RADNA STUDIJA

DIGITALNI NADZOR U SRBIJI

Andrijana Ristić

BCBP Beogradski centar za bezbednosnu politiku

Jul 2023.

DIGITALNI NADZOR U SRBIJI

Izdavač:
Beogradski centar za bezbednosnu politiku (BCBP)
Đure Jakšića 6/5, Beograd, Srbija
www.bezbednost.org, office@bezbednost.org

Autorka:
Andrijana Ristić

Tiraž:
50

Jul 2023.

BCBP Beogradski centar za bezbednosnu politiku

Sadržaj

Uvod

Sve veće oslanjanje građana na digitalne tehnologije i uređaje uticalo je na to da države ali i privatni akteri sve više posežu za raznovrsnim sistemima i alatima za digitalni nadzor građana. Tako su kamere visoke rezolucije, veštačka inteligencija i programi za biometrijsko prepoznavanje, te alati za automatsko prikupljanje podataka sa interneta kao i intruzivni softveri za nadzor mobilnih telefona postali svakodnevna realnost građana širom sveta. Od ovog trenda nažalost ni Srbija nije izuzeta. Tako su domaći istraživački novinari ali i renomirane strane istraživačke organizacije poput Citizens Lab-a utvrdile da su bezbednosne institucije Srbije nabavljale brojne digitalne alate za nadzor građana, uključujući tu i one najintruzivnije, koji su sposobni za tajno infiltriranje i kontrolu digitalnih uređaja, kao i kamere visoke rezolucije koje se lako mogu opremiti softverom za prepoznavanje lica. Ali, ne samo da su bezbednosne institucije nabavljale programe i opremu za digitalni nadzor, već su to činile i one u čiju nadležnost ne spada staranje o nacionalnoj i javnoj bezbednosti, poput, na primer, javnog preduzeća Elektroprivreda Srbije (EPS), Ministarstva trgovine, turizma i telekomunikacija, odnosno tržišne inspekcije i poreske policije.

Širenje digitalnog nadzora u Srbiji je veoma netransparentno i posebno opasno u uslovima kda je Srbija ocenjena kao zarobljena država koju karakteriše zloupotreba državnih resursa zarad lično-partijskih interesa. Iako su ovi izveštaji medija i istraživačkih novinara važni, oni su usmereni na pojedinačne slučajeve te je na osnovu njih teško steći širu sliku o razmerama problema digitalnog nadzora u Srbiji. Zbog toga je važno, polazeći od postojećih izveštaja, mapirati infrastrukturu za digitalni nadzor u Srbiji, odnosno popisati koju su opremu i programe za digitalni nadzor državne institucije nabavljale, da li su one nadležne i ovlašćene da ih koriste, te kako se ove tehnologije zloupotrebljavaju. S obzirom da Srbija teži članstvu u Evropskoj uniji (EU), važno je prikazati i kako EU nastoji da reguliše ovu oblast.

Opis digitalnih tehnologija koje ugrožavaju privatnost građana u Srbiji

Kompanija **Huawei** sklopila je ugovor sa Ministarstvom unutrašnjih poslova o nabavci nekoliko hiljada kamera za pametni video nadzor 2020. godine. Međutim, ono što predstavlja problem jeste nedostatak informacija o tome kako ove kamere zapravo rade i koje informacije one prikupljaju. Postavljene kamere **IPC6625-Z30** i **IPC6225-VRZ-ES** pored toga što vrše video nadzor, takođe mogu da obavljaju i pametnu video analizu koja uključuje identifikaciju objekata, prepoznavanja ciljanih boja i vozila. Pored toga, prva kamera se izdvaja po tome što poseduje optički zum od 30x i infracrvenu lampu koja može da dostigne čak i do 150 metara i u uslovima smanjene vidljivosti, dok druga poseduje obe karakteristike u nešto manjem obimu.[1]

Treba usmeriti pažnju i na sistem za analizu **VCN3020** koji podatke sa pametnih kamera prikazuje u realnom vremenu u centrali, te poseduje i mogućnosti video-reprodukcije. Rezultati analize se zatim čuvaju u sistemu za skladištenje, OceanStore, a ukoliko je neophodna, dalja video analiza može da se ostvari upotrebom **VCM5020** sistem za analitiku, koji pored tradicionalnih načina video analize, koristi i biometrijsku tehnologiju za prepoznavanje lica i analizu ljudskog ponašanja, a sve u cilju identifikovanja osobe na snimku.[2]

Pegaz, sofisticirani program za praćenje, proizvod je još jedne Izraelske kompanije NSO Group. Ovaj špijunski softver sadrži najnapredniju tehnologiju ove vrste koja omogućava korisniku da hakuje nečiji telefon iz daljine, bez da žrtva to primeti. Pegaz može da pristupi kameri i mikrofonu, kao i svim podacima na telefonu uključujući poruke, pozive i elektronsku poštu. Softver ne zahteva od žrtve da klikne sumnjivi link, već bez ikakve interakcije inficira sistem koji napada. Britanski list Gardijan obavio je Projekat Pegaz koji je otkrio prisustvo ovog špijunskog softvera na čak 50 hiljada mobilnih uređaja, uključujući i telefon francuskog predsednika Emanuela Makrona. Brojni slučajevi zloupotrebe ovog špijunskog softvera dovele su do njegove zabrane širom sveta. Ministarstvo trgovine Sjedinjenih Američkih Država stavila je NSO grupu na crnu listu i zabranila trgovinu sa ovom kompanijom bez posebne dozvole, dok je američka kompanija Apple tužila NSO grupu zbog hakovanja njenih korisnika.[3] Mnoge vlade su zabranile kupovinu i posedovanje ovog softvera, a krajem 2022. godine to je učinila i Grčka. [4]

Circles, kompanija koja je povezana sa NSO grupom, takođe se bavi se izradom softvera za nadzor koji koriste slabosti mobilnih sistema u cilju praćenja poziva, poruka i lokacija telefona, bez potrebe da se hakuje uređaj. Klijenti ove kompanije su i pojedine države koje koriste ove tehnologije za kršenje ljudskih prava, a direktno je povezano korišćenje softvera od strane Kraljevske vojske Tajlanda koja je, sumnja se, mučila zatvorenike koji su najverovatnije bili privedeni pomoću ovog softvera.[5]

Cyberbit Solutions je Izraelska kompanija koja proizvodi moćni špijunski softver za hakovanje i špijuniranje računara koji funkcioniše tako što se žrtvi pošalje video link putem mejla, nakon aktiviranja linka špijunski softver se instalira bez znanja žrtve. Jednom kada ovaj softver dobije pristup računaru, on može da pristupi svim dokumentima i podacima koji se na njemu nalaze, nakon čega se posmatranje nastavlja i beleži se svaka nova aktivnost. Postoji nekoliko primera zloupotrebe ovog softvera, ali izdvaja se slučaj u kom je Etiopija vršila špijunske napade protiv Oromo disidenta van Etiopije, ali i protiv Eritrejskih kompanija i vladinih agencija koristeći ovaj softver.[6]

Predator je još jedan špijunski softver nalik Pegazu, koji hakuje telefon žrtve nakon čega dobija pristup svim informacijama na uređaju poput poruka, slika i sačuvanih šifri, a uzgred i pristupa kameri i mikrofonu preko čega špijunira žrtvu i prati pozive. Za razliku od Pegaza, Predator može da aktivira svoj špijunski softver samo ukoliko žrtva klikne na sumnjiv link. Proizvođač ovog softvera je kompanija Cytrox osnovana u Severnoj Makedoniji od strane izraelskih i mađarskih državljana.[7] Smatra se da Predator koriste mnoge vlade za špijuniranje novinara i opozicije. Opasnost od ovakvog softvera postala je poznata javnosti nakon slučaja u kom je Grčka vlada tajno slala novac kompaniji koja prodaje ovaj softver, a zvaničnici su priznali da su ga koristili za prisluškivanje bar jednog novinara i predstavnika Evropskog parlamenta bez sudskog naloga. Ova otkrića pratile su brojne ostavke samog vrha Grčke vlade i pojačane regulacije sličnih softvera.[8]

