UDK 343.14
Pregledni znanstveni rad
Rukopis primljen 7. travnja 2026.
Rukopis prihvaćen 29. travnja 2026.

Marijana Jurić Vukašin
Ured za suzbijanje korupcije i organiziranog kriminaliteta
Ulica kneza Branimira 4, 10 000 Zagreb
ORCiD: https://orcid.org/0009-0001-0009-1649
marijana.juricvukasin@uskok.dorh.hr

Sven Mišković
Ured za suzbijanje korupcije i organiziranog kriminaliteta
Ulica kneza Branimira 4, 10 000 Zagreb
ORCiD: https://orcid.org/0009-0001-1152-2694
sven.miskovic@uskok.dorh.hr

DOKAZI KRIPTIRANOM KOMUNIKACIJOM SKY ECC I ANOM

SAŽETAK

U radu se objašnjava što su elektronički dokazi u kaznenom zakonodavstvu Republike Hrvatske, kakvo je njihovo pribavljanje, način izvođenja u sudskim postupcima te njihova važnost u kaznenom postupku. Također se objašnjava pojam enkripcije te dosad poznati podaci povezani s aplikacijama za kriptiranu komunikaciju EncroChat, Sky ECC i ANOM. Analizira se način pribavljanja navedenih dokaza preko europskih istražnih naloga i zamolnica za međunarodnu pravnu pomoć, a koji su preneseni u Republiku Hrvatsku radi pokretanja i vođenja kaznenih postupaka. Prikazano je trenutačno stanje kaznenih postupaka u Republici Hrvatskoj povezano s dokazima koji se odnose na komunikaciju u aplikacijama za kriptiranu komunikaciju Sky ECC i ANOM te postupanje Ureda za suzbijanje korupcije i organiziranog kriminaliteta u navedenim predmetima od trenutka zaprimanja informacija da su pojedine osobe u svojoj kriminalnoj djelatnosti upotrebljavale navedene aplikacije, u vidu davanja kronologije i mehanizma pribavljanja podataka putem europskih istražnih naloga od Republike Francuske u odnosu na aplikaciju za kriptiranu komunikaciju Sky ECC odnosno putem međunarodne pravne pomoći od Sjedinjenih Američkih Država za aplikaciju za kriptiranu komunikaciju ANOM. Nadalje, daje se prikaz broja kaznenih predmeta koji su trenutačno formirani u Republici Hrvatskoj i u kojima se upotrebljavaju navedeni dokazi te dosad donesene sudske odluke povodom prigovora na zakonitost navedenih dokaza, i to uzimajući u obzir stajališta Suda Europske unije. Zaključno, u radu se daje kratak pregled usporedne sudske prakse u drugim državama članicama Europske unije, ali i državama regije.

Ključne riječi: digitalni dokaz, enkripcija, aplikacije za kriptiranu komunikaciju, EncroChat, ANOM, Sky ECC, međunarodna suradnja

1. Uvod

Kako tehnologija napreduje, tako napreduje i način na koji se pravosuđe suočava s dokazima u kaznenim postupcima. Elektronički dokazi, koji uključuju podatke sačuvane ili prenesene u digitalnom obliku, postali su ključan dio mnogih kaznenih istraga. Poruke s mobilnih telefona, e-pošta, digitalni zapisi i slično sada se rutinski upotrebljavaju kao dokaz u sudnicama. Međutim, dok elektronički dokazi pružaju nove mogućnosti za provođenje istraga i procesuiranje kaznenih djela i počinitelja, oni također postavljaju niz novih izazova – uključujući pitanja o privatnosti, sigurnosti podataka i zakonitosti prikupljanja te uporabe takvih dokaza.

Elektronički dokaz informacija je pohranjena ili prenesena u binarnom obliku[1] koju je moguće izvesti kao dokazni materijal u kaznenom postupku na sudu, s tim da hrvatski Zakon o kaznenom postupku[2] (dalje: Zakon o kaznenom postupku) ne sadržava jasnu definiciju elektroničkoga dokaza.[3] Elektronički dokazi vrlo su važni jer predstavljaju kombinaciju različitih informacija poput teksta, slike, audiosnimke i videosnimke. Prema nekim procjenama 85 % istraga kaznenih djela uključuje elektroničke dokaze u određenom obliku.[4] Elektronički dokazi jedna su vrsta materijalnih dokaza bez obzira na činjenicu što ih je teže evidentirati. U odnosu na materijalne dokaze elektronički dokazi imaju više prednosti. Naime, od elektroničkih je dokaza moguće načiniti točnu kopiju koja se naknadno može istraživati kao da je riječ o originalu, dok je kod materijalnih dokaza to gotovo nemoguće. Pri ispitivanju kopije, a ne originala, izbjegavaju se oštećenja koja bi mogla nastati na originalu tijekom istraživanja. S pomoću forenzičkih alata moguće je vrlo lako odrediti je li elektronički dokaz modificiran ili uništen, pri čemu je elektroničke dokaze vrlo teško uništiti. Naime, čak i kada su „obrisani", elektronički se dokazi u većini slučajeva mogu vratiti. Važnost elektroničkih dokaza i potreba njihove daljnje regulacije prepoznata je i na europskoj razini uz usvajanje tzv. e-evidence paketa

[1] European Commission, „European Evidence Project, European Data Informatics Exchange Framework for Courts and Evidence", dostupno na www.cordis.europa.eu/project/id/608185/reporting/de.

[2] Zakon o kaznenom postupku („Narodne novine" broj 152/2008., 76/2009., 80/2011., 121/2011. – službeni pročišćeni tekst, 91/2012., 143/2012., 56/2013., 145/2013., 152/2014., 70/2017., 126/2019., 126/2019., 80/2022., 36/2024., 72/2025., 13/2026.).

[3] Konkretno, u članku 202. stavku 33. Zakona o kaznenom postupku propisano je da je elektronički (digitalni) dokaz podatak koji je kao dokaz u elektroničkom (digitalnom) obliku pribavljen prema Zakonu o kaznenom postupku.

[4] Vijeće Europske unije, „Bolji pristup e-dokazima u cilju borbe protiv kriminala", dostupno na https://www.consilium.europa.eu/hr/policies/e-evidence/#e-evidence.

koji uključuje Uredbu (EU) 2023/1543[5] i Direktivu (EU) 2023/1544.[6] Uvođenjem novih europskih instrumenata uspostavljaju se temelji za budućnost daljnjeg razvoja pravosudne suradnje u kaznenim stvarima, osobito uz odredbe kojima je naglašena irelevantnost lokacije podataka i nastojanja uspostave izravnog odnosa između države koja podnosi zahtjev i pružatelja usluga.[7] Republika Hrvatska preuzela je navedene instrumente u svoj zakonski okvir uz hrvatski Zakon o prekograničnom pribavljanju elektroničkih dokaza u kaznenim postupcima[8] (dalje: Zakon o prekograničnom pribavljanju elektroničkih dokaza u kaznenim postupcima) koji je stupio na snagu 18. veljače 2026., osim u odredbi glave II. te članaka 17. i 18., koji stupaju na snagu 18. kolovoza 2026., u isto vrijeme kao i Uredba (EU) 2023/1543.

U vezi s pribavljanjem elektroničkog dokaza valja istaknuti kako odredba članka 331. Zakona o kaznenom postupku propisuje da se elektronički (digitalni) dokaz pribavlja primjenom odredaba članka 257., članka 262. i članka 263. Zakona o kaznenom postupku odnosno u okviru dokazne radnje pretrage pokretnih stvari (članka 257.) i dokazne radnje privremenog oduzimanja predmeta (članka 262. i članka 263.). Kako je prethodno spomenuto, Zakonom o prekograničnom pribavljanju elektroničkih dokaza u kaznenim postupcima uspostavlja se novi okvir suradnje s drugim državama članicama Europske unije uvođenjem europskih naloga za dostavljanje i čuvanje elektroničkih dokaza. Međutim, kako glava II. Zakona, kojom je regulirana provedba Uredbe (EU) 2023/1543, stupa na snagu tek 18. kolovoza 2026., ostaje vidjeti hoće li primjena novih pravila uistinu olakšati suradnju i učvrstiti zakonske okvire glede elektroničkih dokaza. U svakom slučaju, prikupljanje elektroničkih dokaza stvara nove izazove za tijela kaznenog progona, pri čemu valja imati u vidu da se dokazne radnje koje se provode u tom pravcu prilagođavaju okolnosti slučaja.

---

5 Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalozima za dostavljanje i europskim nalozima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka. Važno je naglasiti da je u članku 3. stavku 8. navedene Uredbe prvi put izričito u europskoj legislativi propisana definicija elektroničkih dokaza – „podaci o pretplatniku, podaci o prometu ili podaci o sadržaju koje je pohranio pružatelj usluga ili koji su pohranjeni u njegovo ime u elektroničkom obliku u trenutku primitka potvrde europskog naloga za dostavljanje (EPOC) ili potvrde europskog naloga za čuvanje (EPOC-PR)". Uredba je dostupna na https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32023R1543.

6 Direktiva (EU) 2023/1544 Europskog parlamenta i Vijeća od 12. srpnja 2023. o utvrđivanju usklađenih pravila za imenovanje imenovanih subjekata koji imaju poslovni nastan i za imenovanje pravnih zastupnika za potrebe prikupljanja elektroničkih dokaza u kaznenim postupcima.

7 Forlani, Gianluca, *The E-evidence Package, The Happy Ending of a Long Negotiation Saga*, Eucrim Issue 2/2023, 2023., str. 174–181.

8 Zakon o prekograničnom pribavljanju elektroničkih dokaza u kaznenim postupcima („Narodne novine" broj 151/2025.).

U odnosu na izvođenje elektroničkih dokaza valja navesti kako u tom pogledu vrijedi opće pravilo o izvođenju elektroničkih dokaza koje je utvrđeno odredbom članka 430. Zakona o kaznenom postupku, koja propisuje da se elektronički dokazi izvode na način uređen u člancima 329. do 331. Zakona o kaznenom postupku odnosno kao dokaz ispravom, i to čitanjem ili pregledavanjem, te kao dokaz snimkom odnosno reproduciranjem.[9]

Kada je riječ o dokazima u vezi s kriptiranim uređajima, ponajprije moramo imati u vidu pojam enkripcije. Naime, etimologija nas uči da je riječ *enkripcija* nastala od engleske riječi *encryption* i ima značenje šifriranja.[10] Enkripciju možemo promatrati kao proces kojim se podaci ili poruke čine nečitljivim za one koji nemaju određeno znanje ili ključ. Postoje tri osnovne vrste enkripcije: simetrična enkripcija, asimetrična enkripcija i kriptografske *hash*-funkcije.[11] Kod simetrične enkripcije i za šifriranje i za dešifriranje upotrebljava se ista šifra (ključ).[12] Taj ključ mora biti poznat i pošiljatelju i primatelju poruke, ali nikomu drugomu. Simetrična enkripcija brža je i jednostavnija od asimetrične, ali ima problem sigurnoga prijenosa ključa, dok kod asimetrične enkripcije postoji poseban ključ samo za šifriranje i drugi koji služi samo za dešifriranje. Oba ključa nazivaju se još javni i privatni ključ. Javni ključ može se dijeliti s bilo kim, a privatni ključ vlasnik drži u tajnosti.[13] Asimetrična je enkripcija sigurnija i omogućava digitalno potpisivanje poruka, ali je sporija i složenija od simetrične.[14] Kriptografske *hash*-funkcije rade različito u usporedbi sa simetričnim ili asimetričnim šifriranjem po tome što ne upotrebljavaju ključ za šifriranje podataka. Umjesto toga kriptografske *hash*-funkcije primjenjuju algoritam koji se pokreće na datotekama, lozinkama ili drugim podacima za izradu kontrolnog zbroja fiksne duljine koji se zauzvrat može upotrebljavati za provjeru autentičnosti šifriranog sadržaja.[15] Za cjelokupno razumijevanje enkripcije i daljnju raspravu o izazovima za tijela kaznenog progona i kazneno pravosuđe u vezi s njezinom kriminalnom uporabom bitno je razlikovati enkripciju koja se upotrebljava za podatke u prijenosu i enkripciju koja

[9] Garačić, Ana, Novosel, Dragan, *Zakon o kaznenom postupku u sudskoj praksi, Knjiga II., Glava XX. – Glava XXXI.,* Libertin naklada, Rijeka, 2018., str. 124.

[10] *Oxford Dictionary*, https://www.oxfordlearnersdictionaries.com/definition/english/encryption#google_vignette, pristupljeno 31. ožujka 2026.

[11] Stallings, William, *Cryptography and Network Security: Principles and Practice*, 7. izdanje, Pearson Education, 2017., str. 3.

[12] *Ibid*., str. 62.

[13] EU Innovation Hub, „First report on encryption by the EU Innovation Hub for internal security, Publications Office of the European Union" (EU Innovation Hub, 2024.), dostupno na https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf.

