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

Dr Milana PISARIĆ*

ENKRIPCIJA MOBILNOG TELEFONA KAO PREPREKA OTKRIVANJU I DOKAZIVANJU KRIVIČNIH DELA – OSVRT NA UPOREDNA REŠENJA

Računarski podaci sa dokaznim potencijalom nalaze se u sve većem broju izvora, među kojima su od posebnog značaja pametni mobilni telefoni. Kada nadležni organi, za potrebe otkrivanja i dokazivanja krivičnih dela, prikupljaju iz ovog uređaja podatke, potencijalne elektronske dokaze, susreću se sa više normativnih i praktičnih izazova, a jedan od otežavajućih faktora je enkripcija celog internog skladišta podataka. Neretko oni imaju odgovarajuće ovlašćenje za ostvarivanje pristupa sadržaju mobilnog telefona, ali im nedostaju tehničke mogućnosti da, bez posedovanja ključa za dekripciju, ostvare pristup i prikupe podatke u čitljivom obliku. Iako se funkcija enkripcije ne može i ne sme zanemariti u savremenom digitalnom okruženju, ona ima opstruktivno dejstvo na krivičnu istragu. Međutim, ovu prepreku nadležni organi mogu prevazići primenom drugih odgovarajućih mera i radnji. U radu autor analizira taktike i tehnike, odnosno mere i radnje za ostvarivanje pristupa sadržaju mobilnog telefona zaštićenog enkripcijom i razmatra pravne osnove za njihovu primenu.

Ključne reči: *Digitalna forenzika. – Elektronski dokazi. – Mobilni telefon. – Enkripcija.*

* Asistent s doktoratom, Pravni fakultet Univerziteta u Novom Sadu, Srbija, *mpisaric@pf.uns.ac.rs*.

1. UVODNA RAZMATRANJA

Usled razvoja tehnologije pametnih mobilnih telefona i njihove masovne upotrebe, korisnici stvaraju i ostavljaju za sobom veliki broj tragova svojih aktivnosti. Pored toga što je mobilni telefon sredstvo za ostvarivanje komunikacije, u memoriji uređaja pohranjuju su brojni računarski podaci, a pojedini se čuvaju i na serverima pružalaca usluge skladištenja podataka, odnosno „u oblaku". U cilju zaštite računarskih podataka koriste se različiti mehanizmi, a jedan od njih je enkripcija. Iako je nesporno da se enkripcija koristi u legitimne svrhe, ona pogoduje i izvršiocima krivičnih dela.

Podaci koji su sadržani u mobilnom telefonu ili se prenose njegovim posredstvom su potencijalni (elektronski) dokazi i mogu da doprinesu otkrivanju i dokazivanju krivičnih dela. Da bi ih nadležni organi prikupili za potrebe krivičnog postupka, koriste zakonom određena ovlašćenja, pa vrše uviđaj ili pretresanje mobilnog telefona, naređuju veštačenje pohranjenog sadržaja ili sprovode tajni nadzor komunikacije. Međutim, ukoliko su uređaj ili sadržaj pohranjen u njemu ili podaci koji se prenose u računarskoj mreži zaštićeni enkripcijom, prisutne su nezanemarljive pravne i tehničke poteškoće. *Enkripcija otežava prikupljanje elektronskih dokaza* prilikom sprovođenja pojedinih dokaznih radnji, pa nadležni organi koriste *posebne softverske i hardverske alate* za ostvarivanje pristupa uređaju, ekstrakciju pohranjenog sadržaja, odnosno za nadzor elektronske komunikacije. U radu su obrađena pojedina pravna i tehnička pitanja u vezi sa prikupljanjem sadržaja pohranjenog u mobilnom telefonu u kom je primenjena enkripcija celog internog skladišta podataka.

2. ENKRIPCIJA KAO ZAŠTITINI MEHANIZAM

Enkripcija predstavlja matematički proces u kom algoritam koristi određeni ključ da bi šifrovao računarski podatak, odnosno preveo ga iz izvornog, čitljivog oblika (engl. *plain text*) u nečitljivi, nerazumljivi oblik (engl. *cipher text*). Proces suprotan enkripciji je dekripcija (Katz, Lindell 2015, 52). U ovim procesima kompleksni algoritam u računaru koristi ključ da „zamaskira" i „odmaskira" sadržaj.[1] U zavisnosti od ključa, enkripcija može biti simetrična ili asimetrična.[2]

[1] Algoritam i ključ se sastoje iz niza bitova (nula i jedinica), a dužina ključa određuje jačinu enkripcije – određuje koliko različitih „pokušaja" je onome, ko ne poseduje ključ, potrebno da dekriptuje šifrovani tekst. Jačina ključa se ekspo-

Upotrebom enkripcije štite se računarski podaci koji su pohranjeni u uređaju za elektronsku obradu i skladištenje podataka (engl. *encryption at rest*) ili se prenose između takvih uređaja (engl. *encryption in transit*) (Gill, Israel, Parsons 2018, 4). Pohranjeni podaci se enkriptuju po principu simetrične enkripcije, na nivou pojedinačne datoteke, foldera ili particije u uređaju. Ukoliko je enkriptovan celi disk uređaja (engl. *full disk encryption*), neovlašćeno lice (lice koje ne poseduje ključ) ne može pristupiti pohranjenom sadržaju u čitljivom obliku (jer je i svaki pojedinačni računarski podatak pohranjen u uređaju enkriptovan, odnosno šifrovan i u potpunosti nečitljiv).

Počevši od 2010. proizvođači pametnih mobilnih telefona sve češće u drajv za skladištenje podataka ugrađuju softverske proizvode za enkripciju celog internog skladišta podataka (Casey et al. 2011, 130). Do 2014. je takva enkripcija bila predviđena kao opcija, a od 2014. je u uređajima sa *iOS* i *Android* operativnim sistemom konfigurisana kao fabrička postavka, zasnovana na 128-bitnom ili jačem ključu (npr. 256-bitnom).[3] Ovakvo opredeljenje IT kompanija predmet je snažne osude od strane država. Naime, ukoliko je primenjena enkripcija celog internog skladišta podataka u pametnom mobilnom telefonu, prilikom uviđaja, pretresanja ili veštačenja uređaja ne može se bez posedovanja ključa pristupiti pohranjenim podacima u izvornom obliku. Pojava da državni organi, i pored zakonskog ovlašćenja nemaju tehničke mogućnosti da ove radnje sprevedu, označava se terminom „Odlazak u mrak" (engl. „*Going dark*") (Pisarić 2020, 1093). Međutim, iako se ističe da enkripcija predstavlja ozbiljan izazov u otkrivanju i dokazivanju velikog broja krivičnih dela, podaci ne potvrđuju takvu tvrdnju.[4] Osim toga, bez ključa je teško, ali ne i nemoguće pristupiti enkriptovanom uređaju, jer postoje n*ačini da se ovaj zaštitini mehanizam prevaziđe*, odnosno *zaobiđe*.

---

nencijalno povećava sa svakim dodatnim nizom bitova. Tako, ključ veličine jednog bita generiše dva moguća ključa (1 ili 0), dvobitni ključ generiše 2^2 moguća ključa (odnosno 1–1, 1-0, 0–1 ili 0–0) i tako dalje.

[2] Simetrična enkripcija (engl. *symmetric encryption*), odnosno kriptografija privatnog ključa (engl. *private-key cryptography*) je kriptografski proces u kom se jedan te isti ključ koristi i za enkripciju i za dekripciju. Asimetrična enkripcija (engl. *asymmetric encryption*), odnosno kriptografija javnog ključa (engl. *public-key cryptography*) je kriptografski proces u kom se koriste dva različita ključa (jedan za enkripciju a drugi za dekripciju) koji su u posebnoj matematičkoj korelaciji (Swire, Ahmad 2012, 425).

