*Др Александра Илић**

DOI: 10.51204/Zbornik_UMKP_25117A
Оригинални научни рад

КРИПТОВАНА КОМУНИКАЦИЈА У СВЕТЛУ МЕЂУНАРОДНЕ ПРАВНЕ ПОМОЋИ У КРИВИЧНИМ СТВАРИМА

Апстракт: Аутор у раду разматра актуелну проблематику коришћења садржаја криптоване комуникације у кривичним поступцима превасходно из угла међународне правне помоћи у кривичним стварима. Након уводних разматрања у којима је дефинисан појам криптоване комуникације и међународне правне помоћи у кривичним стварима анализирани су поједини изазови међународне правне помоћи у сфери коришћења криптоване комуникације. Посебно је размотрена шифрована комуникација проистекла из Sky ECC и EncroChat апликација и њихово коришћење у кривичним поступцима у контексту упоредних искустава појединих европских држава али и имајући у виду и ситуацију у Србији. С обзиром на значај праксе Европског суда за људска права као и Суда правда Европске уније за разјашњење одређених дилема у околностима међународне правне помоћи у кривичним стварима у случају криптоване комуникације које се последњих година јављају у пракси правосудних органа многих држава, у раду је дат осврт и на тај аспект. На крају је истакнута важност истраживачког новинарства у међународним истрагама криптоване комуникације.

Кључне речи: криптована комуникација, међународна правна помоћ у кривичним стварима, Европски суд за људска права, Суд правде Европске уније, истраживачко новинарство.

1. УВОД

Криптована комуникација је у данашње време постала уобичајени формат у комуникацији између људи подстакнут превасходно различитим

* Ванредни професор, Факултет безбедности Универзитета у Београду, ORCID: https://orcid.org/0000-0001-7298-2347, aleksandra.ilic@fb.bg.ac.rs.

безбедносним изазовима и с тим у вези потребом да се заштити тај сегмент људског функционисања. Шифровање се односи на процес трансформације информација у безбедан формат како би се заштитиле од нежељеног приступа или измена од стране трећих лица како би се обезбедила поверљивост и интегритет података. Као механизам је првобитно коришћен за спречавање читања пресретнутих, руком састављаних, порука. Потом се шифровање развијало током последњих деценија ради заштите дигиталних података и сада је добро успостављено поље истраживања и развоја, уско повезано са рачунарством и математиком.[1] Поред користи које криптовање комуникације доноси људима у свакодневном животу и раду, вишеструке бенефите имају и они који делују с друге стране закона. У намери да буду увек корак или два испред органа откривања и гоњења, учиниоци кривичних дела користе криптовану комуникацију било да се ради о начину извршења кривичих дела или ситуацији када се поменута технологија користи како би се обезбедила потпуна тајност комуникације и заштита од "непозваних" лица. Иако има пуно различитих апликација које омогућавају својим корисницима да тајно односно заштићено комуницирају (иако је свакако у медијском простору код нас најпознатија Sky ECC и EncroChat) њихова суштина је у омогућавању да на криптован начин комуницирају једино корисници исте „платформе".[2] Коришћење поменутих апликација засновано је на посебном протоколу (тзв. OTP протокол или *Off the-Record Messaging*) који обезбеђује моментално шифровање поруке и њену трансмисију преко централних сервера који су се налазили у иностранству, превасходно у Француској и Канади.[3]

Излажење из оквира досадашњих облика комуникације лица која потенцијално чине одређена кривична дела и наслањање у значајној мери на криптованом формату представља изазов за органе гоњења многих држава у којима се јавља потреба да се преиспита доказна употребљивост такве комуникације. Та проблематика посебно долази до изражаја у контексту међународне правне помоћи у кривичним стварима када су укључени надлежни државни органи најмање две државе, од којих једна тражи помоћ (држава молиља), а друга је на захтев прве указује (замољена држава) при чему је замољена држава увек једна, а држава молиља може бити и више.[4] Без улажења детаљније у основ пружања међународне правне помоћи у кривичним стварима, само подсећања ради треба истаћи да када је реч о

1 First Report on Encryption by the Innovation Hub for Internal Security, Luxembourg: Publications Office of the European Union, 2024

2 M. Škulić, „Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje kao što su Sky ECC i EnchroChat", *Crimen,* 1/2024, 4.

3 V. Bajović, „EnroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku", *Crimen*, 2/2022, 155.

4 М. Грубач, Г. П. Илић, М. Мајић, *Коментар Закона о међународној правној помоћи у кривичним стварима*, Београд, 2009, 15.

Србији тај поступак регулисан превасходно Законом о међународној правној помоћи у кривичним стварима[5] (у даљем тексту: ЗМППКС), који се примењује увек када у конкретном случају не постоји потврђен међународни уговор или када одређена питања њиме нису уређена (члан 1), при чему Србија у овом тренутку има потписан билатерални споразум у кривичним стварима са 32 државе.

