**dr Aleksandra RAKOČEVIĆ** *

# DOKAZNI ZNAČAJ PODATAKA PRIBAVLJENIH DEKODIRANJEM KRIPTOVANIH KOMUNIKACIONIH PLATFORMI U CRNOGORSKOM KRIVIČNOM ZAKONODAVSTVU I EVROPSKI STANDARDI

**Sažetak**

*U fokusu istraživanja ovog rada je pravna priroda, odnosno dokazni značaj podataka prikupljenih demontažom šifrovanih telekomunikacionih mreža od strane pravosudnih i policijskih organa jednog broja država članica EU. Cilj istraživanja obuhvata analizu crnogorskog krivičnog zakonodavstva u oblasti specijalnih istražnih tehnika i njihovu usklađenost sa Direktivom 2014/41 EU o Evropskom istražnom nalogu i presudom u predmetu C-670/22 od 30. aprila 2024. godine Evropskog suda pravde u kontekstu obaveze države da krivično zakonodavstvo prilagođava brojnim društvenim promjenama koje generišu i nove oblike kriminaliteta. Glavno istraživačko pitanje glasi: „Da li se kriptovana komunikacija sa platformi Ennetcom, Anom, EncroChat i Sky ECC koje je presrela država u kojoj se ne vodi krivični postupak mogu koristiti kao dokaz u drugoj državi"? Odgovor na ovo pitanje zavisi od ispunjenosti uslova za realizaciju specijalne istražne radnje u nacionalnom zakonodavstvu i njihove kompatibilnosti sa evropskim standardima. U istraživanju dokaznog značaja online nadzora koristiće se metodologija pravnih nauka kroz jedinstvo u pristupu i integralno sagledavanje kvalitativne dimenzije predmeta istraživanja. Na osnovu rezultata istraživanja utvdiće se da li su ispunjeni zahtjevi nužnosti i proporcionalnosti prilikom prosleđivanja dokaza koji su u posjedu zamoljene države, da li se oni mogu koristiti po automatizmu ili se moraju ispuniti još neki uslovi kao što su obavještenje države čiji se državljani nadziru, poštovanje suverenosti države i osiguranje da se ne ugrozi nivo zaštite lica garantovane u toj državi, uspostavljanje balansa između zadiranja u pravo poštovanja privatnog života i komunikacije i neophodnosti zaštite društva od kriminaliteta i slično. Korišćenje dokaza koji su obezbijeđeni nadzorom i*

* Saradnica u nastavi na Pravnom fakultetu Univerziteta Crne Gore, email: rakocevic.a@ucg.ac.me

*dekodiranjem skrivenih komunikacionih platformi ukazuje na brojne izazove i otvorena pitanja koja se tiču zakonitosti njihovog korišćenja u krivičnom postupku u kontekstu masovnog nadzora ne samo učinilaca zločina već i svih osoba koje koriste istu aplikaciju zbog čega se u radu poklanja posebna pažnja rješavanju brojnih problema i otvorenih pitanja u ovoj oblasti.*

**Ključne riječi:** *krivično djelo, kriptovane komunikacije, dokazni značaj, crnogorsko zakonodavstvo, evropski standardi*

## I Uvod

U modernom dobu svijet se susrijeće sa novootkrivenim formama inkriminacija koje uzrokuju nespokojstvo stanovnika, koji doživljavaju neizvjesnost i nestabilnost kao i strepnju od viktimizacije. Izvršavanjem inkriminacija nastaju masovne posljedice i u poslednje vrijeme njihov broj raste, kao što se povisuju i novčana sredstva za borbu protiv tog vida kriminaliteta.[464]. Klasični mehanizmi suzbijanja modernih oblika kriminalnog manifestovanja demonstrirali su manjkavost i neučinkovitost. S tim u vezi nasušna je potreba otkrivanja i primjenjivanja produktivnijih modela suprostavljanja kriminalnim pojavama, u kom pogledu osobitu važnost imaju mjere tajnog nadzora. Savremena tehnička dostignuća vremenom nadomješćuju doskorašnju proceduru kada je u pitanju rasvjetljavanje delikata, koji su počinjeni od strane NN lica. Izrazita upotreba elektronskih tehnologija u kriminalističkom postupanju mogla bi poremetiti ravnotežu između težnje za očuvanjem privatnosti i intime kada je riječ o opiranju nedopuštenom uplitanju u temeljna prava čovjeka i sa druge strane opšteg interesa, koji se odnosi na primjenu modernih elektronskih aplikacija sa ciljem otkrivanja inkriminacija, detektovanja izvršilaca delikta i pribavljanja dokaznih sredstava namijenjenih za sprovođenje postupka u krivično pravnoj stvari. Mjere tajnog nadzora se mogu smatrati nepobitnim i neupitnim ako se prevashodno ustanovi da li su sprovedene u saglasju sa normama procesnog prava i ako se provođenjem istih ostvaruje zakonita i opravdana svrha u opsegu koji je nametnulo moderno demokratsko okruženje.[465] Na međunarodnom planu je izrađen veliki broj dokumenata, od

[464] Rakočević Velimir, *Krivična djela sa elementima organizovanog kriminaliteta-specijalne istražne metode,* Pravni fakultet Podgorica, Podgorica, 2015,336.

[465] Council of Europe, *Guide to ther Case-Law of the European Court of Human Rights*, Strasbourg, 2020,23.

kojih se izdvajaju konvencije, a iste predstavljaju temelj za ustanovljavanje specijalnih istražnih metoda u okviru krivične procedure mnogih zemalja Evrope. [466] Članom 50 Konvencije UN protiv korupcije reguliše se upotreba specijalnih metoda u istražnom postupku, od strane zemalja u toku pretresa u vidu dokaznog sredstva, od kojih se naglašavaju digitalno i ostali vidovi kontrolisanja, tajne aktivnosti i nadzirane pošiljke.[467] Savjet Evrope daje definiciju specijalnih istražnih tehnika i ista glasi: „Tehnike koje primjenjuju nadležni organi u kontekstu krivičnih istraga radi otkrivanja i procesuiranja teških krivičnih djela i osumnjičenih, sa ciljem prikupljanja informacija na način da o tome nemaju informacije ciljana lica“.[468] Izvršena je klasifikacija specijalnih istražnih metoda u državama članicama Evropske unije shodno mehanizmima unutar pravosudnog sistema i shodno posebnim istražiteljskim radnjama čija upotreba služi za primjenjivanje pravnih normi.

