Kretanje kroz digitalni labirint: Izazovi sa kojima se suočava pravosuđe u „rukovođenju" digitalnim dokazima

Pripremila: Azra Bećirović, AIRE Centar

U savremenom društvu enkripcija je postala neizostavna komponenta svakodnevnog života. Snažna enkripcija predstavlja ključnu zaštitu privatnosti i poslovanja. S obzirom na sve veću prisutnost Interneta i digitalnih tehnologija, postoji nekoliko ključnih argumenata koji podržavaju enkripciju među kojima se posebno ističu ljudska prava, pravo na privatnost i slobodu izražavanja.

Enkripcija pruža sredstva za zaštitu naših podataka od prijetnji kao što su hakiranje, krađa identiteta ili neovlašteni pristup. Omogućava nam da komuniciramo sigurno putem digitalnih kanala, čuvajući naše privatne poruke, podatke i informacije od neovlaštenog pristupa. U svijetu u kojem su digitalne komunikacije norma, enkripcija je postala neophodan alat u zaštiti privatnosti i poslovanja.

Međutim, počinioci krivičnih djela, također, zloupotrebljavaju enkripciju kao dio svog *modusa operandi* a problem postaje sve ozbiljniji i privlači pažnju velikog broja evropskih i država u regionu nakon dekripcije komunikacijskih platformi EncroChat i SKY ECC[43]. Takvi slučajevi ukazuju na izazove s kojima se suočavaju vlasti u održavanju sigurnosti i borbi protiv kriminala s obzirom na to da članovi kriminalnih grupa koriste enkripciju kako bi otežali detekciju svojih aktivnosti.

[43] EncroChat i Sky ECC su komunikacijski servisi koji su omogućavali korisnicima da sigurno razmjenjuju poruke i podatke putem posebno dizajniranih uređaja i snažne enkripcije. Ti servisi su pružali visok nivo sigurnosti i privatnosti, omogućavajući korisnicima da komuniciraju bez straha od nadzora ili presretanja poruka. Identitet korisnika je bio zaštićen, a komunikacija se odvijala putem pseudonima ili korisničkih identifikatora, otežavajući tako praćenje ili povezivanje komunikacije sa stvarnim identitetom korisnika. EncroChat je koristio vlastite enkriptirane uređaje, a Sky ECC je bio dostupan kao aplikacija za odabrane pametne telefone. (Op. a.) Više na: https://shorturl.at/ajzLM

Ova situacija predstavlja izazov u održavanju ravnoteže između zaštite privatnosti i potrebe za sigurnošću. S jedne strane, pravo na privatnost je važno ljudsko pravo koje treba poštivati a enkripcija pruža sredstva za zaštitu tog prava. S druge strane, vlasti su odgovorne za održavanje sigurnosti društva i suzbijanje kriminalnih aktivnosti.

U kontekstu krivičnih pravosudnih sistema digitalni dokazi su otvorili mnogobrojna pitanja, uključujući metode otkrivanja komunikacije, prijenosa dokaznih materijala drugim državama i njihovu upotrebu u krivičnim postupcima, kao i pitanje osnovanosti i prihvatljivosti takvih dokaza.

U ovom članku poseban fokus stavljen je na analizu trenutnog stanja pravosudnog sistema u Bosni i Hercegovini u vezi sa suđenjem u predmetima organiziranog kriminala i korupcije, kao i na izazove s kojima se suočavaju sudovi. Izuzetna važnost, u članku, se daje pravičnosti postupka, zaštiti prava pojedinaca, te ulozi nacionalnih sudova u procjeni zakonitosti dokaza.

Analiza prakse bh. pravosuđa u predmetima organiziranog kriminala i korupcije

Prema *Analizi prakse najviših sudova u BiH u slučajevima organiziranog kriminala i korupcije*[44], sudovi razumiju i primjenjuju koncept posebnih istražnih radnji, te se uspješno suočavaju sa izazovima u procesuiranju organiziranog kriminala i korupcije uz poštivanje standarda Evropske konvencije o ljudskim pravima (EKLJP ili Konvencija). Međutim, u vezi s primjenom posebnih istražnih radnji i obavezom da se strogo poštivaju zakonski uvjeti za izdavanje i produženje naredbi, prvostepeni sudovi imaju neka otvorena pitanja.

