

Проф. др Дарко МАРИНКОВИЋ¹

Криминалистичко-полицијски универзитет у Београду

Проф. др Јелена МАТИЈАШЕВИЋ²

Правни факултет за привреду и правосуђе, Нови Сад

ДОИ: 10.5937/bezbednost2602005M

УДК: 343.983:004.7

342.721:343.13

Оригинални научни рад

Примљен: 19. 4. 2026. године

Датум прихватања: 17. 6. 2026. године

Надзор савремених комуникационих технологија у криминалистичким истрагама

Анстракт: Рад анализира комплексни феномен надзора савремених комуникационих технологија и његов значај у криминалистичким истрагама. Полазећи од идентификације технолошких изазова које намећу ОТТ (Over-The-Top) услуге, истраживање поставља теоријски и практични оквир надзора кроз анализу стадијума комуникационог процеса, идентификујући кључне тачке за пресретање информација у дигиталном окружењу. Посебан фокус стављен је на радњу онлајн претраге информационо-техничких система, уз елаборацију правних стандарда и техничких модалитета тзв. форензике уживо. Централни део рада посвећен је оперативним захватима у сфери специјално заштићених комуникационих платформи, анализирајући стање хардверске изолације уређаја и стратешке рањивости серверске инфраструктуре. Критички се преиспитује и надзор над задржаним подацима, уз наглашавање значаја заштите приватности у овој сфери. Закључна разматрања указују на тренд децентрализације комуникација у циљу избегавања мера надзора, који за истражне органе поставља императив дубинског познавања анатомије дигиталних процеса као основног услова за ефикасно сузбијање савременог криминала.

¹ darko.marinkovic@kpu.edu.rs, ORCID 0000-0002-5456-1343

² jelena@pravni-fakultet.info, ORCID 0000-0001-8068-0816

Кључне речи: надзор комуникација, ОТТ услуге, онлајн претраге, криптоване платформе, Sky ECC, задржани подаци.

Увод у тему и идентификација истраживачког проблема

Пре појаве електронских комуникација и дигиталних медија, постојале су само две врсте размене информација – усмена и писмена. Усмена комуникација се већ прилично дуго не одвија само путем кабловске/жичане телефонске мреже – мобилна телефонија је данас постала потпуно доминантна, уз присуство и тзв. сателитских телефона. Отишло се и много даље, мобилни телефони су постали паметни – интегришући у себи нове технологије, донели су револуцију у комуницирању, које је захваљујући интернету постало готово бесплатно. С друге стране, сваки облик комуникација може се обављати и путем компјутера и других сличних уређаја, обухватајући видео-позиве, слике, видео-записе и документа у разним форматима. У том смислу, крај XX и почетак XXI века донео је фундаменталне промене у области комуникационих технологија и начина на који их људи користе.

Као резултат радикално нижих трошкова и свеprisутности интернета, већина људи своје мејлове, календаре, фотографије, видео-записе и друге документе чува код интернет-провајдера (рачунарство у облаку, енгл. *cloud computing*), а не на интерним или преносним меморијама (екстерни HDD, SSD, USB или меморијске картице). И онлајн комуникација, као вид електронске комуникације у којој саговорници на друштвеној мрежи или апликацији за комуникацију истовремено размењују информације, доживела је праву експанзију.

Кључни разлог због којег су традиционалне методе надзора постале оперативно неефикасне лежи у појави тзв. ОТТ (енгл. *Over-The-Top*) услуга. У традиционалном моделу, телекомуникациони оператори контролишу целокупан комуникациони процес – од физичке инфраструктуре (каблови и базне станице), до саме услуге (гласовни позив и SMS), што истражним органима омогућава спровођење надзора директним приступом централи оператора. Појавом ОТТ сервиса, овај модел надзора се из темеља мења. Дигиталне комуникационе платформе користе интернет-везу искључиво као неутрални канал за пренос података, због чега оператор само региструје проток саобраћаја, без могућности декодирања порука или позива који су под контролом независних платформи, заштићени снажном енкрипцијом.

За истражне органе ово ствара двоструки изазов. Први је техничке природе, јер ОТТ сервиси потпуно неутралишу традиционалне системе надзора на нивоу оператора, чинећи садржај унутар интернет цеви *невидљивим* за треће стране. Други изазов се тиче јурисдикције – будући да оператор више не поседује кључеве комуникације, полиција је приморана да (правну) помоћ тражи директно од власника апликација, који су најчешће лоцирани у другим државама, или да примени инвазивније методе надзора на самим крајњим уређајима (енг. *endpoints*). Управо је ова транзиција са традиционалних на ОТТ услуге приморала савремену криминалистику да фокус надзора са мрежне трансмисије помери ка серверској инфраструктури и директној компромитацији комуникационог хардвера.

Стадијуми комуникационог процеса као основа за тајни надзор у дигиталном окружењу

Хипотетички, тајни надзор комуникација које се одвијају на интернету може се реализовати у три стадијума самог комуникационог процеса – при сачињавању и припреми комуникационог садржаја за слање, тј. на комуникационом изворишту/полазишту, затим током самог процеса трансмисије (енг. *data in motion*) и, на крају, када комуникациони садржај дође до примаоца, на комуникационом одредишту. У којем од ових стадијума ће се тајни надзор комуникације реализовати није од посебног значаја када је реч о писаној комуникацији (нпр. е-пошта, SMS), комуникацији сликама, видео-записима или аудио-записима или разним другим подацима који су пре, током и након трансмисије меморисани и као такви доступни у одговарајућој форми и након што комуникација буде обављена – такви садржаји могу се наћи на самим комуникационим уређајима или серверима. Међутим, важно је напоменути да је у фази саме трансмисије процес надзора отежан или онемогућен употребом напредних система енкрипције (шифровања), због чега стадијум надзора на самим комуникационим уређајима (изворишту или одредишту) често постаје оперативно кључан, јер се само на њима подаци налазе у свом изворном, нешифрованом облику.³

³ Duggirala J.: Demystifying End-to-End Encryption: How It Works in Chat Applications, *International Journal of Innovative Research and Creative Technology*, 2022, Volume 8, Issue 2, pp. 1–2.