[14] *Op. cit.* 11, str. 8.

[15] *Ibid*., str. 328.

se upotrebljava za pohranjene podatke – podatke u mirovanju. Šifriranje odnosno enkripcija podataka u prijenosu odnosi se na postupak uporabe enkripcije za zaštitu informacija dok se prenosi s jednog uređaja na drugi. Takva enkripcija sprečava pristup neovlaštenoj trećoj strani i onemogućuje presretanje ili mijenjanje podataka (mrežni promet, tekst poruke, sadržaj unesen u mrežni obrazac ili e-pošta) dok podaci putuju do odredišta preko mreže. Enkripcija za podatke u mirovanju usmjerena je na osiguranje podataka dok su pohranjeni na uređaju ili na poslužitelju. Takva enkripcija može se upotrijebiti za zaštitu datoteke ili cijelog diska.[16]

2. Aplikacije za kriptiranu komunikaciju

Razvoj suvremenih informacijsko-komunikacijskih tehnologija usavršio je i razgranao različite modalitete razmjene informacija među ljudima, pa tako i među potencijalnim počiniteljima kaznenih djela. Tzv. kriptirani uređaji i šifrirana komunikacija upotrebljavaju se jednako u svakodnevnom dijalogu i razmjeni običnih poruka, ali i pri planiranju i počinjenju kaznenih djela. Relativno noviji slučajevi EncroChat, Sky Elliptic-Curve Cryptography (dalje: Sky ECC) i ANOM svojom pojavom izazvali su polemike pri prosuđivanju udovoljava li dokazni materijal u javnom interesu propisanim zakonskim uvjetima da bi određeni segmenti tog materijala bili označeni kao zakoniti dokazi.

Dokazi prikupljeni kriptiranom komunikacijom iz aplikacija Sky ECC i ANOM predstavljaju prekretnicu u borbi protiv organiziranog kriminala u Hrvatskoj, ali i državama regije.[17]

2.1. EncroChat

EncroChat bio je nizozemsko trgovačko društvo sa središnjim poslužiteljem u Francuskoj, u Roubaixu, te je nudio modificirane pametne telefone koji omogućuju

[16] Kanani, Ishva Jitendrakumar, *Securing Data in Motion and at Rest: A Cryptographic Framework for Cloud Security*, International Journal of Science and Research Vol. 9(2), 2020., str. 1965–1968.

[17] Prema podacima iz 2022. u državama zapadnoga Balkana aplikacija Sky ECC pružila je vrijedne informacije glede postojećih kriminalnih skupina, ali je pomogla i u otkrivanju novih. Tako je presretanje poruka otkrilo postojanje zločinačkog udruženja za koje postoji sumnja da je krijumčarilo drogu i oružje iz Albanije i Crne Gore u Bosnu i Hercegovinu, a zatim dalje u države Europske unije – među kojima i u Hrvatsku, Sloveniju, Mađarsku i Njemačku. U Republici Srbiji s pomoću podataka dobivenih preko aplikacije Sky ECC otkrivena su kaznena djela dvojice vodećih pripadnika kriminalnih skupina, a upravo ti podaci služili su boljem razumijevanju načina i opsega njihova djelovanja. Vidi više u: Global Initiative Against Transnational Organized Crime, „Decryption of messaging app provides valuable insight into criminal activities in the Western Balkans and beyond", https://riskbulletins.globalinitiative.net/see-obs-013/01-decryption-of-messaging-app-criminal-activities.html, pristupljeno 31. ožujka 2026.

šifriranu komunikaciju među pretplatnicima. Upotrebljavali su ga ponajprije pripadnici organiziranih kriminalnih skupina za planiranje kriminalnih aktivnosti.

EncroChat uređaji pojavili su se 2016. te su se brzo proširili tijekom svoje četiri i pol godine postojanja, pa je mreža na kraju dosegnula procijenjenih 60 000 pretplatnika u vrijeme zatvaranja trgovačkoga društva u lipnju 2020. Naime, policija se infiltrirala u mrežu između ožujka i lipnja 2020. tijekom istrage diljem Europe. Neidentificirani izvor povezan s EncroChatom objavio je u noći s 12. na 13. lipnja 2020. da će tvrtka prestati s radom zbog policijske akcije.[18]

Prema dostupnim podacima uređaji su se prodavali s unaprijed instaliranim aplikacijama te su bili posebno popularni u Europi iako su se prodavali i na Bliskom istoku i drugdje u svijetu. U srpnju 2020. objavljeno je da je cijena uređaja prvo bila 1000 eura (900 britanskih funti), a zatim 1500 eura (1350 britanskih funti) za šestomjesečni ugovor za uporabu EncroChatove usluge.[19]

Francuska je 2020. osnovala zajednički istražni tim s Nizozemskom čiji je cilj bio demontirati šifriranu telefonsku mrežu koju upotrebljavaju kriminalci. Istraga je omogućila obradu prikupljenih podataka u skladu s francuskim zakonodavstvom i sudskom dozvolom prateći okvire za međunarodnu pravosudnu i policijsku suradnju. To je bilo moguće zahvaljujući članu 706-102-1 francuskog Zakona o kaznenom postupku koji dozvoljava postavljanje tehničkih uređaja za pristupanje, snimanje, skladištenje i prijenos računalnih podataka bez suglasnosti zainteresiranih strana radi učinkovitijeg provođenja istraga u kaznenim predmetima u slučajevima organiziranog kriminala.[20]

2.2. Sky ECC

Trgovačko društvo Sky Global komunikacijska je mreža i pružatelj usluga osnovan 2008. u Vancouveru, Kanada. Razvilo je najveću svjetsku mrežu šifriranih poruka pod nazivom Sky ECC, koja je radila preko tri poslužitelja tvrtke OVHcloud u Roubaixu u Francuskoj. Kao i sve ostale aplikacije za sigurno dopisivanje, bila je namijenjena svima zainteresiranima za maksimalnu sigurnost i privatnost, a da bi aplikacija to omogućila, trebalo ju je upotrebljavati uz odgovarajući modificirani uređaj te je postojala i licencija koja je omogućavala uporabu aplikacije na određeno

[18] Wright, Robert, „Across Europe as French Police Crack Encrypted Network" (Financial Times, 2. srpnja 2020.), https://www.ft.com/content/7006913f-be3d-49b5-8ba7-7c5b78b551b2?syn-25a6b1a6=1, pristupljeno 5. travnja 2026.

[19] Europol, „Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" (Europol, 2. srpnja 2020.), https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, pristupljeno 5. svibnja 2026.

[20] *Ibid.*

vrijeme (tri, šest ili više mjeseci). Cijena licencije prema dostupnim podacima bila je od 600 do 2200 eura. Naime, navedena aplikacija izvorno je razvijena za platformu BlackBerry, međutim s vremenom je navedena aplikacija instalirana i na uređajima Nokia, Google i Apple. Jedna od značajki aplikacije bilo je „samouništenje" poruka nakon vremena koje definira korisnik, a ako mreža nije mogla pristupiti telefonu, poruke bi se čuvale do 48 sati i zatim se izbrisale.[21]

Telefoni su imali i prekidač za isključivanje – ako bi korisnik unio „panic" lozinku, uređaj bi izbrisao njezin sadržaj. Na telefonima na kojima je bila instalirana navedena aplikacija bile su onemogućene kamere, mikrofoni i GPS. Interes za nadzor nad Sky ECC-jem pojavio se kod belgijskih nadležnih tijela nakon što su uvidjeli da su uređaji osumnjičenika zaplijenjeni tijekom njihovih akcija imali tu aplikaciju. U ožujku 2021. Agencija Europske unije za suradnju tijela za izvršavanje zakonodavstva (dalje: EUROPOL) objavila je da je zajednički istražni tim sastavljen od belgijskih, francuskih i nizozemskih policijskih vlasti pratio razmjenu poruka više od 70 000 korisnika Sky ECC-ja i na sigurnom mjestu pohranio odgovarajući sadržaj dobiven presretanjem komunikacija.[22]

Nakon zajedničke operacije nadležna francuska tijela kaznenog progona dostavila su opsežan set podataka pojedinim europskim državama.

Prema informacijama iz njemačkog kaznenog postupka francuski sud u Lilleu, isti kao i onaj u slučaju EncroChat, odobrio je presretanje komunikacije s poslužitelja koji je smješten, kao i u slučaju EncroChat, u Roubaixu (Francuska).[23]

Svaki korisnik Sky ECC-jeve kriptirane komunikacijske platforme pri registraciji na platformu dobivao je jedinstvenu oznaku (userID) i PIN koji ostaje nepromijenjen. Osim toga, svaki korisnik mogao je odabrati korisničko ime koje se moglo promijeniti u bilo kojem trenutku, pa je jedna osoba mogla upotrebljavati isti PIN s različitim korisničkim imenima. Dana 9. ožujka 2021. belgijska policija izvela je oko 200 racija, uhitila 48 osoba i zaplijenila 1,2 milijuna eura u gotovini.[24] Samo su u Belgiji, zaključno s podacima iz ožujka 2022., informacije izdvojene iz komunikacije

[21] Oerlemans, Jan-Jaap, *The Future of Data-Driven Investigations in Light of the Sky ECC Operation*, New Journal of European Criminal Law Vol. 14(4), 2023., str. 2 i 3.

[22] Europol, „New major interventions to block encrypted communications of criminal networks" (Europol, 12. ožujka 2021.), https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks, pristupljeno 5. travnja 2026.

[23] Odluka Saveznog vrhovnog suda Savezne Republike Njemačke od 2. ožujka 2022., broj 5 StR 457/21, para. 11, https://www.bundesgerichtshof.de/SharedDocs/Entscheidungen/DE/Strafsenate/5_StS/2021/5_StR_457-21.pdf?__blob=publicationFile&v=1, pristupljeno 6. travnja 2026.

[24] Organized Crime and Corruption Reporting Project, „Police Arrest 48 After Hacking Cryptophones in Belgium, Netherlands" (Organized Crime and Corruption Reporting Project, 12. ožujka 2021.),

preko aplikacije Sky ECC pružile dokaze za 118 postojećih predmeta, dovele do otvaranja 276 novih istraga i identifikacije čak 888 osumnjičenika. Također, zaplijenjeno je više od 90 tona droge procijenjene vrijednosti od 4,5 milijarde eura te novac i roba u vrijednosti od gotovo 60 milijuna eura.[25]

2.3. ANOM

Operacija ANOM, poznata kao „Trojanski štit" (izvorno *Operation Trojan Shield*), rezultat je suradnje agencija za provođenje zakona iz nekoliko država u operaciji koja se odvijala od 2019. do 2021. godine. U okviru te suradnje došlo je do presretanja milijuna poslanih poruka preko „sigurne aplikacije za razmjenu poruka" ANOM. Uslugu ANOM naširoko su upotrebljavali kriminalci, ali umjesto pružanja sigurne komunikacije ona je zapravo bila trojanski konj koji su razvili Savezni istražni ured Sjedinjenih Američkih Država (dalje: FBI) i Australska savezna policija (dalje: AFP).[26]

Godine 2018. uhićen je Vincent Ramos, osnivač i izvršni direktor kriptiranog *messengera* Phantom Secure, koji su upotrebljavale organizirane kriminalne skupine. Nakon toga FBI je razvio ANOM u suradnji s povjerljivim ljudskim izvorom koji je prethodno radio na *messengeru* Phantom Secure.[27] FBI pokrenuo je operaciju Trojanski štit, koja je uključivala distribuciju navodno sigurne aplikacije diljem svijeta uz pomoć navedenog hakera, među ostalim, s australskim vlastima. Softver ANOM prodan je u više od 90 zemalja, a najviše se upotrebljavao u Njemačkoj, Nizozemskoj, Španjolskoj, Australiji i Srbiji. Moglo se dobiti više od 20 milijuna poruka s više od 11 800 uređaja. „Pretplata" za uporabu uređaja ANOM u Europi je iznosila otprilike 1000 do 1500 eura za šestomjesečno razdoblje. FBI se u ljeto 2019. obratio nepoznatoj trećoj (europskoj) državi koja je postavila vlastiti server i omogućila FBI-u da

https://www.occrp.org/en/news/police-arrest-48-after-hacking-cryptophones-in-belgium-netherlands, pristupljeno 5. travnja 2026.

[25] U: Global Initiative Against Transnational Organized Crime, „Decryption of messaging app provides valuable insight into criminal activities in the Western Balkans and beyond", koji se poziva na *HAA, Eén jaar na operatie Sky: al 888 verdachten geïdentificeerd en drugs ter waarde van 4,5 miljard euro in beslag genomen, De Morgen, 9 March 2022* (bilješka 9), https://riskbulletins.globalinitiative.net/see-obs-013/01-decryption-of-messaging-app-criminal-activities.html, pristupljeno 31. ožujka 2026.