Također, u toj analizi, se naglašava da su moderna komunikacijska sredstva donijela nove izazove za pravosuđe, te da se sudovi već sada susreću s dokazima dobivenim putem kriptiranih komunikacija i međunarodne pravne pomoći za koje tek treba da se razviju novi stavovi i praksa. U pogledu dokaza dobivenih putem međunarodne pravne pomoći još se očekuje konačan zaključak o njihovoj upotrebi u specifičnim situacijama koje su postale bitne za otkrivanje i dokazivanje krivičnih djela.

Pravna priroda digitalnih dokaza u Bosni i Hercegovini

U krivične procesne zakone Bosne i Hercegovine 2003. godine uvedene su posebne istražne radnje s ciljem suzbijanja teškog organiziranog kriminala i suočavanja sa sofisticiranim načinima izvršenja krivičnih djela. Zakon o krivičnom postupku Bosne i Hercegovine (ZKPBiH)[45] i odgovarajući propisi ZKPRS, FBiH i Brčko Distrikta reguliraju izvođenje pretresa pokretnih stvari, uključujući kompjuterske sisteme, uređaje za pohranjivanje podataka i mobilne telefone. Članom 51. stav 2. ZKPBiH propisano je da pretresanje tih predmeta podrazumijeva samo vizuelni pregled podataka bez korištenja računarskih programa za pronalaženje informacija. Međutim, za ekstrakciju izbrisanih podataka[46], pristup skrivenim informacijama i utvrđivanje sadržaja koji nije vidljiv na prvi

[44] Analiza prakse najviših sudova u BiH u slučajevima organiziranog kriminala i korupcije, izdavači: Ustavni sud Bosne i Hercegovine i AIRE Centar, 2023.

[45] Zakon o krivičnom postupku Bosne i Hercegovine („Službeni glasnik BiH“ br. 3/2003, 32/2003 – ispr., 36/2003, 26/2004, 63/2004, 13/2005, 48/2005, 46/2006, 29/2007, 53/2007, 58/2008, 12/2009, 16/2009, 53/2009 - dr. zakon, 93/2009, 72/2013 i 65/2018), čl. od 116. do 122.

[46] Prema članu 25. Odluke o posebnim obavezama pravnih i fizičkih lica koja pružaju telekomunikacijske usluge, administriraju telekomunikacijske mreže i vrše telekomunikacijske djelatnosti u pogledu obezbjeđenja i održavanja kapaciteta koji će omogućiti ovlaštenim agencijama da vrše zakonito presretanje telekomunikacija, kao i kapaciteta za čuvanje i obezbjeđivanje telekomunikacijskih

pogled potrebni su specijalistički računarski programi i sistemi. Za te svrhe se provodi vještačenje koje zahtijeva posebno stručno znanje.[47]

Nekoliko evropskih država[48] ima posebne propise koji reguliraju tajno prisluškivanje kriptiranih elektronskih komunikacija i njihovo dekodiranje. Prema tim propisima, dekodiranje se obično postiže na dva načina: instaliranjem posebnog softvera na uređaje putem fizičkog pristupa nadležnih organa, ili na daljinu ubacivanjem virusa ili „trojanaca". Međutim, zakoni o krivičnim postupcima u BiH ne reguliraju posebno digitalne dokaze i digitalne istrage. Time se postavlja pitanje da li bi komunikacija koja se odvijala putem kriptiranih telefona mogla biti otkrivena preko postojećih dokaznih radnji da međunarodna pravna pomoć nije dostavljala dokaze.

Osnovni problem dokaza pribavljenih putem međunarodne pravne pomoći jeste u tome što se dokazni sistemi različitih država prilično razlikuju. To znači da se mogu postaviti pitanja da li su takvi dokazi pribavljeni na dopušten način, u skladu sa zakonskim uvjetima i propisanim postupkom, te da li pravni poredak omogućava da se koriste ti dokazi kao osnov za presudu.