FinSpy je program za špijuniranje računara i telefona, proizveden od strane nemačkog konglomerata FinFisher-a, koji koristi bezbednosne propuste prilikom ažuriranja softvera kako bi „napao" ciljani uređaj. Jednom instaliran, program prikuplja sve podatke, vrši prisluškivanje poziva i prati lokaciju žrtve. FinFisher se prvi put pojavio u Turskoj 2017. godine, a mete su bili aktivisti koji su učestvovali u demonstracijama protiv vlade. Usled istrage nemačke vlade o poslovanju ove kompanije zbog nelegalne prodaje špijunskog softvera Turskoj vladi koja je povezana sa brojnim kršenjem ljudskih prava i sloboda, FinFisher je proglasila bankrot i obustavila svoje poslovanje.[9] Mnoge druge kompanije proizvode slične softvere i posluju na sličan način, te je dostupnost sličnih alata na tržištu veoma velika.

Cognyte je Izraelska kompanija koja proizvodi softvere za špijunažu koji imaju mogućnost da spajaju, analiziraju i vizualizuju veliki broj različitih skupova podataka u cilju pronalaska informacija i obrazaca ponašanja. Međutim, problem je u tome što ovaj softver često koristi lažne naloge na društvenim mrežama kako bi kroz prevaru izvukao potrebne podatke o žrtvama. Do sada, ovaj softver se uglavnom koristio za špijuniranje novinara, političkih protivnika i aktivista. Činjenica da je *Facebook* blokirao naloge ove kompanije na njihovim platformama ukazuje na opasnost od ovakvih i sličnih softvera[10]. Kompanija je takođe optužena da je njena tehnologija korišćena za masovno kršenje ljudskih prava u Mijanmaru.[11]

Griffeye Analyze, od švedske kompanije Griffeye, je softver za prepoznavanje lica i analizu video snimaka, koji tako prikupljene podatke upoređuje i povezuje sa drugim podacima na internetu[12]. Iako je primarna uloga otkrivanje i sprečavanju seksualne eksploatacije dece, ovaj moćni softver takođe može biti zloupotrebljen u svrhu sukobljavanja vlasti sa članovima opozicije ili aktivistima na protestima, što nije teško zamisliti bez jasnog zakonskog okvira koji ograničava korišćenje ovakvih tehnologija.

Hacking Team je bila italijanska kompanija sa sedištem u Milanu, koja se bavila proizvodnjom špijunskih softvera. Za bezbednosne službe širom sveta posebno su bili zanimljivi njihovi sistemi za daljinsku kontrolu koji su se zasnivali na ciljanom širenju virusa na računare i telefone kroz slanje zaraženih dokumenata čije je preuzimanje pokretalo instaliranje špijunskog softvera koji je dalje vršio prikupljanje podataka sa inficiranih uređaja. Pored početnih uspeha ove kompanije, zloupotreba softvera navela je haktivistu poznatog kao Finias Fišer da upadne u servere Hacking Team-a i objavi 400 gigabajta osetljivih podataka koji su otkrili da je kompanija prodavala svoj softver diktatorskim režimima, poznatim po masovnom kršenju ljudskih prava, dok su žrtve često bili novinari i aktivisti. Kompanija Hacking Team prestala je da postoji, odnosno druga kompanije za sajber bezbednost ju je kupila i preimenovala u Momento Labs.[13]

Trovicor je kompanija koja se bavi presretanjem i obaveštajnom tehnologijom. Poseduje opremu za zakonito presretanje preko specijalizovanih monitoring centara koji mogu da presreću telefonske pozive, SMS poruke i celokupan Internet saobraćaj, takođe poseduje i sisteme za efikasnu obradu i analizu velikog broja podataka. Oprema koju prodaje Trovicor u prošlosti je obeležena kao alat kojima pojedine vlade vrše masovno kršenje ljudskih prava, pa je tako *Privacy International* podneo tužbu protiv kompanije zbog prodaje ove opreme vladi Bahreina koja je istu koristila kako bi špijunirala aktiviste za ljudska prava.[14] Na opasnost proizvoda ove kompanije ukazali su Reporteri bez granica, označivši Trovicor kao „neprijatelja interneta".[15]

Maltego je Nemačka kompanija koja proizvodi platformu za istraživanje koja omogućava korisniku da putem integrisanih i kupljenih baza podataka, kao što je recimo i Social Links, crta po praznom dokumentu tako što pokazuje ko je sa kim povezan, formira veze, grafikone i mape, ali i prati *online* aktivnosti meta. Ova platforma može da mapira i do milion entiteta po istrazi, odnosno 64 hiljade entiteta po zadatoj komandi[16]. Maltego sadrži i besplatne opcije, ali one omogućavaju pristup mnogo manjem broju podataka nego neke naprednije verzije koje uključuju i kupljene baze podataka poput Maltego One ili Maltego Enterprise koji je namenjen za firme i institucije.

Social Links, modul u sklopu Maltego platforme, služi za prikupljanje i analiziranje podataka sa interneta i društvenih mreža. Ovi alati su napravljeni tako da mogu da pronađu identitet osobe sa slike i pronađe tačno sa kojim ljudima je ta osoba povezana i kakva je priroda tog odnosa koristeći softvere za prepoznavanje lica. Smatra se da Social Links ima sposobnost da zadire i u privatne prepiske na društvenim mrežama i da pronađe nečiji broj telefona čak i kada korisnici sakriju podatke te vrste[17].

Ovakvi alati izazivaju veliki stepen opreza, a informacije koje se preko njih mogu dobiti imaju veću vrednost od informacija koje se mogu dobiti tradicionalnim načinima špijuniranja poput prisluškivanja ili video nadzora.

Mozenda je nezavisan program za automatsko izvlačenje podataka sa veb stranica tzv. „veb skrejper". Program ima i mogućnost da menja IP adresu kako bi izbegao da bude blokiran od strane servera, tokom neodobrenog preuzimanja tekstualnog, vizuelnog sadržaja i dokumenata[18].

Clearview AI je američka kompanija koja proizvodi softvere za prepoznavanje lica. Poseduju najveću bazu podataka na svetu od preko 30 milijardi slika koje su preuzete sa interneta, uključujući i slike sa društvenih mreža sa kojih prikupljaju podatke. Njihov softver za prepoznavanje lica ima 99% tačnosti u svim kategorijama, uključujući starosne, polne i rasne. Zbog intruzivnosti ovog softvera, u mnogim državama širom sveta uključujući i u Kanadi, Australiji, Francuskoj, Italiji i Velikoj Britaniji, podnete su tužbe protiv ove kompanije kako bi se sprečilo prikupljanje podataka o ljudima na ovaj način, bez njihove dozvole. U nekim slučajevima, kompaniji je naloženo samo da obriše biometrijske podatke o stanovnicima, dok su Italija i Velika Britanija otišle korak dalje i pored toga kaznili Clearview AI od 10 do 20 miliona evra. Švedska je kaznila svoje policijske snage zbog nezakonitog korišćenja ovog softvera.[19] Do danas, Clearview AI je bio predmet preko 15 pravnih i regulatornih radnji, a taj broj se iz godine u godinu povećava. Kompaniji je zabranjeno da prodaje svoje usluge i u većini američkih kompanija, nakon što je Američka unija za građanske slobode (ACLU) tužila Clearview AI na sudu u Ilinoisu zbog kršenja zakona o privatnosti.[20] Opasnost od zloupotrebe ovog softvera je velika, a sve više država se bori protiv njegove upotrebe.