У сваком случају, без обзира на основ пружања међународне правне помоћи циљ је да се применом принципа солидарности и сарадње међу државама омогући кривично гоњење учинилаца и извршење изречених кривичних санкција и у случајевима када одређене радње у вези са кривичним поступком или извршењем кривичних санкција треба извршити у иностранству. [6]

2. ИЗАЗОВИ МЕЂУНАРОДНЕ ПРАВНЕ ПОМОЋИ У КРИВИЧНИМ СТВАРИМА У СФЕРИ КОРИШЋЕЊА КРИПТОВАНЕ КОМУНИКАЦИЈЕ

Пружање међународне правне помоћи у кривичним стварима у контексту коришћења криптоване комуникације представља изазов за правосудне органе укључених држава и указује на потребу редефинисања у одређеној мери досадашњих стандарда и процедура како би се пре свега одговорило на потребу сузбијања посебно опасних и тешких облика криминалитета. Могло би се рећи да је ово питање само још један корак даље у вишедеценијским напорима да се како глобално тако и у оквиру конкретних држава колико толико држи под контролом криминалитет који представља озбиљну опасност за друштво у целини.

Апликације попут Sky ECC и EnroChat користе се за скривену комуникацију између учинилаца кривичних дела у низу различитих облика криминалне активности. Углавном су у питању тешка кривична дела превасходно она која се односе на деловање организованих криминалних група попут трговине дрогом, сајбер криминала, убистава, прања новца и превара. Свака апликација односно техника шифровања захтева прилагођен приступ од стране органа гоњења како би се покушало разбити шифровање али тако да све буде учињено у складу са законом. Технике које полиција користи за разбијање шифри морају бити адекватно регулисане у националним

5 Закон о међународној правној помоћи у кривичним стварима – ЗМППКС, *Службени лисш СРЈ*, бр. 20/09.

6 А. Илић, „Међународна правна помоћ у кривичним стварима у светлу нове организације кривичног правосуђа", *Раскршћа међународноī кривичноī и кривичноī йрава – реформа йравосудних закона Рейублике Србије* (ур. М. Шкулић, И. Миљуш, А. Шкундрић), Удружење за међународно кривично право, Универзитет у Београду – Правни факултет, Београд, 2023, 70.

законским одредбама, било општим или специјалним, при чему је неопходно поштовати и одговарајућа процедурална правила. У прекограничним случајевима, где се корисници односно учиниоци кривичних дела, њихове жртве, инфраструктура или сервери налазе у различитим земљама, постаје још изазовније спровести истраге уз успешан исход, с обзиром на различите законске оквире у конкретним државама[7].

Бајовић оправдано поставља питање да ли би комуникација која се одвијала путем криптованих телефона у многим државама уопште и могла да буде откривена путем постојећих доказних радњи, да такви докази нису достављени путем међународне правне помоћ.[8] На основу података које садржи заједнички извештај Europol/Eurojust из 2021. године,[9] само Данска, Француска, Немачка, Пољска, Шведска, Швајцарска и Холандија имају одредбе које се посебно баве употребом техничких алата у сврху дешифровања комуникације од стране органа гоњења односно имају тзв. шпијунски софтвер. Извештај Венецијанске комисије из децембра 2024. године[10] помиње још пар европских држава у том смислу: Финска, Италија, Шпанија, Луксембург, Норвешка као и Уједињено Краљевство док је у случају Белгије, Бугарске, Естоније, Мађарске, Литваније, Републике Молдавије, Северне Македоније, Румуније и Словачке Републике (иако то питање није одвојено и аутономно регулисано), коришћење шпијунског софтвера дозвољено под оквиром „специјалних техничких средстава/специјалних истражних мера". У истом извештају се истиче и да је у случају Аустрије првобитно уведен посебан законски оквир о употреби шпијунског софтвера у контексту кривичних истрага али да је потом поништен од стране Уставног суда, који је утврдио да представља несразмерно мешање у људска права. С тим у вези треба истаћи да је шпијунски софтвер изузетно интрузиван алат за надзор који се може користити за ометање електронских уређаја, посебно паметних телефона или рачунара, без знања корисника, и који омогућава оператеру да продре у уређаје и, у зависности од конкретног алата, прати геолокацију у реалном времену, чита све сачуване податке, сву комуникацију (заобилазећи могуће мере заштите, као што је шифровање) и преузима контролу над било којим хардвером и софтвером који је доступан на уређају, као што су микрофони или камере. Ако се не регулише, шпијунски софтвер би могао да се претвори у уређај за 24-часовни надзор, добијајући потпун приступ свим сензорима и информацијама на личном уређају. Ово би га претворило у оружје за надзор које би се могло користити за ограничавање

7 Europol/Eurojust, "Third Report of the Observatory Function on Encryption", 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/3rd_report_of_the_observatory_function_on_encryption-web.pdf , 15. april 2025.

8 В. Бајовић, *op. cit.*, 158.

9 Europol/Eurojust, *op. cit.*

10 Venice Commission , Report on a rule of law and human rights compliant regulation of spyware, Venice Commission, Report No. 1173/2024, 13. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e 17. април 2025

људских права, цензурисање и криминализацију критике и неслагања и узнемиравање (ако не и сузбијање) новинара, активиста за људска права, политичких противника или репресију над организацијама цивилног друштва, као што показују бројни наводи и открића. Стога је кључно обезбедити јасне оквире у вези са употребом шпијунског софтвера од стране државе како би се спречиле и искориниле злоупотребе.[11]

Све поменуте опасности од неконтролисане употребе шпијунског софтвера посебно долазе до изражаја у контексту међународне правне помоћи у кривичним стварима. Остале државе које немају посебно предвиђен механизам за употребу таквог софтвера, могу примењивати опште законске одредбе у тим посебним ситуацијама. Имајући то у виду, може се направити разлика између законских оквира држава које дозвољавају директно нападање шифрованог садржаја и оних које предвиђају употребу алата за приступ садржају пре него што се догоди шифровање или након што се тај садржај дешифрује[12]. Треба истаћи и да су италијански судови у пракси прихватили законитост коришћења тројанских или шпијунских софтвера који, након инсталирања у уређај омогућавају приступ свим подацима који се у њему налазе, као и снимање комуникације па је с тим у вези Врховни касациони суд заузео став да је примена ове мере могућа само у поступцима за најтежа кривична дела попут тероризма и организованог криминала.[13]