Determinisane su naredne posebne istražne tehnike u državama članicama Evropske unije :a) promatranje (surveillance); b) probijanje konverzacija (interception of communications), c) skrivene istrage (secret investigations), d) nadzirana pošiljka (controlled submissions), e) informatore (informants), f) partnerske istražne grupe (joint investigative teams). Sjutrašnjica i djelotvornost kolaboracije, kada je riječ o sprječavanju kvalifikovanih oblika inkriminacija sa međunarodnim elementom umnogome će biti određena sudjelovanjem zajedničkih istražnih timova, jer se bez istih ne bi mogle rasvijetliti počinjene inkriminacije iz oblasti organizovanog kriminaliteta.[469]

[466] Konvencija Savjeta Evrope o pranju, traženju, zaplijeni i konfiskaciji prihoda stečenih kriminalom, (1990). Strazbur, Konvencija UN protiv korupcije, 2000.

[467] Rakočević Velimir, „Tajni nadzor komunikacija u izviđaju i krivičnom postupku i zaštita prava na privatnost”,*Crnogorska revija za bezbjednost*, Podgorica, 2024, 11.

[468] Council of Europe: Committee of Ministers, *Recommendation Rec(2005)10 of the Committee of Ministers to Member States on "Special Investigation Techniques" in Relation to Serious Crimes Including Acts of Terrorism*, 20 April 2005, Rec(2005)10.

[469] Rakočević V,2024,12.

## II Pojam elektronskih dokaza u krivičnom postupku

Shodno prirodi dokaznog sredstva koji predstavlja izvor spoznaje i saznavanja određene pravno relevantne činjenice izvršena je podjela dokaza na lične i materijalne.[470] Veliki uticaj na prirodu dokaznih sredstava u krivičnom postupku imaju informaciono- komunikacione tehnologije. Digitalni nositelji informacija se u savremenom dobu manifestuju kao sredstva izvršenja delikata ili objekti na kojima se očitavaju tragovi krivičnih djela. Digitalni dokazi sadrže informacije koje se nalaze u računarskom obliku i posjeduju značaj činjenica pomoću kojih subjekt utvrđuje postojanje ili nepostojanje relevantnih činjenica na kojima sud zasniva odluku, a koji su obuhvaćeni računarskim uređajima, dok u krivičnom postupku koji je okončan shodno zakonskim odredbama posjeduju dokaznu vrijednost. Riječ je o sadržaju koji se skladišti ili emituje u binarnom obliku i na istom se uobličavaju dokazi.[471] Postoje u sistemima koji preko mreže obezbjeđuju resurse, portabilnim aplikacijama, elektronskoj isporuci, tekstualnoj komunikaciji, zapisima zvuka i video snimcima, raznovrsnim tehnologijama i tako dalje. Vrlo su problematizovana navedena dokazna sredstva kada je u pitanju njihovo pribavljanje i interpretacija. Postavljen je akcenat na vjerodostojnost, signifikantnost i pojmljivost istih od strane nosilaca sudijskih funkcija. Ukoliko bi došlo do dvojbe kada je u pitanju njihova vjerodostojnost, kao i skepse u pogledu tačnosti i ispravnosti ovog vida izvora podataka, u tom slučaju upitni su njegov legitimitet i praktičnost. Iz tog razloga neophodno je eliminisati kontaminaciju i krivotvorine kada je riječ o gore pomenutim izvorima informacija. Od fundamentalnog značaja je da se konkretni izvori informacija pribavljaju u skladu sa procedurom koja počiva na pravilima koja je zakon decidno propisao. Ukoliko navedeno ne bi bilo sprovedeno riječ bi bila o nezakonitim dokazima, a isti se izuzimaju iz cjelokupnih spisa u krivično pravnoj stvari. Kada se elektronski izvori informacija upotrebljavaju, od krucijalne važnosti je cjelovito posmatranje komponenata i sklopa inkriminacija u cilju upotpunjavanja i sveobuhvatnosti

[470] Radulović Drago, *Krivično procesno pravo*, Pravni fakultet Univerziteta Crne Gore, Podgorica, 2015, 160.

[471] Međunarodna organizacija za standardizaciju, Pravila za identifikaciju, pribavljanje i čuvanje digitalnih dokaza, Ženeva 2012.

dokazne konstrukcije. Njihovo pribavljanje i detaljna ekspertiza moraju osigurati vjerodostojnost, signifikantnost i pojmljivost.[472]

Od fundamentalnog značaja jeste Konvencija o računarskom kriminalitetu iz 2009. godine, a ista se odnosi na sprječavanja krivičnih djela koja su orijentirana ka pouzdanosti, kredibilitetu i raspoloživosti komjuterskih sklopova, baza i kompjuterskih podataka uz obuhvatanje preveniranja izigravanja ovih baza podataka. Poglavlje II reguliše materijalne krivično pravne odredbe koje determišu krivična djela kao nezakonit dostup, nezakonito presrijetanje, remećenje informacija, remećenje sistema, protivzakonita upotreba naprava, krivotvorenje koje se povezuje sa kompjuterima, računarske prevare, inkriminacije koje se odnose na dječju pornografiju i delikte povrede autorskih prava. Kada je riječ o procesnom dijelu odredbi ovaj akt predviđa skladištenje i okrilje sačuvanih računarskih podataka, izdavanje naredbe, praćenje i plenidbu sačuvanih podataka, pribavljanje podataka u stvarnom vremenu i presrijetanje podataka koji postoje u supstratu digitalnih korespodencija.[473] Iz navedenog dokumenta se da zaključiti da su odredbe koje on sadrži usmjerene ka pribavljanju izvora informacija u elektronskoj formi protiv izvršioca inkriminacija. Cilj navedenog akta je i pribavljanje informacija u stvarnom vremenu i presrijetanje podataka o kontentu konverzacije. Dopunski protokol odnosno drugi dodatni protokol uz Konvenciju o visokotehnološkom kriminalu, umnogome je poboljšao i ojačao međudržavnu kolaboraciju, kada je riječ o detektovanju digitalnih izvora informacija, pospješivanja postupka prikupljanja i objelodanjivanja elektronskih dokaza. Na taj način stvorena je adekvatna pravna podloga za unapređenje saradništva u borbi protiv kriminalnih aktivnosti protiv bezbjednosti računarskih podataka i učvršćuje kapacitete pravosudnih institucija na polju pribavljanja dokaznih sredstava u elektronskom obliku za pozamašan spektar krivičnih djela. [474]Tako je regulisana procedura za osnaživanje direktne kolaboracije sa provajderima, pravnim entitetima i ostalim učesnicima u ugovornim odnosima, osobito kada je u pitanju nalog za registraciju naziva djelokruga, detektovanja informacija o pretplatniku, provođenja zahtjeva drugog učesnika u ugovornom odnosu za

[472] Rakočević V., 2024, 17.

