u računar ili mobilni telefon na samom „mestu“ (što znači fizički) ili sa daljine. Propisano je i da se tako dobijeni podaci ne mogu koristiti u bilo koje druge svrhe, osim radi istraživanja i otkrivanja krivičnih dela koja su predmet aktuelne istrage istražnog sudije. Međutim, ako se ovim radnjama otkriju druga krivična dela, time se ne konstituše ništavost uzgrednog postupka (član 706–102–4). Na taj se način reguliše tzv. slučajni nalaz, u modalitetu koji je i inače čest kada se radi o posebnim dokaznim radnjama, tj. specijalnim istražnim tehnikama u mnogim savremenim krivičnoprocesnim zakonodavstvima.

U Francuskoj je, pre nego što je „provaljena“, odnosno „presretnuta“ aplikacija *Sky ECC* te omogućeno dobijanje sadržaja velikog broja komunikacija ostvarenih korišćenjem te aplikacije, u sudskoj praksi bilo veoma aktuelno pitanje informacija/dokaza pribavljenih nadzorom komunikacije ostvarene putem aplikacije *EncroChat*. Stoga se francuska sudska praksa uglavnom i tiče prikupljanja informacija/dokaza proisteklih iz korišćenja te aplikacije. Nadzor nad tajnim komuniciranjem korišćenjem aplikacije *EncroChat* ostvaren je početkom 2020. godine, delovanjem zajedničkog francusko-holandskog istražnog tima, uz učešće Evropola, a u skladu sa pravilima međunarodne pravne pomoći i saradnje u okviru EU. Na taj se način došlo u posed čak oko 120 miliona poruka kreiranih/razmenjivanih korišćenjem aplikacije *EncroChat*. U formalnom smislu tu akciju je autorizovao Sud u Lilu, izdavanjem pet naredbi za prikupljanje dokaza na takav način u periodu od 30. januara do 31. marta 2020. godine, a potom je u julu 2021. Apelacioni sud u Nansiju doneo presudu kojom je potvrđena zakonitost takvog načina prikupljanja dokaza, uz konstatovanje da se oni kao zakoniti mogu koristiti u krivičnom postupku.

Okrivljeni i njihovi branioci su presudu Apelacionog suda u Nansiju osporili žalbom Kasacionom sudu, tvrdeći da je prikupljanjem podataka sadržanih u komunikacijama korišćenjem aplikacije *EncroChat* povređeno pravo na privatnost i da je, osim toga, presudom Apelacionog suda povređeno pravo na odbranu jer nije ispoljeno pravo na „jednakost oružja“, kao ni pravo na delotvorno pravno sredstvo, pošto je državno tužilaštvo konsekventno uskraćivalo informisanje o tehničkim načinima na koje se došlo do informacija iz zaštićene komunikacije, korišćenjem aplikacije *EncroChat*, što se temeljilo na zaštiti tajnosti/državne tajne, direktno povezano sa interesima odbrane zemlje. Odbrana je u svojoj žalbi insistirala i na tome da nacionalno istražno-tehničko telo nije oficijelno izdalo potvrdu/sertifikat o autentičnosti podataka prikupljenih dešifrovanjem komunikacije ostvarene u konkretnom slučaju korišćenjem aplikacije *EncroChat*.

Svoju presudu kojom odbija žalbe okrivljenih i branioca francuski Kasacioni sud zasniva na konstataciji da prikupljanjem podataka iz komunikacija ostvarenih

aplikacijom *EncroChat*, koji su potom korišćeni kao dokaz u osporenim presudama, u konkretnom slučaju nije povređeno pravo na privatnost okrivljenih. Delimično su usvojeni argumenti odbrane da je povređeno pravo na „jednakost oružja“ u krivičnom postupku jer su odbrani uskraćene informacije o tehničkim aspektima „presretanja komunikacija“, te joj nije izdata ni potvrda nadležnog tehničkog organa o autentičnosti informacija iz takve „presretnute“ komunikacije. Stoga je Kasacioni sud i zaključio da je u konkretnom slučaju francuska policija bila dužna da pruži informacije o tehničkom načinu na koji je pribavila dokaze iz komunikacija ostvarenih aplikacijom *EncroChat* te da, uz to, priloži i odgovarajuću potvrdu autentičnosti konkretnih informacija do kojih se došlo na takav način.⁵¹

Na temelju presude Kasacionog suda,⁵² o predmetu je ponovo odlučivao Apelacioni sud u Mecu, a nešto kasnije je, nakon slične presude Kasacionog suda, ponovo odlučivao Apelacioni sud u Parizu. Kasacioni sud Francuske je potom u maju 2023. godine, odlučujući o novom slučaju te vrste, a na osnovu analize podataka sadržanih u konkretnim spisima predmeta, konstatovao i da aplikacija *EncroChat* u momentu kada su preuzete informacije sadržane u komunikaciji ostvorenoj posredstvom te aplikacije nije suštinski bila kriptovana, te da zato ni ne postoji obaveza prilaganja potvrde o autentičnosti podataka, koja je, inače, neophodna prema pravilima francuskog zakonodavstva.⁵³

5.3. Italija

Vrhovni sud Italije je 15. jula 2022. godine zauzeo stav da okrivljeni mora imati mogućnost da postavlja pitanja koja se tiču sadržaja poruka prikupljenih nadzorom komunikacije ostvarene aplikacijom/uređajima *Sky ECC*, kao i pravo da zahteva informacije o načinu na koji prikupljene informacije sadržane u tajnoj/zaštićenoj komunikaciji ostvorenoj aplikacijom/uređajem *Sky ECC*, radi omogućavanja da se kontrolišu zakonitost i kredibilnost takve vrste dokaza.

Iz tog stava Vrhovnog suda Italije proizišao je zahtev shodno kojem je državno tužilaštvo dužno da obelodani kako se došlo do informacija sadržanih u tajnoj komunikaciji realizovanog putem aplikacije *Sky ECC*. To se praktično svodi na objašnjenje toka i sadržaja konkretnih akcija kojima su dobijene informacije iz (de)šifrovane komunikacije. Do ove odluke Vrhovnog suda Italije nadležna državna tužilaštva su odbijala da upoznaju odbranu sa informacijama tretiranim kao operativne i tajne, a koje su imale istražni karakter u odnosu na kriptovanu komunikaciju korišćenjem aplikacije *Sky ECC*. I niži sudovi su smatrali da su takvi dokazi prihvatljivi te da nema potrebe za detaljnijim upuštanjem u pitanje njihove zakonitosti jer su te dokaze italijanskim pravosudnim organima prosledile strane sudske vlasti država koje

51 Više o tome: B. Goodwin, *French supreme court dismisses legal challenge to EncroChat cryptophone evidence*. <https://www.computerweekly.com/news/366551078/French-supreme-court-dismisses-legal-challenge-to-EncroChat-cryptophone-evidence>, 27. mart 2024.

52 <https://www.spixnet.com/cybersecurity-blog/2023/03/09/french-supreme-court-rejects-encrochat-verdict-after-lawyers-question-secrecy-over-hacking-operation>, 27. mart 2024.

53 Presuda Kasacionog suda Francuske (*Cour de Cassation*) od 10. maja 2023. ECLI:FR:CCASS:2023:CR00538. <https://www.legifrance.gouv.fr/juri/id/JURITEXT000047545770>, 27. mart 2024.

su članice EU, pa se na osnovu toga pošlo od pretpostavke da je nadzor te vrste komunikacija ostvarenih van Italije sproveden na zakonit način.⁵⁴ Suštinski se ovde radilo o poznatom principu „međudržavnog poverenja“.

Konačno, tim pitanjem se bavio i Ustavni sud Italije,⁵⁵ koji je zaključio da informacije sadržane u tajnoj komunikaciji realizovanoj putem aplikacije *Sky ECC* ne predstavljaju prislušivanje, koje se svodi na posebnu istražnu/dokaznu radnju, i da se u svakom konkretnom slučaju kao osnovno sporno pitanje postavlja ocena da li komunikacija prestaje da bude komunikacija i zatim postaje dokument/isprava onda kada je pohranjena u računaru.

Zatim je nakon svog prvog stava, koji se ticao informacija sadržanih u tajnoj komunikaciji realizovanoj putem aplikacije *Sky ECC*, italijanski Vrhovni kasacioni sud taj zauzeti stav u nekoliko svojih odluka dodatno nadgrađivao, posebno u kontekstu pitanja koja su se ticala evropskog istražnog naloga, što je u EU postalo naročito aktuelno nakon obraćanja berlinskog Regionalnog suda Evropskom sudu pravde. To je činjeno i uz „izvesna „lutanja“. Tako se u odluci italijanskog Vrhovnog kasacionog suda od 26. oktobra 2023. godine, broj 44154/2023,⁵⁶ konstatuje da u sistemu evropskog istražnog naloga za prihvatanje rezultata presretanja komunikacija koje su već sprovedene u inostranstvu nije dovoljno da su takvi dokazi autorizovani odlukom suda države članice EU, na osnovu zakonskih propisa te države, već je neophodno proveriti i da li su ti dokazi (presretanje) kao takvi prihvatljivi prema pravilima italijanskog prava. Vrhovni kasacioni sud Italije konstatuje i da Direktiva EU koja se tiče evropskog istražnog naloga uopšte ne reguliše upotrebljivost dokaza pribavljenih tim nalogom, prepuštajući taj aspekt pravu konkretne države, bez prejudiciranja koje bi se ticalo ocene poštovanja prava na odbranu i garancija fer postupka prilikom evaluacije dokaza pribavljenih evropskim istražnim nalogom. Takođe se konstatuje da kada bi se utvrdilo da su istražne aktivnosti sprovedene u inostranstvu bile nezakonite jer su sprovedene bez neophodne sudske odluke, to bi se reflektovalo i na nacionalni postupak i dovelo do nemogućnosti korišćenja takvih dokaza.

Italijanski Vrhovni kasacioni sud se posebno bavio evropskim istražnim nalogom u kontekstu njegove upotrebe radi pribavljanja dokaza, pa tako posebno objašnjava da on mora biti „nužan“ i „proporcionalan“ svrsi krivičnog postupka, uz uzimanje u obzir prava lica za koje se vodi istraga ili koje je optuženo. Posebno se ističe da radnje koje se tiču nadzora nad telefonskom komunikacijom ili drugim vidovima daljinske razmene informacije moraju biti precizirane jer spadaju u aktivnosti koje limitiraju pravo na privatnost, garantovano Evropskom konvencijom o ljudskim pravima, te stoga moraju biti sprovedene na način koji obezbeđuje adekvatnu

54 Više o tome: B. Goodwin, *Italian Supreme Court calls for prosecutors to disclose information on Sky ECC hacking operation*. <https://www.computerweekly.com/news/252525734/Italian-Supreme-Court-calls-for-prosecutors-to-disclose-information-on-Sky-ECC-hacking-operation>, 28. mart 2024.

55 <https://www.devita.law/sky-ecc-chat-acquisition-the-order-of-referral-to-the-united-sections/?lang=en>, 28. mart 2024.

56 <https://canestrinilex.com/en/readings/legality-check-of-skyecc-evidence-is-mandatory-ita-supreme-court-4415423>, 29. mart 2024.

sudsku kontrolu, dok pristup dokumentima i podacima sadržanim u kompjuterima ili drugi oblici komunikacija moraju uvek da budu sudski autorizovani.

Veoma je interesantna i odluka italijanskog Vrhovnog kasacionog suda broj 47798, od 30. novembra 2023. godine, u kojoj se prvo konstatuje da informacije sa „Sky ECC platforme“ potiču iz zajedničke operacije francuske, belgijske i holandske policije, što je dovelo do pristupa i dekrpcije komunikacije/„četo vanja“ više od 70.000 korisnika iz različitih zemalja, samo 2021. godine, da bi se potom, uz oslanjanje i na pomenutu odluku Ustavnog suda Italije (*Constitutional Court's ruling 170/2023*),⁵⁷ posebno naglasilo da sud primećuje da pravila italijanskog Zakona o krivičnom postupku omogućavaju korišćenje dokumenata i podataka pohranjenih u kompjuterima, uz pravljenje razlike između njih i prisluškivanja.⁵⁸

Potom se konstatuje da je, zahvaljujući toj razlici između podataka koji su „u progresu“, što znači prisluškivanja/nadzora u realnom vremenu komunikacije koja je u toku i podataka koji su „kristalizovani“ u memoriji uređaja/kompjutera, bilo moguće da se koristi evropski istražni nalog, koji je inicirao tužilac. Konstatuje se i da u odnosu na takve dokaze nije potrebna autorizacija italijanskog suda/sudije, ako su oni pribavljeni u skladu sa pravilima sudskog postupka strane države, iz čega proizlazi da se sudska zaštita ostvaruje samo u stranom pravnom sistemu. Dalje se u toj odluci Vrhovnog kasacionog suda Italije neposredno odstupa od dela rezonovanja u njegovoj prethodnoj odluci (No. 44154, 2. novembar 2023), tako što se konstatuje ne samo da je dovoljna sudska autorizacija u stranoj državi prema pravilima njenog prava već i da onda kada se primenjuje evropski istražni nalog radi dobijanja dokaza koji se tiču komunikacije već pohranjene u računarima, nema mesta ni primeni pravila Zakona o krivičnom postupku koja se odnose na prisluškivanje/presretanje aktuelnih (živih) razgovora, već se primenjuju pravila o pribavljanju dokumenata/isprava.

Konačno, italijanski Vrhovni kasacioni sud, tj. zajednička sednica njegovih odeljenja, zauzeo je potom, početkom 2024. godine, nakon izvesnog „lutanja“, kolebanja i nesigurnosti po tom pitanju, načelni stav da u Italiji dokazi iz komuniciranja korišćenjem posebnih aplikacija, kao što su *Sky ECC* i *EnchroChat*, mogu da budu dokaz (*Court of Cassation in Italy rules: Sky ECC communications are legal evidence*), pod određenim i inače postojećim zakonskim uslovima.⁵⁹

5.4. Crna Gora

U Crnoj Gori se aktuelno vodi više krivičnih postupaka u kojima se, između ostalog, pojavljuju i informacije/dokazi proistekli iz (de)šifrovane komunikacije, ostvarene korišćenjem posebnih aplikacija za zaštićenu/tajnu komunikaciju.⁶⁰ Radi

57 <https://www.sistemapenale.it/it/documenti/corte-costituzionale-2023-170-conflitto-attribuzione-senato-procura-firenze-caso-renzi>, 28. mart 2024.

58 <https://www.devita.law/sky-ecc-chat-acquisition-the-order-of-referral-to-the-united-sections/?lang=en>, 29. mart 2024.

59 <https://sot.com.al/english/aktualitet/gjykata-e-kasacionit-ne-itali-vendos-komunikimet-ne-sky-ecc-jane-prov-i647568>, 1. april 2024.

60 Više o tome: Grupa autora (2023). *Izdvajanje nezakonito pribavljenih dokaza u krivičnom postupku – principi iz prakse Evropskog suda za ljudska prava i sudska praksa u Crnoj Gori*, ur. T. Gorjanc Prelević, Podgorica, p. 34–35.

se pre svega o aplikaciji *Sky ECC*, odnosno kriptovanoj komunikaciji ostvarenoj mobilnim telefonima modifikovanim da rade u režimu aplikacije *Sky ECC*. Još uvek nema pravnosnažnih presuda zasnovanih na toj vrsti dokaza,⁶¹ a u aktuelnim krivičnim postupcima se uglavnom prihvataju osnovne teze nadležnih državnih tužilaca da su to dokazi pribavljeni mehanizmom međunarodne krivičnopravne pomoći te da je u tom pogledu ključno da je konkretna procesna/dokazna radnja koju je preduzeo strani pravosudni organ sprovedena u skladu sa zakonom konkretne države kojoj pripada taj pravosudni organ.

