УДК 343.983.2:004.056.55
CERIF: S 149, S 160
DOI: 10.51204/Anali_PFBU_21205A

Др Милана ПИСАРИЋ*

ЕНКРИПЦИЈА МОБИЛНОГ ТЕЛЕФОНА КАО ПРЕПРЕКА ОТКРИВАЊУ И ДОКАЗИВАЊУ КРИВИЧНИХ ДЕЛА – ОСВРТ НА УПОРЕДНА РЕШЕЊА

Рачунарски подаци са доказним потенцијалом налазе се у све већем броју извора, међу којима су од посебног значаја паметни мобилни телефони. Када надлежни органи, за потребе откривања и доказивања кривичних дела, прикупљају из овог уређаја податке, потенцијалне електронске доказе, сусрећу се са више нормативних и практичних изазова, а један од отежавајућих фактора је енкрипција целог интерног складишта података. Неретко они имају одговарајуће овлашћење за остваривање приступа садржају мобилног телефона, али им недостају техничке могућности да, без поседовања кључа за декрипцију, остваре приступ и прикупе податке у читљивом облику. Иако се функција енкрипције не може и не сме занемарити у савременом дигиталном окружењу, она има опструктивно дејство на кривичну истрагу. Међутим, ову препреку надлежни органи могу превазићи применом других одговарајућих мера и радњи. У раду аутор анализира тактике и технике, односно мере и радње за остваривање приступа садржају мобилног телефона заштићеног енкрипцијом и разматра правне основе за њихову примену.

Кључне речи: *Дигитална форензика. – Електронски докази. – Мобилни телефон. – Енкрипција.*

* Асистент с докторатом, Правни факултет Универзитета у Новом Саду, Србија, *mpisaric@pf.uns.ac.rs*.

1. УВОДНА РАЗМАТРАЊА

Услед развоја технологије паметних мобилних телефона и њихове масовне употребе, корисници стварају и остављају за собом велики број трагова својих активности. Поред тога што је мобилни телефон средство за остваривање комуникације, у меморији уређаја похрањују су бројни рачунарски подаци, а поједини се чувају и на серверима пружалаца услуге складиштења података, односно „у облаку". У циљу заштите рачунарских података користе се различити механизми, а један од њих је енкрипција. Иако је неспорно да се енкрипција користи у легитимне сврхе, она погодује и извршиоцима кривичних дела.

Подаци који су садржани у мобилном телефону или се преносе његовим посредством су потенцијални (електронски) докази и могу да допринесу откривању и доказивању кривичних дела. Да би их надлежни органи прикупили за потребе кривичног поступка, користе законом одређена овлашћења, па врше увиђај или претресање мобилног телефона, наређују вештачење похрањеног садржаја или спроводе тајни надзор комуникације. Међутим, уколико су уређај или садржај похрањен у њему или подаци који се преносе у рачунарској мрежи заштићени енкрипцијом, присутне су незанемарљиве правне и техничке потешкоће. *Енкрипција отежава прикупљање електронских доказа* приликом спровођења појединих доказних радњи, па надлежни органи користе *посебне софтверске и хардверске алате* за остваривање приступа уређају, екстракцију похрањеног садржаја, односно за надзор електронске комуникације. У раду су обрађена поједина правна и техничка питања у вези са прикупљањем садржаја похрањеног у мобилном телефону у ком је примењена енкрипција целог интерног складишта података.

2. ЕНКРИПЦИЈА КАО ЗАШТИТИНИ МЕХАНИЗАМ

Енкрипција представља математички процес у ком алгоритам користи одређени кључ да би шифровао рачунарски податак, односно превео га из изворног, читљивог облика (енгл. *plain text*) у нечитљиви, неразумљиви облик (енгл. *cipher text*). Процес супротан енкрипцији је декрипција (Katz, Lindell 2015, 52). У овим процесима комплексни алго-

ритам у рачунару користи кључ да „замаскира“ и „одмаскира“ садржај.[1] У зависности од кључа, енкрипција може бити симетрична или асиметрична.[2]

Употребом енкрипције штите се рачунарски подаци који су похрањени у уређају за електронску обраду и складиштење података (енгл. *encryption at rest*) или се преносе између таквих уређаја (енгл. *encryption in transit*) (Gill, Israel, Parsons 2018, 4). Похрањени подаци се енкриптују по принципу симетричне енкрипције, на нивоу појединачне датотеке, фолдера или партиције у уређају. Уколико је енкриптован цели диск уређаја (енгл. *full disk encryption*), неовлашћено лице (лице које не поседује кључ) не може приступити похрањеном садржају у читљивом облику (јер је и сваки појединачни рачунарски податак похрањен у уређају енкриптован, односно шифрован и у потпуности нечитљив).

Почевши од 2010. произвођачи паметних мобилних телефона све чешће у драјв за складиштење података уграђују софтверске производе за енкрипцију целог интерног складишта података (Casey et al. 2011, 130). До 2014. је таква енкрипција била предвиђена као опција, а од 2014. је у уређајима са *iOS* и *Android* оперативним системом конфигурисана као фабричка поставка, заснована на 128-битном или јачем кључу (нпр. 256-битном).[3] Овакво опредељење ИТ компанија предмет је снажне осуде од стране држава. Наиме, уколико је примењена енкрипција целог интерног складишта података у паметном мобилном телефону, приликом увиђаја, претресања или вештачења уређаја не може се без поседовања кључа приступити похрањеним подацима у изворном облику. Појава да државни органи, и поред законског овлашћења немају техничке могућности да ове радње спреведу, означава се термином

[1] Алгоритам и кључ се састоје из низа битова (нула и јединица), а дужина кључа одређује јачину енкрипције – одређује колико различитих „покушаја“ је ономе, ко не поседује кључ, потребно да декриптује шифровани текст. Јачина кључа се експоненцијално повећава са сваким додатним низом битова. Тако, кључ величине једног бита генерише два могућа кључа (1 или 0), двобитни кључ генерише 2^2 могућа кључа (односно 1–1, 1-0, 0–1 или 0–0) и тако даље.

[2] Симетрична енкрипција (енгл. *symmetric encryption*), односно криптографија приватног кључа (енгл. *private-key cryptography*) је криптографски процес у ком се један те исти кључ користи и за енкрипцију и за декрипцију. Асиметрична енкрипција (енгл. *asymmetric encryption*), односно криптографија јавног кључа (енгл. *public-key cryptography*) је криптографски процес у ком се користе два различита кључа (један за енкрипцију а други за декрипцију) који су у посебној математичкој корелацији (Swire, Ahmad 2012, 425).

[3] За 128-битни кључ постоји 2^{128}, односно 340,282,366,920,938,463,463,374 ,607,431,768,211,456 могућих комбинација, док се код 256-битног кључа тај број подиже на квадрат.

„Одлазак у мрак“ (енгл. „*Going dark*“) (Писарић 2020, 1093). Међутим, иако се истиче да енкрипција представља озбиљан изазов у откривању и доказивању великог броја кривичних дела, подаци не потврђују такву тврдњу.[4] Осим тога, без кључа је тешко, али не и немогуће приступити енкриптованом уређају, јер постоје н*ачини да се овај заштитини механизам превазиђе*, односно *заобиђе*.