[26] Europol, „800 criminals arrested in biggest ever law enforcement operation against encrypted communication" (Europol, 8. lipnja 2021.), https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication, pristupljeno 5. travnja 2026.

[27] Computer Weekly, „FBI planned a sting against An0m cryptophone users over drinks with Australian investigators" (Computer Weekly, 11. lipnja 2021.), https://www.computerweekly.com/news/252502260/FBI-planned-a-sting-against-An0m-cryptophone-users-over-drinks-with-Australian-investigators,

pristupljeno 27. svibnja 2026.

prima nove podatke sa servera ANOM putem sudskog naloga u okviru uzajamne pravne pomoći. Naime, softver na kriptotelefonima bio je programiran tako da se kopija svake poslane poruke potajno šalje na poslužitelj izvan Sjedinjenih Američkih Država koji se nalazio u nepoznatoj trećoj zemlji, gdje se prvo dekriptirao, a zatim ponovno šifrirao i prosljeđivao sljedećem poslužitelju. Ostale zemlje, iako su bile uključene u tekuću operaciju, bile su obaviještene u prilično kasnoj fazi operacije. Prema zasad dostupnim podacima uređaji ANOM imali su aplikaciju za razmjenu poruka koja se izvodi na sustavu android. Ti pametni telefoni bili su posebno prilagođeni kako bi onemogućili normalne funkcije kao što su govorna telefonija, e-pošta ili usluge lokacije. Aplikacija se otvarala unosom šifre unutar aplikacije kalkulatora.[28] Nakon sporog početka stopa distribucije ANOM-a porasla je od sredine 2019., do listopada 2019. bilo je nekoliko stotina korisnika, a do svibnja 2021. bilo je 11 800 uređaja s instaliranim ANOM-om. Operacija je kulminirala nalozima za pretragu koji su istodobno izvršeni diljem svijeta 8. lipnja 2021.

3. Postupanje Ureda za suzbijanje korupcije i organiziranog kriminaliteta u kaznenim postupcima u kojima se upotrebljavaju dokazi kriptiranom komunikacijom

Od prosinca 2021. do ožujka 2026. hrvatski Ured za suzbijanje korupcije i organiziranog kriminaliteta (dalje: USKOK) na temelju podnesenih kaznenih prijava i rezultata dokaznih radnji pribavljenih putem pravosudne suradnje s Francuskom i Sjedinjenim Američkim Državama pokrenuo je istrage u 19 predmeta. Od njih je za osam predmeta pred Županijskim sudom u Zagrebu podignuta optužnica, za sedam predmeta optužnica je podignuta pred Županijskim sudom u Splitu, a četiri predmeta još su u fazi istrage.

Individualno gledano riječ je o broju predmeta kojem ne bi trebalo pridavati određenu kvantitativnu vrijednost, međutim valja naglasiti kako je u tih 19 predmeta istragom obuhvaćeno ukupno 176 osoba (pravnih i fizičkih). Inkriminirana kaznena djela povezana su ponajprije s organiziranim kriminalom koji je povezan s krijumčarenjem droge i oružja te s izvršenjem kaznenih djela protiv života i tijela, dok je dio inkriminacija povezan i sa zlouporabom položaja i ovlasti koju su počinile službene osobe.

Osim toga USKOK trenutačno ima četiri predmeta u fazi istrage te veći broj predmeta koji su u fazi izvida tijekom kojih se pribavljaju podaci putem europskih istražnih naloga upućenih Francuskoj za kriptiranu komunikaciju zabilježenu putem

[28] Cox, Joseph, „We Got the Phone the FBI Secretly Sold to Criminals", (Vice, 8. srpnja 2021.) https://www.vice.com/en/article/anom-phone-arcaneos-fbi-backdoor/, pristupljeno 6. travnja 2026.

Sky ECC-ja ili putem međunarodne pravne pomoći od Sjedinjenih Američkih Država za komunikaciju zabilježenu u aplikaciji ANOM.

U vezi s načinom pribavljanja navedenih dokaza valja istaknuti kako su podaci iz aplikacije Sky ECC dobiveni preko izdanih europskih istražnih naloga koje je Republici Francuskoj uputio USKOK, i to tako da su europski istražni nalozi dostavljeni nadležnom pravosudnom tijelu Republike Francuske preko Agencije Europske unije za suradnju u kaznenom pravosuđu (dalje u tekstu: EUROJUST). Nakon toga sadržaj navedene komunikacije USKOK-u je dostavljen na temelju odobrenja nadležnoga francuskog suda u Lilleu.

U odnosu na aplikaciju za kriptiranu komunikaciju ANOM USKOK je informacije i podatke pribavio od nadležnog pravosudnog tijela Sjedinjenih Američkih Država putem međunarodne pravne pomoći, i to tako da je uputio zamolnice preko Ministarstva pravosuđa, uprave i digitalne transformacije Republike Hrvatske nadležnom pravosudnom tijelu Sjedinjenih Američkih Država za pribavljanje sadržaja poruka prema uređajima i iz uređaja ANOM te digitalnih podataka za jedinstvene korisničke identifikatore (dalje: JID) pojedinih naziva. Ministarstvo pravosuđa, uprave i digitalne transformacije Republike Hrvatske od Ministarstva pravosuđa Sjedinjenih Američkih Država zaprimilo je tražene podatke. Naime, Odjel za međunarodne odnose u Ministarstvu pravosuđa Sjedinjenih Američkih Država pribavio je od FBI-a vanjsku jedinicu (engl. *flash drive*) na kojoj se nalazi sadržaj svih komunikacija (tekst i zvuk) prema uređajima i iz uređaja ANOM JID identificiranih kao da pripadaju hrvatskim državljanima i digitalnih podataka za JID-ove određenih naziva.

Europski istražni nalozi odnosno zamolnice za međunarodnu pravnu pomoć sačinjeni su na temelju rezultata izvida koje je proveo USKOK i policijski službenici.

Nadalje, nakon zaprimanja komunikacije preko aplikacija za kriptiranu komunikaciju Sky ECC i ANOM najprije je utvrđen identitet počinitelja kaznenih djela analizom sadržaja te komunikacije, ali i tako da je sadržaj kriptirane komunikacije uspoređen sa svim policiji dostupnim evidencijama poput prelazaka državne granice, lokacijama mobilnih telefona, podataka o korištenju autocesta i sl.

Tijekom predistrage i istrage, osim već navedenih dokaza, pribavljani su i dodatni dokazi uz provedene pretrage osoba, doma i drugih prostorija, osobnih automobila, informatičkih uređaja, provođenjem vještačenja, ispitivanjem svjedoka, a u određenim slučajevima prije početka istrage primjenjivane su i posebne dokazne radnje prema okrivljenicima.

4. Odluke sudova u Republici Hrvatskoj u povodu iznesenih prigovora zakonitosti dokaza kriptiranom komunikacijom SKY ECC i ANOM

Poveznica kaznenih predmeta utemeljenih na Sky ECC-ju i ANOM-u njihov je međunarodni karakter. Drugim riječima, te su međunarodne akcije vrlo važne za Republiku Hrvatsku u dijelu u kojem su njezini državljani dovedeni u vezu s kaznenim djelima obuhvaćenim informacijama i podacima pribavljenim uporabom aplikacija Sky za kriptiranu komunikaciju ECC i ANOM. Stoga je međunarodni karakter pribavljanja tih informacija i podataka ključan za ocjenu mogu li se rezultati tako provedenih radnji upotrijebiti kao dokaz u hrvatskom kaznenom postupku, pri čemu je situacija u slučaju ANOM složenija jer je jedna „nepoznata" država članica Europske unije poslužila kao tampon zona – posrednik u postizanju zakonitosti provedenih radnji. Naime, poslužitelj iBot koji je primao kopiju svake poslane poruke preko aplikacije ANOM nalazio se na teritoriju jedne države članice Europske unije. U toj državi u listopadu 2019. godine izdan je sudski nalog koji je u konačnici omogućio, na temelju bilateralnog ugovora o uzajamnoj pravnoj pomoći između te države i Sjedinjenih Američkih Država, izradu kopije poslužitelja i primanje sadržaja od strane američkih vlasti. Valja naglasiti da je navedena država zahtijevala očuvanje anonimnosti unatoč tomu što su njezini motivi za to nerazjašnjeni.[29]

Nakon što je Ured za suzbijanje korupcije i organiziranog kriminaliteta podignuo optužnice pred Županijskim sudom u Zagrebu i Županijskim sudom u Splitu, sudovi su navedene optužnice dostavili okrivljenicima i njihovim braniteljima na odgovor. U podnesenim odgovorima na optužnice glavnina prigovora odnosi se na zakonitost dokaza pribavljenih putem međunarodne pravne pomoći od Sjedinjenih Američkih Država i europskog istražnog naloga od Francuske s tim da u bitnome iz istih razloga te uz istu argumentaciju osporavaju zakonitost navedenih dokaza.

Naime, okrivljenici i njihovi branitelji u vezi s dokazima koji se odnose na komunikaciju putem aplikacije za kriptiranu komunikaciju Sky ECC u pravilu su isticali kako izostaju dokazi o načinu pribave te načinu utvrđivanja pošiljatelja poruka na aplikacijama za kriptiranu komunikaciju te potrebu utvrđenja sljedivosti dokaza (tzv. *chain of custody*) koja bi trebala pratiti kretanja svakog pojedinog dokaza od njegova prikupljanja i čuvanja, analize i rukovanja s tako prikupljenim dokazom, a dodatno se isticalo da obrani nije omogućen uvid u izvornike hakiranih poruka. Stoga je obrana predlagala da se pribave podaci o tome postoji li sporazum između francuskih i nizozemskih vlasti prema kojem će nizozemske vlasti postupati u odnosu na server

[29] Wahl, Thomas, *What Remains of the ordre public in Transnational Surveillance? A Commentary on the Decisions of the Federal Court of Justice and the Federal Constitutional Court in the ANOM Proceedings,* Eucrim Issue 4/2025, Preprint, str. 2.

Sky ECC-ja, na koji način i primjenom koje tehnologije je došlo do presretanja, tj. ulaska nizozemskih vlasti u sadržaj platforme Sky ECC, je li do presretanja došlo u realnom vremenu ili su iz servera preuzeti već pohranjeni podaci, gdje su i kako čuvani podaci pribavljeni hakiranjem predmetnog servera, kada su i kako šifrirani podaci „prevedeni", tj. dešifrirani, o kojem je softveru riječ i tko ga je izradio, jesu li francuske ili nizozemske vlasti u bilo kojem trenutku tijekom operacije presretanja izvijestile hrvatske vlasti o operaciji, kada su i kako hrvatske vlasti prvi put obaviještene o prepisci svojih državljana i sadržaju te prepiske.

Nadalje je isticano kako su nalozi francuskog suda izdani za potrebe postupka u Francuskoj te se ne odnose na druge postupke, posebice ne u drugim državama Europske unije koje u tom nalogu nisu ni navedene, te da nije poznato na kojim je zakonskim odredbama utemeljeno postupanje francuskih i nizozemskih vlasti pri pristupanju serveru Sky ECC-ja, kako su i primjenom koje tehnologije podaci pribavljeni te je li o provođenju posebnih mjera bilo upoznato nadležno tijelo u Republici Hrvatskoj.

Također, isticano je kako je na temelju naloga francuskog suda provođen tzv. masovni nadzor,[30] radnja koju hrvatsko zakonodavstvo ne poznaje, pa se zbog toga europskim istražnim nalogom nije ni mogla tražiti dostava takva dokaza.

U odnosu na dokaze koji se odnose na komunikaciju preko aplikacije za kriptiranu komunikaciju ANOM okrivljenici i njihovi branitelji u bitnome su navodili identične prigovore koji su isticani i u pogledu komunikacije putem aplikacije za kriptiranu komunikaciju Sky ECC, pa je tako isticano kako je riječ o masovnom praćenju svih korisnika te platforme bez prethodnog utvrđivanja postojanja osnove sumnje u počinjenje kaznenih djela. Navođeno je da je takvo masovno presretanje komunikacije korisnika kriptirane mreže u suprotnosti s hrvatskim kaznenim zakonodavstvom, koje poznaje posebne mjere samo prema konkretnim osobama, i to samo kada postoje osnove sumnje da su počinili konkretna kaznena djela. Nadalje, da je masovno presretanje komunikacije ostvarene preko te kriptirane mreže inače provela strana država na temelju neutvrđenog naloga treće države, da je prijeporan način na koji su presretane i dekriptirane informacije, da je nejasno koji su alati upotrijebljeni za presretanje komunikacije i jesu li takvi alati uopće dopušteni, da je američki FBI, koji stoji iza masovnog presretanja komunikacije korisnika te kriptirane mreže, zaobišao pravne propise (s obzirom na to da u Sjedinjenim Američkim Državama nije dozvoljeno masovno presretanje komunikacija), zatim da je server kojim je presretao komunikacije postavio u treću zemlju, članicu Europske Unije, da Sjedinjene Američke Države ne žele otkriti o kojoj je trećoj zemlji (u kojoj je

[30] Vidi više u: Burić, Zoran, Engelhart, Marc, Novokmet, Ante i Roksandić, Sunčana, *Upotrebljivost rezultata masovnog nadzora komunikacija kao dokaza u hrvatskom kaznenom postupku – slučaj Sky ECC*, Hrvatski ljetopis za kaznene znanosti i praksu Vol. 30(2), 2023., str. 243–274.

postavljen server za presretanje komunikacije) riječ, a također ni dostaviti relevantne podatke o sudskom nalogu te treće države na temelju kojeg su osporavani podaci pribavljeni.

