Europski parlament
2019-2024

Dokument s plenarne sjednice

A9-0189/2023

22.5.2023

IZVJEŠĆE

o ispitivanju navodnih kršenja i nepravilnosti u primjeni prava Unije u pogledu uporabe Pegasusa i ekvivalentnog špijunskog softvera za nadzor
(2022/2077(INI))

Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor

Izvjestiteljica: Sophie in ‘t Veld

SADRŽAJ

Stranica

NACRT REZULTATA

o ispitivanju navodnih kršenja i nepravilnosti u primjeni prava Unije u pogledu uporabe Pegasusa i ekvivalentnog špijunskog softvera za nadzor
(2022/2077(INI))

Europski parlament,

– uzimajući u obzir članak 226. Ugovora o funkcioniranju Europske unije,

– uzimajući u obzir odluku Europskog parlamenta od 10. ožujka 2022. o osnivanju, nadležnostima, brojčanom sastavu i trajanju mandata Istražnog odbora za istraživanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor te o određivanju predmeta istrage,

– uzimajući u obzir članke 54. i 208. Poslovnika,

– uzimajući u obzir izvješće Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (A9-0189/2023),

Opći uvod

1. U srpnju 2021. skupina istraživačkih novinara, nevladinih organizacija i istraživača okupljenih u projektu Pegasus objavila je izvješće na temelju popisa koji posjeduje s oko 50 000 telefonskih brojeva koji su možda bili meta špijunskog softvera Pegasus. Autoritarne i demokratske vlade širom svijeta u velikoj se mjeri koriste takvim špijunskim softverom, uz sudski nadzor i bez njega, a mete su novinari, odvjetnici, suci, aktivisti, političari i državni dužnosnici. I pojedinci u Europskoj uniji bili su mete špijunskog softvera, neke su hakirali akteri izvan EU-a, a neke akteri iz Unije, uključujući vladina tijela. Većina vlada država članica, ako ne i sve, kupile su špijunski softver, u načelu za potrebe kaznenog progona i sigurnosti. Međutim, postoji mnogo dokaza da je špijunski softver u nekoliko država članica zlouporabljen isključivo u političke svrhe, s kritičarima i članovima oporbe kao metama, ili u vezi s korupcijom. U nalazima istrage Pegasus i drugi špijunski softver za nadzor povezuju se s raznim kršenjima ljudskih prava koja su počinile vlade, uključujući praćenje, ucjene, kampanje sramoćenja, zastrašivanje i uznemiravanje. To izaziva zabrinutost na više razina pravnog poretka EU-a u pogledu zaštite podataka i privatnosti, slobode izražavanja, slobode tiska, slobode udruživanja, mehanizama pravne zaštite, pravnog lijeka i poštenog suđenja te demokratskih procesa i institucija. Iako uporaba špijunskog softvera može proći ispitivanje nužnosti i razmjernosti u slučaju ozbiljnih prijetnji nacionalnoj sigurnosti, zlouporaba špijunskog softvera u političke svrhe iznimno je alarmantna i ozbiljan je razlog za zabrinutost u pogledu postupovne i materijalne zakonitosti nadzornih praksi te razine zaštite zajamčene europskim i nacionalnim pravom. Takva zlouporaba špijunskog softvera izravno ugrožava temeljna prava i demokraciju, temeljne vrijednosti EU-a. Naknadna izvješća istraživačkih medija i drugi izvori pokazali su da se špijunski softver izvozi iz zemalja EU-a u treće zemlje s nedemokratskim režimima i visokim rizikom od kršenja ljudskih prava, što je očito kršenje pravila EU-a za izvoz. Industrija špijunskog softvera snažna je u EU-u

zahvaljujući vrlo povoljnim uvjetima poslovanja.

2. U odgovoru na taj rastući skandal Europski parlament odlučio je 10. ožujka 2022. osnovati istražni odbor u skladu s člankom 226. UFEU-a kako bi istražio navodna kršenja ili nepravilnosti u primjeni prava Unije u pogledu uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor („PEGA”). Kršenje predstavlja nezakonito postupanje, bilo u smislu djelovanja ili propusta kojima se krši zakon, institucija ili tijela EU-a ili tijela država članica pri primjeni i provedbi prava EU-a, a nepravilnosti u primjeni znače loše ili nepostojeće upravne postupke, do kojih dolazi, na primjer, ako se ne poštuju načela dobre uprave. Primjeri nepravilnosti u primjeni uključuju nepravilnosti i propuste, zlouporabu ovlasti, nepoštenje, neispravnost ili nekompetenciju, diskriminaciju, ali i kašnjenja koja su se mogla izbjeći, odbijanje pružanja informacija, nemar i druge nedostatke koji podrazumijevaju lošu primjenu prava Unije.