2.1. Упоредна искуства у поступцима међународне правне помоћи у кривичним стварима - криптована комуникација

На националном нивоу, и даље пред судовима широм Европе, постоји доста случајева у којима се разматра односно оспорава прихватљивост доказа прибављених путем пресретања шифрованих комуникационих платформи.[14] Према подацима објављеним у оквиру Eurojust's Cybercrime Judicial Monitor[15] у низу држава се поставило то питање. На овом месту ће бити поменута само нека искуства. Тако је у Немачкој, Савезни суд правде одбацио жалбу поднету након пресуде коју је донео Регионални суд у Хамбургу 15. јула 2021. године (пресуда за кривична дела трговине дрогом). Суд је пресудио да се подаци са EncroChat-а које је проследила Француска могу

11 *Ibidem.*

12 Europol/Eurojust, *op. cit.*

13 *Ibidem.*

14 EU innovation hub for internal security, First report on encryption, 2024 https://www.eurojust.europa.eu/sites/default/files/assets/eu-innovation-hub-first-report-on-encryption.pdf, 15. april 2025.

15 Eurojust, Cybercrime Judicial Monitor, Issue 9, 2024 https://www.eurojust.europa.eu/sites/default/files/assets/cybercrim-judicial-monitor-issue-9.pdf, 16. april 2025.

користити као доказ само ако служе сврси истраге тешких кривичних дела[16]. Пре тога су немачки судови у више случајева и практично без превише оклевања прихватали као доказе информације произишле из надзора остварених коришћењем апликације EnchroChat.[17] Такође, у Француској, суд је потврдио одредбе члана 706-102-1 Кривичног законика Француске у сврху добијања овлашћења за спровођење прикупљања података.[18] У поменутом члану је прописано да истражни судија у истрази организованог криминалитета може, након прибављања мишљења јавног тужиоца, да дозволи истражитељима да угради технички уређај како би се приступило подацима, они снимили, похранили и пренели без сагласности лица којем такви подаци припадају. Самом законском одредбом је потом прецизирано и да се технички уређај може поставити у рачунар или мобилни телефон на лицу места односно физички или са даљине.[19] Поред тога, суд је одлучио да техника прикупљања може бити тајна из разлога националне безбедности. Ова пресуда уследила је након раније повољне одлуке Француског уставног суда од 8. априла 2022. године.[20]

Што се тиче Италије, Врховни касациони суд је разматрао упућивање од нижег суда у Риму, којим је одбијен захтев туженог за откривање информација о полицијским методама које се користе за прикупљање и дешифровање података SkyECC-а. У том упућивању су изнете тврдње да с обзиром да су материјал прибавили Европол и страни правосудни органи на основу Европског истражног налога, информације могу бити коришћене без даљег испитивања на основу претпоставке да је пресретање законито извршено. Међутим, Врховни касациони суд је пресудио да се шифроване поруке које су добили Европол и стране власти не могу користити на претпретресном рочишту, осим ако тужиоци не објасне како су такви докази прибављени. Врховни касациони суд је истакао да принцип унакрсног испитивања подразумева дијалектички поступак, не само у погледу прегледа прибављеног материјала, већ и у погледу начина прибављања наведеног материјала. Према ставу Врховног касационог суда, окривљени би требало да буде у могућности да доведе у питање не само садржај, већ и поступак прикупљања и истраживања овог материјала, како би се одбрани дала пуна права и како би се проценила релевантност, поузданост и доказна вредност прикупљеног материјала. Поред наведеног, 2023. године је донето још неколико пресуда Врховног касационог суда Италије у вези са платформама за шифровану комуникацију, попут SkyECC и EncroChat, којима су потврђене раније позитивне одлуке о валидности и употребљивости прикупљених података у судским поступцима.[21] Такође, 29. фебруара 2024. године, здружена кривична одељења

16 EU innovation hub for internal security, *op. cit.*, 16.
17 М.Шкулић, *op. cit.*, 28.
18 EU innovation hub for internal security, *op. cit.*, 16.
19 М.Шкулић, *op. cit.*, 23.
20 EU innovation hub for internal security, *op. cit.*, 16.
21 *Ibidem*.

Врховног касационог суда Италије издала су привремене информације о исходу два кривична поступка у вези са употребом криптоване комуникације дешифроване од стране иностраног органа а које ће у наредном периоду бити допуњене комплетним пресудама.[22]