Dokazne zabrane su, prema pravilima krivičnog procesnog prava Crne Gore, uređene na sličan način, kao što je to i inače tipično za evropskokontinentalno krivično procesno zakonodavstvo, tako što se zabranjuju i korišćenje određenih dokaza i dokaznih sredstava, kao i vrednovanje određenih dokaza.⁶² Osim toga, potrebno je i da takva procesna/dokazna radnja nije alternativno realizovana: 1) suprotno načelima pravnog sistema Crne Gore ili 2) opšteprihvaćenim pravilima međunarodnog prava.⁶³ U međuvremenu, u Crnoj Gori postoji i prvostepena presuda utemeljena, između ostalog, i na dokazima pribavljenim putem međunarodne pravne pomoći u krivičnim stvarima, gde se prema prethodno objašnjenim kriterijumima ocenjuje da li je reč o dokazu u vidu *isprave*, koji se suštinski svodi na informacije potekle iz šifrovane/kriptovane komunikacije u odnosu na koju je ostvaren nadzor nadležnih organa stranih država.

Suština je da, kao i inače kada se radi o pružanju/dobijanju međunarodne pravne pomoći u krivičnim stvarima, nije neophodno da je konkretna procesna/dokazna radnja sprovedena u drugoj zemlji u skladu sa propisima države koja zahteva/dobija međunarodnu krivičnopravnu pomoć već je sasvim dovoljno da je postupljeno prema relevantnim propisima države u kojoj je konkretna radnja preduzeta. Takvi stavovi nadležnih državnih tužilaca u konkretnim krivičnim postupcima u Crnoj Gori prihvatani su od sudova u različitim oblicima njihove funkcionalne nadležnosti. Tako su rezonovali i sudije za istragu, pre svega prilikom određivanja pritvora, kao i sud u postupku kontrole optužnice, a konačno, to je prihvatilo i jedno prvostepeno veće nadležnog suda, odnosno kao što se to objašnjava u fusnoti 60, u međuvremenu već postoji i jedna pravnosnažna presuda, koja je između ostalog utemeljena i na dokazima iz *Sky ECC* komunikacije.

Konačno, nedavno je i Ustavni sud Crne Gore (odluka U-III br. 745/23 i 746/23) odlučivao o ustavnoj žalbi koja se ticala ustavnopravne opravdanosti određivanja pritvora u jednom konkretnom slučaju, gde se, između ostalog, osporavalo

61 Doduše, kao što je to istaknuto u izlaganju specijalnog tužioca Specijalnog tužilaštva Crne Gore, na Konferenciji *Korišćenje kriptovane komunikacije u krivičnom postupku*, održanoj 18. i 19. aprila 2024. godine u Beogradu, u organizaciji Delegacije EU u Srbiji, Kancelarije Saveta Evrope u Beogradu, Ambasade SAD u Beogradu, kao i Misije OEBS-a u Beogradu, u Crnoj Gori je u međuvremenu, tj. nedavno i jedna presuda zasnovana, između ostalog, na dokazima iz *Sky ECC* komunikacije, postala pravnosnažna. Interesantno je da se, kada je reč o toj presudi, radi o dokazima „oslobađajućeg karaktera“, koji su potkrepili tvrdnju konkretnog okrivljenog da je izložen torturi, odnosno zahvaljujući mučenju (što je tek naknadno dokumentovano/dokazano podacima iz kriptovane komunikacije), prethodno priznao krivično delo koje nije zaista izvršio.

62 M. Škulić (2012). *Krivično procesno pravo*, Podgorica, p. 205.

63 M. Škulić (2009). *Komentar Zakonika o krivičnom postupku Crne Gore*, Podgorica, p. 113.

i postojanje osnovane sumnje kao materijalnog i obaveznog uslova za određivanje pritvora okrivljenog u krivičnom postupku, koja je, između ostalog, u konkretnom slučaju bila utemeljena i na podacima pribavljenim iz dešifrovane tajne komunikacije ostvarene korišćenjem aplikacije *Sky ECC*.

Vodeći postupak po više ustavnih žalbi radi vođenja jedinstvenog postupka i donošenja jedne odluke, s obzirom na to da je ustavnim žalbama osporeno isto rešenje Vrhovnog suda Crne Gore (Kr-S br. 12/23 od 10. jula 2023. godine), a pozivajući se i na stav Evropskog suda za ljudska prava,⁶⁴ Ustavni sud Crne Gore je zaključio da „u smislu standarda koji proizlaze iz prakse Evropskog suda za ljudska prava koju slijedi Ustavni sud u okolnostima konkretnog slučaja u osporavanim rješenjima nije izostala analiza činjenica vezanih za utvrđivanje osnovanosti sumnje i stepenu potrebnom za produženje pritvora“. Osim toga, Ustavni sud Crne Gore je u konkretnom slučaju „imao u vidu i činjenicu da se radi o pritvoru koji je produžen u početnom stadijumu postupka, odnosno u svrhu vođenja istrage u kojoj se svestrano prikupljaju činjenice i dokazi od značaja za dalji tok i ishod krivičnog postupka i kada se pokazuje potreba da se otklone rizici mogućeg neprisustvovanja podnosioca ovoj fazi postupka. Ustavni sud ukazuje da se u predmetima produžavanja pritvora u istrazi ne razmatra niti odlučuje o krivici okrivljenog. Stoga se ne može ulaziti ni u pojedina činjenična pitanja niti ocjenu dokaza. O postojanju osnovane sumnje kod primjene mjere određivanja pritvora zaključuje se iz sadržaja relevantnih dokaza koje Ustavni sud nije ovlašćen cijeliti u ovoj fazi postupka“.

5.5. Nemačka i aktiviranje Suda pravde Evropske unije

Nemački sudovi su u više slučajeva i praktično bez previše oklevanja prihvatili kao dokaze informacije proizišle iz nadzora ostvarenih korišćenjem aplikacije *EncroChat*. Prvi izuzetak je nastao odlukom Regionalnog/zemaljskog suda u Berlinu, koji je u julu 2021. godine u jednom konkretnom predmetu zaključio da se ne radi o prihvatljivim dokazima.⁶⁵ Svi drugi okružni i regionalni/zemaljski nemački sudovi su u više navrata prihvatili kao dokaze informacije proizišle iz nadzora ostvarenih korišćenjem aplikacije *EncroChat*. Prethodno je i nemački Savezni sud zauzeo stav da su takvi dokazi prihvatljivi u nemačkom krivičnom postupku.⁶⁶

Konačno, berlinski Regionalni/zemaljski sud (*Landgericht Berlin*) je, u skladu sa posebnim mehanizmom svojstvenom pravu EU, kojim nadležni državni organi zemalja EU mogu od Suda pravde EU tražiti tumačenje određenih spornih pravnih

64 Ustavni sud Crne Gore (odluka U-III br. 745/23 I 746/23), na temelju jednog veoma poznatog slučaja iz prakse Evropskog suda za ljudska prava (*Simons protiv Belgije*), koji je komentarisano u prethodnom tekstu, a svodi se na stav da pitanje zakonitosti i upotrebe dokaza nije nužno pitanje o kojem treba odlučiti kod odlučivanja o pritvoru, izveo je svoj stav prema kojem u konkretnoj fazi postupka on „nije ovlašćen“ da ocenjuje relevantne dokaze.

65 J. Diehl, R. Lehberger, C. Meyer-Heuer, *Landgericht Berlin lässt Encrochat-Daten nicht zu*. <https://www.spiegel.de/panorama/justiz/berlin-landgericht-laesst-encrochat-daten-nicht-zu-a-6dd9be2e-f558-40fa-9995-2f8136581f8e>, 14. septembar 2023.

66 Vid. Germany: Federal Court of Justice Confirms Use of Evidence in EncroChat Cases, EURO-CRIM 1/2022. 36–37. https://eucrim.eu/media/issue/pdf/eucrim_issue_2022-01.pdf#page=38, 1. april 2024.

pitanja koja se pojave u praksi, podneo zahtev za interpretativnim izjašnjanjem Suda pravde EU.⁶⁷ Odlukom Berlinskog regionalnog/zemaljskog suda,⁶⁸ niz pitanja je postavljen Sudu pravde EU, a ključna su bila sledeća: 1) pitanje *nadležnosti* – da li je nemačko tužilaštvo bilo nadležno za podnošenje zahteva za evropski istražni nalog, s obzirom na to da bi, shodno pravilima iz nemačkog Zakonika o krivičnom postupku, državno tužilaštvo moralo dobiti nalog/odluku nemačkog suda da prikupe takve podatke ako su poticali iz Nemačke, 2) pitanje *procesno relevantnog stepena sumnje* – da li bi u državi čiji su organi sprovodili konkretnu dokaznu radnju, morao postojati isti stepen sumnje⁶⁹ kao i u državi u kojoj se potom rezultati takve dokazne radnje koriste kao dokaz u krivičnom postupku, i 3) pitanje *zakonitosti* – da li evropski istražni nalog mora da izda *sudija* da bi se dobili dokazi ako pribavljanje dokaza u sličnom domaćem predmetu, prema pravilima u konkretnom slučaju nemačkog Zakonika o krivičnom postupku, treba da naredi sudija? U daljem tekstu će se posebno objasniti stav generalnog advokata Suda pravde EU u odnosu na ova i druga pitanja koja je postavio berlinski regionalni/zemaljski sud.

6. PRAKSA U SRBIJI U POGLEDU DOKAZA PROISTEKLIH IZ (DE)ŠIFROVANE KOMUNIKACIJE OSTVARENE KORIŠĆENJEM POSEBNIH APLIKACIJA/UREĐAJA

U Srbiji je praksa koja se tiče dokazne vrednosti/verodostojnosti (de)šifrovane komunikacije koja je ostvarena korišćenjem posebnih aplikacija i posebno prilagođenih mobilnih telefona još uvek relativno oskudna, ali se već naziru i neka osnovna dokazna pitanja o kojima će odluke donositi nadležni sudovi i neki početni trendovi u sudskoj praksi te vrste. Kada je reč o konkretnim aplikacijama/uređajima namenjenim/korišćenim za tajnu/šifrovanu komunikaciju, do sada se jedino radi o aplikaciji *Sky ECC*, koja je i inače u javnosti najpoznatija aplikacija te vrste, a u svetlu do sada zapaženih slučajeva širom sveta, smatra se da je poslednjih godina bila veoma široko primenjivana u „miljeu organizovanog kriminaliteta“.

Praksa u Srbiji u pogledu dokaza proisteklih iz (de)šifrovane komunikacije ostvarene korišćenjem posebnih aplikacija/uređaja za sada se isključivo tiče stavova Apelacionog suda u Beogradu, kao žalbene instance u odnosu na odluke prvostepenog suda u konkretnim situacijama, to jest u odnosu na konkretne odluke Višeg suda u Beogradu, Posebnog odeljenja za organizovani kriminal.

Dve su situacije uočene u dosadašnjoj praksi: 1) ukidanje prvostepene presude koja je, između ostalog, bila zasnovana i na dokazima iz „presretnute“ komunikacije

67 T. Wahl. *EnchroChat Turns into a Case for the CJEU*. <https://eucrim.eu/news/encrochat-turns-into-a-case-for-the-cjeu/>, 29. septembar 2023.

68 LG Berlin (525 KLs) 279 Js 30/22 (8/22) – Beschluss vom 19. Oktober 2022. <https://www.hrr-strafrecht.de/hrr/lg/22/279-js-30-22.php>, 29. septembar 2023.

69 U stvari, to pitanje implicira da bi stepen sumnje morao da bude „bar isti“, odnosno minimalno istovetan, a po logici stvari, to bi uvek bilo adekvatno/ispunjeno i kada se radi o višem stepenu sumnje, što bi se tada svodilo na varijantu poznatog pravnog pravila – „ko može više može i manje“, odnosno radilo bi se o slučaju da ukoliko se postupalo uz postojanje višeg stepena sumnje, onda takav stepen sumnje obuhvata i odgovarajući niži stepen sumnje.

Sky ECC, pri čemu Apelacioni sud u Beogradu, Posebno odeljenje, u tom slučaju nije zaključilo da se radi o pravno nevaljanim dokazima, odnosno dokazima koji su nezakoniti sami po sebi ili prema načinu pribavljanja, već je samo ustanovilo da je prvostepeni sud takve dokaze pogrešno identifikovao/pojmovno odredio u krivičnoprocesno-dokaznom smislu, odnosno da nije pravilno označio iz koje su dokazne radnje oni proizašli u konkretnom slučaju, te u koju vrstu dokaza spadaju u skladu sa opštim krivičnoprocesno-dokaznim pravilima, kao i 2) odbijanje žalbi protiv rešenja prvostepenog suda kojim je potvrđena optužnica, zasnovana između ostalog i na dokazima iz „presretnute“ komunikacije *Sky ECC*, kada je Apelacioni sud u Beogradu, Posebno odeljenje, zauzeo stav da su ti dokazi zakoniti i da predstavljaju ispravu u krivičnoprocesno-dokaznom smislu, do koje se došlo primenom mehanizama iz domena međunarodne pravne pomoći u krivičnim stvarima.

6.1. *Ukidanje prvostepene presude zbog pogrešnog označavanja vrste dokazne radnje iz koje je proistekao konkretan dokaz/zbog pogrešnog definisanja vrste dokaza – kada su ti podaci iz komunikacije Sky ECC*

Apelacioni sud u Beogradu, žalbeno veće Posebnog odeljenja za organizovani kriminalitet, ukinuo je svojim rešenjem prvostepenu presudu Višeg suda u Beogradu, Posebnog odeljenja za organizovani kriminal i vratio postupak na ponovno suđenje.⁷⁰ Presudom Apelacionog suda u Beogradu, žalbenog veća Posebnog odeljenja za organizovani kriminal, nije sam po sebi negiran dokazni značaj informacija pribavljenih iz komunikacije *Sky ECC*, do kojih se došlo mehanizmom međunarodnopravne pomoći u krivičnim stvarima, ali je osporen način rezonovanja prvostepenog suda, i to u dva osnovna pravca: s jedne strane, od prvostepenog suda se zahteva da se detaljnije pozabavi pitanjem zakonitosti konkretnog dokaza, dok se, s druge strane, ističe da je prvostepeni sud tu vrstu dokaza pogrešno poistovetio sa jednom posebnom dokaznom radnjom iz srpskog Zakonika o krivičnom postupku. Osim toga, povezano sa drugim pravcem rezonovanja prvostepenog suda, koji je doveden u pitanje rešenjem Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal, osporeno je i podvođenje konkretnih dokaza, proizašlih iz dešifrovanja komunikacije ostvarene aplikacijom *Sky ECC*, pod vrstu *slučajnog nalaza* proisteklog iz sprovedene posebne dokazne radnje.