3. Za potrebe ove istrage odbor PEGA primijenio je širok pristup tome što predstavlja špijunski softver, odnosno špijunski softver za nadzor koji je instaliran na mobilne uređaje iskorištavanjem slabih točaka informacijske tehnologije. Tijekom istrage upotrijebljena je i definicija „robe za kibernadzor” utvrđena u Uredbi o robi s dvojnom namjenom: prema toj se definiciji opisuje kao „roba s dvojnom namjenom posebno osmišljena kako bi se omogućio prikriveni nadzor fizičkih osoba praćenjem, izdvajanjem, prikupljanjem ili analiziranjem podataka iz informacijskih i telekomunikacijskih sustava”. Komisija je u rujnu 2022. u svojem prijedlogu Akta o slobodi medija predložila definiciju špijunskog softvera u kojoj ga je opisala kao „svaki proizvod s digitalnim elementima posebno dizajniran za iskorištavanje ranjivosti u drugim proizvodima s digitalnim elementima koji omogućuje tajni nadzor fizičkih ili pravnih osoba praćenjem, izvlačenjem, prikupljanjem ili analizom podataka iz takvih proizvoda ili od fizičkih ili pravnih osoba koje upotrebljavaju takve proizvode, posebice tajnim snimanjem poziva ili drugim načinom upotrebe mikrofona uređaja krajnjeg korisnika, snimanjem fizičkih osoba, strojeva ili njihove okoline, kopiranjem poruka, fotografiranjem, praćenjem aktivnosti pregledavanja, praćenjem geolokacije, prikupljanjem drugih podataka generiranih s pomoću senzora ili praćenjem aktivnosti na više uređaja krajnjih korisnika, pri čemu predmetna fizička ili pravna osoba nije o tome bila obaviještena na određeni način niti je izrijekom pristala”.

4. Odbor PEGA započeo je s radom 19. travnja 2022. prikupljanjem informacija putem javnih saslušanja, misija, savjetovanja sa stručnjacima, zahtjeva za podatke, dokaza i istraživanja.

5. Tijekom nekoliko javnih saslušanja istraživalo se funkcioniranje špijunskog softvera. Špijunski softver vrsta je zlonamjernog softvera koji prati aktivnosti korisnika bez njihova znanja ili privole. Takve aktivnosti špijuniranja mogu uključivati praćenje unosa znakova preko tipkovnice, praćenje aktivnosti i prikupljanje podataka te druge oblike krađe podataka. Špijunski softver obično se širi kao Trojan, odnosno iskorištavanjem slabih točaka softvera[1]. Špijunski softver može se instalirati na daljinu na mobilnim telefonima unaprijed odabranih pojedinaca, čak i preko granica. U nekim se slučajevima telekomunikacijske mreže rabe za prijenos špijunskog softvera na ciljani

[1] https://www.enisa.europa.eu/topics/incident-response/glossary/malware.

uređaj. Nakon što špijunski softver infiltrira sustav, onemogućava zaštitne mehanizme i sigurnosna ažuriranja. Zaraženi uređaj zatim prenosi prikupljene podatke s uređaja i omogućuje akterima da provode nadzor u stvarnom vremenu čitanjem ulaznih tekstualnih poruka, praćenjem poziva i lokacija te pristupom zvuku i videozapisima putem mikrofona i kamere uređaja i njihovu snimanju.

6. Za razliku od uobičajenog prisluškivanja, uz koje je moguće samo praćenje komunikacije u stvarnom vremenu, špijunski softver omogućava potpun, retroaktivan pristup datotekama i porukama nastalima u prošlosti, lozinkama i metapodacima o prijašnjoj komunikaciji. To znači da sudska odluka o datumu početka i trajanju operacije nadzora nije učinkovita zaštitna mjera jer se špijunskim softverom omogućuje potpun retroaktivan pristup podacima. Tehnički je također moguće lažno predstavljanje osobe koja je meta špijunskog softvera nakon pristupa digitalnim vjerodajnicama i identitetu te osobe. Meti je iznimno teško otkriti je li došlo do neovlaštenog pristupa špijunskim softverom. Špijunski softver ostavlja malo ili nimalo tragova na uređaju meta, a čak i ako se otkrije, vrlo je teško dokazati tko je odgovoran za napad.