Kad je riječ o dokazima koji se odnose na komunikaciju preko aplikacije za kriptiranu komunikaciju Sky ECC, a zbog prethodno iznesenih prigovora okrivljenika i njihovih branitelja da je riječ o nezakonitim dokazima, optužna vijeća Županijskog suda u Zagrebu u dva odvojena predmeta donijela su rješenja broj Kov-Us-35/2023 od 28. ožujka 2024., a koje je potvrđeno rješenjem Visokog kaznenog suda Republike Hrvatske broj I Kž-Us-88/2024 od 19. studenog 2024. i Kov-Us-36/2023 od 26. ožujka 2024., a koje je potvrđeno rješenjem Visokog kaznenog suda Republike Hrvatske broj I Kž-Us-76/2024 od 19. veljače 2025. Navedenim pravomoćnim sudskim odlukama utvrđeno je da su dokazi koji se odnose na komunikaciju preko aplikacije za kriptiranu komunikaciju Sky ECC proglašeni zakonitim.

U odnosu na predmete koji se vode pred Županijskim sudom u Splitu u jednom predmetu sudac istrage još je tijekom istrage donio rješenje kojim je odbio prigovor obrane da je riječ o nezakonitim dokazima (rješenje je potvrđeno rješenjem Visokog kaznenog suda Republike Hrvatske broj I Kž-Us-43/2024-6 od 16. srpnja 2024.), dok je optužno vijeće Županijskog suda u Splitu donijelo rješenje Kov-Us-14/2024 od 19. veljače 2025. koje je potvrđeno rješenjem Visokog kaznenog suda Republike Hrvatske broj I Kž-US-36/2025 od 3. rujna 2025. Sudskim odlukama pravomoćno je utvrđeno kako je riječ o zakonitim dokazima, dok su u dva odvojena predmeta optužna vijeća Županijskog suda u Splitu zauzela stav kako su dokazi koji se odnose na komunikaciju preko aplikacije za kriptiranu komunikaciju Sky ECC također zakoniti (Kov-Us-10/2024 od 25. srpnja 2025. i Kov-Us-9/2024 od 17. studenog 2025.), time da se navedeni predmeti zbog žalbe okrivljenika nalaze na Visokom kaznenom sudu Republike Hrvatske.

U odnosu na pravomoćne sudske odluke povezane sa zakonitošću dokaza iz aplikacije za kriptiranu komunikaciju Sky ECC valja istaknuti kako je Visoki kazneni sud Republike Hrvatske u svojim odlukama zauzeo stav da je riječ o pribavljanju dokaza prema odredbama nacionalnog, francuskog prava i prenošenju tih dokaza u kazneni postupak u Republici Hrvatskoj na temelju prava Europske unije, ponajprije Direktive 2014/41/EU Europskog parlamenta i vijeća od 3. travnja 2014. o Europskom istražnom nalogu u kaznenim stvarima[31] (dalje: Direktiva o EIN-u) i hrvatskoga Zakona o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije[32] (dalje: ZPSKS-EU). S obzirom na činjenicu da osporeni

[31] Direktiva 2014/41/EU Europskog parlamenta i vijeća od 3. travnja 2014. o Europskom istražnom nalogu u kaznenim stvarima, SL 2014., L 130, str. 1. i ispravak SL 2015., L 143, str. 16.

[32] Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije („Narodne novine" broj 91/2010., 81/2013., 124/2013., 26/2015., 102/2017., 68/2018., 70/2019.,

dokazi u naravi predstavljaju digitalne dokaze o ostvarenoj komunikaciji okrivljenika preko aplikacije za kriptiranu komunikaciju Sky ECC valjalo je njihovo korištenje u kaznenom postupku razmotriti s aspekta prava na obranu i prava na nepovredivost osobnog i obiteljskog života (prava na privatnost). Prava obrane sadržana su u pravu na pravično suđenje koje je zajamčeno člankom 29. Ustava Republike Hrvatske[33] (dalje: Ustav) i člankom 6. Konvencije za zaštitu ljudskih prava i temeljnih sloboda[34] (dalje: Konvencija).

Članak 6. Konvencije ne postavlja nikakva pravila o dopuštenosti dokaza, dok Europski sud za ljudska prava (dalje: ESLJP) navodi kako ocjena pravičnosti postupka uključuje i ispitivanje načina na koji su dokazi pribavljeni odnosno uporabljeni[35] te u tom pravcu ESLJP provjerava je li dokaz pribavljen povredom nekog konvencijskog prava. Pritom samo iskazi pribavljeni zlostavljanjem, protivno zabrani iz članka 3. Konvencije, automatski dovode do povrede članka 6. Konvencije,[36] dok se u protivnom nastavlja s provođenjem testa[37] te se razmatra kvaliteta dokaza (pouzdanost i točnost), važnost dokaza i poštovanje prava obrane u smislu je li okrivljeniku pružena prilika za to da ospori vjerodostojnost dokaza i usprotivi se njihovoj uporabi.

U pogledu prava Europske unije Sud Europske unije (u daljnjem tekstu: SEU) u više je svojih odluka naveo kako se načelno samo nacionalnim pravom određuju pravila o dopuštenosti dokaza.[38] Dakle, treba utvrditi je li pojedini dokaz pribavljen protivno pravu Europske unije, a ako jest, treba utvrditi je li s obzirom na rečena načela potrebno njegovo izdvajanje u smislu odredbi članka 10. stavka 2. točke 3. Zakona o kaznenom postupku.

No, SEU je u presudi od 30. travnja 2024., EncroChat, broj C-670/22. (ECLI:EU:C:2024:372) u činjenično sličnom predmetu komunikacije zaštićene

141/2020., 18/2024.).

[33] Ustav Republike Hrvatske („Narodne novine" broj 56/1990., 135/1997., 8/1998. – službeni pročišćeni tekst, 113/2000., 124/2000. – službeni pročišćeni tekst, 28/2001., 41/2001. – službeni pročišćeni tekst, 76/2010., 55/2001. – službeni pročišćeni tekst, 5/2014., 85/2010. – službeni pročišćeni tekst).

[34] Konvencije za zaštitu ljudskih prava i temeljnih sloboda („Narodne novine" – Međunarodni ugovori broj 18/1997., 6/1999. – pročišćeni tekst, 8/1999. – ispravak, 14/2002., 1/2006., 13/2017.).

[35] Presuda Europskog suda za ljudska prava, Lisica protiv Hrvatske, broj zahtjeva 20100/06 od 25. veljače 2010., § 59.

[36] Presuda Europskog suda za ljudska prava, Jalloh protiv Njemačke, broj zahtjeva 54810/00 od 11. srpnja 2006., § 105.

[37] Presuda Europskog suda za ljudska prava, Bykov protiv Rusije, broj zahtjeva 4378/02 od 10. ožujka 2009. § 90 i presuda Europskog suda za ljudska prava, Bašić protiv Hrvatske, broj zahtjeva 22251/13 od 25. listopada 2016., § 43–48.

[38] Presuda SEU od 6. listopada 2020., La Quadrature du Net i dr., broj C-511/18, C-512/18 i C-520/18, EU:C:2020:791, točka 222.

sveobuhvatnim šifriranjem tumačio Direktivu o EIN-u te načela ekvivalentnosti i djelotvornosti kao i članak 14. stavak 7. Direktive o EIN-u koji nalaže poštovanje prava obrane i pravičnost postupka. Prema pravnom stajalištu SEU-a za odluku o izdvajanju nije dovoljno utvrditi da je europski istražni nalog nezakonito izdan, nego i da su u kaznenom postupku povrijeđena prava obrane u pogledu učinkovite mogućnosti osporavanja dokaza, što uključuje postupak u cjelini.

U vezi s pitanjem u čijoj je nadležnosti bilo izdavanje europskih istražnih naloga Visoki kazneni sud Republike Hrvatske navodi kako je odredbama ZPSKS-EU-a normirana nadležnost domaćih tijela te je u članku 6. stavku 2. ZPSKS-EU-a propisano da europske istražne naloge izdaje državno odvjetništvo i sud koji vodi postupak, dok je u članku 7. stavku 1. ZPSKS-EU-a propisana neposredna dostava europskih istražnih naloga koje je izdao državni odvjetnik nadležnom tijelu, a u stavku 2. propisano je da europski uhidbeni nalog i europski istražni nalog izdan na propisanom obrascu domaći sudovi dostavljaju neposredno nadležnom tijelu države izvršenja, pri čemu odredbe ZPSKS-EU-a treba dovesti u vezu s Direktivom o EIN-u koja je u taj zakon prenesena. Naime, prema članku 1. stavku 1. te Direktive europski istražni nalog izdaje ili potvrđuje pravosudno tijelo radi pribavljanja dokaza provođenjem posebnih istražnih mjera ili prosljeđivanja dokaza, a prema članku 2. stavku 2. „tijelo izdavatelj" je i „javni tužitelj nadležan u dotičnom predmetu". Stoga je potrebno naglasiti razliku između europskog istražnog naloga (koji se izdaje radi izvršenja jedne ili nekoliko posebnih istražnih radnji odnosno mjera u drugoj državi članici, „državi izvršenja", radi pribavljanja dokaza) od europskog istražnog naloga (koji se izdaje radi pribavljanja dokaza koji su već u posjedu nadležnih tijela države izvršiteljice). Prema tome državno odvjetništvo kao pravosudno istražno tijelo, a ne sud, bilo je ovlašteno samostalno izdati europski istražni nalog radi prijenosa dokaza koji su bili u posjedu nadležnog tijela u Republici Francuskoj.[39] Navedeno ima uporište i u navedenoj presudi SEU-a EncroChat, koja navodi: „… Ako je na temelju prava države izdavateljice, u potpuno unutarnjoj situaciji u toj državi, za određivanje istražne mjere s ciljem prosljeđivanja dokaza koji su u posjedu nadležnih nacionalnih tijela nadležan javni tužitelj, on je obuhvaćen pojmom 'tijelo izdavatelj'…". Budući da nije sporno da državni odvjetnik pribavljene dokaze u jednom kaznenom predmetu u svrhu vođenja kaznenog postupka može prenositi drugom nadležnom državnom

[39] Općenito u kontekstu pitanja koja su otvorena korištenjem europskih istražnih naloga i priznavanjem na taj način pribavljenih dokaza znanstveni krugovi još su prije desetak godina isticali da će prva reakcija na Direktivu o europskom istražnom nalogu najvjerojatnije biti obilježena zatvorenim pristupom promjenama. Odnosno predvidjeli su da će države zauzeti pristup usmjeren na zaštitu suvereniteta država i nacionalnih standarda zaštite temeljnih prava u prekograničnom prikupljanju dokaza, a koji u konačnici neće opstati. Vidi više u: Daniele, Marcello, *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, New Journal of European Criminal Law Vol. 6(2), 2015.

odvjetništvu, prema citiranom stavu SEU-a za izdavanje europskih istražnih naloga nije bilo potrebno odobrenje suda.