Sistem socijalnih karata

Sistem masovnog digitalnog nadzora putem veštačke inteligencije uveden je u Srbiji kroz program socijalnih karata koji prati aktivnost pojedinaca (pristupa se podacima iz državnih evidencija) i njihovih kontakata sa drugim ljudima, na osnovu čega izračunava mogući prihod i samim tim određuje da li je neko na spisku za socijalnu pomoć ili ne. Ceo proces je automatizovan tako da ukoliko se pojedinac potpuno ne uklapa u parametre koji su postavljeni, ispada iz sistema socijalne zaštite. Ovim sistemom su posebno pogođeni pripadnici romske zajednice čiji su minimalni dodatni prihodi od prodavanja sekundarne sirovine dovoljni da ih algoritam izbriše sa spiska. Od početka primene ove tehnologije, socijalnu pomoć je izgubilo preko 22000 građana Srbije[21].

Pored diskriminacije, veliki problem predstavlja i to što sistem neprekidno prikuplja ogromne količine podataka o građanima, te ugrožava njihovo prava na privatnost. Tako, sistem socijalnih karti prikuplja preko 130 podataka o korisnicima i njihovim bližnjima koristeći algoritam čiji način funkcionisanja nije poznat javnosti, a informacija o tome se čuva pod izgovorom zaštite nacionalne bezbednosti. Interesantna je i činjenica da sistemu nedostaje i adekvatan vid zaštite i kontrole, jer je prilikom njegove

izrade izostala adekvatna procena rizika. Takođe, u Zakonu o socijalnim kartama izostalo je i definisanje specijalnih mera koje bi sprečile izvoz podataka i deljenje sa trećim stranama.[22] Sličan sistem je bio aktivan nekoliko godina u Holandiji, ali je zabranjen je odlukom Okružnog suda u Hagu početkom 2020. godine upravo zbog nedostataka koje ima i ovaj u Srbiji. Sve u svemu, postojeći sistem socijalnih karata predstavlja alat za sistemsku diskriminaciju ugroženih grupa i uskraćivanje socijalne pomoći pod velom „objektivnosti" algoritma i još jedan vid masovne kontrole građana koji zarad primanja neophodne socijalne pomoći, moraju da se odreknu svog prava na privatnost.

Data centar Kragujevac

Podaci srpskih građana i institucija od 2020. godine smešteni su u Državnom data centru u Kragujevcu, a 2022. godine otvoren je još jedan objekat koji čuva podatke vojske, policije i Bezbednosno-informativne agencije, u sklopu kojeg se nalazi i prva državna platforma za veštačku inteligenciju.[23] U celu inicijativu Srbija je uz pomoć Svetske banke uložila 55 miliona evra i smatra se da su podaci vrlo dobro zaštićeni i od fizičkih i od sajber napada.[24] Vlada je osnovala Data cloud technology doo koja se nalazi u potpunom vlasništvu države i koja obavlja komercijalne poslove.[25] U sklopu Državnog data centra nalaziće se i regionalni centar kineske kompanije „Huawei" za skladištenje podataka za južnu i jugoistočnu Evropu, dok je Narodna Republika Kine data centru donirala opremu iste kompanije u vrednosti od 2 miliona evra.[26]

Međutim, iako ova inicijativa ima podršku stručnjaka i međunarodnih organizacija, može biti problematična činjenica da se Državni data centar nalazi u ograđenom dvorištu objekta u kojem radi odeljenje Bezbednosno-informativne agencije u Kragujevcu. Danilo Savić, direktor preduzeća Data cloud technology doo Kragujevac, ukazuje da je lokaciju bilo jako teško pronaći, te da nisu ni razmišljali o ovom problemu. On takođe dodaje i da pripadnici odeljenja BIA u Kragujevcu neće imati pristup objektima koji čuvaju podatke građana i da će pristup podacima morati da dobiju na drugi način.[27] Uzimajući u obzir brojne slučajeve u kojima su radnici BIA i policije, kao i drugih državnih organa davali osetljive podatke pojedincima u medijima i iz političkih partija, teško je poverovati u ovu tvrdnju. Koncentracija podataka na jednom mestu olakšava njenu zaštitu ali i olakšava njihovu upotrebu u različite svrhe, uključujući tu i nadzor i kontrolu građana o čemu svedoče digitalne autokratije poput Kine.

Naziv tehnologije	Tip tehnologije	Opis tehnologije	Vrsta nadzora	Institucije koje koriste tehnologiju	Status tehnologije
IPC6625-Z30	Pametne kamere	Obavljaju video nadzor, poseduju sposobnosti pametne video analize (identifikacija objekata, prepoznavanje ciljanih boja i vozila). Poseduje optički zum 30x i in-fracrvenu lampu koja doseže i do 150m	Masovni nadzor	MUP (2020)	Aktivna
IPC6625-Z30	Pametne kamere	Obavljaju video nadzor, poseduju sposobnosti pametne video analize (identifikacija objekata, prepoznavanje ciljanih boja i vozila). Poseduje optički zum 30x i infracrvenu lampu koja doseže i do 150m	Masovni nadzor	MUP (2020)	Aktivna
VCN3020	Sistem za analizu	Prikazuje podatke sa pametnih kamera u realnom vremenu, poseduje sposobnost video-reprodukcije i naprednu analizu (bio-metrijski nadzor za pre-poznavanje lica i analizu ljudskog ponašanja)	Masovni nadzor	MUP (2020)	Aktivna
Griffeye Analyze	Sistem za analizu	Softver za prepozna-vanje lica i analizu video snimaka, koji tako prikupljene podatke upoređuje i povezuje sa drugim podacima na internetu	Targetirani nadzor	MUP (2021)	Aktivna
Cognyte	Sistem za analizu podataka	Spaja, analizira i vizualizuje veliki broj različitih skupova podataka u cilju pronalaska informacija i obrazaca ponašanja.	Targetirani nadzor	Ministarstvo trgovine, turizma i tele-komunikacija (2021)	Aktivna
Maltego	Sistem za istraživanje na internetu	Omogućava korisniku da kroz istraživanje baza podataka napravi vizuelni prikaz sa kim je sve žrtva povezana, zatim kreira mape i grafikone, ali i prati online aktivnost meta. Platforma može da mapira i do milion entiteta po istrazi.	Targetirani nadzor	MUP, Tržišna inspekcija, Poreska uprava	Aktivna

Naziv tehnologije	Tip tehnologije	Opis tehnologije	Vrsta nadzora	Institucije koje koriste tehnologiju	Status tehnologije
Social Links	Sistem za istraživanje podataka na internetu	Služi za prikupljanje i analiziranje podataka sa interneta i društvenih mreža. Može da pronađe identitet osobe sa slike i tačno sa kojim ljudima je ta osoba povezana i kakva je priroda tog odnosa koristeći softvere za prepoznavanje lica. Smatra se da može da zadire u privatne prepiske i pristupi informacijama koje drugim korisnicima nisu vidljive.	Targetirani nadzor	Tržišna inspekcija, Poreska uprava	Aktivna
Mozenda	Sistem za istraživanje podataka na internetu	Služi za automatsko izvlačenje podataka sa veb stranica tzv. „veb skrejping“	Targetirani nadzor	Tržišna inspekcija	Aktivna
Clearview AI	Sistem za analizu	Služi za prepoznavanje lica i poseduje najveću bazu podataka na svetu od preko 30 milijardi slika koje su preuzete sa interneta, uključujući i slike sa društvenih mreža sa kojih prikupljaju podatke	Targetirani nadzor	MUP (2020)	?
Circles	Špijunski softver	Koristi slabosti mobilnih sistema u cilju praćenja poziva, poruka i lokacija telefona, bez potrebe hakovanja uređaja	Targetirani nadzor	BIA (2015) - test	?
Cyberbit Solutions	Špijunski softver	Služi za hakovanje i špijuniranje računara tako što se žrtvi pošalje video link putem mejla, nakon aktiviranja linka špijunski softver se instalira bez znanja žrtve. Prikuplja sve podatke sa uređaja	Targetirani nadzor	Predstavili proizvode u Srbiji	?
Trovicor	Špijunski softver	Služi za za zakonito presretanje preko specijalizovanih monitoring centara koji mogu da presreću telefonske pozive, SMS poruke i celokupan internet saobraćaj, takođe poseduje i sisteme za efikasnu obradu i analizu velikog broja podataka	Targetirani nadzor	Policijska Služba za borbu protiv organizovanog kriminala (2010)	?

