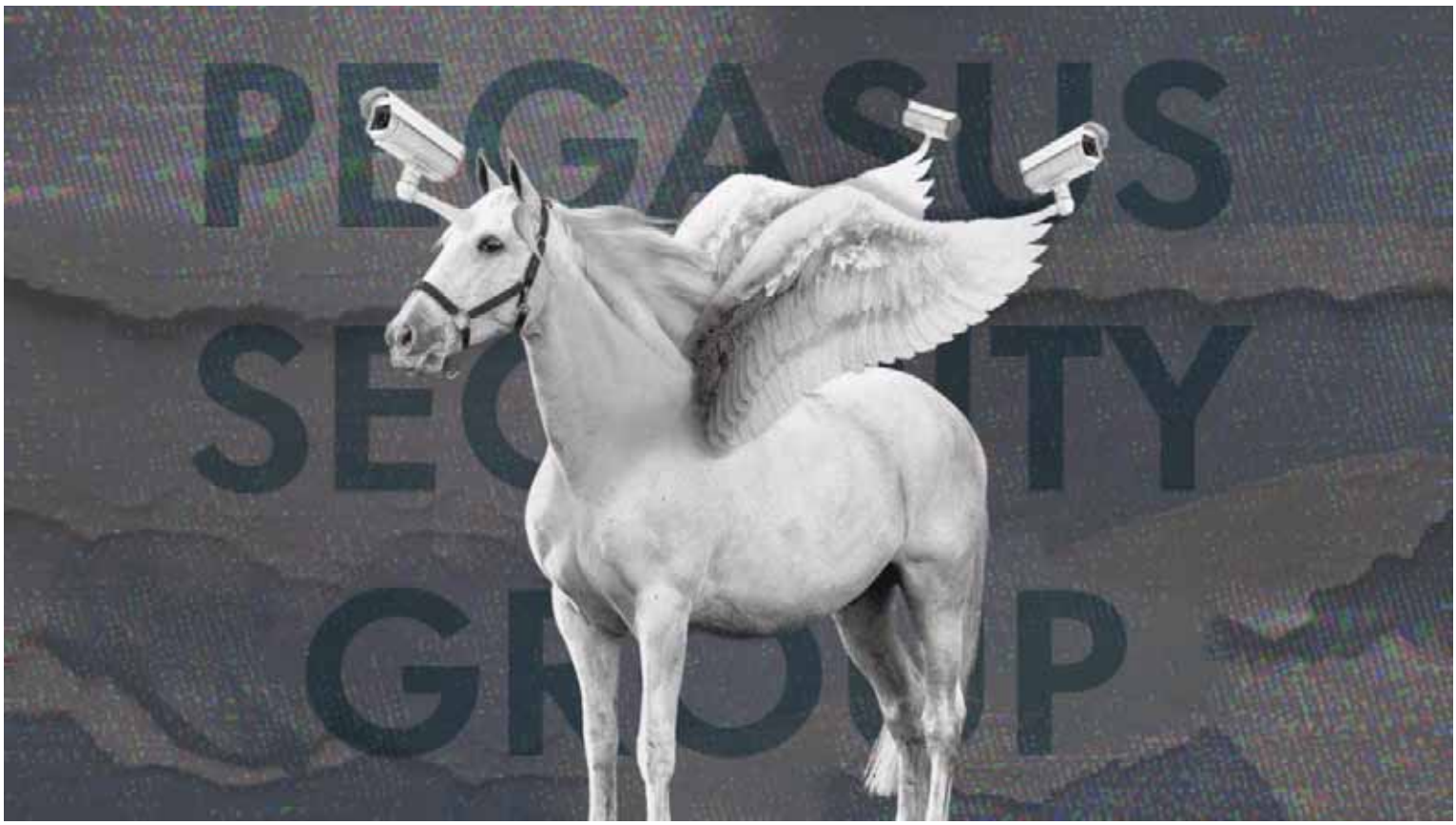
Tehnologija i demokracija (3): Zlatno doba špijuniranja i nadziranja

Autor/ica: Velibor Mandić 16 prosinca, 2022(https://faktograf.hr/2022/12/16/)

U trećem dijelu serijala "Tehnologija i demokracija" analiziramo opasnosti nadzora kojeg je omogućila tehnologija.



