UPOREDNA ISKUSTVA
I PREPORUKE ZA CRNU GORU

CeMI
CENTAR ZA MONITORING I ISTRAŽIVANJE

DOPUŠTENOST UPOTREBE KRIPTO-KOMUNIKACIJA KAO DOKAZA U KRIVIČNIM POSTUPCIMA

DOPUŠTENOST UPOTREBE KRIPTO-KOMUNIKACIJA KAO DOKAZA U KRIVIČNIM POSTUPCIMA

UPOREDNA ISKUSTVA I PREPORUKE ZA CRNU GORU

Izdavač:
Centar za monitoring i istraživanje (CeMI)
Bul. Svetog Petra Cetinjskog 96, VI/12
E-mail: info@cemi.org.me
www.cemi.org.me

Urednik:
Zlatko Vujović

Autor:
Vladimir Simonović

Istraživački tim:
Vladimir Simonović
Alen Nikezić

Štampa:
SmartPrint

Tiraž:
100

Godina izdanja:
2023

UVOD

Kako tehnologija napreduje, tako napreduje i način na koji se pravosuđe suočava s dokazima u krivičnim postupcima. Elektronski dokazi, koji uključuju podatke sačuvane ili prenesene u digitalnom obliku, postali su ključan dio mnogih krivičnih istraga. Poruke s mobilnih telefona, e-pošta, digitalni zapisi i slično sada se rutinski koriste kao dokaz u sudnicama. Međutim, dok elektronski dokazi pružaju nove mogućnosti za sprovođenje istraga i procesuiranje zločina, oni takođe postavljaju niz novih izazova, uključujući pitanja o privatnosti, sigurnosti podataka i zakonitosti prikupljanja i upotrebe takvih dokaza. Upotreba dokaza prikupljenih upadom u kriptovane aplikacije, poput EncroChat-a, Sky ECC, Anom i dr. su primjeri koji ilustriraju ove složene probleme.

U ovom policy briefu naša glavna pažnja biće usmjerena na slučajeve koji se odnose na EncroChat, imajući u vidu da su se neke od najistaknutijih sudskih postupaka u evropskim zemljama odigrale upravo u kontekstu korišćenja ove aplikacije, dok razlike između ove dvije platforme, uprkos navodima koje smo mogli čuti u javnosti, nijesu od značaja za pitanje dopuštenosti podataka iz Sky ECC aplikacije kao dokaza u sudskim postupcima. Ipak, s obzirom da se radi o platformi koju su koristili pojedinci protiv kojih se vode krivični postupci u Crnoj Gori, ne možemo zanemariti Sky ECC.

Nakon retrospektive u kojoj na sažet način opisujemo ove platforme i kako je došlo do otkrića koje je rezultiralo akcijama protiv organizovanih kriminalnih grupa širom Evrope, ključna tema koju ovaj policy brief obrađuje odnosi se na zakonitost upotrebe dokaza na sudu prikupljenih „hakovanjem" u platforme za zaštićenu komunikaciju. Ovo je posebno relevantno u svijetlu šireg pitanja prava na privatnost u digitalnom dobu i prava na pravično suđenje. Važno je razjasniti da li, kada i kako ovi elektronski dokazi mogu biti korišćeni u krivičnim postupcima, u skladu s pravilima o dokazima i zahtjevima za pravičnim suđenjem. U tom cilju, ovaj dokument sadrži komparativnu analizu različitih evropskih država koje su se bavile ovom problematikom, u nadi da će njihovo iskustvo omogućiti bolje razumijevanje pristupa različitih jurisdikcija, ali i identifikovati moguće modele za implementaciju u drugim državama, pa i u Crnoj Gori. Policy brief pruža uvid u pravne stavove i odluke sudova u Francuskoj, Njemačkoj, Norveškoj, Holandiji i Italiji, a u vezi sa zakonitošću upotrebe kripto-komunikacije kao dokaza na sudu i moguće reperkusije u kontekstu zaštite ljudskih prava. Ove zemlje su odabrane zbog njihove

relevantnosti i značajnih sudskih postupaka koji su se odigrali u kontekstu korišćenja ovih dokaza.

Na kraju, na osnovu našeg istraživanja, policy brief sadrži zaključke i preporuke za dalje korake, koji se fokusiraju na pronalaženje ravnoteže između potrebe za efikasnim sprovođenjem pravde i zaštitom temeljnih ljudskih prava.

I. ENCROCHAT I SKY ECC: RETROSPEKTIVA

EncroChat i Sky ECC su platforme za kriptovanu komunikaciju, dizajnirane za zaštitu korisničkih poruka od neovlašćenog pristupa kroz napredne enkripcione algoritme. Kriptovana komunikacija odnosi se na proces kodiranja informacija ili poruka tako da samo ovlašćene strane mogu da ih razumiju. Osnovna ideja je da se informacije transformišu iz njihovog originalnog, čitljivog formata u neki nečitljiv oblik, koristeći algoritme i ključeve za šifrovanje i dešifrovanje. Ova metoda se često koristi za zaštitu osjetljivih podataka od neovlašćenog pristupa i smanjenje rizika od presretanja poruka od strane trećih strana.

1.1. EncroChat

EncroChat je platforma koja koristi Android uređaje sa dva operativna sistema, jedan standardni Android i drugi EncroChat sistem za kriptovane poruke, glasovne pozive i finansijske transakcije. Na internet stranici kompanije, koja je u ovom trenutku i dalje funkcionalna, nalazi se spisak usluga i funkcionalnosti koje je EncroChat pružao svojim korisnicima. [1]

Francuska je 2017. pokrenula istragu o EncroChat-u nakon što su pripadnici policijskih jedinica često pronalazili telefone s tom aplikacijom u akcijama protiv organizovanih kriminalnih grupa. Zahvaljujući tehničkoj analizi, francuske vlasti su uspjele da probiju enkripciju i pristupe korisničkoj komunikaciji. Kako je EncroChat bio široko korišćen među kriminalnim mrežama, 2019. godine francuske vlasti su otvorile slučaj ka Eurojustu. Istraga je omogućila obradu prikupljenih podataka u skladu sa francuskim zakonodavstvom i sa sudskom dozvolom, kroz okvire za međunarodnu pravosudnu i policijsku saradnju.[2]

1 https://encrophone.com/en/

2 Europol/Eurojust (2020), „Razbijanje šifrovane mreže šalje šok talase kroz organizovane kriminalne grupe širom Evrope“, Europol, 2. jul 2020. godine. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

Ovo je bilo moguće zahvaljujući članu 706-102-1 francuskog ZKP-a[3] koji dozvoljava postavljanje tehničkih uređaja za pristupanje, snimanje, skladištenje i prenos kompjuterskih podataka, bez saglasnosti zainteresovanih strana, u cilju efikasnijeg sprovođenja istraga u krivičnim predmetima u slučajevima organizovanog kriminala.

Intercepcija poruka preko EncroChat-a završena je 13. juna 2020. godine, kada je kompanija upozorila korisnike da su se vlasti infiltrirale u platformu i savjetovala im da odmah odbace uređaje.[4] Pokretanje istrage nije inicirano samo zbog pronalaženja kriptovanih uređaja kod kriminalaca tokom policijskih akcija, već i zbog načina na koji su se uređaji reklamirali korisnicima, postojanja tzv. panic mode-a za brisanje svih podataka u slučaju kompromitacije, nemogućnosti identifikacije vlasnika kompanije i visoke cijene uređaja, kao i mogućnosti kupovine istog kriptovalutama, što je vlastima ukazivalo na to da se ovi uređaju koriste za prikrivanje kriminalnih aktivnosti. Nakon probijanja enkripcije EncroChat-a, uslijedile su akcije protiv organizovanih kriminalnih grupa u više evropskih država. U nekima od njih već imamo prve sudske presude u slučajevima gdje je EncroChat komunikacija korištena kao dokaz na sudu. Interesantni su navodi da je između 90 i 100% korisnika EncroChat aplikacije bilo povezano sa organizovanim kriminalnim grupama. [5]

1.2. Sky ECC

Slično EncroChat-u, Sky ECC koristi sopstvenu kriptovanu platformu za slanje zaštićenih poruka, e-pošte i datoteka, sa dodatnim funkcijama zaštite. Oba sistema pružaju visok nivo privatnosti i sigurnosti. Međutim, upotreba uređaja sa ovakvom vrstom zaštite se povezuje sa kriminalnim aktivnostima.