У Холандији је Врховни суд први пут одлучивао о законитости коришћења података из шифрованих телефонских комуникација. Суд је пресудио да су подаци које су пренеле канадске власти легитимно коришћени као доказ у кривичном поступку. Ова одлука се односила на хаковање Еуротерминала у Антверпену у Белгији 2020. године. Осумњичени су били умешани у увоз и трговину кокаином великих размера. Истрага је почела на основу пресретнутих порука које су стизале од EncroChat-а и SkyECC-а. Одбрана је оспорила легитимност операција у вези са овим шифрованим комуникационим услугама. Суд је утврдио да су ове операције биле легитимне и да су спроведене у складу са националним законом[23]. Суд је изјавио да није у надлежности холандског судије да преиспитује да ли је начин на који је истрага спроведена под одговорношћу страних власти у складу са правилима права која се примењују у дотичној земљи за спровођење те истраге. Такође истакнуто је и да је у вези са применом истражног овлашћења у иностранству под одговорношћу страног органа, овлашћење односно ауторизација холандског истражног судије потребна само ако су истражне мере, које треба да спроведе страни орган, затражене од стране холандског органа. То би подразумевало ситуацију када страни орган обавести холандске власти да намерава да пресретне или је пресрео телекомуникације док се телекомуникациона адреса лица које треба пресрести или је пресретнуто користи на територији Холандије. Суд се осврнуо и на могућност одбране да испита законитост начина на који су докази прибављени, а све имајући у виду принцип једнакости оружја као једну од карактеристика ширег концепта правичног суђења. У том смислу, Суд се осврнуо на став ЕСЉП да право на откривање релевантних доказа није апсолутно право и истакао да у сваком кривичном поступку могу постојати супротстављени интереси, као што су с једне стране национална безбедност или потреба заштите сведока који су у опасности од одмазде или чување тајних метода истрага злочина а с друге се налазе права оптуженог која се морају упоредити[24]. Јасно је из става Врховног суда Холандије да се може доказивати супротно, а терет таквог доказивања, по логици ствари, пада на оне субјекте којима је то у интересу, а то су окривљени и његов бранилац али се и од суда очекује да поклони пажњу тим питањима[25]. Поједини аутори су такође сагласни да су одлуке холандских судова адекватне и транспарентне али

22 Eurojust, Cybercrime Judicial Monitor, *op. cit.*, 15.
23 EU innovation hub for internal security, *op. cit.*, 16.
24 Eurojust – Cybercrime Judicial Monitor, *op. cit.*, 17.
25 М.Шкулић, *op. cit.,* 23.

да се такав закључак не може извести у односу на поступање других органа формалне социјалне контроле (пре свега полиције).[26]

За крај треба поменути примере Норвешке и Црне Горе као држава које нису чланице Европске Уније. Врховни суд је пресудио у корист раније одлуке Окружног суда у Ослу да је материјал из шифроване комуникационе услуге (тј. EncroChat) дозвољен као доказ у кривичном случају трговине дрогом. Ову одлуку је првобитно потврдио норвешки Апелациони суд. Претпоставка за закључак Врховног суда била је да су докази легално прибављени у складу са француским законом.[27]

У случају Црне Горе ради се о подацима достављеним од стране ЕУРОПОЛ-а о пресретању комуникација остварених путем апликације SkyECC за мобилне телефоне, из којих произилази да су од стране правосудних органа Републике Француске вршени тајни надзор и претрес сервера апликације SkyECC, која је криптована и заштићена и коју је користило више лица са територије Црне Горе, а и из других држава, док достављени докази, по тврдњи тужилаштва, указују на основану сумњу да су окривљени били корисници поменуте апликације[28]. При томе су се користили шифрама које су идентификоване и комуницирали су путем порука, размене фотографија и другог материјала, а таква комуникација упућује на основану сумњу о деловању криминалне организације у правцу набавке и држања ватреног оружја. У конкретном случају изостала је од стране првостепеног суда оцена доказног значаја ове комуникације, уосталом као и осталих доказа 'на којима се темељи оптужница[29].

2.2. Искуство Србије

Што се тиче ситуације у Србији у погледу коришћења садржаја дешифроване криптоване комуникације, она произилази у овом тренутку из одговарајуће праксе Апелационог суда у Београду (АСБ) у чијој надлежности је одлучивање по жалбама на одлуке првостепених судова. Имајући у виду специфичност предмета у којима се јавља потреба за тумачењем АСБ, у питању су одређене одлуке Вишег суда у Београду, Посебног одељења за организовани криминал.

Став АСБ јесте да приликом оцене доказне прихватљивости података прикупљених од стране надлежних иностраних органа надзором сервера платформе SkyECC треба најпре имати у виду да ли су исти прибављени у складу с важећим прописима Републике Француске и на основу одлуке

26 P. Hartel, R.V.Wegberg, "Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases", *Crime Science,* 5/2023, 7.

27 EU innovation hub for internal security, *op. cit.*, 7.

28 Г. П. Илић *et al.*, *Коментар Законика о кривичном поступку - дванаесто измењено и допуњено издање*, Ј.П. Службени гласник, 2024, 549.

29 Апелациони суд Црне Горе, Квсж, бр. 143/23 од 12. јуна 2023.

надлежног правосудног органа те земље.[30] При томе је предмет замолнице било достављање доказа и доказног материјала, па је нејасна тврдња првостепеног суда да докази садржински одговарају доказној радњи рачунарско претраживање података (чл. 178–180. Законика о кривичном поступку[31] (у даљем тексту ЗКП) с обзиром да рачунарско претраживање података подразумева претраживање већ обрађених личних и других података и њихово поређење са подацима који се већ налазе у базама података које се односе на осумњиченог и кривично дело па се сходно томе, по логици ствари врше на серверима који се налазе на нашој територији док се у конкретном случају ради о криптованој комуникационој платформи са серверима у иностранству. Ни закључак првостепеног суда да се наведени подаци могу сматрати случајним налазом (члан 164. ЗКП) није јасан[32] с обзиром да предметна SkyECC комуникација није прибављена применом мера према одређеном лицу па ни према организаторима или припадницима организоване криминалне групе окривљеног Вељка Беливука и других, већ према свим корисницима SkyECC телефона.