2.1. Лозинка и кључ

Процесе енкрипције и декрипције омогућава софтвер који се заснива на *средству за верификацију и аутентификацију приступа*: *лозинци* (енгл. *password*, *passphrase*), која представља низ алфанумеричких или симболичких карактера,[5] обрасцу (енгл. *pattern*) или одређеној биометријској карактеристици корисника (отисак прста, ретине ока и сл). Основна функција овог средства је онемогућавање приступа садржају уређаја лицу које не познаје лозинку или образац, односно не поседује/прикаже биометријске карактеристике. Чињеница да је корисник изабрао лозинку као средство за верификацију и аутентификацију приступа није уједно и знак да је уређај енкриптован – то је случај само уколико је енкрипција предвиђена као фабричка поставка или је корисник изабрао да користи енкрипцију, а криптографски систем се заснива на лозинци. Само тада, осим онемогућавања приступа неовлашћеном лицу, *лозинка има улогу и у процесу енкрипције/декрипције* – докле год је уређај закључан, истовремено је енкриптован, као и садржај похрањен

[4] Примера ради, у извештајима Окружног јавног тужилаштва у Менхетну наводи се да Тужилаштво није могло због енкрипције да изврши наредбу за претресање 111 мобилних телефона у периоду септембар 2014 – октобар 2015, односно 423 мобилна телефона током две године (у периоду септембар 2014 – октобар 2016); за првих десет месеци у 2017. од 1200 наредби за претресање мобилних телефона 700 није могло да се изврши због енкрипције; у периоду од маја до августа 2018. у форензичкој лабораторији је од 589 уређаја више од пола, тј. 366 (62%) уређаја било заштићено енкрипцијом, од чега скоро половина уређаја (165) није могла да се декриптује. Такође, тврди се да је удео енкриптованих ајфона у форензичкој лабораторији порастао је са 59.6% у 2014 на 82.2% у 2019, али се не наводи о ком броју уређаја се ради. Видети, Manhattan District Attorney's Office 2015, 9; Manhattan District Attorney's Office 2016, 8; Manhattan District Attorney's Office 2017, 5; Manhattan District Attorney's Office 2018, 2; Manhattan District Attorney's Office 2019, 4.

[5] Алфанумерички су слова A–Z и a–z и бројеви 0–9, а симболички карактери су .,+-&? итд.

у њему, а када корисник унесе лозинку и пријави се у систем, уређај се откључава, диск уређаја се декриптује и може се приступити садржају у изворном облику.

Лозинка *није исто што и кључ*, тј. не користи се директно у процесу енкрипције/декрипције (у супротном енкрипција не би имала јаку заштитну улогу), него се *кључ изводи из лозинке*, тако што се ствара најмање један тајни кључ који енкриптује кључ који енкриптује уређај. Другим речима, лозинка сама по себи није кључ за декрипцију, али уношењем лозинке декриптује се кључ за декрипцију чиме се декриптује уређај и приступа диску уређаја. Без познавања лозинке је немогуће декриптовати кључ, а без кључа је немогуће декриптовати диск уређаја. Корисник уређаја, по правилу, не зна, тј. не поседује кључ, али му је зато лозинка позната.

Иако лозинка није исто што и кључ и није та којом се енкриптује уређај, преко ње се енкриптује/декриптује кључ, па се, по добијању лозинке, она користи за откључавање мобилног телефона, односно за декрипцију кључа. Када је уређај откључан, сви подаци похрањени у њему, који су пре тога били у шифрованом, доступни су у читљивом облику (осим уколико су додатно енкриптовани применом софтвера за енкрипцију или скривени посебним техникама). Из тог разлога *надлежни органи настоје да дођу, ако не до кључа, онда до лозинке*, применом различитих тактика за остваривање приступа уређају заштићеном енкрипцијом.

2.2. Рањивости у систему енкрипције

Уколико је криптографски систем (у хардверу и/или софтверу) правилно конфигурисан, кључ се не може извести без лозинке. Међутим, уколико у систему постоје одређене грешке (багови), оне су узрок његове *рањивости* које се могу *употребити за превазилажење или заобилажење заштите* коју пружа енкрипција. Ове рањивости се експлоатишу употребом софтвера или низа команди и акција, локално на уређају (енгл. *hands-on*) или са даљине (енгл. *drive-by*),[6] а како су карактеристичне за одређену верзију уређаја и оперативног система, потребно је да се зна која је рањивост специфична за дату комбинацију хардвера и софтвера, да би се с успехом могла користити.

[6] Примера ради, тако што корисник посети малициозну или заражену веб страницу или отвори мејл са малициозним садржајем (Bellovin et al. 2014, 23).

Државни органи надлежни за откривање и доказивање кривичних дела користе рањивости криптографског система, јер њихова употреба олакшава, односно омогућава проналазак кључа/лозинке или, пак, омогућава приступ уређају и похрањеном садржају без употребе кључа/лозинке. До потребних рањивости надлежни органи долазе тако што их сами проналазе или купују на тржишту, а на располагању су им форензички алати који се заснивају на њиховој експлоатацији. Ово представља практичан изазов, јер захтева поседовање техничке експертизе за откривање и употребу рањивости, односно значајне финансијске трошкове за куповину рањивости или форензичких алата који се на њима заснивају. С тим у вези, поставља се питање да ли је вероватноћа за успех довољно велика да би се употреба таквих рањивости могла сматрати корисном и оправданом, и да ли постоји одговарајући правни оквир. Одговори на ова питања могу се дати када се сагледају предности и недостаци употребе рањивости, као технике, у различитим тактикама за остваривање приступа мобилном телефону заштићеном енкрипцијом.

3. ОСТВАРИВАЊЕ ПРИСТУПА МОБИЛНОМ ТЕЛЕФОНУ ЗАШТИЋЕНОМ ЕНКРИПЦИЈОМ

За остваривање приступа мобилном телефону у ком је примењена енкрипција целог интерног складишта података постоје две тактичке стратегије: 1) врши се напад на енкрипцију, уређај се декриптује и приступа се похрањеном садржају (стратегија *превазилажења* енкрипције), и 2) не врши се напад на енкрипцију, него се садржају похрањеном у уређају приступа на други начин (стратегија *заобилажења* енкрипције) (слично, Orin, Schneier 2018, 996). У оквиру ових стратегија користи се више тактика, од којих се неке заснивају на употреби кључа/лозинке а друге на употреби рањивости у криптографском систему. Тактике и технике за приступ енкриптованом уређају углавном произлазе из дигиталне форензике, а да би резултирале електронским доказом, морају се применити у оквиру одговарајућег овлашћења надлежних органа за предузимање појединих мера и радњи.

3.1. Превазилажење енкрипције

У стратегији превазилажења енкрипције ради остваривања приступа садржају похрањеном у мобилном телефону, у ком је примењена енкрипција целог интерног складишта података, надлежни органи настоје да употребом кључа и/или лозинке декриптују енкриптовани уређај. Ради се о следећим тактикама: а) проналазак кључа/лозинке; б) погађање кључа/лозинке; в) упућивање захтева за предају лозинке/кључа.

3.1.1. Проналазак кључа/лозинке

До *кључа* се може доћи применом *техника криптоанализе*,[7] међу којима се истиче *напад споредним каналима* (енгл. *side-channel attack*). Ове технике региструју, мере и анализирају физичке карактеристике уређаја,[8] искоришћавањем рањивости у физичкој имплементацији криптографског система уређаја. Да би се могле применити, потребно је поставити сензор у непосредној близини уређаја, који о њему прикупља информације (па и кључ[9]).

Аналогно проналаску кључа за отварање браве у физичком свету, надлежни органи током вршења увиђаја, претресања стана и других просторија или претресања лица могу пронаћи *лозинку*, која је записана (нпр. на папиру) или сачувана на други начин (нпр. у датотеци у неком другом уређају) и потом је употребити за остваривање приступа уређају. Поред тога, лозинка се може сазнати и применом одређених алата за тајни надзор над уређајем – тако што се остварује физички приступ уређају ради постављања хардверских алата, односно приступ уређају са даљине ради инсталирања софтверских алата.

---

[7] Под тим се подразумева употреба математичких правила за превазилажење криптографске заштите (National Institute of Standards and Technology 2006).

[8] Преко одговарајућих сензора могу се прикупити информације о покрету, звуцима, електромагнетним исијавањима уређаја док ради, потрошњи енергије, времену које је потребно уређају да изврши криптографски алгоритам и сл. (видети, Pfefferkorn 2017, 1395).

[9] До кључа се може доћи прикупљањем и анализом електромагнетних исијавања или звука које поизводе физичке компоненте криптографског система, односно звука који испушта процесор уређаја или анализом струјних токова између делова уређаја док се уређај енкриптује/декриптује (енгл. *key-recovery attack*). Видети, Bright 2014.