SKY ECC je pružao neke dodatne funkcionalnosti i slojeve zaštite koji nijesu bili dostupni na EncroChat platformi. Na primjer, SKY ECC je koristio enkripciju

3 Moguće su situacije u kojima se pribjegava korišćenju tehničkog sredstva koje ima za cilj da, bez saglasnosti lica čiji se podaci koriste, na bilo kom mjestu ima pristup, snimanje, čuvanje i prenos kompjuterskih podataka, kao što su podaci koji se čuvaju u računarskom sistemu, koji se prikazuju na monitoru za korisnika sistema automatske obrade podataka, podaci koji su uneseni upotrebom karaktera ili oni podaci koji se primaju ili šalju putem spoljnih jedinica. Državni republički tužilac ili sudija za istragu mogu odrediti bilo koje ovlašćeno fizičko ili pravno lice upisano na neku od lista predviđenu za obavljanje tehničkih radnji kojima se omogućava realizacija tehničkog uređaja iz prvog stava ovog člana, kao i da državni tužilac ili sudija za istragu može takođe propisati korišćenje državnih sredstava koja podliježu nacionalnoj odbrambenoi tajnosti u oblicima predviđenim u poglavlju I naslova IV ZKP-a.

4 Europol/Eurojust, op.cit.

5 https://www.france24.com/en/20200702-european-police-shut-criminal-phone-network-used-to-plan-murders

sa dva ključa, dok je EncroChat koristio jedan ključ. Enkripcija sa dva ključa se obično odnosi na asimetričnu enkripciju, gdje se koristi par ključeva: jedan javni ključ za šifrovanje podataka i jedan privatni ključ za dešifrovanje. U ovom kontekstu, asimetrična enkripcija omogućava veći nivo sigurnosti jer čak i ako neko uspije da presretne javni ključ, neće moći da dešifruje poruku bez odgovarajućeg privatnog ključa. S druge strane, enkripcija sa jednim ključem obično se odnosi na simetričnu enkripciju. U simetričnoj enkripciji, isti ključ se koristi za šifrovanje i dešifrovanje poruke. Iako sigurno, ovo predstavlja problem ako se ključ kompromituje, jer će tada napadač moći da dešifruje sve poruke koje su šifrovane tim ključem. Takođe, Sky ECC je nudio različite mehanizme zaštite protiv zloupotrebe, kao što su tzv. panic buttons koji omogućavaju korisnicima da brzo i diskretno obrišu sve osjetljive informacije. Veći nivo zaštite privatnosti značio je i veću cijenu uređaja, pa je polugodišnja pretplata na Sky ECC platformu koštala između 950-2.600 EUR, dok je pretplata na EncroChat platformu koštala između 1.000-1.500 EUR.

Prema navodima Eurojust-a, Sky Global, poznata po platformi Sky ECC, preuzela je veliki broj korisnika organizovanih kriminalnih grupa nakon pada EncroChat-a.[6] U martu 2021. godine, Belgija, Francuska i Holandija pokrenule su operaciju protiv Sky ECC-a, nakon istrage o kriminalnim mrežama koje su koristile ovu platformu. Tvrdnje belgijske policije navode da je Sky ECC korišćen za koordinaciju ilegalnih aktivnosti, uključujući trgovinu drogom i oružjem.[7] Vlasti su probile Sky ECC enkripciju, što je dovelo do velikog broja hapšenja i zapljene imovine u Evropi. Izvršni direktor Sky Global-a, Žan-Fransoa Eap, i bivši distributer Sky Global uređaja Tomas Herdman, optuženi su u SAD-u za učestvovanje u kriminalnim radnjama koje su omogućile uvoz i distribuciju narkotika kroz prodaju šifrovanih uređaja.[8] U optužnici se navodi da su Sky Global uređaji dizajnirani da spriječe praćenje komunikacije kriminalnih organizacija, te da je firma ostvarila veliki profit olakšavajući njihove kriminalne aktivnosti i štiteći ih od organa reda, uz upotrebu digitalnih valuta za olakšanje ilegalnih transakcija. [9]

6 https://www.europol.europa.eu/media-press/newsroom/news/new-major-interventions-to-block-encrypted-communications-of-criminal-networks

7 Ibidem

8 Meghan E. Heesch i Joshua C. Mellor (2021), „Izvršni direktor i saradnik kompanije Sky Global optuženi za pružanje šifrovanih komunikacionih uređaja kako bi pomogli međunarodnim narko-dilerima da izbjegnu pravosudne organe", Kancelarija saveznog tužioca, Južni okrug Kalifornije, 12. mart 2021. godine. https://www.justice.gov/usao-sdca/pr/sky-global-executive-and-associate-indicted-providing-encrypted-communication-devices

9 Ibidem

II. KOMPARATIVNA ANALIZA: PRAVNI ODZIVI NA KRIPTO-KOMUNIKACIJU U EVROPI

U međunarodnim istragama koje je izvela francuska policija, kada je riječ o EncroChat i Sky ECC platformama, konstantno je u fokusu dilema o primjeni inostranih metoda istraživanja u nacionalnim pravosudnim procesima. Dok se s jedne strane ispituje koliko su rezultati istrage čvrsti i podložni reviziji od strane advokata odbrane i postupajućeg suda, s druge strane se razmatra njihova zakonitost i koliko su u skladu sa osnovnim načelima pravičnog suđenja.

Unutar brojnih evropskih jurisdikcija već smo svjedoci prvih osuđujućih presuda, čije su osnove bili dokazi prikupljeni putem nadzora uređaja koji su koristili prethodno opisane aplikacije za zaštitu komunikacije, ali bilo je i suprotnih odluka u kojima su sudovi stali na stanovište da se sadržaj komunikacije prikupljene nadzorom kriptovane komunikacije ne može koristiti kao dokaz u sudskom postupku. U ovom poglavlju, bavićemo se analizom načina na koji su različite evropske države pristupile pitanju legalnosti upotrebe dokaza dobijenih od strane država koje su vršile nadzor nad platformama o kojima smo pisali u prethodnom poglavlju. Naš fokus biće usmjeren prema argumentima suprotstavljenih strana, pravnim dilemama i presudama koje su proizišle u vezi sa ovom složenom temom, ističući uticaj raznovrsnih pravnih okvira na tretiranje ovakve vrste dokaza, kao i prakse Evropskog suda za ljudska prava (ESLJP) u kontekstu prava na pravično suđenje.

2.1. Francuska

U slučaju koji je vođen pred francuskim sudovima, gdje su dokazi prikupljeni pomoću EncroChat platforme, odbrana je izrazila sumnje u autentičnost i pouzdanost takvih dokaza. Ove sumnje proistekle su iz netransparentnosti metoda kojima su francuske vlasti pristupile ovim informacijama. Tužilaštvo se, pak, ogradilo od davanja uvida u detalje istrage, ukazujući na zaštitu nacionalne bezbjednosti kao primarni razlog. Nakon odluke Apelacionog suda u Nansiju kojom je upotreba EncroChat dokaza proglašena zakonitom, odbrana je uložila žalbu Vrhovnom sudu.