7. Odbor PEGA od nacionalnih tijela nije dobio odgovore ili je dobio samo šture odgovore o nabavi i uporabi špijunskog softvera u njihovim državama članicama i o proračunskim aspektima. Dobavljači i države koje izdaju izvozne dozvole (najviše Izrael) ne objavljuju nikakve informacije o kupcima. Tijela mnogih država članica odboru PEGA nisu dostavila smislene informacije o pravnim okvirima kojima se uređuje uporaba špijunskog softvera ili o uporabi špijunskog softvera u njihovim državama članicama koje već nisu bile javno poznate, uglavnom zbog nacionalnih zakonskih zahtjeva koji se odnose na tajnost i povjerljivost.

8. Neke države članice koristile su se špijunskim softverom i odbile su se očitovati o tome pozivajući se na nacionalnu sigurnost, koja, u skladu s člankom 4. stavkom 2. Ugovora o Europskoj uniji (UEU), „ostaje isključiva odgovornost svake države članice”. Međutim, u sudskoj praksi Suda Europske unije i Europskog suda za ljudska prava navodi se da se pitanja nacionalne sigurnosti moraju uskladiti s temeljnim pravima i demokratskim normama koje su čvrsto ugrađene u pravo EU-a. Iako je na državama članicama da definiraju svoje osnovne interese sigurnosti i donesu prikladne mjere da osiguraju svoju unutarnju i vanjsku sigurnost, Sud EU-a smatra da „sama činjenica da je nacionalna mjera donesena radi zaštite nacionalne sigurnosti ne može dovesti do neprimjenjivosti prava Unije i osloboditi države članice obveze da nužno poštuju to pravo[2]” te je pojasnio kriterije koje države članice moraju pratiti pri definiranju pitanja nacionalne sigurnosti. Nekoliko država članica tvrdilo je da je uporaba špijunskog softvera potrebna zbog nacionalne sigurnosti i da se time isključuje primjenjivost prava EU-a. Međutim, kada države članice navedu puko upućivanje na nacionalnu sigurnost kao takvu, ograničenje temeljnih prava ne može se opravdati nacionalnom sigurnošću. Pravo EU-a mora se primjenjivati uz sve zaštitne mjere koje su njime predviđene. Postoje brojni dokazi o zlouporabi špijunskog softvera zbog razloga koji nisu povezani s nacionalnom sigurnošću. Države članice ne bi trebale moći izbjeći odgovornost za takve teške zlouporabe špijunskog softvera pukim upućivanjem na nacionalnu sigurnost. Zbog te je nejasnoće bilo teško dobiti dovoljno informacija tijekom

[2] Presuda od 6. listopada 2020. *Privacy International* protiv *Secretary of State for Foreign and Commonwealth Affairs i drugi*, C-623/17, EU:C:2020:790.

saslušanja i misija te nakon podnošenja zahtjeva za informacije. Nedovoljno jasna definicija nacionalne sigurnosti i nacionalna tijela koja preširoko tumače njezino područje primjene otežavaju razumijevanje opravdanosti uporabe špijunskog softvera.

9. Međutim, objedinjavanjem informacija iz različitih izvora odbor PEGA uspio je rekonstruirati djelomičnu, ali jasnu sliku te utvrditi pitanja koji izazivaju zabrinutost i zahtijevaju daljnju istragu.

10. Može se sa sigurnošću pretpostaviti da se vlasti u svim državama članicama služe špijunskim softverom na ovaj ili onaj način, neke zakonito, a neke nezakonito. Špijunski softver moguće je nabaviti izravno ili putem opunomoćenika, brokerskog društva ili posrednika. Također je moguće dogovoriti konkretne usluge umjesto kupnje samog softvera. Mogu se nuditi i dodatne usluge kao što je osposobljavanje osoblja ili pružanje usluga poslužitelja. Špijunski softver ne treba promatrati zasebno, već kao dio širokog raspona proizvoda i usluga koji se nude na rastućem i unosnom globalnom tržištu. Važno je shvatiti da je kupnja i uporaba špijunskog softvera vrlo skupa: troškovi se mjere u milijunima eura. Ipak, u mnogim državama članicama taj izdatak nije uključen u redoviti proračun, što omogućuje izbjegavanje nadzora.

11. Iz informacija koje je dostavila Grupa NSO može se zaključiti da je Pegasus prodan u najmanje 14 država članica EU-a te da su ugovori s dvjema državama raskinuti. Nije poznato na koje se države to odnosi, ali općenito se pretpostavlja da se radi o Poljskoj i Mađarskoj. Međutim, nije moguće provjeriti tu informaciju sve dok Grupa NSO ili izraelska vlada ne izdaju službenu izjavu o raskidu ugovora.