Naziv tehnologije	Tip tehnologije	Opis tehnologije	Vrsta nadzora	Institucije koje koriste tehnologiju	Status tehnologije
Hacking Team	Špijunski softver	Služi za hakovanje na daljinu i prikupljanje podataka sa hakovanih uređaja	Targetirani nadzor	BIA, Ministarstvo odbrane (2012)	?
FinSpy	Špijunski softver	Koristi bezbednosne propuste prilikom ažuriranja softvera kako bi „napao“ ciljani uređaj. Jednom instaliran, program prikuplja sve podatke, vrši prisluškivanje poziva i prati lokaciju žrtve	Targetirani nadzor	BIA (2015)	X
Predator	Špijunski softver	Služi za hakovanje telefona žrtve nakon čega se dobija pristup svim informacijama na uređaju poput poruka, slika i sačuvanih šifri, a uzgred i pristupa kameri i mikrofonu preko čega špijunira žrtvu i prati pozive	Targetirani nadzor	Otkriveno korišćenje u Srbiji	?
Pegaz	Špijunski softver	Softver sadrži najnapredniju tehnologiju ove vrste koja omogućava korisniku da hakuje nečiji telefon iz daljine, bez da žrtva to primeti. Pegaz može da pristupi kameri i mikrofonu, kao i svim podacima na telefonu uključujući i porukama, pozivima i elektronskoj pošti. Softver ne zahteva od žrtve da klikne sumnjivi link, već bez ikakve interakcije inficira sistem.	Targetirani nadzor	Otkriveno korišćenje u Srbiji	?

Tabela 1. Prikaz digitalnih tehnologija čije testiranje i upotreba su otkriveni u Srbiji

Neefikasnost digitalnog nadzora

Vlade širom sveta pravdaju uvođenje biometrijskog nadzora i špijunskih softvera argumentom da ove tehnologije značajno doprinose u borbi protiv raznih oblika kriminala. Međutim, ovaj argument je prevaziđen i koristi se kako bi stanovništvo, pod uticajem straha za sopstvenu bezbednost, lakše prihvatilo uvođenje novih mehanizama (digitalne) kontrole. Ovo je slučaj i sa Srbijom. Međutim, prvenstveno treba utvrditi da li su ove tehnologije stvarno toliko korisne u otkrivanju i sprečavanju kriminala, s obzirom da se ocena njihove efikasnosti do sada više zasnivala na poverenju, a ne toliko na realnim dostignućima.

Istraživanja pokazuju da ove tehnologije, a posebno masovni biometrijski nadzor, pored toga što ugrožavaju privatnost stanovništva, nisu efikasne u sprečavanju kriminala i terorizma. Pre svega, sistemi masovnog nadzora svake sekunde skeniraju okolinu i prikupljaju ogromnu količinu raznih podataka, a inspektorima je često teško da u moru informacija izdvoje značajne od nepotrebnih. Analiza terorističkih napada širom sveta pokazala je da masovni nadzor nije efikasan u prevenciji nasilnih zločina i da se ovi slučajevi rešavaju pomoću klasičnih istraživačkih metoda i ljudske inteligencije. Američka Nacionalna obaveštajna agencija je na Bostonskom maratonu, održanom 2013. godine, vršila masovni nadzor i uprkos tome, dva brata neprimetno su podmetnula i detonirala dve bombe blizu cilja, ubivši troje. Čak i u procesu potere za počiniocima, relevantne informacije dolazile su od stranih vlada i od pregledanja slika i snimaka napravljenih od strane privatnih lica. Takođe, braća su bila na listi posmatranja - *TIDE*, ali uprkos tome što je američka obaveštajna agencija pratila njihovu komunikaciju, nije uspela da otkrije teroristički plan[28].

Ilustrativan je i slučaj Roberta Džulijan-Borčak Vilijamsa koga je policija Detroita pogrešno uhapsila 2020. godine zbog sumnje da je počinio krivično delo krađa imovine. Glavni dokaz protiv njega bila je fotografija sa video nadzora koja je provučena kroz softver za prepoznavanje lica, čime je softver identifikovao Vilijamsa kao počinioca. Međutim nakon hapšenja i ispitivanja osumnjičenog policija je otkrila da je softver pogrešno identifikovao Vilijamsa.[29] Ovde možemo primetiti dva problema. Prvi je taj što sistemi za prepoznavanje lica mogu da pogreše, pogotovo ako se radi o ljudima druge rase, jer je sistem najprecizniji kada su u pitanju beli muškarci. Drugi problem jeste taj što se policija u ovim slučajevima oslanjala samo na informacije koje pružaju ove tehnologije, a ne na tradicionalne istraživačke metode.

Kada govorimo o Srbiji, jedan od poznatijih slučajeva kada su napredne tehnologije bile nedovoljne za otkrivanje počinioca krivičnih dela jeste slučaj ubistva jednog od lidera kosovskih Srba, Olivera Ivanovića 2018. godine. I pored velikog broja kamera koje su postavljene u blizini mesta ubistva, do danas nisu pronađeni snimci koji bi mogli biti korišćeni za pronalazak počinioca. Takođe, interesantna je i činjenica da su na tom području nadležni pripadnici srpske policije i bezbednosnih službi[30]. I pored svih ovih dostupnih alata, ovaj slučaj ostao je nerešen.

Zloupotrebe digitalnih tehnologija za nadzor

Najveća opasnost od implementacije masovnog biometrijskog nadzora i sistema za analizu, kao i špijunskih softvera jeste to što postoji velika mogućnost njihove zloupotrebe, pogotovo kada je neke od ovih tehnologija, poput izraelskog špijunskog softvera Pegaz ili Predator, skoro nemoguće detektovati. Državne institucije najčešće zloupotrebljavaju ove tehnologije njihovim korišćenjem u svrhu vršenja nadzora nad političkim protivnicima, aktivistima i novinarima. Ove zloupotrebe su veoma važne u državama sa polu-demokratskim i nedemokratskim sistemima, jer ona može da dovede u opasnost slobodu i živote političkih protivnika vlasti. Tako su, na primer, u Rusiji slučajevi zloupotrebe biometrijskog nadzora prilično česti, a broj slučajeva je znatno povećan nakon Ruske invazije na Ukrajinu. Ove tehnologije koriste se radi identifikacije lica koja učestvuju na protestima protiv vlasti, a od skora najveće mete predstavljaju upravo aktivisti koji učestvuju u antiratnim protestima i novinari koji pišu kritičke tekstove protiv Putinovog režima. Učešće ovih ljudi u protestima često se kažnjava privođenjem, zadržavanjem ili hapšenjem, nakon što ih jedna od preko 3000 biometrijskih kamera snimi i identifikuje. Situacija sa zloupotrebom ovih tehnologija se pogoršava, a ruska policija je od nedavno počela da preventivno privodi aktiviste i novinare u periodu neposredno pre održavanja važnih događaja, ili u slučaju kada su planirani veliki antiratni protesti. Istraga Rojtersa je pokazala da je biometrijski nadzor igrao značajnu ulogu u hapšenju nekoliko stotina političkih neistomišljenika.[31]