[3] Za 128-bitni ključ postoji 2^{128}, odnosno 340,282,366,920,938,463,463,374,607, 431,768,211,456 mogućih kombinacija, dok se kod 256-bitnog ključa taj broj podiže na kvadrat.

[4] Primera radi, u izveštajima Okružnog javnog tužilaštva u Menhetnu navodi se da Tužilaštvo nije moglo zbog enkripcije da izvrši naredbu za pretresanje 111 mobilnih telefona u periodu septembar 2014 – oktobar 2015, odnosno 423 mobilna telefona tokom dve godine (u periodu septembar 2014 – oktobar 2016); za prvih deset

2.1. Lozinka i ključ

Procese enkripcije i dekripcije omogućava softver koji se zasniva na *sredstvu za verifikaciju i autentifikaciju pristupa*: *lozinci* (engl. *password*, *passphrase*), koja predstavlja niz alfanumeričkih ili simboličkih karaktera,[5] obrascu (engl. *pattern*) ili određenoj biometrijskoj karakteristici korisnika (otisak prsta, retine oka i sl). Osnovna funkcija ovog sredstva je onemogućavanje pristupa sadržaju uređaja licu koje ne poznaje lozinku ili obrazac, odnosno ne poseduje/prikaže biometrijske karakteristike. Činjenica da je korisnik izabrao lozinku kao sredstvo za verifikaciju i autentifikaciju pristupa nije ujedno i znak da je uređaj enkriptovan – to je slučaj samo ukoliko je enkripcija predviđena kao fabrička postavka ili je korisnik izabrao da koristi enkripciju, a kriptografski sistem se zasniva na lozinci. Samo tada, osim onemogućavanja pristupa neovlašćenom licu, *lozinka ima ulogu i u procesu enkripcije/dekripcije* – dokle god je uređaj zaključan, istovremeno je enkriptovan, kao i sadržaj pohranjen u njemu, a kada korisnik unese lozinku i prijavi se u sistem, uređaj se otključava, disk uređaja se dekriptuje i može se pristupiti sadržaju u izvornom obliku.

Lozinka *nije isto što i ključ*, tj. ne koristi se direktno u procesu enkripcije/dekripcije (u suprotnom enkripcija ne bi imala jaku zaštitnu ulogu), nego se *ključ izvodi iz lozinke*, tako što se stvara najmanje jedan tajni ključ koji enkriptuje ključ koji enkriptuje uređaj. Drugim rečima, lozinka sama po sebi nije ključ za dekripciju, ali unošenjem lozinke dekriptuje se ključ za dekripciju čime se dekriptuje uređaj i pristupa disku uređaja. Bez poznavanja lozinke je nemoguće dekriptovati ključ, a bez ključa je nemoguće dekriptovati disk uređaja. Korisnik uređaja, po pravilu, ne zna, tj. ne poseduje ključ, ali mu je zato lozinka poznata.

Iako lozinka nije isto što i ključ i nije ta kojom se enkriptuje uređaj, preko nje se enkriptuje/dekriptuje ključ, pa se, po dobijanju lozinke, ona koristi za otključavanje mobilnog telefona, odnosno za dekripciju ključa. Kada je uređaj otključan, svi podaci pohranjeni u njemu, koji su pre toga bili u šifrovanom, dostupni su u čitljivom obliku (osim ukoliko su dodatno enkriptovani prime-

meseci u 2017. od 1200 naredbi za pretresanje mobilnih telefona 700 nije moglo da se izvrši zbog enkripcije; u periodu od maja do avgusta 2018. u forenzičkoj laboratoriji je od 589 uređaja više od pola, tj. 366 (62%) uređaja bilo zaštićeno enkripcijom, od čega skoro polovina uređaja (165) nije mogla da se dekriptuje. Takođe, tvrdi se da je udeo enkriptovanih ajfona u forenzičkoj laboratoriji porastao je sa 59.6% u 2014 na 82.2% u 2019, ali se ne navodi o kom broju uređaja se radi. Videti, 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] Alfanumerički su slova A–Z i a–z i brojevi 0–9, a simbolički karakteri su .,+-&? itd.

nom softvera za enkripciju ili skriveni posebnim tehnikama). Iz tog razloga *nadležni organi nastoje da dođu, ako ne do ključa, onda do lozinke*, primenom različitih taktika za ostvarivanje pristupa uređaju zaštićenom enkripcijom.

2.2. Ranjivosti u sistemu enkripcije

Ukoliko je kriptografski sistem (u hardveru i/ili softveru) pravilno konfigurisan, ključ se ne može izvesti bez lozinke. Međutim, ukoliko u sistemu postoje određene greške (bagovi), one su uzrok njegove *ranjivosti* koje se mogu *upotrebiti za prevazilaženje ili zaobilaženje zaštite* koju pruža enkripcija. Ove ranjivosti se eksploatišu upotrebom softvera ili niza komandi i akcija, lokalno na uređaju (engl. *hands-on*) ili sa daljine (engl. *drive-by*),[6] a kako su karakteristične za određenu verziju uređaja i operativnog sistema, potrebno je da se zna koja je ranjivost specifična za datu kombinaciju hardvera i softvera, da bi se s uspehom mogla koristiti.

Državni organi nadležni za otkrivanje i dokazivanje krivičnih dela koriste ranjivosti kriptografskog sistema, jer njihova upotreba olakšava, odnosno omogućava pronalazak ključa/lozinke ili, pak, omogućava pristup uređaju i pohranjenom sadržaju bez upotrebe ključa/lozinke. Do potrebnih ranjivosti nadležni organi dolaze tako što ih sami pronalaze ili kupuju na tržištu, a na raspolaganju su im forenzički alati koji se zasnivaju na njihovoj eksploataciji. Ovo predstavlja praktičan izazov, jer zahteva posedovanje tehničke ekspertize za otkrivanje i upotrebu ranjivosti, odnosno značajne finansijske troškove za kupovinu ranjivosti ili forenzičkih alata koji se na njima zasnivaju. S tim u vezi, postavlja se pitanje da li je verovatnoća za uspeh dovoljno velika da bi se upotreba takvih ranjivosti mogla smatrati korisnom i opravdanom, i da li postoji odgovarajući pravni okvir. Odgovori na ova pitanja mogu se dati kada se sagledaju prednosti i nedostaci upotrebe ranjivosti, kao tehnike, u različitim taktikama za ostvarivanje pristupa mobilnom telefonu zaštićenom enkripcijom.

3. OSTVARIVANJE PRISTUPA MOBILNOM TELEFONU ZAŠTIĆENOM ENKRIPCIJOM

Za ostvarivanje pristupa mobilnom telefonu u kom je primenjena enkripcija celog internog skladišta podataka postoje dve taktičke strategije: 1) vrši se napad na enkripciju, uređaj se dekriptuje i pristupa se pohranjenom sadr-

[6] Primera radi, tako što korisnik poseti malicioznu ili zaraženu veb stranicu ili otvori mejl sa malicioznim sadržajem (Bellovin et al. 2014, 23).

žaju (strategija *prevazilaženja* enkripcije), i 2) ne vrši se napad na enkripciju, nego se sadržaju pohranjenom u uređaju pristupa na drugi način (strategija *zaobilaženja* enkripcije) (slično, Orin, Schneier 2018, 996). U okviru ovih strategija koristi se više taktika, od kojih se neke zasnivaju na upotrebi ključa/lozinke a druge na upotrebi ranjivosti u kriptografskom sistemu. Taktike i tehnike za pristup enkriptovanom uređaju uglavnom proizlaze iz digitalne forenzike, a da bi rezultirale elektronskim dokazom, moraju se primeniti u okviru odgovarajućeg ovlašćenja nadležnih organa za preduzimanje pojedinih mera i radnji.

