Intervju s Krešimirom Kamberom, Jurisconsult: Praksa Evropskog suda za ljudska prava – dokazi prikupljeni korištenjem kriptiranih aplikacija

Pripremile: Elma Veledar Arifagić i Azra Bećirović, AIRE Centar

Sadržaj komunikacija kriptiranih aplikacija (SKY/Anom) koji je pribavljen od strane tijela progona Republike Francuske dostavljen je tijelima Bosne i Hercegovine kao „informacija". Postupci u Bosni i Hercegovini su u fazi istrage, a korištenje kriptiranih aplikacija predstavlja temu o kojoj se razgovara kako u pravosuđu, tako i u široj javnosti. Sugovornik *Pravne hronike* na ovu temu je Krešimir Kamber, pravni savjetnik u Direkciji pravnih konsultacija pri Registru Evropskog suda za ljudska prava (Jurisconsult) i višegodišnji istraživač u oblasti zaštite ljudskih prava u krivičnom procesnom pravu.

Kada je u pitanju praksa Evropskog suda za ljudska prava (Sud), Kamber upućuje na predmete vezane za Tursku.

„Trenutno jedina praksa u vezi s kriptiranim aplikacijama su predmeti protiv Turske, a koji se odnose na određivanje pritvora zbog korištenja *ByLock* aplikacije. U predmetu *Üçdağ protiv Turske*[17] Sud je odlučio da sama činjenica postojanja instalirane aplikacije *ByLock* nije dovoljna za osnovanu sumnju određivanja pritvora, već moraju postojati još neki drugi određeni dokazi da bi se uopće radilo o osnovanoj sumnji," pojašnjava Kamber.

Premda je ova odluka vodeća u praksi po ovom pitanju, Kamber napominje da se trenutno pred Velikim vijećem vodi predmet u kojem se osporava korištenje aplikacija, tj. određenih presumpcija koje su stvorene u turskom sustavu za osude.

„Sad se ne razmatra predmet s aspekta članka 5 i određivanja pritvora, nego s aspekta članka 6 i korištenja takvih dokaza, odnosno takve presumpcije. Riječ je o predmetu *Yalçınkaya protiv Turske*[18]. Tu se radi o velikom broju aplikacija pred Sudom protiv Turske vezano uz te osude. Ogroman broj ljudi je osuđen u biti zbog toga što su imali tu aplikaciju instaliranu na telefonu, što je bilo dovoljno da im se odredi pritvor. Dakle, u biti je to za sada jedina praksa koja se odnosi na kriptirane aplikacije. Naravno, postoji praksa koja se bavi pitanjima pretrage mobitela, oduzimanja predmeta, zadiranja u privatnost, itd. Tu su problemi slični, ali nisu jednaki kao kod kriptiranih aplikacija," napominje Kamber.

No, koji se dokazi mogu prikupljati putem kriptiranih aplikacija, a koji ne?

„Naša praksa razlikuje standarde koji se odnose na *metadata* podatke i same sadržaje komunikacije. *Metadata* bi bila činjenica da su dva telefona određenog dana uspostavila kontakt, što je zaštićeno s aspekta članka 8 Konvencije, jer mora postojati jamstvo zaštite i proporcionalnost miješanja. Veća

[17] *Üçdağ protiv Turske*, presuda izrečena 25. maja 2021., predstavka br. 23314/19.

[18] *Yalçınkaya protiv Turske*, presuda izrečena 2. februara 2006., predstavka br. 14796/03.

zaštita je u situaciji kada se stvarno presretne sadržaj konkretnog razgovora. Tu su standardi još veći. Međutim, i u kontekstu zaštite s aspekta članka 8 uvijek se cijene zakonitost, nužnost miješanja, arbitrarnost u postupanju," dodaje Kamber.

Naš sugovornik nas upućuje na prava iz Evropske konvencije o ljudskim pravima koja mogu biti ugrožena prilikom postupanja.

„Prvo i primarno, postoji mogućnost ugrožavanja prava iz članka 8, a zatim i prava iz članka 6. Nadalje, vidimo da i kod određivanja pritvora dolazi do kršenja ljudskih prava s aspekta članka 5 stavke 1 i 3. Treba voditi računa i o tome da li je bila predvidiva osuda koja se temelji na korištenju kriptiranih aplikacija. Ovaj predmet koji je pred Velikim vijećem ispituje i članak 7. Pored navedenog, interesantno je da ukoliko se radi o novinarima, članak 10 garantira zaštitu novinarskog izvora. U predmetu *Big Brother Watch i drugi protiv Ujedinjenog Kraljevstva*[19] koji se odnosio na mogućnost da država može pretraživati ogroman broj informacija, postavilo se pitanje, ukoliko se radi o novinarima, da postoji i zadiranje u tajnost novinarskog izvora gdje moraju biti osigurana dodatna sredstva zaštite. Sud je u ovom predmetu pojasnio neophodne garantije kako bi se osigurala zaštita povjerljivog novinarskog materijala u skladu sa člankom 10."