U vezi sa pitanjem zakonitosti dokaza proizašlih iz „dešifrovanja“ komunikacije putem aplikacije *Sky*, Apelacioni sud u Beogradu praktično daje smernice kako pristupiti aplikaciji *Sky* da bi se prihvatila kao dokaz tako što zaključuje da nije dovoljno konstatovati da je takav konkretan dokaz pribavljen putem međunarodne pravne pomoći. U rešenju Apelacionog suda u Beogradu, Posebno odeljenje za organizovani kriminal, navodi se: „Prvostepeni sud je propustio da najpre navede jasne i argumentovane razloge u pogledu zakonitosti dostavljene predmetne Skaj komunikacije po kriterijumima države u kojoj je pribavljena i to kroz analizu načina na koji je ona pribavljena u Republici Francuskoj, a u sklopu navedenog i kroz ocenu da li

⁷⁰ Rešenje Posebnog odeljenja za organizovani kriminal Apelacionog suda u Beogradu Kž1 Po1 23/22 od 7. aprila 2023. Vid. sajt Apelacionog suda u Beogradu: <http://cdn-host.bgdream.net/lt/archive/ok-donete-odluke/2023/7>, 1. septembar 2023.

je navedena komunikacija pribavljena na način koji nije u suprotnosti sa načelima našeg pravnog sistema i opšteprihvaćenim pravilima međunarodnog prava.“ Ovdje svakako treba imati u vidu da, kao što je to već objašnjeno u prethodnom tekstu, francusko pravo omogućava da se takva vrsta dokaza koristi u krivičnom postupku, isto kao što je i sam način „razbijanja“ zaštićene komunikacije putem posebne vrste „hakovanja“ od istražnih organa preduzet u skladu sa pravilima francuskog prava.

Inače, nije sasvim jasno na koja „načela našeg pravnog sistema“ misli Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, u svom rešenju (navedenom u prethodnom tekstu), jer to nije konkretno objašnjeno, a ni pitanje zakonitosti dokaza se ne rešava nekim posebnim načelima već je uređeno relevantnim odredbama Zakonika o krivičnom postupku, a u sklopu opštih dokaznih načela, poput načela slobodne ocene dokaza, te pravila o pravnoj nevaljanosti određene vrste dokaza, bilo samih po sebi, bilo zbog načina na koji su pribavljeni, što je i objašnjeno u prethodnom tekstu. Takođe je prilično nejasan zahtev da se oceni da li je komunikacija pribavljena na način koji nije u suprotnosti sa opšteprihvaćenim pravilima međunarodnog prava. Naime, nije jasno o kojim bi se ovde „opšteprihvaćenim pravilima međunarodnog prava“ radilo, a pojam „opšteprihvaćena pravila međunarodnog prava“ je sam po sebi često i prilično fluidan, te potencijalno podložan i veoma elastičnim/kaučuk tumačenjima. Bilo bi inače sasvim dovoljno da se Apelacioni sud zadržao na zahtevu da se mora raditi o zakonitim dokazima, to jest informacijama koje mogu da posluže kao dokaz ukoliko su pribavljene na zakonit način,⁷¹ pri čemu je uobičajeno da se zakonitost dokaza proisteklih iz međunarodne pravne pomoći ocenjuje sa stanovišta zakonskih/ustavnih pravila same države čiji su nadležni organi pribavili takve informacije/dokaze, odnosno koji su izveli konkretne dokazne radnje.

U rešenju Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal, posebno se konstatuje da je prvostepeno pretresno veće bilo dužno „da analizira činjenice da iz dokaza i podataka u spisima predmeta proizilazi“, da je „vođena zajednička istraga holandskih, belgijskih i francuskih nadležnih organa i da je kriptovano rešenje za telefone sa aplikacijom *Sky ECC* bilo korišćeno od strane kriminalnih organizacija koje su delovale u navedene tri države, a neke i na međunarodnom nivou“. Zatim se objašnjava i da su pretresanje i zaplena podataka sadržanih u bazi podataka sa server platforme *Sky ECC* preduzeti na osnovu odluke nadležnog pravosudnog organa Republike Francuske o dozvoli postavljanja tehničkih uređaja za hvatanje informatičkih podataka na eksternoj vezi servera, koja je doneta 21. decembra 2020. godine, u skladu sa krivičnoprocesnim propisima Republike Francuske, kako bi se hvatali kriptografski elementi svakog telefona koji koristi sistem šifrovanja, koji, kada se kombinuje sa kriptografskim elementima dobijenim iz presretanja, omogućava dešifrovanje individualnih poruka koje primaju ti telefoni.

71 Naime, i inače se u rešenju Apelacionog suda navodi da je prvostepeni sud prilikom ocene da li se dokazi „sa Skaja“ mogu koristiti kao dokaz „trebalo najpre da ima u vidu da su isti pribavljeni u skladu sa važećim propisima Francuske i na osnovu odluke pravosudnog organa te zemlje“, što se potom nepotrebno povezuje sa pitanjem ocenjivanja da li je način pribavljanja potencijalno bio suprotan opšteprihvaćenim pravilima međunarodnog prava.

Kada je reč o karakteru izvora dokaza i vrsti dokazne radnje u konkretnom slučaju, Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, zaključuje da je prvostepeni sud dokaze proistekle iz aplikacije Skaj pogrešno podveo pod posebnu radnju računarska pretraga podataka, što pritom nije dobro ni obrazložio, odnosno u pogledu čega daje nejasne razloge. To se objašnjava time što su, imajući u vidu da je predmet zamolnice bilo dostavljanje dokaza i dokaznog materijala, a ne preduzimanje određene dokazne radnje, „nejasni navodi prvostepenog suda da dokazi pribavljeni od strane nadležnog organa Republike Francuske sadržinski odgovaraju dokaznoj radnji i dokazima koji su pribavljeni saglasno odredbama Zakonika o krivičnom postupku Srbije“, koje se odnose na posebnu dokaznu radnju računarskog pretraživanja podataka. Tako je i s obzirom na to da računarsko pretraživanje podataka podrazumeva pretraživanje već obrađenih i ličnih podataka i potom njihovo poređenje sa podacima koji se već nalaze u bazama podataka koji se odnose na osumnjičenog i krivično delo i, shodno tome i po logici stvari, ta se posebna dokazna radnja „vrši na serverima koji se nalaze na našoj teritoriji, dok se u konkretnom slučaju radi o kriptovanoj komunikacionoj platformi sa serverima u inostranstvu“.⁷²

Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, utvrđuje u svom rešenju i da su nejasni navodi prvostepenog suda da se dokazi pribavljeni od nadležnih organa Republike Francuske koji su pribavljeni u predmetu Posebnog odeljenja Višeg suda u Beogradu koji se vodi protiv jednog drugog okrivljenog i drugih okrivljenih u drugom krivičnom postupku, kao slučajni nalaz, mogu koristiti i u konkretnom krivičnom postupku, iz kojeg je proizišla prvostepena presuda o kojoj se odlučivalo u žalbenom postupku. Čini se da nije bilo neophodno da se prvostepeni sud na takav način uopšte i upušta u problem slučajnog nalaza, o kojem svakako nije reč u konkretnom slučaju.

6.2. Rešenja o odbijanju žalbi protiv rešenja prvostepenog suda o potvrđivanju optužnice utemeljene, između ostalog, i na dokazima iz komunikacije Sky ECC

Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, doneo je do sada dva rešenja o odbijanju žalbi protiv rešenja prvostepenog suda o potvrđivanju optužnice utemeljene između ostalog i na dokazima iz komunikacije Sky ECC, odnosno informacijama/dokazima proisteklim iz „presretute“ kriptovane komunikacije ostvarene posebnom aplikacijom za zaštitu komunikacije. Sadržina oba rešenja je veoma slična. Kada je reč o stavu da su optužnice, između ostalog, zasnovane i na dokazima iz komunikacije ostvarene putem aplikacije Sky ECC, suština je da Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, utvrđuje kako vrstu dokaza i vrstu dokazne radnje, kao i formu procesno-dokaznog mehanizma iz kojeg su takvi dokazi proistekli, tako i konkretan načelni dokazni

⁷² Ove je od značaja i da Zakonik o krivičnom postupku Srbije posebno ne reguliše/definiše digitalne dokaze već ih u članu 2. stav 1. tačka 26. podvodi pod ispravu: „Računarski podatak koji je podoban ili određen da služi kao dokaz činjenica koje se utvrđuju u postupku predstavlja ispravu.“

kvalitet/kredibilitet takvih dokaza. Kada je u pitanju određivanje vrsta dokaza i definisanje vrste dokazne radnje/procesno-dokaznog mehanizma iz kojeg takav dokaz potiče, konstatuje se da je reč o dokazu koji, u skladu sa opštim krivičnoprocesnim pravilima, predstavlja ispravu pribavljenu primenom mehanizama međunarodne pravne pomoći u krivičnim stvarima, a kada se radi o načelnom kvalitetu/kredibilitetu konkretnih dokaza te vrste, utvrđuje se da se u konkretnim slučajevima radi o zakonitim dokazima, odnosno dokazima koji su pravno valjani.

U svom rešenju Kž2-Po1 214/23, od 1. decembra 2023. godine,⁷³ kojim je odbio žalbu prvostepenog suda o potvrđivanju optužnice, Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, zauzeo je stav da su zakoniti dokazi dobijeni putem međunarodnopravne pomoći, koji su pribavljeni od nadležnih organa Republike Francuske, čime je potvrđen stav prvostepenog suda (10 Kž2-Po1 214/23), koji je svojim rešenjem potvrdio optužnicu Tužilaštva za organizovani kriminal/Javnog tužilaštva za organizovani kriminal – Kto. br. 55/23 od 9. maja 2023. godine. Naime, tim rešenjem Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal, prihvaćen je kao pravilan stav prvostepenog suda da „dokazi pribavljeni putem međunarodne pravne pomoći u krivičnim stvarima, od nadležnih pravosudnih organa Republike Francuske, nisu nezakoniti dokazi, s obzirom da nisu pribavljeni protivno odredbi člana 16 ZKP“.

Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, tako je zaključio „uvidom u spise predmeta iz čega proizlazi da je u konkretnom slučaju Tužilaštvo za organizovani kriminal, zamolnicom MP br.66/22 od 10.06.2022. godine, od pravosudnih organa Republike Francuske, zatražilo pružanje međunarodne pravne pomoći u krivičnim stvarima, u vidu dostavljanja dokaza i dokaznog materijala – zadržanih podataka sa platforme SKY ECC koju su koristili osumnjičeni i potencijalni osumnjičeni, kao i oštećeni, u predistražnom postupku tužilaštva, a koji sadrže glasovne poruke, tekstualne poruke, video zapise i fotografije, potom podatke o lokaciji (GPS ili druge koordinate, naziv lokacije, bazne stanice i dr.) mobilne terminalne opreme, odnosno mobilnih telefona, na kojoj su se nalazili prilikom korišćenja navedene platforme, IMEI brojeve mobilnih telefona koje su koristili navedene SKY ECC PIN, SKY ECC NICKNAME, za koje su dati parametri kao i naredbe nadležnog pravosudnog organa Republike Francuske, na osnovu koje je izvršen pretres i zaplena podataka sadržanih u bazi podataka sa servera platforme SKY ECC na teritoriji Evrope“.

Prema stavu Apelacionog suda u Beogradu, Posebno odeljenje za organizovani kriminal, „predmetni dokazi i dokazni materijal – podaci sa platforme *Sky ECC* pribavljeni su na osnovu dokaznih radnji inostranog organa pri čemu se u ovom slučaju primenjuje opšti princip poverenja u pravni sistem druge države kao opšteprihvaćeno pravilo međunarodnog prava. Apelacioni sud u Beogradu, Posebno odeljenje, posebno ističe da je odredbom člana 3. stav 1. Evropske konvencije o međusobnom

73 Rešenje Apelacionog suda u Beogradu, Posebno odeljenje za organizovani kriminal – Kž2-Po1 214/23, od 1. decembra 2023. godine, pribavljeno je na osnovu zahteva podnetog u skladu sa Zakonom o slobodnom pristupu informacijama od javnog značaja – dopis Apelacionog suda u Beogradu – Cy II 17a 38/24 od 8. aprila 2024.

pružanju pravne pomoći u krivičnim stvarima, koja je potvrđena od Savezne Republike Jugoslavije,⁷⁴ propisano da će zamoljena strana, u skladu sa načelima koje predviđa njeno zakonodavstvo, izvršavati zamolnice koje se odnose na krivične predmete koje budu uputili sudski organi strane molilje, a koje se odnose na obavljanje istražnih radnji ili dostavljanje dokaznog materijala, dosijea ili dokumenata“.

Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, u pogledu odredbe člana 16. ZKP, kojom je propisano da se sudske odluke ne mogu zasnivati na dokazima koji su, neposredno ili posredno, sami po sebi ili prema načinu pribavljanja, u suprotnosti sa nekim od sledećih opciono definisanih izvora prava; a) Ustavom, b) samim Zakonikom o krivičnom postupku, c) drugim zakonom ili d) opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima, nalazi da je pravilan stav prvostepenog suda (predmet 10 Kž2-Po1 214/23) da „predmetni dokazi“, što znači oni koji potiču iz *Sky ECC*, pribavljeni putem međunarodne pravne pomoći u krivičnim stvarima, nisu suprotni domaćim zakonima, ni potvrđenim međunarodnim ugovorima, ni opšteprihvaćenim pravilima međunarodnog prava. Konstatuje se u tom smislu da se prvostepeni sud pravilno poziva na princip poverenja u pravni sistem druge države, što u konkretnom slučaju znači – Republike Francuske. Iz toga proizlazi i zaključak Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal, da se „može pretpostaviti da su dokazi u Republici Francuskoj pribavljeni zakonito, u skladu sa unutrašnjom regulativom, pri čemu je postojala naredba nadležnog pravosudnog organa, na osnovu koje su predmetni dokazi pribavljeni, a potom, na osnovu zamolnice upućene pravosudnim organima Republike Francuske, u postupku pružanja međunarodne pravne pomoći, pribavljeni od strane Tužilaštva za organizovani kriminal“.

Na temelju svega prethodno navedenog, Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, zaključuje da je pravilan zaključak prvostepenog suda da, u konkretnom slučaju, dokazi proistekli iz komunikacije *Sky ECC* nisu nezakoniti dokazi, pa da stoga nema mesta ni njihovom izdvajanju. Osim toga, Apelacioni sud u Beogradu, Posebno odeljenje, ističe da je prvostepeni sud pravilno imao u vidu i da naše pravo ne reguliše posebno digitalne dokaze, već ih podvodi pod ispravu, propisujući odredbom člana 2. stav 1. tačka 26. ZKP da je „isprava“ svaki predmet ili računarski podatak koji je podoban ili određen da služi kao dokaz činjenice koja se utvrđuje u postupku (član 83. stav 1. i 2).

Po sadržini i suštinskoj argumentaciji, prethodnom rešenju Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal, veoma je slično i njegovo rešenje Kž2-Po1 5/24, od 5. januara, 2024. godine, kojim se odbijaju kao neosnovane žalbe protiv protiv rešenja prvostepenog suda o potvrđivanju optužnice (K-Po1 br. 173/23 – Kv-Po1 br. 711/23 od 17. novembra 2023. godine).⁷⁵

Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, u svom rešenju Kž2-Po1 5/24, od 5. januara 2024. godine, konstatuje da je Veće pr-

74 *Sl. list SRJ – Međunarodni ugovori*, 10/2001.