Također, povezano s pravom Europske unije, u kontekstu postupanja EUROPOL-a i EUROJUST-a i njihovih uloga u zajedničkom istražnom radu francuskih, nizozemskih i belgijskih nadležnih tijela tijekom prikupljanja, analize, obrade i razmjene informacija povezanih sa komunikacijom iz aplikacije Sky ECC valja spomenuti i nedavnu presudu SEU-a u predmetu C-T-1180/23 od 25. veljače 2026.[40] Navedenom presudom odbijena je tužba za poništenje i odštetu koju je B. W. podnio protiv EUROPOL-a i EUROJUST-a tražeći poništenje sporazuma ZIT-a,[41] akata EUROPOL-a i EUROJUST-a donesenih na temelju sporazuma te, u skladu s time, i obrade, analize i dijeljenja podataka sa Sky ECC-jeva servera koji se odnose na njega. U relevantnom dijelu presude SEU obrazlaže da su sve radnje poduzete u vezi s prikupljanjem podataka sa servera Sky ECC-ja provedene „u jasno utvrđenom okviru koji je imao posebnu, izričitu i zakonitu svrhu, i to u okviru posebne operacije koja se odnosila na uslugu Sky ECC čiji je cilj, među ostalim, bio utvrditi identitet njezinih korisnika u svrhu kaznenih progona i to putem zajedničkog istražnog tima koji ima isti cilj te koji je stvoren posebnim sporazumom kojim su Kraljevina Belgija, Francuska Republika i Kraljevina Nizozemska izričito utvrdile njegove ciljeve, a u kojima je EUROPOL sudjelovao".[42] Također, SEU je utvrdio da su tužiteljevi podaci bili povezani s posebnom istragom koja se odnosila na uslugu Sky ECC te da iz spisa ne proizlazi da su podaci koje je obradio EUROPOL netočni ili da im nije bila osigurana odgovarajuća razina sigurnosti s obzirom na to da su proslijeđeni samo državama ili agencijama koje su izravno ili neizravno sudjelovale u zajedničkom istražnom timu te da su se upotrebljavali isključivo za potrebe kaznenih postupaka koji su bili pokrenuti protiv tužitelja.[43] U pogledu zadiranja u temeljna prava utvrđena člancima 7. i 8. Povelje Europske unije o temeljnim pravima[44] (dalje: Povelja) SEU

[40] Presuda SEU, Opći sud (peto vijeće) od 25. veljače 2026., broj T-1180/23.

[41] Ovaj je sporazum sklopljen na temelju članka 13. Konvencije koju je Vijeće donijelo u skladu s člankom 34. Ugovora o Europskoj uniji o uzajamnoj pomoći u kaznenim stvarima između država članica Europske unije (SL 2000 C 197, str. 3) te Okvirne odluke Vijeća od 13. lipnja 2002. o zajedničkim istražnim timovima (SL 2002 L 162, str. 1).

[42] *Op. cit.* (bilj. 40.) para. 171.

[43] *Ibid.*, para. 175.

[44] Povelja Europske unije o temeljnim pravima 2016/C 202/02 u članku 7. propisuje poštovanje privatnog i obiteljskog života, doma i komuniciranja, a u članku 8. zaštitu osobnih podataka. Glede obrade takvih podataka člankom 8. stavkom 2. regulirano je da se oni moraju obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom.

je utvrdio da borba protiv teških kaznenih djela, u koju ulazi i suzbijanje nezakonite trgovine opojnim drogama, može opravdati takva zadiranja.[45]

Iz navedene presude jasno proizlazi da je SEU zaključio, s obzirom na to je tužitelj osoba protiv koje se vodi kazneni postupak zbog uvoza kokaina, da se time dostatno opravdava eventualna zadiranja u temeljna prava predviđena Poveljom prilikom prikupljanja, obrade i razmjene informacija dobivenih sa Sky ECC-jeva servera. Takvim stajalištem odražava se glavna ideja zbog koje su prikupljanje i obrada navedenih informacija i počeli, a to je suzbijanje teških oblika kaznenih djela.

Nadalje, ključni prigovor obrane bio je da uvjet iz članka 6. stavka 1. točke b Direktive o EIN-u odnosno članka 42.c. točke 2. ZPSKSEU-a nije bio ispunjen jer istražna radnja navedena u europskom istražnom nalogu nije mogla biti određena u „sličnom domaćem slučaju" te da su osporeni dokazi pribavljeni uz „masovni nadzor", pri čemu je došlo do povrede Ustavom i Konvencijom zajamčenog prava na privatnost, što se po svojoj prirodi protivi hrvatskom javnom poretku. Međutim, osporeni dokazi pribavljeni su u okviru francuske istrage na temelju naloga francuskog suda, dok su europskim istražnim nalogom tako pribavljeni dokazi preneseni u Republiku Hrvatsku. Nadalje, a kako to navodi Visoki kazneni sud Republike Hrvatske, pravo na privatnost relativno je, a ne apsolutno pravo, a klauzulu javnog poretka treba promatrati u kontekstu prava i obveza država članica Europske unije. Dakle, riječ je o dokazima koje je prikupila jedna država članica Europske unije u skladu sa svojim nacionalnim pravom, a ne o dokazima koji su prikupljeni na temelju odredbi Zakona o kaznenom postupku ni o dokazima koje je Republika Francuska izvela, tj. pribavila na molbu Republike Hrvatske. U tom smislu, osobito imajući na umu načelo uzajamnog povjerenja i odane suradnje iz članka 4. stavka 3. podstavka 1. Ugovora o Europskoj uniji, stajalište je Visokog kaznenog suda Republike Hrvatske kako dokaze pribavljene u zasebnom, francuskom postupku, treba ocijeniti iz aspekta njihove usklađenosti s Ustavom, Konvencijom i Poveljom (točka 6.) koja u sebi uključuje i elemente ocjene vjerodostojnosti dokaza te prava obrane koja se promatraju u cjelini postupka. Tomu treba dodati da prema pravnom stajalištu SEU-a i ESLJP-a pravilnost zasebnog postupka prikupljanja dokaza treba ispitati pred sudovima Republike Francuske.[46] Navedeno proizlazi i iz točke 100. navedene presude EncroChat, ali i iz odluke ESLJP-a od 24. rujna 2024. u predmetu A. L. i E. J. protiv Francuske[47] koja se odnosi na činjenično sličan predmet u kojem

[45] Vidi: Presuda SEU od 7. rujna 2023., Lietuvos Respublikos generalinė prokuratūra, broj C-162/22, EU:C:2023:631, točka 37.

[46] Rješenje Visokog kaznenog suda Republike Hrvatske, broj I Kž-Us-88/2024 od 19. studenog 2024., str. 7.

[47] Presuda Europskog suda za ljudska prava, A. L. i E. J. protiv Francuske, broj zahtjeva 44715/20 i 47930/21 od 24. rujna 2024.

su digitalni dokazi pribavljani u okviru francuske istrage u predmetu EncroChat preneseni europskim istražnim nalogom i upotrijebljeni u kaznenom postupku u Ujedinjenom Kraljevstvu (vidi osobito točke 105. i 145. u pogledu dostupnog pravnog sredstva). Upravo je poštovanje zahtjeva pravičnosti, a koje se uvijek ispituje u cjelini postupka – što uključuje i raspravnu fazu postupka, suština presude SEU-a EncroChat, a naposljetku i presude ESLJP-a Yüksel Yalçinkaya protiv Turske.[48]

Nadalje, važno je istaknuti da je SEU naveo kako je „točno da je cilj članka 6. stavka 1. točke b Direktive o EIN-u izbjeći zaobilaženje pravila i jamstava predviđenih pravom države izdavateljice", ali da je za primjenu te odredbe ključno provjeriti je li prikupljanje i prosljeđivanje tako prikupljenih dokaza europskim istražnim nalogom imalo kao cilj i učinak takvo zaobilaženje. U vezi s navedenim Visoki kazneni sud Republike Hrvatske ističe kako su osporeni dokazi pribavljeni u zasebnoj domaćoj istrazi druge države članice Europske unije, pa nema riječi o tome da bi sudovi Republike Francuske izdavali naloge za pribavljanje tih dokaza radi njihova „uvoza" u Republiku Hrvatsku. Štoviše, prema tumačenju SEU-a iz presude EncroChat člankom 6. stavkom 1. točkom (b) Direktive o EIN-u ne zahtijeva se da se na izdavanje europskog istražnog naloga radi prosljeđivanja dokaza koji su već u posjedu nadležnih tijela države izvršiteljice primjenjuju iste materijalne pretpostavke kao one koje se primjenjuju na prikupljanje tih dokaza u državi izdavateljici.[49, 50]

Dakle, u pogledu europskog istražnog naloga za prenošenje dokaza bilo je potrebno razmotriti jesu li u čisto unutarnjoj situaciji bili ispunjeni uvjeti za prosljeđivanje dokaza. Utvrđeno je da osporeni dokazi odgovaraju slučajnom nalazu pribavljenom posebnim dokaznim radnjama koji upućuje na drugo djelo i počinitelja, dakle ne i onog zbog kojeg su posebne dokazne radnje određene, a koji se prema odredbi članka 335. stavka 6. Zakona o kaznenom postupku prosljeđuje državnom odvjetniku.[51]

---

48 Presuda Europskog suda za ljudska prava, Yüksel Yalçinkaya protiv Turske, broj zahtjeva 15669/20 od 26. rujna 2023.

49 *Op. cit.* (bilj. 46.), str. 7 i 8.

50 Takvi dokazi, koji su već u posjedu države izvršiteljice, praktično i dalje odražavaju načelo *locus regit actum* prema kojem država izvršiteljica primjenjuje svoje nacionalno procesno pravo pri provođenju istražne radnje, a što je jasno po samoj prirodi stvari u ovom slučaju. Međutim, ovdje valja naglasiti da postoji i pravilo *forum regit actum*, koje svoj temelj nalazi u Konvenciji o uzajamnoj pravnoj pomoći u kaznenim stvarima među državama članicama EU-a iz 2000. godine, a prema kojem država izvršiteljica pri provođenju istražne radnje postupa prema procesnom pravu države koja je uputila zahtjev za pružanje međunarodne pravne pomoći ako to nije u skladu s temeljnim postulatima njezina prava. Vidi više o razlikovanju *locus/forum regit actum* u: Karsai, Krisztina, *Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters*, Hungarian Journal of Legal Studies 60(2), 2019., str. 155–172.

51 *Op. cit.* (bilj. 46.), str. 8.

Nadalje, Visoki kazneni sud Republike Hrvatske navodi kako nalozi francuskih sudova kojima su određene intruzivne mjere presretanja, snimanja i transkripcije elektroničkih komunikacija između dvaju poslužitelja (servera), postavljanja uređaja za prikupljanje podataka radi pristupa računalnim podacima, snimanja, čuvanja i prenošenja podataka na način kako su pohranjeni u računalnom sustavu odgovaraju nalozima za provođenje posebnih dokaznih radnji iz članka 332. Zakona o kaznenom postupku osobito posebnih dokaznih radnji presretanja, prikupljanja i snimanja računalnih podataka koje nalaže sudac istrage i koje je moguće odrediti i prema predmetu i nepoznatom počinitelju za jedno od kataloških djela. Prema tome, u sličnoj, potpuno domaćoj situaciji, prenošenje dokaza pribavljenih posebnim dokaznim radnjama koji upućuju na drugo kataloško kazneno djelo i počinitelja državnom odvjetniku utemeljeno je na odredbama Zakona o kaznenom postupku, pa je ispunjen daljnji uvjet iz članka 42.c. točke 2. ZPSKSEU-a u vezi s člankom 6. stavkom 1. točkom b Direktive o EIN-u.[52]

Također, Visoki kazneni sud Republike Hrvatske[53] zaključuje kako je izdavanje europskog istražnog naloga za prenošenje dokaza bilo nužno i razmjerno svim okolnostima predmeta. Izdavanje europskog istražnog naloga služilo je izbjegavanju opasnosti od nekažnjavanja osoba koje su počinile kazneno djelo, što je legitiman cilj prema pravu EU-a.[54] Naime, riječ je o podacima do kojih se došlo presretanjem telekomunikacija internetskog pružatelja usluga Sky ECC. S obzirom na to da se okrivljenicima stavlja na teret počinjenje više teških kaznenih djela (među ostalim zločinačkog udruženja, neovlaštene proizvodnje i prometa drogama u sastavu zločinačkog udruženja, nedozvoljenog posjedovanja, izrade i nabavljanja oružja i eksplozivnih tvari u sastavu zločinačkog udruženja) te s obzirom na težinu posljedice i međunarodni karakter inkriminirane djelatnosti, može se zaključiti da je ograničenje koje okrivljenici trpe zbog zadiranja u njihova temeljna prava uslijed izdavanja europskog istražnog naloga kojim su osporeni dokazi kojima se zadiralo u njihovu privatnost preneseni razmjerno ostvarenju navedenog legitimnog cilja.[55]

Nadalje, Visoki kazneni sud Republike Hrvatske ističe kako u vrijeme provođenja tajnih mjera u okviru samostalne istrage Republika Francuska nije imala saznanja da pristupa komunikacijama subjekata koji se nalaze na teritoriju Republike Hrvatske niti su oni bili identificirani. Tako pribavljeni dokazi nalazili su se u posjedu Republike Francuske i tek su europskim istražnim nalogom preneseni u kazneni postupak u

52 *Ibid.*

53 *Ibid.*

54 Presuda SEU-a od 6. rujna 2016., Petruhhin, broj C-172/15., ECLI:EU:C:2016:630.

55 *Op. cit.* (bilj. 46.), str. 9.