U slučaju pred Vrhovnim sudom razmatrana su tri centralna argumenta vezana za zakonitost prikupljanja podataka iz uređaja za zaštitu komunikacije.[10]

Kao prvi argument odbrana je istakla da je postupak presretanja podataka nezakonit jer krši pravo na privatnost, te da su modifikacije na EncroChat mreži neusaglašene s francuskim ZKP-om. Sud je odbio ovu tačku žalbe, smatrajući modifikacije neophodnim i zakonitim tehničkim operacijama za prikupljanje podataka.[11]

U drugom argumentu, odbrana je istakla da je izostavljanje dokumentacije iz postupka pred sudom u Lilu, koji je bio nadležan za istragu o EncroChat-u narušilo princip sudskog nadzora nad postupcima tužilaštva, kao i da je prekršen čl. 6 EKLJP koji garantuje pravo na pravično suđenje. Sud je ovaj argument takođe odbacio, konstatujući da je relevantna dokumentacija iz postupka u Lilu bila dostupna optuženima i istražnim sudijama, što je omogućilo procjenu pravičnosti prikupljenih dokaza.[12]

Treći argument odnosio se na tajnost operacije protiv EncroChat-a i nemogućnost da se utvrdi autentičnost i pouzdanost dokaza. Odbrana je navela da je tajnost istrage u suprotnosti sa pravom optuženih na jednakost oružja i efikasan pravni lijek, te da francuski Krivični zakonik zahtijeva od vlasti da pruže detalje o operaciji prikupljanja podataka, kao i sertifikat o autentičnosti kojim se potvrđuje tačnost i autentičnost dokaza koji se koriste kao dokaz, što je u ovom slučaju izostalo. Vrhovni sud se djelimično složio sa ovim argumentom, konstatujući odsustvo tehničkih informacija o postupku prikupljanja podataka i nepostojanje potvrde o vjerodostojnosti podataka. Kao rezultat toga, Vrhovni sud je poništio odluku Apelacionog suda u Nansiju i uputio predmet na ponovno suđenje Apelacionom sudu u Mecu.[13] Ovaj sud je utvrdio da, imajući u vidu da poruke koje je francuska policija prikupila nijesu bile šifrovane, nije bilo potrebe za sertifikatom koji bi potvrdio njihovu autentičnost. Očekivano, odbrana je uložila žalbu na takvu odluku Apelacionog suda, ali je Vrhovni sud istu odbio i na taj način konačno potvrdio zakonitost upotrebe konkretnih EncroChat dokaza u ovom postupku.[14]

Odredbe francuskog ZKP-a koje su omogućile istražnim organima da prikupe

10 Bill Goodwin (2022), French Supreme Court rejects EncroChat verdict after lawyers question secrecy over hacking operation, ComputerWeekly.com, 12. oktobar 2022. godine. https://www.computerweekly.com/news/252525971/French-Supreme-Court-rejects-EncroChat-evidence-after-lawyers-question-defence-secrecy

11 Ibid

12 Ibid

13 Ibid

14 Bill Goodwin (2023), French supreme court dismisses legal challenge to EncroChat cryptophone evidence, ComputerWeekly.com, 6. septembar 2023. godine. https://www.computerweekly.com/news/366551078/French-supreme-court-dismisses-legal-challenge-to-EncroChat-cryptophone-evidence

sporne dokaze bile su i predmet odlučivanja Ustavnog suda. Prema stavu Ustavnog suda, detaljnije obrazloženom u odluci od 22. aprila 2022. godine,[15] odredbe francuskog ZKP-a koje regulišu pribavljanje i obradu podataka u istragama, u skladu su sa Ustavom Francuske. Ovo je zasnovano na nizu razloga. Prvo, odredbe ZKP-a pružaju složene mehanizme koji omogućavaju državnim organima pristup kriptovanim ili inače zaštićenim informacijama, ali pod striktnim uslovima i pod nadzorom suda. Drugo, postoji jasna procedura za angažovanje stručnih lica za dešifrovanje podataka, koji podliježu zakletvi i etičkim standardima. Treće, posebni protokoli i rokovi su uvedeni za korišćenje državnih sredstava koja su dio nacionalne odbrambene tajne, sa mogućnošću prekida radnji od strane ovlašćenih organa. Ustavni sud je zaključio da ovi mehanizmi omogućavaju efikasnu istragu uz istovremeno osiguravanje zaštite prava pojedinaca i očuvanje nacionalnih interesa, te da se na ovaj način omogućava ravnoteža između efikasnosti u krivičnim postupcima i građanskih sloboda, pa su samim tim u skladu sa Ustavom Francuske.

2.2. Njemačka

Jedan od značajnijih slučajeva u kojima je EncroChat komunikacija prihvaćena kao dokaz dolazi iz Njemačke.

Naime, Savezni sud pravde je odbacio žalbu na presudu Okružnog suda u Hamburgu iz 2021. godine, kojom je optuženi osuđen na pet godina zatvora zbog trgovine narkoticima. Optuženi je u ovom predmetu osporavao zakonitost upotrebe EncroChat komunikacije kao dokaza u postupku koji se vodio protiv njega. Ova komunikacija je bila dostavljena Njemačkoj Saveznoj kriminalističkoj policiji posredstvom Europola. Ti podaci su ukazivali na brojne ozbiljne zločine koji su počinjeni na teritoriji Njemačke.

U svijetlu ovih saznanja, Centralna kancelarija za borbu protiv internet kriminala pri Opštem tužilaštvu u Frankfurtu, pokrenula je istrage protiv više nepoznatih osoba. U istražnoj fazi, upućen je Evropski istražni nalog (EIO) francuskim vlastima, koji je obuhvatao zahtjev za prenos svih EncroChat podataka koji se odnose na Njemačku i dozvolu za njihovu upotrebu u okviru njemačkih krivičnih postupaka. Francuski sud je odobrio oba zahtjeva, čime je omogućena dalja istraga.[16]

15 Odluka Ustavnog suda Francuske br. 2022-987 QPC, dostupna na: https://www.conseil-constitutionnel.fr/decision/2022/2022987QPC.htm

16 Odluka Vrhovnog suda Savezne Republike Njemačke br. 5 StR 457/21 od 1. marta 2022. godine. Dostupno na: https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2022&nr=127966&linked=bes&Blank=1&file=dokument.pdf

Kako bi utvrdio da li je moguće koristiti ove podatke kao dokaze u sudskom postupku, Savezni sud je morao da odgovori na tri pitanja: 1) da li je došlo do povrede procesnog prava, 2) da li to pravo, ukoliko je povrijeđeno, štiti prava osumnjičenog i 3) da li interes osumnjičenog prevazilazi interes tužilaštva?

Sud nije našao povredu procesnog prava koja bi uticala na zakonitost upotrebe ovih podataka kao dokaza na sudu. Prije svega, nije smatrao da treba da procjenjuje zakonitost načina na koji su francuske vlasti došle do podataka, jer bi to predstavljalo kršenje principa međusobnog povjerenja kojim je uređena saradnja između država članica Evropske unije. Sud nije našao ni da je došlo do povrede principa proporcionalnosti, s obzirom na ozbiljnu prirodu kriminaliteta protiv kojeg je bila usmjerena mjera presretanja komunikacije. Sud je cijenio, sa aspekta procesnih pretpostavki i primjenu člana 31 Direktive o EIO. U ovom dijelu utvrdio je da je postojala povreda, jer su francuske vlasti bile u obavezi da obavijeste njemačke vlasti da se vodi istraga protiv lica na njenoj teritoriji,[17] ali ova povreda nije mogla uticati na (ne) zakonitost upotrebe EncroChat komunikacije u sudskom postupku, jer svrha člana 31 EIO nije zaštita prava osumnjičenog, već zaštita suvereniteta države u kojoj se vodi istraga.

Sud je posebno cijenio i dopuštenost dokaza sa aspekta člana 6 EIO, koji zahtijeva da nalog mora da bude proporcionalan i da jedna država ne može tražiti od druge ono što ne bi mogla učiniti na bazi sopstvenog zakonodavstva. Što se tiče prvog zahtjeva, sud nije našao ništa što bi ukazivalo na neproporcionalnost. Kada je riječ o drugom zahtjevu, podsjećamo da njemačko tužilaštvo nije tražilo od istražnih organa Francuske da sprovode mjere tajnog nadzora, već samo da im proslijede rezultate istrage, te prema stavu Saveznog suda, ne postoji uslov da francuske istražne mjere moraju da budu dopuštene i u njemačkom zakonodavstvu da bi dostavljeni podaci bili dopušteni pred sudovima u Njemačkoj.