75 Rešenje Apelacionog suda u Beogradu, Posebno odeljenje za organizovani kriminal – Kž2-Po1 5/24, od 5. januara 2024. godine, pribavljeno je na osnovu zahteva podnetog u skladu sa odredbama Zakona o slobodnom pristupu informacijama od javnog značaja – dopis Apelacionog suda u Beogradu – Cy II 17a 40/24 od 10. aprila 2024. godine.

vostepenog suda, ispitujući konkretnu optužnicu Javnog tužilaštva za organizovani kriminal Kto br. 81/23 od 11. oktobra 2023. godine, nakon razmatranja spisa predmeta, zajedno sa odgovorima na optužnicu branilaca okrivljenih, stalo na stanovište da „skup činjenica navedenih u optužnici koje proizlaze iz dokaza prikupljenih u predistražnom i istražnom postupku, neposredno potkrepljuju osnovanu sumnju da su okrivljeni preduzeli radnje sadržane u dispozitivu optužnice opisane kao krivična dela koja im se stavljaju na teret i ujedno opravdavaju podizanje optužbe u konkretnoj krivičnopravnoj stvari“.

Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, u rešenju Kž2-Po1 5/24 od 5. januara 2024. godine, utvrđuje da je prvostepeni sud izveo zaključak o postojanju opravdane sumnje kao materijalnog uslova za optuženje u konkretnom slučaju u odnosu na svaki od bitnih elemenata krivičnih dela i okrivljenih ponaosob, a na bazi svih dokaza pribavljenih u toku predistražnog i istražnog postupka. Tu se posebno ističu tri vrste dokaza: 1) pisana dokumentacija, 2) isprave dobijene putem međunarodne pravne pomoći u krivičnim stvarima od nadležnih pravosudnih organa Republike Francuske, iz kojih proizlazi sadržina komunikacija putem aplikacije *Sky ECC* u spornom periodu, i 3) iskazi pojedinih ispitanih svedoka. Dakle, iz toga proizlazi da se podaci proistekli iz komunikacije ostvarene korišćenjem aplikacije *Sky ECC* smatraju ispravom, kao posebnom vrstom dokaza opšteg karaktera, do kojeg se došlo primenom mehanizma međunarodne pravne pomoći u krivičnim stvarima.

Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, u rešenju Kž2-Po1 5/24 od 5. januara 2024. godine konstatuje i da je prvostepeni sud, prilikom odlučivanja u postupku sudske kontrole optužnice, ocenio i navode iz odgovora na optužnicu branilaca okrivljenih kojima se ističe da predloženi dokazi, i to komunikacije ostvarene putem aplikacije *Sky ECC*, predstavljaju dokaze koji se moraju izdvojiti, a što branioci ističu i u svojim žalbama, nalazeći da ni ti navodi branilaca nisu od uticaja na drugačiju odluku suda, imajući u vidu da je dokazni materijal u spisima predmeta – podaci sa platforme *Sky ECC*, pribavljen na osnovu dokaznih radnji inostranih organa, dostavljen putem međunarodne pravne pomoći od nadležnih pravosudnih organa Republike Francuske, a povodom zamolnice Tužilaštva za organizovani kriminal MP br. 66/22 od 10. juna 2022. i MP br. 18/23 od 22. februara 2023. godine. Ovde se navodi i delovanje opšteg principa poverenja u pravni sistem druge države, kao opšteprihvaćeno pravilo međunarodnog prava, zbog čega je, i po oceni Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal, pravilan zaključak prvostepenog suda da nema mesta izdvajanju komunikacije – materijala sa aplikacije *Sky ECC* iz spisa.⁷⁶

U rešenju Kž2-Po1 5/24, od 5. januara 2024. godine, Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal, zaključuje se i da je s

76 I u tom rešenju Apelacionog suda u Beogradu, Posebnog odeljenja za organizovani kriminal (Kž2-Po1 5/24 od 5. januara 2024. godine), konstatuje se da naše pravo ne reguliše posebno digitalne dokaze, već ih podvodi pod isprave, saglasno odredbi člana 2. stav 1. tačka 26. ZKP, kojom je propisano da je „isprava“ svaki predmet ili računarski podatak koji je podoban ili određen da služi kao dokaz činjenice koja se utvrđuje u postupku (član 83. st. 1. i 2. ZKP), dok je članovima 138. i 139. ZKP uređeno dokazivanje ispravom kao opštom dokaznom radnjom.

obzirom na sve prethodno navedeno, veće prvostepenog suda izvelo pravilan zaključak da u konkretnom slučaju dokazi proistekli iz komunikacije ostvarene korišćenjem aplikacije *Sky ECC* sami po sebi ni prema načinu pribavljanja nisu u suprotnosti sa Ustavom, ni zakonima Republike Srbije, ni opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima, budući da su pribavljeni u postupku pružanja međunarodne pravne pomoći, na osnovu zamolnice nadležnog tužilaštva, od pravosudnih organa Republike Francuske, u kojoj su navedeni dokazi pribavljeni na osnovu naredbe nadležnog organa, pa je stoga pravilan zaključak prvostepenog suda da se ne radi o nezakonitim dokazima.⁷⁷ U svom rešenju Kž2-Po1 5/24, od 5. januara 2024. godine, Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, posebno ističe da konkretni „dokazi proistekli iz korišćenja SKY ECC aplikacije nisu dokazi do kojih se došlo preduzimanjem posebnih dokaznih radnji, među kojima je i tajni nadzor komunikacije, a koje inače, naše pravo poznaje“.

U svom rešenju Kž2-Po1 5/24, od 5. januara 2024. godine, Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, osvrće se i na sledeće navode branilaca okrivljenih: 1) da su dokazi pribavljeni putem aplikacije *Sky* nezakonito pribavljeni dokazi i da ih kao takve treba izdvojiti iz sudskih spisa, 2) da domaće zakonodavstvo o tom pitanju nema zauzet stav, 3) da bi se određeni podatak mogao koristiti kao dokaz, morao bi biti pribavljen na zakonom propisani način, kao i 4) da prepiska *Sky ECC* ne bi mogla da bude otkrivena primenom dokaznih radnji koje ZKP predviđa niti tehnologijama kojima raspolaže Republika Srbija.⁷⁸ Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, sve te navode ocenjuje kao neosnovane, ističući da je prvostepeni sud u tom pogledu dao jasne, detaljne i argumentovane razloge, koje je sud pravnog leka u postupku sudske kontrole optužnice u svemu kao pravilne prihvatio.

7. EVROPSKI SUD ZA LJUDSKA PRAVA

Evropski sud za ljudska prava nije se do sada neposredno bavio problematikom dokazne vrednosti/verodostojnosti/zakonitosti informacija/dokaza proizišlih iz (de)šifrovane tajne komunikacije tehničkim sredstvima/posebnim aplikacijama za kriptovanje, a pre svega u kontekstu razmatranja dejstva čl. 5 i 6 Evropske konvencije o ljudskim pravima i osnovnim slobodama. Međutim, postoje slučajevi koji su posredno povezani sa tim pitanjem, a tiču se prava na privatnost sadržanog u članu 8. EKLJP.

Osim toga, nedavno se ESLJP bavio i dokazima koji su se ticali aplikacije za kriptovanje komunikacije tehničkim sredstvima, ali se u tom slučaju nije upuštao

77 U svom rešenju (Kž2-Po1 5/24, od 5. januara 2024. godine) kojim kao neosnovane odbija žalbe protiv rešenja prvostepenog suda o potvrđivanju konkretne optužnice, Apelacioni sud u Beogradu, Posebno odeljenje za organizovani kriminal, ističe i da „veće prvostepenog suda prilikom odlučivanja u konkretnoj krivičnopravnoj stvari nije prejudiciralo odluku sudećeg veća, jer je samo ono ovlašćeno da vrši ocenu dokaza izvedenih na glavnom pretresu, naročito protivrečnih dokaza i da na bazi te ocene donese odluku u pogledu krivice okrivljenih u pogledu krivičnih dela koja su predmet optužbe“.

78 Uporedi: V. Bajović, p. 160.

u načelno vrednovanje takve vrste dokaza već se ograničio na načelno razmatranje vrednosti određenog dokaza kao potencijalno „ekskluzivnog“ dokaza protiv konkretnog okrivljenog u konkretnoj situaciji.

Naravno, i kada se i inače radi o stavovima Evropskog suda za ljudska prava (ESLJP), kao i kada se radi o aktuelnom pitanju dokaza proizišlih iz (de)šifrovane/kriptovane komunikacije tehničkim sredstvima, treba svakako imati u vidu da taj sud nije kasacioni sud. Naime, odredbe EKLJP koje se odnose na krivičnoprocesne garancije doživljavaju svoju primenu i u postupcima pred ESLJP u Strazburu, a pošto su njegove odluke obavezujuće za države članice Saveta Evrope, one imaju svoje indirektno ili direktno reperkusije i za nacionalna pravosuđa. Taj sud može utvrditi da je povređeno određeno pravo sadržano u EKLJP, a sam postupak pred njim se može započeti na dva načina – odgovarajućim zahtevom (žalbom) države ili individualnom žalbom, ali Evropski sud za ljudska prava nudi samo supsidijarnu osnovnu pravnu zaštitu, jer on nije nekakva „superrevizionarna/nadrevizionarna instanca“, a individualna žalba, koja ne mora biti u posebnoj formi, tom sudu se može podneti tek nakon što se iscrpe sva odgovarajuća pravna sredstva na nacionalnom nivou.⁷⁹

Nezavisno od vrste postupka (da li je pokrenut od države ili pojedinca), odluke ESLJP imaju samo „inter partes“ dejstvo, pa tako država članica (stranka) EKLJP može odlukom ESLJP biti obavezana da sanira povredu prava, nadoknadi štetu te spreči istovetne povrede u budućnosti, a ESLJP može takođe, prema članu 41. EKLJP, i samostalno da dosudi pravično obeštećenje ako se nacionalnim pravom omogućava samo nepotpuno saniranje povrede.⁸⁰ Osim toga, odluke ESLJP nemaju automatsko kasaciono dejstvo u odnosu na neku krivičnu presudu, koja je već postala pravnosnažna, tako da radi omogućavanja dejstva odluka tog suda države članice moraju da propišu posebne procesne mehanizme, kao što je utvrđivanje posebnog razloga za ponavljanje krivičnog postupka radi otklanjanja povrede na koju svojom odlukom ukazuje ESLJP, odnosno ustanovljavanje drugih vrsta (vanrednih) pravnih lekova, čijom se primenom na nacionalnom nivou omogućava oživotvorenje odluke tog suda.

7.1. ESLJP i pravo na privatnost u vezi sa nadzorom kriptovane komunikacije

Dvojica državljana Ujedinjenog Kraljevstva se u svojoj zemlji krivično gone na osnovu dokaza koje su sa aplikacije *EncroChat* pribavili nadležni francuski organi (*A. L. protiv Francuske*, pred. br. 44715/20, i *E. J. protiv Francuske*, pred. br. 47930/21).

Predstavke su podneli protiv Francuske, tvrdeći da im je preuzimanjem komunikacije povređeno pravo na privatnost iz člana 8. Konvencije i da im u Francuskoj u vezi sa tom navodnom povredom prava nije bilo na raspolaganju delotvorno pravno sredstvo. Dakle, te predstavke nisu prevashodno podnete zbog korišćenja

79 H. Satzger (2018). *Internationales und Europäisches Strafrecht – Strafanwendungsrecht, Europäisches Straf- und Strafverfahrensrecht, Völkerstrafrecht*, 8. Auflage, Baden, Baden, p. 143.

80 H. Satzger, *ibidem*.

tako pribavljenih dokaza u krivičnom postupku protiv njih već se one tiču primarno povrede prava na privatnost, a u vezi sa tom potencijalnom povredom, i povrede prava na delotvorno pravno sredstvo (član 13. Konvencije), uz isticanje i povrede prava na pravično suđenje u Ujedinjenom Kraljevstvu, mada bi inače povreda tog prava iz člana 6. Konvencije svakako mogla nastati ukoliko bi se ocenilo da se radi o nezakonitim dokazima.

Kao što je i objašnjeno u prethodnom tekstu, ESLJP se nije do sada direktno bavio pitanjem zakonitosti informacija/dokaza proizišlih iz (de)šifrovane tajne komunikacije ostvarene korišćenjem posebnih aplikacija, a pomenuti slučajevi, koji se primarno tiču potencijalne povrede prava na privatnost, mogu u osnovi samo indirektno da budu od značaja za to svakako centralno pitanje.

7.2. Nedavni slučaj pred ESLJP koji se ticao jednog krivičnog postupka u Turskoj

U svojoj odluci *Yüksel Yalçınkaya v. Türkiye*,⁸¹ ESLJP je utvrdio povredu prava na pravično suđenje (član 6. Konvencije) konkretnog okrivljenog, protiv kojeg je kao dokaz korišćena ekskluzivno činjenica da je koristio/imao instaliranu određenu aplikaciju namenjenu tajnom/zaštićenom komuniciranju. To je bila aplikacija *ByLock*,⁸² koju je imao/koristio konkretni okrivljeni, kojem je na teret stavljeno, a za šta je potom i pravnosnažno osuđen, članstvo u jednoj organizaciji koju turske vlasti smatraju terorističkom i za koju se u Turskoj ističe da je „stajala iza“ propalog pokušaja državnog udara. U Turskoj se samo članstvo u organizacijama te vrste (terorističkim) tretira kao posebno krivično delo. Inače, formalno nije jedini dokaz bio samo posedovanje aplikacije *ByLock* u konkretnom slučaju (iako je to bio osnovni/glavni dokaz), već je „potkrepljujućim dokazom“ uz to, korišćena i činjenica da je okrivljeni, osim što je u svom telefonu imao takvu aplikaciju, posedovao i račun u jednoj banci za koju su nadležne turske vlasti smatrale da je redovno koriste pripadnici konkretne organizacije („Gulani“), koja se u Turskoj zvanično smatra terorističkom.

U svojoj odluci *Yüksel Yalçınkaya v. Türkiye*, ESLJP se u stvari, nije suštinski ni bavio pitanjem zakonitosti/pravne valjanosti nadzora kriptovane komunikacije zahvaljujući korišćenju konkretne aplikacije namenjene zaštiti tajnosti komuniciranja niti se na bilo koji način upuštao u bilo kakvu ocenu neke načelne dokazne upotrebljivosti i dokazne verodostojnosti te vrste informacija. ESLJP se, naprotiv, isključivo i krajnje limitirano orijentisao na ocenu da li se zaključak turskog krivičnog suda da je konkretan okrivljeni/osuđeni član terorističke organizacije mogao temeljiti jedino i isključivo, odnosno pretežno na činjenici da je posedovao/koristio aplikaciju koju, inače, imaju/koriste pripadnici konkretne organizacije koja se u Turskoj sma-

81 <https://hudoc.echr.coe.int/fre#%7B%22tabview%22%3A%5B%5D%22document%22%3A%5B%5D%22item%22%3A%5B%5D%22%7D>, 25. mart 2024.

82 Ova aplikacija je omogućavala kriptovano komuniciranje između njenih korisnika, koji bi se identifikovali samo u limitiranom obimu, što znači; korisničkim imenom, kodom i šifrom koja je bila kriptovana, a razmenjivane poruke su čuvane na računaru-serveru u kriptovanoj formi. Sama aplikacija *ByLock* bila je dostupna za preuzimanje (*download*), a dominantno je korišćena u Turskoj.

tra terorističkom. Zaključeno je da se takvo rezonovanje turskih sudova, koje samo posjedovanje konkretne aplikacije, čak i bez dokaza da je ona uopšte korišćenja za tajno/zaštićeno komuniciranje, kao i bez ikakvih relevantnih podataka o sadržaju eventualno tako, to jest zahvaljujući aplikaciji *ByLock*, ostvarene komunikacije, samo po sebi smatra „ekskluzivnim dokazom“ članstva u terorističkoj organizaciji, u konkretnom slučaju ispoljava kao kršenje prava na pravično (*fair*) suđenje. Naime, turski nadležni organi su ustanovili da je okrivljeni poslao/primio više od 300 poruka korišćenjem aplikacije *ByLock*, ali je otkriven sadržaj svega par tih poruka, a sam taj sadržaj se svodio na razmatranje određenih religijskih pitanja, u pogledu čega je okrivljeni tokom krivičnog postupka vođenog protiv njega u Turskoj, kao potom, i u predstavi Evropskom sudu za ljudska prava, tvrdio da je baš takav sadržaj njegove „presretnute“ komunikacije dokaz da aplikaciju nije koristio u „terorističke“ svrhe.