Када је реч о комуникацији која се обавља разговором у реалном времену, било да је реч о аудио-позиву или видео-позиву, надзор је по правилу могуће реализовати само док се он одвија. То је последица чињенице да се таква ефемерна (пролазна) комуникација уобичајено не меморише аутоматски на самим уређајима, нити на серверима преко којих се процес одвија. Зато се мера тајног надзора мора спроводити синхронизовано са комуникационим процесом (онлајн надзор), с обзиром на то да најчешће не постоји могућност њеног одложеног или накнадног надзора из базе података. И у овим случајевима комуникација технички може бити пресретнута на три тачке – уређају пошиљаоца (изворишту), током процеса трансмисије кроз комуникациони канал (мрежу) или уређају примаоца (одредишту). Уколико се у комуникацији користи напредна енкрипција, пресретање у фази трансмисије даје само нечитљив дигитални запис, због чега се тежиште надзора поново помера ка самим крајњим уређајима, где се звук и слика налазе у свом изворном, аналогном облику.⁴

Онлајн претраге/даљинско претраживање информационо-техничких система и уређаја

Савремени облици комуникација путем интернета подразумевају енкрипцију података која се одвија аутоматски, без активних радњи корисника – класичне телефонске везе данас све више мења интернет-телефонија (енг. *Voice over Internet Protocol – VoIP*), у којој се говорни сигнал разбија у *IP* пакете који се усмеравају преко интернета, да би се на одредишту поново реконструисали у изворни сигнал.⁵ Кључни изазов за полицијски рад представља чињеница да већина модерних апликација унутар *VoIP* протокола имплементира енкрипцију с краја на крај комуникационог канала (енг. *End-to-End*

⁴ Pisarić M.: Communications encryption as an investigative obstacle, *Journal of Criminology and Criminal Law*, 2022, vol. 60, no. 1, p. 68.

Више – Ellyson L.: *The Impact of Encryption Technologies on Criminal Investigations in Canada: A Balanced Approach to the 'Going Dark' Problem in Light of Self-Incrimination and Privacy Considerations*, (PhD Dissertation, Dalhousie University, Schulich School of Law, 2023) [Unpublished], pp. 247–252, (https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?params=/context/phd_disserations/article/1026/&path_info=LauraEllyson2022.pdf)

⁵ Okafor F., Fagbohunmi G., Eneh I.: Improving the Scalability of Wireless Sensor Networks by Reducing Sink Node Isolation, *Micro Wave International Journal of Science & Technology*, Vol. 7, No. 1, December 2014, pp. 43–44.

Encryption – E2EE), која приступ подацима гарантује искључиво корисницима (енг. *user-only-access*).

Концепт E2EE доминантно почива на асиметричној криптографији, у којој сваки корисник поседује пар кључева – јавни и приватни. Заштита коју пружа E2EE престаје оног тренутка када дође до компромитације приватног кључа на самој крајњој тачки. То је оперативно могуће остварити физичким приступом уређају, инсталацијом малвера (енг. *malware*) или експлоатацијом техничких рањивости (енг. *vulnerabilities*) самог софтвера, чиме се подаци чине доступним у њиховом изворном облику.

Чињеница да се интернет комуникација шифрује на самом изворишту, а дешифрује тек на одредишту, у потпуности онемогућава надзор садржаја током преноса мрежним каналима. Пред истражне органе се поставља сложен оперативни проблем – како приступити уређајима који су у сталном поседу осумњичених, а на којима се чувају кључни подаци. Поред увида у меморисани садржај (*подаци у мирувању*, енг. *data at rest*), од посебног значаја је и континуирано праћење активности у реалном времену ради утврђивања идентитета саучесника и динамике криминалне групе.

Техничко решење овог проблема представља инсталирање тзв. *државних тројанаца* (енг. *Govware, Remote Policing Intrusion Software*), специјализованих алата који се прикривено имплементирају у рачунарске систем или паметни телефон. Иако спадају у ширу категорију малвера, ови програми су дизајнирани да компромитују безбедносне функције уређаја и заобиђу контроле приступа.⁶ У криминалистичким истрагама се најчешће примењују *тројански коњи* (енг. *trojan horses*) и *спијунски софтвери* (енг. *spyware*). Поред њих, користе се и специфични алати попут *читача откуцаја на тастатури* (енг. *keyloggers*) за прикупљање лозинки, као и *руткитови* (енг. *rootkits*) који обезбеђују невидљивост процеса надзора унутар самог оперативног система чак и за напредне антивирусне програме.⁷

⁶ Angiano C.: A Review of Mobile Surveillanceware: Capabilities, Countermeasures, and Research Challenges, *Electronics*, 2025, 14, 2763, pp. 1–4.

О компаративно-правним решењима примене државних тројанаца/малвера види – *Venice Commission – Report on a rule of law and human rights compliant regulation of spyware*, Council of Europe, (<https://www.venice.coe.int/files/Spyware/T03-E.htm>)

⁷ Види – Ivanović Z.: *Kriminalistički aspekti visokotehnološkog kriminala*, Beograd, 2021, p. 388.