3.1. Prevazilaženje enkripcije

U strategiji prevazilaženja enkripcije radi ostvarivanja pristupa sadržaju pohranjenom u mobilnom telefonu, u kom je primenjena enkripcija celog internog skladišta podataka, nadležni organi nastoje da upotrebom ključa i/ili lozinke dekriptuju enkriptovani uređaj. Radi se o sledećim taktikama: a) pronalazak ključa/lozinke; b) pogađanje ključa/lozinke; v) upućivanje zahteva za predaju lozinke/ključa.

3.1.1. Pronalazak ključa/lozinke

Do *ključa* se može doći primenom *tehnika kriptoanalize*,[7] među kojima se ističe *napad sporednim kanalima* (engl. *side-channel attack*). Ove tehnike registruju, mere i analiziraju fizičke karakteristike uređaja,[8] iskorišćavanjem ranjivosti u fizičkoj implementaciji kriptografskog sistema uređaja. Da bi se mogle primeniti, potrebno je postaviti senzor u neposrednoj blizini uređaja, koji o njemu prikuplja informacije (pa i ključ[9]).

Analogno pronalasku ključa za otvaranje brave u fizičkom svetu, nadležni organi tokom vršenja uviđaja, pretresanja stana i drugih prostorija ili pretresanja lica mogu pronaći *lozinku*, koja je zapisana (npr. na papiru) ili sa-

[7] Pod tim se podrazumeva upotreba matematičkih pravila za prevazilaženje kriptografske zaštite (National Institute of Standards and Technology 2006).

[8] Preko odgovarajućih senzora mogu se prikupiti informacije o pokretu, zvucima, elektromagnetnim isijavanjima uređaja dok radi, potrošnji energije, vremenu koje je potrebno uređaju da izvrši kriptografski algoritam i sl. (videti, Pfefferkorn 2017, 1395).

[9] Do ključa se može doći prikupljanjem i analizom elektromagnetnih isijavanja ili zvuka koje poizvode fizičke komponente kriptografskog sistema, odnosno zvuka koji ispušta procesor uređaja ili analizom strujnih tokova između delova uređaja dok se uređaj enkriptuje/dekriptuje (engl. *key-recovery attack*). Videti, Bright 2014.

čuvana na drugi način (npr. u datoteci u nekom drugom uređaju) i potom je upotrebiti za ostvarivanje pristupa uređaju. Pored toga, lozinka se može saznati i primenom određenih alata za tajni nadzor nad uređajem – tako što se ostvaruje fizički pristup uređaju radi postavljanja hardverskih alata, odnosno pristup uređaju sa daljine radi instaliranja softverskih alata.

U prvom slučaju se vrši tajni, fizički pristup uređaju na koji se potom postavljaju hardverske komponente koje beleže podatke, no, kako je njih potrebno fizički instalirati na uređaju i nakon toga preuzeti, postoji rizik da ih korisnik uoči. U drugom slučaju se vrši svojevrstan upad u uređaj, tako što se *sa daljine* (npr. preko virusa ili trojanca) u njemu instalira softverski alat, *koji presreće i snima pojedine podatke* – između ostalog, kucanje lozinke na tastaturi, koje potom šalje na računar nadležnih organa. Ovakav princip rada nije delotvoran u pogledu enkripcije uređaja koja se zasniva na lozinci, jer se može primeniti tek nakon otključavanja uređaja, odnosno unosa lozinke, pa softver lozinku ne može ni da registruje.[10]

3.1.2. Pogađanje ključa/lozinke

Ukoliko ne postoji način da se ključ/lozinka pronađu, nadležni organi vrše „*napad na silu*" (engl. *brute force attack*), što predstavlja sistematično isprobavanje različitih kombinacija ključa/lozinke do pronalaska prave, analogno isprobavanju kombinacija za otvaranje sefa u fizičkom svetu. Primena ove taktike ne stvara neke posebne pravne probleme.

S obzirom na to da je u trenutnim tehnološkim okvirima napad na silu usmeren na *ključ* izuzetno težak, gotovo nemoguć zadatak,[11] ovakav pristup se usmerava na *lozinku*. Uspešnost pronalaska lozinke zavisi od jačine lozin-

[10] Međutim, ukoliko su ispunjeni uslovi predviđeni zakonom, moguće je sa daljine vršiti pretresanje računara, bez obzira na primenjenu enkripciju – no, tada se radi o strategiji zaobilaženja enkripcije.

[11] Ukoliko bi svako od sedam milijardi ljudi koristio deset super-računara od kojih bi svaki testirao milijardu kombinacija za 128-bitni ključ u sekundi, bilo bi potrebno 77.000.000.000.000.000.000.000.000 godina da se „nasilno" pronađe odgovarajući ključ za dekripciju. Videti, Arora 2012. Primenom neke od tehnika kriptoanalize, koje se zasnivaju na ranjivostima u primeni algoritma za enkripciju ili samom algoritmu, moguće je smanjiti broj pokušaja koji je potreban da se pronađe ključ prilikom „napada na silu". Primera radi, iako algoritam naizgled nasumično proizvodi šifrovan tekst, moguće je uočiti određene obrasce za olakšano pogađanje ključa – koristeći poznate slabosti u *AES*-256 algoritmu moguće je pronaći pravi ključ „isprobavanjem" svega 2^{70} umesto 2^{256} kombinacija. Videti, Biryukov et al. 2009.

ke, koja je određena dužinom niza[12] i vrstom karaktera u nizu,[13] ali i od tehničke opremljenosti nadležnih organa. Pojedini forenzički alati se zasnivaju na ovom principu – uređaj se povezuje sa mobilnim telefonom, i nakon što, ponavljanjem pokušaja sa različitim kombinacijama lozinke, pronađe lozinku i ostvari pristup telefonu, ekstahuje sistem datoteka u potpunosti.[14]

Iako sama po sebi lozinka ne pruža neku posebnu zaštitu, jer algoritmi za „pogađanje" lozinke u modernim računarima mogu u nekoliko sekundi isprobati milione kombinacija lozinke, problem predstavljaju dodatne mere zaštite ugrađene u mobilne telefone: onemogućeno povezivanje telefona sa drugim hardverskim komponentama,[15] ograničen broj pogađanja, vremensko odlaganje novih pokušaja nakon određenog broja neuspelih pokušaja ili čak brisanje celokupnog sadržaja uređaja.[16]

Mogućnost eventualnog „razbijanja" algoritama za enkripciju (eng. *cracking*) zavisi u velikoj meri i od budućeg razvoja kvantnih računara (engl. *quantum computers*). Videti, Gomes 2018, 42–47.

12 Primera radi, za lozinku od četiri numerička karaktera postoji 10.000 kombinacija, koje čovek može da isproba za dan ili dva, a računar za nekoliko sekundi.

13 Odnosno, da li se koriste samo numerički ili alfanumerički karakteri. Bošnjak i Brumen (Bošnjak, Brumen 2018, 315) ukazuju na to da je prosečna dužina niza karaktera manja od osam i da se koriste predvidivi obrasci u nizovima, pri čemu korisnici često koriste veoma proste lozinke, tipa 1234 i slično. Videti, National Cyber Security Center 2019.

14 Jedan od najefikasnijih forenzičkih alata je proizvela američka kompanija Grejšift (eng. *Grayshift*). Radi se o hardverskom alatu koji se naziva „sivi ključ" (engl. *GrayKey*).

15 Primera radi, isprobavanje kombinacija lozinke na ajfonu moguće je samo na telefonu, ali ne i na nekom drugom uređaju s kojim bi se povezao, jer se od 2012. u hardver ugrađuje jedinstveni identifikator (engl. *Unique ID*,*UID*) koji onemogućava da se bez unosa lozinke sadržaj telefona pregleda ili kopira na drugi uređaj. Nakon pojave *GrayKey* uređaja, Epl je 2018. u operativni sistem *iOS 11.4.1* ugradio *default* bezbednosnu stavku – tzv. *USB restricting mode*, koji onemogućava da se bez unosa lozinke pristupi zaključanom ajfonu koji je povezan preko *USB* porta sa računarom i drugim *plug-in* uređajima (kao što je *GrayKey*) (Apple, Inc. 2020).