U svojoj odluci *Yüksel Yalçınkaya v. Türkiye*, ESLJP je afirmisao i svoj stav da se *Bykov* test (objašnjen u prethodnom tekstu) primjenjuje i u kontekstu ocene zakonitosti elektronskih/digitalnih dokaza. Zaključuje se i da je posebno važan element dokumentovanje sleda postupanja (*chain of custody*), što se ilustruje slučajem *Horvatić v. Croatia* (§ 341).⁸³ Kada je reč o njegovoj odluci *Yüksel Yalçınkaya v. Türkiye*, ESLJP se bavi i pitanjem „pristupa izvornom dokaznom materijalu“, u pogledu čega konstatuje da je „to pravo važno, ali ga je moguće i limitirati uz odgovarajuće mere balansa“. Takođe se konstatuje, uz oslonac na stavove iz slučaja *Stojkovic v. France and Belgium* (§§ 55–56),⁸⁴ da sa stanovišta člana 6. Konvencije postoji dužnost suda da utvrdi da je li došlo do povrede prava pojedinca u inostranstvu, s aspekta uticaja takvih povreda na pravično suđenje u nacionalnom sistemu.

8. SUD PRAVDE EVROPSKE UNIJE I SPORNA PITANJA KOJA MU JE POSTAVIO REGIONALNI SUD U BERLINU

Sudu pravde Evropske unije je, kao što je to objašnjeno u prethodnom tekstu, niz pitanja postavio berlinski Regionalni sud. Ta su se pitanja primarno ticala pravne valjanosti evropskog istražnog naloga u konkretnom slučaju, iz kojeg je proizišao transfer dokaza iz Francuske u Nemačku. Kao što je to i uobičajeno prema pravilima postupka pred Sudom pravde EU/Evropskim sudom pravde (*European Court of Justice – ECJ*), poseban generalni advokat,⁸⁵ kao visokorangiran funkcioner u Sudu pravde EU, kreira svoje mišljenje o konkretnom slučaju. To mišljenje ima odgovarajući preliminarni karakter, a generalni advokat ima i pravo/mogućnost da sasluša stranke koje iznose argumente i kontraargumente koji se tiču konkretnog slučaja. Nakon toga, njegovo mišljenje postaje osnova na kojoj Sud pravde EU donosi svoju odluku.

Generalni advokat Suda pravde EU se u svom nedavnom mišljenju od 26. oktobra 2023. godine (*C-670/22*)⁸⁶ izjasnio u odnosu na čitav niz pitanja koja je Evrop-

83 <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-173907%22%5D%7D>. 28. mart 2024.

84 Application No. 25303/08, judgment of 27 October 2011, final on 27 January 2012. <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-118243%22%5D%7D>, 28. mart 2024.

85 Engl. *advocate general*, franc. *avocat general*.

86 *Case C-670/22*, delivered on 26 October 2023. <https://eucrim.eu/ecj-eu-criminal-law-cases-overview/>, 1. novembar 2023.

skom sudu pravde postavio nadležni berlinski regionalni/zemaljski sud. Ta pitanja su se primarno ticala dokaznog kredibiliteta u jednoj državi EU, dokaza pribavljenih u drugoj državi EU tehničkim merama nadzora komunikacije korisnika posebne aplikacije za tajno/zaštićeno komuniciranje, a potom transferisanih u sklopu mehanizama međunarodne krivičnopravne pomoći u okviru EU, što se pre svega ticalo evropskog istražnog naloga (EIN). Ovde je bilo značajno i pitanje eventualnog pravljenja razlike između transferisanja već postojećih/pribavljenih dokaza i efektivnog pribavljanja novih dokaza. Dakle, suština tog mišljenja generalnog advokata svodi se na tumačenje Direktive EU o evropskom istražnom nalogu, izdatom sa ciljem transfera dokaza koje već poseduje druga država u sastavu EU, a koje je prethodno pribavila shodno pravilima sopstvenog pravnog sistema.

Konkretne evropske istražne naloge podnelo je državno tužilaštvo Frankfurta tražeći da se primenom takvog istražnog mehanizma iz domena međunarodne krivičnopravne pomoći na nivou EU od nadležnih francuskih organa dobije dozvola za transfer podataka dobijenih nadzorom aplikacije *EnchroChat*, sprovedne aktivnostima zajedničkog holandsko-francuskog istražnog tima, što se ticalo postojanja sumnje da NN lica vrše krijumčarenje i trgovinu drogama u okviru organizovanih kriminalnih grupa.

Krivični sud u Lilu je dozvolio pravosudnim organima prenos i upotrebu takvih podataka koji se odnose na nemačke korisnike aplikacije *EnchroChat*, telekomunikacione mreže koja je potencijalnim korisnicima nudila „skoro potpunu anonimnost“. Na bazi takvog transfera podataka iniciran je potom i krivični postupak pred Regionalnim/zemaljskim sudom u Berlinu „protiv M.N.“, koji se zasnivao na „presretnutim podacima“, prosleđenim primenom mehanizma evropskog istražnog naloga. Iz toga je potom proizišlo pitanje da li se u konkretnom slučaju radilo o kršenju direktive EU kojom se regulišu pravila primene evropskog istražnog naloga, te u vezi sa time, da li takvi dokazi, ako bi se utvrdilo da su prekršena ta pravila, mogu da se koriste u krivičnom postupku.

Generalni advokat Suda pravde EU u svom mišljenju konstatuje da se sama operacija zajedničkog istražnog tima Francuske i Belgije svodila na unošenje „trojanskog softvera“ u server koji se nalazio u Francuskoj (*Roubaix*), u proleću 2020. godine, što je formalno omogućeno/autorizovano odlukom Krivičnog suda u Lilu u Francuskoj. Na taj način su prikupljeni podaci iz komunikacije korisnika aplikacije *EncroChat* iz 122 zemlje, uključujući i oko 46.000 korisnika u Nemačkoj. Tokom video-konferencije održane 9. marta 2020. godine, Evrodžast (*European Union Agency for Criminal Justice Cooperation*) informisao je sve članice o merama nadzora nad komunikacijama ostvarenim putem aplikacije *EncroChat* i nameri da se podaci transferišu. Tada su predstavnici nemačke savezne policije (*Bundeskriminalamt*) pokazali interes da dobiju prikupljene podatke o komunikaciji nemačkih korisnika aplikacije *EncroChat*. Iz toga su kasnije i proizišli prethodno objašnjeni evropski istražni nalozi.

Naime, na temelju primljenih dokaza, Državno tužilaštvo u Frankfurtu je započelo istrage protiv pojedinih korisnika aplikacije *EncroChat*. Zatim je optužilo u konkretnom slučaju jednog okrivljenog za nekoliko krivičnih dela koja su se ticala krijumčarenja droge i protivzakonitog posedovanja narkotika u Nemačkoj. Taj krivični

postupak je bio u toku u vreme kada se berlinski Regionalni sud obratio Sudu pravde EU. Postavljen je niz pitanja, od koji su dva osnovna bila: 1) da li je izdavanjem evropskog istražnog naloga od Državnog tužilaštva u Frankfurtu prekršena Direktiva EU o evropskom istražnom nalogu i 2) ukoliko je evropski istražni nalog izdat suprotno pravilima iz Direktive, da li se mogu isključiti dokazi u krivičnom postupku koji se vodi protiv okrivljenog?

Generalni advokat Suda pravde EU se u svom mišljenju posebno bavio brojnim pitanjima, kao što su sledeća.

- 1) Pitanje interpretacije „koncepta organa koji izdaje istražni nalog“ u smislu člana 6(1) Direktive EU o istražnom nalogu. Naime, postavilo se pitanje da li je za izdavanje istražnog naloga radi pribavljanja dokaza koji su već locirani u državi koja je sprovela odgovarajuće radnje (Francuska u konkretnom slučaju) nadležan sudija koji inače u Nemačkoj ima nadležnost za sprovođenje sličnih posebnih dokaznih radnji.
- 2) Pitanje koje se tiče mogućeg postupanja suprotno pravilima Direktive EU o evropskom istražnom nalogu, onda kada se radi o već pribavljenim dokazima u državi izvršenja (Francuska u konkretnom slučaju), ostvarenih prisluškivanjem komunikacija, a posebno kada je reč o podacima o komunikacionom saobraćaju, tako što je sproveden nadzor svih korisnika pretplaćenih na odgovarajuću uslugu komunikacije, a pritom prethodno nije bilo konkretnih dokaza o izvršenju teških krivičnih dela od pojedinačno označenih, to jest individualizovanih korisnika.
- 3) Pitanje koje se odnosi na dozvoljenost/nedozvoljenost prisluškivanja u državi koja je izdala evropski istražni nalog – da li član 6(1)(b) Direktive o evropskom istražnom nalogu onemogućava primenu tog naloga radi transfera podataka o ostvarenoj telekomunikaciji koji već postoje u izvršnoj državi (u ovom slučaju: Francuska), a kada bi inače, osnovna mera prisluškivanja države izvršenja (Francuska) bila zabranjena prema zakonu države izdavanja (u ovom slučaju: Nemačka) u nekom sličnom domaćem slučaju?
- 4) Pitanje karaktera preduzetih istražnih mera – da li mera koja podrazumeva infiltriranje terminalnih uređaja radi prikupljanja podataka o saobraćaju, lokaciji i komunikaciji internet-bazirane komunikacione usluge predstavlja prisluškivanje telekomunikacija u smislu člana 31. Direktive o evropskom istražnom nalogu?
- 5) Pitanje mogućeg dokaznog *ultima ratio* koncepta – da li je suprotno pravu EU, a posebno principu efikasnosti, ako se upotreba dokaza u krivičnom postupku, čije je dobijanje bilo suprotno pravu Evropske unije upravo zato što prethodno nije postojala sumnja o izvršenom konkretnom krivičnom delu, opravdava balansiranjem interesa koji proizlaze iz težine krivičnih dela za koja je kasnije, zahvaljujući analizi pribavljenih dokaza, utvrđeno da su izvršena?

Generalni advokat Suda pravde EU u svom mišljenju, između ostalog, zaključuje da je pitanje o mogućnosti/dozvoljenosti prenošenja dokaza koji se sastoje od

presretnute komunikacije pribavljene za jednu krivičnu istragu ili postupak u drugu istragu ili drugi postupak stvar nemačkog zakona, a samo to pitanje nije rešeno Direktivom o evropskom istražnom nalogu već se, umesto toga, u Direktivi samo poziva na zakon države iz koje je nalog izdat. U mišljenju se konstatuje i da nemački zakon ne zabranjuje prenos presretnute komunikacije iz jednog krivičnog postupka u drugi, što se ilustruje i primerom da ako nemački zakon zabranjuje domaći prenos presretnute telekomunikacije iz jednog krivičnog slučaja u drugi, onda bi organ koji izdaje nalog bio sprečen i da naredi takav prekogranični prenos.

Konačno, generalni advokat Suda pravde EU je izveo nekoliko *privremenih zaključaka*, od kojih su neki veoma opširni, a neki, obrnuto, prilično sažeti, pa će se u daljem tekstu izneti samo osnovne postavke sadržane u tim privremenim zaključcima, iz čega i proizlazi suština intepretativnog stava zauzetog u mišljenju generalnog advokata Suda pravde EU u konkretnom slučaju.

Prema *prvom privremenom zaključku*, princip međusobnog priznavanja, na kojem počiva sistem evropskog istražnog naloga, nalaže da nadležni nemački organi tom postupku pripisuju istu vrednost kao da je on sproveden u pravnim okvirima domaće države, što važi čak i ako bi nemački sud u konkretnom slučaju odlučio drugačije. Taj zaključak je praćen i konstatacijom da je otkrivanje nemačkih korisnika *EnchroChat-a* u konkretnom slučaju bila konsekvencija, a ne razlog za presretanje komunikacije. Kada je mera u državi izvršenja odobrena od sudije, evropski istražni nalog za prenos takvih dokaza takođe ne mora biti izdat od sudije, čak i ako bi prema zakonu države izdavanja naloga prikupljanje dokaza morao da naredi sudija, a činjenica da je prisluškivanje sprovedeno na teritoriji druge države članice ne utiče na razliku u određivanju organa izdavanja naloga.

Prema *drugom privremenom zaključku*, onda kada je osnovna sprovedena mera u državi izvršenja odobrena od sudije, evropski istražni nalog za transfer takvih dokaza ne mora biti izdat od sudije, čak i ako bi prema zakonu države izdavanja naloga prikupljanje dokaza moralo biti naređeno od sudije. Pravo EU ne zahteva da se evropski istražni nalog za prenos postojećih dokaza prikupljenih prisluškivanjem telekomunikacija izdaje od suda, ako nacionalno pravo predviđa da javni/državni tužilac može narediti takav prenos u sličnom domaćem slučaju. Ocena nužnosti i proporcionalnosti evropskog istražnog naloga kojim se zahteva prenos postojećih dokaza u nadležnosti je organa izdavanja naloga, uz mogućnost pregleda/preispitivanja od nadležnog nacionalnog suda. Takva ocena mora uzeti u obzir da pristup nacionalnog organa podacima o presretnutoj komunikaciji predstavlja ozbiljno mešanje u privatni život lica koja su pogođena konkretnom merom iz koje je proisteklo prikupljanje podataka, a to mešanje mora biti uravnoteženo sa ozbiljnim javnim interesom u istrazi i gonjenju krivičnih dela.

Treći privremeni zaključak se tiče procene neophodnosti i proporcionalnosti zahteva za prenos postojećih dokaza putem evropskog istražnog naloga, što se svodi na isticanje da takva procena mora uzeti u obzir da pristup nacionalnom organu podacima o presretnutoj komunikaciji predstavlja ozbiljno mešanje u privatni život osoba koje su pogođene te da takvo mešanje mora biti uravnoteženo sa ozbiljnim javnim interesom u istrazi i gonjenju krivičnih dela. U mišljenju se

ističe da kada se izda evropski istražni nalog za prenos dokaza koji su već u posedu druge države, upućivanje na sličan domaći slučaj prema članu 6(1)(b) Direktive 2014/41/EU Evropskog parlamenta i Saveta od 3. aprila 2014. o evropskom istražnom nalogu zahteva od organa izdavanja da utvrdi da li i pod kojim uslovi-ma relevantno nacionalno pravo dozvoljava prenos dokaza prikupljenih prisluškivanjem komunikacije između krivičnih postupaka na domaćem nivou. Prilikom odlučivanja da li može izdati evropski istražni nalog za prenos postojećih dokaza, organ izdavanja ne može ocenjivati zakonitost prikupljanja dokaza u državi izvršenja čiji se prenos zahteva putem evropskog istražnog naloga. Sama činjenica da su osnovne mere preduzete na teritoriji države izdavanja ili su bile u interesu te države ne utiče na prethodni odgovor.