Međutim, postoje i oprečna mišljenja. Okružni sud u Berlinu nije se složio sa stavom Saveznog suda, i podnio je zahtjev za tumačenjem relevantnog prava

17 Član 31 glasi: „Kada je nekoliko država članica u poziciji da pruži potrebnu tehničku pomoć, EIO bi trebalo poslati samo jednoj od njih, a prioritet treba dati državi članici u kojoj se osoba nalazi. Države članice u kojima se predmet presretanja nalazi i od kojih nije potrebna tehnička pomoć za izvođenje presretanja trebale bi biti obaviještene o tome u skladu s ovom Direktivom. Međutim, kada tehničku pomoć nije moguće dobiti samo od jedne države članice, EIO se može prenijeti na više izvršnih država." https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041&from=EN

Evropskom sudu pravde,[18] postavljajući niz pitanja, od kojih kao najznačajnija možemo da izdvojimo sljedeća tri:

Prvo pitanje se odnosi na zakonitost EIO koji su izdale njemačke vlasti, tj. da li je nalog pravilno izdat u kontekstu člana 6(1)(b) Direktive o EIO, koji zahtijeva da se EIO može izdati samo ako su istražne mjere navedene u nalogu mogle biti naložene pod istim uslovima u sličnom domaćem slučaju. Okružni sud u Berlinu izrazio je sumnju da bi se EIO mogao koristiti za prenos podataka ako bi metode nadzora koje je koristila Francuska bile nedopuštene prema njemačkom zakonu u sličnom domaćem slučaju.

Drugo pitanje tiče se zakonitosti korišćenja dokaza koji su potencijalno dobijeni u suprotnosti sa zakonima EU. Sud postavlja pitanje da li takve dokaze treba isključiti iz krivičnih postupaka u skladu sa principom efikasnosti i principom ekvivalencije. Pitanje je posebno usmjereno ka činjenici da **tajnost francuskih mjera nadzora onemogućava nezavisnu provjeru tačnosti i pouzdanosti podataka, što je centralno za efikasnu odbranu.**[19]

Sud u Berlinu je postavio i pitanje da li je u skladu sa pravom Evropske unije, konkretno sa principom efikasnosti, koristiti dokaze prikupljene na nezakonit način ukoliko je počinjeni prekršaj ozbiljan, čak i ako ta ozbiljnost nije bila poznata kada su dokazi prvi put prikupljeni. Sud ističe da, prema osnovnim principu efikasnosti, nacionalni zakoni treba da štite prava optuženog tako da ne doživi nepravedne neugodnosti u toku krivičnog postupka zbog dokaza koji su nezakonito prikupljeni, i sugeriše da se ova zaštita može postići na dva načina: ili isključenjem nezakonito prikupljenih dokaza iz postupka ili tako što će se tokom ocjene dokaza uzeti u obzir činjenica da su isti prikupljeni na nezakonit način. Sud prednost daje isključenju dokaza.

Prema mišljenju opšte pravobraniteljke Evropskog suda pravde, od 26. oktobra 2023. godine,[20] dokazi su pribavljeni u skladu sa zakonom, ali opšti pravobranilac nije dao mišljenje o tome da li su isti dopušteni u krivičnim postupcima u Njemačkoj ili u drugim državama članicama Evropske unije, jer pravo EU ne sadrži norme o dopuštenosti dokaza,[21] već je to stvar nacionalnog zakonodavstva, na šta upućuje i praksa ESLJP.[22] Sa druge strane, u mišljenju se ističe da su države članice vezane principom uzajamnog priznavanja, koji

18 Odluka Okružnog suda u Berlinu o upućivanju pitanja Evropskom sudu pravde, od 19.10.2022 – (525 KLs) 279 Js 30/22 (8/22), st. 31. https://www.burhoff.de/asp_weitere_beschluesse/inhalte/7384.htm
19 Ibid, st. 71
20 Vidi više: https://curia.europa.eu/juris/document/document.jsf;jsessionid=4667734026567B77078D-65D21E14FC73?text=&docid=279144&pageIndex=0&doclang=en&mode=req&dir=&occ=-first&part=1&cid=3556492
21 Ibid, st. 117
22 Ibid, st. 123

od njih zahtijeva da prihvate zakonitost francuske operacije presretanja koju su odobrili francuski sudovi, osim ako bi te mjere bile nezakonite u sudskim postupcima u Francuskoj.[23]

2.3. Norveška

U Norveškoj je Vrhovni sud odlučivao po žalbi tri lica osuđena za trgovinu veće količine narkotika izvršenu kao dio aktivnosti organizovane kriminalne grupe. [24]

Norveškoj nacionalnoj kriminalnoj policiji (Kripos) je u martu 2020. godine dat pristup podacima norveških korisnika EncroChat-a. Na osnovu ovih podataka, identifikovano je nekoliko korisnika telefona i ustanovljeni su osnovi sumnje za više lica. Kripos je potom dobio dozvolu od Regionalnog suda u Oslu da prati komunikaciju, između ostalog, tri optužena u slučaju koji je došao do Vrhovnog suda Norveške. U junu 2020. godine, nakon što je policija Osla preuzela podatke od Kriposa, tužilaštvo je dobilo saglasnost francuskih vlasti da te podatke koristi kao dokaze u krivičnom postupku.

Jedan od ključnih argumenata odbrane bio je da dokazi moraju biti izuzeti jer su ih strane vlasti u stvari pribavile u Norveškoj, a ne u Francuskoj, te da su bile u obavezi da postupaju u skladu sa članom 216 o norveškog ZKP-a, prema kojem, kada postoji osnovana sumnja da postoji pokušaj ili da je izvršeno krivično djelo, policija mora imati dozvolu suda za čitanje računarskih podataka koji nijesu javno dostupni. Međutim, Vrhovni sud je odbacio takve navode, potvrđujući presude prvostepenog i Apelacionog suda, i u svojoj presudi pozvao se na postojeće presedane.

Osnovno pitanje u ovom slučaju, identično je pitanju koje je postavljeno u Njemačkoj – da li podaci prikupljeni od stranih vlasti mogu služiti kao dokaz u norveškom krivičnom postupku? Iako norveški zakon ne reguliše upotrebu takvih podataka, postoje presedani koji dozvoljavaju korišćenje dokaza legalno prikupljenih u drugim zemljama, čak i ako takav pristup ne bi bio legalan u Norveškoj.

Ovaj princip je prvi put potvrđen u slučaju prisluškivanja norveškog državljanina u Španiji. U toj presudi se navodi da, ako jedno lice izabere da živi u zemlji sa drugačijim ograničenjima kontrole komunikacija od onih koji postoje u Norveškoj, to lice ne može očekivati da informacije dobijene kroz

23 Ibid, st. 48

24 Odluka Vrhovnog suda Norveške po žalbi br. HR-2022-1314-A, (predmet br. 22-027874STR-HRET), (predmet br. 22-027879STR-HRET) i (predmet br. 22-027883STR-HRET), dostupno na: https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2022-1314-a.pdf

legalnu kontrolu komunikacija u toj zemlji budu neprihvatljive kao dokaz u Norveškoj. Ukoliko su informacije stečene u skladu sa norveškim vrijednostima i koriste se kao dokaz za krivično djelo u relevantnoj zemlji, one trebaju biti dopuštene kao dokaz u Norveškoj, **pod uslovom da optuženi ima pristup tim informacijama.**[25] U drugom slučaju na koji se Vrhovni sud pozvao, navodi se da, ukoliko bi se zahtijevalo da strane policijske i pravosudne institucije primjenjuju norveške procesne zakone u krivičnim slučajevima, to bi ometalo međunarodnu saradnju u borbi protiv prekograničnog kriminala, što ne bi bilo prihvatljivo.[26]

2.4. Holandija

Potreba da optuženi ima pristup dokazima koji se koriste u postupku protiv njega, predstavlja jedan od kamena temeljaca svake odbrane. U holandskim postupcima povodom EncroChat dokaza, odbrana je zastupala mišljenje da bi svaki podatak prikupljen putem nadzora nad EncroChat platformom trebalo biti dostupan odbrani.