16 Na primer, u operativnom sistemu ajfona je ugrađena opcija koja usporava rad procesora nakon neuspelog unosa lozinke (Apple, Inc. 2020 b). Nakon četiri neuspela pokušaja mora se sačekati jedan minut do novog unosa niza karaktera, a nakon daljih neuspeha vremenski period u kom nije moguće pogađanje se povećava na pet minuta za šesti pogrešni unos, na 15 minuta za sedmi i osmi pogrešni unos, i na jedan sat za deveti. Postoji i mogućnost da se ajfon konfiguriše tako da se svi podaci u njemu izbrišu nakon desetog neuspelog unosa.

3.1.3. Upućivanje zahteva za predaju ključa/lozinke

Umesto pronalaska ili pogađanja ključa/lozinke, nadležni organi mogu da ih traže od onoga ko ih poseduje ili ima saznanja o njima.

Zahtev za *predaju ključa* upućuje se *proizvođaču* od koga se traži da omogući pristup enkriptovanom uređaju u konkretnom slučaju (engl. *exceptional access*). U ovoj situaciji, nakon što dođu u posed mobilnog telefona, saznaju njegov jedinstveni identifikacioni broj i pribave potrebna odobrenja (npr. naredbu o pretresanju uređaja), nadležni organi se obraćaju proizvođaču uređaja, zahtevajući od njega da: a) otključa uređaj koji mu se pošalje, b) otključa uređaj sa daljine, ili b) nadležnim organima preda ključ.

U jednom trenutku je pred proizvođače bio postavljen zahtev da prilikom proizvodnje u uređaj instaliraju ključ, koji bi se čuvao u depozitu kod nadležnih organa, a koji bi ih koristili po potrebi, međutim, od toga se odustalo (tzv. „prvi kripto rat“).[17] Proizvođač bi mogao da upotrebi, odnosno preda ključ i time omogući dekripciju uređaja i pristup pohranjenim podacima pod uslovom da ključeve za enkripciju/dekripciju uređaja čuva u depozitu,[18] što za sada nije slučaj (tzv. „drugi kripto rat“[19]).

Zahtev za predaju lozinke upućuje se *korisniku* uređaja, od koga se traži da: a) otkrije lozinku nadležnim organima, ili b) unese lozinku i preda otključan telefon, ili v) upotrebi svoje biometrijske karakteristike i preda otključan telefon. Ukoliko postupi po zahtevu nadležnog organa, radi se o *dobrovoljnoj*

---

[17] Tokom devedestih godina 20. veka pokušalo se sa stvaranjem hibridnog rešenja koji bi istovremeno omogućilo i razvoj informacione tehnologije i sposobnost nadziranja tog razvoja od strane države. Plan je bio da se ustanovi sistem pristupa državnih organa ključu za dekripciju u izuzetnim okolnostima. Tada je osmišljen standard deponovane enkripcije (engl. *Escrowed Encryption Standard: EES*), odnosno sistem deponovanja ključa (engl. *key escrow*). Naime, bio je kreiran set čipova (tzv. *Clipper Chip*) koji bi se ugrađivao u uređaje – država bi ključeve za enkripciju distribuirala IT kompanijama, a kopiju ključa ugrađenog u svaki pojedinačni uređaj čuvala bi u depozitu. Na taj način bi državni organi, po potrebi, imali pristup ključevima za dekriptovanje enkriptovanih podataka. Ovaj sistem je napušten usled jakog pritiska grupa za zaštitu građanskih prava i akademskog koncenzusa da se na ovaj način ne obezbeđuje tajnost komunikacija. Više o tome, videti Schneier 2015.

[18] Čak i ukoliko bi proizvođač čuvao ključeve i primio od nadležnih organa zahtev za njihovu predaju, postavlja se pitanje koji bi mrežni protokol bio korišćen za slanje ključa; na koji način bi zahtev bio autentifikovan, odnosno kako bi proizvođač imao potvrde o identitetu za sve nadležene organe širom sveta; na koji način bi se rezultati odnosili samo za konkretan uređaj, tako da se spreči da nadležni organi ne traže pristup uređaju koji nije u njihovom posedu i slično. Osim toga, to bi zahtevalo skupe i dugotrajne promene u hardverskim i softverskim komponentama uređaja.

[19] Видети фн. 24.

dekripciji. Međutim, postavlja se pitanje da li se lice može prinuditi da dekriptuje uređaj, odnosno da li mu se mogu izreći sankcije u slučaju odbijanja da postupi po zahtevu (*prinudna dekripcija*), naročito ako se radi o okrivljenom, s obzirom na privilegiju od samooptuživanja.[20] Kako smatra i Terzian (Terzian 2015, 1139), prinudna dekripcija je dozvoljena i potrebna da bi se ostvarila ravnoteža između interesa krivičnog postupka i privatnosti korisnika, jer u suprotnom enkripcija pravo nadležnih organa da pristupe uređaju transformiše u pravo okrivljenog da uništi dokaze protiv sebe, čineći ih nepristupačnim i nečitljivim. U slučaju postojanja izričite zakonske odredbe, postavilo se pitanje da li bi se sankcije mogle izreći prema okrivljenom koji tvrdi da mu lozinka nije poznata, da se ne seća i slično (videti Koops 2010, 435), no, da bi se okrivljeni mogao sankcionisati, nužno je da se nedvosmisleno utvrdi da on zna lozinku i da ne želi da je otkrije ili upotrebi.

Odgovor na ova pitanja zavisi od toga šta se od okrivljenog zahteva. Pojedina zakonodavstva čak sadrže izričite odredbe o prinudnoj dekripciji, na osnovu kojih se okrivljeni može sankcionisati ukoliko odbije da postupi po zahtevu da preda lozinku, odnosno da preda otključani telefon upotrebom lozinke ili biometrijskih karakteristika.

Tako, u Belgiji na osnovu člana 88*quater* Zakonika o krivičnoj istrazi[21] istražni sudija ili policija može *narediti licu*, pa i *osumnjičenom*, za koga se pretpostavlja da ima saznanja o računarskom sistemu koji je predmet istraživanja ili o uslugama koje omogućavaju zaštitu ili šifrovanje podataka koji se čuvaju, obrađuju ili prenose u tom sistemu, da *pruži informacije* o radu ovog sistema i o tome kako mu pristupiti, odnosno kako pristupiti podacima koji se u sistemu čuvaju, obrađuju ili prenose u razumljivom obliku (st. 1). U slučaju da lice, pa i osumnjičeni, *odbije* da otkrije lozinku, može se sankcionisati kaznom zatvora od šest meseci do tri godine i/ili novčanom kaznom od 26 do 20.000 evra. Ukoliko odbije da postupi po zahtevu u trenutku, kada je moglo da se spreči izvršenje krivičnog dela ili se umanje njegove posle-

[20] Privilegija od samooptuživanja je međunarodnopriznati pravni standard i predstavlja aspekt prava na pravično suđenje, koji podrazumeva, prema stavu Evropskog suda za ljudska prava (ECHR), da se okrivljeni ne može prinuditi da sam sebe inkriminiše i preda dokaze koji ga optužuju jer ima pravo da se brani ćutanjem (ECHR, *Saunders v. United Kingdom*, 17 December 1996.) Ova privilegija se *ne odnosi na prinudno uzimanje* od okrivljenog predmeta i uzoraka koji postoje *nezavisno od njegove volje*, kao što su uzorci krvi, urina i slično. Međutim, privilegija je povređena i ukoliko se od okrivljenog traži da sam sebe optuži tako što će *predati inkriminišuće dokaze* (npr. isprave, kao u predmetu ECHR, *Chambaz v. Switzerland*, 5 April 2012).