[473] Zakon o potvrđivanju Konvencije o računarskom kriminalu, Službeni list CG-Međunarodni ugovori, br. 4/2009.

[474] Drugi dodatni protokol uz Konvenciju o visokotehnološkom kriminalu, 2020.

neodložno dopremanje informacija o korisniku usluga i informacija o saobraćaju, detektovanja uskladištenih digitalnih podataka bez odlaganja u vanrednom slučaju, partnerske istražne grupe i zajedničkih istražnih postupaka, zaštite podataka o ličnosti i tako dalje.

## III Pravna priroda podataka pribavljenih dešifrovanjem kriptovanih aplikacija

U predmetnom radu provedena je analiza pravne prirode i dokazne relevantnosti korespodencija realizovanih upotrebom Sky ECC aplikacije, za koju se može sa pouzdanošću tvrditi da je izrazito prisutna u krivičnim postupcima koji se vode za krivična djela, koja potpadaju pod organizovani kriminalitet, u našoj državi i mnogobrojnim zemljama Evrope i označava slojevit dokazni fenomen.

Izvršioci inkriminacija već duži vremenski period ne upotrebljavaju klasične oblike konverzacije, zbog postojanja bojazni od činjenice da budu kontrolisani od strane oficijelnih struktura. S tim u vezi masovna je primjena kriptovanih tehnologija kojima se garantuje bezbjedno odašiljanje podataka. Elektronski izvori informacija poput korespodencije putem mobilnog aparata, mejlova i tako dalje, umnogome pogoduju učinkovitosti i djelotvornosti, kada je u pitanju detektovanje i gonjenje izvršilaca zločina. Upotreba digitalnih izvora informacija pribavljenih kontrolom i dešifrovanjem prikrivenih konverzacijskih aplikacija upućuje na mnoge rizike i upitna je validnost i legitimitet njihove primjene u okviru krivične procedure, a u smislu pojačanog praćenja kako izvršilaca inkriminacija, tako i drugih lica koja konzumiraju identični primjenjljivi program, koje može ugroziti pravo na privatnost. U pitanju su Ennetcom, Anom, EncroChat i Sky ECC šifrovane platforme i njihovim dekodiranjem pribavljene su informacije koje su poslužile kao osnov za krivično gonjenje velikog broja lica zbog osnovane sumnje da su počinili mnogobrojna krivična djela.[475]

Navedene konverzacijske aplikacije upotrebljavaju se za tajnu korespondenciju upotrebom specijalnih primjenljivih programa za uzajamno davanje i uzimanje informacija koje su utemeljene na Off-the –Record Messaging, koji je kriptografski protokol. Preimućstvo OTR metoda u cilju čuvanja informacija ogleda se u momentalnom kriptovanju informacija koji se potom dopremaju preko primarnih sistema koji obezbjeđuju resurse do

[475] Rakočević V, 2024, 18.

konačnog recipijenta. Važno je istaknuti da je ovaj način konverzacije bio neprikladan za implementaciju mjera tajnog nadzora, sa razloga skrivanja identiteta pretplatnika, čija obilježja nisu postojala na platformi.

Proglasom Europol/Eurojusta koji je objavljen u julu mjesecu 2020.godine i nozi naziv "Demontaža šifrovane mreže šokira organizovane kriminalne grupe širom Evrope", prezentovani su učinci zajedničkog istražnog tima za dekodiranje EncroChat kriptovane mobilne telefonije. Istaknuli su da je u prethodnom periodu njihova timska istraga obezbijedila probijanje, distribuiranje i ispitivanje velikog broja poruka, a iste su prosleđivane između počinilaca kriminalnih radnji u cilju vršenja krivičnih djela sa elementima organizovanog kriminaliteta. Naglašava se da su se oficijelne strukture, koje primjenjuju propise umnogome upoznale sa navedenim informacijama u stvarnom vremenu, putem "ramena nesuđenih pošiljalaca". Dalje je navedeno da su zemlje Evrope, u novijem periodu uzdrmanije usljed aktivnosti zločinačkih grupacija, a one su široko zastupljene i izuzetno adaptabilne što imputira ugrožavanje sigurnosti na evropskom podneblju. Ističu da su malverzacije povezane sa šifrovanim konverzacijskim napravama krucijalni katalizator zločinačkih djelovanja. Policijske i pravosudne strukture Francuske već sedam godina promatraju mobilne uređaje koje upotrebljavaju osigurani konverzacijski materijal EncroChat, sa razloga što su primijetili da su mobilni uređaji naznačenih obilježja često pojavljivani u aktivnostima protiv zločinačkih grupa i važna činjenica da pomenuto pravno lice radi sa sistema za obezbjeđivanje resursa u Francuskoj. Nadalje je obezbijeđeno montiranje elektronske naprave koja nadilazi shemu kodiranja i istovremeno dostup korespondenciji pretplatnika. Aplikacija EncroChat godine 2020. predstavljala je jednog od vodećih mobilnih operatera kriptovane elektronske korespondencije sa izrazitom intervencijom lica kod kojih postoje osnovi sumnje da su počinioci velikog broja delikata, gdje po incidenci preovlađuju nedozvoljena proizvodnja, držanje i stavljanje u promet kokaina i kanabisa i krivično djelo pranja novca. Eskalacija kriptovane mobilne platforme EncroChat koju su koristile zločinačke grupe diljem planete, dovela je do toga da postupajući organi Francuske tokom 2019. godine započnu krivični postupak u EU Agency for Criminal Justice Cooperation protiv Holandije. U prethodnom postupku pribavljene su informacije shodno odredbama francuskih propisa i uz odobrenje suda, u opsegu internacionalne krivično pravne kooperacije. Informacije bivaju ispostavljane Holandiji, dok agencija EU koja se bavi