Naime, član 6 Evropske konvencije o ljudskim pravima (EKLJP) zahtjeva od tužilaštva da odbrani pruži pristup svim relevantnim dokazima koji garantuje optuženom adekvatno vrijeme i sredstva za pripremu odbrane. Ipak, relevantnost dokaza može se dovoditi u pitanje, a optuženi treba da pruži valjane razloge zahtjeva za pristupom dokazima. Iako je u sistemu gdje tužilaštvo razmatra činjenice za i protiv osumnjičenog, postoji obaveza da se obezbijedi pravičnost, sama procjena tužilaštva o relevantnosti dokaza može biti neusklađena sa zahtjevima čl. 6 st. 1 EKLJP. Međutim, važno je naglasiti da pravo na otkrivanje relevantnih dokaza nije apsolutno. U krivičnim postupcima postoje suprotstavljeni interesi (kao što su nacionalna bezbjednost ili zaštita svjedoka) koji se moraju uravnotežiti sa pravima optuženog.[27] U nekim situacijama, **potrebno je zadržati određene dokaze od odbrane kako bi se očuvali temeljna prava drugih lica ili zaštitio javni interes. No, takva ograničenja prava odbrane su dozvoljena samo ukoliko su apsolutno neophodna**, uz postojanje odgovarajućih mjera koje nadoknađuju potencijalne poteškoće za odbranu. [28]

U slučajevima pred holandskim sudovima, branioci optuženih su insistirali na pregledu dokaza kojima je tužilaštvo raspolagalo, sa ciljem provjere njihovog

25 Ibidem
26 Ibidem
27 Nacionalna bezbjednost isticana je kao argument za odbijanje otkrivanja dokaza.
28 Evropski sud za ljudska prava, Vodič o članu 6 Evropske konvencije o ljudskim pravima - Pravo na pravično suđenje (krivični aspekt), 2022, str. 37/130. https://www.echr.coe.int/documents/guide_art_6_criminal_eng.pdf

integriteta i pouzdanosti, ali i u potrazi za mogućim dokazima koji bi mogli biti u korist njihovih klijenata.[29] Odbrani je djelimično omogućen uvid u tražene podatke. Prema praksi holandskih sudova, odbrana je imala pravo na pristup EncroChat podacima, ali samo onim podacima koji su relevantni za konkretan slučaj, tj. ne i podacima iz drugih krivičnih istraga. Analizu ovih podataka odbrana je mogla vršiti u Holandskom forenzičkom institutu. Pritom, odbrana je koristila isti analitički softver kao i tužilaštvo i mogla je dobiti kopiju relevantnih EncroChat podataka. Vrhovni sud Holandije smatra ovaj pristup zakonitim i usklađenim sa principom jednakosti oružja.[30]

Uprkos argumentima odbrane koji dovode u pitanje integritet i pouzdanost dokaza protiv njihovih klijenata, odbrana nije uspjela da ospori pouzdanost EncroChat podataka, a često su postojali višestruki izvori dokaza. Kao rezultat, nijedan podatak iz EncroChat operacije koji je tužilaštvo predložilo nije bio isključen iz holandskih krivičnih predmeta.[31] Takođe, poput Njemačke i Norveške, krivični sud u Holandiji smatra da nije na tom sudu da provjerava adekvatnost pravnog osnova za istražne radnje sprovedene od strane druge države. Kako ističe ovaj sud, njegov zadatak je ograničen na osiguranje da se upotrebom rezultata strane istrage u krivičnom postupku ne krši pravo na pravično suđenje. [32]

Pitanje upotrebe EncroChat i Sky ECC dokaza pred sudovima u Holandiji bilo je i predmet odlučivanja Vrhovnog suda te zemlje. Na zahtjev dva okružna suda, Vrhovni sud bio je pozvan da odgovori na dva preliminarna pitanja. Prvo pitanje se odnosilo na princip međusobnog povjerenja između država u kontekstu zajedničkih istraga, posebno da li podaci prikupljeni od francuske policije korišćenjem nepoznatih tehnika mogu biti korišćeni kao dokaz na holandskim sudovima. Drugo pitanje se ticalo relevantnosti EU direktiva 2002/58/EC i 2016/680, koje se bave obradom ličnih podataka i privatnošću.

Vrhovni sud Holandije je u svojoj odluci[33] zaključio da se Direktiva 2002/58/EC ne može primijeniti jer podaci iz aplikacija za zaštitu komunikacije nijesu bili zadržani od strane pružalaca usluga kako je to direktiva zahtijevala, dok je relevantnost Direktive 2016/680 odbačena kao nebitna za rješavanje preliminarnih pitanja.

---

29 J.J. Oerlmans i D.A.G. van Toor (2022), Pravni aspekti EncroChat operacije: perspektiva ljudskih prava, Evropski časopis za kriminal, krivično pravo i krivičnu pravdu, 30 (2022), 309–328. https://brill.com/view/journals/eccl/30/3-4/article-p309_006.xml?language=en

30 Ibid

31 Ibid

32 Odluka Okružnog suda u Roterdamu od 25. juna 2021. godine, para. 3.2.4. https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBROT:2021:6113

33 Odluka Vrhovnog suda Holandije, od 13. juna 2023. godine. https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:HR:2023:913

Vrhovni sud je svojom odlukom ograničio sposobnost holandskih sudova da nadziru zakonitost stranih istraga, polazeći od pretpostavke da su takve istrage vođene legitimno, osim ako nije dokazano suprotno odlukom u stranoj državi. U suštini, stav Suda značio je da dok istrage koje sprovode saradničke države ne krše prava zajamčena EKLJP, one će se smatrati zakonitim i prihvatljivim. Sud je takođe naglasio da pravo na osporavanje dokaza nije apsolutno i da može biti balansirano protiv suprotstavljenih interesa, kao što je nacionalna sigurnost. Takođe je ograničio ulogu nacionalnog suda u daljem ispitivanju metoda prikupljanja dokaza kada su ti metodi zaštićeni kao državna tajna druge države.

2.5. Italija

Italija predstavlja izuzetak od prethodno navedenih država u kojima je prihvaćena upotreba dokaza pribavljenih upadom u aplikacije za zaštićenu komunikaciju. Ujedno, u slučaju Italije radi se o komunikaciji pribavljenoj upadom u Sky ECC aplikaciju. Slučaj se ticao zakonitosti određivanja pritvora licu optuženom za trafiking narkotika.

U odluci od 15. jula 2022. godine,[34] Vrhovni sud Italije je istakao da optuženi ne može u potpunosti da razumije istragu ili prirodu dokaza protiv njega bez pristupa tim materijalima. Sud je naglasio da detalji o tome kako je dokaz prikupljen, uključujući „hvatanje i dešifrovanje telematskih tokova" sa Sky ECC-a, moraju biti otkriveni odbrani kako bi se osiguralo pravično suđenje, što je u ovom slučaju izostalo, a bilo je neophodno za procjenu relevantnosti, pouzdanosti i vrijednosti dokaza.

Kako se ističe u odluci, u osnovi krivičnog postupka je imperativ da dokazi moraju biti u skladu sa osnovnim principima italijanskog pravnog sistema, naročito sa pravom na odbranu. Stoga, pažljiva procjena načina na koji su dokazi prikupljeni od suštinske je važnosti da bi se osiguralo da pravo na odbranu nije narušeno. U presudi se naglašava da obje strane moraju imati priliku da se izjasne ne samo o prikupljenim dokazima, već i o načinu na koji su isti prikupljeni, te da je ova procjena od ključnog značaja i u situacijama kada se odlučuje o pritvoru, što je ovdje bio slučaj. Ako dokaz ima uticaj na odluku sudije o određivanju pritvora, metode prikupljanja tog dokaza moraju biti pažljivo razmotrene. Specifičan fokus se stavlja na dokaze dobijene iz digitalnih komunikacija, kao što su elektronske poruke. U tom smislu, neophodno je provjeriti da li sadržaj poruka precizno odgovara originalno poslatim i primljenim porukama, kao i da li korisnički nalozi odgovaraju

34 Cass, 32915/22, https://canestrinilex.com/en/readings/due-process-requires-transparency-of-evidence-gathering-in-sky-ecc-proceeding-cass-3291522

stvarnim pošiljaocima i primaocima poruka.

Na prvi pogled, odluka Vrhovnog suda Italije izgleda kao značajno odstupanje od prakse sudova u drugim članicama EU. U svim prethodno navedenim državama, sudovi su poštovali princip međusobnog povjerenja i nijesu preispitivali zakonitost postupaka koji su izvedeni u drugim državama članicama. Međutim, ključna distinkcija u italijanskom slučaju leži u prirodi predstavljenih informacija. Za razliku od drugih EU država, gdje su dokazi dobijeni direktno od pravosudnih organa kroz mehanizme međunarodne pravosudne saradnje, u Italiji su informacije dobijene od Europol-a kao dio međunarodne policijske saradnje.