12. Dodatne je informacije moguće izvući iz popisa sudionika sajma ISS (Intelligence Support Systems) World, održanog 2013., koji ima nadimak „Bal prisluškivača”. Uz izuzetak Portugala i Luksemburga, sve su trenutačne države članice EU-a bile prisutne na tom sajmu, gdje ih je zastupao širok spektar organizacija, uključujući lokalne policije[3]. Grupa NSO proteklih je godina postala glavni sponzor tog događaja, ali na popisu sponzora navode se i Intellexa, Candiru, RCS i mnogi drugi[4].

13. Države članice nisu samo kupci koji kupuju komercijalni špijunski softver od dobavljača, već imaju i druge različite uloge u trgovini tim softverom. Neke su domaćini dobavljačima špijunskog softvera, druge su preferirane destinacije za financijske i bankarske usluge, a treće nude sudionicima te industrije državljanstvo i boravište.

14. U velikoj većini država članica obavještajne službe regulirane su pravnim okvirom, često s odredbama o organizaciji i funkcioniranju tih službi te njihovim mandatima i ovlastima, uključujući načine djelovanja i uvjete za njihovu uporabu, kao i mehanizmima nadzora koji uključuju izvršnu kontrolu, parlamentarni nadzor, stručna tijela i sudski nadzor. Međutim, izražena je zabrinutost zbog popustljivih obavještajnih okvira određenih zemalja, neučinkovitih provjera, blagih praksi nadzora i političkog uplitanja**.**

15. Jasno je da se špijunskim softverom koristi i policija, a ne samo obavještajne agencije.

[3] https://wikileaks.org/spyfiles/docs/ISS-2013-Sche2013-en.pdf.
[4] https://www.issworldtraining.com/iss_europe/sponsors.html.

Postoji ozbiljan razlog za zabrinutost u pogledu prihvatljivosti takvih materijala kao dokaza na sudu u kontekstu policijske i pravosudne suradnje u EU-u, među ostalim u okviru Europola i Eurojusta, ako su izvori takvih informacija metode istrage primijenjene bez odgovarajućeg sudskog nadzora. Ovisno o nacionalnom zakonodavstvu, uporaba špijunskog softvera zakonita je u istragama pod sudskim nadzorom.

16. Zlouporaba špijunskog softvera prijetnja je demokraciji i temeljnim pravima. Na temelju otkrića u projektu Pegasus Sjedinjene Američke Države poduzele su nekoliko koraka kako bi ga istražile i regulirale. Dosad je bilo vrlo malo djelovanja u EU-u. Potrebno je utvrditi jasna pravila o uporabi špijunskog softvera i trgovini njime, po mogućnosti u suradnji s drugim zemljama, kao što je SAD.

I. Uporaba špijunskog softvera u EU-u

I.A Poljska

17. Predstavnici ministarstava odbili su se sastati s izaslanstvom odbora. U odgovoru na upitnik koji je poslao odbor PEGA 15. srpnja 2022. poljske vlasti nisu odgovorile na sva pitanja i ustrajale su na tome da su postojeće odredbe dovoljne i da djeluju potpuno u skladu sa zakonom[5]. Osim toga, ministar unutarnjih poslova Mariusz Kaminski odbio je poziv odbora PEGA na razmjenu mišljenja[6].

18. Misija odbora PEGA za utvrđivanje činjenica u Poljskoj u rujnu 2022. bila je od ključne važnosti za prikupljanje informacija i činjenica o uporabi špijunskog softvera Pegasus. Na sastancima održanima u Varšavi pojavila su se nova saznanja o nezakonitoj uporabi intruzivnog softvera za nadzor protiv demokratskih dionika u Poljskoj. Članovi su saznali kako je ukinut sustav pravnih i institucionalnih provjera i ravnoteže kako bi se omogućilo usmjeravanje kibernetičkog oružja za vojne namjene na pojedince koji se smatraju političkim protivnicima. Zbog toga je došlo do teškog kršenja ključnih demokratskih standarda i prava građana propisanih zakonima EU-a i Poljske. To je još jedna dimenzija krize vladavine prava u Poljskoj.