Ilustracija: Jordi Ilić / Faktograf

Ne bismo vas željeli plašiti ili vam uvaljivati neku paranoju, ali jeste li baš sto posto sigurni da vas neka državna tajna služba sada ne gleda i ne sluša putem vašeg zaraženog telefona ili nekog drugog tehnološki naprednog uređaja u kući, uredu ili automobilu? Sjećate li se telefonskog poziva s nepoznatog broja na koji niste ni odgovorili? Možda se upravo tada instalirao neki *spyware*, nevidljiva špijunska aplikacija koja vam, da toga niste niti svjesni, potpuno samostalno rovari po emailovima, profilima, porukama i fotografijama.

Pametni telefon vam se nekad čudno ponaša, ništa se ne otvori kada tapnete na zaslonu, baterija se brzo prazni, telefon se pregrijava, odjednom troši podatkovnog prometa više od očekivanog, treba mu dugo da bi se isključio? Sve to ponekad se događa kod većine telefona, ali ako ste aktivist, novinar, političar, kriminalac, imućniji pojedinac, trebate znati da ste ponešto zanimljiviji za nadzor i špijuniranje, ne samo u tamo nekim totalitarnim režimima već i u našim vrlim demokracijama.

Spyware svuda, spyware oko nas

Špijunski softver (spyware) kupuju službe iz mnogih demokratskih država i naveliko prisluškuju, no vrlo je teško utvrditi koliko tim postupcima sustavno narušavaju ljudska prava jer se o svemu sazna tek kada izbiju neke afere poput onih sa spywareom Pegasus i njegove upotrebe u, primjerice, demokratskoj Španjolskoj.

Barem 65 osoba u Kataloniji i Baskiji, pokrajinama koje prijete odcjepljenjem od Španjolske, nije imalo pojma da im je telefon zaražen (https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/) sofisticiranim Pegasusom izraelske proizvodnje, a radi se o članovima EU parlamenta, katalonskim političarima, sucima i članovima organizacija civilnog društva.

Potom je objavljeno (https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware) da su i španjolski premijer i ministrica obrane koristili zaražene telefone, te je krenula istraga koja bi trebala utvrditi tko u sigurnosno-obavještajnim službama odlučuje o tako opsežnim političkim špijunažama bez precizne demokratski utvrđene procedure.

Pegasus je pronađen (https://www.theguardian.com/news/series/pegasus-project) i na telefonima mnogih političara i novinara, među ostalim u Francuskoj i Mađarskoj, a u Sjedinjenim Državama FBI je tvrdio da ga neće upotrebljavati, što je pobio (https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html?) New York Times predočavajući dokumente (https://int.nyt.com/data/documenttools/nso-fbi-document/c6a146297cb8e21c/full.pdf) koji potvrđuju da su agenti itekako bili zainteresirani za takvu vrst sofisticiranog špijuniranja.

Nema stopostotne zaštite

Digitalni špijunski alat Pegasus proizvod je izraelske tvrtke NSO Group koja se reklamira kao pomagač vladama u održavanju javne sigurnosti, te odupiranju od terorizma, kriminala i globalnih prijetnji, s cijenama licenci u milijunima dolara, zajamčenim vrhunskim špijuniranjem i brzom instalacijom u kojoj žrtva nema gotovo nikakvih šansi za zaštitu. Pegasus se naime, u najboljim danima uvlačio u telefon bez da korisnik bilo što klikne – bilo je dovoljno tek da se telefonu uputi poziv koji je mogao ostati i neodgovoren. Proizvođači najpoznatijih operativnih sustava, za iPhone i Android pametne

telefone, poručuju da kontinuirano rade na zaštiti od špijunskih napadača, no punu zaštitu teško mogu zajamčiti jer dobri programeri znaju da zapravo nema uređaja koji se ne može hakirati, s obzirom na to da sve ovisi samo o sposobnosti i upornosti hakera.

Pegasus je inače tek jedan od brojnih alata koji mogu raditi što ih volja kada se uvuku u telefon, među ostalim uključivati kameru i mikrofon.