[21] Član je unet sledećom izmenom: 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

dice, može mu se izreći kazna zatvora od jedne do pet godina i/ili novčana kazna od 500 do 50.000 evra. Osim toga, od lica koje poseduje odgovarajuća saznanja (izuzev osumnjičenog i lica navedenih u čl. 156 Zakona o krivičnoj istrazi) može se tražiti da pokrene sistem ili, u zavisnosti od slučaja, da preda, odnosno učini dostupnim relevantne podatke u razumljivom obliku (st. 2), a nepostupanje je sankcionisano u st. 3 Belgijski Ustavni sud je ocenio da stav 1 ovog člana nije u suprotnosti sa privilegijom od samooptuživanja, jer se od okrivljenog traži da pruži informaciju (koja postoje nezavisno od njegove volje) koja omogućava pristup uređaju – za razliku od situacije kada bi se od njega tražilo da preda otključani uređaj i aktivno učestvuje u prikupljanju dokaza protiv sebe (videti, Cour constitutionnelle, 20 février 2020, n° 28/2020, *Rev. dr. pén.*, 2020/11, p. 1051–1057).

Član 434–15–2 francuskog Krivičnog zakonika[22] predviđa sankcionisanje svakog lica, pa i osumnjičenog, kaznom zatvora od tri godine i novčanom kaznom od 270.000 evra, ukoliko *odbije* da postupi po sudskoj naredbi *da preda lozinku ili je primeni radi otključavanja uređaja* koji je korišćen za pripremu, omogućavanje ili izvršavanje krivičnog dela, odnosno kaznom od pet godina zatvora i novčanom kaznom od 450.000 evra u slučaju da je odbijanje učinjeno u trenutku kada je ono moglo da spreči izvršenje krivičnog dela ili umanji njegove posledice. Rešavajući pitanje ustavnosti ovog člana i usaglašenost sa pravom okrivljenog da ćuti i sam sebe ne inkriminiše, francuski Ustavni savet je 2018. zauzeo stav da sama po sebi *odredba nije u suprotnosi sa privilegijom od samooptuživanja*, jer njen cilj nije da se od okrivljenog dobije priznanje niti sadrži pretpostavku krivice, nego jedino omogućava dekripciju uređaja i razjašnjavanje činjenica, a radi se o koji postoje *nezavisno od volje okrivljenog*. Međutim, nije dovoljno je da se u istrazi nedvosmisleno utvrdi da postoji kriptografski sistem koji je korišćen za pripremu, omogućavanje ili izvršavanje krivičnog dela, nego i da je okrivljeni toga svestan i da ima sposobnost da uređaj dekriptuje (videti, Le Conseil Constitutionnel, Décision n° 2018–696 QPC du 30 mars 2018, Journal officiel électronique authentifié n° 0076 du 31/03/2018).

U norveški Zakonik o krivičnom postupku je 2017. unet član 199a koji predviđa da policija može u toku pretresanja uređaja za obradu podataka da naredi svakom licu da preda informacije potrebne za ostvarivanje pristupa tom uređaju ili *da uređaj otključa preko sistema biometrijske autentifikacije*. Ukoliko lice odbije da postupi po takvom zahtevu, policija može po odobrenju javnog tužioca da *izvrši prinudnu autentifikaciju*. Ukoliko to nalažu ra-

[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.

zlozi hitnosti, policija može u ovom smislu da primeni silu na licu mesta, o čemu bez odlaganja obaveštava javnog tužioca (navedeno prema: Eurojust 2017, 9).

U teoriji se mogu naći i drugačiji stavovi. Tako privilegija od samooptuživanja štiti okrivljenog samo u pogledu zahteva da nadležnim organima otkrije lozinku, ali ne i ukoliko se od njega traži da nadležnim organima preda otključan uređaj nakon što unese lozinku ili da upotrebi svoje biometrijske karakteristike. Naime, lozinka je sama po sebi inkriminišuća, jer njeno iznošenje može da dovede do eventualnog otkrivanja inkriminišućih dokaza, što bi značilo da se od okrivljenog traži da svedoči sam protiv sebe u svojoj stvari, a što ne bi bilo u skladu sa principom *nemo tenetur* (tako i Winkler 2013, 211). Bez obzira na to koja se analogija koristi (ključ i brava, kombinacija u sefu i sl) nesumnjivo se radi o tajnom ključu koji je poznat samo okrivljenom, a od njega se zapravo traži da protiv svoje volje upotrebi sadržaj svog uma i otkrije nešto što ne postoji nezavisno od njegove volje i znanja, i time postane karika u lancu koja dovodi do otkrivanja dokaza protiv samog sebe i sopstvenog optuživanja (tako i Wareham 2017, 264).

Ukoliko, pak, nadležni organi jasno i nedvosmileno utvrde da uređaj sadrži inkriminišući sadržaj, i da je okrivljenom lozinka poznata, pa od njega zahtevaju da je upotrebi, tj. unese i preda otključan telefon, iako se od njega traži da aktivno sarađuje sa nadležnim organima, ne bi se mogao pozivati na privilegiju od samooptuživanja, jer se ne traži da protiv sebe kazuje (da otkrije lozinku), nego da dela na određeni način (da unese lozinku) (Kerr 2019, 769).

Što se tiče biometrijske verifikacije i autentifikacije, iako je ovo korisnicima predstavljeno kao revolucionarni, najbezbedniji način za zaštitu pristupa telefonu, u pravnoj realnosti upotreba klasične lozinke uživa veću pravnu zaštitu. Kako to Lemus (Lemus 2017, 554) uočava, otisak prsta je fizička karakteristika koja postoji nezavisno od volje okrivljenog i državni organi imaju pravo da prinude okrivljenog da protivno svojoj volji učestvuje u prikupljanju potencijalno inkriminišućih dokaza, kao i prilikom uzimanja drugih uzoraka (npr. krvi) – od okrivljenog se ne traži da iznese sadržaj svog uma, nego da iskaže tu karakteristiku (stavljanjem prsta na telefon radi otključavanja). Slično obrazloženje nalazi se i u inostranoj sudskoj praksi – primera radi: prinudno stavljanje prsta osumnjičenog na mobilni telefon radi otključavanja uređaja je dozvoljeno, pa policija primenjuje dozvoljenu i potrebnu prinudu (Court of First Instance The Hague, case 09/818727–17, 12. 3. 2018, navedeno prema: Eurojust 2018, 12), i na taj način se ne krši *nemo tenetur* princip, jer otisak prsta postoji nezavisno od volje osumnjičenog (Court of North-Holland – criminal chamber, 14. 12. 2018, navedeno prema, Eurojust

2019, 8). Suprotan stav zauzeo je, primera radi, norveški Vrhovni sud, određujući da se član 157 Zakonika o krivičnom postupku, koji uređuje fizički pregled i prinudno uzimanje uzoraka od osumnjičenog radi razjašnjavanja činjenica u rešavanju krivične stvari, ne može primeniti na prinudno stavljanje prsta osumnjičenog u cilju otključavanja i pristupa njegovom mobilnom telefonu (Supreme Court, case nr. 2016/908, 30. 8. 2016, navedeno prema: Eurojust 2016, 32).

3.2. Zaobilaženje enkripcije

U strategiji zaobilaženja enkripcije primenjuju se taktike koje se ne zasnivaju na upotrebi ključa/lozinke, nego se pristup sadržaju, pohranjenom u uređaju koji je zaštićen enkripcijom, ostvaruje na drugi način, dok se mehanizmi zaštite koje enkripcija pruža u potpunosti ignorišu. Radi se o sledećim taktikama: a) ostvarivanje pristupa sadržaju uređaja iskorišćavanjem ranjivosti u sistemu enkripcije, b) ostvarivanje pristupa sadržaju uređaja u trenutku kada je dekriptovan, i v) ostvarivanje pristupa kopiji sadržaja.