У првом случају се врши тајни, физички приступ уређају на који се потом постављају хардверске компоненте које бележе податке, но, како је њих потребно физички инсталирати на уређају и након тога преузети, постоји ризик да их корисник уочи. У другом случају се врши својеврстан упад у уређај, тако што се *са даљине* (нпр. преко вируса или тројанца) у њему инсталира софтверски алат, *који пресреће и снима поједине податке* – између осталог, куцање лозинке на тастатури, које потом шаље на рачунар надлежних органа. Овакав принцип рада није делотворан у погледу енкрипције уређаја која се заснива на лозинци, јер се може применити тек након откључавања уређаја, односно уноса лозинке, па софтвер лозинку не може ни да региструје.[10]

3.1.2. Погађање кључа/лозинке

Уколико не постоји начин да се кључ/лозинка пронађу, надлежни органи врше „*напад на силу*“ (енгл. *brute force attack*), што представља систематично испробавање различитих комбинација кључа/лозинке до проналаска праве, аналогно испробавању комбинација за отварање сефа у физичком свету. Примена ове тактике не ствара неке посебне правне проблеме.

С обзиром на то да је у тренутним технолошким оквирима напад на силу усмерен на *кључ* изузетно тежак, готово немогућ задатак,[11] овакав приступ се усмерава на *лозинку*. Успешност проналаска лозинке зависи

[10] Међутим, уколико су испуњени услови предвиђени законом, могуће је са даљине вршити претресање рачунара, без обзира на примењену енкрипцију – но, тада се ради о стратегији заобилажења енкрипције.

[11] Уколико би свако од седам милијарди људи користио десет супер-рачунара од којих би сваки тестирао милијарду комбинација за 128-битни кључ у секунди, било би потребно 77.000.000.000.000.000.000.000.000 година да се „насилно“ пронађе одговарајући кључ за декрипцију. Видети, Arora 2012. Применом неке од техника криптоанализе, које се заснивају на рањивостима у примени алгоритма за енкрипцију или самом алгоритму, могуће је смањити број покушаја који је потребан да се пронађе кључ приликом „напада на силу“. Примера ради, иако алгоритам наизглед насумично производи шифрован текст, могуће је уочити одређене обрасце за олакшано погађање кључа – користећи познате слабости у *AES*-256 алгоритму могуће је пронаћи прави кључ „испробавањем“ свега 2^{70} уместо 2^{256} комбинација. Видети, Biryukov et al. 2009. Могућност евентуалног „разбијања“ алгоритама за енкрипцију (енг. *cracking*) зависи у великој мери и од будућег развоја квантних рачунара (енгл. *quantum computers*). Видети, Gomes 2018, 42–47.

од јачине лозинке, која је одређена дужином низа[12] и врстом карактера у низу,[13] али и од техничке опремљености надлежних органа. Поједини форензички алати се заснивају на овом принципу – уређај се повезује са мобилним телефоном, и након што, понављањем покушаја са различитим комбинацијама лозинке, пронађе лозинку и оствари приступ телефону, екстахује систем датотека у потпуности.[14]

Иако сама по себи лозинка не пружа неку посебну заштиту, јер алгоритми за „погађање" лозинке у модерним рачунарима могу у неколико секунди испробати милионе комбинација лозинке, проблем представљају додатне мере заштите уграђене у мобилне телефоне: онемогућено повезивање телефона са другим хардверским компонентама,[15] ограничен број погађања, временско одлагање нових покушаја након одређеног броја неуспелих покушаја или чак брисање целокупног садржаја уређаја.[16]

[12] Примера ради, за лозинку од четири нумеричка карактера постоји 10.000 комбинација, које човек може да испроба за дан или два, а рачунар за неколико секунди.

[13] Односно, да ли се користе само нумерички или алфанумерички карактери. Бошњак и Брумен (Bošnjak, Brumen 2018, 315) указују на то да је просечна дужина низа карактера мања од осам и да се користе предвидиви обрасци у низовима, при чему корисници често користе веома просте лозинке, типа 1234 и слично. Видети, National Cyber Security Center 2019.

[14] Један од најефикаснијих форензичких алата је произвела америчка компанија Грејшифт (енг. *Grayshift*). Ради се о хардверском алату који се назива „сиви кључ" (енгл. *GrayKey*).

[15] Примера ради, испробавање комбинација лозинке на ајфону могуће је само на телефону, али не и на неком другом уређају с којим би се повезао, јер се од 2012. у хардвер уграђује јединствени идентификатор (енгл. *Unique ID*,*UID*) који онемогућава да се без уноса лозинке садржај телефона прегледа или копира на други уређај. Након појаве *GrayKey* уређаја, Епл је 2018. у оперативни систем *iOS 11.4.1* уградио *default* безбедносну ставку – тзв. *USB restricting mode*, који онемогућава да се без уноса лозинке приступи закључаном ајфону који је повезан преко *USB* порта са рачунаром и другим *plug-in* уређајима (као што је *GrayKey*) (Apple, Inc. 2020).

[16] На пример, у оперативном систему ајфона је уграђена опција која успорава рад процесора након неуспелог уноса лозинке (Apple, Inc. 2020 b). Након четири неуспела покушаја мора се сачекати један минут до новог уноса низа карактера, а након даљих неуспеха временски период у ком није могуће погађање се повећава на пет минута за шести погрешни унос, на 15 минута за седми и осми погрешни унос, и на један сат за девети. Постоји и могућност да се ајфон конфигурише тако да се сви подаци у њему избришу након десетог неуспелог уноса.

3.1.3. Упућивање захтева за предају кључа/лозинке

Уместо проналаска или погађања кључа/лозинке, надлежни органи могу да их траже од онога ко их поседује или има сазнања о њима.

Захтев за *предају кључа* упућује се *произвођачу* од кога се тражи да омогући приступ енкриптованом уређају у конкретном случају (енгл. *exceptional access*). У овој ситуацији, након што дођу у посед мобилног телефона, сазнају његов јединствени идентификациони број и прибаве потребна одобрења (нпр. наредбу о претресању уређаја), надлежни органи се обраћају произвођачу уређаја, захтевајући од њега да: а) откључа уређај који му се пошаље, б) откључа уређај са даљине, или б) надлежним органима преда кључ.

У једном тренутку је пред произвођаче био постављен захтев да приликом производње у уређај инсталирају кључ, који би се чувао у депозиту код надлежних органа, а који би их користили по потреби, међутим, од тога се одустало (тзв. „први крипто рат“).[17] Произвођач би могао да употреби, односно преда кључ и тиме омогући декрипцију уређаја и приступ похрањеним подацима под условом да кључеве за енкрипцију/декрипцију уређаја чува у депозиту,[18] што за сада није случај (тзв. „други крипто рат“[19]).

---

[17] Током деведестих година 20. века покушало се са стварањем хибридног решења који би истовремено омогућило и развој информационе технологије и способност надзирања тог развоја од стране државе. План је био да се установи систем приступа државних органа кључу за декрипцију у изузетним околностима. Тада је осмишљен стандард депоноване енкрипције (енгл. *Escrowed Encryption Standard: EES*), односно систем депоновања кључа (енгл. *key escrow*). Наиме, био је креиран сет чипова (тзв. *Clipper Chip*) који би се уграђивао у уређаје – држава би кључеве за енкрипцију дистрибуирала ИТ компанијама, а копију кључа уграђеног у сваки појединачни уређај чувала би у депозиту. На тај начин би државни органи, по потреби, имали приступ кључевима за декриптовање енкриптованих података. Овај систем је напуштен услед јаког притиска група за заштиту грађанских права и академског концензуса да се на овај начин не обезбеђује тајност комуникација. Више о томе, видети Schneier 2015.

[18] Чак и уколико би произвођач чувао кључеве и примио од надлежних органа захтев за њихову предају, поставља се питање који би мрежни протокол био коришћен за слање кључа; на који начин би захтев био аутентификован, односно како би произвођач имао потврде о идентитету за све надлежене органе широм света; на који начин би се резултати односили само за конкретан уређај, тако да се спречи да надлежни органи не траже приступ уређају који није у њиховом поседу и слично. Осим тога, то би захтевало скупе и дуготрајне промене у хардверским и софтверским компонентама уређаја.

[19] Видети фн. 24.