Čak i u demokratskim državama sa dobrim pravnim sistemom i dugom pravnom tradicijom vladavine prava, možemo pronaći slučajeve zloupotrebe. U Sjedinjenim Američkim Državama, Njujorška policija je priznala da je koristila softvere za prepoznavanje lica kako bi identifikovala aktiviste koji su učestvovali na „Black Lives Matter“ protestima povodom ubistva Džordža Flojda od strane policijskih službenika 2020. godine. U jednom slučaju, policija se pojavila na vratima Davida Ingrama, 28-ogodišnjeg aktiviste i učesnika protesta, nakon što ga je softver za prepoznavanje lica identifikovao. Policija je tvrdila da se softver koristio samo na slici koja je uzeta sa uličnih video kamera, ali očevici koji su se okupili ispred Ingramove kuće su tvrdili da se policija koristila slikom sa društvenih mreža, što predstavlja prekoračenje predviđenih ograničenja Njujorške policije. Njujorška policija koristi Clearview AI od 2011 godine, te je vrlo verovatno da je upravo ovaj softver za prepoznavanje lica korišćen.[32] Od sličnih zloupotreba nije bila imuna ni Austrija, gde je policija koristila sistem za biometrijski nadzor za identifikaciju demonstranata.[33]

Srbija

Od ovakve vrste zloupotreba ni Srbija nije imuna, pa je nezakonito praćenje i prisluškivanje postalo svakodnevnica sa kojom žive opozicioni političari, aktivisti i novinari u Srbiji. Nezakonito prikupljene informacije često završavaju u rukama predstavnika vladajućih partija, ali i urednika provladinih medija. Takozvana afera „Vulingejt“[34], nastala početkom 2020. godine nepobitno je dokazala ovu praksu. Naime, ministar odbrane

Aleksandar Vulin je govoreći za „Tanjug“ oštro kritikovao autorski tekst Dragana Šutanovca, bivšeg ministra odbrane i aktuelnog člana jedne opozicione partije, koji je napisan za „Nedeljnik“. Međutim, sam tekst još uvek nije bio objavljen i postojao je samo u imejl prepisci između Šutanovca i Veljka Lalića, glavnog urednika „Nedeljnika“. Smatra se da su ti podaci jedino mogli biti dostupni ukoliko su Šutanovac ili Lalić, ili čak obojica, bili pod nadzorom, te su bezbednosne službe presrele njihovu prepisku. Iz ministarstva su tvrdili da je do greške došlo u njihovoj PR službi, te da su oni mislili na tekst tabloida „Kurir“, a ne „Nedeljnika“. O ovom slučaju odlučivao je Odbor za kontrolu službi bezbednosti, koji je nakon vanredne kontrole Vojno-bezbednosne agencije, jednoglasno usvojio da VBA nije primenjivala posebne postupke i mere kojima bi se mogli prikupiti podaci iz međusobne komunikacije. Bitno je i napomenuti da se u Odboru za kontrolu službi bezbednosti u to vreme nije nalazio ni jedan opozicioni političar, kao i činjenicu da je međunarodna medijska organizacija „Reporteri bez granica“ javno pozvala vlast da dalje istraži ovaj događaj[35].

Samo u maju 2023. godine, desila su se još dva slična slučaja zloupotrebe posebnih mera i postupaka. Prvi slučaj desio se početkom maja, kada je glavni urednik tabloida „Informer“ tokom gostovanja na televiziji „Pink“ ekskluzivno otkrio da urednik Mreže za istraživanje kriminala i korupcije (KRIK), Stevan Dojčinović, već pet meseci sprema tekst u saradnji sa američkom medijskom organizacijom „The New York Times“, u kom se klan Veljka Belivuka povezuje sa državom i da će taj tekst biti objavljen narednog dana. Dojčinović je ubrzo nakon toga odgovorio na tviteru da je informacija tačna, ali se pitao kako je urednik Informera došao do te informacije i da li je opet u pitanju bila „saradnja“ sa službama bezbednosti.[36]

Sredinom maja Informer je objavio članak u kom se još jednom ekskluzivno otkriva vest da će britanski list „Gardijan“ objaviti članak u kom se kritikuje vlast predsednika Aleksandra Vučića, a da će im sagovornici biti „srpski hejteri iz NVO“, odnosno predstavnici Beogradskog centra za bezbednosnu politiku (BCBP) i Biroa za društvena istraživanja (BIRODI). Nameće se ovde pitanje odakle Informeru ova informacija tri dana pre objavljivanja članka i da li je ovo opet slučaj nelegalnog prisluškivanja novinara i istraživača.[37]

Ista situacija ponovila se i tokom majskih protesta „Srbija protiv nasilja“, kada su se aktivisti zapitali da li ih vlast prisluškuje nakon što je predsednik Vučić objavio da će aktivisti tokom protesta blokirati most Gazelu, iako ta informacija nije bila poznata javnosti, već se o toj opciji razgovaralo dan ranije, na štabu protesta.[38] Da su aktivisti pod digitalnim nadzorom ukazao je i događaj iz 2021. godine kada je u Novom sadu održan jedan od brojnih ekoloških protesta. Pripadnici ekološkog pokreta „Eko Straža“ primetili su da ih pojedini učesnici snimaju svojim telefonima, koristeći posebne softvere za prepoznavanje lica. Njihov strah donekle je i potvrđen činjenicom da su pojedinim građanima, na kućnu adresu, stizali prekršajni nalozi zbog učešća u blokadi saobraćajnice, iako ih niko na protestu nije legitimisao. Zakon dozvoljava pripadnicima policijskih snaga da snimaju javni skup uz prethodnu najavu, ali korišćenje biometrijskog nadzora ne spada u njihova ovlašćenja i ozbiljno narušava privatnost građana. Ovaj slučaj zloupotrebe biometrijskog nadzora protiv političkih protivnika, ostao je nerasvetljen.

Nadležnosti i ovlašćenja državnih institucija za digitalni nadzor

Državne institucije u Srbiji su nabavljale digitalne programe i tehnologije za nadzor građana što međutim nije ispraćeno promenom zakonskog okvira. Postavlja se onda pitanje zakonitosti upotrebe ovih softvera i alata odnosno da li su one nadležne i ovlašćene da ih primenjuju. Zbog toga ćemo u ovom delu rada prikazati nadležnosti i ovlašćenja državnih institucija Srbije koje su nabavljale digitalne tehnologije za nadzor građana.

Bezbednosno-informativna agencija

U odnosu na drugu regulativu koja reguliše rad državnih institucija koje su nabavljale tehnologije za digitalni nadzor, Zakon o Bezbednosno-informativnoj agenciji sadrži najpreciznije odredbe koje uređuju njihove nadležnosti i ovlašćenja. Kako stoji u članu 9 „Agencija u obavljanju poslova iz svoje nadležnosti primenjuje odgovarajuće operativne metode, mere i radnje, kao i odgovarajuća operativno-tehnička sredstva kojima se obezbeđuje prikupljanje podataka". Zakonom je definisano kada se mogu koristiti posebne mere, ko ih odobrava, kao i dužina njihovog trajanja. Posebne mere podrazumevaju tajni nadzor i snimanje komunikacije *bez obzira na oblik i tehnička sredstva preko kojih se obavlja ili nadzor* elektronske ili druge adrese, tajni nadzor i snimanje komunikacije na javnim mestima i mestima kojima je pristup ograničen ili u prostorijama, statistički elektronski nadzor komunikacije i informacionih sistema u cilju pribavljanja podataka o komunikaciji ili lokaciji korišćene mobilne terminalne opreme, *računarsko pretraživanje već obrađenih ličnih i drugih podataka i njihovo upoređivanje sa podacima koji su prikupljeni primenom mera*, i tajni nadzor i snimanje mesta, prostorija i predmeta, uključujući i uređaje za automatsku obradu podataka i opreme na kojoj se čuvaju ili se mogu čuvati elektronski zapisi (Zakon o BIA, član 13). Zakon međutim ne spominje mogućnost upotrebe biometrijskog nadzora i obrade podataka.