I četvrti *privremeni zaključak* se odnosi na proporcionalnost, ali u odnosu na potencijalno ozbiljno mešanje u neka od osnovnih ljudskih prava, gde je posebno važno pitanje nadležnosti organa koji može narediti radnje takvog karaktera. Zaključuje se da pravo EU ne zahteva da evropski istražni nalog za prenos postojećih dokaza prikupljenih prisluškivanjem telekomunikacija obavezno izdaje sud, ako nacionalno pravo predviđa da i javni/državni tužilac može narediti takav prenos u sličnom domaćem slučaju.

Peti privremeni zaključak se tiče obaveze međusobnog/uzajamnog obaveštavanja država u slučajevima istraga usmerenih na otkrivanje krivičnih dela.⁸⁷ Zaključeno je da država članica koja, tokom svoje samostalne krivične istrage ili postupka, presreće telekomunikacije na teritoriji druge države članice mora obavestiti tu drugu državu o presretanju. To obaveštenje može biti upućeno bilo kojoj vlasti koju država članica koja preduzima presretanje smatra odgovarajućom jer ta država ne može znati koja je vlast nadležna u sličnom domaćem slučaju. Država članica koja, tokom svoje samostalne krivične istrage ili postupka, presreće telekomunikacije na teritoriji druge države članice mora obavestiti tu drugu državu o presretanju. Obaveštenje može biti upućeno bilo kom organu koji država članica koja presreće telekomunikaciju smatra odgovarajućom, s obzirom da ta država ne može znati koji je organ nadležan u sličnom domaćem slučaju. Svrha člana 31. Direktive 2014/41 je da štiti kako pojedinačne korisnike telekomunikacija koji su „pogođeni“/na koje se odnosi, tako i suverenitet obaveštene države članice.

Šesti privremeni zaključak tiče se prihvatljivosti dokaza, što se svodi na konstataciju da pravo EU u ovom trenutku svog razvoja ne reguliše dopuštenost dokaza prikupljenih putem evropskog istražnog naloga eventualno izdatog suprotno zahtevima sadržanim u Direktivi EU o tom nalogu. Dopuštenost dokaza je pitanje nacionalnog prava, ali se ono ipak mora usaglasiti i sa zahtevima prava na odbranu iz članova 47. i 48. Povelje o osnovnim pravima EU.

Od posebnog su značaja *dve pretpostavke* koje se prema zauzetom stavu i mišljenju generalnog advokata Suda pravde EU tiču konkretnog slučaja, a koje imaju i načelni karakter, kada je reč o dokazima pribavljenim u jednom državi EU, a po-

87 To je praćeno i posebnim objašnjenjem da je svrha člana 31. Direktive EU o evropskom istražnom nalogu da paralelno zaštiti: 1) kako pojedinačne korisnike telekomunikacija koji mogu biti pogođeni konkretnim istražnim aktivnostima tako i 2) suverenitet obaveštene države članice EU.

tom primenom mehanizma evropskog istražnog naloga transferisani u drugu državu članicu EU. Jedno je *pretpostavka zakonitosti*, a drugo je *pretpostavka poštovanja ljudskih prava*.⁸⁸

Naravno, treba imati na umu da se ovde, kada je reč o pretpostavkama zakonitosti/poštovanja ljudskih prava, a što je i logična konsekvenca uloge Suda pravde EU u pravnom sistemu same Evropske unije, radi o takvim pretpostavkama koje se neposredno tiču uzajamnog odnosa pravnih sistema država koje su članice EU, a u normativnim okvirima pravila međusobnog pružanja/dobijanja krivičnopravne pomoći između država u sastavu EU, što znači na nivou same Evropske unije.

8.1. Sud pravde EU i pretpostavka zakonitosti

Generalni advokat Suda pravde EU zaključuje da državni organ koji je izdao evropski istražni nalog nije dužan da procenjuje da li su osnovne mere kojima su dokazi prikupljeni u drugoj državi članici EU, a koji se transferišu pravnim mehanizmom evropskog istražnog naloga, zakonito sprovedene u državi članici koja je izvršila evropski istražni nalog. Ta se mogućnost čak smatra isključenom.

To se konkretizuje i stavom da je prilikom izdavanja evropskog istražnog naloga za transfer postojećih dokaza organ koji je izdao nalog vezan principom međusobnog priznavanja, kojim se na nivou Evropske unije podržava međudržavna saradnja u krivičnim stvarima. U mišljenju generalnog advokata Suda pravde EU konstatuje se i da bi drugačije bilo jedino ako bi se u postupku pred francuskim sudom utvrdilo da su preduzete mere bile nezakonite shodno pravilima francuskog prava. Pri tome uvek mora postojati mogućnost pokretanja takvog postupka od lica na koje su se odnosile mere, odnosno kojeg se tiče evropski istražni nalog. Ukoliko nema takve inicijative, sam organ koji izdaje evropski istražni nalog nije ovlašćen da po službenoj dužnosti dovodi u pitanje zakonitost naloga.

Ovde treba imati u vidu i da je konkretni okrivljeni u krivičnom postupku pred nadležnim nemačkim sudom („M. N.“), ostvarujući svoje pravo na odbranu, tvrdio da postoji razlika između transfera dokaza i samih mera/radnji putem kojih su dokazi prikupljeni, a što omogućava zaobilazanje zaštite osumnjičenih ili optuženih osoba prema zakonu države koja je izdala evropski istražni nalog. Prema njegovom mišljenju, nemačke vlasti/nadležni organi su se obratile svojim francuskim „kolegama“ kako bi dobile dokaze suprotno nemačkom zakonu.

Međutim, prema stavu generalnog advokata Suda pravde EU, okolnosti tog konkretnog slučaja ne ukazuju na sumnju u zloupotrebu postupaka prekograničnih istraga, a sama Francuska je stekla sporne dokaze tokom sopstvene krivične istrage. Zaključuje se da čak i ako bi ti dokazi bili od interesa i za Nemačku, Francuska ih nije prikupljala u svrhu nemačke krivične istrage. Dakle, u mišljenju generalnog advokata Suda pravde EU ističe se da čak i ako je tačno da nemački sudija ne bi odobrio da se takvo „presretanje“ sprovodi u Nemačkoj, francuske vlasti su preduzele takve mere u skladu sa francuskim zakonom i uz odobrenje nadležnog francuskog suda.

⁸⁸ <https://curia.europa.eu/juris/document/document.jsf?jsessionid=EEF3F45D476085A9ADBA8A86C66FF78D?text=&docid=279144&pageIndex=0&doclang=en&mode=req&dir=&occ=first&par=1&cid=100225>, 1. novembar 2023.

8.2. Sud pravde EU i pretpostavka poštovanja ljudskih prava

Generalni advokat Suda pravde EU zaključuje da iako se krivični pravni sistemi država članica značajno razlikuju, to ne znači da jedan sistem štiti osnovna prava osumnjičenih i optuženih, dok ih, obrnuto, drugi pravni sistem krši.

Naprotiv, u mišljenju generalnog advokata Suda pravde EU ističe se posebno da se pravosudna saradnja između država članica EU u krivičnim stvarima temelji na pretpostavci da sve članice EU poštuju osnovna ljudska prava. Objašnjava se da iako se ta pretpostavka može dovesti u pitanje u određenom slučaju pred nadležnim sudom, to svakako ne dovodi u pitanje princip međusobnog poverenja koji stoji iza evropskog istražnog naloga i drugih instrumenata saradnje u krivičnim stvarima između država članica Evropske unije.

8.3. Presuda Evropskog suda pravde od 30. aprila 2024.

Veliko veće Evropskog suda pravde je 30. aprila 2024. godine, donelo presudu u predmetu C-670/22,⁸⁹ u postupku pokrenutom (što je detaljno objašnjeno u prethodnom tekstu), zahtevom Regionalnog suda u Berlinu od 19. oktobra 2022. godine, a koji je u Evropski sud pravde primljen 24. oktobra, 2022. godine. Zahtev berlinskog regionalnog suda ticao se niza pitanja koja je on smatrao spornim,⁹⁰ a

89 Radi se o preliminarnom tekstu, koji još uvek nije u potpunosti „zvaničan“, a što se i striktno navodi u zaglavlju tog teksta (*Provisional text – JUDGMENT OF THE COURT (Grand Chamber)*, 30 April 2024). Kako je reč o veoma aktuelnom pitanju i s obzirom na to da će i prema uobičajenoj praksi, zvaničan tekst, tj. sadržaj presude Evropskog suda pravde, svakako biti veoma sličan ovom preliminarnom/provizornom tekstu te presude, on se i komentariše u ovom delu članka, koji je inače završen i predat radi objavljivanja, znatno pre nego što je provizorni tekst presude Evropskog suda pravde postao dostupan. Prema pravilima Evropskog suda pravde, tekst presude postaje zvaničan tek kada se izradi njegova finalna verzija i kada se ona dostavi svim subjektima postupka kojima se presuda oficijelno i obavezno dostavlja. Period pripreme za štampu časopisa dao je priliku autoru da i uvrštavanjem ove „najnovije novosti“ koja se tiče dokaznog značaja komunikacije ostvarene aplikacijama za kriptovanje, članak učini aktuelnijim i korisnijim kako za krivičnoprocesnu teoriju, tako i za praksu organa krivičnog postupka. Naravno, to se sada čini u jednom relativno sažetom, ali u ipak dovoljno ilustrativnom obliku.

90 Zahtev se ticao preliminarnog utvrđivanja pravila korektnog tumačenja relevantnih odredbi koje se tiču Evropskog istražnog naloga, u kontekstu principa ekvivalencije/proporcionalnosti i efektivnosti/delotvornosti (*the interpretation of Article 2(c), Article 6(1) and Article 31 of Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ 2014 L 130, p. 1), and of the principles of equivalence and effectiveness.*).

Dakle, u ovom slučaju, ne samo da se radi o konkretnom krivičnom predmetu, već je reč i o isključivo pitanju koje je od značaja kako za određene konkretne krivične postupke u Nemačkoj (*primarno*), tako *supsidijarno* i za druge „slične“ krivične postupke u drugim državama EU, koje jedino i mogu da koriste postojeće mehanizme krivičnopravne pomoći i saradnje u samoj EU, gde spada i Evropski istražni nalog. Formalno se ovo uopšte ni ne tiče država koje nisu u EU, ali kao što će se to objasniti u daljem tekstu (a delom je objašnjeno i u prethodnom tekstu koji se tiče preliminarnih zaključaka Generalnog advokata koji postupa pred Evropski sudom pravde), stavovi Evropskog suda pravde mogu ipak, imati određene efekte i u drugim evropskim državama, ali isključivo i limitirano kao neka vrsta mogućeg „putokaza“ prilikom tumačenja određenih potencijalno spornih pitanja, ali nikako ne i direktno, te formalno obavezujuće, kao kada se radi o državama koje su članice Evropske unije.

koja su se pojavila u konkretnom krivičnom postupku protiv otkrivenog M.N.⁹¹ Veliki deo provizornog teksta Evropskog suda pravde od 30. aprila 2024. godine je istovetan ili veoma sličan prethodno već objašnjenim zaključcima Generalnog advokata koji postupa pred Sudom pravde EU, poput objašnjenja relevantnih pravila koja se tiču pružanja/dobijanja pomoći u krivičnim stvarima između nadležnih organa država članica EU, a posebno pravila koja se odnose na Evropski istražni nalog. Takođe se detaljno navode sva konkretna pitanja koja je postavio Regionalni sud u Berlinu, kao i relevantni stavovi drugih nadležnih organa u konkretnom krivičnom postupku u Nemačkoj, odnosno povezano s tim itd.

Zahtev za preliminarnu odluku Suda pravde EU omogućava sudovima i drugim nadležnim organima država članica EU u postupcima koji se odvijaju pred njima, odnosno koje oni vode, da upućuju Sudu pravde pitanja o tumačenju prava EU ili postavljaju pitanja o validnosti određenih akata na nivou EU. Sud pravde EU nije taj koji donosi odluku u bilo kojem konkretnom postupku, već je na nacionalnom sudu da svoju odluku donese skladu sa odlukom Suda pravde EU, koja je potom, u precedentnom smislu i na sličan način obavezujuća i za druge nacionalne sudove u državama članica EU, koji se suoče sa sličnim pitanjem. Dakle, stavovi Suda pravde EU su striktno i formalno obavezujući samo za sudove/druge nadležne organe, država koje su članice Evropske unije.

Posebno su od značaja sledeće konstatacije sadržane u provizornom tekstu presude Evropskog suda pravde u predmetu C-670/22:⁹²

- 1) Evropski istražni nalog koji se odnosi na transfer dokaza koji su već u posedu nadležnih organa države koja izvršava nalog (u ovom slučaju Francuska), ne podrazumeva obavezno da o tome odluči sud, već je moguće da do takvog transfera dođe i na osnovu odluke državnog/javnog tužioca, ako je on u konkretnoj državi nadležan, kada se radi o suštinski sličnim „domaćim slučajevima“, koji se tiču naloga da se dostave dokazi koji su već prikupljeni/pribavljeni.
- 2) Javni/državni tužilac (u ovom slučaju nemački), ne isključuje se od mogućnosti izdavanja Evropskog istražnog naloga za prenos dokaza koji su već u posedu nadležnih organa države izvršenja Evropskog istražnog naloga (članice EU), u kojoj su ti dokazi pribavljeni presretanjem telekomunikacija korisnika mobilnih telefona koji preko specijalnog softvera i modifikovanog hardvera, omogućavaju kriptovanu/šifrovanu komunikaciju, pod uslovom da Evropski istražni nalog ispunjava sve uslove koji su propisani nacionalnim pravom države čiji organ izdaje Evropski istražni nalog u domaćem izrazito sličnom slučaju.
- 3) Izdavanje Evropskog istražnog naloga podleže istim uslovima koji se primenjuju i kada se radi o transmisiji istih dokaza/iste vrste dokaza u suštinski sličnim domaćim slučajevima u konkretnim državama članicama EU. Međutim, to ne znači da moraju biti ispunjeni potpuno isti materijalni

91 <https://curia.europa.eu/juris/document/document.jsf?text=&docid=285365&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=323072>, 9. maj 2024.

92 <https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-04/cp240077en.pdf>, 9. maj 2024.

uslovi koji se primenjuju radi pribavljanja dokaza. Činjenica je da su nadležni francuski organi u Nemačkoj i za potrebe svojih nemačkih „partnera“ prikupljali dokaze, u principu je irelevantna u ovom slučaju. Međutim, sud pred kojim se vodi postupak mora biti u mogućnosti da preispita poštovanje osnovnih prava lica o „kojima se radi“ i kojih se ticao realizovani Evropski istražni nalog, a što su praktično okrivljeni u konkretnom krivičnom postupku.

- 4) O merama koje se sastoje u infiltraciji uređaja, čija je svrha prikupljanje podataka o saobraćaju, lokaciji i komunikaciji baziranoj na uslugama interneta, mora biti obavestena država članica EU, u kojoj se nalazi subjekat na kojeg se takve mere odnose (u ovom slučaju je to Nemačka).⁹³ Nadležni organ države članice EU ima i pravo odlučivanja da se takva mera ne sme sprovesti ili da se mora prestati sa njenim sprovođenjem, ukoliko ona ne bi bila dozvoljena u sličnom domaćem slučaju. Svrha ovih prava i dužnosti nije samo garantovanje poštovanja suvereniteta država članica EU, već i zaštita prava lica o kojima se radi, a što znači, okrivljenih u konkretnim krivičnim postupcima.
- 5) Od nacionalnih krivičnih sudova u državama članicama EU, zahteva se da zanemare/odbace dokaze, u kontekstu krivičnog postupka protiv lica za koje se sumnja da je učinilo krivično delo, kada su ispunjena dva kumulativno formulisana uslova: a) ako konkretno lice nije (bilo) u poziciji da komentariše te dokaze, što znači da ih opovrgava i da im oponira, kao i b) kada je verovatno da će ti dokazi imati preovlađujući uticaj, na utvrđivanje činjenica.