Захтев за предају лозинке упућује се *кориснику* уређаја, од кога се тражи да: а) открије лозинку надлежним органима, или б) унесе лозинку и преда откључан телефон, или в) употреби своје биометријске карактеристике и преда откључан телефон. Уколико поступи по захтеву надлежног органа, ради се о *добровољној декрипцији*. Међутим, поставља се питање да ли се лице може принудити да декриптује уређај, односно да ли му се могу изрећи санкције у случају одбијања да поступи по захтеву (*принудна декрипција*), нарочито ако се ради о окривљеном, с обзиром на привилегију од самооптуживања.[20] Како сматра и Терзиан (Terzian 2015, 1139), принудна декрипција је дозвољена и потребна да би се остварила равнотежа између интереса кривичног поступка и приватности корисника, јер у супротном енкрипција право надлежних органа да приступе уређају трансформише у право окривљеног да уништи доказе против себе, чинећи их неприступачним и нечитљивим. У случају постојања изричите законске одредбе, поставило се питање да ли би се санкције могле изрећи према окривљеном који тврди да му лозинка није позната, да се не сећа и слично (видети Koops 2010, 435), но, да би се окривљени могао санкционисати, нужно је да се недвосмислено утврди да он зна лозинку и да не жели да је открије или употреби.

Одговор на ова питања зависи од тога шта се од окривљеног захтева. Поједина законодавства чак садрже изричите одредбе о принудној декрипцији, на основу којих се окривљени може санкционисати уколико одбије да поступи по захтеву да преда лозинку, односно да преда откључани телефон употребом лозинке или биометријских карактеристика.

Тако, у Белгији на основу члана 88*quater* Законика о кривичној истрази[21] истражни судија или полиција може *наредити лицу*, па и *осумњиченом*, за кога се претпоставља да има сазнања о рачунарском

[20] Привилегија од самооптуживања је међународнопризнати правни стандард и представља аспект права на правично суђење, који подразумева, према ставу Европског суда за људска права (ECHR), да се окривљени не може принудити да сам себе инкриминише и преда доказе који га оптужују јер има право да се брани ћутањем (ECHR, *Saunders v. United Kingdom*, 17 December 1996.) Ова привилегија се *не односи на принудно узимање* од окривљеног предмета и узорака који постоје *независно од његове воље*, као што су узорци крви, урина и слично. Међутим, привилегија је повређена и уколико се од окривљеног тражи да сам себе оптужи тако што ће *предати инкриминишуће доказе* (нпр. исправе, као у предмету ECHR, *Chambaz v. Switzerland*, 5 April 2012).

[21] Члан је унет следећом изменом: Loi du 25 decembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code pénal, en vue d'améliorer les méthodes particulières de recherche et certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales, Moniteur Belge 17. 1 .2017

систему који је предмет истраживања или о услугама које омогућавају заштиту или шифровање података који се чувају, обрађују или преносе у том систему, да *пружи информације* о раду овог система и о томе како му приступити, односно како приступити подацима који се у систему чувају, обрађују или преносе у разумљивом облику (ст. 1). У случају да лице, па и осумњичени, *одбије* да открије лозинку, може се санкционисати казном затвора од шест месеци до три године и/или новчаном казном од 26 до 20.000 евра. Уколико одбије да поступи по захтеву у тренутку, када је могло да се спречи извршење кривичног дела или се умање његове последице, може му се изрећи казна затвора од једне до пет година и/или новчана казна од 500 до 50.000 евра. Осим тога, од лица које поседује одговарајућа сазнања (изузев осумњиченог и лица наведених у чл. 156 Закона о кривичној истрази) може се тражити да покрене систем или, у зависности од случаја, да преда, односно учини доступним релевантне податке у разумљивом облику (ст. 2), а непоступање је санкционисано у ст. 3 Белгијски Уставни суд је оценио да став 1 овог члана није у супротности са привилегијом од самооптуживања, јер се од окривљеног тражи да пружи информацију (која постоје независно од његове воље) која омогућава приступ уређају – за разлику од ситуације када би се од њега тражило да преда откључани уређај и активно учествује у прикупљању доказа против себе (видети, Cour constitutionnelle, 20 février 2020, n° 28/2020, *Rev. dr. pén.*, 2020/11, p. 1051–1057).

Члан 434–15–2 француског Кривичног законика[22] предвиђа санкционисање сваког лица, па и осумњиченог, казном затвора од три године и новчаном казном од 270.000 евра, уколико *одбије* да поступи по судској наредби *да преда лозинку или је примени ради откључавања уређаја* који је коришћен за припрему, омогућавање или извршавање кривичног дела, односно казном од пет година затвора и новчаном казном од 450.000 евра у случају да је одбијање учињено у тренутку када је оно могло да спречи извршење кривичног дела или умањи његове последице. Решавајући питање уставности овог члана и усаглашеност са правом окривљеног да ћути и сам себе не инкриминише, француски Уставни савет је 2018. заузео став да сама по себи *одредба није у супротности са привилегијом од самооптуживања*, јер њен циљ није да се од окривљеног добије признање нити садржи претпоставку кривице, него једино омогућава декрипцију уређаја и разјашњавање чињеница,

[22] Loi n° 2016–731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, Journal Officiel du 4 juin 2016.

а ради се о који постоје *независно од воље окривљеног*. Међутим, није довољно је да се у истрази недвосмислено утврди да постоји криптографски систем који је коришћен за припрему, омогућавање или извршавање кривичног дела, него и да је окривљени тога свестан и да има способност да уређај декриптује (видети, Le Conseil Constitutionnel, Décision n° 2018–696 QPC du 30 mars 2018, Journal officiel électronique authentifié n° 0076 du 31/03/2018).

У норвешки Законик о кривичном поступку је 2017. унет члан 199а који предвиђа да полиција може у току претресања уређаја за обраду података да нареди сваком лицу да преда информације потребне за остваривање приступа том уређају или *да уређај откључа преко система биометријске аутентификације*. Уколико лице одбије да поступи по таквом захтеву, полиција може по одобрењу јавног тужиоца да *изврши принудну аутентификацију*. Уколико то налажу разлози хитности, полиција може у овом смислу да примени силу на лицу места, о чему без одлагања обавештава јавног тужиоца (наведено према: Eurojust 2017, 9).

У теорији се могу наћи и другачији ставови. Тако привилегија од самооптуживања штити окривљеног само у погледу захтева да надлежним органима открије лозинку, али не и уколико се од њега тражи да надлежним органима преда откључан уређај након што унесе лозинку или да употреби своје биометријске карактеристике. Наиме, лозинка је сама по себи инкриминишућа, јер њено изношење може да доведе до евентуалног откривања инкриминишућих доказа, што би значило да се од окривљеног тражи да сведочи сам против себе у својој ствари, а што не би било у складу са принципом *nemo tenetur* (тако и Winkler 2013, 211). Без обзира на то која се аналогија користи (кључ и брава, комбинација у сефу и сл) несумњиво се ради о тајном кључу који је познат само окривљеном, а од њега се заправо тражи да против своје воље употреби садржај свог ума и открије нешто што не постоји независно од његове воље и знања, и тиме постане карика у ланцу која доводи до откривања доказа против самог себе и сопственог оптуживања (тако и Wareham 2017, 264).

Уколико, пак, надлежни органи јасно и недвосмилено утврде да уређај садржи инкриминишући садржај, и да је окривљеном лозинка позната, па од њега захтевају да је употреби, тј. унесе и преда откључан телефон, иако се од њега тражи да активно сарађује са надлежним органима, не би се могао позивати на привилегију од самооптуживања, јер се не тражи да против себе казује (да открије лозинку), него да дела на одређени начин (да унесе лозинку) (Kerr 2019, 769).