Iako Zakon o Bezbednosno-informativnoj agenciji preciznije određuje odredbe koje se tiču nadležnosti i ovlašćenja u odnosu na druge slične zakone, ova određenja i dalje nisu dovoljno jasna. Prvi problem nalazimo u članu 2 u kojem je oblast delovanja definisana vrlo široko i odnosi se na zaštitu bezbednosti Republike Srbije i ustavnog poretka. Ovakva definicija, bez daljeg preciziranja, daje odrešene ruke pripadnicima Agencije da široko tumače šta je sadržina nacionalne bezbednosti, što stvara prostor za zloupotrebe. Propust predstavlja i nedostatak odredbi o prikupljanju i obradi podataka korišćenjem biometrijskih tehnologija i digitalnih alata za nadzor.

Vojnobezbednosna agencija

Vojnobezbednosna agencija, slično kao i Bezbednosno informativna agencija, nešto preciznije uređuje poslove i nadležnosti nego što to čine drugi zakoni. U okviru bezbednosne zaštite Ministarstva odbrane i Vojske Srbije, VBA, između ostalog, otkriva, istražuje i prikuplja dokaze za određena krivična dela, zatim prikuplja, analizira, obrađuje i procenjuje kontraobaveštajne podatke iz svoje nadležnosti (Zakon o Vojno bezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, član 6). VBA je ovlašćena da prikuplja podatke primenom posebnih postupaka i mera kada se podaci ne mogu prikupiti na drugi način ili je njihovo prikupljanje u vezi sa nesrazmernim rizikom po život i zdravlje ljudi i imovinu, odnosno sa nesrazmernim troškovima (Zakon o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, član 11). U članu 12 navode se posebni postupci i mere tajnog prikupljanja podataka iz nadležnosti VBA uz korišćenje "tehničkih sredstava". Međutim, u daljem tekstu zakona nigde nije definisano šta su to tehnička sredstva, a neke odredbe i dalje su preširoko određene.

Policija

Zakon o policiji sadrži vrlo *opšte odredbe* o zaštiti građana i otkrivanju i rasvetljavanju krivičnih dela i ne pominje se korišćenje ovih i sličnih tehnologija (Zakon o policiji, član 30). Nešto su detaljnije odredbe u Zakon o krivičnom postupku. Dokazne radnje protiv lica uključuju proveru računa i sumnjivih transakcija putem informacija koje dostavljaju banke i druge finansijske institucije (Zakon o krivičnom postupku, član 143). Posebne dokazne radnje poput tajnog nadzora komunikacije i tajnog praćenja ovlašćene su da preduzimaju policija, BIA i VBA (Zakon o krivičnom postupku, članovi 166-173). Računarsko pretraživanje podataka po ovlašćenju sprovode policija, BIA, VBA, ali i carinske, poreske ili druge službe ili drugi državni organ koji na osnovu zakona vrši javna ovlašćenja (Zakon o krivičnom postupku, članovi 178-180).

Poreska uprava

Poreska uprava ima, između ostalog, nadležnost da prikuplja dokaze u poreskom postupku i to raznim sredstvima uključujući i „*svako drugo sredstvo* kojim se činjenice mogu utvrditi" (Zakon o poreskom postupku i poreskoj administraciji, član 43). Poreska uprava dalje pruža poreske usluge, vrši poresku kontrolu i sprovodi radnje u cilju otkrivanja poreskih krivičnih dela (poreska policija). Poreska policija postupa kao organ unutrašnjih poslova i ovlašćena je da, u skladu sa zakonom, preduzima *sve potražene radnje, izuzev ograničenja kretanja* (Zakon o poreskom postupku i poreskoj administraciji, član 135). Bez daljeg pojašnjenja, ovakvo definisanje ostavlja prostor za zloupotrebu biometrijske tehnologije.

Tržišna inspekcija

Zakon o inspekcijskom nadzoru određuje inspekciju kao organ u sastavu, unutrašnja organizaciona jedinica ili inspektori organa državne uprave, odnosno organa autonomne pokrajine ili jedinice lokalne samouprave ili drugog subjekta sa javnim ovlašćenjima, koja vrši inspekcijski nadzor (Zakon o inspekcijskom nadzoru, član 3). Inspekcija prikuplja podatke i prati i analizira stanje u oblasti inspekcijskog nadzora koja je u njenom delokrugu. Ti poslovi uključuju prikupljanje i analizu podataka dobijenih pomoću kontrolnih listi, vođenjem anketa i istraživanja javnog mnjenja i *drugim neposrednim prikupljanjem podataka*, što je prilično opširna odredba (Zakon o inspekcijskom nadzoru, član 8).

Tržišnu inspekciju i tržišne inspektore uređuje Zakon o trgovini, ali u njemu se ne navodi da postoji mogućnost tržišne inspekcije da koristi sofisticirane biometrijske tehnologije. Ovlašćenja tržišnog inspektora su prilično široko određena, a između ostalog uključuju i fotografisanje, vršenje video-snimanja prostora u kojem se vrši nadzor, odnosno robe i drugih predmeta koji su predmet nadzora, prikupljanje podatka relevantnih za predmet nadzora i zahtevanje pomoć od policije ili komunalne milicije (Zakon o trgovini, član 48). Radi obezbeđenja dokaza u Zakonu se samo navodi da tržišni inspektor može privremeno oduzeti određenje predmete (Zakon o trgovini, član 64).

***

Nakon prikaza nadležnosti i ovlašćenja državnih organa koji su u koristili, koriste i/ili su izrazili interesovanje za korišćenje špijunskih softvera, biometrijskog nadzora i drugih intruzivnih tehnologija, jasno je da su njihova ovlašćenja i nadležnosti određeni dosta široko. Čak i onda kada su detaljnije ispisane posebne mere kao u Zakonu o BIA, svrha upotrebe je određena preširoko te obuhvata zaštitu bezbednost i ustavnog poretka Republike Srbije kao i istraživanje, prikupljanje, obradu i procenu podataka bez daljeg pojašnjenja na koji način i kojim alatima je ovo predviđeno. Ne postoje, dakle, odredbe koje jasno ukazuju da BIA ili VBA mogu da koriste biometrijsku obradu podataka kao i digitalne tehnologije za nadzor. Nedovoljno jasne zakonske odredbe ostavljaju prostor za zloupotrebu i za prekoračenje ovlašćenja koja bi ovi organi trebalo da imaju. Tehnologija se razvija veoma brzo, dok zakoni ostaju isti. Usled pojave sve intruzivnijih i pristupačnijih tehnologija, neophodna je izmena zakona i preciziranje odredba u njima kako bi pravni sistem više odgovarao trenutnom stanju u zemlji i EU čijem članstvu Srbija teži.

Regulacija biometrijskog nadzora u EU

Članstvo u Evropskoj uniji (EU) je (i dalje) prioritet politike Srbije, te u tom pogledu ima obavezu da pravni okvir usklađuje sa regulativom u EU. Zbog toga je važno kako je EU uredila oblast biometrijskog nadzora i obrade podataka, odnosno kako će ga urediti u narednom periodu, te u kojoj meri Srbija odstupa od EU regulative. Na narednim stranama ćemo dati kratki prikaz i analizu ove oblasti u EU.