Republici Hrvatskoj.[56] Tajne mjere provedene u francuskoj istrazi prema tumačenju SEU-a iz presude EncroChat potpadaju pod „presretanje komunikacije" iz članka 31. stavka 1. Direktive o EIN-u, što znači da se o njima mora obavijestiti tijelo koje je u tom pogledu odredila država članica na čijem se državnom području nalazi subjekt presretanja, i to ne samo radi zaštite suverenosti te države nego i radi zaštite osoba na koje se odnosi mjera presretanja telekomunikacija jer obaviještena država, u slučaju kada se presretanje ne bi odobrilo u sličnom domaćem slučaju, može obavijestiti nadležno tijelo države koje presreće da se sav presretani materijal ne može upotrijebiti. No prema daljnjem tumačenju iz presude EncroChat, ako država članica koja presreće ne može utvrditi nadležno tijelo obaviještene države članice, ta se obavijest može poslati bilo kojem tijelu te države koje država članica koja presreće smatra prikladnim, ali, kako bi se osigurao koristan učinak članka 31. Direktive o EIN-u, obaviješteno tijelo mora po službenoj dužnosti proslijediti obavijest nadležnom tijelu, što je prema članku 42.an ZPSKS-EU-a Županijski sud u Zagrebu. Međutim, u kaznenim predmetima u Republici Hrvatskoj dokazi preneseni Europskim istražnim nalogom već su kao takvi bili u posjedu Republike Francuske. Okrivljenici nisu lišeni zaštite iz članka 31. Direktive o EIN-u jer se o zakonitosti, a time i o mogućnosti uporabe osporenih dokaza, odlučuje u ovom postupku prvo pred optužnim vijećem, a bude li optužnica potvrđena, i poslije tijekom suđenja. Zbog toga je sud osnovano zaključio kako bilo kakvo kršenje obveza iz odredbe članka 42.an ZPSKS-EU-a u vezi s člankom 31. Direktive o EIN-u samo za sebe ne dovodi ujedno i do nezakonitosti dokaza. Takav zaključak u skladu je s tumačenjem iz presude EncroChat prema kojem za odluku o izdvajanju nije dostatno to da bi EIN bio izdan protivno obvezama iz članka 31. Direktive o EIN-u, nego je ključno ostvarivanje mogućnosti učinkovitog očitovanja o tim dokazima, što se odnosi na postupak u cjelini.

Nadalje, u vezi s dokazima koji se odnose na komunikaciju putem aplikacije za kriptiranu komunikaciju ANOM, a zbog iznesenih prigovora okrivljenika i njihovih branitelja da je riječ o nezakonitim dokazima, optužno vijeće Županijskog suda u Splitu donijelo je rješenje broj Kov-Us-6/2024 od 17. rujna 2024. kojim je utvrdio kako je riječ o zakonitim dokazima. To rješenje potvrdio je Visoki kazneni sud Republike Hrvatske svojim rješenjem broj I Kž-Us-167/2024 od 17. travnja 2025.

Naime, Visoki kazneni sud u svojoj odluci[57] u bitnome navodi kako je s pravom prvostupanjski sud utvrdio da za prenošenje dokaza putem međunarodne pravne pomoći u domaći postupak nije bio potreban nalog suca istrage. Tim više jer tijela progona Republike Hrvatske nisu inicirala bilo kakvo prikupljanje dokaza u drugoj

[56] *Ibid.*

[57] Rješenje Visokog kaznenog suda Republike Hrvatske od 17. travnja 2025., broj I Kž-Us-167/2024, str. 5.

državi (ishođenjem kakva naloga za provođenje tajnih mjera), nego je riječ o tome da su postojeći, neovisno pribavljeni dokazi naknadno preneseni u domaći kazneni postupak.

Međutim, Visokom kaznenom sudu Republike Hrvatske nisu prihvatljiva utvrđenja prvostupanjskog suda kako je operacija „Trojanski štit", u kojoj su pribavljeni osporeni dokazi, bila potpuno „u skladu sa zakonom" u smislu prakse ESLJP-a. Naime, ključna je činjenica u stvari ta što je sudski nalog za prikupljanje podataka izdan u neimenovanoj državi članici EU-a, što znači da su okrivljenici lišeni stvarne i učinkovite mogućnosti provjere zakonitosti takva naloga i njegove provedbe bilo u ovom postupku, bilo pred sudovima te države članice. Prema tome, kako uvjet „zakonitosti" uključuje i postojanje i pristup zaštitnim mjerama, a kako okrivljenici nemaju mogućnost propitkivanja zakonitosti sudskog naloga jer nema podataka čak ni o tom u kojoj je državi članici takav nalog izdan, ocjena je Visokog kaznenog suda Republike Hrvatske kako provedba operacije „Trojanski štit" odnosno prikupljanje osporenih dokaza nije posve u skladu s uvjetima „zakonitosti" u smislu članka 8. stavka 1. Konvencije. Zato su dokazi prikupljeni povredom prava na privatnost (osobni i obiteljski život) osoba koje su bile obuhvaćene.[58]

Dakle, utvrđeno je da su osporeni računalni podaci pribavljeni uz povredu prava na privatnost. Ti podaci važni su dokazi, ali nisu jedini. Prvostupanjski sud utvrdio je da je uporaba platforme ANOM bila odluka korisnika, a sadržaj komunikacije ovisio je samo o volji korisnika. Okrivljenici imaju mogućnost osporavati zakonitost uporabe tih dokaza pred optužnim vijećem, ali i na raspravi, bude li optužnica potvrđena. Vjerodostojnost dokaza utvrđuje se na raspravi u dokaznom postupku, pa bi utvrđivanje pouzdanosti i istinitosti osporenih dokaza u fazi postupka pred optužnim vijećem prekoračilo ovlasti dane optužnom vijeću. Zato treba zaključiti da operacija „Trojanski štit", u kojoj su osporeni računalni podaci pribavljeni, nije povrijedila pravo na obranu u mjeri koja bi u tom stadiju postupka osporene dokaze činila nezakonitim u smislu odredbe članka 10. stavka 2. točke 2. Zakona o kaznenom postupku.[59] Međutim, kako je utvrđeno da su osporeni računalni podaci prikupljeni povredom prava na privatnost (osobni i obiteljski život), bilo je potrebno utvrditi i jesu li oni zbog toga nezakoniti u smislu odredbe članka 10. stavka 2. točke 2. Zakona o kaznenom postupku ili ih, unatoč toj povredi, treba konvalidirati u smislu odredbe članka 10. stavka 3. Zakona o kaznenom postupku.[60] U konkretnom slučaju riječ je o kaznenim djelima iz nadležnosti županijskog suda, i to teškim oblicima terećenih kaznenih djela. Osim toga, prema optužnici riječ je o kaznenom djelu neovlaštene proizvodnje i prometa drogama u sastavu zločinačkog udruženja, a treba uzeti u obzir i iznimnu društvenu opasnost od zlouporabe droga, globalnost te pojave i posljedične bolesti ovisnosti i njezin negativan

58 *Ibid.*

59 *Ibid.*, str. 6.

60 *Ibid.*, str. 7.

utjecaj na živote i zdravlje građana, osobito djece i mladih osoba, te nastojanja hrvatskog društva da se zlouporaba suzbije. Zbog svega toga ocjena je Visokog kaznenog suda Republike Hrvatske da u ovom predmetu interes kaznenog progona i kažnjavanja počinitelja preteže nad povredom prava na nepovredivost osobnog i obiteljskog života u okolnostima u kojima se, prema optužnici, okrivljenici pozivajući se na pravo na privatnost služe kriptiranim uređajima radi trgovanja kokainom.[61]

Prema tome ocjena je Visokog kaznenog suda Republike Hrvatske da su u konkretnom predmetu ispunjeni uvjeti iz članka 10. stavka 2. točke 3. Zakona o kaznenom postupku, zbog čega nema mjesta izdvajanju osporenih računalnih podataka kao nezakonitih dokaza u smislu odredbe članka 10. stavka 2. točke 2. Zakona o kaznenom postupku. Ujedno, uporaba osporenih računalnih podataka nije protivna ni javnom poretku Republike Hrvatske jer je njime dopuštena mogućnost konvalidacije dokaza pribavljenih povredom prava na privatnost (osobni i obiteljski život). Zato postupovna pravila iz Zakona o kaznenom postupku nisu mjerodavna jer je riječ o dokazima koji su pribavljeni putem međunarodne pravne pomoći, prema drukčijim procesnim pravilima, pri čemu su u žalbama izostale bilo kakve tvrdnje da bi tijela progona Republike Hrvatske inicirala kakvo prikupljanje dokaza u drugoj državi. Ovdje je riječ o tome da su postojeći, neovisno pribavljeni dokazi naknadno preneseni u domaći kazneni postupak. Osporeni dokazi već su bili u posjedu SAD-a, koji ih je prethodno putem međunarodne pravne pomoći pribavio od neimenovane države članice EU-a. Osim toga, čak i kad bi tajne mjere koje je provela neimenovana država članica EU-a u kojoj je izdan sudski nalog za prikupljanje podataka s poslužitelja mogle potpasti pod „presretanje komunikacije" iz članka 31. stavka 1. Direktive o EIN-u, neobavještavanje nadležnog tijela države članice na čijem se državnom području nalazi subjekt presretanja ne znači i da se presretani materijal automatski zbog toga ne može upotrijebiti, a kako je to presudio SEU u presudi EncroChat. Naime, u skladu je s tumačenjem iz presude EncroChat, za odluku o izdvajanju ključno je ostvarivanje mogućnosti učinkovitog očitovanja o tim dokazima, što se odnosi na postupak u cjelini.[62]

5. Sudska praksa odabranih država

Iako pravo Europske unije teži usklađivanju pravnih sustava država članica, osobito uz načelo međusobnog povjerenja,[63] dokazi pribavljeni dešifriranjem kriptirane

[61] *Ibid.*, str. 7.

[62] *Ibid.*, str. 8.

[63] Navedeno načelo predstavljeno je kao plod težnji da se olakša „klasični" sustav međunarodne pravne pomoći i suradnje. U listopadu 1999. na sastanku Europskog vijeća doneseni su Tamperski zaključci (*Tampere European Council 15 and 16 October 1999 Presidency Conclusions*) kojima je načelo međusobnog povjerenja/priznanja prepoznato kao „kamen temeljac pravosudne suradnje u građanskim i

komunikacije otvorili su brojna sporna pitanja i pokrenuli javne rasprave. Kao što je prethodno opisano na primjerima u sudskoj praksi Republike Hrvatske, slični prigovori isticani su i u kaznenim postupcima drugih država članica Europske unije.

U tom smislu potrebno je spomenuti sudsku praksu Savezne Republike Njemačke, i to postupak u predmetu u kojem je okrivljenik osporavao zakonitost uporabe dokaza koji su proizišli dešifriranjem komunikacije s EncroChata.[64] U konačnici Savezni sud pravde odbio je žalbu protiv presude Zemaljskog suda u Hamburgu iz 2021. kojom je navedeni okrivljenik osuđen na pet godina zatvora zbog trgovine drogom. Naime, njemačka tijela tijekom istrage uputila su europski istražni nalog francuskim vlastima i tako zatražila prijenos svih EncroChat podataka povezanih sa Saveznom Republikom Njemačkom, a francuski sud odobrio je oba njihova zahtjeva za dopuštenje za uporabu takvih dokaza u njemačkim kaznenim postupcima. Pri utvrđivanju zakonitosti takvih dokaza Savezni sud razmatrao je je li došlo do povrede procesnog prava, štiti li to pravo, ako je povrijeđeno, prava osumnjičenika te nadilazi li interes osumnjičenika u konkretnom slučaju interes državnog odvjetništva. U svojem obrazloženju Savezni sud istaknuo je kako nije potrebno ispitivati zakonitost načina na koji su podaci pribavljeni od francuskih vlasti jer bi to bilo protivno načelu međusobnog povjerenja na kojem se temelji pravosudna suradnja država članica Europske unije. Glede utvrđivanja razmjernosti između interesa osumnjičenika i interesa državnog odvjetništva Sud nije utvrdio povrede predmetnog načela uzevši u obzir težinu kaznenih djela koja su se osumnjičenom stavljala na teret, a koja su bila predmet mjere presretanja komunikacije. Međutim, Sud je utvrdio procesnu povredu koja se ticala primjene članka 31. Direktive o europskom istražnom nalogu jer su francuske vlasti bile dužne obavijestiti njemačka tijela o tome da se vodi istraga protiv osoba na njihovu području. Neovisno o navedenom, istovjetno hrvatskoj sudskoj praksi, Sud je zauzeo stajalište da takva povreda nije mogla utjecati na zakonitost korištenja EncroChata u sudskom postupku jer svrha navedenog članka nije zaštita prava osumnjičenika, nego same države koja provodi istragu. Valja naglasiti da je Sud posebno razmatrao i dopuštenost takvih dokaza u kontekstu članka 6. Direktive o EIN-u,[65] pri čemu je zaključio da ne postoji uvjet prema kojem bi istražne mjere provedene u Francuskoj morale biti dopuštene prema njemačkom pravu kako bi dostavljeni podaci bili dopušteni kao dokaz pred sudovima Savezne Republike Njemačke. Kao i u slučaju Republike Hrvatske, riječ je o situaciji u kojoj njemačko

kaznenim postupcima u Europskoj Uniji", v. točku 33. Tamperskih zaključaka. Tamperski zaključci dostupni su na adresi https://www.europarl.europa.eu/summits/tam_en.htm, pristupljeno 15. travnja 2026.