Špijuni hvale i Paragon (https://www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/?sh=7e53fb78153b) koji također stiže iz Izraela i koji je u stanju provaliti u šifriranu komunikaciju na aplikacijama poput WhatsApp, Signal, Facebook Messenger ili Gmail, a na balkanskim prostorima dika i uzdanica je proizvod tvrtke osnovane (https://balkaninsight.com/2022/01/06/wine-weapons-and-whatsapp-a-skopje-spyware-scandal/) u Skopju, prigodno nazvan Predator, koji je već u upotrebi u Srbiji, Grčkoj, Armeniji, Egiptu, Indoneziji i drugim državama.

U Grčkoj je izbila prilična frka (https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html) oko Predatora jer je pronađen na telefonima novinara i oporbenjaka, no tamošnja Vlada tvrdi da nema ništa s tim, iako potiho priznaje ostvarene kontakte s tvrtkom koja je isti spyware pokušala uvaliti Ukrajini. Na samom početku rata Ukrajina je, naime, željela nabaviti Pegasus ali je izraelska vlada to blokirala (https://www.nytimes.com/2022/03/23/us/politics/pegasus-israel-ukraine-russia.html), kao i u slučaju Estonije, jer se izbjegava zamjerati Rusiji. Potom su Ukrajinci razmatrali i ponudu za Predator, ali su od nje, prema dosad dostupnim podacima, odustali.

Saznati točno tko što od opisane tehnologije po svijetu koristi je teško jer sve ponude, pregovori, narudžbe i isporuke odvijaju se potiho i kroz zaobilazne kanale, tako da je istraživačima potrebno prilično vremena i živaca kako bi došli do barem malo podataka.

Autokrat u telefonu i wc-školjci

Industrija špijunskih digitalnih alata je izvan kontrole i dobro joj ide uništavanje demokratskih standarda i institucija, među ostalim i zato što se spyware, kako kaže (https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert) kanadski profesor **Ronald Deibert**, često koristi s ciljem hakiranja oporbe uoči izbora – takvi slučajevi su zabilježeni u Poljskoj i Indiji. Kao jedan od najpoznatijih boraca protiv neregulirane digitalne špijunaže, Deibert u tekstu (https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert) pod naslovom "Autokrat u vašem iPhoneu – kako plaćenički spyware ugrožava demokraciju," poziva na donošenje striktnih zakonskih odredbi prije nego što situacija izmakne kontroli i ugrozi demokratske poretke. On, naime, smatra da opasnost za

demokraciju postaje ozbiljna zato što su elite u nekoj državi u stanju svu raspoloživu modernu špijunsku tehnologiju upotrijebiti kako bi neutralizirale političku oporbu, utišale kritičare, potkopavale neovisno novinarstvo i provodile samovolju bez ikakvih posljedica.

Radi se o igri mačke i miša koju je gotovo nemoguće zaustaviti jer naše digitalne uređaje, kojih je sve više, uvijek će netko pokušati hakirati i dočepati se dragocjenih informacija. Što god se spaja (https://www.washingtonpost.com/technology/interactive/2022/amazon-smart-home/) na mrežu potencijalna je meta hakera – pametni zvučnici, televizori, kamere na ulaznim vratima i sigurnosni sustavi, termostati, pametne žarulje, digitalni satovi, robotski usisivači prašine, napredne bežične slušalice i wc školjka (https://www.cnbc.com/2019/01/08/kohlers-7000-numi-2point0-toilet-with-amazon-alexa-built-in.html) s ugrađenim zvučnicima, ambijentalnom rasvjetom, grijanom daskom i povlačenjem vode pomoću glasovne naredbe. U našem domu smo se zapravo već potpuno okružili uređajima koji nas mogu danonoćno špijunirati i nekome slati prikupljene podatke.

Nasmiješi se, kamera te snima

Čim izađemo, na nekom bi nas uglu u kadar mogla uhvatiti kamera i pomoću tehnologije prepoznavanja lica povezati da smo neki dan bili i na stadionu gdje smo, dok smo grleno navijali, usnimljeni pomoću sofisticiranih sustava za nadzor i identifikaciju na velikim okupljanjima. Možda imamo peh da su nam crte lica sumnjive i budemo uhićeni za krađu čarapa u dućanu, premda smo zapravo bili u bolnici gdje nam se rađalo dijete. Upravo takav slučaj se dogodio (https://gizmodo.com/facial-recognition-cops-police-sole-basis-arrests-study-1849859483) u New Yorku prije četiri godine gdje je policajac u potrazi za lopovom para čarapa uključio bazu podataka s licima, usporedio s nadzornom snimkom iz trgovine i bio uvjeren da je našao krivca.