8.3.1. *Realan efekat presude Evropskog suda pravde od 30. aprila 2024.*

Presuda Evropskog suda pravde, koja za sada postoji samo u „provizornom obliku“ i formalno još uvek ne i kao zvaničan tekst, ali čiji je sadržaj već sada prilično jasan, formalno obavezuje samo države članice EU, odnosno nadležne organe tih država i to isključivo u kontekstu primene pravila EU koja se tiču krivičnopravne saradnje država članica/njihovih nadležnih organa, a posebno vezano za primenu mehanizma Evropskog istražnog naloga.

Određeni rezoni Evropskog suda pravde formalno ispoljeni u njegovoj presudi C-670/22, mogu u određenoj meri imati uticaja i na rezonovanje sudske prakse evropskih država koje nisu članice EU, ali koje načelno pripadaju istom/sličnom pravnom ambijentu i evropskoj pravnoj tradiciji, ali naravno, samo do mere koja proizlazi iz primene relevantnog nacionalnog prava. Njih će u ovom pogledu pre

93 Inače, u kontekstu prirode telekomunikacija ostvarenih putem korišćenja aplikacija/prilagodjenih uređaja za kriptovano/šifrovano/tajno komuniciranje, ovaj uslov deluje prilično „fluidno“, imajući u vidu da se komunikacije ove vrste najčešće nisu ni ostvarivale uopšte, ili bar ne kompletno, na teritoriji države na kojoj je fizički bio „subjekt pod nadzorom“. Naime, ne samo da su se „žive“ komunikacije, odnosno komunikacije koja su aktuelno bile u toku u vreme presretanja/nadzora, realizovale preko računarskih mreža i servera najčešće u drugoj državi, već je u stvari, najveći deo te presretnute komunikacije bio „iz prošlosti“, tj. radilo se o komunikaciji koja je ranije ostvarena, odnosno koja je realizovana pre presretanja/nadzora, a potom pohranjena u računarima koji su služili kao server, takođe najčešće u nekoj trećoj državi, kada je potom, tako „sačuvana komunikacija“, bila predmet tzv. presretanja.

svega, obavezivati kako opšta dokazna pravila njihovih zakon(ik)a o krivičnom postupku, kao i pravila sadržana u izvorima prava međunarodne pravne pomoći u krivičnim stvarima, a koja su i korišćena za dobijanje konkretnih dokaza sadržanih u kriptovanoj komunikaciji. U izvore tih pravila spadaju pre svega: Evropska konvencija (Konvencija Saveta Evrope) o međusobnom pružanju pravne pomoći u krivičnim stvarima sa dodatnim protokolom, međunarodni ugovori o pravnoj pomoći u krivičnim stvarima sa konkretnim državama, Budimpeštanska konvencija o „sajber“ (kibernetičkom) kriminalitetu, kao naravno i nacionalni zakoni koji se tiču međunarodne krivičnopravne pomoći, poput u Srbiji Zakona o međunarodnoj pravnoj pomoći u krivičnim stvarima.

Kada je reč o državama članicama EU, njih posebno obavezuje stav Suda pravde EU da mere kojima su pribavljeni konkretni dokazi, kasnije transferisani primenom Evropskog istražnog naloga, moraju biti moguće u nekom suštinski/izrazito sličnom domaćem slučaju. To verovatno ne bi trebalo da bude sporno kada se radi o državama koje su imale zajedničke istražne timove i čiji su organi zajednički/kordinisano učestvovali u pribavljanju dokaza presretanjem komunikacija ostvarenih aplikacijama/prilagođenim uređajima za kriptovanje komunikacije. Takav je slučaj sa Francuskom, Belgijom i Holandijom. Tada je naravno, svakako ispunjen i uslov da su nadležni organi države članice EU u kojoj se nalazi subjekat na kojeg se takve mere odnose, bili obavešteni o preduzimanju mera, ako je takav „subjekt“ bio u nekoj od tih država, čiji su nadležni organi bili i u sastavu zajedničkog istražnog tima. I nemačko krivično procesno pravo (što je od posebnog značaja, jer je i odlučivanje Evropskog suda pravde bilo inicirano zahtevom nemačkog suda), kao i većina drugih krivičnoprocesnih prava država članica EU poznaje slične mere koje se tiču određenih posebnih dokaznih radnji te vrste. Ovaj zahtev se formalno ne tiče država koje nisu članice EU.

Takođe, kada se radi o obavezi obaveštavanja države na čijoj je teritoriji „subjekt koji je predmet nadzora“ i ona se isključivo odnosi na države članice EU i to posredstvom već postojećih mehanizama zvanične komunikacije nadležnih organa tih država u okviru kako Evropol-a, tako i posebno Evrodžasta, a takve obaveze formalno nema kada se radi o državama koje nisu članice EU, niti u odnosu na te države postoje takvi komunikacioni kanali, kao kada su u pitanju države koje su članice EU.

9. ZAKLJUČAK

Često se kada je reč o nadzoru/dešifrovanju komunikacije koja je kriptovana posebnim aplikacijama/modifikovanim uređajima za zaštitu tajnosti komuniciranja lica koja su informacije razmenjivala korišćenjem takvih aplikacija/uređaja, razmišlja o postojanju/nepostojanju povrede na privatnost lica koja su komunicirala na takav način. To se, naravno, neposredno povezuje i sa potencijalnom dokaznom nevalidnošću/pravnom nevaljanošću/nezakonitošću takvih informacija/dokaza, ako bi se utvrdilo da su pribavljeni povredom prava na privatnost, a u kontekstu toga bi se onda moglo raditi i o povredi prava na pravično suđenje. Dakle, suština je ovde da se pravo na privatnost najčešće ne posmatra izolovano i samo po sebi, kao

potencijalno povređeno, već se smatra da ako je ono povređeno, iz toga posledično proizlaze i druge dalekosežne krivičnoprocesno-dokazne konsekvence.

Treba imati na umu i u tim situacijama da je privatnost od ogromne važnosti u svim sferama ljudskog života, pa je, samim tim, ogroman značaj prava na privatnost, koje nije samo zakonsko, već je kako ustavnog, tako i „konvencijskog“ ranga. Međutim, privatnost nije bezobalna, a nije bezobalno ni pravo na privatnost. I ono se može u određenim restriktivno propisanim slučajevima zakonski i ustavnopravno legitimno ograničiti. Dakle, pravo na privatnost ipak ima i svoje jasno omeđene granice, koje se u pravnim državama, zasnovanim na vladavini prava, mogu utvrditi samo na zakonite i ustavnopravno opravdane/legitimne načine.

Kada je reč o korišćenju šifrovane/kriptovane komunikacije u praksi, te dešifrovanja/dekriptovanja takve komunikacije od nadležnih organa pojedinih država primenom posebnih tehničkih načina/metoda, u oceni postojanja moguće povrede prava na privatnost korisnika posebnih aplikacija/uređaja namenjenih tajnoj/zaštićenoj komunikaciji uvek se mora posebno uzeti u obzir pre svega osnovni cilj korišćenja te vrste komuniciranja. Dakle, tu bi jedno od osnovnih pitanja bilo svedeno na ocenu da li je konkretan korisnik te vrste aplikacija/uređaja, kojima je na takav način štitio svoju komunikaciju od tzv. presretanja, odnosno nadzora i prisluškivanja, to činio da bi tako čuvao svoju privatnost ili je tako postupao iz potpuno drugih razloga. Čini se da se u praksi pretežno, ako ne i isključivo (bar u do sada postojećoj/uočenoj praksi), radi o sasvim drugim razlozima, koji se, pre svega, tiču zaštićenog komuniciranja sa ciljem vršenja krivičnih dela ili njihovog prikrivanja, kriminalnog organizovanja, često i na multinacionalnom/transnacionalnom nivou i sl., mada ne treba, naravno, krajnje načelno isključiti ni mogućnost eventualnog korišćenja takve kriptovane komunikacije i u neke druge svrhe, što, takođe, može biti, između ostalog, predmet dokaznog rezonovanja suda u krivičnom postupku u svakom konkretnom slučaju. Iz toga proizlazi i da odgovarajući rizik korišćenja, kao i „presretanja“ i tzv. provaljivanja takve šifrovane komunikacije, koja predstavlja ne samo krajnje neuobičajen način komuniciranja u odnosu na druge redovne načine, poput korišćenja regularne mobilne telefonije, slanja imejl poruka, ali i korišćenja nekih inače uobičajenih aplikacija, kao što su *Viber*, *WhatsApp* i sl., kada se radi o mogućnosti „provaljivanja“ te vrste veoma atipičnog komuniciranja, dominantno snose sami korisnici posebnih aplikacija/uređaja. To ima neposredan značaj i u razmatranju moguće povrede njihovog prava na privatnost, onda kada je sasvim očigledno, te u krivičnoprocesnom smislu dokazano, da oni takav način zaštićenog komuniciranja nisu koristili radi zaštite svoje privatnosti već iz sasvim drugih razloga, koji se suštinski ne mogu smatrati legitimnim.

Čini se i da je posebno važno pitanje dokaznog značaja fotografija koje su razmenjivane komuniciranjem koje se ostvarivalo korišćenjem posebnih aplikacija/uređaja za tajno/zaštićeno komuniciranje. Same te fotografije, onda kada je isključena mogućnost eventualne foto-montaže te kada je pouzdano potvrđena njihova autentičnost, što je *questio facti* u svakom konkretnom slučaju, a u kontekstu i svih drugih dokaza te na temelju opštih dokaznih pravila, što podrazumeva i delovanje načela slobodne ocene dokaza i slobodnog uverenja suda/organa postupka, predstavljaju poseban materijalni dokaz, proistekao iz elektronskih/digitalnih dokaza

pribavljenih iz (de)šifrovane tajne/zaštićene komunikacije korišćenjem posebnih aplikacija/uređaja za kriptovanje razmene informacija tokom komuniciranja.

Nacionalni sudovi će se verovatno i dalje, u neposrednom budućem vremenu, kada se radi o informacijama/dokazima proisteklim iz (de)šifrovane tajne/zaštićene komunikacije korišćenjem posebnih aplikacija/uređaja za kriptovanje razgovora/razmene informacija tokom komuniciranja, primarno baviti pitanjem karaktera tako pribavljenih informacija, u smislu ocene da li je reč o *ispravi pribavljenoj putem međunarodne pravne pomoći*, koja suštinski predstavlja elektronski/digitalni dokaz, ili je u pitanju druga vrsta dokaza. To bi se uglavnom svelo na dokaz do kojeg se došlo određenom posebnom dokaznom radnjom, odnosno specijalnom istražnom tehnikom, zakonski primarno kreiranom za prikupljanje/zadobijanje dokaza koji se tiču nekih krivičnih dela koja se uobičajeno otežano otkrivaju klasičnim/opštim dokaznim radnjama, kao što je to tipično za krivična dela organizovanog kriminaliteta, kada uobičajeno u praksi, tokom „istražnih faza krivičnog postupka“, postoji tipičan „dokazno-informativni deficit“. Ovde se, po svemu sudeći, radi o posebnoj vrsti elektronskih/digitalnih dokaza, a dosadašnja sudska praksa, kako u Srbiji, tako i ona uporednopravna, očigledno se primarno usmerava na tretiranje tih dokaza kao isprava, odnosno elektronskih/digitalnih dokaza u zakonodavstvima/praksi država koje poznaju i formalno takvu posebnu vrstu dokaza.

Naime, čini se da ne samo određene posebne dokazne radnje propisane pravilima srpskog Zakonika o krivičnom postupku već ni slične mere/radnje u vidu posebnih istražnih tehnika koje postoje u drugim evropskim državama ne mogu da se podvedu pod aktivnosti kojima su u konkretnim slučajevima, akcijom francuske, belgijske i holandske policije, pribavljene informacije iz (de)šifrovane tajne/zaštićene komunikacije, realizovane korišćenjem posebnih aplikacija/uređaja za kriptovanje razgovora/razmene informacija tokom komuniciranja. Izuzetak je donekle i pre svega Francuska, čije zakonodavstvo poznaje i posebnu dokaznu radnju/specijalnu istražnu tehniku infiltracije u računarski sistem. Stoga je verovatnije da će sudska praksa većine evropskih država, kao i Srbije, vremenom i definitivno zauzeti stav da je to posebna vrsta specifičnog elektronskog/digitalnog dokaza u vidu isprave. Konačno, to je i do sada pretežno bio slučaj i u uporednoj praksi nekih evropskih sudova, koja se donekle kristalizovala, nakon izvesnih kolebanja, pa i „lutanja“ u nekim zemljama. Sve to je već detaljnije objašnjeno u prethodnom tekstu.

Za razliku od sudova država članica EU, koje su veliku pažnju posvetili tom pitanju u kontekstu pravila Evropske unije koja se tiču evropskog istražnog naloga, koji je bio osnovni mehanizam na nivou EU za dobijanje informacija/dokaza iz (de)šifrovane tajne/zaštićene komunikacije, ostvarene korišćenjem posebnih aplikacija za kriptovanje komunikacije, za sudove u Srbiji, kao državi koja nije članica EU i koja ne koristi/nije koristila evropski istražni nalog, to pitanje nije neposredno relevantno, pa samim tim i nema neki „ključni značaj“. Međutim, i za srpske sudove je značajno ocenjivanje i dokazno vrednovanje ključnog pitanja, koje se svodi na ocenu da li je primena odgovarajućih mehanizama međunarodne krivičnopravne pomoći radi dobijanja informacija/dokaza iz (de)šifrovane tajne/zaštićene komunikacije ostvarene posebnim aplikacijama u svakom konkretnom slučaju bila realizo-

vana u skladu sa relevantnim pravilima pružanja/dobijanja međunarodne pravne pomoći u krivičnim stvarima.

I kada/ako se u sudskoj praksi zaključi da se radi o ispravi koja sadrži podatke o ranije već realizovanoj komunikaciji korišćenjem posebnih aplikacija/uređaja za kriptovanje razgovora/razmene informacija tokom komuniciranja, kao posebnoj vrsti elektronskog/digitalnog dokaza, biće relevantno i pitanje ocene zakonitosti/pravne valjanosti načina njenog pribavljanja. To, naravno, proizlazi iz opštih zakonskih pravila. U tom pogledu će ključno biti primenjivanje jednog od osnovnih kriterijuma koji se tiče dokazne upotrebljivosti informacija/dokaza pribavljenih/izvedenih u stranoj državi, a to je da li je konkretna procesna/dokazna radnja sprovedena prema relevantnim pravilima same te konkretne strane države. Dakle, suština je u oceni da li takva radnja/procesna/istražna aktivnost, izvorno prema relevantnim zakonskim pravilima konkretne strane države, može da se smatra zakonitom/pravno valjanom i da li rezultati takve konkretne procesne/dokazne radnje u samoj toj državi u kojoj je ona sprovedena mogu načelno da imaju odgovarajući dokazni karakter/kredibilitet. Ovde je, kao i inače u pružanju/dobijanju međunarodne pravne pomoći u krivičnim stvarima, posebno značajan tradicionalni princip poverenja u pravosuđe država sa kojima se inače, na temelju odgovarajućih izvora prava, poput bilateralnih ili multilateralnih ugovora pre svega, ostvaruje saradnja u krivičnopravnom smislu te uzajamno i dobija i pruža međunarodna pravna pomoć u krivičnim stvarima.