3.2.1. Ostvarivanje pristupa sadžaju uređaja iskorišćavanjem ranjivosti u sistemu enkripcije

Sam po sebi ključ je teško „slomiti", ali ukoliko u sistemu enkripcije postoje određene ranjivosti, one se mogu upotrebiti za ostvarivanje pristupa sadržaju pohranjenom u enkriptovanom uređaju, čak i bez posedovanja ključa. Do ovakvih ranjivosti se dolazi na dva načina: prethodnim, namernim ugrađivanjem u sistem ili pronalaskom i eksploatacijom postojećih ranjivosti.

U prvom slučaju radi se o tzv. „ulasku na zadnja vrata" (engl. *backdoors*). Tokom devedesetih godina 20. veka pojedine države su bez uspeha pokušale da proizvođače softvera za enkripciju i uređaja prinude da usvoje tehničke uslove koji bi omogućili „ulazak na zadnja vrata", a slični zahtevi postoje i danas – događaj sa kraja 2015.[23] je okidač za ponovno pokretanje debate

[23] Nakon što je oduzela mobilni telefon marke *iPhone 5C* decembra 2015, iako ovlašćena naredbom za pretresanje, policija nije mogla da pristupi sadržaju enkriptovanog mobilnog telefona marke ajfon, jer nije mogla da „pogodi" lozinku za otključavanje, bez opasnosti da se ti sadržaji bespovratno izgube. Ovo iz razloga što je u operativnom sistemu uređaja bila ugrađena opcija samobrisanja (engl. *auto-erase*), usled koje su svi podaci mogli da budu izbrisani nakon određenog broja

oko enkripcije koja još uvek traje u političkoj, naučnoj i stručnoj javnosti.[24] I pored toga što su zahtevi nadležnih organa legitimni, u stručnoj javnosti (Abelson et al. 2015, 18–20) je prisutan koncenzus da je sa tehničke strane nemoguće enkripciju oslabiti samo malo, bez da se ostavi prostor za potencijale ranjivosti u celokupnom sistemu enkripcije.

---

neuspelih pokušaja da se pogodi lozinka za pristup, čim je onemogućeno vršenje „napada na silu". Sudskom naredbom Eplu je naloženo da pruži tehničku pomoć policiji otklanjanjem ovakve zaštite iz operativnog sistema, čime bi se omogućio neograničen broj pogađanja lozinke, bez da se podaci izbrišu sa telefona, na koji način bi policija dobila mogućnost izuzetnog pristupa sadržaju enkriptovanog uređaja. Kompanija je odbila da postupi po naredbi, obrazalužući svoj stav potrebom da se zaštiti sigurnost svih korisnika, jer bi navodno bilo nemoguće da se samo za jedan uređaj učini ovakav izuzetak, a da se ne ugrozi bezbednost operativnog sistema i time omogući neovlašćeni pristup uređajima svih drugih korisnika. Spor između Epla i FBI jer je kompanija odbijala da dekriptuje enkripcijom zaštićeni ajfon nije rezulturao konačnom sudskom odlukom, jer je policija povukla svoj zahtev, nakon što je uspela da otključa telefon.

[24] Ova debata se označava Drugim kripto ratom. Tako je na sastanku ministara Ujedinjenog Kraljevstva, SAD, Kanade, Australije i Novog Zelanda 2018. izneto je opredeljenje ovih država ka stvaranju pravnog okvira za obavezivanje IT kompanija da prilagode postojeće, odnosno usvoje nove tehničke uslove koji bi omogućili da nadležni državni organi mogu da ostvare pristup enkriptovanim uređajima. Videti, Five Country Ministerial, 2018. Inače, Australija je prva država koja je usvojila takav propis – Zakon o pomoći i pristupu iz 2018. (Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, No. 148, 2018). Na osnovu ovog zakona nadležni državni organi u slučaju potrebe da se pristupi uređaju zaštićenom enkripcijom mogu da zahtevaju od kompanija (koji su proizvođači uređaja, kreaori softvera za enkripciju, pružaoci usluga elektronskih komunikacija, pristupa internetu, čuvanja podataka u oblaku) da pruže tehničku pomoć (engl. *technical assistance notice*), pa i da stvore mogućnost ulaska na zadnja vrata (engl. *technical capability notice*). Slično tome, u SAD je početkom 2020. u zakonodavnu proceduru pred američkim Senatom unet predlog zakona kojim bi se IT kompanija obavezale da ograniče upotrebu enkripcije (*The Eliminating Abusive and Rampant Neglect of Interactive Technologies Act: EARN IT Act*), međutim, propis još uvek nije usvojen.

Do skoro je na nivou EU bilo prisutno jasno i nedvosmisleno protivljenje ozakonjenju „ulaska na zadnja vrata", međutim, sve se više govori o stvaranju odgovarajućeg pravnog instrumenta koji bi omogućio targetiran pristup podacima uprkos enkripciji (Pisarić 2020, 615). U rezoluciji iz novembra 2020 Savet EU ističe da se nadležni organi u velikoj meri u istrazi velikog broj akrivilnih dela oslanjaju na preretanje komunicija koje je tehnički neizvodljivo zbog enkripcije a da ne postoji odgovarajući supstitut za ovu radnju. Zbog toga se mora naći odgovarajući pravni instrument primenjiv u trenutnom tehničkom okruženju – drugim rečima da se IT obaveže da omogući targetiran pristup podacima uprkos enkripciji. Videti, Council of the European Union, 2020.

U drugom slučaju nadležni organi, uprkos enkripciji, ostvaruju pristup uređaju i *ekstrahuju sadržaj*, koristeći ranjivosti u postojećim sistemima, koje pronalaze sami ili ih kupuju na tržištu. Osim toga, nadležnim organima su na raspolaganju brojni alati koji se zasnivaju na otkrivenim a neprevaziđenim ranjivostima u softverskim i hardverskim komponentama mobilnih telefona, a koji omogućavaju ekstrakciju podataka iz uređaja zaštićenih enkripcijom.[25] Performanse ovih alata za se jasno vide iz godišnjih izveštaja Programa za testiranje alata za digitalnu forenziku američkog Nacionalnog instituta za standarde i tehnologiju – prema poslednjim izveštajima, i pored enkripcije i dodatnih mera zaštite, postoje alati koji ekstrahuju gotovo sve podatke iz zaključanih, enkriptovanih uređaja i instaliranih aplikacija (videti, National Institute of Standards and Technology 2019). Ovi podaci su značajni jer pokazuju da, uprkos tvrdnjama da enkripcija predstavlja nezanemarljivu prepreku za rad nadležnih oragana, forenzički alati koji funkcionišu po standardima digitalne forenzike ipak omogućavaju prikupljanje podataka iz enkriptovanog uređaja. Međutim, da bi njihova upotreba rezultirala elektronskim dokazima, moraju biti ispunjeni uslovi propisani za pretresanje i veštačenje mobilnog telefona i poštovana ograničenja utvrđena u naredbi za pretresanje, odnosno veštačenje (Pisarić 2019, 208).

3.2.2. Ostvarivanje pristupa sadržaju uređaja u trenutku kada je dekriptovan

Kako je ceo disk enkriptovan samo dok je uređaj zaključan, kroz ovu taktiku se nastoji da se uređaju pristupi u momentu kada ga enkripcija ne štiti, odnosno kada je otključan. Naime, kada korisnik unese sredstvo za autentifikaciju i verifikaciju, uređaj se otključava i dekriptuje, a lozinka se čuva u privremenoj (RAM) memoriji, dokle god je uređaj uključen i otključan. To znači da se preuzimanjem kontrole nad uređajem u tim okolnostima omogućava pristup pohranjenom sadržaju u izvornom obliku, pa i lozinci (koja se na taj način može saznati i naknadno koristiti). Ovakav pristup ostvaruje se kroz fizičku kontrolu nad uređajem ili sa daljine.

[25] Među tim alatima se ističu proizvodi izraelske firme Selebrit (eng. *Cellebrite*), prvenstveno *Universal Forensic Extraction Device: UFED Premium*.