Greške zbog nesavršenosti digitalnih identifikacija lica ne događaju se rijetko i nevinim građanima mogu nanijeti mnogo štete, te im narušiti prava na privatnost i jednakost pred zakonom, kažu (https://mcusercontent.com/672aa4fbde73b1a49df5cf61f/files/2c2dd6de-d325-335d-5d4e-84066159df71/Forensic_Without_the_Science_Face_Recognition_in_U.S._Criminal_Investigations.pdf) u detaljnoj studiji iz američkog Georgetown sveučilišta, te podsjećaju kako se ne tako davno sasvim drugačije govorilo o značaju privatnosti i anonimnosti u demokratskom okruženju.

Udruženje brojnih američkih državnih agencija i predstavnika policije su, naime, o opasnostima tehnologija prepoznavanja lica u izvještaju iz 2011. godine zapisali: (https://www.eff.org/files/2013/11/07/09_-_facial_recognition_pia_report_final_v2_2.pdf)“Potencijalna šteta identifikacije je u tome što povećava vladinu moć kontrole pojedinaca (…) To može dodatno spriječiti nečiju sposobnost da bude anoniman (…). Anonimnost je važno pravo u slobodnom društvu u mjeri u kojoj štiti ljude od pristranosti temeljene na njihovim identitetima i omogućuje ljudima da slobodnije glasaju, govore i udružuju se štiteći ih od opasnosti odmazde.”

Svakodnevica nam se, barem se tako čini, u proteklih desetak godina prilično promijenila jer, kako danas stvari stoje, svi smo manje više odustali od anonimnosti i pristali da bivamo stalno praćeni na vlastitim uređajima, bilo legalno, polulegalno ili čak ilegalno.

Neka službe rade svoj posao

Kada bismo međutim popričali s nekim iz državnih obavještajnih agencija vjerojatno bismo čuli ponešto drugačije stavove jer u današnje vrijeme bez špijunaže i nadzora propale bi neke važne istrage.

U Njemačkoj je nedavno uhićena grupa koja je, kako su tamošnji organi gonjenja objasnili, kanila srušiti demokratsku vlast i uz pomoć Rusa preuzeti vlast u državi. Neke informacije o djelovanju te grupe njemački su obavještajci saznali i kroz uvid u online prepiske u aplikacijama WhatsApp i Telegram.

Po Europi su razbacani mnogi ekstremisti svakojakih političkih uvjerenja, stotine bivših članova ISIS-a, kriminalci, mafijaši, trgovci drogom, oružjem, ljudima, korumpirani političari i potkupljivi poduzetnici, te nam svima bude drago kada se razbije neka mutna ekipa koju USKOK pohapsi u pet ujutro. Tada ne razmišljamo je li se možda tijekom sofisticiranih prisluškivanja nekome narušilo neko pravo jer prihvaćamo da, kako se to obično kaže, službe odrađuju svoj posao.

FBI sve dozna

I američke su agencije odradile zadatke u istrazi oko napada na zgradu Kongresa u Washingtonu šestog siječnja 2021. godine tako što je Google identificirao skoro šest tisuća telefona koji su se nalazili u blizini zgrade toga dana.

Google, naime, gotovo uvijek znade gdje su naši telefoni jer se prikupljaju podaci iz GPS, WiFi i Bluetooth mreža, a državnim organima gonjenja takvi detalji mogu biti vrlo dragocjeni. FBI je od Googlea za najsumnjivije iz napada na Kongres, njih oko tisuću i pol, zatražio i detalje o brojevima telefona, Google računima i email adresama, a odvjetnički timovi branjenika pokušavaju srušiti sve informacije kao mogući dokaz te zatražiti da se suradnja Googlea i FBI-ja smatra narušavanjem ustavom zajamčene privatnosti.

Nalazimo se na skliskom terenu kada god tehnološka kompanija odluči predati podatke koje zatraže državni organi gonjenja jer teško je složiti se u kojem je slučaju to opravdano, a u kojem nije.