У склопу разматрања наведене аргументације коју је истакао АСБ може се рећи за други и трећи аргумент да су смислени. С друге стране, није јасно, нарочито с обзиром на међународне документе на које се АСБ позвао у својој одлуци, како је дошао до закључка о обавези домаћег суда да провери да ли су подаци с платформе SkyECC прибављени у складу с важећим француским прописима. У поступку пружања међународне правне помоћи у кривичним стварима се примењује правило *locus regit actum*. При томе је у конкретном случају била реч о, као што је исправно приметио АСБ, већ прикупљеном доказном материјалу, а у поступцима пружања међународне помоћи у кривичним стварима напушта се и начело о двострукој кажњивости (то је случај у земљама Европске уније), па је тешко разумети да би захтев за проверу законитости поступања у замољеној држави у вези с прикупљеним доказима имао неко оправдање.[33]

3. КРИПТОВАНА КОМУНИКАЦИЈА И ПРАКСА ЕВРОПСКОГ СУДА ЗА ЉУДСКА ПРАВА И СУДА ПРАВДЕ ЕВРОПСКЕ УНИЈЕ

Као што је већ поменуто коришћење криптоване комуникације односно дешифровање њеног садржаја и коришћење у кривичним поступцима отвара низ питања и производи многобројне дилеме, а посебно оне које се тичу

30 Апелациони суд у Београду, Кж1. По1. бр. 23/22 од 7. априла 2023.

31 Законик о кривичном поступку - ЗКП, Службени гласник РС, бр. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – одл. УС и 62/21 – одл. УС.

32 Г. П. Илић *et al.*, *op. cit.,* 549.

33 *Ibidem.*

заштите легитимних интереса појединца. У том смислу, током последњих година у пракси Европског суда за људска права (ЕСЉП) разматрана је проблематика масовног пресретања комуникација. Чињеница је да је захваљујући откривању и пресецању платформи EncroChat и SkyECC у великој мери дошло до откривања и спречавања многих кривичних дела, што у складу са чланом 8. став 2. Европске конвенције за заштиту људских права и основних слобода (ЕКЉП) чини оправданим задирање јавних власти у право појединаца на неповредивост комуникације али је дискутабилно да ли је то обављено у складу са законом и захтевима које је ЕСЉП поставио у својој досадашњој пракси. Све то представља предмет посебне дискусије када се има у виду да примењеним мерама није само пресецана комуникација лица која се доводе у везу са извршењем одређених кривичних дела већ свих корисника EncroChat и Sky ECC телефона.[34]

Став ЕСЉП исказан у предмету *Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva* јесте да иако судско одобрење представља важно јемство, оно само по себи није ни неопходно ни довољно за осигурање усаглашености законских решења са захтевима члана 8. ЕКЉП. Од кључног значаја јесте начин на који се систем пресретања комуникација примењује у пракси, а то подразумева провере и уравнотежену примену овлашћења и (не)постојање доказа о њиховој злоупотреби. Иако свака држава има широко поље слободне процене да одлучи да ли ће применити режим масовног пресретања комуникација, анализа овлашћења обавештајне службе Уједињеног Краљевства указала је на два недостатка.[35] Први се односи на непостојање надзора над поступком одабира, а то укључује избор органа којима ће бити поверено спровођење пресретања комуникације, особе које врше одабир, критеријуме за издвајање пресретнутих комуникација и избор прикупљеног материјала који ће бити анализиран. Поред тога, не постоје било какве стварне гаранције помоћу којих би се вршио избор повезаних комуникационих података за испитивање. Све то упућује на закључак да постојећи законски механизам масовног надзора комуникација у Уједињеном Краљевству не испуњава стандарде који се везују за квалитет закона и услед тога је утврђена повреда члана 8. ЕКЉП.[36] У истом предмету Велико веће ЕСЉП је истакло пре свега да масовни надзор комуникација није нужно противан ЕКЉП али да такав систем мора бити праћен „заштитним мерама од краја до краја" (*end-to-end safeguards*; *garanties de bout en bout*), а то значи да неопходност и сразмерност предузетих мера мора бити на националном нивоу оцењивана у свим фазама поступка. Другим речима, активности масовног пресретања морају бити од почетка под режимом одобрења од стране независног органа – приликом одређивања предмета

34 В. Бајовић, *op. cit.,* 173.

35 Г. П. Илић *et al*., *op. cit.,* 543.

36 *Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva*, application nos. 58170/13, 62322/14 и 24960/15, 13. септембар 2018.

и обима операције – и да активности морају бити под надзором и независном контролом предузетом *a posteriori*.[37]

У случају *Yüksel Yalçınkaya protiv Turske,* разматрајући конкретно проблематику криптоване комуникације, ЕСЉП је најпре анализирао њен значај у светлу члана 7. ЕКЉП.[38] У конкретном случају закључак о припадништву оружаној терористичкој организацији почивао је у одлучујућој мери на употреби критоване апликације за размену порука ByLock. Другим речима, припадништво није законито утврђено, на индивидуализован начин, испитивањем објективних и субјективних елемената кривичног дела. Главно питање је било да ли је његова осуда била довољно предвидљива с обзиром на захтеве домаћег права, посебно у погледу кумулативних материјалних и психичких елемената кривичног дела онаквих какви су се појавили у релевантном правном оквиру. Посебно је морало бити доказано да је оптужени имао органску везу са организацијом засновану на континуитету, разноврсности и интензитету својих активности и да је знао да је организација учинила или имала за циљ да учини злочине и да је морао имати специфичну намеру за реализацију тог циља. Тумачење домаћих судова је повезивало на готово аутоматски начин кривичну одговорност са корисницима апликације ByLock што је имало за последицу повреду члана 7. ЕКЉП. У својој одлуци ЕСЉП се није суштински ни бавио питањем правне ваљаности надзора криптоване комуникације захваљујући коришћењу конкретне апликације намењене заштити тајности комуницирања нити се на било који начин упуштао у било какву оцену неке начелне доказне употребљивости и доказне веродостојности те врсте информација.[39]