III. DOPUŠTENOST I UTICAJ KRIPTO-KOMUNIKACIJE KAO DOKAZA U CRNOGORSKOM PRAVOSUĐU

Već više od godinu dana crnogorska javnost je putem medija imala priliku da se upozna sa (navodno) dijelom sadržine Sky ECC komunikacije lica koja su osumnjičena, a neka od njih kasnije optužena za izvršenje teških krivičnih djela iz oblasti organizovanog kriminala. Advokati zastupaju stav da podaci koje je SDT primilo preko Europola predstavljaju isključivo operativne podatke, koji se ne mogu koristiti kao dokaz na sudu. Neki advokati ističu da su ovi podaci pribavljeni krivičnim djelom, jer su istražni organi druge države „hakovanjem" i ubacivanjem „virusa" došli do podataka, iako neke države, poput Francuske koja je učestvovala u ovoj akciji dozvoljavaju takve i slične istražne radnje.

Uprkos stavu branilaca, Viši sud u Podgorici potvrdio je više optužnica u kojima je Specijalno državno tužilaštvo (SDT) kao dokaz predložilo komunikaciju putem Sky ECC aplikacije. U jednoj od optužnica koju je SDT podiglo 30. decembra 2022. godine,[35] može se vidjeti pravni osnov za upotrebu ovih dokaza. Prema optužnici, dokazi su prikupljeni u skladu sa Zakonom o međunarodnoj pravnoj pomoći u krivičnim stvarima, a metode prikupljanja nijesu nužno morale biti u skladu sa krivičnim zakonikom Crne Gore, pod uslovom da nijesu protivne domaćim pravnim principima i međunarodnom pravu.

35 Optužnica SDT-a Kt-S br. 172/22

Naime, prema članu 45 Zakona o međunarodnoj pomoći u krivičnim stvarima Crne Gore, *procesna radnja koju je preduzeo strani pravosudni organ u skladu sa svojim zakonom biće u krivičnom postupku izjednačena sa odgovarajućom procesnom radnjom koju preduzima domaći pravosudni organ, osim ako to nije u suprotnosti sa načelima domaćeg pravnog sistema i opšteprihvaćenim pravilima međunarodnog prava.* Iako nije navedeno u optužnici, treba podsjetiti da postoje i drugi međunarodni instrumenti saradnje koji omogućavaju razmjenu podataka između istražnih organa. Naime, tužilaštvo jedne države može podijeliti podatke sa drugim državama putem međunarodne pravosudne saradnje bez potrebe za prethodnim formalnim zahtjevom. Ova mogućnost propisana je članom 11 Drugog dodatnog protokola Evropske konvencije o međusobnom pružanju pravne pomoći u krivičnim stvarima[36] i članom 26 Budimpeštanske konvencije o računarskom kriminalu.[37]

U prethodno navedenoj optužnici se dalje naglašava da revizija stranog prava nije preduslov za prenos dokaza koje su francuske vlasti pribavile po francuskom zakonu i crnogorski krivični postupak. Ključno je da su dokazi prikupljeni u skladu sa zakonima zemlje u kojoj su prikupljeni, u ovom slučaju Francuske. Na osnovu principa uzajamnog priznavanja i povjerenja u međunarodnoj pravosudnoj saradnji, dokazi su preneseni crnogorskim vlastima. U optužnici se takođe ističe da nema zakonskog spora u vezi sa dokazima prikupljenim putem Sky ECC aplikacije, ni od strane francuskih sudova, ni od strane ESLJP ili Evropskog suda pravde, te stoga ne postoji razlog da se tvrdi nezakonitost, odnosno neprihvatljivost tih dokaza pred crnogorskim sudovima.

Kada je riječ o samim odlukama Višeg suda u Podgorici kojima su potvrđene optužnice u kojima je tužilaštvo kao dokaze predložilo komunikaciju putem

36 Nadležni organi jedne strane ugovornice mogu, ne dirajući u sopstvene istrage ili postupke i bez prethodno upućenog zahtjeva, dostaviti nadležnim organima druge strane ugovornice informacije, do kojih su došli u okviru sopstvenih istraga, ukoliko smatraju da bi takve informacije pomogle njihovom primaocu u pokretanju ili provođenju istrage ili postupka, ili bi mogle dovesti do upućivanja zahtjeva od strane te države, shodno odredbama ove Konvencije ili njenih dodatnih protokola. Strana ugovornica, koja je dostavila informacije, može u skladu sa svojim zakonodavstvom odrediti uslove pod kojima primalac može koristiti dostavljanje informacije. Strana ugovornica, koja je primila informacije, se obavezuje na poštovanje postavljenih uslova. Svaka strana ugovornica može u bilo koje vrijeme, izjavom upućenom generalnom sekretaru Savjeta Evrope, izjaviti da zadržava pravo da se ne pridržava uslova postavljenih od strane koja joj je dostavila informacije, shodno, osim kada je prethodno obaviještena o prirodi dostavljenih informacija i saglasna sa njihovim dostavljanjem.

37 Članica može, u granicama svog nacionalnog prava, bez prethodnog zahtjeva, da drugoj članici proslijedi informacije do kojih je došla u okviru sopstvenih istraga ukoliko smatra da bi otkrivanje takvih informacija moglo pomoći članici koja ih prima u pokretanju ili vođenju istrage ili drugih procedura koje se tiču kažnjivih djela ustanovljenih u skladu sa ovom Konvencijom, ili bi moglo voditi tome da ta članica uputi, na osnovu ovog poglavlja, zahtjev za međusobnu saradnju. Prije nego što dostavi takve informacije, članica koja ih dostavlja može zahtijevati da one budu čuvane u tajnosti ili da se mogu koristiti samo pod određenim uslovima. Ukoliko članica koja prima informacije ne može da prihvati takav zahtjev, ona mora o tome da obavijesti članicu koja dostavlja informacije, koja će nakon toga odlučiti da li će ipak da proslijedi informacije. Ukoliko članica prihvati informacije pod određenim uslovima, ti uslovi će za nju biti obavezujući.

Sky ECC aplikacije, uključujući i prethodno navedenu optužnicu, [38]prema trenutnoj sudskoj praksi u Crnoj Gori, ovi dokazi su prihvatljivi u postupku kontrole optužnice i cijeniće se na glavnom pretresu. Prema riječima predsjednika Višeg suda u Podgorici, o *prihvatljivosti dokaza pribavljenih SKY aplikacijom može se govoriti samo na osnovu pravosnažne presude, i radi se o dokazima koji će se kao takvi i cijeniti*.[39] Nije realno očekivati da će se sudska praksa u ovom dijelu izmijeniti bez prethodne odluke Vrhovnog suda o ovim pitanjima ili odluke nekog relevantnog međunarodnog tijela. Razloge za ovakvu situaciju možemo tražiti i u kratkim rokovima za kontrolu zakonitosti dokaza u postupku kontrole optužnice, a posebno imajući u vidu da se u velikom broju predmeta radi o glavnim dokazima. Uzimajući u obzir i da odbrana ima na raspolaganju mogućnost predlaganja novih dokaza, što može dovesti do isključenja onih dokaza koje je predložilo tužilaštvo, logika kojom se vode sudije u postupku kontrole optužnice je u tom kontekstu jasna i očekivana.

Ipak, postoji nekoliko okolnosti koje zabrinjavaju. Prije svega, nosioci najviših državnih funkcija nijesu pokazali dovoljan stepen odgovornosti u slučajevima tzv. Sky ECC predmeta, već su neki od njih svjesno kršili pretpostavku nevinosti javnim izjavama na račun optuženih, što je potvrdio i Zaštitnik ljudskih prava i sloboda.[40] Izjave takvog tipa mogu se okarakterisati i kao vrsta političkog pritiska na rad suda i tužilaštva.