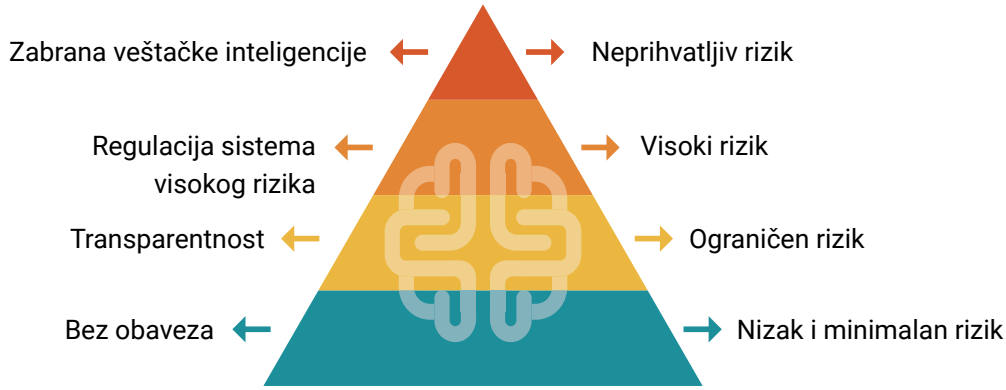
Evropska Unija uređuje polje biometrijskog nadzora u nekoliko različitih dokumenata od kojih su najznačajniji Povelja EU o osnovnim pravima (CFR), Generalna uredba o zaštiti podataka EU (GDPR) i Policijska direktiva (LED). Pored toga, pojavila se i inicijativa da se zakonodavstvo u ovom polju objedini u posebnom Predlogu zakona o veštačkoj inteligenciji koji je sredinom juna odobren velikom većinom u Evropskom parlamentu, a o budućnosti zakona dalje odlučivaće se kroz takozvane „trijaloge", pregovore između Evropskog parlamenta, Evropske Komisije i Saveta ministara.

Povelja uređuje oblasti prava na privatnost, prava na zaštitu podataka, kao i oblast koja se bavi borbom protiv diskriminacije. Prema odredbama GDPR i LED, procesuiranje slika lica mora da se vrši u skladu sa zakonom i principom proporcionalnosti, a procesuiranje takođe mora biti transparentno i pravedno, odnosno nediskriminatorno. Pored toga, podaci se analiziraju samo u specifične, eksplicitne i legitimne svrhe što znači da predviđena svrha mora biti formulisana dovoljno precizno da lice čiji se podaci obrađuju može da predvidi svrhu za koju će se njeni podaci obrađivati. I u ovom slučaju treba da se ispuni princip proporcionalnosti, zaštite podataka, ali i drugih uslova kao što su osnovana sumnja i ograničena pretraga.

Evropska komisija je 2020. godine objavila Beli papir o veštačkoj inteligenciji koji je predlagao određivanje specifičnih situacija u kojima bi bilo dozvoljeno vršiti biometrijski nadzor. Grupa eksperata na visokom nivou EU za veštačku inteligenciju zalagala se za jasniju definiciju veštačke inteligencije, kao i da se jasnije odredi kada i kako ona sme da se koristiti za razlikovanje identifikovanja ljudi od pronalaženja i praćenja ljudi, kao i razlikovanje ciljanog od masovnog nadzora. Evropski parlament tražio je ograničavanje softvera za prepoznavanje lica u nekoliko navrata, prvo u vidu potpunog moratorijuma na korišćenje sistema za prepoznavanje lica na javnim mestima od strane organa javnih vlasti, u zdravstvenim i obrazovanim ustanovama, kao i moratorijuma na korišćenje ovih sistema od strane policijskih snaga.

Evropska komisija 2021. godine objavila je Predlog akta o veštačkoj inteligenciji koji se tiče korišćenja veštačke inteligencije i rizika koji nastaju usled toga. Ovaj dokument nalaže zabranu naročito štetne prakse veštačke inteligencije koje su u suprotnosti sa vrednostima Unije, a koje manipulišu ljudsko ponašanje kroz korišćenje tehnika podsvesne komunikacije i sistema društvenog bodovanja i socijalnih karata. On takođe klasifikuje sisteme veštačke inteligencije prema nivou rizika na sisteme neprihvatljivog,

visokog, ograničenog i niskog ili minimalnog rizika. Sistemi neprihvatljivog rizika potpuno su zabranjeni, sistemi visokog rizika zahtevaju regulaciju, dok su sistemi ograničenog rizika uslovljeni su transparentnošću, za sisteme niskog ili minimalnog rizika nisu određene obaveze. Evropski parlament je usvoji ovaj predlog 14. juna 2023. godine.



Akt o veštačkoj inteligenciji klasifikovaće različite sisteme veštačke inteligencije prema nivou rizika. Slika: Evropska Komisija

Dijagram 1. Predlog akta o veštačkoj inteligenciji i tretman različitih vrsta rizika

Predlog sadrži pooštrene kriterijume klasifikacije alata veštačke inteligencije, prema kojima će niz aplikacija biti zabranjen za upotrebu na teritoriji EU, kao na primer:

- sistemi biometrijske identifikacije u realnom vremenu u javnim prostorima,
- biometrijski sistemi kategorizacije prema ličnim svojstvima kao što su rod, rasna i etnička pripadnost, verska i politička orijentacija,
- prediktivni policijski sistemi zasnovani na profilisanju,
- sistemi za prepoznavanje emotivnih stanja, odnosno njihova upotreba u policiji, na graničnim prelazima, radnom mestu i u obrazovnim institucijama,
- automatizovano prikupljanje biometrijskih podataka sa društvenih mreža ili snimaka sigurnosnih kamera.

Biometrijska identifikacija dozvoljena je samo i isključivo u slučajevima istraga ozbiljnih krivičnih dela uz odobrenje suda.[39] Zakon treba da reguliše sisteme za generisanje sadržaja, predikcija, preporuka ili odluka koje utiču na okruženja – uključujući alate za interakciju sa ljudima, kao što je *ChatGPT,* pametne sisteme za nadzor ili aplikacije koje se mogu koristiti za generisanje tzv. *deepfake* sadržaja.[40]

O budućnosti zakona raspravljaće Evropski parlament, Evropska Komisija i Savet ministara kroz takozvani „trijalog“ gde će se suprotstaviti stavovi država članica koje

smatraju da su ovakvi sistemi korisni u borbi protiv kriminala, i eksperata za ljudska prava koji smatraju da biometrijski nadzor ne mora automatski da donese i veću bezbednost. Ukoliko bude odobren, zakon će verovatno stupiti na snagu najranije 2025. godine.[41] Ovaj zakon će imati veliki uticaj na pravne sisteme širom sveta u oblasti regulacije veštačke inteligencije, kao jedan od prvih koji uređuje ovu materiju.

Takođe, ovaj akt je značajan za budućnost regulacije veštačke inteligencije u Srbiji, pogotovo u svetlu predlaganih rešenja sadržanih u Nacrtu zakona o unutrašnjim poslovima, čija je namera bila da legalizuju primenu biometrijskog nadzora. U slučaju da EU usvoji akte o veštačkoj inteligenciji, masovna upotreba biometrijskog nadzora u Srbiji bi bila u suprotnosti sa pravnim sistemom EU sa kojim se Srbija usklađuje kako bi ostvarila uslov za članstvo.

Izvori i beleške

1 Marko Crnjanski, „Sve je više Huawei kamera na beogradskim ulicama – čemu služe i da li prepoznaju tvoje lice?“, *Netokracija,* June 17, 2020, https://www.netokracija.rs/huawei-kamere-beograd-171048.