Што се тиче биометријске верификације и аутентификације, иако је ово корисницима представљено као револуционарни, најбезбеднији начин за заштиту приступа телефону, у правној реалности употреба класичне лозинке ужива већу правну заштиту. Како то Лемус (Lemus 2017, 554) уочава, отисак прста је физичка карактеристика која постоји независно од воље окривљеног и државни органи имају право да принуде окривљеног да противно својој вољи учествује у прикупљању потенцијално инкриминишућих доказа, као и приликом узимања других узорака (нпр. крви) – од окривљеног се не тражи да изнесе садржај свог ума, него да искаже ту карактеристику (стављањем прста на телефон ради откључавања). Слично образложење налази се и у иностраној судској пракси – примера ради: принудно стављање прста осумњиченог на мобилни телефон ради откључавања уређаја је дозвољено, па полиција примењује дозвољену и потребну принуду (Court of First Instance The Hague, case 09/818727–17, 12. 3. 2018, наведено према: Eurojust 2018, 12), и на тај начин се не крши *nemo tenetur* принцип, јер отисак прста постоји независно од воље осумњиченог (Court of North-Holland – criminal chamber, 14. 12. 2018, наведено према, Eurojust 2019, 8). Супротан став заузео је, примера ради, норвешки Врховни суд, одређујући да се члан 157 Законика о кривичном поступку, који уређује физички преглед и принудно узимање узорака од осумњиченог ради разјашњавања чињеница у решавању кривичне ствари, не може применити на принудно стављање прста осумњиченог у циљу откључавања и приступа његовом мобилном телефону (Supreme Court, case nr. 2016/908, 30. 8. 2016, наведено према: Eurojust 2016, 32).

3.2. Заобилажење енкрипције

У стратегији заобилажења енкрипције примењују се тактике које се не заснивају на употреби кључа/лозинке, него се приступ садржају, похрањеном у уређају који је заштићен енкрипцијом, остварује на други начин, док се механизми заштите које енкрипција пружа у потпуности игноришу. Ради се о следећим тактикама: а) остваривање приступа садржају уређаја искоришћавањем рањивости у систему енкрипције, б) остваривање приступа садржају уређаја у тренутку када је декриптован, и в) остваривање приступа копији садржаја.

3.2.1. Остваривање приступа саджају уређаја искоришћавањем рањивости у систему енкрипције

Сам по себи кључ је тешко „сломити", али уколико у систему енкрипције постоје одређене рањивости, оне се могу употребити за остваривање приступа садржају похрањеном у енкриптованом уређају, чак и без поседовања кључа. До оваквих рањивости се долази на два начина: претходним, намерним уграђивањем у систем или проналаском и експлоатацијом постојећих рањивости.

У првом случају ради се о тзв. „уласку на задња врата" (енгл. *backdoors*). Током деведесетих година 20. века поједине државе су без успеха покушале да произвођаче софтвера за енкрипцију и уређаја принуде да усвоје техничке услове који би омогућили „улазак на задња врата", а слични захтеви постоје и данас – догађај са краја 2015.[23] је окидач за поновно покретање дебате око енкрипције која још увек траје у политичкој, научној и стручној јавности.[24] И поред тога што

[23] Након што је одузела мобилни телефон марке *iPhone 5C* децембра 2015, иако овлашћена наредбом за претресање, полиција није могла да приступи садржају енкриптованог мобилног телефона марке ајфон, јер није могла да „погоди" лозинку за откључавање, без опасности да се ти садржаји бесповратно изгубе. Ово из разлога што је у оперативном систему уређаја била уграђена опција самобрисања (енгл. *auto-erase*), услед које су сви подаци могли да буду избрисани након одређеног броја неуспелих покушаја да се погоди лозинка за приступ, чим је онемогућено вршење „напада на силу". Судском наредбом Еплу је наложено да пружи техничку помоћ полицији отклањањем овакве заштите из оперативног система, чиме би се омогућио неограничен број погађања лозинке, без да се подаци избришу са телефона, на који начин би полиција добила могућност изузетног приступа садржају енкриптованог уређаја. Компанија је одбила да поступи по наредби, образалажући свој став потребом да се заштити сигурност свих корисника, јер би наводно било немогуће да се само за један уређај учини овакав изузетак, а да се не угрози безбедност оперативног система и тиме омогући неовлашћени приступ уређајима свих других корисника. Спор између Епла и ФБИ јер је компанија одбијала да декриптује енкрипцијом заштићени ајфон није резултурао коначном судском одлуком, јер је полиција повукла свој захтев, након што је успела да откључа телефон.

[24] Ова дебата се означава Другим крипто ратом. Тако је на састанку министара Уједињеног Краљевства, САД, Канаде, Аустралије и Новог Зеланда 2018. изнето је опредељење ових држава ка стварању правног оквира за обавезивање ИТ компанија да прилагоде постојеће, односно усвоје нове техничке услове који би омогућили да надлежни државни органи могу да остваре приступ енкриптованим уређајима. Видети, Five Country Ministerial, 2018. Иначе, Аустралија је прва држава која је усвојила такав пропис – Закон о помоћи и приступу из 2018. (Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, No. 148, 2018). На основу овог закона надлежни државни органи у случају потребе да се приступи уређају

су захтеви надлежних органа легитимни, у стручној јавности (Abelson et al. 2015, 18–20) је присутан концензус да је са техничке стране немогуће енкрипцију ослабити само мало, без да се остави простор за потенцијале рањивости у целокупном систему енкрипције.

У другом случају надлежни органи, упркос енкрипцији, остварују приступ уређају и *екстрахују садржај*, користећи рањивости у постојећим системима, које проналазе сами или их купују на тржишту. Осим тога, надлежним органима су на располагању бројни алати који се заснивају на откривеним а непревазиђеним рањивостима у софтверским и хардверским компонентама мобилних телефона, а који омогућавају екстракцију података из уређаја заштићених енкрипцијом.[25] Перформансе ових алата за се јасно виде из годишњих извештаја Програма за тестирање алата за дигиталну форензику америчког Националног института за стандарде и технологију – према последњим извештајима, и поред енкрипције и додатних мера заштите, постоје алати који екстрахују готово све податке из закључаних, енкриптованих уређаја и инсталираних апликација (видети, National Institute of Standards and Technology 2019). Ови подаци су значајни јер показују да, упркос тврдњама да енкрипција представља незанемарљиву препреку за рад надлежних орагана, форензички алати који функционишу по стандардима дигиталне форензике ипак омогућавају прикупљање података из енкриптованог уређаја. Међутим, да би њихова употреба

заштићеном енкрипцијом могу да захтевају од компанија (који су произвођачи уређаја, креаори софтвера за енкрипцију, пружаоци услуга електронских комуникација, приступа интернету, чувања података у облаку) да пруже техничку помоћ (енгл. *technical assistance notice*), па и да створе могућност уласка на задња врата (енгл. *technical capability notice*). Слично томе, у САД је почетком 2020. у законодавну процедуру пред америчким Сенатом унет предлог закона којим би се ИТ компанија обавезале да ограниче употребу енкрипције (*The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act: EARN IT Act*), међутим, пропис још увек није усвојен.

До скоро је на нивоу ЕУ било присутно јасно и недвосмислено противљење озакоњењу „уласка на задња врата“, међутим, све се више говори о стварању одговарајућег правног инструмента који би омогућио таргетиран приступ подацима упркос енкрипцији (Pisarić 2020, 615). У резолуцији из новембра 2020 Савет ЕУ истиче да се надлежни органи у великој мери у истрази великог број акривилних дела ослањају на преретање комуницира које је технички неизводљиво због енкрипције а да не постоји одговарајући супституит за ову радњу. Због тога се мора наћи одговарајући правни инструмент примењив у тренутном техничком окружењу – другим речима да се ИТ обавеже да омогући таргетиран приступ подацима упркос енкрипцији. Видети, Council of the European Union, 2020.

[25] Међу тим алатима се истичу производи израелске фирме Селебрит (енг. *Cellebrite*), првенствено *Universal Forensic Extraction Device: UFED Premium*.

резултирала електронским доказима, морају бити испуњени услови прописани за претресање и вештачење мобилног телефона и поштована ограничења утврђена у наредби за претресање, односно вештачење (Писарић 2019, 208).

3.2.2. Остваривање приступа садржају уређаја у тренутку када је декриптован

Како је цео диск енкриптован само док је уређај закључан, кроз ову тактику се настоји да се уређају приступи у моменту када га енкрипција не штити, односно када је откључан. Наиме, када корисник унесе средство за аутентификацију и верификацију, уређај се откључава и декриптује, а лозинка се чува у привременој (RAM) меморији, докле год је уређај укључен и откључан. То значи да се преузимањем контроле над уређајем у тим околностима омогућава приступ похрањеном садржају у изворном облику, па и лозинци (која се на тај начин може сазнати и накнадно користити). Овакав приступ остварује се кроз физичку контролу над уређајем или са даљине.