Naš ZKP u članu 3 eksplicitno propisuje obavezu pridržavanja pretpostavke nevinosti za državne organe, medije, udruženja građana, javne ličnosti i druga lica. I ESLJP je zauzeo jasan stav da obaveza poštovanja pretpostavke nevinosti ne obavezuje samo sudiju ili sud, već i druge javne vlasti.[41] U istom predmetu Sud je utvrdio povredu pretpostavke nevinosti iz čl. 6 st. 2 EKLJP, zbog javnih izjava ministra unutrašnjih poslova Francuske protiv optuženog.[42] U slučaju Konstas protiv Grčke,[43] ESLJP je utvrdio kršenje pretpostavke nevinosti usljed neprikladnih izjava grčkog ministra pravde i zamjenika ministra finansija. Izjave su bile upućene prema optuženima koji su bili osuđeni u prvostepenom postupku, dok je postupak pred apelacionim sudom još uvijek bio u toku. Prema mišljenju Zaštitnika ljudskih prava i sloboda, *izjave predsjednika Vlade prešle su prag dopuštenosti slobode informisanja, u smislu zaštite prava drugih kao jednog od kvalifikatornih osnova i prekršile pretpostavku nevinosti.*[44]

38 https://sudovi.me/vspg/sadrzaj/JQRl
39 https://www.cdm.me/hronika/predsjednik-viseg-suda-o-dokazima-iz-sky-aplikacije-samo-na-osnovu-pravosnazne-presude/
40 Mišljenje Zaštitnika ljudskih prava i sloboda Crne Gore br. 236/23 od 2. avgusta 2023. godine. https://www.ombudsman.co.me/docs/1694250636_02082023_preporuka_pcg.pdf
41 Allenet de Ribemont protiv Francuske, predstavka br. 15175/89, od 10. februara 1995.
42 Ibid
43 Predstavka br. 53466/07, od 24. maja 2011. godine.
44 Mišljenje Zaštitnika ljudskih prava i sloboda, op.cit., str. 17

Kada govorimo o slobodi informisanja, važno je osvrnuti se i na jedan od dugogodišnjih problema u radu crnogorskih medija, koji takođe često krše pretpostavku nevinosti. U kontekstu Sky ECC slučajeva, bilo je moguće primijetiti na desetine medijskih naslova koji predstavljaju sadržaj te komunikacije na način kao da je krivica optuženih već neupitno utvrđena u krivičnom postupku, iako je jedan od zadataka tužilaštva u ovim postupcima da dokaže autentičnost dokaza, i da komunikacija zaista pripada optuženima. Prema ESLJP, iako je izvještavanje medija o aktuelnim događajima dio slobode izražavanja koja je zagarantovana članom 10 EKLJP, prema stavu ESLJP, takve kampanje i publikacije mogu dovesti u pitanje pravičnost suđenja, tako što utiču na javno mnjenje, i samim tim na one koji treba da odluče o krivici optuženog.[45]

U samo dvije optužnice u kojima je SDT koristilo Sky ECC dokaze čija sadržina je objavljivana i u medijima, optuženo je ukupno 27 lica kojima je ovakvim postupcima ugroženo pravo na pretpostavku nevinosti kao jedan od elemenata prava na pravično suđenje.

U kontekstu medijskih objava Sky ECC komunikacije, posebno zabrinjava okolnost da je dio sadržine ove komunikacije bio dostupan javnosti, tj. neki mediji su objavljivali i nastavljaju da objavljuju djelove Sky ECC komunikacije, navodno na osnovu uvida u dokumentaciju EUROPOL-a koja je dostavljena crnogorskim istražnim organima. Osim detalja vezanih za krivična djela koja se optuženima stavljaju na teret, u javnosti su počele da izlaze i druge informacije iz privatnog života, ne samo lica obuhvaćenih optužnicama, već i lična prepiska nosilaca pravosudnih funkcija koje nijesu predmet nijedne optužnice, čime se grubo krši pravo na privatnost svih tih lica. Tužilaštvo još uvijek nije pokrenulo istragu u cilju otkrivanja kako su mediji došli u posjed ovih podataka. Osim moguće povrede pretpostavke nevinosti, kao i povrede prava na privatnost, postoji i opasnost od ugrožavanja zaštite tajnosti podataka u istrazi, te samim tim integriteta istrage, kao i opasnost od ugrožavanja saradnje domaćih istražnih organa sa organima stranih država.

45 Khuzhin i ostali protiv Rusije, st. 93, predstavka br. 13470/02, od 23. januara 2009. godine.

ZAKLJUČCI I PREPORUKE

Najnovija tehnološka dostignuća nastavljaju da otvaraju nove dimenzije u načinu na koji se pravosuđe bavi dokazima, naročito u kontekstu zaštićene komunikacije. Naime, prepoznajući sveprisutnu ulogu elektronskih dokaza u krivičnim istragama, u proteklih par godina imali smo priliku da pratimo kako se pravosuđe suočava sa kompleksnošću i izazovima koje takvi dokazi sa sobom nose. I dok digitalna era pruža nove mogućnosti za vršenje krivičnih djela na način koji državnim organima ograničava ili čak onemogućava otkrivanje i dokazivanje istih, ali i za istragu i procesuiranje zločina, pitanja poput zakonitosti prikupljanja i upotrebe ovakvih dokaza postaju sve relevantnija.

Posmatrajući dosadašnju praksu, jasno je da zakonitost prikupljanja ovih dokaza, njihova autentičnost, kao i mogućnost odbrane da se izjasni o njima, predstavljaju ključne aspekte u razmatranju upotrebe dokaza pribavljenih presretanjem zaštićene komunikacije. Iako se na prvi pogled čini da je zakonitost prikupljanja dokaza ključno pitanje, dublje sagledavanje ove tematike otkriva da je mogućnost odbrane da se izjasni o dokazima zapravo polazno pitanje. Naime, ova mogućnost odbrani omogućava da osporava zakonitost i autentičnost predloženih dokaza, te na taj način pruži sveobuhvatan odgovor na navode tužilaštva. Sudovi u različitim evropskim zemljama su, bez obzira na konačnu odluku o prihvatanju ili odbijanju dokaza, bili dužni da omoguće odbrani uvid u dokaze ili da otkriju način na koji su isti prikupljeni. Međutim, ne radi se o apsolutnom pravu odbrane. Ni praksa ESLJP ne tretira ovo pravo kao apsolutno, već ga ograničava zaštitom temeljnih prava drugih lica i zaštitom javnog interesa.

Konačan ishod postupaka u evropskim zemljama u kojima su se vodili postupci u vezi sa EncroChat i Sky ECC dokazima, zavisio je uglavnom od detalja nacionalnog zakonodavstva. Ovo je, u suštini potvrdila i opšta pravobraniteljka Evropskog suda pravde, Tamara Ćapeta, koja je u svom mišljenju zauzela stav da je Njemačka dobila dokaze od Francuske na zakonit način, ali da zakonitost upotrebe tih dokaza u krivičnim postupcima zavisi od nacionalnog zakonodavstva.

Primjeri iz drugih država koji su prethodno opisani daju jednu, reklo bi se, prilično jasnu sliku o tome kako se sudovi u državama članicama Evropske unije ophode prema ovim dokazima. U postupcima pred francuskim sudovima, zakonitost postupanja istražnih organa Francuske je utvrđena i više se ne dovodi u pitanje, što je igralo značajnu ulogu u odlukama drugih država u kojima su se vodili i u kojima se vode postupci zasnovani na EncroChat i Sky

ECC dokazima. Sudovi u Njemačkoj i Holandiji smatraju da ne treba ulaziti u ocjenjivanje zakonitosti postupanja istražnih organa druge države, već treba poći od principa međusobnog povjerenja i međusobnog priznavanja, dok Norveška ide korak dalje, i dopušta upotrebu ovakvih dokaza koji su legalno prikupljeni u drugim zemljama, čak i ako takav pristup ne bi bio legalan u njihovoj zemlji. Kada je riječ o Italiji, odluka Vrhovnog suda Italije bazirana je na činjenici da je tužilaštvo kao dokaz priložilo operativne podatke Europola, a ne dokaze dostavljene od strane suda druge države.