Државни тројанци се примарно користе за креирање тзв. *скривених врата* (енг. *backdoor*), односно за успостављање неовлашћеног приступног пута који заобилази стандардне сигурносне протоколе и механизме аутентификације.⁸ На тај начин, истражни орган може конспиративно прикупљати акредитиве за приступ веб-локацијама, пратити активности корисника или вршити анонимну претрагу целокупне меморије уређаја. Реч је о специфичном облику *дигиталне форензике уживо* (енг. *live forensics*), с обзиром на то да се прикупљање доказног материјала врши док је оперативни систем покренут и активан, што омогућава приступ подацима који би у супротном остали заштићени енкрипцијом или трајно изгубљени гашењем уређаја. У зависности од оперативних потреба, ови алати омогућавају и регистровање притисака на тастере (чиме се пресреће порука пре него што је алгоритам шифрује), континуирано бележење садржаја екрана (енг. *screenshots*), као и директан надзор над аудио-позивима и видео-позивима унутар VoIP апликација. Најрадикалнија функција ових софтвера огледа се у могућности даљинске активације микрофона и камере, чиме се уређај без знања корисника претвара у средство за амбијентално звучно и оптичко снимање непосредног окружења.⁹

Инсталација државних тројанца на циљаном рачунарском систему или паметном телефону по правилу се може извршити на два начина. Први је онлајн, инфицирањем применом метода фишинга (енг. *phishing*) или фарминга (енг. *pharming*), при чему корисник несвесно преузима злонамерни прилог уз поруку или отвара заражену веб-страницу.¹⁰ Други начин је физички, путем тајног приступа истражног

⁸ Специфичност скривених врата у криминалистичком контексту огледа се у томе што овај метод обезбеђује трајан и независан приступ информационом систему. За разлику од простог прикупљања корисничких лозинки, *backdoor* остаје оперативан чак и у случајевима када корисник промени своје приступне акредитиве, јер софтверски алат одржава сопствени комуникациони канал који функционише паралелно са регуларним сигурносним подешавањима уређаја.

⁹ Gercke, M.: *Understanding Cyber Crime: Phenomena, Challenges and Legal Response*, Telecommunication Development Sector, 2012, (<https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>)

¹⁰ У оквиру савремених онлајн метода инсталације, посебно се издвајају тзв. *zero-click* напади. За разлику од традиционалног фишинга, овај метод не захтева никакву интеракцију или активну радњу корисника (попут отварања прилога или клика на линк). Инфицирање се обавља експлоатацијом скривених рањивости у самим апликацијама – нпр. путем специфично модификованог долазног видео-позива на платформама попут Вотсапа (*WhatsApp*) или Ајмесеца (*iMessage*), чиме

органа уређају (нпр. посредством прикривеног иследника или тајним уласком у просторије). Инсталација државних тројанаца омогућава спровођење истражне радње познате као *онлајн претрага* (енг. *online/remote search*, нем. *Online-Durchsuchung*), односно даљинско претраживање информационо-техничких система, што представља један од најсофистициранијих облика савременог прикупљања дигиталних доказа.¹¹ Њена кључна дистинкција у односу на традиционално пресретање комуникација огледа се у истражном обухвату – док се класичан надзор фокусира искључиво на проток информација у реалном времену, *онлајн претрага* омогућава ретроспективни увид у целокупан *дигитални живот* корисника уређаја. Тиме се брише граница између надзора комуникације и класичног претресања стана, с обзиром на то да истражни орган добија приступ не само размењеним порукама, већ и најинтимнијим подацима у мировању – од приватних бележака и историје претраге, до докумената који никада нису били намењени размени.

се омогућава прикривена инсталација тројанца чак и ако корисник не прихвати позив. Више – *Forensic Methodology Report: How to catch NSO Group's Pegasus*, 18 July 2021, Amnesty International, (<https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>)

¹¹ Vaciago G., Ramalho D. S.: Online searches and online surveillance: the use of trojans and other types of malware as means of obtaining evidence in criminal proceedings, *Digital Evidence and Electronic Signature Law Review*, vol. 13 (2016), pp. 88–96.

У савременој криминалистичкој теорији и пракси, увођење онлајн претрага представља суштинску прекретницу у начину третирања приватности у дигиталном добу. Пионирску улогу у правном дефинисању ове мере имао је немачки *Савезни уставни суд* (BVerfG), који је пресудом из 2008. године закључио да традиционални закони о претресу стана нису применљиви на сферу дигиталних података. Суд је констатовао да савремени рачунарски системи нису пуке дигиталне фасцикле, већ уређаји који представљају епицентар приватности корисника. Ова историјска пресуда утемељила је ново основно људско право – *право на поверљивост и интегритет информационо-техничких система* (нем. *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), уз дефинисање три ригорозна услова примене онлајн претрага: 1) могу се применити искључиво у истрагама најтежих облика криминала; 2) за примену је неопходан судски налог, уз доказ да примена блажих метода не може уродити плодом; 3) током примене се мора заштитити приватна сфера живота, која није предмет истраге. Види – Abel W., Schafer B.: The German Constitutional Court on the Right to Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, *SCRIPTed*, Volume 6, Issue 1, April 2009, pp. 106–112.

Криптоване комуникације – технолошки изазови и оперативни модалитети надзора

Унапређене могућности пресретања електронских комуникација натерале су криминалне организације да се окрену модалитетима комуникације који се тешко прате. Један од њих је комуницирање путем недовршених и непослатих имејл порука, тзв. драфтова, који функционише на принципу дигиталног *мртвог сандучета* (енг. *dead drop*). Осим тога, савремени преступници се све чешће враћају и *дигиталној стеганографији*, односно скривању инкриминишућих порука унутар наизглед безазлених дигиталних фајлова (попут слика или аудио-записа), што представља додатни ниво заштите који захтева напредне алате за детекцију.¹² Безбедносне структуре широм света потврђују да су тзв. *групни разговори* (енг. *chats*) унутар *онлајн игара* посебно погодно тло за прикривену комуникацију. У документу *Искоришћавање игара и виртуелног окружења од стране терориста* (енг. *Exploiting Terrorist Use of Games & Virtual Environments*)¹³ из 2008. године, који је постао доступан јавности захваљујући Сноудену (Snowden), наводи се да је америчка NSA (енг. *National Security Agency*) спроводила масовни надзор у заједницама видео-игара. Служба је чак вршила инфилтрацију својих агената под легендом у виртуелне светове игара, верујући да их терористичке ћелије користе као алтернативне комуникационе мреже које пружају висок степен анонимности.¹⁴