„Dakle, kod zaštite novinarskih izvora podataka, mogu se očekivati komplicirane situacije, na primjer u situaciji da se nekom novinaru presretne komunikacija uspostavljena između dva telefona, a za koju se još uvijek nužno ne zna tko su vlasnici, i da se komunikacija nastavi kroz neko vrijeme, te da novinar prima podatke od neke kriminalne skupine, koje on onda objavljuje. Tu bi moglo doći do komplikacije i pitanja da li to predstavlja zaštitu novinarske tajne i na koji način izdvojiti podatak u pogledu kaznenog djela od novinarske komunikacije," ukazuje Kamber.

U pogledu međunarodnog karaktera pribavljanja dokaza naš sugovornik u nastavku ističe sljedeće: „Kad se radi o pribavljanju dokaza u inozemstvu, po mom mišljenju, nužno je voditi računa o zakonitosti njihovog pribavljanja u nacionalnom sustavu. Dakle, da postoje odgovarajuća jedinstvena pravila. Kad kažem „zakonitost", pri tome mislim ne samo na postojanje pravne norme, nego i na kvalitetu pravne norme, koja mora biti predvidiva, jasna, dostupna. Dakle, mora postojati zakonitost kod prikupljanja tog dokaza u nacionalnom sustavu, i onda kada je utvrđeno da postoji u nacionalnom sustavu, dolazimo do onog problema u vezi s principom *locus regit actum* ili *forum regit actum*. Da li će nacionalni sustav zauzeti stav da se zakonitost usmjeri prema zakonima države u kojima je radnja poduzeta – što bi bio princip *locus regit actum* – i u tom slučaju bi se u nacionalnom sustavu, gdje se provodi postupak, provela samo neka opća kontrola zakonitosti, ali više u smislu javnog poretka. Recimo, u slučaju javnog poretka BiH, cijenile bi se osnovne vrijednosti javnog poretka BiH, kao što su zaštita, pravo pojedinca, vladavina prava, itd. Dakle, ne bi se išlo u finese, na primjer da li je nalog trajao tri ili pet dana, ili da li ga je trebalo izdati jedno ili drugo tijelo, da li ga je trebalo dobro obrazložiti, itd. To bi već bilo ono što nacionalni sud u kojem se provodi postupak, kod *locus regit actum*, ne bi ispitivao."

Kamber ističe: „Evropska konvencija Vijeća Evrope o uzajamnoj sudskoj pomoći predviđa *locus regit actum*. Da li je ona zastarjela ili ne, to za sada možemo ostaviti po strani. Ono što je interesantno je da ta Konvencija predviđa *locus regit actum*, dakle da se procjenjuje na osnovu zakonitosti države u kojoj je radnja poduzeta. Ona ima prednost čak i nad bilateralnim ugovorima, koje bi države mogle imati. Ovo znači da se na temelju te Konvencije provodi međunarodna saradnja, preko koje se dobijaju dokazi. Interesantno je i to da čak i oni koji su u teoriji veliki pobornici *forum regit actum* kažu da u situaciji kada država naknadno, kao što je to ovdje slučaj, spontano od druge države dobije

[19] *Big Brother Watch i drugi protiv Ujedinjenog Kraljevstva* [Vv], presuda izrečena 25. maja 2021., predstavke br. 58170/13 i dvije druge.

informacije, tj. kada je stvar već gotova, ne može se retroaktivno zahtijevati da se dokazi pribave po pravilima države u kojoj se vodi postupak (*forum regit actum*). Dakle, u biti se mora „živjeti" s tim da su informacije sada tu i da se iz njih treba izvući najbolje što je moguće," zaključuje Kamber.

Ukratko, naš sugovornik dalje ističe da bi nacionalni sudovi u takvim situacijama trebali razmatrati zakonitost na jednom općem nivou, u smislu da ti dokazi nisu stvarno pribavljeni na način koji podriva javni poredak države u kojoj se vodi postupak. Bitno je istaći da, s aspekta Evropskog suda i članka 6, a osvrćući se na predmet *Stojković protiv Belgije i Francuske*[20], „postoji obaveza da se u kontekstu članka 6 prigovori odbrane uzmu u obzir, da se razmotre i da se na njih odgovori. Nacionalni sudovi ta pitanja neće moći samo ignorirati."