KUPNJA PEGASUSA

19. Bivša predsjednica vlade i aktualna zastupnica u Europskom parlamentu Beata Szydło, zajedno s bivšim ministrom vanjskih poslova Witoldom Waszczykowskim, prisustvovala je u studenome 2016. večeri priređenoj u domu tadašnjeg predsjednika vlade Izraela Benjamina Netanyahua[7]. Sljedeće godine u srpnju, Szydło i Netanyahu sastali su se s čelnicima vlada zemalja Višegradske skupine. Navodno su razgovarali o „jačanju suradnje u području inovacija i visokih tehnologija” i „pitanjima povezanim sa široko shvaćenim pojmom sigurnosti građana”[8]. Nedugo nakon održavanja tog sastanka 2017. poljska vlada kupila je Pegasus nakon sastanka kojem su prisustvovali predsjednik vlade Mateusz Morawiecki, mađarski predsjednik vlade Viktor Orbán i

[5] Odgovor stalnog predstavnika Poljske u EU-u Andrzeja Sadósa odboru PEGA 7. rujna 2022.
[6] Odgovor ministra unutarnjih poslova Mariusza Kaminskog odboru PEGA u dopisu 12. srpnja 2022.
[7] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29. siječnja 2022.
[8] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29. siječnja 2022.

Netanyahu.[9]

20. Poljska vlada i vođa PiS-a Jarosław Kaczyński prvotno su zanijekali kupnju Pegasusa[10]. Međutim, početkom siječnja 2022. potvrdili su da je poljska vlada kupila špijunski softver[11] [12] [13]. U istom mjesecu otkriveno je da je Vrhovni ured za reviziju 2018. prikupio ključne dokaze povezane s kupnjom Pegasusa tijekom revizije Fonda za pravosuđe kojim upravlja Ministarstvo pravosuđa i koji je osnovan radi pružanja potpore žrtvama kaznenih djela. Bivši načelnik poljskog Vrhovnog ureda za reviziju (NIK) i neovisni senator Krzysztof Kwiatkowski 18. siječnja 2022. svjedočili su o kupnji Pegasusa pred izvanrednim odborom Senata za slučajeve nadzora uporabom sustava Pegasus[14]. Nakon što je oslobođen obveze čuvanja tajne povezane s položajem, odboru je dostavio dva računa kojima se potvrđuje kupnja špijunskog softvera za Središnji ured za borbu protiv korupcije (CBA) u vrijednosti od 25 milijuna PLN iz Fonda za pravosuđe kojim upravlja Ministarstvo pravosuđa[15]. Kwiatkowski je potvrdio da je NIK pronašao račune Poljske narodne banke kojima se dokazuje prijenos[16].

21. Račune je izdalo društvo Matic Sp. z o.o., koje je djelovalo kao posrednik preko kojeg je ured CBA obavio tu kupnju[17]. Društvo Matic Sp. z o.o. sa sjedištem u Varšavi bavi se informatikom i sigurnosti, a vlasnici su osobe koje su bili aktivne u zajednici obavještajnih i sigurnosnih službi u komunističkom razdoblju[18].

22. Prema listu Wyborcza, društvo Matic postalo je dioničko društvo neposredno nakon kupnje Pegasusa u studenome 2017. i posluje s dozvolom Ministarstva unutarnjih poslova za trgovanje tehnologijama sa sigurnosnim službama i policijom te oružjem[19]. Društvo ima i posebnu licenciju Agencije za unutarnju sigurnost, koja je posljednji put izdana 2019., zbog čega može čuvati tajnost određenih povjerljivih informacija do kraja desetljeća[20]. Predstavnici društva Matic odbili su se sastati s istražnim odborom te podijeliti informacije.

23. U skladu s poljskim pravom rad ureda CBA može se financirati samo iz državnog

[9] Financieele Dagblad, „De wereld deze week: het beste uit de internationale pers”, 7. siječnja 2022.
[10] https://www.politico.eu/article/poland-government-scrambles-minimize-hacking-backlash/.
[11] Financieele Dagblad, „Liberalen Europarlement eisen onderzoek naar spionagesoftware”, 12. siječnja 2022.
[12] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/.
[13] Siječanj 2022, Financial Times, https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e, 8. veljače 2022.
[14] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18. siječnja 2022.
[15] ONET, https://wiadomosci.onet.pl/kraj/wiceminister-michal-wos-nie-wiem-co-to-jest-pegasus/e9fbrvh, 3. siječnja 2022.; Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4. siječnja 2022.
[16] The Wire, https://thewire.in/world/poland-audit-office-invoice-pegasus-purchase-reopen-investigation, 4. siječnja 2022.; Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18. siječnja 2022.
[17] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17. siječnja 2022.
[18] https://ipn.gov.pl/en/about-the-institute.
[19] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17. siječnja 2022.
[20] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17. siječnja 2022.