¹² Један од познатијих оперативних примера примене дигиталне стеганографије забележен је 2012. године, када су обавештајне службе пресреле дигитални материјал Ал Каиде. Анализом наизглед безазлених датотека, откривено је да су оперативни планови за будуће нападе били сакривени унутар порнографских видео-записа. Коришћењем специјализованих алгоритама, преступници су уградили преко 100 докумената са инструкцијама у саме пикселе и фрејмове видео-фајла, чиме су подаци постали потпуно невидљиви за стандардне безбедносне филтере. Види – Robertson N., Cruickshank P., Lister T.: *Document shows origins of 2006 plot for liquid bombs on planes*, CNN, April 30, 2012, (<https://edition.cnn.com/2012/04/30/world/al-qaeda-documents>)

¹³ *NSA files: games and virtual environments paper*, NSA document, written in 2008 and titled *Exploiting Terrorist Use of Games & Virtual Environments*, The Guardian, Monday 9 December 2013, (<https://www.theguardian.com/world/interactive/2013/dec/09/nsa-files-games-virtual-environments-paper-pdf>)

¹⁴ Elliott J.: *World of Spycraft: NSA and CIA Spied in Online Games*, ProPublica, Dec. 9, 2013, (<https://www.propublica.org/article/world-of-spycraft-intelligence-agencies-spied-in-online-games>)

Пре великог терористичког напада у Паризу 2015. године,¹⁵ белгијски министар унутрашњих послова изнео је став да је изузетно тешко пратити комуникације терориста које се одвијају путем популарне конзоле за игру *Sony PlayStation*, наводећи примере ранијих хапшења у којима су на овим уређајима пронађени читави оперативни планови акција.¹⁶ Три дана касније, терористи су напали главни град Француске, користећи, између осталог, управо ову платформу за координацију својих активности, упркос тврдњама компаније Сони (*Sony*) да предузима све мере заштите.

Последњих година полицијске акције су готово доминантно усмерене на откривање информација које се размењују путем криптованих телефона који су постали следећа, кључна степеница у настојању преступника да остваре максималну сигурност својих комуникација. Док Вотсап (*WhatsApp*), Сигнал (*Signal*) или Телеграм (*Telegram*) шифрују само комуникациони канал, криптовани телефони обезбеђују читав еко-систем, укључујући и сам хардвер уређаја, путем специјализованих хардверских сигурносних модула (енг. *Hardware Security Module – HSM*). Криптографски кључеви су у овим случајевима смештени у изолованим процесорским зонама, као што су ТЕЕ (*Trusted Execution Environments*) или *Secure Enclave*, који поседују *антидампер* функције за аутоматско уништавање података у случају покушаја неовлашћеног приступа (енг. *brute-force*). Додатно, опција самоуништења порука (енг. *self-destructive messages*) трајно онемогућава или отежава накнадну форензичку реконструкцију комуникације.

Иако савремени системи за заштићену комуникацију имплементирају највише стандарде безбедности (телефон може бити најјача тврђава на свету), сама комуникација унутар њих мора ићи преко сервера, због чега они представљају њихову најкритичнију оперативну тачку. У том смислу јавља се специфичан оперативни парадокс: што је систем изолованији и сигурнији од спољних напада, он утолико постаје рањивији изнутра. Уколико безбедносне агенције преузму контролу над серверском инфраструктуром – било физичком запленом, инсталацијом

¹⁵ Терористички напад у Паризу одиграо се 13. и 14. новембра 2015. године, изведен је координисаном акцијом на шест локација у граду, са најмање 130 смртно настрадалих.

¹⁶ Graham L.: *Terrorists are using PlayStation 4 to communicate: Lawmaker*, CNBC, Nov. 16, 2015, (<https://www.cnn.com/2015/11/16/terrorists-using-playstation-4-to-communicate.html>)

софтверских пресретаца или притиском на произвођаче,¹⁷ отвара се могућност за интерну компромитацију целокупног комуникационог еко-система. Различити технички приступи у три историјски најважнија случаја продора у криптоване комуникације илуструју ову рањивост.

У случају Енкрочета (*EncroChat*) француска полиција је применила метод инфичирања одозго – уместо разбијања енкрипције сваког уређаја понаособ, компромитован је централни сервер преко којег је свим телефонима послато модификовано ажурирање софтвера (тзв. *supply chain attack*).¹⁸ У основи, радило се о малверу који је инструисао уређаје да дешифровани садржај порука директно проследи истражним органима. Код *Sky ECC*-ја је примењен директнији криптоаналитички напад на нивоу инфраструктуре система (напредна пресретања комуникационог тока, тзв. *Man-in-the-Middle*), којим је полиција пресретала кључеве за дешифровање у транзиту ка серверу.¹⁹ То је

¹⁷ Под притиском на произвођаче у контексту дигиталног надзора подразумевају се различити облици државне и законске принуде усмерене ка технолошким компанијама ради омогућавања тзв. законитог приступа (енг. *lawful access*) шифрованим подацима. Примарно, то обухвата издавање тајних судских налога за сарадњу уз забрану обавештавања јавности (енг. *gag orders*), условљавање дозвола за рад на националном тржишту постављањем локалних сервера доступних службама безбедности, као и захтеве за имплементацију намерних пропуста у коду, познатијих као задња врата (енг. *backdoors*). Као драстичан пример истиче се случај сервиса *Lavabit* (2013), чији је власник угасио компанију не пристајући да поступи по судском налогу и преда криптографске кључеве америчким властима. Према – *Lavabit email service abruptly shut down citing government interference*, *The Guardian*, (<https://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden>)