U kontekstu preduzimanja posebnih istražnih radnji u drugim državama i dokaza pribavljenih putem međunarodne pravne pomoći Evropski sud za ljudska prava u slučaju *Stojković protiv Francuske i Belgije*[49] ističe da vlasti države koja provodi krivični postupak nisu odgovorne za pravni okvir kojim se uređuju uvjeti za pribavljanje dokaza. Ipak, od njih se zahtijeva da osiguraju da radnje preduzete u državi koja je dostavila dokaze ne krše prava odbrane, čime se potvrđuje pravičnost postupka koji se vodi pod njihovim nadzorom. U konačnici, pravičnost se mora procjenjivati u svjetlu postupka posmatranog u cjelini.

Standardi Evropskog suda za ljudska prava

Sudija Evropskog suda za ljudska prava Tim Eicke ističe da član 6. Konvencije garantira pravo na pravično suđenje, ali da ne propisuje pravila o prihvatljivosti dokaza ili o njihovoj ocjeni. Sud je jasno usvojio stav da, dokle god je suđenje pojedincu u cjelini "pravično"[50], prihvatljivost dokaza i njihova ocjena su pitanja kojima, prije svega, treba da se bave nacionalno pravo i nacionalni sudovi.

Cjelovit odgovor na pitanje o faktorima koji su značajni za ukupnu procesnu pravičnost prilikom procjene korištenih dokaza obuhvata nekoliko ključnih elemenata. Između ostalog, u slučaju *Bykov protiv Rusije*[51] Evropski sud za ljudska prava je predstavio konkretan test kojim se ocjenjuje da li je postupak bio pravičan kao cjelina. Test se sastoji od odgovora na sljedeća pitanja:

1. Priroda navodne nezakonitosti dokaza, te da li je povrijeđeno neko konvencijsko pravo? U tom kontekstu član 8. Konvencije može postati relevantan i treba se vratiti na njega.

podataka („Službeni glasnik BiH" broj 104 od 29. decembra 2006, 58/07), svi operateri telekomunikacija, mrežni operateri, davatelji usluga i davatelji pristupa su obavezni da čuvaju podatke najmanje 12 mjeseci.

[47] Kao primjer se mogu navesti: prvostepena presuda broj S1 2 K 034358 20 K od 9. aprila 2021. godine i drugostepena presuda broj S1 2 K 034358 21 Kž od 27. jula 2021. godine. (Op.a.)

[48] To su: Francuska, Njemačka, Nizozemska, Danska, Poljska, Švedska i Švajcarska. Više na: https://shorturl.at/vBCUX

[49] *Stojković protiv Francuske i Belgije*, predstavka broj 25303/08, presuda od 27. oktobra 2011. godine.

[50] *Moreira Ferreira protiv Portugala (broj 2)* [VV], predstavka broj 19867/12, stav 83.b, presuda od 11. jula 2017. godine, i *Schenk protiv Švajcarske*, predstavka broj 10862/84, st. 45-46, presuda od 12. jula 1988. godine.

[51] *Bykov protiv Rusije*, predstavka broj 4378/02, presuda od 10. marta 2009. godine.

2. Sud treba da razmotri kvalitet dokaza o kome je riječ i okolnosti pod kojima su dokazi pribavljeni. Posebno je važno da se razmotri da li takve okolnosti dovode u sumnju pouzdanost ili tačnost dokaza? U tom kontekstu informacije o načinu na koji je dokaz pribavljen mogu imati važnu ulogu. Također, potrebno je pažljivo razmotriti pitanja o kvalitetu dokaza, njihovoj pouzdanosti i tačnosti.
3. Da li je podnosilac predstavke imao mogućnost da osporava pribavljene dokaze?
4. Značaj dokaza u postupku koji se ogleda u tome da li su dokazi o kojima je riječ bili odlučujući za ishod krivičnog postupka, i/ili da li su postojali drugi dokazi koji podržavaju optužnicu ili osuđujuću presudu?