kooperacijom pravosudnih organa u krivičnim predmetima, osigurava kreiranje zajedniče istražne grupe uz aktivnu angažovanost Europola i Eurojusta u periodu 2020.godine. Počevši od 2018.godine Europol je kontinuirano angažovan kada je riječ o prvoj fazi prethodnog postupka koji se sprovodi u Francuskoj i Holandiji u ulozi informacionog središta i metodičko strategijske potpore. Krucijalna funkcija Europola se sastojala u omogućavanju autentičnog planetarnog upliva u dimenzije i djelovanje zločinačkih asocijacija kao ishod okončanih prvih faza prethodnih postupaka. Masovna raspoloživa grupa Europola analizirala je u stvarnom periodu višemilionske izjave i informacije za vrijeme istražnog postupka, naizmjenično pregledala i istražila informacije i omogućila i šifrovala zajedno sa saradnicima raspodjelu podataka zemljama odakle potiču počinioci inkriminacija. Godine 2020. probijanje EncroChat razmjene podataka se finalizuje u momentu svjesnosti odgovornog lica predmetnog privrednog društva činjenice presrijetanja komukacije od strane postupajućih organa i naloga pretplatnicima da devastiraju mobilne uređaje. Kada je riječ o EncroChat mobilnim uređajima oni se prezentuju klijentima kao sigurna aparatura za nepogrešivu diskreciju s obzirom na činjenicu da ne postoji identifikovanje aparata ili modula koji sadrži jedinstveni broj sa nalogom pretplatnika i isti se dobavljaju shodno kriterijumima, kojima se obezbjeđuje nepostojanje uporedivosti. Nadalje se garantuje perfektna komocija vezana za dva sučelja, to jeste obostrani program za rukovođenje uređajima, kodirano sučelje je tajno i nema slikovnih zapisa, zvučnika, GPS i USB priključaka. Posjedovao je aplikacije za osiguranje nesankcionisanja pretplatnika, što znači momentalno uklanjanje prepiski sadržanih u krajnjim aparatima priključenih na mrežu njihovih akceptora, poseban lični identifikacioni broj koji je prilagođen za momentalno uklanjanje cjelokupnih informacija na aparatu i eliminisanje informacija ako dođe do višestrukih upisa netačnih šifri. Na taj način je garantovano efikasno uništavanje diskreditujućih prepiski.[476]

Nadalje francuski, američki, belgijski i holandski inspektori dekodiraju ostale kriptovane platforme poput Sky ECC, ANOM i Exclu čime se

[476] Europol/Eurojust, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, 2020, https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe pristup 15.X 2024. godine.

garantuje dostup nekoliko biliona prepiski koje su dijeljene putem naznačenih aplikacija. SkyECC mreža djeluje po principu šifrovanja i posjeduje dva ključa koji obezbjeđuju isključivo adresantu i recipijentu upoznavanje sa supstratom prepiski. Za enkripciju prepiski je služio jedan od dva ključa dok je namjena drugog bila usmjerena na njihovo dekodiranje. U pitanju je nelinearno šifrovanje sa izrazito visokim stepenom sigurnosti koji zabranjuje dešifrovanje prepiski bez registrovanja dva ključa. Oficijelne strukture su u toj situaciji prvenstveno detektovale šifrovanu korespodenciju iz date aplikacije, potom dekodirale raznovrsne kriptovane prepiske. Francuska, belgijska i holandska policija su sprovodile kontrolu nad cjelokupnom konverzacijom zaključno sa 2021. godinom i tada je FBI realizovao konfiskaciju dok je titular prava svojine na predmetnoj aplikaciji gonjen.[477]

Informacije koje proističu iz kriptovanih korespodencija prikupljene su dvojako odnosno pregledom supstrata kriptovane konverzacije ili neposrednom kontrolom nad razmijenjenim prepiskama. Sky ECC mreža shodno podacima postupajućih organa velikog broja zemalja starog kontinenta upotrebljavana je za činjenje inkriminacija poput nedozvoljene trgovine drogom i oružjem izvršenih od organizovanih zločinačkih grupa i ista je dešifrovana presrijetanjem Sky ECC šifrovanja. S tim u vezi sudski organi imaju obavezu da tokom razmatranja o legitimnosti i relevantnosti izvora informacija ustanove modalitet obezbjeđenja istih. Sistematizovanje konverzacije nosilaca kriminalnih aktivnosti uglavnom se obavlja upotrebom specijalnih istražnih tehnika ili pregledom mobilnog aparata za skladištenje informacija u digitalnom obliku i pod datim okolnostima zdravoumno lice nikako ne može negirati njihov dokazni kredibiltet. Kriptovana korespodencija prouzrokuje da informacije nijesu pribavljene korišćenjem tehnika na tačno određena lica već u okviru sveopšte kontrole neutvrđenog procenta lica. U situaciji ako bi se podaci pribavljeni dekodiranjem šifrovane razmjene prepiski posmatrali kao dokazno sredstvo u određenim krivičnim stvarima tad se postavljaju raznolike pravne nedoumice, osobito kada je riječ

[477] Lyons H. Judd (2021- 09.03.) *Cracing of encrypted messaging service dealt major blow to organised crime*, The Brussels Times, **https://www.brusselstimes.com/news/belgium-all-news/159039/cracking-of-encrypted-text-messaging-service-sky-ecc-app-dealt-major-blow-to-organised-crime**,2021,1, pristup 21. X 2024. godine.

o zemljama u okviru kojih informacije nijesu neposredno pribavljene.[478] U slučaju da su dokazi obezbijeđeni preko internacionalne krivično pravne pomoći uobičajenost je da njihov legitimitet nije upitan i isti se većinom ravnaju sa aktivnostima u prvoj fazi prethodnog postupka u zemlji molilji. Podaci obezbijeđeni posredstvom internacionalne detektivske kolaboracije Interpola i Europola se smatraju službenim informacijama i bitna su podloga za upotrebu mjera tajnog nadzora.

Nadalje sudovi SAD-a, Australije, Njemačke, Francuske i Holandije oglasili su krivim pojedina lica, a čije su odluke najvećim dijelom zasnovane na informacijama pribavljenim upotrebom EncroChat aplikacije, dok u našoj državi ne postoji sudska odluka sa klauzulom pravosnažnosti u okviru koje je supstrat ove konverzacije isključivi izvor informacija. Sudovi u našoj državi su potvrdili optužnice a u okviru istih predložena su dokazna sredstva koja se vezuju za Sky konverzaciju. Oficijelne strukture su se pozivale na Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima.[479] U odluci se ističe da su izvori informacija pribavljeni shodno propisima zemalja u kojima su osigurani i uvažavani su postulati međusobnog priznavanja i pouzdanja i isti su relevantni u zemlji molilji. Kada je riječ o postupcima u krivičnim stvarima branioci okrivljenih su bili stanovišta da je riječ o dokaznim sredstvima koji su nevjerodostojni, krivotvoreni i obezbijeđeni protivzakonitim tehnikama. Državne strukture nadležne za procesuiranje učinilaca krivičnih djela u određenom nizu predmeta nisu omogućili uvid u dokumentaciju iz prve faze prethodnog postupka ističući skrivenost informacija i navodeći argumente državne sigurnosti. Pravilo jeste obezbjeđenje gonjenim licima da koriste srazmjerna sredstva pa su s tim u vezi zahtijevane informacije o načinu pribavljanja informacija i garancija istinitosti i vjerodostojnosti dokaza. Kako ne egzistiraju tehnološki podaci o postupku pribavljanja informacija i tačnosti dokaznih sredstava ustanovljeno je da postupajuće strukture nisu kodirale prepiske, sa kog razloga ne može se istinitost tih podataka podvesti pod skepsu. S tim u vezi Vrhovni sudovi su utvrdili legitimnost dokaza.[480]