¹⁸ Richards J.: *EncroChat Hack: Why it Happened and What it Means for the EncroChat User*, REEDS, (<https://www.reeds.co.uk/insight/encrochat-hack/>)

¹⁹ Прецизни технички детаљи о методама коришћеним за разбијање енкрипције *Sky ECC* у великој мери су остали непознати. У стручној јавности се указује на неколико техничких поступака који су могли бити коришћени у спровођењу ове операције. Једна од могућности је да су истражитељи искористили већ познате слабости у инфраструктури или софтверу *Sky ECC*-ја, које су омогућиле заобилажење или пробијање енкрипције. Могуће је и да су полицијски агенти успели да инфичирају *Sky ECC* мрежу путем компромитованих уређаја или апликација, што им је омогућило директан приступ нешифрованим порукама. Не искључује се ни могућност примене софистицираних метода дешифровања, развијених у сарадњи са стручним лицима и уз подршку Европола и других међународних агенција.

Према – *What Happened to Sky ECC – The Largest Cryptophone Hack: What Went Down*, Kaymera, (<https://blog.kaymera.com/industry-news-and-articles/what-happened-to-sky-ecc>);

Goodwin B.: *Police Crack World's Largest Cryptophone Network as Criminals Swap EncroChat for Sky ECC*, Computer Weekly, March 2021, (<https://www.computerweekly.com/>)

омогућило да се у реалном времену и ретроактивно²⁰ читају стотине милиона порука. Случај разбијања ANOM-а (енг. *Operation Trojan Shield*) представља најсофистициранији облик криминалистичко-обавештајне инфилтрације у којој су ФБИ и партнерске службе примениле концепт тзв. медене замке (енг. *honeypot*)²¹ – креиравши под легендом сопствену компанију и инфраструктуру коју су у криминалном миљеу представили као апсолутно безбедну, навели су преступнике да је користе несвесни да се свака информација размењена унутар ње слива у полицијске базе.

Иако је разбијање глобалних платформи, попут *Sky ECC*-ја и Енкрочета, примарно резултат стратешких удара на серверску инфраструктуру, оперативна рањивост криптованих комуникација се не исцрпљује искључиво на том нивоу. Чак и у ситуацијама где сервери остају нетакнути, безбедност система може бити компромитована и кроз три додатна правца деловања. Први се састоји у нападу на крајњи уређај. Истражни органи располажу високоциљаним методама попут *zero-day* експлоатације, које се у основи свODE на коришћење непознатих рањивости у самом коду крипто-апликација које омогућавају компромитацију уређаја без икакве интеракције корисника.

Ипак, најефикаснији метод на овом нивоу остаје физичка заплена уређаја, чија је успешност директно условљена стањем терминала у тренутку успостављања контроле над њим. Будући да криптовани телефони поседују ригорозне антитајпер функције и механизме који аутоматски бришу или трајно закључавају меморију у случају гашења

news/252497565/Police-crack-worlds-largest-cryptophone-network-as-criminals-swap-EncroChat-for-Sky-NCC)

²⁰ Оперативни значај пробоја у централне сервере огледа се у могућности комбиновања надзора у реалном времену и ретроактивног приступа подацима. Док се класично пресретање односи на *податке у покрету/транзиту* (енг. *data in motion*), преузимање криптографских кључева омогућава истражним органима да откључају и базе података са претходно ускладиштеним порукама, познатим као подаци у мировању (енг. *data at rest*). На тај начин, компромитација *Sky ECC* платформе није резултирала само увидом у текуће планове криминалних група, већ и у комплетну историју њихових комуникација која је годинама уназад била меморисана на серверима у шифрованом облику.

²¹ Davis N.: *The FBI's Operation Trojan Shield: Infiltrating Criminal Groups through their Phones*, American University Washington, DC, August 27, 2021, (<https://www.american.edu/sis/centers/security-technology/operation-trojan-shield.cfm>)

Trojan Shield: Europol details massive organized crime sting, DW, June 8, 2021, (<https://www.dw.com/en/trojan-shield-europol-details-massive-organized-crime-sting/a-57808917>)

(енг. *reboot*) или неуспешних покушаја приступа, истражни органи имају изузетно кратак временски оквир за деловање. Од пресудног је значаја примена форензике уживо, која подразумева да уређај буде заплењен у откључаном стању (током саме употребе) или да му осумњичени омогући приступ. Уколико, пак, дође до активације заштитних механизма, подаци у радној меморији (RAM) постају трајно недоступни, чиме чак и најнапреднији алати попут оних које нуди *Cellebrite* постају бескорисни.²² Због тога се тактика хапшења корисника оваквих платформи пажљиво планира како би се уређај обезбедио пре него што дође до аутоматског ресетовања система, што представља једини сигуран пут за екстракцију дешифрованих порука и криптографских кључева директно са крајњег уређаја.

Други ниво деловања фокусира се на експлоатацију аналогног окружења уређаја, с обзиром на то да ниједан криптографски алгоритам не може заштитити информације изван самог хардвера. Применом напредних метода амбијенталног надзора, полиција може снимати сам садржај порука док се оне исписују на екрану уређаја. Истовремено, уградња звучних сензора омогућава пресретање гласовне комуникације у тренутку њеног изговарања, чиме се заобилази свака препрека дигиталне енкрипције, јер се информација прикупља у њеном изворном, аналогном облику.

Трећа могућност доласка до информација у криптованим платформама фокусира се на људски фактор и тактичку инфилтрацију. Највећа рањивост сваког затвореног система остаје сам корисник – инфилтрација прикривених иследника у комуникационе групе омогућава полицији увид у дешифровани садржај у реалном времену, без потребе за пробојем технолошке заштите. Поред тога, примена института *сарадника правде*, који предају своје уређаје и шифре органима гоњења, често служи као дигитални пут уласка у читаву мрежу саучесника.