Uzimajući u obzir te aspekte u cjelokupnoj procjeni pravičnosti postupka u odnosu na konkretan predmet i činjenice, važnost istrage i kažnjavanja za konkretno krivično djelo pažljivo će se razmotriti u odnosu na prava pojedinca da se dokazi protiv njega prikupe na zakonit način. Sud je naglasio da se „opći principi pravičnosti iz člana 6. primjenjuju na sve krivične postupke, nezavisno od toga o kojoj vrsti djela je riječ. Briga za javni interes ne može opravdati mjere koje poništavaju samu suštinu prava odbrane podnosioca predstavke... koja su garantirana članom 6. Konvencije“[52].

Kada je riječ o posebnim istražnim radnjama - pod kojima se, prije svega, podrazumijevaju tajni nadzor nad komunikacijama i korištenje prikrivenih istražitelja – možemo da se pozovemo na predmet *Ramanauskas protiv Litve*[53] pred Evropskim sudom. U tom predmetu Sud je uvažio teškoće sa kojima se suočava policija prilikom traženja i prikupljanja dokaza radi otkrivanja i istraživanja krivičnih djela. Kako bi obavila taj zadatak, policija sve više mora da koristi prikrivene istražitelje, doušnike i tajne istražne tehnike naročito u borbi protiv organiziranog kriminala i korupcije[54]. U skladu sa tim, upotreba posebnih istražnih metoda, posebno prikrivenih tehnika, sama po sebi ne predstavlja povredu prava na pravično suđenje. Međutim, zbog opasnosti od policijskog podsicanja koje takve tehnike uključuju, one moraju da se upotrebljavaju unutar jasno postavljenih okvira, kako ne bi došlo do povrede prava na pravično suđenje[55].

Kada razmatramo član 8. Konvencije i zakonitosti dokaza pribavljenih korištenjem posebnih istražnih mjera, postavljaju se pitanja da li je zadiranje u prava pojedinca u skladu sa zakonom, da li teži legitimnom cilju i da li je neophodno u demokratskom društvu? Da bi mjera bila „u skladu sa zakonom“, mora postojati pravni okvir koji je predvidljiv i koji osigurava zaštitu od proizvoljnog zadiranja u prava pojedinca. Kada je u pitanju „presretanje“ podataka prenesenih putem komunikacionih tehnologija, važno je razlikovati „masovno presretanje podataka“ i ciljano individualizirano presretanje. To razlikovanje utječe na minimalnu neophodnu zaštitu kako bi se spriječila zloupotreba ovlaštenja.

U dosadašnjoj praksi ESLJP je razvio nekoliko kriterija za zaštitu tajnog nadzora komunikacija, koji moraju biti propisani zakonom kako bi se spriječile zloupotrebe[56]. U tom smislu ESLJP

[52] *Ibidem*, stav 93.

[53] *Ramanauskas protiv Litvanije* [VV], predstavka broj 74420/01, presuda od 5. februara 2008. godine.

[54] *Ibidem*, stav 49.

[55] *Ibidem*, stav 51.

[56] *Huvig protiv Francuske*, predstavka broj 11105/84, presuda od 24. aprila 1990, *Kruslin protiv Francuske*, predstavka broj 11801/85, presuda od 24. aprila 1990, *Valenzuela Contreras protiv Španije*, predstavka broj 27671/95, presuda od 30. jula 1998, *Weber i Saravia protiv Njemačke*, predstavka broj 54934/00, odluka o prihvatljivosti od 29. juna 2006, i *Association for European Integration and Human Rights i Ekimdzhiev*, predstavka broj 62540/00, presuda od 28. juna 2007. godine.

ispituje da li domaće zakonsko rješenje jasno definira:

1. prirodu i vrstu krivičnih djela zbog kojih se može donijeti naredba o pretresu,
2. kategoriju lica čija se komunikacija može presresti,
3. ograničenje trajanja presretanja,
4. postupak za prikupljanje, korištenje i skladištenje prikupljenih podataka,
5. mjere opreza pri prenošenju podataka drugim stranama,
6. okolnosti u kojima se pribavljeni podaci mogu, ili moraju izbrisati ili uništiti.