Uzmite primjerice anonimnu prijetnju da je u nekoj hrvatskoj osnovnoj školi podmetnuta bomba, te da policija pročeprka tko je najvjerojatniji počinitelj putem digitalnih alata i suradnje s Googleom, Facebookom ili nekom drugom tvrtkom. U takvom slučaju vjerojatno biste bili zadovoljni jer je počinitelj lociran i uhvaćen.

No, što biste rekli ako vam je kćer, vrla i pristojna djevojka, nekim slučajem u državi u kojoj je zabranjen pobačaj i vi joj naručite taksi da otputuje u susjednu državu u kojoj je prekid neželjene trudnoće legalan? Organi države u kojoj je pobačaj protuzakonit (https://www.theguardian.com/world/2022/may/03/us-abortions-travel-wave-of-restrictions) mogli bi pokrenuti istragu, prikupiti digitalne podatke o lociranju i putovanju, te strpati djevojku u zatvor zbog izvršene radnje koja je protivna zakonu. U takvom slučaju vaš će stav o digitalnom nadzoru i prisluškivanju biti politički i ideološki obojen, odnosno bit ćete za ili protiv ovisno jeste li "za život" ili "za izbor."

Kako ne bi dolazilo do nesporazuma i prijepora u ovo zlatno doba za svakojako digitalno prisluškivanje, poželjno bi bilo što prije donijeti (https://www.euractiv.com/section/justice-home-affairs/news/experts-eu-regulation-of-spy-software-needed-but-unlikely/) jasne zakonske regulative, kako u pojedinim državama tako i na međunarodnoj razini, među ostalim i zato što špijuniranje više nije moguće teritorijalno ograničiti.

No, pravni sustavi Hrvatske, Europske unije, Sjedinjenih Država ili Ujedinjenih naroda već dugo kaskaju (https://pro.bloomberglaw.com/brief/regulation-and-legislation-lag-behind-technology/) za napretkom tehnologije i sporo reagiraju na promjene, te tako omogućuju da bilo tko može biti žrtva špijunskog šikaniranja bez ozbiljnijih posljedica, radilo se tu o članu Europskog parlamenta, istraživačkom novinaru ili bilo kome od vas.

Ostali nastavci serijala "Tehnologija i demokracija":

> Od pluga i motike do Facebooka i robotike (1) (https://faktograf.hr/2022/12/14/tehnologija-i-demokracija-1-od-pluga-i-motike-do-facebooka-i-robotike/)

> Utjecaj tehnodivova na izbore (2) (https://faktograf.hr/2022/12/15/tehnologija-i-demokracija-2-utjecaj-tehnodivova-na-izbore/)

Kruh naš svagdašnji dorađen genomski (4) (https://faktograf.hr/2022/12/23/tehnologija-i-demokracija-4-kruh-nas-svagdasnji-doraden-genomski/)

Umjetna inteligencija i pojeftinjenje kile mozga (5). (https://faktograf.hr/2022/12/27/tehnologija-i-demokracija-5-umjetna-inteligencija-i-pojeftinjenje-kile-mozga/)

Ovaj tekst je dio serijala "Tehnologija i demokracija" u kojem analiziramo utjecaj brzih tehnoloških promjena na demokratska društva. Tekst je objavljen u okviru programa poticanja novinarske izvrsnosti Agencije za elektroničke medije.

KAMERE (HTTPS://FAKTOGRAF.HR/TAG/KAMERE/), NADZOR (HTTPS://FAKTOGRAF.HR/TAG/NADZOR/), TEHNOLOGIJA I DEMOKRACIJA (HTTPS://FAKTOGRAF.HR/TAG/TEHNOLOGIJA-I-DEMOKRACIJA/)

LIVE BLOG

DEZINFORMACIJE O KORONAVIRUSU (HTTPS://FAKTOGRAF.HR/LIVE-BLOG-DEZINFORMACIJE-O-KORONAVIRUSU/)

Imate prijedloge, pohvale ili kritike? Uočili ste neku izjavu za koju vjerujete da bi je Faktograf trebao obraditi? Sumnjate u točnost viralnih objava na društvenim mrežama? Pišite nam na info@faktograf.hr (mailto:info@faktograf.hr) ili nas kontaktirajte putem Twittera (https://twitter.com/FaktografHR) ili Facebooka (https://www.facebook.com/faktografhr).