Kada govorimo o upotrebi ovih dokaza pred crnogorskim sudovima, i naš Zakona o međunarodnoj pravnoj pomoći u krivičnim stvarima, kao i potvrđene međunarodne konvencije u ovoj oblasti, sadrže ove principe. Može se zaključiti da su, samom činjenicom da ih Viši sud tako tretira, dokazi prikupljeni putem Sky ECC aplikacije zakoniti, tj. dopušteni su u postupku kontrole optužnice, što ujedno i predstavlja fazu postupka u kojoj se cijeni njihova zakonitost. Ipak, može se zaključiti i da je njihova konačna sudbina i dalje jednim dijelom nepoznata.

Naime, iako ZKP ne propisuje eksplicitno mogućnost preispitivanja zakonitosti dokaza na glavnom pretresu, on isto ne zabranjuje. U praksi je (čak nedavno) dolazilo do predlaganja novih dokaza od strane odbrane u toku glavnog pretresa, na osnovu kojih su izuzeti dokazi predloženi od strane tužilaštva. Osim toga što može doći do ovakve situacije, izvjesno je i da će sudbina ovih dokaza, tj. njihova dopuštenost u sudskim postupcima, zavisiti i od odluka međunarodnih pravosudnih tijela, ako zauzmu konkretan stav po ovom pitanju, kao i od buduće harmonizacije propisa u ovoj oblasti, koja neće ostaviti prostor za nejasnoće ili slobodne interpretacije, već će jasno definisati okvire upotrebe takvih dokaza.

Na kraju, treba istaći da je princip pravičnog suđenja, u čijem okviru je i pretpostavka nevinosti, jedna od vrijednosti koja odražava stepen razvoja pravne države i demokratskog društva. Nepridržavanje temeljnih principa zaštite ljudskih prava dovodi do erozije povjerenja građana u institucije, ali i do potencijalnih negativnih odluka na međunarodnom nivou. Neodgovorno, neprofesionalno i neetičko ponašanje državnih i drugih javnih funkcionera, ali i medija, nije zanemarljivo i nije bez posljedica. Zato je veoma važno da svi oni postupaju na način kojim se štite i poštuju temeljna ljudska prava. To nije samo moralni imperativ, već i praktična neophodnost za održavanje pravne države i demokratskog poretka.

PREPORUKE:

1. Modernizovati procesno zakonodavstvo

Za efikasno reagovanje na izazove koje digitalizacija i kriptokomunikacija postavljaju pred pravosudni sistem, neophodno je modernizovati Zakonik o krivičnom postupku. Osim što je potrebno jasno definisati šta se sve podrazumijeva pod digitalnim dokazima, potrebno je uspostaviti jasne protokole i standarde za njihovu autentifikaciju i upotrebu u krivičnim postupcima. Ovi standardi bi trebali obuhvatiti protokole za sertifikaciju kojima se potvrđuje validnost i autentičnost digitalnih dokaza, kao i kriterijume koji moraju biti ispunjeni da bi ti dokazi bili dopušteni u postupku.

U nedostatku takvih normi važna je uloga Vrhovnog suda, koji bi trebao da usvoji jasne standarde i smjernice o tome da li se i kako digitalni dokazi poput onih prikupljenih putem Sky ECC komunikacije, mogu prikupljati, koristiti i ocjenjivati u krivičnim postupcima, sa posebnim osvrtom na zaštitu ljudskih prava. Pitanje je ne samo tehničke prirode (kako osigurati dokaz) već i kako garantovati pravično suđenje. U tom cilju Vrhovni sud bi trebalo da prati odluke i smjernice drugih država koje su se susrele sa istom problematikom, kao i odluke međunarodnih pravosudnih organa, kao što su ESLJP i Evropski sud pravde.

2. Dosljedno poštovati pretpostavku nevinosti

Komentari i izjave o postupcima koji još uvijek traju mogu imati negativan uticaj na ljudska prava optuženih, konkretno na njihovo pravo na pravično suđenje. Takve izjave, kada dolaze od visokih državnih funkcionera mogu se percipirati i kao svojevrstan oblika vršenja pritiska na tužilaštvo i na sud. Političari i javni funkcioneri trebali bi da se uzdržavaju od komentarisanja konkretnih slučajeva i da izbjegavaju upućivanje derogativnih komentara, kako o optuženima, tako i o radu sudova ili pojedinih sudija, kako zbog očuvanja nezavisnosti pravosuđa, tako i zbog zahtjeva za poštovanjem ljudskih prava svih građana.

Kada je riječ o medijima, u izvještavanju o krivičnim postupcima koji su u toku, mediji bi trebali da budu svjesni uticaja koji njihovi naslovi i sadržaj mogu imati na javno mnjenje i pravičnost suđenja. Mediji treba da koriste neutralan jezik kojim se ne pretpostavlja krivica, kako bi se minimizirao potencijalni uticaj na sudsku nepristrasnost i integritet pravosudnog sistema, i u krajnjem pravo optuženih da budu smatrani nevinim, što je jedan od elemenata pravičnog suđenja.

3. Očuvati integritet i povjerenje u međunarodnoj saradnji

Potrebno je ozbiljno shvatiti mogući negativni uticaj koji curenje informacija u javnost može imati na međunarodnu saradnju u budućim istragama. Treba

preduzeti sve neophodne korake da se očuva povjerenje i integritet saradnje sa stranim istražnim organima. U tom smislu, neophodno je sprovesti istragu kako bi se utvrdilo ko je odgovoran za curenje informacija, kako bi se preduzele odgovarajuće pravne radnje.

4. Obezbijediti veći stepen bezbjednosti sudova

Imajući u vidu da se optužena lica u predmetima u kojima se koriste dokazi iz Sky ECC aplikacije, uglavnom nalaze u pritvoru, a u svjetlu prošlogodišnjeg hakerskog napada na informacioni sistem Vlade i ovogodišnje krađe dokaza iz depoa Višeg suda, neophodno je usvojiti sigurnosne protokole kako na fizičkom, tako i na digitalnom nivou, kako ne bi dolazilo do nepotrebnog odlaganja ročišta za glavnu raspravu ili čak do odbacivanja optužnica uslijed kompromitacije dokaza.

Takođe je potrebno nastaviti rad na implementaciji novog jedinstvenog informacionog sistema pravosuđa, koji je trenutno u zastoju, za šta je potrebno izdvojiti znatno više novčanih sredstava od trenutno predviđenih. Osim toga, informacioni sistem pravosuđa ne treba biti zavisan od informacionog sistema Vlade Crne Gore. Zato je nužno razviti mehanizme za određeni stepen decentralizacije. Cilj je osigurati da pravosudni informacioni sistem nastavi da funkcioniše bez prepreka, čak i ako je informacioni sistem Vlade kompromitovan ili nefunkcionalan. Zaposlenima treba omogućiti i obuku iz oblasti sajber bezbjednosti da bi se umanjila mogućnost ljudske greške, koja često služi kao tačka upada za napadače.

5. Organizovati obuke o novim tehnologijama i elektronskim dokazima u sudskim postupcima

Složenost digitalne tehnologije zahtijeva određeni nivo stručnosti među nosiocima pravosudnih funkcija. Stoga treba uvesti kontinuiranu edukaciju koja će pratiti brzi tehnološki napredak. Obuka sudija i tužilaca u novim tehnologijama i elektronskim dokazima trebalo bi da bude oblikovana na način koji odgovara njihovim potrebama, sprovođenjem procjene potreba, uzimajući u obzir postojeće međunarodne standarde i instrumente saradnje, posebno Budimpeštansku konvenciju o sajber kriminalu. Svi nosioci sudijskih funkcija trebalo bi da preduzmu program kontinuiranog obrazovanja u novim tehnologijama i elektronskim dokazima.

Takođe, trebalo bi uvesti sistem podsticaja u vezi sa sudijskom i tužilačkom obukom u ovim oblastima. Učestvovanje u međunarodnim projektima za sudijsku obuku u elektronskim dokazima dodatno bi ojačalo poziciju sudstva i ključno je za efikasno rješavanje prekogranične prirode problema vezanih za elektronske dokaze.

ISBN 978-9911-556-07-3

9 789911 556073 >

CIP- КАТАЛОГИЗАЦИЈА У ПУБЛИКАЦИЈИ
НАЦИОНАЛНА БИБЛИОТЕКА ЦРНЕ ГОРЕ, ЦЕТИЊЕ

ISBN 978-9911-556-07-3
COBISS.CG-ID 27922692