Ako se dokazi prikupljaju u okviru ciljanog presretanja komunikacije zbog nacionalne sigurnosti, primjenjuje se šest istih minimalnih uvjeta, ali se dodaju još dva:

1. planovi za nadzor provođenja mjera tajnog nadzora,
2. mehanizmi za obavještavanje o presretnutoj komunikaciji i njenom sadržaju, kao i pravni lijekovi koji su predviđeni nacionalnim pravom.

U predmetu *Big Brother Watch protiv Ujedinjenog Kraljevstva [VV]*[57] Sud je pažljivo razmotrio razliku između ciljanih presretanja i masovnih presretanja podataka. Na prvom mjestu utvrđeno je da masovno i neusmjereno prikupljanje komunikacijskih podataka, uključujući i podatke o aktivnostima na Internetu, predstavlja kršenje prava na privatnost iz člana 8. Sud je naglasio da je potrebno da svako prikupljanje takvih podataka bude opravdano i proporcionalno.

Također je zaključeno da nedostatak adekvatnih pravnih mehanizama za zaštitu od zloupotrebe takvog nadzora predstavlja kršenje prava na privatnost. Sud je istaknuo da su postojali nedostaci u britanskom zakonodavstvu koji su omogućavali da se pristupi takvim podacima bez adekvatnih mjera kontrole i nadzora.

Presuda je, također, obuhvatila i pitanje pristupa stranih obavještajnih agencija obavještajnim podacima. Sud je zaključio da postojanje ovlaštenja da druge države pristupe takvim podacima mora biti podvrgnuto strogim i jasno definiranim ograničenjima kako bi se osigurala zaštita prava na privatnost.

Izazovi s kojima se suočavaju sudovi u Engleskoj i Velsu u vezi sa digitalnim dokazima

Nakon što su francuski i nizozemski istražitelji presreli komunikacijski sistem EncroChat i prenijeli prikupljene podatke vlastima Ujedinjenog Kraljevstva, sa izazovima u vezi sa digitalnim dokazima suočili su se i sudovi u Engleskoj i Velsu. Naime, naosnovu dostavljenih materijala, Nacionalna agencija za borbu protiv kriminala (NCA) pokrenula je operaciju *Venetic*[58], opsežnu kriminalističku istragu protiv više organiziranih kriminalnih grupa i teških krivičnih djela.

Sudija Krunskog suda u Kenterberiju Mark Weekes istakao je da su britanski sudovi pažljivo razmotrili pitanje zakonitosti dokaza dobijenih presretanjem komunikacije EncroChat. Posebna pažnja posvećena je i pitanju da li bilo eventualnih povreda zakona prilikom prijenosa tih podataka od Francuske.

Naime, u Ujedinjenom Kraljevstvu postoje zakoni koji zabranjuju da se koriste presretnuti materijali u telekomunikacijama. To je prvo bilo regulirano Zakonom o presretanju komunikacija iz 1985. godine, a kasnije su to regulirali Zakon o uređenju istražnih ovlaštenja (RIPA) iz 2000, te novi Zakon o istražnim ovlaštenjima iz 2016. godine.

[57] *Watch protiv Ujedinjenog Kraljevstva* [VV], predstavka broj 58170/13 i još 2, presuda od 25. maja 2021. godine.

[58] https://shorturl.at/kpuTX, pristupljeno: 10. juna 2023. godine.

U ovom slučaju jedno od ključnih pitanja bilo je kako tretirati poruke poslane putem aplikacije EncroChat u skladu sa Zakonom o istražnim ovlaštenjima iz 2016. godine. Te poruke su bile osnova za rad tužilaštva u konkretnom predmetu. Postojala je dilema da li se te poruke mogu pravilno smatrati materijalom na koji se odnosi nalog o ciljanom presretanju opreme (*eng. Targeted Equipment Interference warrant – TEI*), što bi ih činilo prihvatljivim kao dokaz, ili se te poruke moraju tumačiti kao dio naloga o ciljanom presretanju (*eng. Targeted Interception warrant – TI*), što bi ih činilo korisnim kao obavještajnim podacima, ali ne i prihvatljivim kao dokaz.