У првом случају, да би се заобишао заштитини механизам, надлежни органи настоје да, након претходног планирања,[26] најпре остваре *физичку контролу над уређајем* у моменту док је откучан,[27] а затим на лицу места спроведу дигиталну истрагу на „живом" систему,[28] уколико су за то постоји одговарајући правни оквир (Писарић 2019, 131).

---

[26] Кејси и сарадници (Casey et al. 2011, 134) тврде да је за успех ове тактике неопходно претходно планско прикупљање података о техничкој софистицираности корисника, месту и времену употребе уређаја, физичким карактеристикама локације на којој ће преузети контрола над уређајем, оперативном систему и хардверској конфигурацији уређаја, евентуалним додатним мерама заштите у уређају, врсти енкрипције и сл. Ови подаци су потебни како би се створила стратегија деловања, тако да се повећа фактор изненађења и смањи могућност да се уређај искључи или оштети.

[27] Примера ради, полиција је након вишегодишње истраге незаконитих активности на црном тржишту даркнета, Пут свиле, дошла до рачунара његовог оснивача управо применом ове тактике. Из претходно прикупљених података произашло је да он користи рачунар у градској библиотеци, па су два службена лица у цивилу исценирала дистракцију, а трећи је одузео рачунар који је био откључан и декриптован. На тај начин је превазиђен проблем енкрипције целог диска, а оснивач Пута свиле је осуђен на доживотну казну затвора. Видети, Mullin 2015.

[28] Стандардно поступање у случају сумње на енкрипцију целог диска је да се из *RAM* меморије уређаја прикупљају непостојани подаци (енгл. *volatile data*), међу којима су од нарочите важности лозинка и други подаци потребни за отваривање приступа енкриптованим садржајима, пре него што се уређај пренесе у форензичку лабораторију (Pisarić 2015, 243).

У другом случају остварује се приступ уређају са даљине, односно спроводи се *даљинско претресање декриптованог уређаја у реалном времену*. Другим речима, надлежни органи предузимају својеврсно хаковање, како би за потребе кривичног поступка остварили приступ подацима похрањеним у уређају заштићеном енкрипцијом. „Хаковање" се врши применом малициозног софтвера (малвера), који се инсталира у уређај (остваривањем тајног, физичког приступа уређају) или са даљине, а успешност ове тактике зависи од техничких могућности надлежних органа.[29]

Како се кроз даљинско претресање уређаја угрожава приватност корисника и безбедност уређаја компромитовањем поузданости и интегритета система енкрипције, примена ове тактике је оправдана само под условом да постоји одговарајући правни основ за предузимање ове радње, која је неопходна за остваривање легитимног циља, а да је ограничење људских права потребно и сразмерно остварењу тог циља (Office of the United Nations High Commissioner for Human Rights 2018, 6). Другим речима, само ако је претресање уређаја са даљине изричито уређено законом као посебна доказна радња, чија примена би била ограничена на нарочито тешка кривична дела, под условом да не постоје блаже мере за остаривања циља (Hennessey 2016), чиме би били испоштовани принципи легалитета, сразмерности и супсидијарности.

Изричите законске одредбе о даљинском претресању уређаја постоје у свега неколико држава. Тако немачки Законик о кривичном поступку[30] у члану *100b* регулише тајно претресање уређаја и прикупљање похрањеног садржаја са даљине. Радња се може одредити наредбом суда само према лицу за које постоји основана сумња да је извршио неко од нарочито тешких, таксативно набројаних кривичних дела (односно да је покушао извршење, уколико је покушај кажњив), под условом да је утврђивање чињеница или лоцирање осумњиченог знатно теже или немогуће спровођењем других радњи. Белгијски Законик о кривичној истрази у члану *90ter* предвиђа да истражни судија може наредити да се тајно, уз помоћ техничких средстава, изврши даљинско претресање уређаја које користи лице осумњичено за неко од таксативно набројаних кривичних дела, и то само у изузетним случајевима, уколико то захтевају интереси истраге а потребне чињенице се не могу утврдити на други начин. Судија у наредби може одредити и тајни ула-

[29] Подаци о алатима који се користе у ову сврху нису доступни јавности.

[30] Strafprozeßordnung In der Fassung der Bekanntmachung vom 7. 4. 1987 (BGBl. I S. 1074, ber. S. 1319) zuletzt geändert durch Gesetz vom 30. 3. 2021 (BGBl. I S. 448) m.W.v. 2. 4. 2021.

зак у дом или други простор у ком се уређај налази, примену техничких средстава у циљу заобилажења мера заштите и инсталирање техничких средстава за декрипцију уређаја. Члан *588 septies* шпанског Законика о кривичном поступку[31] предвиђа да, уколико постоји сумња да је лице извршило неко од кривичних дела из набројаних група тешких кривичних дела, судија може наредити инсталирање софтвера којим се спроводи даљински електронски надзор уређаја, првобитно на месец дана, с могућношћу продужења до три месеца

Поред одговарајућег правног оквира, нужно је да се алати који омогућавају даљински приступ и претресање, развијају и тестирају у складу са стандардизованим правилима, како не би компромитовали информациону безбедност, нарушили интегритет електронских доказа, нити омогућили несразмерно и неселективно прикупљање података.

3.2.3. Остваривање приступа копији садржаја

Уколико су подаци садржани у енкриптованом телефону истовремено похрањени на серверу пружаоца услуге складиштења података (односно као бекап „у облаку“) надлежни органи могу да упуте захтев пружаоцу услуге да те податке преда. Наиме, као што се, уместо остваривања увида у мејлове похрањене у енкриптованом уређају, тражи од пружаоца услуга електронских комуникација да преда копију мејлова, тако се, уместо покушаја декрипције мобилног телефона, захтева од пружаоца услуге складиштења података „у облаку“ да преда бекап копију садржаја мобилног телефона која се чува на његовом серверу.

Након што се утврди да се корисник мобилног телефона определио за бекаповање похрањеног садржаја и да таква копија постоји „у облаку“, [32] да би се ова тактика могла применити потребно је да надлежни

[31] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal, „BOE“ núm. 260, de 17/09/1882 – одредба је у Законик унета 2015, кроз Capítulo IX del Título VIII del Libro II introducido por el apartado dieciocho del artículo único de la L.O. 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica („B.O.E.“ 6 octubre).

[32] Корисници ајфона имају на располагању могућност да садржај телефона похране као бекап у „облаку“ на ајклауд платформи (енгл. *iCloud*), којој се приступа преко посебног налога (*@icloud.com*, *@me.com и @mac.com*). У андроид телефонима се са првом пријавом на Гугл налог (преко ɥимејл адресе) врши бекаповање подешавања телефона и синхронизовање контаката, обележива-

органи имају одговарајуће овлашћење да захтевају предају копије.[33] Пружалац услуге би могао да поступи по оваквом захтеву под условом да такви подаци постоје у конкретном случају, а фактичка могућност зависи од тога да ли су копије садржаја „у облаку" похрањене у *plaintext* или у шифрованом облику (у ком случају могућност пружаоца услуге да их преда надлежним органима у читљивом облику зависи од врсте енкрипције која је примењена[34]).

Адекватност копије да буде замена за садржај похрањен у енкриптованом мобилном телефону зависи од тога који садржај се бекапује и колико је времена прошло од последњег бекапа. Иако бекап садржаја мобилног телефона обухвата обиље података који могу бити од користи за надлежне органе, ипак се, и то у најбољем случају, „у облаку" не чувају сви подаци који су иначе похрањени у уређају, па је због тога „облак" само алтернатива а не супститут остваривању приступа енкриптованом мобилном телефону.

ча страница, лозинки и др, а након тога се аутоматски (докле год корисник не искључи ту опцију) бекапују одређени садржаји на Гугловим серверима за складиштење података „у облаку" (нпр. фотографије се бекапују у *Google Photos*, а поруке, датотеке и фолдери у *Google Drive*). Корисници мобилног телефона могу да изаберу да се бекап садржаја у уређају уопште не ствара и не чува ни на једном серверу.