Након падова платформи Енкрочета и *Sky ECC*-ја, амбијент криптованих комуникација постао је знатно фрагментисанији. Преступници су се окренули мањим, наизглед безбеднијим еко-системима, што потврђују резултати најновијих међународних операција – пробој

²² Sutikno T., Busthomi I.: Capabilities of Cellebrite Universal Forensics Extraction Device in mobile device forensics, *Computer Science and Information Technologies*, Vol. 5, No. 3, November 2024, p. 256.

у платформу „Дух” (*Ghost*) операцијом „Кракен” (*Kraken*) септембра 2024. године пример је успешне инфилтрације у софтверска ажурирања система,²³ док је демонтирање платформе Матрикс (*MATRIX*) у децембру исте године показало да чак и најсофистицираније мреже са десетинама дисперзованих сервера остају рањиве на координисане акције (међународних) истражних тимова.²⁴

Надзор метаподатака – задржани подаци и заштита приватности

Савремени надзор над електронским комуникацијама, с обзиром на објекат надзора, испољава се у два основна облика – први се фокусира на увид у садржину комуникације, док се други односи на прикупљање података о техничким атрибутима процеса комуницирања, без увида у њен садржај. Такви подаци добијају на значају масовном применом дигиталних уређаја који аутоматски бележе и чувају бројне пратеће референце комуникационог процеса, попут врсте комуникације, извора и одредишта, времена почетка, трајања и завршетка, идентификационих података комуникационог уређаја (нпр. *IMEI*, *IMSI*, *IP* адреса), као и његових прецизних локација у тренутку комуникације. У криминалистичкој и правној терминологији ови подаци се називају *задржаним подацима* (енг. *retained data*) или *метаподацима* (енг. *metadata*) и подједнако су релевантни како за традиционалну телефонију, тако и за уређаје који служе за комуникацију путем интернета. Из перспективе људских права, у експлоатацији задржаних података лежи највећа опасност од масовног или неселективног надзора – пракса општег задржавања метаподатака, без посебних критеријума, омогућава надлежним органима креирање детаљних профила кретања, навика и друштвених контаката појединаца. У правној теорији овај концепт је

²³ *Operation Kraken: AFP continues to uncover alleged criminality on organised crime app*, Australian Federal Police, December 2024, <https://www.afp.gov.au/news-centre/media-release/operation-kraken-afp-continues-uncover-alleged-criminality-organised>

²⁴ International investigators take down encrypted messaging service MATRIX used by criminals, Insight EU Monitoring, The Hague, 3 December 2024, https://ieu-monitoring.com/editorial/international-investigators-take-down-encrypted-messaging-service-matrix-used-by-criminals/491832?utm_source=ieu-portal

познат као теорија мозаика (енг. *Mosaic Theory*),²⁵ према којој било који појединачни, изолован *метаподатак* (нпр., једна локација или један позив) сам по себи не открива много, али њихово масовно прикупљање/кумулација и међусобно повезивање/корелација склапају целовиту слику (приватног) живота појединца.

Питању третмана задржаних података посебну пажњу је посветила Европска унија, доневши *Директиву о приватности и електронским комуникацијама* (енг. *Privacy and electronic communications directive, 2002/58/EC*)²⁶ која дефинише категорију задржаних података, док *Директива о задржавању података* (енг. *Data retention directive, 2006/24/EC*)²⁷ прописује обавезе за оператере да задржавају податке о комуникацији у периоду од шест месеци до две године. Међутим, Суд правде ЕУ је 2014. Године *Директиву о задржавању података* прогласио неважећом у случају *Дигитална права Ирске*²⁸ оценивши њене одредбе несразмерним задирањем у приватност грађана, јер масовно прикупљање података крши *Повељу ЕУ о основним правима* (енг. *Charter of Fundamental Rights of the European Union, 2000*).²⁹ Ову рестриктивну линију

²⁵ Концепт теорије мозаика, у контексту дигиталног надзора и IV амандмана на Устав САД-а, афирмисао је Врховни суд у предмету *United States v. Jones* (2012). Судија Сотомажор је у пресуди истакла да масовно прикупљање наизглед безазлених података о кретању омогућава држави да реконструише нечије политичке, религијске и сексуалне афинитете. Види – Schlabach G.: Privacy in the cloud: The mosaic theory and the stored communication act, *Stanford Law Review*, Vol. 67, No. 3, March 2015, pp. 680–686.

²⁶ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219>)

²⁷ *Data retention directive*, (<https://eur-lex.europa.eu/eli/dir/2006/24/oj/eng>)

²⁸ Организација *Дигитална права Ирске* (*Digital Rights Ireland, DRI*) тужила је ирске власти и ЕУ због закона који су обавезивали оператере да масовно и неселективно чувају податке о електронским комуникацијама свих грађана. Тврдили су да таква пракса крши основна права на приватност и заштиту података, гарантована Повељом ЕУ о основним правима. Суд правде ЕУ је поништио Директиву 2006/24/EC – последице пресуде су те да државе ЕУ више нису обавезне да масовно задржавају податке, већ морају осмислити циљане и пропорционалне мере у вези са овим питањем. Неке државе (нпр. Француска и Немачка) покушале су да уведу нове законе, али су и они касније доведени у питање због сличних проблема. Став заузет у пресуди чини основу свих каснијих одлука Суда правде ЕУ које ограничавају задржавање података и штите приватност грађана. Према – *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293>)

²⁹ *Charter of Fundamental Rights of the European Union*, (https://www.europarl.europa.eu/charter/pdf/text_en.pdf).

Суд је додатно потврдио и пооштрио у пресуди *Tele2 Sverige* (2016)³⁰, зауевши децидан став да *чак ни борба против тешког криминала не може оправдати опште и неселективно задржавање метаподатака*.