Друго питање се тицало испуњености захтева за правичношћу суђења. У случају да одбрана није имала могућност да испита поузданост и веродостојност података добијених са сервера апликације за размену криптованих порука, домаћи судови су били дужни да то учине са нарочитом строгошћу. То није био случај, а ни образложења нису садржала одговоре на спорна питања која је постављала одбрана.[40] Посебно, домаћи судови нису ни навели разлоге за спорно неоткривање, нити су одговорили на захтев подносиоца захтева за независно испитивање података ради провере њиховог садржаја и интегритета, нити на његове забринутости у вези са њиховом поузданошћу. Последица је била повреда права на правично суђење из члана 6. став 1. ЕКЉП.

Питање прихватљивости података добијених тајним надзором криптоване комуникације остварене преко платформе EncroChat размотрио је Суд правде Европске уније. У контексту истраге коју су спровеле француске

37 *Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva* (Велико веће), application nos. 58170/13, 62322/14 и 24960/15, 25. мај 2021.

38 *Yüksel Yalçınkaya protiv Turske* (Велико веће), application no. 15669/20, 26. септембар 2023.

39 М. Шкулић, *op. cit.,* 38.

40 Г. П. Илић *et al*., *op. cit.,* 550.

власти, испоставило се да су оптужени користили шифроване мобилне телефоне који су радили под лиценцом „EncroChat“ како би вршили кривична дела првенствено везана за трговину дрогом. Ти мобилни телефони имали су посебан софтвер и модификовани хардвер који је омогућавао шифровану комуникацију од краја до краја (*end-to-end*; *de bout en bout*), преко сервера у Рубеу (Француска), коју није било могуће пресрести конвенционалним истражним средствима („услуга EncroChat“).[41] Француска полиција је, уз помоћ холандских стручњака, успела да осмисли рачунски програм у виду „тројанског коња“ који је, на основу одлуке суда, 2020. инсталиран провајдеру услуге EncroChat, а налазио се у Француској. Услугу EncroChat је користило 32.477 корисника из 122 земље, а 4.600 било је у Немачкој. Због тога се Земаљски суд у Берлину обратио Суду правде у Луксембургу са питањем да ли и под којим условима материјал прикупљен од стране француске полиције може да буде, на основу европског истражног налога, коришћен у кривичном поступку пред немачким судом.[42]

Генерални адвокат Суда правде Европске уније у свом мишљењу, између осталог, закључује да је питање о могућности преношења доказа који се састоје од пресретнуте комуникације прибављене за једну кривичну истрагу или поступак у другу истрагу или други поступак ствар немачког закона, а само то питање није решено Директивом о европском истражном налогу[43] већ се, уместо тога, у Директиви само позива на закон државе из које је налог издат[44]. Међутим, захтев о постојању истих материјалних претпоставки у две државе се не поставља када је реч о прослеђивању доказа које већ поседују органи замољене државе. Посебно је наглашено да у вези с тим доказима доносилац налога није овлашћен да надзире правилност поступка у којем их је замољена држава прикупила. На крају, али не мање важно, приликом приступа терминалима с циљем пресретања комуникација мора се обавестити одређени орган у држави чланици Европске уније на чијој територији се налази субјект пресретања.[45]

4. УЛОГА ИСТРАЖИВАЧКОГ НОВИНАРСТВА У МЕЂУНАРОДНИМ ИСТРАГАМА КРИПТОВАНЕ КОМУНИКАЦИЈЕ – ПРОЈЕКАТ “CRIME MESSENGER”

Имајући у виду специфичност проблематике и тешкоће које постоје на путу препознавања доказног значаја криптоване комуникације како

41 Суд правде Европске уније (Велико веће), C-670/22, 30. април 2024.
42 *Ibidem.*
43 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.
44 М. Шкулић, *op. cit.,* 41, 42.
45 Суд правде Европске уније (Велико веће), C-670/22, 30. април 2024.

унутар једне државе тако и у контексту међудржавне сарадње у кривичним стварима требало би поменути и неке алтернативне видове истраживања значаја такве комуникације који представљају резултат истраживачког новинарства.

Један од таквих ангажмана реализован је у оквиру пројекта „Crime Messenger". Истрага „Crime Messenger" подразумевала је сарадњу између 13 медијских партнера широм Европе и Канаде и представља најсвеобухватнији увид до сада у оно што представља „Sky Global" као и начин на који су се његови производи продавали и користили.[46]

Тим новинара је добио приступ цурењу близу 3.800 докумената из француске судске истраге о Sky ECC-u, где је Париски суд централизовао европске поступке против људи повезаних са компанијом. Новинари су такође прегледали судске поднеске, корпоративне документе и друге јавне евиденције.[47] Успели су да прибаве и извештаје овлашћених полицијских службеника и доказе пронађене на Sky телефонима, као што су транскрипти ћаскања и фотографије дроге и оружја послатих преко Sky апликације. Између осталог, у неким случајевима, те датотеке подразумевају и полицијске резимее порука пронађених на телефонима. Ове датотеке су затим укрштене са доказима добијеним из јавних евиденција и судских докумената у Холандији, Немачкој, Канади, Белгији и Србији, а допуњене су интервјуима многих кључних играча у Sky универзуму.