2 Ibid.

3 Dana Priest, Craig Timberg and Souad Mekhennet, “Private Israeli spyware used to hack cellphones of journalists, activists worldwide”, *The Washington Post*, July 18, 2021, https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/ .

4 „Greece passes intelligence bill banning the sale of spyware“, *The Guardian*, December 9, 2022, https://www.theguardian.com/world/2022/dec/09/greece-passes-intelligence-bill-banning-the-sale-of-spyware.

5 Bill Marczak, John Scott-Railton, Siddharth Prakash Rao, Siena Anstis, and Ron Deibert, “Running in Circles, Uncovering the Clients of Cyberespionage Firm Circles”, *Citizen Lab,* December 1, 2020, https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

6 Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert, “Champing at the Cyberbit, Ethiopian Dissidents Targeted with New Commercial Spyware”, *Citizen Lab,* December 6, 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/#:~:text=This%20report%20describes%20how%20Ethiopian,PhD%20student%2C%20and%20a%20lawyer..

7 Aleksa Tešić, „Izraelski softveri za špijunažu: Građani Srbije na meti Predatora“, *Birn*, March 3, 2022, https://birn.rs/izraelski-softveri-za-spijunazu-gradani-srbije-na-meti-predatora/.

8 Moira Lavelle, „Reporters dig up more links between Greek government and spyware“, *Al Jazeera,* November 17, 2022, https://www.aljazeera.com/news/2022/11/17/reporters-dig-up-more-links-between-greek-government-and-spyware.

9 „Munich-based tech company FinFisher is dissolved after investigations“, *ECCHR,* https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/.

10 Ibid.

11 Sing, Evie Kim, “Israel’s Cognyte embroiled in Myanmar in spyware scandal”, *Identity week,* January 16, 2023, https://identityweek.net/israels-cognyte-embroiled-in-myanmar-in-spyware-scandal/.

12 Griffeye, accesed June 5, 2023, https://www.griffeye.com.

13 Lorenzo Franceschi-Bicchierai, „Hacking Team Founder: ‘Hacking Team is Dead’“, *VICE,* May 26, 2020, https://www.vice.com/en/article/n7wbnd/hacking-team-is-dead.

14 Privacy International et al. vs. Trovicor, *OECD*, accessed June 5, 2023, https://www.oecdwatch.org/complaint/privacy-international-et-al-vs-trovicor/.

15 „Uvoz i upotreba opreme za nadzor u Srbiji: Slučaj Trovicor“, *Share foundation,* November 28, 2013, https://resursi.sharefoundation.info/sr/resource/uvoz-i-upotreba-opreme-za-nadzor-u-srbiji-slucaj-trovicor/.

16 Aleksa Tešić, „Softveri za obradu ličnih podataka, potencijalna pretnja po privatnost građana“, *Birn*, June 3, 2022, https://birn.rs/softveri-za-obradu-licnih-podataka-potencijalna-pretnja-po-privatnost-gradana/.

17 Ibid.

18 Ibid.

19 "About ClearviewAI's mockery of human rights, those fighting it, and the need for EU to intervene." *Reclaim your face,* March 28, 2022, https://reclaimyourface.eu/about-clearviewai-mockery-human-rights-those-fighting-eu-interveen/.

20 James Clayton and Ben Derico, "Clearview AI used nearly 1m times by US police, it tells the BBC." *BBC,* March 27, 2023, https://www.bbc.com/news/technology-65057011.

21 Natalija Jovanović and Dušan Komarčević, "Digitalizacija bede u Srbiji: Skinuti sa pomoći jer prodaju sekundarne sirovine", *Radio Slobodna Evropa,* November 29, 2022, https://www.slobodnaevropa.org/a/srbija-socijalne-karte-algoritam/32153869.html.

22 Ibid.

23 „Otvoren drugi objekat Državnog data centra u Kragujevcu." *RTS,* July 7, 2022, https://www.rts.rs/lat/vesti/drustvo/4877424/otvoren-drugi-objekat-drzavnog-data-centra-u-kragujevcu.html.

24 Marko Crnjanski, „Ekskluzivno: Posetili smo Državni data centar u Kragujevcu od 14.000m² – jedan od najmodernijih u ovom delu Evrope", *Netokracija,* February 4, 2021, https://www.netokracija.rs/data-centar-kragujevac-180295.

25 Marijana Avakumović, „Američke i kineske kompanije čuvaju podatke u Kragujevcu", *Politika*, March 5, 2022, https://www.politika.rs/scc/clanak/501173/Americke-i-kineske-kompanije-cuvaju-podatke-u-Kragujevcu.

26 Brane Kartalović, „Data-centar u dvorištu BIA", *Politika*, October 30, 2019, https://www.politika.rs/scc/clanak/440891/Data-centar-u-dvoristu-BIA

27 Ibid.

28 Jennifer Stisa Granick, "Mass Spying Isn't Just Intrusive---It's Ineffective", *Wired,* March 2, 2017, https://www.wired.com/2017/03/mass-spying-isnt-just-intrusive-ineffective/.

29 Kashmir Hill, „Wrongfully Accused by an Algorithm." *The New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

30 Slobodan Maričić, „Kosovo i Oliver Ivanović, četiri godine kasnije: Kada će biti rešeno ubistvo jednog od lidera kosovskih Srba." *BBC*, January 16, 2022, https://www.bbc.com/serbian/lat/srbija-59998523.

31 Lena Masri, "Facial recognition is helping Putin curb dissent with the aid of U.S. tech." *Reuters,* March 28, 2023, https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/.

32 James Vincent, „NYPD used facial recognition to track down Black Lives Matter activist", *The Verge*, August 18, 2020, https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

33 Andreea Belu, "Evidence: Biometric mass surveillance in EU", *LinkedIn*, April 6, 2021, https://www.linkedin.com/pulse/evidence-biometric-mass-surveillance-eu-andreea-belu/.

34 "Afera "Vulingejt": Kako je ministar pročitao neobjavljeni tekst u Nedeljniku?", *Nedeljnik*, February 2, 2020, https://www.nedeljnik.rs/afera-vulingejt-kako-je-ministar-procitao-neobjavljeni-tekst-u-nedeljniku-citajte-u-novom-broju/.

35 „Skupština Srbije: VBA nije prisluškivala Šutanovca i urednika lista Nedeljnik", *Radio Slobodna Evropa*, February 21, 2020, https://www.slobodnaevropa.org/a/30447609.html.

36 „Stevan Dojčinović: Priča o Belivuku i vlastima izlazi sutra u Njujork Tajmsu, ali odakle to Vučićević zna?", *Danas*, May 2, 2023, https://www.danas.rs/vesti/politika/stevan-dojcinovic-prica-o-belivuku-i-vlastima-izlati-sutra-u-njujork-tajmsu-ali-odakle-to-vucicevic-zna/.

37 „Informer četiri dana ranije otkrio ko su sagovornici Gardijana u tekstu o Vučiću", *N1*, May 16, 2023, https://n1info.rs/vesti/informer-cetiri-dana-ranije-otkrio-ko-su-sagovornici-gardijana-u-tekstu-o-vucicu/.

38 Ibid.

39 „Čekajući evropski zakon o AI: široka zabrana biometrije i prediktivnih policijskih sistema.“, *Share foundation*, May 26, 2023, https://www.sharefoundation.info/sr/cekajuci-evropski-zakon-o-ai-siroka-zabrana-biometrije-i-prediktivnih-policijskih-sistema/.

40 Ibid.

41 Masha Borak, “EU Parliament approves AI Act amid heated biometrics debates”, *Biometric update*, June 4, 2023, https://www.biometricupdate.com/202306/eu-parliament-approves-ai-act-amid-heated-biometrics-debates.

BCBP Beogradski centar za bezbednosnu politiku

bezbednost.org