Међутим, поставља се практично питање: шта ако је у одређеним случајевима за потребе кривичног поступка или националне безбедности потребан приступ подацима из прошлости? На пример, у истрази се може јавити потреба да се провере метаподаци који се односе на лице осумњичено за терористички акт, како би се утврдили његово кретање и контакти током припремања кривичног дела. Ако такви подаци, за тај период, нису били обухваћени правилима циљаног задржавања, у смислу да је осумњичени тада већ био под циљаним надзором у вези са другим кривичним делом, они нису сачувани, па им полиција не може ретроактивно приступити јер фактички не постоје. С друге стране, они би постојали да се примењују правила неселективног чувања метаподатака. То је један од разлога зашто су многе државе ЕУ у дилеми како најбоље регулисати ову област и помирити захтеве за заштитом приватности и потребама истраге. Већина њих је на становишту да неселективно чување података не треба дозволити, осим у изузетним ситуацијама – нпр., у случају постојања озбиљне и реалне претње по националну безбедност (терористички напади, шпијунажа, оружани сукоби и сл.), држава може увести привремене мере масовног/неселективног задржавања података, које морају бити орочене, тј. усклађене са трајањем такве опасности/претње. Такође, неселективно задржавање података би могло доћи у обзир на одређеним географским подручјима на којима постоји повећана криминална активност или у односу на специфичне категорије лица, попут повратника или осумњичених за тешка кривична дела, при чему такво задржавање не би било орочено.

Као одговор на строге захтеве Суда правде ЕУ о забрани неселективног задржавања података, све чешће се афирмише механизам *хитног очувања података* (енг. *expedited preservation of data*), дефинисан чланом 16. Будимпештанске конвенције и разрађен Другим додатним

³⁰ *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*, EUR-lex (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0203>).

Анализу пресуде види – *Lynskey O.*: *Tele2 Sverige AB and Watson et al: Continuity and Radical Change*, (<https://www.europeanlawblog.eu/pub/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/release/1>)

протоколом³¹, у доктрини познат као модел *брзог замрзавања података* (енг. *quick freeze*). Предност модела брзог замрзавања је у томе што омогућава истражним органима да обезбеде дигиталне доказе пре него што они нестану, док истовремено штити приватност осталих грађана. Иако не решава проблем ретроактивног приступа подацима из периода пре него што је сумња настала, он се данас сматра најпропорционалнијим решењем које успоставља равнотежу између ефикасности истраге и заштите људских права.

Закључна разматрања и перспективе дигиталног надзора

Анализа надзора савремених комуникација имплицира да се налазимо у ери перманентног технолошког надметања између органа кривичног гоњења и софистицираних припадника криминалних миљеа. Основни закључак је да класични методи надзора, засновани на сарадњи са традиционалним телекомуникационим операторима, неповратно губе битку пред ОТТ услугама и напредним системима енкрипције.

Успеси међународних полицијских операција, попут оних усмерених на платформе *Sky ECC*, *Енкрочет* и *ANOM*, директно су проистекли из експлоатације њихове централизоване серверске архитектуре. Сервери су послужили као стратешка слаба тачка – *капија кроз коју су истражни органи успели да уђу у криптоване еко-системе*. Међутим, управо су ове истраге убрзале развијање нових модалитета криминалног прикривања. Преступници се убрзано окрећу децентрализованим комуникационим системима – попут платформе „Сесија” (*Session*) или апликација заснованих на отвореном матрикс (*Matrix*) протоколу – који функционишу без јединственог централног сервера. Коришћењем технологија *P2P* повезивања и дистрибуираних мрежа (*DApps*), подаци се фрагментишу широм глобалне мреже независних

³¹ Конвенција о високотехнолошком криминалу (позната као Будимпештанска конвенција) из 2001. године (http://www.podaci.net/_z1/2129877/Z-pkvkri03v0919.html) и Други додатни протокол уз Конвенцију о високотехнолошком криминалу о појачаној сарадњи и откривању електронских доказа из 2022. године (<https://rm.coe.int/0900001680a639fc>)

чворова (појединачних серверских тачака).³² На тај начин се онемогућава примена традиционалних института заплене централне инфраструктуре, јер подаци више не бораве на јединственој локацији, што судске налоге упућене провајдерима чини оперативно неефикасним.

Овај прелазак на тзв. *архитектуру без центра* поставља пред криминалистику нови, комплекснији изазов. У дигиталном окружењу, у ком затворени комуникациони еко-систем више нема јединствену *улазну капију* у виду централне серверске инфраструктуре, традиционалне истражне методе губе своју примарну мету, због чега се тежиште надзора у потпуности мора преусмерити на крајње уређаје и напредне методе инфилтрације. У свету децентрализованих мрежа, способност реконструкције *мозаика дигиталних доказа* не зависи од формално издате судске наредбе/налога за спровођење мере тајног надзора, упућене централном провајдеру, већ од дубинског разумевања техничке анатомије комуникационог процеса.

У том смислу, успех будућих криминалистичких истрага више неће зависити искључиво од законских оквира, већ и од оперативне способности истражитеља/криминалиста да се адаптирају на надолазеће злоупотребе информационих технологија и вештачке интелигенције. У дигиталном добу, познавање технолошких процеса и способност идентификовања кључних тачака рањивости система – од аналогног извора информације пре процеса енкрипције, преко стања података у радној меморији уређаја, па све до специфичне мрежне архитектуре – постају кључна претпоставка за успех доказног поступка.