[33] Орган поступка може да захтева остваривање увида у садржај похрањен на ајклауд платформи уколико постоји судска наредба, а потребно је да се наведе одговарајући *Apple ID* или адреса мејл налога, а уколико су непознати, пуно име и број телефона или физичка адреса корисника како би се идентификовао. Видети, Apple, Inc. 2020d. За надлежне државне органе ван САД важе иста правила, с тим да се захтев упућује у оквиру механизма за пружање међународне правне помоћи у кривичним стварима. Видети, Apple, Inc. 2020e. Од Гугла се у оквиру одговарајућих процедура може захтевати да преда податке бекаповане на његовим серверима. Видети, Google 2021.

[34] Бекап на Гугловим серверима је заштићен енкрипцијом а кључ се изводи из корисникове лозинке за Гугл налог (за поједине податке се изводи из лозинке за мобилни телефон), при чему ни Гугл не поседује кључ, па не може предати надлежним органима копију садржаја која се чува „у облаку". Видети, Google 2020. Садржај у ајклауд платформи је енкриптован локално на серверу, 128-битним *AES* алгоритмом, али Епл поседује кључ за декрипцију, па те податке може предати надлежним органима. Уколико се, пак, подаци чувају на платформи треће стране (нпр. *Amazon Web Services* или *Google Cloud Platform*), Епл кључ не поседује. Поједини подаци (нпр. подаци о здрављу, плаћању, лозинке за *Wi-Fi* мрежу) заштићени су *end-to-end* енкрипцијом, а кључ се изводи из лозинке коју само корисник зна, тако да ни Епл нема приступ овим подацима у изворном облику. Видети, Apple, Inc. 2020c.

4. ЗАКЉУЧАК

То што енкрипција целог интерног складишта података у мобилном телефону представља препреку у истрази, нарочито тешких кривичних дела, не би се смело користити се као аргумент против ње. Тврди се да се проблем „одласка у мрак“ може превазићи једино обавезивањем произвођача уређаја, твораца софтвера и пружалаца услуга складиштења података „у облаку“ да ослабе енкрипцију у уређајима, апликацијама и услугама, односно да задрже техничку способност да поступе по захтеву надлежних органа за остваривање приступа декриптованим садржајима, тј. да омогуће „улазак на задња врата“. Овакав захтев поставља пред компаније безбедносне, економске и техничке изазове и неприхватљив је, јер не постоји начин да се енкрипција ослаби и заобиђе за једног корисника/уређај а да се не угрози целокупан систем енкрипције. Поред тога, захтев није ни оправдан – без обзира на то што енкрипција представља препреку у истрази, она није непремостива, јер постоје други начини да се приступи подацима похрањеним у енкриптованом уређају.

У оквиру стратегије превазилажења енкрипције, тактика проналаска кључа/лозинке може дати успеха чак и применом класичних криминалистичких тактика и техника, што зависи од околности конкретног случаја. Успешност тактике погађања кључа/лозинке је условљена техничким могућностима надлежних органа, односно применом форензичких алата који се заснивају на „нападу на силу“ или применом техника криптоанализе. У погледу упућивања захтева окривљеном за предају лозинке, њега штити привилегија од самооптуживања уколико се од њега тражи да открије садржај свог ума и искаже лозинку, али не и уколико се од њега захтева да преда уређај откључан након уноса лозинке или биометријске карактеристике јер оне постоје независно од његове воље. Искоришћавање постојећих рањивости у систему енкрипције се своди на употребу одговарајућих форензичких алата за екстракцију података и примењује се уколико су испуњени законски услови за претресање и вештачење мобилног телефона, уз поштовање ограничења утврђених у наредби за претресање, односно наредби за вештачење, а успех у примени тактике зависи од техничке опремљености надлежних органа. Постоје стандардизовни форензички алати који су подобни за екстракцију садржаја из енкриптованих мобилних телефона, што показују резултати о њиховом тестирању. Остваривање приступа уређају са даљине у моменту док је декриптован представља својеврсно хаковање, па је нужно да је изричито предвиђено и уређено законом као посебна доказна радња, нарочито уз поштовање принципа легалитета, сразмерности и супсидијарности.

Успешност упућивања захтева пружаоцу услуга складиштења података „у облаку“ да преда копију садржаја мобилног телефона зависи од тога да ли се и који подаци складиште на њиховом серверу, да ли су и којом врстом енкрипције заштићени на серверу, односно да ли их пружаоци услуге могу надлежним органима предати.

Приказане тактике и технике нису идеално решење за превазилажење проблема енкрипције, ни у правном ни у техничком смислу. Неке од њих захтевају значајна финансијска средстава и стручност, док су друге упитне са становишта безедности информационих система, с једне стране, и заштите права корисника, а нарочито права окривљеног, с друге стране. Међутим, њихов значај се огледа у томе што показују да ипак постоје начини да се проблем енкрипције макар донекле превазиђе. Очигледно је да је, и поред и упркос енкрипцији, претресање и вештачење мобилног телефона могуће извршити, кроз употребу одговарајућих алата, уз помоћ којих се врши екстракција података из уређаја у складу са принципима дигиталне форензике, а све у постојећим правним оквирима, а да обавезивање компанија да ослабе енкрипцију или проширивање овлашћења надлежних органа није оправдано а тиме ни неопходно.

ЛИТЕРАТУРА

[1] Abelson, Harold, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner. 2015. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. Cambridge.

[2] Arora, Mohit. 2012. How Secure Is AES Against Brute Force Attacks? *EE Times*. July 5. *http://www.eetimes.com/document.asp*, последњи приступ 14. јула 2020.

[3] Bellovin, Steven, Matt Blaze, Sandy Clark, Susan Landau. 1/2014, Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet. *Northwestern Journal of Technology and Intellectual Property* 12: 1–64.

[4] Biryukov, Alex, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, Adi Shamir. 2009. Key Recovery Attacks of Practical Complexity on AES Variants with up to 10 Rounds. 299–319. u *Advances in Cryptology – EUROCRYPT 2010*, ed. Henri Gilbert. Berlin, Heidelberg: Springer.

[5] Bošnjak, Leon, Boštjan Brumen. 1/2018. Rejecting the Death of Passwords: Advice for the Future. *Computer Science and Information Systems* 16: 313–332.

[6] Casey, Eoghan, Geoff Fellows, Matthew Geiger, Gerasimos Stellatos. 2/2011.The growing impact of full disk encryption on digital forensics. *Digital Investigation* 8: 129–134.

[7] Gill, Lex, Tamir Israel, Christopher Parsons. 2018. *Citizen Lab and the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic: Shining a Light on the Encryption Debate: a Canadian Field Guide*. Toronto.

[8] Gomes, Lee. 4/2018. Quantum computing: Both here and not here. *IEEE Spectrum*: 42–47.

[9] Hennessey, Susan. 2016. Lawful hacking and the case for a strategic approach to Going Dark. *Brookings*. October 7. *https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/*, последњи приступ 16. јула 2020.

[10] Jonathan, Katz, Yehuda Lindell. 2015. *Introduction to modern cryptography*, 2nd Edition. London.

[11] Kerr, Orin, Bruce Schneier. 4/2018. Encryption Workarounds. *Georgetown Law Journal* 106: 989–1019.

[12] Kerr, Orin. 4/2019. Compelled Decryption and the Privilege Against Self-Incrimination. *Texas Law Review* 97: 767–799.

[13] Koops, Bert-Jaaps. 2010. Commanding decryption and the privilege against self-incrimination. 431–445. *New trends in criminal investigation and evidence: Volume II*, eds. C. M. Breur, M. M. Kommer, J. F. Nijboer, J. M. Reijntjes. Antwerpen-Groningen-Oxford: Intersentia.

[14] Lemus, Efren. 2/2017. When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones. *SMU Law Review* 70: 533–561.

[15] Pisarić, Milana. 2015. Challenges of Recovering and Analyzing Volatile Data. *Thematic Conference Proceedings of International Significance Archibald Reiss Days* 3: 241–245.

[16] Писарић, Милана. 2019. *Електронски докази у кривичном поступку*. Нови Сад.

[17] Писарић, Милана. 3/2020. Енкрипција као препрека откривању и доказивању кривичних дела. *Зборник радова Правног факултета у Новом Саду* 54: 1079–1100.