[478] Simović N. Miodrag, Šikman Mile, „Sadržaj šifrovane komunikacije ( Ennetcom, EncroChat, SkyECC, ANOM, Excly) kao dokaz u krivičnom postupku“, *Pravo i pravda*, Udruženje sudija/sudaca u Federaciji Bosne i Hercegovine, 2023, 227.

[479] Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima, Službeni list CG, br.4/2008, 36/2013.

[480] Goodwin Bill (2022). *French Supreme Court reject EncroChat verdict after lawyers question secrecy over hacking operation,*

Neophodno je napomenuti da su informacije u zemljama EU prikupljane putem Evropskog istražnog naloga shodno principu uzajamnog povjerenja. Sa tog razloga ne može se dovoditi u pitanje legitimitet dokaza koji su prikupljeni u drugoj zemlji jer bi bio diskutabilan suverenitet iste.

U savremeno doba u većini zemalja nije formirana institucionalna baza za skriveno presrijetanje šifrovane korespodencije u svrhu dekriptovanja materijala. U pitanju je internet kontrola, neovlašćeni pristup hardveru i tako dalje. [481] Kontrola nad Sky ECC konverzacijom, na koji način su prikupljeni dokazi, ne može se sprovesti unutar mnogih zemalja. U slučaju da se ustanovi da su dokazna sredstva obezbijeđena činjenjem inkriminacije iz grupe krivičnih djela protiv bezbjednosti računarskih podataka a riječ je o krivičnom djelu pravljenje i unošenje računarskih virusa iz člana 351 KZ CG korišćenje navedenog dokaznog sredstva smatralo bi se nezakonitim.[482]

Kada je riječ o dokaznoj sadržini koja proističe iz Sky ECC prepiski, ista ne smije da bude glavni izvor informacija na kojoj bi se zasnivala presuda kojom se okrivljeni oglašava krivim, naprotiv ona bi morala biti u sadejstvu sa ostalim personalnim i stvarnim dokazima. Jedan od izazova jeste skladištenje informacija koje nisu analizirane i kasnija upotreba istih. U slučaju da branioci okrivljenih lica nisu upoznati sa sadržinom predmeta i ne raspolažu znanjem na koji način su informacije prikupljene, promatrane i izviđavane, u toj situaciji odbrana ne može se očitovati na korišćenje informacija koje proističu iz kodiranih platformi. Najzad neophodno je da se obezbijedi da branioci i branjenici upoznaju materijal iz prepiski što podrazumijeva tehnike prikupljanja i raspolaganja sadržajem od trenutka donošenja akta da se prikupi sadržaj do čina prosleđivanja oficijelnim strukturama. Na ročištima tokom vođenja krivičnog postupka od velikog je značaja da se ispitaju sve komponente prikupljanja i transfera Sky komunikacija a isto je obuhvaćeno pravom na odbranu u svrhu analize legitimnosti i tačnosti svih vidova pomenute konverzacije. Okrivljenom mora biti omogućeno pravo na pristup sudu i pravo na postupak odgovarajućeg kvaliteta. Ukoliko dođe do upotrebe digitalnih informacija, koje nisu

https://www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy, pristup 1. XI 2024. godine.

[481] Bajović Vanja, „Encrochat i Sky ECC komunikacija kao dokaz u krivičnom postupku“, *CRIMEN (XII)*, 2/2022, 154.

[482] Rakočević V, 2024, 21.

analizirane, tvore se izrazite šanse za narušavanje vjerodostojnosti istih. Otvaraju se i pitanja eksplikacije, datih informacija, koje može podrivati vjerodostojnost dokaznog sredstva.[483]

## IV Presuda Suda pravde Evropske unije u predmetu C-670/22 od 30. aprila 2024. godine

U ovom radu postavljen je akcenat na presudu u predmetu C-670/22 od 30.aprila 2024. godine Suda pravde Evropske unije i učvršćena su pravila o pravnom pitanju od opšteg značaja koja su upravljena ka tome da informacije prikupljene probijanjem šifrovanih telekomunikacionih naprava u ostalim zemljama se ne upotrebljavaju mahinalno, već isključivo pod određenim kriterijumima. U pitanju je presuda koja se većinom odnosi na Evropski istražni nalog preko koga su Sky ECC informacije proslijeđene državama članicama Evropske unije. Sud pravde Evropske unije naglašava da se krucijalnost i srazmjernost specijalnih istražnih metoda definišu saglasno domaćem zakonodavstvu zemlje koja je naložila, odnosno zemlje u kojoj se dokazno sredstvo upotrebljava, što imputira činjenicu da se identična tehnika ustanovljava pod identičnim parametrima i u legislativnom okviru druge zemlje gdje se informacije primjenjuju. Zemlja članica na čijem području obitavaju osobe, čija se konvezacija kontroliše neophodno je da bude informisana o toj činjenici i u onim situacijama kada stručna podrška iste nije neophodna za sprovođenje mjera tajnog nadzora. U navedenoj odluci zahtijeva se uvažavanje prava okrivljenog kao i pravo na pristup sudu i postupak odgovarajućeg kvaliteta, dok iz svega se da zaključiti da okrivljeni ima prostora da spori prikupljenu dokaznu građu. Istaknuta odluka ima pravne posljedice na podneblju država članica Evropske unije, međutim ona bi pod određenim okolnostima mogla biti primjenjivana i kada je riječ o zemljama van zajednice evropskih naroda. Podaci koji su produkt kodirane konverzacije prvenstveno se preko Europola prosleđuju pravosudnim institucijama članica u vidu operativnih podataka a nakon toga shodno propisima procesnog prava u okvirima međunarodne pomoći u krivičnim stvarima.