64 *Op. cit.* (bilj. 23.).

65 Članak 6. propisuje da tijelo izdavatelj može izdati EIN samo kada je to potrebno i proporcionalno svrsi postupka uzimajući u obzir prava osumnjičenika i ako istražna mjera navedena u EIN-u može biti određena u sličnom domaćem slučaju.

državno odvjetništvo nije od francuskih istražnih tijela tražilo provođenje istražnih radnji, nego samo dostavu rezultata istrage.[66]

S druge strane, upravo je njemačka sudska praksa, konkretno Zemaljski sud u Berlinu, kao reakciju na prethodno iznesena pravna stajališta uputila zahtjev za prethodnu odluku Sudu Europske unije. Taj je zahtjev rezultirao donošenjem presude od 30. travnja 2024. u predmetu M. N. (EncroChat), broj C-670/22 (ECLI:EU:C:2024:372), o kojoj je već bilo riječi.[67]

U kaznenim postupcima pred nizozemskim sudovima u kojima su se upotrebljavali podaci iz EncroChata obrane okrivljenika pozivale su se na članak 6. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda zahtijevajući od tužiteljstva da im omogući pristup svim relevantnim dokazima kako bi provjerili njihovu pouzdanost. Nizozemski sudovi tada su uspostavili praksu prema kojoj je obrani omogućen pristup dokazima, ali samo u mjeri u kojoj su podaci relevantni za konkretni predmet. Podaci se mogu analizirati u Nizozemskom forenzičkom institutu uz uporabu analitičkog softvera. Pritom valja naglasiti da je Vrhovni sud Nizozemske zauzeo stav kako je takav pristup zakonit i usklađen s načelom jednakosti oružja. Navedeni institut proveo je istraživanje koje je pokazalo da poruke pribavljene od francuskih pravosudnih tijela nisu bile različite od poruka koje su pronađene na oduzetim mobitelima korisnika koji su upotrebljavali EncroChat. U konačnici, obrana nije uspjela osporiti pouzdanost podataka iz EncroChata, pa tako nijedan takav podatak posljedično nije bio izdvojen kao nezakonit dokaz u nizozemskim kaznenim postupcima.[68]

Talijanska sudska praksa zauzima restriktivnije stajalište glede dokaza kriptiranom komunikacijom pritom naglašavajući važnost prava na pošteno suđenje i prava obrane općenito. Primjerice, Vrhovni sud Italije donio je 15. srpnja 2022.[69] odluku kojom je za dokaze pribavljene putem aplikacije Sky ECC naglasio da je u takvim slučajevima potrebno objasniti na koji su način takvi elektronički dokazi pribavljeni, uključujući i način na koji su oni presretani i dešifrirani. Sud je naglasio da dokazi moraju biti u skladu s temeljnim načelima talijanskog prava, osobito uzimajući u obzir zajamčena

[66] Simonović, Vladimir, *Admissibility of the Use of Encrypted Communications as Evidence in Criminal Proceedings: Comparative Experiences and Recommendations for Montenegro*, Centre for Monitoring and Research (CEMI), 2023., str. 11.

[67] Vidi poglavlje 4. ODLUKE SUDOVA U REPUBLICI HRVATSKOJ U POVODU IZNESENIH PRIGOVORA ZAKONITOSTI DOKAZA KRIPTIRANOM KOMUNIKACIJOM SKY ECC I ANOM.

[68] Oerlemans, Jan-Jaap i van Toor, D. A. G. *Legal Aspects of the EncroChat Operation: A Human Rights Perspective*, European Journal of Crime, Criminal Law and Criminal Justice 30(3–4), 2022., str. 309–328.

[69] Presuda Vrhovnog kasacijskog suda Italije od 15. srpnja 2022., broj 32915/22, https://canestrinilex.com/en/readings/due-process-requires-transparency-of-evidence-gathering-in-sky-ecc-proceeding-cass-3291522, pristupljeno 5. travnja 2026.

prava obrane. U skladu s navedenim stajalište je talijanske sudske prakse da obje strane u postupku moraju imati mogućnost očitovati se o prikupljenim dokazima, ali i o metodama njihova prikupljanja. Međutim, valja naglasiti da su talijanska tijela, za razliku od drugih država članica Europske unije u kojima su elektronički dokazi prikupljeni neposredno od pravosudnih tijela putem mehanizama međunarodne pravosudne suradnje, dokaze pribavila od EUROPOL-a kao dio međunarodne policijske suradnje.[70]

Države u regiji, odnosno zemlje zapadnog Balkana, ne primjenjuju legislativu Europske unije jer nisu zemlje članice, pa samim time u njihovo pravo nije utkano načelo međusobnog povjerenja niti se one na njega trebaju oslanjati.[71] Unatoč tomu postoji više sudskih odluka koje su dokaze iz kriptirane komunikacije ocijenile zakonitima. Primjerice, u sudskoj praksi Republike Srbije sudovi su prihvaćali dokaze koji se tiču komunikacije iz aplikacije Sky ECC kao zakonite. S obzirom na to da Kazneni zakon Republike Srbije ne poznaje istražne mjere usporedive s prikupljanjem računalnih podataka, sudovi su tretirali podatke iz Sky ECC-ja kao pisane dokumente dobivene putem međunarodne pravne pomoći, a temelj za to pronađen je u Kaznenom zakonu i Kaznenom postupovnom zakonu Republike Srbije, u kojima su računalni podaci još uvijek izjednačeni s pisanom dokumentacijom.[72] Slično je i u Bosni i Hercegovini, gdje je 10. srpnja 2025. godine donesena prva presuda u predmetu s dokazima pribavljenima putem komunikacije preko aplikacije Sky ECC. U konkretnom slučaju riječ je o okrivljeniku koji je proglašen krivim zbog počinjenja djela organiziranog kriminala i neovlaštenog prometa opojnim drogama.[73] U Crnoj Gori u srpnju 2025. godine Vrhovni sud Crne Gore potvrdio je presudu suda nižeg stupnja kojom se dokazi pribavljeni putem aplikacije Sky ECC smatraju zakonitima.[74] Prema ocjeni suda dokumentacija je pribavljena na zakonit način preko međunarodne pravne pomoći u skladu s odredbama Europske konvencije o uzajamnoj sudskoj pomoći u kaznenim stvarima iz 1959. i Konvencije Ujedinjenih naroda protiv transnacionalnog organiziranog kriminala iz 2000., a koje čine dio pravnog poretka Crne Gore.[75]

---

70 *Ibid.*

71 Zemlje koje nisu članice Europske unije i dalje se oslanjaju na tradicionalne oblike međunarodne pravne pomoći i pravosudne suradnje, i to ponajprije na konvenciju Vijeća Europe, odnosno Europsku konvenciju o uzajamnoj sudskoj pomoći u kaznenim stvarima iz 1959. i njezinim protokolima iz 1978., 2001. i 2025. godine.

72 Bajović, Vanja i Ćorić, Vesna, *Encrochat and Sky ECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision*, European Journal of Crime, Criminal Law and Criminal Justice 33, Brill Nijhoff, 2025., str. 235–262.

73 Presuda Suda Bosne i Hercegovine, broj S1 2 K 047599 23 K) od 10. srpnja 2025.

74 Presuda Apelacionog suda Crne Gore, broj Kt-S 56/22 od 21. ožujka 2025.

75 *Ibid.*

6. Zaključak

Zaključno valja navesti kako je iz rezultata dosadašnjeg postupanja utvrđeno kako su uređaji s instaliranim aplikacijama za kriptiranu komunikaciju Sky ECC i ANOM prodavani među članovima zločinačkih organizacija kao novi, visoko razvijeni uređaji koje tijela kaznenog progona ne mogu „probiti". Nisu bili na raspolaganju javnosti putem uobičajenih distribucijskih mreža niti ih je svatko mogao nabaviti npr. preuzimanjem javno dostupne aplikacije. Sam „kriptirani uređaj" nije bilo moguće kupiti u slobodnoj prodaji, a i cijena takva uređaja bila je znatno viša od uobičajene cijene usporedivog „nekriptiranog" mobilnog uređaja. Zajedničko obilježje u odnosu na dokaze koji se odnose na komunikaciju putem aplikacije za kriptiranu komunikaciju Sky ECC i ANOM prosljeđivanje je podataka drugim državama radi provođenja kaznenog postupka. Stoga govorimo o istragama usmjerenim prethodno prikupljenim podacima. Naime, potrebno je razlikovati prikupljanje od pribavljanja elektroničkih dokaza. Prikupljanje dokaza predstavlja zahvate u komunikaciju pojedinih osoba, što neizbježno obuhvaća u zadiranje u njihova temeljna ljudska prava, dok pribavljanje dokaza znači isključivo pribavljanje dokaznog materijala koji je već bio prikupljen. S tim u vezi u odluci Suda EU-a broj C-670/22 u predmetu EncroChat jasno je da su navedeni uvjeti za zakonit prijenos od već pribavljenih dokaza. Naime, u predmetima koji su formirani u Republici Hrvatskoj europskim istražnim nalogom pribavljeni su dokazi koji su se već nalazili u posjedu države izvršiteljice i na taj način država izdavatelj ne može dovoditi u pitanje zakonitost mjera kojima su dokazi prikupljeni. Naime, pitanje zakonitosti dokaza koji se odnose na komunikaciju okrivljenika putem servera za kriptiranu komunikaciju SkyECC i ANOM bilo je predmetom razmatranja pred sudovima u Republici Hrvatskoj, no ta pitanja već su se u više kaznenih predmeta pojavila pred sudovima drugih država članica Europske unije. Iz pravomoćnih odluka Županijskog suda u Zagrebu i Županijskog suda u Splitu u povodu iznesenih prigovora obrane okrivljenika u pogledu zakonitosti dokaza koji se temelje na komunikaciji putem aplikacije za kriptiranu komunikaciju Sky ECC i ANOM sud nalazi da nije riječ o nezakonitim dokazima iz članka 10. stavka 2. Zakona o kaznenom postupku. Naime, navedeni dokazi ne mogu se smatrati nezakonitim jer procesna zakonodavstva Republike Hrvatske i Republike Francuske nisu potpuno jednaka, pa se stoga nikako hrvatskim procesnim zakonom ne može izričito propisati kada bi dokazi koji su pribavljeni u inozemnoj istrazi i za potrebe istraživanja kaznenog djela u stranoj državi bili pribavljeni povredom odredaba hrvatskog kaznenog postupka. U konačnici, i europsko i međunarodno pravo počivaju na suradnji država te se sve više razvijaju u smjeru jačanja načela uzajamnog povjerenja, što je osobito važno u kontekstu borbe protiv organiziranog kriminala i teških kaznenih djela kao ključnih transnacionalnih izazova. Zaključno valja istaknuti kako su razmatranja u ovom konkretnom radu rezultat dosad poznatih podataka u vezi s aplikacijama za kriptiranu komunikaciju Sky ECC i ANOM te dosad donesenih odluka sudova u Republici Hrvatskoj. Osnovno pitanje koje se pojavljuje u tim

postupcima upravo je zakonitost navedenih dokaza te mogućnost njihove uporabe u sudskim postupcima pred domaćim sudovima.