U prvom slučaju, da bi se zaobišao zaštitini mehanizam, nadležni organi nastoje da, nakon prethodnog planiranja,[26] najpre ostvare *fizičku kontrolu nad uređajem* u momentu dok je otkučan,[27] a zatim na licu mesta sprovedu digitalnu istragu na „živom" sistemu,[28] ukoliko su za to postoji odgovarajući pravni okvir (Pisarić 2019, 131).

U drugom slučaju ostvaruje se pristup uređaju sa daljine, odnosno sprovodi se *daljinsko pretresanje dekriptovanog uređaja u realnom vremenu*. Drugim rečima, nadležni organi preduzimaju svojevrsno hakovanje, kako bi za potrebe krivičnog postupka ostvarili pristup podacima pohranjenim u uređaju zaštićenom enkripcijom. „Hakovanje" se vrši primenom malicioznog softvera (malvera), koji se instalira u uređaj (ostvarivanjem tajnog, fizičkog pristupa uređaju) ili sa daljine, a uspešnost ove taktike zavisi od tehničkih mogućnosti nadležnih organa.[29]

Kako se kroz daljinsko pretresanje uređaja ugrožava privatnost korisnika i bezbednost uređaja kompromitovanjem pouzdanosti i integriteta sistema enkripcije, primena ove taktike je opravdana samo pod uslovom da postoji odgovarajući pravni osnov za preduzimanje ove radnje, koja je neophodna za ostvarivanje legitimnog cilja, a da je ograničenje ljudskih prava potrebno i srazmerno ostvarenju tog cilja (Office of the United Nations High Commissioner for Human Rights 2018, 6). Drugim rečima, samo ako je pretresanje uređaja sa daljine izričito uređeno zakonom kao posebna dokazna radnja,

[26] Kejsi i saradnici (Casey et al. 2011, 134) tvrde da je za uspeh ove taktike neophodno prethodno plansko prikupljanje podataka o tehničkoj sofisticiranosti korisnika, mestu i vremenu upotrebe uređaja, fizičkim karakteristikama lokacije na kojoj će preuzeti kontrola nad uređajem, operativnom sistemu i hardverskoj konfiguraciji uređaja, eventualnim dodatnim merama zaštite u uređaju, vrsti enkripcije i sl. Ovi podaci su potebni kako bi se stvorila strategija delovanja, tako da se poveća faktor iznenađenja i smanji mogućnost da se uređaj isključi ili ošteti.

[27] Primera radi, policija je nakon višegodišnje istrage nezakonitih aktivnosti na crnom tržištu darkneta, Put svile, došla do računara njegovog osnivača upravo primenom ove taktike. Iz prethodno prikupljenih podataka proizašlo je da on koristi računar u gradskoj biblioteci, pa su dva službena lica u civilu iscenirala distrakciju, a treći je oduzeo računar koji je bio otključan i dekriptovan. Na taj način je prevaziđen problem enkripcije celog diska, a osnivač Puta svile je osuđen na doživotnu kaznu zatvora. Videti, Mullin 2015.

[28] Standardno postupanje u slučaju sumnje na enkripciju celog diska je da se iz *RAM* memorije uređaja prikupljaju nepostojani podaci (engl. *volatile data*), među kojima su od naročite važnosti lozinka i drugi podaci potrebni za otvarivanje pristupa enkriptovanim sadržajima, pre nego što se uređaj prenese u forenzičku laboratoriju (Pisarić 2015, 243).

[29] Podaci o alatima koji se koriste u ovu svrhu nisu dostupni javnosti.

čija primena bi bila ograničena na naročito teška krivična dela, pod uslovom da ne postoje blaže mere za ostarivanja cilja (Hennessey 2016), čime bi bili ispoštovani principi legaliteta, srazmernosti i supsidijarnosti.

Izričite zakonske odredbe o daljinskom pretresanju uređaja postoje u svega nekoliko država. Tako nemački Zakonik o krivičnom postupku[30] u članu *100b* reguliše tajno pretresanje uređaja i prikupljanje pohranjenog sadržaja sa daljine. Radnja se može odrediti naredbom suda samo prema licu za koje postoji osnovana sumnja da je izvršio neko od naročito teških, taksativno nabrojanih krivičnih dela (odnosno da je pokušao izvršenje, ukoliko je pokušaj kažnjiv), pod uslovom da je utvrđivanje činjenica ili lociranje osumnjičenog znatno teže ili nemoguće sprovođenjem drugih radnji. Belgijski Zakonik o krivičnoj istrazi u članu *90ter* predviđa da istražni sudija može narediti da se tajno, uz pomoć tehničkih sredstava, izvrši daljinsko pretresanje uređaja koje koristi lice osumnjičeno za neko od taksativno nabrojanih krivičnih dela, i to samo u izuzetnim slučajevima, ukoliko to zahtevaju interesi istrage a potrebne činjenice se ne mogu utvrditi na drugi način. Sudija u naredbi može odrediti i tajni ulazak u dom ili drugi prostor u kom se uređaj nalazi, primenu tehničkih sredstava u cilju zaobilaženja mera zaštite i instaliranje tehničkih sredstava za dekripciju uređaja. Član *588 septies* španskog Zakonika o krivičnom postupku[31] predviđa da, ukoliko postoji sumnja da je lice izvršilo neko od krivičnih dela iz nabrojanih grupa teških krivičnih dela, sudija može narediti instaliranje softvera kojim se sprovodi daljinski elektronski nadzor uređaja, prvobitno na mesec dana, s mogućnošću produženja do tri meseca.

Pored odgovarajućeg pravnog okvira, nužno je da se alati koji omogućavaju daljinski pristup i pretresanje, razvijaju i testiraju u skladu sa standardizovanim pravilima, kako ne bi kompromitovali informacionu bezbednost, narušili integritet elektronskih dokaza, niti omogućili nesrazmerno i neselektivno prikupljanje podataka.

---

[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.

[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 – odredba je u Zakonik uneta 2015, kroz 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).

3.2.3. Ostvarivanje pristupa kopiji sadržaja

Ukoliko su podaci sadržani u enkriptovanom telefonu istovremeno pohranjeni na serveru pružaoca usluge skladištenja podataka (odnosno kao bekap „u oblaku“) nadležni organi mogu da upute zahtev pružaocu usluge da te podatke preda. Naime, kao što se, umesto ostvarivanja uvida u mejlove pohranjene u enkriptovanom uređaju, traži od pružaoca usluga elektronskih komunikacija da preda kopiju mejlova, tako se, umesto pokušaja dekripcije mobilnog telefona, zahteva od pružaoca usluge skladištenja podataka „u oblaku“ da preda bekap kopiju sadržaja mobilnog telefona koja se čuva na njegovom serveru.

Nakon što se utvrdi da se korisnik mobilnog telefona opredelio za bekapovanje pohranjenog sadržaja i da takva kopija postoji „u oblaku“, [32] da bi se ova taktika mogla primeniti potrebno je da nadležni organi imaju odgovarajuće ovlašćenje da zahtevaju predaju kopije.[33] Pružalac usluge bi mogao da postupi po ovakvom zahtevu pod uslovom da takvi podaci postoje u konkretnom slučaju, a faktička mogućnost zavisi od toga da li su kopije sadržaja „u oblaku“ pohranjene u *plaintext* ili u šifrovanom obliku (u kom slučaju mogućnost pružaoca usluge da ih preda nadležnim organima u čitljivom obliku zavisi od vrste enkripcije koja je primenjena[34]).