Pravosudne institucije u nekolicini država oglasili su krivim određena lica većinom na temelju dokaznih sredstava pribavljenih primjenom EncroChat aplikacije. U našoj državi pokrenuto je mnoštvo postupaka u

[483] *Ibid*.

kojima nezaobilazni dokazi se crpe iz dekodirane Sky ECC platforme. Ne egzistira zasad niti jedna presuda koja je postala pravoznažna a u kojoj se odlučne činjenice utvrđuju putem datog vida izvora informacija. U trenutnim procedurama sudska vlast uvažava poimanja tužilačke strane da su dokazna sredstva pribavljena preko međunarodne pomoći i, da je dokazna aktivnost inostrane institucije realizovana shodno propisima te države. U našem sistemu je nedopuštena upotreba pojedinih dokaza i dokaznih sredstava, kao i da aktivnosti u prethodnom postupku budu usaglašeni sa principima domaćeg prava i opšteprihvaćenim pravilima međunarodnog prava.

Veliko vijeće Evropskog suda pravde je 30. aprila 2024. godine, odlučilo u predmetu C-670/22, a povodom zahtjeva za prethodnu odluku na osnovu člana 267 UFEU-a Zemaljskog suda u Berlinu od 19. oktobra 2022.godine, a koji je u sudsku instituciju zaprimljen dana 24. oktobra, 2022. godine.[484] Zahtjev Zemaljskog suda u Berlinu se odnosio na veliki broj pitanja a koja su sagledavana i ocijenjena diskutabilnim, a ista su se manifestovala u predmetnom krivičnom postupku pokrenutom protiv osobe M.N. [485]Pozamašan segment probnog odlomka Evropskog suda pravde od 30. aprila 2024. godine je identičan ili izuzetno blizak zaključcima Generalnog advokata koji djeluje pred Sudom pravde EU, kao na primjer eksplikacija značajnih propisa koja su vezana za obezbjeđivanje podrške u krivičnim predmetima u odnosu postupajućih struktura država članica EU, a naročito propisa koji se bave Evropskim istražnim nalogom. U presudi se ističu i mnoga eklatantna pitanja koja je prezentovao pomenuti Regionalni sud u Berlinu, i izrazito važna stanovišta ostalih oficijelnih struktura u predmetnom krivičnom postupku u Njemačkoj. Postavljeni zahtjev za preliminarnu presudu Suda pravde EU je obezbijedio pravosudnim strukturama zemalja članica EU u krivičnim stvarima koji teku, odnosno pred kojima oni postupaju, da ukazuju Sudu pravde na pitanja od značaja za interpretaciju prava EU ili da upućuju na pitanja o valjanosti pojedinih propisa u okvirima Evropske unije. Vrlo je važno istaći da Sud pravde EU nije taj koji presuđuje u tačno određenom postupku, nego je na domaćim pravosudnim institucijama

[484] Judgment 30/04/2024-M.N. (EncroChat) Case C-670/22.

[485] European Court of Justice, *Judgment of the Court (Grand Chamber) C-670/22 of 30 April 2024*, https://curia.europa.eu/juris/document/document.jsf?text=&docid=285365&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=323072 , pristup 8. XI 2024. godine.

da usklade svoja odlučivanja sa presudom Suda pravde EU, koja je zatim, u značenju izvora prava i kroz identičan modalitet obligatorna i za ostale domaće pravosudne strukture unutar država članica EU, koji se nađu pred istovjetnim pravnim dvojbama.[486] Dolazimo do zaključka da, načelni pravni stavovi Suda pravde EU izričito i faktički obavezuju oficijelne strukture, zemalja koje su članice Evropske unije. Izrazito su važne naredne tvrdnje i formulacije koje su sastavni dio sadržaja presude Evropskog suda pravde u predmetu C-670/22.[487]

1) Evropski istražni nalog se vezuje za prenos izvora informacija koje se nalaze u faktičkoj vlasti oficijelnih struktura države članice koja realizuje nalog (u konkretnoj sistuaciji u pitanju je Francuska), i ne potencira se da je sud u obavezi da donese akt u vezi sa tim, već se prijenos može vršiti i na temelju odluke državnog tužilaštva, u situaciji kada je u određenoj državi isto ovlašćeno da postupa, i onda kada je riječ o gotovo identičnim „nacionalnim stvarima“, za koje se vezuje nalog kako bi se priložili dokazi koji su ranije obezbijeđeni.

2) Državni tužilac (u konkretnoj situaciji njemački), ne odbacuje šansu kada je u pitanju izdavanje Evropskog istražnog naloga za transfer dokaznih sredstava koji se nalaze kod postupajućih struktura države izvršenja Evropskog istražnog naloga, a koja je članica Evropske unije, u kojoj su informacije prikupljene probijanjem konverzacija pretplatnika elektronskih naprava koji putem jedinstene zbirke kompjuterskih programa i usavršenog hardvera, obezbjeđuju kodiranu korespodenciju, pod pretpostavkom da Evropski istražni nalog zadovoljava sve kriterijume koje reguliše domaći zakonodavni okvir države čija nadležna institucija izdaje Evropski istražni nalog u nacionalnom izuzetno podudarnom slučaju.

3) Kada je u pitanju izdavanje Evropskog istražnog naloga pribjegava se sličnim pretpostavkama koji se koriste i kad je riječ o transferu identičnih dokaza u gotovo istovjetnim nacionalnim situacijama u određenim zemljama članicama EU. Važno je napomenuti da nije neophodno ispunjenje onih uslova koji se koriste kada je riječ o obezbjeđenju dokaznih sredstava. Ono

[486] Škulić Milan, „Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje-kao što su Sky ECC i EnchroChat”, *Crimen*, Beograd 2024, 46.
[487] *Ibid.*

što nije od značaja u konkretnom primjeru jeste fakat da su ovlašćene francuske oficijelne strukture u Njemačkoj shodno potrebama njemačkih saradnika pribavljali dokazna sredstva. Najzad, postupajući organ koji rukovodi krivičnim postupkom mora imati ovlašćenje da razmotri i analizira uvažavanje temeljnih ljudskih prava lica u pitanju i na koje se odnosi sprovedeni Evropski istražni nalog, a radi se o okrivljenim licima u određenom krivičnom postupku.[488]

4) Kada su u pitanju tehnike koje se odnose na inkorporiranje telekomunikacionih aparata, koje imaju za cilj pribavljanje informacija o prometu, području i konverzaciji koja se zasniva na online sadržaju, o istima je neeophodno da bude informisana država članica EU, na čijem prostoru obitava lice zbog kojeg se mjere i sprovode. U konkretnoj situaciji u pitanju je Njemačka. [489] Postupajuća struktura države članice EU posjeduje ovlašćenje izjašnjavanja o tome da se takva aktivnost ne bi trebalo realizovati ili da je neophodno okončati ostvarenje iste, u slučaju da takva radnja ne bi bila prihvaćena u istovjetnoj domaćoj situaciji. Cilj ovog korpusa prava i obaveza nije samo obezbjeđenje uvažavanja suvereniteta država članica EU, nego i štićenje prava okrivljenih lica, u konkretnim krivičnim postupcima.