Литература

1. Anglano, C. (2025). A review of mobile surveillanceware: Capabilities, countermeasures, and research challenges. *Electronics*, 14(1).
2. Abel, W., & Schafer, B. (2009). The German Constitutional Court on the right in confidentiality and integrity of information technology systems: A case report on BVerfG, NJW 2008, 822. *SCRIPTed*, 6(1): 106–123. <https://doi.org/10.2966/scrip.060109.106>

³² Chetry A., Sharma U.: Anonymity in decentralized apps: Study of implications for cybercrime investigations, *International Journal of Experimental Research and Review*, Vol. 32: 195–205 (2023), pp. 195–198.

3. LRQA. (n.d.). An introduction to zero-click attacks. <https://www.lrqa.com/>
4. Chetry, A., & Sharma, U. (2023). Anonymity in decentralized apps: Study of implications for cybercrime investigations. *International Journal of Experimental Research and Review*, 32, 195–205. <https://doi.org/10.52756/ijerr.2023.v32.017>
5. Davis, N. (2021, August 27). The FBI's Operation Trojan Shield: Infiltrating criminal groups through their phones. American University Washington College of Law.
6. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others & Kärntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12, ECLI:EU:C:2014:238 (Court of Justice of the European Union, April 8, 2014).
7. Duggirala, J. (2022). Demystifying end-to-end encryption: How it works in chat applications. *International Journal of Innovative Research and Creative Technology*, 8(2).
8. Elliott, B. (2021, June 8). How the FBI hacked an encrypted phone network and caught the world's most wanted criminals. ProPublica. <https://www.propublica.org/article/how-the-fbi-hacked-an-encrypted-phone-network-and-caught-the-worlds-most-wanted-criminals>
9. Ellyson, J. (2024). The use of spyware in criminal investigations: A comparative analysis of legal frameworks [Doctoral dissertation].
10. Amnesty International. (2021, July 18). Forensic methodology report: How to catch NSO Group's Pegasus. Amnesty International.
11. Europol. (n.d.). Equilibrium between security and privacy: New report on encryption. Europol.
12. Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union, Telecommunication Development Bureau.
13. Goodwin, B. (2021, March). Police crack world's largest cryptophone network as criminals swap EncroChat for Sky ECC. *Computer Weekly*.
14. Ivanović, Z. (2021). Kriminalistički aspekti visokotehnološkog kriminala. Beograd.
15. The University of Tennessee, Knoxville. (n.d.). Information security: Understanding zero-day vulnerabilities.
16. Lavabit. (n.d.). Lavabit email service abruptly shut down citing government interference. *The Guardian*.

17. Lynskey, O. (n.d.). Tele2 Sverige AB and Watson et al.: Continuity and radical change.
18. National Security Agency. (2008). Exploiting terrorist use of games & virtual environments. National Security Agency. (Objavljeno u The Guardian, December 9, 2013).
19. Okafor, F., Fagbohunmi, G., & Eneh, I. (2014). Improving the scalability of wireless sensor networks by reducing sink node isolation. *MicroWave International Journal of Science & Technology*, 7(1).
20. Europol. (n.d.). Operational Taskforce LIMIT. Europol.
21. Pisarić, M. (2022). Communications encryption as an investigative obstacle. *Journal of Criminology and Criminal Law*, 60(1).
22. Robertson, N., Cruickshank, P., & Lister, T. (2012, April 30). Document shows origins of 2006 plot for liquid bombs on planes. CNN.
23. Richards, J. (n.d.). EncroChat hack: Why it happened and what it means for the EncroChat user. REEDS.
24. Schlabach, G. (2015). Privacy in the cloud: The mosaic theory and the stored communication act. *Stanford Law Review*, 67(3), March.
25. Sommerhalder, M., et al. (Eds.). (2023). Hardware security module. U Trends in data protection and encryption technologies. Springer Nature Switzerland.
26. Sutikno, T., & Busthomi, I. (2024, November). Capabilities of Celebrite Universal Forensics Extraction Device in mobile device forensics. *Computer Science and Information Technologies*, 5(3).
27. Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others. (n.d.). EUR-Lex.
28. Thankappan, M., Rifa-Pous, H., & Garrigues, C. (2023, January). Multi-channel man-in-the-middle attacks against protected Wi-Fi networks and their attack signatures. U Proceedings of the 7th International Conference on Computer, Communication, and Signal Processing (ICCCSP), Chennai, India.
29. Duality. (n.d.). Trusted execution environment.
30. Trojan Shield: Europol details massive organized crime sting. (2021, June 8). DW.
31. Vaciago, G., & Ramalho, D. S. (2016). Online searches and online surveillance: The use of trojans and other types of malware as means of obtaining evidence in criminal proceedings. *Digital Evidence and Electronic Signature Law Review*, 13.

32. Council of Europe, European Commission for Democracy through Law (Venice Commission). (n.d.). Report on a rule of law and human rights compliant regulation of spyware.
33. Kaymera. (n.d.). What happened to Sky ECC – The largest cryptophone hack: What went down.

Surveillance of Modern Communication Technologies in Criminal Investigations

Abstract: *The paper analyzes the complex phenomenon of monitoring modern communication technologies and its significance in criminal investigations. Starting with the identification of technological challenges posed by OTT (Over-the-Top) services, the research establishes a theoretical and practical framework for surveillance by analyzing the stages of the communication process and identifying key interception points within the digital environment. Special focus is placed on online search operations and remote forensic examination of information systems, with an elaboration on legal standards and technical modalities of live forensics. The central part of the paper is dedicated to operational measures involving specially protected communication platforms, analyzing hardware device isolation and strategic vulnerabilities of server infrastructure. Furthermore, the paper critically examines the monitoring of retained data, emphasizing the importance of privacy protection in this domain. Concluding remarks point to a trend of communication decentralization aimed at evading surveillance, which imposes an imperative for investigative bodies to possess an in-depth understanding of the anatomy of digital processes as a fundamental prerequisite for the effective suppression of modern crime.*

Keywords: *communication surveillance, Over-The-Top services, online searches, encrypted platforms, Sky ECC, retained data.*