[18] Pisarić, Milana. 2020. Encryption as a challenge for European law enforcement agencies. *Thematic Conference Proceedings of International Significance Archibald Reiss Days* 10: 611–619.

[19] Pfefferkorn, Riana. 5/2017. Everything Radiates: Does the Fourth Amendment Regulate Side-Channel Cryptanalysis?. *Connecticut Law Review* 49: 1393–1452.

[20] Schneier, Bruce. 2015. History of the First Crypto War. *Schneier Blog*. *https://www.schneier.com/blog/archives/2015/06/history_of_the_.html*, последњи приступ 14. јула 2020.

[21] Swire, Peter, Kenesa Ahmad. 1/2012. Encryption and Globalization. *Columbia Science and Technology Law Review* 13: 416–481.

[22] Terzian, Dan. 4/2015. Forced Decryption as Equilibrium— why it's Constitutional and how Riley Matters. *Northwestern University Law Review* 109: 1131–1140.

[23] Wareham, Jason. 3/2017. Cracking the Code: The Enigma of the Selfincrimination Clause and Compulsory Decryption of Encrypted Media. *Georgetown Law Technology Review* 1: 247–268.

[24] Winkler, Andrew. 2/2013. Password Protection and Self-Incrimination: Applying the Fifth Amendment Privilege in the Technological Era. *Rutgers Computers and Technology Law Journal* 39: 194–215.

ОСТАЛИ ИЗВОРИ

[1] Apple, Inc. 2020a. *Using USB accessories with iOS 11.4.1 and later*. April 15. *https://support.apple.com/en-us/HT208857*, последњи приступ 31. маја 2021.

[2] Apple, Inc. 2020b. *Apple Platform Security*. *https://support.apple.com/guide/security/passcodes-sec20230a10d/web*, последњи приступ 31. маја 2021.

[3] Apple, Inc. 2020c. *iCloud security overview*. *https://support.apple.com/en-us/HT202303#:~:text=Data%20security,end%2Dto%2Dend%20encryption*, последњи приступ 31. маја 2021.

[4] Apple, Inc. 2020d. *Legal Process Guidelines Government & Law Enforcement outside the United States. https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf*, последњи приступ 31. маја 2021.

[5] Apple, Inc. 2020e. *Legal Process Guidelines: U. S. Law Enforcement*. *https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf*, последњи приступ 31. маја 2021.

[6] Bright, Peter. 2014. Stealing Encryption Keys Through the Power of Touch. *Ars Technica.* August 21. *http://arstechnica.com/security/2014/08/stealing-encryption-keys-through-the-power-of-touch/*, последњи приступ 31. маја 2021.

[7] Council of the European Union. 2020. *Resolution on Encryption – Security through encryption and security despite encryption*. 24 November 2020. *https://data.consilium.europa.eu/doc/document/ST-13084–2020-REV-1/en/pdf*, последњи приступ 31. маја 2021.

[8] Eurojust. 2019*. Cybercrime Judicial Monitor – Issue 5*. *https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2019–12_CJM-5_EN.pdf*, последњи приступ 31. маја 2021.

[9] Eurojust. 2018*. Cybercrime Judicial Monitor – Issue 4. https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2018–12_CJM-4_EN.pdf*, последњи приступ 31. маја 2021.

[10] Eurojust. 2017. *Cybercrime Judicial Monitor – Issue 3*. *https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2017–12_CJM-3_EN.pdf*, последњи приступ 31. маја 2021.

[11] Eurojust. 2016. *Cybercrime Judicial Monitor – Issue 2*. *https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/2016–11_CJM-2_EN.pdf*, последњи приступ 31. маја 2021.

[12] Five Country Ministerial. 2018. *Statement of Principles on Access to Evidence and Encryption*. *https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018*, последњи приступ 31. маја 2021.

[13] Google. 2021. *Transparency Report Help Center, Request for User Information*. *https://support.google.com/transparencyreport/answer/7381458?hl=en*, последњи приступ 31. маја 2021.

[14] Manhattan District Attorney's Office. 2015. *Report on Smartphone encryption and Public safety*. New York. *https://www.manhattanda.org/wp-content/themes/dany/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf*, последњи приступ 31. маја 2021.

[15] Manhattan District Attorney's Office. 2016. *Report on Smartphone encryption and Public safety*, *An update to the November 2015 Report.* New York. *https://www.manhattanda.org/wp-content/themes/dany/files/Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety:%20An%20Update.pdf*, последњи приступ 31. маја 2021.

[16] Manhattan District Attorney's Office. 2017. *Third Report on Smartphone encryption and Public safety*. New York. *https://www.manhattanda.org/wp-content/themes/dany/files/2017%20Report%20of%20the%20Manhattan%20District%20Attorney%27s%20Office%20on%20Smartphone%20Encryption.pdf*, последњи приступ 31. маја 2021.

[17] Manhattan District Attorney's Office. 2018. *Report on Smartphone encryption and Public safety, An update to the November 2017 Report*. New York. *https://www.manhattanda.org/wp-content/uploads/2018/11/2018-Report-of-the-Manhattan-District-Attorney27s-Office-on-Smartphone-En....pdf*, последњи приступ 31. маја 2021.

[18] Manhattan District Attorney's Office. 2019. *Report on Smartphone encryption and Public safety, An update to the November 2018 Report*. New York. *https://www.manhattanda.org/wp-content/uploads/2019/10/2019-Report-on-Smartphone-Encryption-and-Public-Safety.pdf*, последњи приступ 31. маја 2021.

[19] Mullin, Joe. 2015. Sunk: How Ross Ulbricht ended up in prison for life. *Ars Technica.* May 29. *https://arstechnica.com/tech-policy/2015/05/sunk-how-ross-ulbricht-ended-up-in-prison-for-life/*, последњи приступ 31. маја 2021.

[20] National Cyber Security Center. 2019. *Most hacked passwords revealed as UK cyber survey exposes gaps in online security*. April 21. *https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security*, последњи приступ 31. маја 2021.

[21] National Institute of Standards and Technology. 2006. *Glossary of Key Information Security Terms*. April 25. *https://www.govinfo.gov/content/pkg/GOVPUB-C13-b1ff2496095efdbb0a71d72f6b607595/pdf/GOVPUB-C13-b1ff2496095efdbb0a71d72f6b607595.pdf*, последњи приступ 31. маја 2021.

[22] National Institute of Standards and Technology. 2019. *Test Result for Mobile Device Acqusition Tool: UFED InField Kiosk v7.5.0.875*. September 27. *https://www.dhs.gov/sites/default/files/publications/testresultsnistmobiledeviceacquisitiontool-ufedinfieldkiosk_v7.5.0.875.pdf*, последњи приступ 31. маја 2021.

[23] Office of the United Nations High Commissioner for Human Rights. 2018. *Report of the United Nations High Commissioner for Human Rights*: *The Right to Privacy in the Digital Age*, *https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement*, последњи приступ 31. маја 2021.

Milana PISARIĆ, PhD

Assistant Lecturer, University of Novi Sad Faculty of Law, Serbia

MOBILE PHONE ENCRYPTION AS AN OBSTACLE IN CRIMINAL INVESTIGATION – REVIEW OF COMPARATIVE SOLUTIONS

Summary

In detecting criminal offences, the police increasingly rely on electronic evidence. Due to ubiquitous digitization, data in electronic form with probative potential is found in an increasing number of sources. When the competent authorities need to collect potential electronic evidence from mobile phones, they face several normative and practical challenges. One of the important aggravating factors is the full-disk encryption of the device. Although functions of encryption cannot and must not be neglected in the modern digital environment, it has an obstructive role in criminal investigation. The competent authorities often have the appropriate authority to access the contents of a mobile phone, but they lack the technical ability to gain such access and collect data. After explaining the basic principles of encryption of mobile phones, the author analyzes the possible approaches for gaining access to a device protected by encryption, and indicates the possible legal basis for their application.

Key words: *Digital investigation. – Electronic evidence. – Mobile phones. – Encryption.*

Article History:
Received: 21. 7. 2020.
Accepted: 8. 6. 2021.