Kao i inače, tako i u oceni prihvatljivosti kao dokaza podataka proisteklih iz (de)šifrovane tajne/zaštićene komunikacije korišćenjem posebnih aplikacija za kriptovanje razgovora/razmene informacija tokom komuniciranja, nema čudotvornog „recepta“ koji to pitanje definitivno rešava po nekakvom „automatizmu“ i apsolutno jednako za svaki konkretan slučaj.

Generalno i načelno, što važi i za sve druge dokaze koji se izvode u krivičnom postupku i na kojima se temelje/mogu temeljiti odluke krivičnog suda o predmetu krivičnog postupka, tako se i dokazi proistekli iz (de)šifrovane tajne/zaštićene komunikacije korišćenjem posebnih aplikacija/uređaja za kriptovanje razgovora/razmene informacija tokom komuniciranja ocenjuju kako pojedinačno, tako i u njihovoj međusobnoj vezi sa drugim dokazima, koji egzistiraju u svakom konkretnom slučaju/krivičnom postupku, a sve to u kontekstu delovanja opštih dokaznih načela, poput načela slobodne ocene dokaza i principa slobodnog uverenja suda/organa postupka.

Inače, nekada se kod nas iznosi i stanovište da su podaci prikupljeni nadzorom komunikacije ostvarene korišćenjem aplikacija za kriptovanje isključivo *operativni podaci*, bez neposrednog krivičnoprocesno-dokaznog značaja. Naravno, takav stav je legitiman, isto kao što je legitiman i suprotan stav da se radi o načelno pravno valjanim dokazima, pribavljenim mehanizmom međunarodne krivičnopravne pomoći. Naravno, konačnu reč u odnosu na takve suprostavljene stavove, će svakako dati sud u krivičnom postupku, gde će svakako ključnu ulogu imati sudovi najvišeg ranga, a u „krajnjoj liniji“ Vrhovni sud Srbije. Međutim, ovde je od posebnog značaja i obraćanje pažnje na određene krivičnoprocesne konsekvence koje mogu proizići iz ocene u koju kategoriju spadaju konkretne informacije/dokazi, zavisno od faze krivičnog postupka u kojoj do takve ocene dolazi.

Onda kada se takve informacije isključivo smatraju podacima „operativnog značaja“, one se nekada poistovećuju sa indicijama. Ovde treba posebno imati u vidu da se s jedne strane, u Zakoniku o krivičnom postupku ne koristi termin „operativni podaci“, te da s druge strane, naš Zakonik o krivičnom postupku, kao što to ni inače, ne čine ni drugi savremeni zakon(ic)i o krivičnom postupku ne poznaje formalnu podelu na tzv. posredne dokaze (indicije) i neposredne dokaze, iako neki „tragovi“ takve podele sasvim nepotrebne postoje u zakonskim definicijama procesno relevantnih stepena sumnje, ali i „izvesnosti“, što je velika greška zakonodavca, koja ipak, nema neke posebne praktične posledice. Takvih definicija ni inače nema u savremenim zakon(ic)ima o krivičnom postupku.

Podela na posredne i neposredne dokaze, nekada veoma karakteristična za stare inkvizitorske zakon(ik)e o krivičnom postupku, je u modernom krivičnom procesnom pravu isključivo i samo od čisto teorijskog značaja. Stoga, kada se govori o „operativnim podacima“, to nikako ne može biti sinonim za indicije ili tzv. posredne dokaze u teorijskom smislu, već se tu može raditi jedino o podacima koji imaju određeni isključivo informativni značaj u najranijim procesnim fazama, poput našeg nekadašnjeg prekrivičnog postupka ili sadašnjeg predistražnog postupka, odnosno tokom neformalne istrage u državama koje imaju policijsku istragu/tužilačko-policijsku istragu, bez podele na dve istražne faze, kao što je to slučaj u našem krivičnom postupku.

Kada se radi o krivičnom postupku Srbije, operativni podaci su s jedne strane, isključivo vezani za predistražni postupak, dok s druge strane, oni načelno ni ne smeju dospeti u kasnije stadijume krivičnog postupka, niti kao takvi, ako bi greškom ipak bili/ostali u spisima predmeta u kasnijim procesnim fazama (naročito onim sudskim), oni ostvaruju bilo kakav dokazni značaj. Međutim, onda kada su informacije proizišle iz nadzora komunikacije ostvarene korišćenjem aplikacija za kriptovanje, već uvedene u krivični postupak, te predložene/korišćene od strane javnih tužilaca kao dokazi na kojima se temelji određeni procesno relevantan stepen sumnje, ili su čak od strane suda prihvaćeni u nekim procesnim stadijumima (poput kontrole optužnice), kao dokazi, oni nakon toga, više ne mogu da budu „transformisani“ u operativne podatke, već se o njima svakako mora *dokazno rezonovati* prema opštom dokaznim pravilima. To znači da se tada prema stavu suda, utemeljenom na slobodnoj oceni dokaza i slobodnom uverenju, te uz postupanje po svim ostalim opštim dokaznim pravilima, takve informacije/dokazi procesno-dokazno vrednuju, iz čega potom, proizlazi da se kao ishod takvog vrednovanja; može jedino raditi; bilo o *pravno valjanim dokazima*, bilo o *pravno nevaljanim dokazima*, sa svim procesnim konsekvencama koje iz toga proizlaze. Ovde je posebno značajno da bi onda kada se oceni da su u pitanju pravno nevaljani/nezakoniti dokazi, to moglo da ima i veoma dalekosežne posledice skopčane sa dokaznom koncepcijom o „plodovima otrovnog drveta“. Čini se da se to najčešće gubi iz vida kada se problematika operativnih podataka povezuje sa informacijama koje su kao potencijalni ili aktuelni dokazi (zavisno od toga da li su samo predloženi od strane javnog tužioca „kao dokaz“, ili su već prihvaćeni kao dokaz od suda u određenom procesnom stadijumu), već uveliko uvedene u sudske faze krivičnog postupka.

Konačno, samo vreme (koje je i ovde, kao i inače, svojevrsno „majstorsko rešeto“), u kojem će se realizovati i buduća sudska praksa (čije se osnovne konture donekle naziru već sada), a pre svega stavovi najviših sudova konkretnih država, pa i stavovi srpskih sudova, pokazaće kakav je realan značaj, pa i stepen relevantnosti niza faktora, koji bi načelno mogli imati uticaj na dokaznu verodostojnost takvih informacija/dokaza, proisteklih iz veoma specifičnih istražnih metoda. Takva sudska praksa koja će se ticati (de)šifrovane tajne/zaštićene komunikacije, korišćenjem posebnih aplikacija za kriptovanje razgovora/razmene informacija tokom komuniciranja, u pravnim državama zasnovanim na vladavini prava, kao i inače, mora nastati i delovati u zakonito i pravično sprovedenim krivičnim postupcima.

LITERATURA

- Aleksić Ž., Škulić M. (2020). *Kriminalistika*, 11. izmenjeno i dopunjeno izdanje. Beograd.
- Ambos K. (2018). *Internationales Strafrecht – Strafanwendungsrecht, Völkerstrafrecht, Europäisches Strafrecht, Rechtshilfe*, 5. Auflage. München.
- Bajović V. (2022). EncroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku, *Crimen*, 2.
- Beulke W. (2000). *Strafprozessrecht*. Heidelberg.
- Beulke W., Swoboda S. (2020). *Strafprozessrecht*, 15. Neu bearbeitete Auflage. Heidelberg.
- Brodag W. D. (2001). *Kriminalistik – Grundlagen der Verbrechenbekämpfung*. Stuttgart, München.
- Vasiljević, T. (1981). *Sistem krivičnog procesnog prava SFRJ*, 3. izmenjeno i dopunjeno izdanje. Beograd.
- Damaška M. (1960). Procesne posledice upotrebe dokaza dobivenih na nedozvoljen način, *Naša zakonitost*, 3–6.
- Diehl J., Lehberger R, Meyer-Heuer C. *Landgericht Berlin lässt Encrochat-Daten nicht zu*. <https://www.spiegel.de/panorama/justiz/berlin-landgericht-laesst-encrochat-daten-nicht-zu-a-6dd9be2e-f558-40fa-9995-2f8136581f8e>, 14. septembar 2023.
- Fletcher M., Löff R, Gilmore B. (2008). *Eu Criminal Law and Justice*. Cheltenham, Northampton.
- Goodwin B. *French supreme court dismisses legal challenge to EncroChat cryptophone evidence*. <https://www.computerweekly.com/news/366551078/French-supreme-court-dismisses-legal-challenge-to-EncroChat-cryptophone-evidence>, 27. mart 2024.
- Goodwin B. *Italian Supreme Court calls for prosecutors to disclose information on Sky ECC hacking operation*. <https://www.computerweekly.com/news/252525734/Italian-Supreme-Court-calls-for-prosecutors-to-disclose-information-on-Sky-ECC-hacking-operation>, 28. mart 2024.
- Grubač M. (2002). *Krivično procesno pravo – Uvod i opšti deo*, 2. izmenjeno i dopunjeno izdanje. Beograd.
- Grupa autora (2023). *Izdavanje nezakonito pribavljenih dokaza u krivičnom postupku – principi iz prakse Evropskog suda za ljudska prava i sudska praksa u Crnoj Gori*, ur. T. Gorjanc Prelević. Podgorica.
- Gutkes O. *Digital Evidence in Criminal Law*. https://www.ecba.org/extdocserv/conferences/tallinn2012/recdev_france.pdf, 6. april 2024.

- Kaiser S. (1999). *Die Drei-Stufen-Theorie zur Bestimmung von Beweisverboten im Strafprozess?* Frankfurt, Berlin.
- Marković B. (1937). *Udžbenik sudskog krivičnog postupka Kraljevine Jugoslavije*. Beograd.
- Miljuš I. (2022). *Načelo jednakosti „oružja“ u krivičnom postupku*. Beograd.
- Oerlemans J. J., van Toor D. A. G. (2022). Legal Aspects of the EncroChat Operation: A Human Rights Perspective, *European Journal of Crime, Criminal Law and Criminal Justice*, 30. Online Publication Date: 27 Dec 2022. https://brill.com/view/journals/eccl/30/3-4/article-p309_006.xml?language=en, 22. januar 2024.
- Roxin C. (1998). *Strafverfahrensrecht*, 25. Auflage. München.
- Roxin C., Schöneman B. (2017). *Strafverfahrensrecht*, 29. Auflage. München.
- Satzger H. (2018). *Internationales und Europäisches Strafrecht – Strafanwendungsrecht, Europäisches Straf- und Strafverfahrensrecht, Völkerstrafrecht*, 8. Auflage. Baden, Baden.
- Schaefer K. (1976). *Strafprozessrecht – Eine Einführung*. Berlin, New York.
- Scheb J. M. (1999). *Criminal Law and Procedure*. Belmont, Bonn, Boston, Washington.
- Stojanović Z. (2018). *Međunarodno krivično pravo*, 12. izdanje. Beograd.
- Stojanović Z., Škulić, M., Delibašić V. (2018). *Osnovi krivičnog prava, Knjiga II – Krivično procesno pravo – Krivični postupak kroz praktičnu primenu*. Beograd.
- Čavoški K. (2017). *O pravdi i pravičnosti*. Beograd.
- Škulić M. (2009). *Komentar Zakonika o krivičnom postupku Crne Gore*. Podgorica.
- Škulić M. (2012). *Krivično procesno pravo*. Podgorica.
- Škulić M. (2012). *Začeci evropskog krivičnog procesnog prava, Zbornik škole prava Evropske unije, III sesija*. Podgorica.
- Škulić M. (2022). *Krivično procesno pravo*, 13. izdanje. Beograd.
- Škulić M. (2022). *Međunarodno krivično pravo – prostorno važenje krivičnog prava, krivično pravo međunarodnog porekla, međunarodna krivičnopravna pomoć, začeci krivičnog prava EU*. Beograd.
- Škulić M. (2022). *Kriminalistika*. Beograd.
- Škulić M. (2022). *Međunarodno krivično pravo*. Beograd.
- Škulić M. (2023). *Osnovi krivičnog prava Sjedinjenih Američkih Država*, 2. izmenjeno i dopunjeno izdanje. Beograd.
- Škulić M., Bugarski, T. (2015). *Krivično procesno pravo*. Novi Sad.
- Ulsamer G. (hrsg.) (1996). *Lexikon des Rechts – Strafrecht – Strafverfahrensrecht*, 2. überarbeitete und erweiterte Auflage.
- Wahl T. *EnchroChat Turns into a Case for the CJEU*. <https://eucrim.eu/news/encrochat-turns-into-a-case-for-the-cjeu/>, 29. septembar 2023.
- Walder H. (1965). *Die Vernehmung des Beschuldigten*. Hamburg.

Milan Škulić*

EVIDENTIAL SIGNIFICANCE OF INFORMATION FROM
COMMUNICATIONS OBTAINED BY ENCRYPTION
APPLICATION/MODIFIED DEVICES –
SUCH AS *SKY ECC* AND *ENCHROCHAT*

SUMMARY

In the article is presented one view of information and potential evidence from communication, obtained using special devices and applications for encryption of communication. In particular, the phenomenon of the *Sky ECC* application is explained, which is not only the most commented on in the media, but is current in a whole series of current criminal proceedings, especially in the sphere of organized crime, both in Serbia and throughout Europe, but also in the world in general.

After analysing the basic evidentiary rules in the positive criminal procedural legislation of Serbia, which in principle could be important when it comes to the evaluation of the evidentiary credibility of information derived from communication made with special applications for encryption of conversations, in the article are explained relevant examples from the comparative judicial practice of a number of European countries. Very current cases of this type that were resolved in Serbia were also explained. The practice of the European Court of Human Rights, which concerns the possible violation of the right to privacy due to the interception of communications made with special applications, was also analysed. Special attention was given to the opinion of the General advocate who acts before the Court of Justice of the European Union in relation to a series of questions that the Regional Court in Berlin put to that court, which concern the information resulting from the application of the European investigative warrant, which was previously obtained in France by a special operative– tactical ways to collect data from communications encrypted by the *EnchroChat* application.

In conclusion, it is emphasized that there is no miracle recipe that will absolutely solve all evidentiary problems that arise or may arise when dealing with information from communications made with special applications for encryption of conversations. The time in which the future judicial practice will be implemented (the basic contours of which can already be seen relatively clearly), and above all the positions of the highest courts of specific countries, including the positions of the Serbian courts, will show the real importance and the degree of relevance of a number of factors, which could in principle have an impact on the evidentiary credibility of such information/evidence. Of course, such judicial practice, as usual, the practice of courts in the legal environment of the rule of law, must arise in legally and fairly conducted criminal procedures.

Key words: Evidence, Encrypted Communication, *Sky ECC*, Criminal Procedure, Comparative Law, European Court of Human Rights, EU Court of Justice

* Faculty of Law, University of Belgrade, Judge of the Constitutional Court of Serbia, *skulic@ius.bg.ac.rs*