POVEZANO

PITALI STE (/TAG/PITALI-STE/)

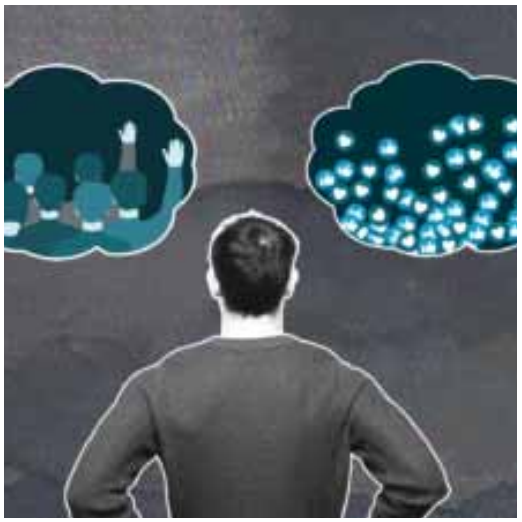
Tehnologija i demokracija (5): Umjetna inteligencija i pojeftinjenje kile mozga (https://faktograf.hr/2022/12/27/tehnologija-i-demokracija-5-umjetna-inteligencija-i-pojeftinjenje-kile-mozga/)

27 prosinca, 2022

Tehnologija i demokracija (4): Kruh naš svagdašnji dorađen genomski (https://faktograf.hr/2022/12/23/tehnologija-i-demokracija-4-kruh-nas-svagdasnji-doraden-genomski/)

23 prosinca, 2022

(https://faktograf.hr/2022/12/23/tehnologija-



Tehnologija i demokracija (2): Utjecaj tehnodivova na izbore (https://faktograf.hr/2022/12/15/tehnologija-i-demokracija-2-utjecaj-tehnodivova-na-izbore/)

15 prosinca, 2022

(https://faktograf.hr/2022/12/15/tehnologija-i-demokracija-2-utjecaj-tehnodivova-na-izbore/)

NAJČITANIJE

Ne, ova snimka nema nikakve veze s porazom Hrvatske od Argentine. Nastala je 2015. (https://faktograf.hr/2022/12/15/ne-ova-snimka-nema-nikakve-veze-s-porazom-hrvatske-od-argentine-nastala-je-2015/)

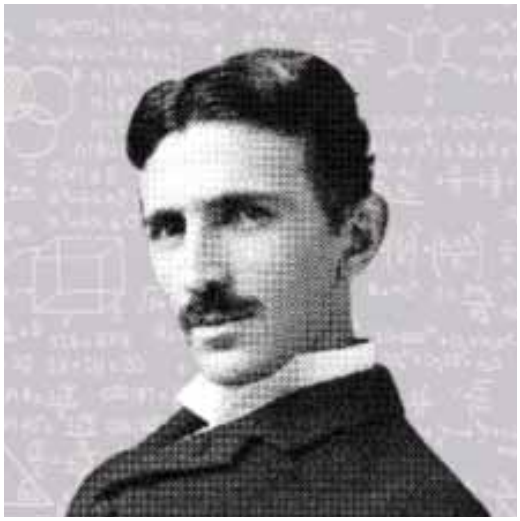
15 prosinca, 2022

(https://faktograf.hr/2022/12/15/ne-ova-snimka-nema-nikakve-veze-s-porazom-hrvatske-od-argentine-nastala-je-2015/)

Sindikalni rat preko leđa radnika Čistoće (https://faktograf.hr/2022/12/16/sindikalni-rat-preko-leda-radnika-cistoce/)

16 prosinca, 2022

(https://faktograf.hr/2022/12/16/sindikalni-rat-preko-leda-radnika-cistoce/)



Širi se video s dezinformacijama o izumima Nikole Tesle (https://faktograf.hr/2022/11/21/siri-se-video-s-dezinformacijama-o-izumima-nikole-tesle/)

21 studenoga, 2022

(https://faktograf.hr/2022/11/21/siri-se-video-s-dezinformacijama-o-izumima-nikole-tesle/)

(https://www.facebook.com/journalismproject/programs/third-party-fact-checking)

(https://seecheck.org/)

(https://ifcncodeofprinciples.poynter.org/profile/faktograf-udruga-za-informiranu-javnost)