BIBLIOGRAFIJA

1. Burić, Zoran, Engelhart, Marc, Novokmet, Ante i Roksandić, Sunčana, *Upotrebljivost rezultata masovnog nadzora komunikacija kao dokaza u hrvatskom kaznenom postupku – slučaj Sky ECC*, Hrvatski ljetopis za kaznene znanosti i praksu Vol. 30(2), 2023.
2. Bajović, Vanja i Ćorić, Vesna, *Encrochat and Sky ECC Data as Evidence in Criminal Proceedings in Light of the CJEU Decision*, European Journal of Crime, Criminal Law and Criminal Justice 33, Brill Nijhoff, 2025.
3. Daniele, Marcello, *Evidence Gathering in the Realm of the European Investigation Order: From National Rules to Global Principles*, New Journal of European Criminal Law Vol. 6(2), 2015.
4. Forlani, Gianluca, *The E-evidence Package, The Happy Ending of a Long Negotiation Saga* Eucrim Issue 2/2023, 2023.
5. Garačić, Ana i Novosel, Dragan, *Zakon o kaznenom postupku u sudskoj praksi*, Knjiga II. Glava XX. – Glava XXXI., Libertin naklada, Rijeka, 2018.
6. Kanani, Ishva Jitendrakumar, *Securing Data in Motion and at Rest: A Cryptographic Framework for Cloud Security*, International Journal of Science and Research Vol. 9(2), 2020., str. 1965–1968.
7. Karsai, Krisztina, *Locus/Forum Regit Actum – a Dual Principle in Transnational Criminal Matters*, Hungarian Journal of Legal Studies 60(2), 2019.
8. Oerlemans, Jan-Jaap, *The Future of Data-Driven Investigations in Light of the Sky ECC Operation* New Journal of European Criminal Law Vol. 14(4), 2023.
9. Oerlemans, Jan-Jaap i van Toor, D. A. G. *Legal Aspects of the EncroChat Operation: A Human Rights Perspective* European Journal of Crime, Criminal Law and Criminal Justice 30(3–4), 2022.
10. Simonović, Vladimir, *Admissibility of the Use of Encrypted Communications as Evidence in Criminal Proceedings: Comparative Experiences and Recommendations for Montenegro*, Centre for Monitoring and Research (CEMI), 2023.
11. Stallings, William, *Cryptography and Network Security: Principles and Practice*, 7. izdanje, Pearson Education, 2017.
12. Wahl, Thomas, *What Remains of the ordre public in Transnational Surveillance? A Commentary on the Decisions of the Federal Court of Justice and the Federal Constitutional Court in the ANOM Proceedings,* Eucrim 4/2025, Preprint.

PROPISI I DOKUMENTI:

1. Direktiva (EU) 2014/41 Europskog parlamenta i vijeća od 3. travnja 2014. o Europskom istražnom nalogu u kaznenim stvarima (SL 2014., L 130, str. 1. i ispravak SL 2015., L 143), https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex%3A32014L0041, pristupljeno 5. svibnja 2026.

2. Direktiva (EU) 2023/1544 Europskog parlamenta i Vijeća od 12. srpnja 2023. o utvrđivanju usklađenih pravila za imenovanje imenovanih subjekata koji imaju poslovni nastan i za imenovanje pravnih zastupnika za potrebe prikupljanja elektroničkih dokaza u kaznenim postupcima, https://eur-lex.europa.eu/legal-content/hr/ALL/?uri=CELEX:32023L1544, pristupljeno 5. svibnja 2026.

3. Konvencija za zaštitu ljudskih prava i temeljnih sloboda („Narodne novine" – Međunarodni ugovori broj 18/1997., 6/1999. – pročišćeni tekst, 8/1999. – ispravak, 14/2002., 1/2006., 13/2017.).

4. Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalozima za dostavljanje i europskim nalozima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32023R1543, pristupljeno 5. svibnja 2026.

5. Ustav Republike Hrvatske („Narodne novine" broj 56/1990., 135/1997., 113/2000., 28/2001., 76/2010., 5/2014.).

6. Zakon o kaznenom postupku („Narodne novine" broj 152/2008., 76/2009., 80/2011., 121/2011., 91/2012., 143/2012., 56/2013., 145/2013., 152/2014., 70/2017., 126/2019., 126/2019., 130/2020., 80/2022., 36/2024., 72/2025., 13/2026.).

7. Zakon o pravosudnoj suradnji u kaznenim stvarima s državama članicama Europske unije („Narodne novine" broj 91/2010., 81/2013., 124/2013., 26/2015., 102/2017., 68/2018., 70/2019., 141/2020., 18/2024.).

8. Zakon o prekograničnom pribavljanju elektroničkih dokaza u kaznenim postupcima („Narodne novine" broj 151/2025.).

PRESUDE I DRUGE ODLUKE:

1. Apelacioni sud Crne Gore, presuda od 21. ožujka 2025., broj Kt-S 56/22.

2. Europski sud za ljudska prava, presuda u predmetu Lisica protiv Hrvatske, broj zahtjeva 20100/06 od 25. veljače 2010., § 59.

3. Europski sud za ljudska prava, presuda u predmetu Jalloh protiv Njemačke, broj zahtjeva 54810/00 od 11. srpnja 2006., § 105.

4. Europski sud za ljudska prava, presuda u predmetu Bykov protiv Rusije, broj zahtjeva 4378/02 od 10. ožujka 2009. § 90.

5. Europski sud za ljudska prava, presuda u predmetu Bašić protiv Hrvatske, broj zahtjeva 22251/13 od 25. listopada 2016., § 43–48.

6. Europski sud za ljudska prava, presuda u predmetu A. L. i E. J. protiv Francuske, broj zahtjeva 44715/20 i 47930/21 od 24. rujna 2024.

7. Europski sud za ljudska prava, presuda u predmetu Yüksel Yalçinkaya protiv Turske, broj zahtjeva 15669/20 od 26. rujna 2023.

8. Sud Bosne i Hercegovine, presuda od 10. srpnja 2025., broj S1 2 K 047599 23 K.

9. Sud Europske unije, presuda Općeg suda (peto vijeće) od 25. veljače 2026., predmet broj T-1180/23.

10. Sud Europske unije, presuda od 6. listopada 2020., predmet broj C-511/18, C-512/18 i C-520/18 (La Quadrature du Net i dr.).

11. Sud Europske unije, presuda od 30. travnja 2024., predmet broj C-670/22 (EncroChat).

12. Sud Europske unije, presuda od 6. rujna 2016., predmet broj C-172/15 (Petruhhin).

13. Sud Europske unije, presuda od 7. rujna 2023., predmet broj C-162/22 (Lietuvos Respublikos generalinė prokuratūra).

14. Savezni vrhovni sud Savezne Republike Njemačke, odluka od 2. ožujka 2022., broj 5 StR 457/21.

15. Visoki kazneni sud Republike Hrvatske, rješenje od 19. studenog 2024., predmet broj I Kž-Us-88/2024.

16. Visoki kazneni sud Republike Hrvatske, rješenje od 17. travnja 2025., predmet broj I Kž-Us-167/2024.

17. Vrhovni kasacijski sud Italije, presuda od 15. srpnja 2022., broj 32915/22.

MREŽNI IZVORI:

1. Computer Weekly, „FBI planned a sting against An0m cryptophone users over drinks with Australian investigators" (Computer Weekly, 11. lipnja 2021.), https://www.computerweekly.com/news/252502260/FBI-planned-a-sting-against-An0m-cryptophone-users-over-drinks-with-Australian-investigators, pristupljeno 27. svibnja 2026.

2. Cox, Joseph, „We Got the Phone the FBI Secretly Sold to Criminals" (Vice, 8. srpnja 2021.), https://www.vice.com/en/article/anom-phone-arcaneos-fbi-backdoor/, pristupljeno 6. travnja 2026.

3. EU Innovation Hub, „First report on encryption by the EU Innovation Hub for internal security, Publications Office of the European Union" (EU Innovation Hub, 2024.), dostupno na: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf.

4. European Commission, „European Evidence Project, European Data Informatics Exchange Framework for Courts and Evidence", www.cordis.europa.eu/project/id/608185/reporting/de, pristupljeno 1. travnja 2026.

5. Europol, „Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe" (Europol, 2. srpnja 2020.), https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, pristupljeno 5. svibnja 2026.

6. Europol, „New major interventions to block encrypted communications of criminal networks" (Europol, 12. ožujka 2021.), https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks, pristupljeno 5. travnja 2026.

7. Europol, „800 criminals arrested in biggest ever law enforcement operation against encrypted communication" (Europol, 8. lipnja 2021.), https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication, pristupljeno 5. travnja 2026.
8. Global Initiative Against Transnational Organized Crime, „Decryption of messaging app provides valuable insight into criminal activities in the Western Balkans and beyond", https://riskbulletins.globalinitiative.net/see-obs-013/01-decryption-of-messaging-app-criminal-activities.html, pristupljeno 31. ožujka 2026.
9. Organized Crime and Corruption Reporting Project „Police Arrest 48 After Hacking Cryptophones in Belgium, Netherlands" (Organized Crime and Corruption Reporting Project, 12. ožujka 2021.), https://www.occrp.org/en/news/police-arrest-48-after-hacking-cryptophones-in-belgium-netherlands, pristupljeno 5. travnja 2026.
10. Oxford Dictionary: https://www.oxfordlearnersdictionaries.com/definition/english/encryption#google_vignette, pristupljeno 31. ožujka 2026.
11. Vijeće Europske unije, „Bolji pristup e-dokazima u cilju borbe protiv kriminala", https://www.consilium.europa.eu/hr/policies/e-evidence/#e-evidence, pristupljeno 31. ožujka 2026.

EVIDENCE FROM SKY ECC AND ANOM ENCRYPTED COMMUNICATION

ABSTRACT

The paper explains the concept of electronic evidence in the criminal legislation of the Republic of Croatia, its methods of acquisition, how it is presented in court proceedings, and its importance in criminal proceedings. It also explains the concept of encryption, as well as the currently available information regarding encrypted communication platforms EncroChat, Sky ECC, and ANOM. Furthermore, the paper analyses the methods of obtaining such evidence through European Investigation Orders and requests for international legal assistance, as well as the transfer of such evidence to the Republic of Croatia for the purposes of initiating and conducting criminal proceedings. It also presents the current state of criminal proceedings in the Republic of Croatia concerning evidence related to communication via encrypted communication platforms Sky ECC and ANOM, as well as the actions of the Office for the Suppression of Corruption and Organised Crime in these cases from the moment information was received that certain individuals had used these platforms in their criminal activities. This is done by providing a chronology and an overview of the mechanisms for obtaining data through European Investigation Orders from the French Republic in relation to the Sky ECC platform, and through international legal assistance from the United States of America in relation to the ANOM platform. Furthermore, the paper provides an overview of the number of criminal cases currently pending in the Republic of Croatia in which such evidence is used, as well as the court decisions rendered to date concerning objections to the legality of such evidence, particularly in the context of the case law of the Court of Justice

of the European Union. In conclusion, the paper offers a brief overview of comparative case law in other Member States of the European Union and in countries in the region.

Keywords: digital evidence, encryption, encrypted communication platforms, EncroChat, ANOM, Sky ECC, international cooperation

Marijana Jurić Vukašin državnoodvjetnička je savjetnica u Uredu za suzbijanje korupcije i organiziranog kriminaliteta i doktorska kandidatkinja na Pravnom fakultetu Sveučilišta u Zagrebu. Tijekom studija bila je demonstratorica na Katedri za teoriju prava i sudjelovala je u radu Pravne klinike u Zagrebu kao studentska mentorica u Grupi za pomoć i zaštitu žrtava kaznenih djela. Nakon diplomiranja 2022. godine upisala je doktorski studij kaznenopravnih znanosti i počela raditi kao odvjetnička vježbenica, a u listopadu 2024. položila je pravosudni ispit. Od 2023. godine uključena je u praćenje razvoja pravnih pitanja vezanih uz osobe s duševnim smetnjama u Povjerenstvu za zaštitu osoba s duševnim smetnjama pri Ministarstvu pravosuđa, uprave i digitalne transformacije Republike Hrvatske. Također, od rujna 2024. sudjeluje kao istraživačica i administratorica na Erasmus+ projektu „Development and Implementation of Anti-Corruption Education Programs for Universities in Bulgaria, Greece and Croatia", a od veljače 2026. kao istraživačica na projektu „RISE Balkans: Osnaživanje glasova mladih: odgovornost, integritet, solidarnost i građanski angažman na Balkanu".

Sven Mišković diplomirao je 2007. na Pravnome fakultetu Sveučilišta u Zagrebu, a 3. prosinca 2010. položio je pravosudni ispit s posebnom pohvalom. Od 30. prosinca 2010. zaposlen je kao savjetnik u Županijskom državnom odvjetništvu u Zagrebu te je 8. travnja 2013. stupio na dužnost zamjenika općinske državne odvjetnice u Općinskom državnom odvjetništvu u Zagrebu. Dana 15. rujna 2014. upućen je u Ured za suzbijanje korupcije i organiziranog kriminaliteta kao zamjenik ravnatelja, dok je od 1. siječnja 2023. do 4. lipnja 2024. bio je voditelj Odjela tužitelja u Uredu za suzbijanje korupcije i organiziranog kriminaliteta, pri čemu je 29. siječnja 2024. imenovan zamjenikom županijskog državnog odvjetnika u Županijskom državnom odvjetništvu u Zagrebu. Istodobno je nastavio rad kao zamjenik ravnatelja Ureda za suzbijanje korupcije i organiziranog kriminaliteta. Od 5. lipnja 2024. do 31. prosinca 2025. obavljao je poslove vršitelja dužnosti ravnatelja Ureda za suzbijanje korupcije i organiziranog kriminaliteta, nakon čega je 1. siječnja 2026. stupio na dužnost ravnatelja Ureda za suzbijanje korupcije i organiziranog kriminaliteta. Dana 24. svibnja 2019. dodijeljena mu je Državnoodvjetnička nagrada.