У августу 2024. године, након вишегодишње истраге француских судија, извршни директор Sky Global, Жан-Франсоа Еп (Jean-Francois Eap), и још 30 људи повезаних са компанијом – укључујући високопозициониране запослене у Sky компанији, дистрибутере и локалне продавце – оптужени су за криминално удруживање, прање новца и дистрибуцију шифрованих уређаја без одговарајуће регистрације. Еп је такође оптужен у САД за наводно олакшавање међународне трговине дрогом путем Sky телефона. Еп и друге личности повезане са Sky апликацијом негирале су било каква кривична дела. Сам пројекат „Crime Messenger" такође се ослања на информације из ових кривичних оптужница.[48]

Почетком ове године Париски суд је по други пут одбио пуштање уз кауцију бизнисмена Томаса Хердмана, из Канаде, који се суочава са оптужбама за дистрибуцију шифрованих телефона, наводећи да представља ризик од бекства и да правда мора бити спроведена. Хердман се већ четири године налази у притвору у Француској и чека и даље на суђење, као вероватно

46 Balkan Criminals Planned Murders Using Encrypted Phones from Canadian Start-Up Sky Global, Organized Crime and Corruption Reporting Project, 2024 https://www.occrp.org/en/project/the-crime-messenger/sky-phones-were-distributed-through-serbias-most-brutal-criminal-networks, 13. април 2025.

47 Frédéric Zalac and Paul Émile d'Entremont, The Crime Messenger, https://www.cbc.ca/newsinteractives/features/the-crime-messenger, 12. април 2025.

48 Balkan Criminals Planned Murders Using Encrypted Phones from Canadian Start-Up Sky Global, *op. cit.*

једини са списка од 31 оптужених који се налази на француској територији. Канађанин, који негира све оптужбе, оптужен је за 22 кривична дела, укључујући прање новца од организоване трговине дрогом путем дистрибуције шифрованих телефона компаније Sky ECC.[49]

У основи поставило се питање улоге компаније односно њених представника у одвијању организованог криминалног деловања. Да ли су стварно потпуно ван тог процеса, како су представници Sky Global компаније тврдили и да је њихова једина мисија била да направе алат који омогућава приватну комуникацију па да се самим тим њихова улога исцрпљивала у продаји телефона који омогућавају шифровану комуникацију која сама по себи није спорна и постала је уобичајена. Из компаније су такође тврдили да су услови коришћења забрањивали криминалне активности али да свакако нису били у могућности да спрече евентуалне злоупотребе од стране одлучног и технолошки вичног корисника. Међутим, докази које су новинари добили у оквиру пројекта „Crime Messenger" показују да су неки од најпродуктивнијих корисника телефона били личности организованог криминала.[50] Свакако треба сачекати епилог покренутих поступака што ће потрајати с обзиром да је планирано да се тек у пролеће 2026. године у Паризу одржи заседање у специјалном кривичном суду док је, с друге стране, тренутни статус америчког случаја нејасан. Што се тиче поменутог заседања у француском суду, том приликом би веће од петорице судија требало да обави саслушање у случају против свих 30 људи оптужених за умешаност у дистрибуцију шифрованих мобилних телефона које наводно користе припадници организованих криминалних група.[51]

5. ЗАКЉУЧАК

Развој технологије је непрекидан процес који се манифестује у свим сферама функционисања савременог човека. Поред позитивних аспеката тог развоја како за појединце тако и друштво у целини, технолошки напредак погодује и лицима која делују са друге стране закона. Једна од сфера у којој је то посебно изражено су комуникације о чему сведочи проблематика која је обрађивана у раду.

Потреба за безбедном комуникацијом у данашње време када је тешко сачувати приватност постала је универзални стандард коме теже сви људи подједнако. Ипак, у случају вршења одређених кривичних дела и деловања појединих криминалних организација то је постало посебно изражено. С друге стране, неопходност сузбијања посебно опасних облика криминалног

49 Canadian businessman remains in French jail, accused of distributing Sky ECC cryptophones https://www.computerweekly.com/news/366619740/Canadian-businessman-remains-in-French-jail-accused-of-distributing-Sky-ECC-cryptophones, 12. април 2025.

50 Frédéric Zalac and Paul Émile d'Entremont, *op. cit.*

51 Canadian businessman remains in French jail, *op. cit.*

деловања односно откривања и гоњења учинилаца тих дела довела је до значајних измена у сфери процедура које се у том смислу предузимају. Досадашњи законски оквири за предузимање радњи доказивања у многим државама више нису у довољној мери адекватни што води ка одговарајућим модификацијама и прилагођавањима а све у циљу ефикасног сузбијања одређених облика криминала попут организованог или тероризма.