Na pripremnom ročištu sudija Dove je saslušao dokaze o toj temi i zaključio da „u vrijeme kada su poruke postale dostupne, one nisu 'bile prenošene'"[59], što znači da nisu bile presretnute. Optuženi su uložili žalbu tvrdeći da je sudija donio netačan zaključak. Nakon analize određenog broja dokaza i zakonskih aspekata, lord Burnett, predsjednik Vrhovnog suda, zaključio je da podaci u sistemu EncroChat nisu bili prenošeni u trenutku kada su bili preuzeti. Stoga se ti podaci mogu ispravno smatrati podacima koji su bili „pohranjeni u sistemu, ili pohranjeni od sistema (bilo prije, bilo poslije samog čina prijenosa)"[60].

Rezultat korištenja materijala prikupljenih putem aplikacije EncroChat je bilo donošenje 950 osuđujućih presuda do sada, uglavnom na osnovu priznanja krivice. Međutim, još oko 1.800 optuženih čeka suđenje u predmetima u kojima su dokazi iz sistema EncroChat ključni. Ta situacija je dovela do velikog kašnjenja u rješavanju predmeta, jer je bilo potrebno razjasniti pravna pitanja u vezi sa prihvatljivosti tih dokaza.

U vezi sa tim, nedavno je podnesena i predstavka ESLJP. Ujedno, u slučaju *A. L. i E. J. protiv Francuske* Evropski sud za ljudska prava prvi put će se baviti pitanjem da li je razmjena dokaza pribavljenih posebnim istražnim radnjama u skladu sa zakonom. S obzirom na to da se predmet trenutno razmatra pred Sudom, ostaje nam da čekamo ishod.

***

U kompleksnom digitalnom labirintu bh. pravosuđe se suočava sa brojnim pitanjima prihvatljivosti i zakonitosti prikupljanja i korištenja digitalnih dokaza. Tako, uspostavljanje ravnoteže između zaštite privatnosti i borbe protiv kriminala postaje sve zahtjevniji zadatak posebno u današnjem vremenu, kada enkripcija istovremeno štiti privatnost i podatke pojedinca i kompanije, ali služi i kao alat kriminalcima. Analiza pravnih standarda i prakse u BiH otkriva da je potrebno unaprijediti krivične procesne zakone i sudsku praksu kada je riječ o digitalnim dokazima i istragama. Štaviše, nepostojanje posebnih zakonskih odredaba koje bi definirale digitalne istrage i dokaze, u BiH otvara pitanje da li bi postojeće propisane istražne radnje bez međunarodne pravne pomoći bile dovoljne da bi se otkrila komunikacija koja se odvijala putem kriptiranih telefona?

Evropski sud za ljudska prava daje smjernice o faktorima koje treba uzeti u obzir tokom sudskih postupaka kao što su ocjena pravičnosti postupka, te razmatranje razlike između ciljanih i masovnih presretanja podataka radi sprečavanja zloupotrebe nadzora u kontekstu garancije prava na privatnost. Međutim, ključna pitanja ostaju: Kako pravosuđe može uspostaviti delikatnu ravnotežu između privatnosti i pravde u digitalnom dobu? Kako bh. pravni okvir i sudska praksa mogu odgovoriti na složene izazove koji se javljaju tokom prikupljanja i korištenja digitalnih dokaza? Kako bh. pravosuđe može osigurati integritet u borbi protiv organiziranog kriminala i korupcije u doba tehnologije koja se stalno razvija?

[59] Lord Burnett, predsjednik Vrhovnog suda, *Kruna protiv Murraya i drugih* [2023] EWCA Crim 282 (16. mart 2023. godine).

[60] *Ibidem*.