5) Od domaćih postupajućih organa u državama članicama EU, potražuje se da odstrane dokazna sredstva, kada je u pitanju vođenje krivičnog postupka protiv osobe za koju postoji osnovana sumnja da je izvršila inkriminaciju, i to u sljedeća dva slučaja: a) ako to određeno lice nije bilo u mogućnosti da daje primjedbe na te dokaze, odnosno da ih demantuje i da ih osporava, kao i b) kada je očito da će ti dokazi imati dominantnu ulogu. na utvrđivanje pravno relevantnih činjenica.

[488] Škulić M, 2024, 47.

[489] Ne samo da su se aktuelne konverzacije probijale i kontrolisale i sprovodile putem kompjuterskih sistema i to najučestalije u drugoj zemlji, nego je najobimniji sadržaj te korespodencije bio iz prošlih vremena, da bi ona zatim bila pohranjena u uređajima koji su predstavljali server.

**A. Stvarni uticaj presude Evropskog suda pravde od 30. aprila 2024.**

Presuda Evropskog suda pravde, čija je sadržina izuzetno precizna, nedvosmislena, obavezujuća je na području država članica EU, odnosno obavezuje njihove ovlašćene postupajuće strukture i to u potpunosti u pravcu implementacije propisa Evropske unije, a koja se odnosi na kolaboraciju država članica Evropske unije to jeste njihovih postupajućih struktura, sa stavljanjem akcenta na realizaciju instrumenta Evropskog istražnog naloga. Pojedini stavovi i gledišta Evropskog suda pravde koji su pretočeni u okviru navedene presude u predmetu C-670/22, mogli bi u adekvatnom obimu posjedovati upliv i na razmatranje prakse pravosudnih institucija onih država starog kontinenta koje nisu članice EU, međutim one se suštinski ubrajaju i čine dio gotovo istovjetnog pravnog okruženja i priklonjene su evropskoj praksi i baštini, međutim, isključivo do granice koja izvire i proističe iz praktičnog provođenja mjerodavnog domaćeg prava. Dakle postaviće se kao obligatorna za države u pitanju generalna zakonska rješenja, kada je riječ o konkretnom krivičnom postupku, kao i rješenja koja su sastavni dio izvora međunarodnog prava i koja su primjenjivana za prikupljanje i pribavljanje preciznih i opipljivih dokaznih sredstava koja su proistekla iz šifrovane konverzacije. Sljedeći su izvori gore navedenih pravila: Evropska konvencija (Konvencija Savjeta Evrope) o međusobnom pružanju pravne pomoći u krivičnim stvarima sa dodatnim protokolom, međunarodni ugovori o pružanju pravne pomoći u krivičnim stvarima sa određenim državama, Budimpeštanska konvencija o „sajber“ (kibernetičkom) kriminalitetu, i domaća zakonska rješenja u pogledu međunarodne krivičnopravne pomoći, poput u Crnoj Gori Zakona o međunarodnoj pravnoj pomoći u krivičnim stvarima.[490]

Stanovište Suda pravde EU o tehnikama pomoću kojih su prikupljena određena dokazna sredstva, potom transportovani provjedbom Evropskog istražnog naloga, je obligatorno na području država članica EU, a trebalo bi se prihvatiti i kada je riječ o gotovo podudarnom domaćem postupku. Navedeno nije upitno kod država koje su posjedovale zajedničke istražne grupe i čija tijela su udruženo i kolektivno participirala u prikupljanju dokaznih sredstava probijanjem prepiski realizovanih putem platformi za kodiranje korespodencije. Istovjetna situacija je bila sa Francuskom,

[490] Škulić M, 2024, 48.

Belgijom i Holandijom. U tim situacijama zadovoljen je uslov da su postupajuće strukture države članice EU na čijem području egzistira lice na koga su te aktivnosti usmjerene, bili informisani o sprovođenju radnji, u slučaju da je to lice bilo u nekoj od datih zemalja, čije su postupajuće strukture bile dio zajedničkog istražnog tima. Najzad, njemačko krivično procesno pravo i krivična zakonodavstva drugih država članica EU sadrže srodne tehnike i odnose se na konkretne specifične dokazne aktivnosti takve prirode. Naglašeni zahtjev se istinski ne odnosi na zemlje koje ne pripadaju zajednici evropskih država.Važno je istaći da kada je riječ o dužnosti informisanja države na čijem je području „subjekt koji je predmet nadzora" i ona se u potpunosti tiče zemalja članica i to kroz sprovođenje aktuelnih sistema i instrumenata oficijelne konverzacije postupajućih struktura tih država unutar Europol-a, i Eurodžasta, i ta dužnost zvanično ne postoji na podneblju zemalja izvan Evropske unije, i kada je o njima riječ ne egzistiraju istovrsni konverzacioni putevi.[491]

## V Zaključak

U današnjem vremenu ne može se opovrgnuti niti negirati konstatacija i determinantna da je probijanje i presrijetanje kriptovanih modela konverzacije učinilaca inkriminacija koje su sprovele postupajuće strukture određenog broja zemalja starog kontinenta značajno pridonijelo detektovanju teških oblika inkriminacija sa elementima organizovanog kriminaliteta. Uglavnom, kako bi konkretni materijal bio smatran dokazom u krivičnom postupku nužno je ustanoviti polazište i vjerodostojnost istog. Branjenici sa njihovim braniocima imaju neprikosnoveno pravo da daju primjedbe na te dokaze, odnosno da ih demantuju. S tim u vezi neophodno je ispitati na koji način se došlo do zaštićenih konverzacija to jeste ustanoviti mehanizam prikupljanja izvora informacija. Države, u čijim okvirima su pribavljena dokazna sredstva, shodno domaćem zakonodavstvu nemaju dužnost da mehanizam prikupljanja dokaza učine transparentnim, što bi moglo rezultirati propadanjem istih. Posebno je otežavajuća situacija da u posjedu osumnjičenih lica ne budu otkriveni šifrovani mobilni uređaji gdje bi se stvorila uzročna veza sa dokaznim sredstvima pribavljenim preko međunarodne pravne pomoći u krivičnim stvarima. Kontrola konverzacija treba da važi za tačno određene pojedince a ne isključivo za Sky platformu, a