---

[32] Korisnici ajfona imaju na raspolaganju mogućnost da sadržaj telefona pohrane kao bekap u „oblaku“ na ajklaud platformi (engl. *iCloud*), kojoj se pristupa preko posebnog naloga (*@icloud.com*, *@me.com i @mac.com*). U android telefonima se sa prvom prijavom na Gugl nalog (preko džimejl adrese) vrši bekapovanje podešavanja telefona i sinhronizovanje kontakata, obeleživača stranica, lozinki i dr, a nakon toga se automatski (dokle god korisnik ne isključi tu opciju) bekapuju određeni sadržaji na Guglovim serverima za skladištenje podataka „u oblaku“ (npr. fotografije se bekapuju u *Google Photos*, a poruke, datoteke i folderi u *Google Drive*). Korisnici mobilnog telefona mogu da izaberu da se bekap sadržaja u uređaju uopšte ne stvara i ne čuva ni na jednom serveru.

[33] Organ postupka može da zahteva ostvarivanje uvida u sadržaj pohranjen na ajklaud platformi ukoliko postoji sudska naredba, a potrebno je da se navede odgovarajući *Apple ID* ili adresa mejl naloga, a ukoliko su nepoznati, puno ime i broj telefona ili fizička adresa korisnika kako bi se identifikovao. Videti, Apple, Inc. 2020d. Za nadležne državne organe van SAD važe ista pravila, s tim da se zahtev upućuje u okviru mehanizma za pružanje međunarodne pravne pomoći u krivičnim stvarima. Videti, Apple, Inc. 2020e. Od Gugla se u okviru odgovarajućih procedura može zahtevati da preda podatke bekapovane na njegovim serverima. Videti, Google 2021.

[34] Bekap na Guglovim serverima je zaštićen enkripcijom a ključ se izvodi iz korisnikove lozinke za Gugl nalog (za pojedine podatke se izvodi iz lozinke za mobilni telefon), pri čemu ni Gugl ne poseduje ključ, pa ne može predati nadležnim organima kopiju sadržaja koja se čuva „u oblaku“. Videti, Google 2020. Sadržaj u ajklaud platformi je enkriptovan lokalno na serveru, 128-bitnim *AES* algoritmom, ali Epl poseduje ključ za dekripciju, pa te podatke može predati nadležnim organima.

Adekvatnost kopije da bude zamena za sadržaj pohranjen u enkriptovanom mobilnom telefonu zavisi od toga koji sadržaj se bekapuje i koliko je vremena prošlo od poslednjeg bekapa. Iako bekap sadržaja mobilnog telefona obuhvata obilje podataka koji mogu biti od koristi za nadležne organe, ipak se, i to u najboljem slučaju, „u oblaku" ne čuvaju svi podaci koji su inače pohranjeni u uređaju, pa je zbog toga „oblak" samo alternativa a ne supstitut ostvarivanju pristupa enkriptovanom mobilnom telefonu.

4. ZAKLJUČAK

To što enkripcija celog internog skladišta podataka u mobilnom telefonu predstavlja prepreku u istrazi, naročito teških krivičnih dela, ne bi se smelo koristiti se kao argument protiv nje. Tvrdi se da se problem „odlaska u mrak" može prevazići jedino obavezivanjem proizvođača uređaja, tvoraca softvera i pružalaca usluga skladištenja podataka „u oblaku" da oslabe enkripciju u uređajima, aplikacijama i uslugama, odnosno da zadrže tehničku sposobnost da postupe po zahtevu nadležnih organa za ostvarivanje pristupa dekriptovanim sadržajima, tj. da omoguće „ulazak na zadnja vrata". Ovakav zahtev postavlja pred kompanije bezbednosne, ekonomske i tehničke izazove i neprihvatljiv je, jer ne postoji način da se enkripcija oslabi i zaobiđe za jednog korisnika/uređaj a da se ne ugrozi celokupan sistem enkripcije. Pored toga, zahtev nije ni opravdan – bez obzira na to što enkripcija predstavlja prepreku u istrazi, ona nije nepremostiva, jer postoje drugi načini da se pristupi podacima pohranjenim u enkriptovanom uređaju.

U okviru strategije prevazilaženja enkripcije, taktika pronalaska ključa/lozinke može dati uspeha čak i primenom klasičnih kriminalističkih taktika i tehnika, što zavisi od okolnosti konkretnog slučaja. Uspešnost taktike pogađanja ključa/lozinke je uslovljena tehničkim mogućnostima nadležnih organa, odnosno primenom forenzičkih alata koji se zasnivaju na „napadu na silu" ili primenom tehnika kriptoanalize. U pogledu upućivanja zahteva okrivljenom za predaju lozinke, njega štiti privilegija od samooptuživanja ukoliko se od njega traži da otkrije sadržaj svog uma i iskaže lozinku, ali ne i ukoliko se od njega zahteva da preda uređaj otključan nakon unosa lozinke ili biometrijske karakteristike jer one postoje nezavisno od njegove volje.

Ukoliko se, pak, podaci čuvaju na platformi treće strane (npr. *Amazon Web Services* ili *Google Cloud Platform*), Epl ključ ne poseduje. Pojedini podaci (npr. podaci o zdravlju, plaćanju, lozinke za *Wi-Fi* mrežu) zaštićeni su *end-to-end* enkripcijom, a ključ se izvodi iz lozinke koju samo korisnik zna, tako da ni Epl nema pristup ovim podacima u izvornom obliku. Videti, Apple, Inc. 2020c.

Iskorišćavanje postojećih ranjivosti u sistemu enkripcije se svodi na upotrebu odgovarajućih forenzičkih alata za ekstrakciju podataka i primenjuje se ukoliko su ispunjeni zakonski uslovi za pretresanje i veštačenje mobilnog telefona, uz poštovanje ograničenja utvrđenih u naredbi za pretresanje, odnosno naredbi za veštačenje, a uspeh u primeni taktike zavisi od tehničke opremljenosti nadležnih organa. Postoje standardizovni forenzički alati koji su podobni za ekstrakciju sadržaja iz enkriptovanih mobilnih telefona, što pokazuju rezultati o njihovom testiranju. Ostvarivanje pristupa uređaju sa daljine u momentu dok je dekriptovan predstavlja svojevrsno hakovanje, pa je nužno da je izričito predviđeno i uređeno zakonom kao posebna dokazna radnja, naročito uz poštovanje principa legaliteta, srazmernosti i supsidijarnosti. Uspešnost upućivanja zahteva pružaocu usluga skladištenja podataka „u oblaku" da preda kopiju sadržaja mobilnog telefona zavisi od toga da li se i koji podaci skladište na njihovom serveru, da li su i kojom vrstom enkripcije zaštićeni na serveru, odnosno da li ih pružaoci usluge mogu nadležnim organima predati.

Prikazane taktike i tehnike nisu idealno rešenje za prevazilaženje problema enkripcije, ni u pravnom ni u tehničkom smislu. Neke od njih zahtevaju značajna finansijska sredstava i stručnost, dok su druge upitne sa stanovišta bezednosti informacionih sistema, s jedne strane, i zaštite prava korisnika, a naročito prava okrivljenog, s druge strane. Međutim, njihov značaj se ogleda u tome što pokazuju da ipak postoje načini da se problem enkripcije makar donekle prevaziđe. Očigledno je da je, i pored i uprkos enkripciji, pretresanje i veštačenje mobilnog telefona moguće izvršiti, kroz upotrebu odgovarajućih alata, uz pomoć kojih se vrši ekstrakcija podataka iz uređaja u skladu sa principima digitalne forenzike, a sve u postojećim pravnim okvirima, a da obavezivanje kompanija da oslabe enkripciju ili proširivanje ovlašćenja nadležnih organa nije opravdano a time ni neophodno.

LITERATURA

[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*, poslednji pristup 14. jula 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/*, poslednji pristup 16. jula 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] Pisarić, Milana. 2019. *Elektronski dokazi u krivičnom postupku*. Novi Sad.

[17] Pisarić, Milana. 3/2020. Enkripcija kao prepreka otkrivanju i dokazivanju krivičnih dela. *Zbornik radova Pravnog fakulteta u Novom Sadu* 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*, poslednji pristup 14. jula 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.

OSTALI IZVORI

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

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

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

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

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