У том процесу прилагођавања новонасталим околностима долази до многобројних недоумица на који начин поступати са садржајем такве шифроване комуникације, посебно ако се до ње дође у поступцима међународне правне помоћи у кривичним стварима. Досадашња упоредна искуства могу помоћи државама у разјашњавању сопствених дилема али би могла да буду и пут ка изменама и унификацији решења, нарочито у оквиру сличних правних система али и подручја која су повезана чињеницом прекограничне сарадње учинилаца кривичних дела што оправдава циљ заједничке акције усмерене ка сузбијању тешких облика криминалитета. Посебан значај у том смислу има пракса ЕСЉП али и Суда правде Европске уније како би се олакшао и убрзао процес усклађивања решења у различитим државама али и водило рачуна о легитимним интересима појединаца који морају бити заштићени без обзира на оправданост задирања у приватност комуникације.

Као и у многим другим сегментима, и овде се испољава важност улоге медија у осветљавању проблематике. Један од примера истраживачког новинарства презентован у раду указује на значај алтернативног приступа у анализи феномена који још увек нису довољно препознати и истражени уобичајеним каналима.

ЛИТЕРАТУРА

Bajović V. „EnroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku", *Crimen*, 2/2022.

Грубач М., Илић Г. П., Мајић М., *Коментар Закона о међународној правној помоћи у кривичним стварима*, Правни факултет у Београду, ЈП Службени гласник, Београд, 2009.

Илић А., „Међународна правна помоћ у кривичним стварима у светлу нове организације кривичног правосуђа", *Раскршћа међународног кривичног и кривичног права – реформа правосудних закона Републике Србије,* (ур. Шкулић М., Миљуш И., Шкундрић А.), Удружење за међународно кривично право, Универзитет у Београду – Правни факултет, Београд, 2023.

Илић Г. П., Бељански, С., Мајић, М. и Трешњев, А., *Коментар Законика о кривичном поступку*, Дванаесто измењено и допуњено издање, ЈП Службени гласник, Београд, 2024.

Hartel P., Wegberg R, "Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases", *Crime Science,* 5/2023.

Škulić M., „Dokazni značaj informacija iz komunikacije ostvarene aplikacijama/modifikovanim uređajima za kriptovanje kao što su Sky ECC i EnchroChat", *Crimen,* 1/2024, 3–55.

ИНТЕРНЕТ ИЗВОРИ

Balkan Criminals Planned Murders Using Encrypted Phones from Canadian Start-Up Sky Global, Organized Crime and Corruption Reporting Project, 2024 https://www.occrp.org/en/project/the-crime-messenger/sky-phones-were-distributed-through-serbias-most-brutal-criminal-networks.

Canadian businessman remains in French jail, accused of distributing Sky ECC cryptophones https://www.computerweekly.com/news/366619740/Canadian-businessman-remains-in-French-jail accused-of-distributing-Sky-ECC-cryptophones

EU innovation hub for internal security, First report on encryption, 202 https://www.eurojust.europa.eu/sites/default/files/assets/eu-innovation-hub-first-report-on-encryption.pdf

Eurojust, Cybercrime Judicial Monitor, Issue 9, 2024 https://www.eurojust.europa.eu/sites/default/files/assets/cybercrim-judicial-monitor-issue-9.pdf

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

Frédéric Zalac and Paul Émile d'Entremont, The Crime Messenger, https://www.cbc.ca/newsinteractives/features/the-crime-messenger

Venice Commission, Report on a rule of law and human rights compliant regulation of spyware, Venice Commission, Report No. 1173/2024, 13. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2024)043-e

ПРАВНИ ИЗВОРИ

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

Закон о међународној правној помоћи у кривичним стварима – ЗМППКС, *Службени лист СРЈ*, бр. 20/09.

Законик о кривичном поступку - ЗКП, *Службени гласник РС*, бр. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – одл. УС и 62/21 – одл. УС.

СУДСКА ПРАКСА

Апелациони суд у Београду, Кж1. По1. бр. 23/22 од 7. априла 2023.

Апелациони суд Црне Горе, Квсж, бр. 143/23 од 12. јуна 2023.

Big Brother Watch i ostali protiv Ujedinjenog Kraljevstva, application nos. 58170/13, 62322/14 и 24960/15, 13. септембар 2018.
Суд правде Европске уније (Велико веће), C-670/22, 30. април 2024.
Yüksel Yalçınkaya protiv Turske (Veliko veće), application no. 15669/20, 26. septembar 2023.

Aleksandra Ilić, PhD*

ENCRYPTED COMMUNICATION IN THE LIGHT OF INTERNATIONAL LEGAL ASSISTANCE IN CRIMINAL MATTERS

Summary

The author of the paper discusses the current issues of using encrypted communication content in criminal proceedings primarily from the perspective of international legal assistance in criminal matters. After introductory considerations in which the concept of encrypted communication and international legal assistance in criminal matters is defined, certain challenges of international legal assistance in the sphere of using encrypted communication are analyzed. Encrypted communication resulting from the Sky ECC and EncroChat applications and their use in criminal proceedings are particularly considered in the context of comparative experiences of individual European countries, but also taking into account the situation in Serbia. Given the importance of the practice of the European Court of Human Rights and the Court of Justice of the European Union for clarifying certain dilemmas in the circumstances of international legal assistance in criminal matters in the case of encrypted communication that have arisen in recent years in the practice of judicial authorities of many countries, the paper also provides a review of this aspect. Finally, the importance of investigative journalism in international investigations of encrypted communications was highlighted.

Keywords: encrypted communication, international legal assistance in criminal matters, European Court of Human Rights, Court of Justice of the European Union, investigative journalism.

* Associate Professor, University of Belgrade – Faculty of Security Studies, aleksandra.ilic@fb.bg.ac.rs.