[491] *Ibid.*

odvajanje informacija sa sistema koji preko mreže obezbjeđuje resurse upućuje na nesrazmjernost metode. Kada je u pitanju dokazni značaj te vrste podataka ne može za iste garantovati tvrdnja da je dokaz pribavljen putem međunarodne krivično pravne pomoći. Pri integralnom poimanju situacije neophodno je bilo ustanoviuti kojim mehanizmom je druga zemlja pribavila dokazni sadržaj i da li su te radnje u opreČnosti sa domaćim pravilima. Najzad krucijalno je napomenuti da se Sky mreža ni u moderno doba ne može promatrati i nadgledati upotrebom mjera tajnog nadzora zbog manjka i nedovoljnosti digitalnih sistema kojima naša država barata. U konačnom važno je istaći da će vrijeme koje je pred nama i u kojem će se ostvarivati buduća sudska praksa i iznad svega načelni pravni stavovi i shvatanja najviših istanci pojedinih država demonstrirati kakva je zapravo vrijednost i nivo značajnosti niza faktora, koji bi suštinski mogli imati efekat na dokazni kredibilitet one vrste podataka, koji potiču iz izuzetno specifičnih istražnih metoda.

**Aleksandra RAKOČEVIĆ, PhD***

# EVIDENCE VALUE OF DATA OBTAINED BY DECODING ENCRYPTED COMMUNICATION PLATFORMS IN MONTENEGRO CRIMINAL LEGISLATION AND EUROPEAN STANDARDS

Summary

*The focus of the research of this paper is the legal nature, i.e. the evidentiary significance of the data collected by the dismantling of encrypted telecommunication networks by the judicial and police authorities of a number of EU member states. The aim of the research includes the analysis of Montenegrin criminal legislation in the area of special investigative techniques and their compliance with Directive 2014/41 EU on the European Investigation Order and the judgment in case C-670/22 of April 30, 2024 of the European Court of Justice in the context of the state's obligation to adapt criminal legislation to numerous social changes that generate new forms of crime. The main research question is: "Can encrypted communications from the Ennetcom, Anom, EncroChat and Sky ECC platforms intercepted by the country where the criminal proceedings are not conducted, be used as evidence in another state"? The answer to this question depends on the fulfillment of the conditions for the implementation of special investigative action in the national legislation and their compatibility with European standards. In researching the evidentiary importance of online surveillance, the methodology of legal sciences will be used through unity in approach and integral consideration of the qualitative dimension of the research subject. Based on the results of the research, it will be determined whether the requirements of necessity and proportionality are met when forwarding evidence that is in the possession of the requested state, whether it can be used automatically, or whether other conditions must be met, such as*

* Teaching Assistant, Faculty of Law, University of Montenegro; e-mail: rakocevica@ucg.ac.me

*notification of the state whose citizens are being monitored, compliance sovereignty of the state and ensuring that the level of protection of persons guaranteed in that state is not jeopardized, establishing a balance between encroachment on the right to respect private life and communication and the necessity of protecting society from crime et cetera. The use of evidence provided by surveillance and decoding of hidden communication platforms points to numerous challenges and open questions regarding the legality of their use in criminal proceedings in the context of mass surveillance not only of perpetrators of crimes but also of all persons who use the same application, which is why the paper presents a special attention to solving numerous problems and open questions in this area.*

**Keywords:** *criminal offence, encrypted communications, evidentiary significance, Montenegrin legislation, European standards*

## Literatura

Bajović Vanja, ,, Encrochat i Sky ECC komunikacija kao dokaz u krivičnom postupku“, *CRIMEN (XII)*, 2/2022.

Council of Europe: Committee of Ministers, *Recommendation Rec(2005)10 of the Committee of Ministers to Member States on "Special Investigation Techniques" in Relation to Serious Crimes Including Acts of Terrorism*, 20 April 2005, Rec(2005)10.

Council of Europe, *Guide to ther Case-Law of the European Court of Human Rights*, Strasbourg, 2020.

Drugi dodatni protokol uz Konvenciju o visokotehnološkom kriminalu, 2020.

Europol/Eurojust, *Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe*, 2020, https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe pristup 15.X 2024.godine.

Goodwin Bill, *French Supreme Court reject EncroChat verdict after lawyers question secrecy over hacking operation*, 2022, https://www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy. pristup 1. XI 2024.godine.

European Court of Justice, *Judgment of the Court (Grand Chamber) C-670/22 of 30 April 2024*, https://curia.europa.eu/juris/document/document.jsf?text=&docid=285365&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=323072 , pristup 8.XI 2024.godine.

Judgment -30/04/2024-M.N. ( EncroChat) Case C-670/22.

Konvencija Savjeta Evrope o pranju, traženju, zaplijeni i konfiskaciji prihoda stečenih kriminalom, (1990). Strazbur.

Konvencija UN protiv korupcije, 2000.

Lyons H. Judd (2021- 09.03.). *Cracing of encrypted messaging service dealt major blow to organised crime*, The Brussels Times, https://www.brusselstimes.com/news/belgium-all-news/159039/cracking-of-encrypted-text-messaging-service-sky-ecc-app-dealt-major-blow-to-organised-crime,2021,1, pristup 21. X 2024.godine.

Međunarodna organizacija za standardizaciju, *Pravila za identifikaciju, pribavljanje i čuvanje digitalnih dokaza*, Ženeva 2012.

Radulović Drago, *Krivično procesno pravo*, Pravni fakultet Univerziteta Crne Gore, Podgorica, 2015.

Rakočević Velimir, *Krivična djela sa elementima organizovanog kriminaliteta-specijalne istražne metode*, Pravni fakultet Podgorica, Podgorica, 2015.

Simović N. Miodrag, Šikman Mile, ,,Sadržaj šifrovane komunikacije ( Ennetcom, EncroChat, SkyECC, ANOM, Excly) kao dokaz u krivičnom postupku", *Pravo i pravda*, Udruženje sudija/sudaca u Federaciji Bosne i Hercegovine, 2023.

Rakočević Velimir, ,,Tajni nadzor komunikacija u izviđaju i krivičnom postupku i zaštita prava na privatnost*",Crnogorska revija za bezbjednost*, Podgorica, 2024.

Škulić Milan, ,,Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje-kao što su Sky ECC i EnchroChat", *Crimen*, Beograd 2024.

Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima, *Službeni list CG*, br.4/2008, 36/2013.

Zakon o potvrđivanju Konvencije o računarskom kriminalu, *Službeni list CG*-Međunarodni ugovori, br. 4/2009.