„Zakonitost bi morala biti ispitana, s tim da se postavlja pitanje u kojoj mjeri i u kojoj fazi postupka se ona procjenjuje, te u kojoj mjeri tijelo ulazi u procjenu. Kod pritvora su rokovi naprosto prekratki da bi se nadležni organ koji odlučuje o pritvoru mogao upuštati u detaljnu ocjenu zakonitosti, pogotovo kod ovako kompliciranih predmeta. Treba biti realan, neka osnovna osporavanja zakonitosti mogu trajati danima, mogu se izvoditi brojni dokazi, mogu se tražiti daljnji podaci putem međunarodne pomoći, ispitivati svjedoci, itd. Pri tome se odluka o pritvoru donosi u roku od 24 sata. Prema tome, po logici stvari, ne možemo u fazi odlučivanja o pritvoru očekivati da se odlučuje o svim detaljima zakonitosti. Isti princip se može primijeniti i na fazu u kojoj se pritvor produžava. Ovo znači da će nacionalni sustav sam odrediti u kojoj fazi će vršiti kontrolu zakonitosti. Nije od presudnog značaja da li će se kontrola zakonitosti vršiti u fazi potvrđivanja optužnice ili u kasnijoj fazi rasprave. S aspekta članka 6 takva pitanja ne bi bila toliko odlučujuća, jer se posmatra postupak kao cjelina," dodaje Kamber.

Kratko smo se osvrnuli na potrebu tehnološkog napretka, stručnosti i posjedovanja stručnih vještina organa gonjenja, počev od policijskih organa, preko sudova, do vještaka.

„Kad se gleda taj izvanredan sustav koji nazivamo **administriranje elektroničkih dokaza u postupku**[21], naročito onih koji su izdvojeni iz mobitela, možemo se osvrnuti na FORMOBILE projekat. U tom projektu prepoznato je 9 faza administriranja elektroničkih dokaza, od kojih se 6 odnosi na prethodni postupak. Ovo nam govori koliko je bitna stručnost, kako se nehajnim radnjama ne bi kompromitirala autentičnost i valjanost pribavljenih dokaza. Naravno, stavimo po strani da bi bilo kakve namjerne radnje tijela progona, kojima bi se modificirali neki dokazi, bile kazneno djelo. Međutim, može se naprosto dogoditi da se, nehajno, prilikom izručenja, ti dokazi na neki način kompromitiraju i to predstavlja realnu opasnost. Dakle, tijela progona bi morala biti osposobljena i vjerojatno bi morali postojati specijalizirani forenzički eksperti, tj. kompjuterski forenzičari, koji bi mogli retroaktivno procijeniti je li došlo do kompromitiranja, jer mi kao informatički laici bismo to teško mogli," napominje.

[20] *Stojkovic protiv Belgije i Francuske*, 27. oktobra 2011., predstavka br. 25303/08.

[21] Slika 1: Administriranje elektroničkih dokaza u postupku; *FORMOBILE Guidance to Checklist Preparation for Legal Practitioners* – Izvor: https://formobile-project.eu/downloads/publications-public-deliverables

Slika 1: Administriranje elektroničkih dokaza u postupku

Pitali smo i šta su budući izazovi u kontekstu rada pravosuđa s dokazima pribavljenim putem novih tehnologija.

„Cijeli niz tih pitanja se otvara s elektroničkim tehnologijama. Mislim da bi tu pravosuđe, ako želi biti barem ukorak s tim, trebalo predviđati i ići naprijed, pripremati se za neke buduće situacije, a što najčešće nije slučaj. Kad-tad će nam doći npr. pitanje da li se podaci pretraživanog mobitela nalaze u Americi ili su tamo gdje je i mobitel. S istim pitanjima će se susretati i boriti vrhovni sudovi i ustavni sudovi po cijeloj Evropi, te će biti potrebno da se zauzimaju neka stajališta. Mislim da pravosuđe trenutno ne razmatra takva pitanja, jer se nije susretalo s njima. Zatim, postoji i pitanje nekonzistentnosti. Na primjer, u američkim vrhovnim sudovima u pojedinim državama pojavilo se pitanje primjene zaštite od samooptuživanja u kontekstu prisile kod pretrage mobitela. Postavlja se pitanje da li se od osumnjičene osobe može zahtijevati da otvori mobitel i, ukoliko odbije, da li se može na to natjerati ili je dotična osoba zaštićena s aspekta slobode od samooptuživanja. Neki vrhovni sudovi u Americi su zauzeli stav da je osoba zaštićena, dok neki imaju stav da osobe nisu zaštićene u tom slučaju. U Nizozemskoj imamo slučaj gdje je osumnjičenom fizički uzeta ruka i stavljen prst na telefon kako bi se isti otključao, takva radnja otvara mnogo drugih pitanja. Tu bi se vjerojatno moralo raditi na daljnjoj edukaciji. Vjerujem da nam je svima potrebna dodatna edukacija u tom smislu," zaključuje intervju.