proračuna. Međutim, kupnja Pegasusa financirana je iz Fonda za pravosuđe, koji nije dio državnog proračuna, već javni fond namijenjen žrtvama kaznenih djela[21]. Stoga je kupnjom prekršeno poljsko pravo. Osim toga, izvorne uredbe kojima se uređuje taj fond ne dopuštaju njegovu uporabu za financiranje rada posebnih službi[22]. Međutim, u rujnu 2017. Michał Woś, zamjenik ministra pravosuđa[23] i bliski suradnik ministra pravosuđa Zbigniewa Ziobre[24], iznio je prijedlog za izmjenu financijskog plana Fonda za pravosuđe Odboru za javne financije Sejma (donji dom poljskog parlamenta). Zastupnici su odobrili tu izmjenu. Kad je poslije otkriveno da se Fond za pravosuđe koristio za financiranje Pegasusa za ured CBA, zastupnici su izjavili da „na sjednici odbora o tome uopće nije bilo govora”[25]. Stoga se čini da ih je vlada dovela u zabludu. Iako je NIK dostavio službenu obavijest Uredu javnog tužitelja o kršenju zakona u pogledu uporabe sredstava iz Fonda za pravosuđe za kupnju Pegasusa 2017., ne očekuje se da će Ured javnog tužitelja poduzeti mjere u vezi s tim predmetom, s obzirom na trenutačno institucijsko i političko okruženje.

24. Woś je također zatražio od Ministarstva financija odobrenje za preraspodjelu 25 milijuna PLN potrošenih na Pegasus iz Fonda za pravosuđe za „druge aktivnosti” čiji je cilj „suzbijanje učinaka kaznenih djela”. Zamjenik ministra odobrio je prijenose iz Fonda za pravosuđe uredu CBA. Međutim, nakon što je Woś u siječnju 2022. upitan o kupnji, prvotno je zanijekao da zna išta o samom alatu Pegasus, a kamoli da ga je država kupila, ali je u međuvremenu potvrdio kupnju. Nije jasno kako su se financirali tekući troškovi za uporabu Pegasusa.

25. Objavljeno je da je Grupa NSO do sada prodala Pegasus 14 zemalja u Europi. Međutim, Grupa NSO priznala je i da je opozvala licencije dvjema od tih zemalja[26]. U svjedočenju odboru PEGA Grupa NSO izjavila je da istražuje „pitanja” povezana s uporabom Pegasusa samo kad primi informacije od zviždača ili putem medija. Kad Grupa NSO primi pritužbe, istražuje ih i preispituje te poslije može onemogućiti uporabu Pegasusa akterima koji su ga zlouporabili[27]. Na temelju brojnih medijskih izvješća o uporabi Pegasusa u Poljskoj, vrlo je vjerojatno da je Poljska bila jedna od tih dviju zemalja s obzirom na to da je prekršila uvjete uporabe NSO-a; međutim, to nije potvrđeno.

---

[21] The Guardian, „More Polish opposition figures found to have been targeted by Pegasus spyware”, 17. veljače 2022.; The Guardian, „Polish senators draft law to regulate spyware after anti-Pegasus testimony”, 24. siječnja 2022.; Izvješće Europske komisije o vladavini prava za 2022., poglavlje o Poljskoj, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, str. 26.; Gazeta Wyborcza, https://www.rp.pl/polityka/art19250101-gazeta-wyborcza-jak-kupowano-pegasusa-dla-cba, 3. siječnja 2022.

[22] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18. siječnja 2022.

[23] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4. siječnja 2022.; Gazeta Wyborcza, https://wyborcza.pl/7,75398,27966080,jak-ziobro-kupowal-pegasusa-dla-cba.html, 3. siječnja 2022.

[24] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4. siječnja 2022.

[25] https://polishnews.co.uk/pegasus-reports-of-surveillance-and-backstage-of-the-purchase-themis-judges-association-on-a-possible-breach-of-the-law-appeal-to-appoint-a-commission-of-inquiry/, 4. siječnja 2022.

[26] Rasprava s Grupom NSO, Misija Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Izraelu, srpanj 2022.

[27] Svjedočanstvo Chaima Gelfanda, glavnog savjetnika i glavnog službenika za praćenje usklađenosti, NSO, odboru PEGA, 21. lipnja 2022.

26. Otkad je prvi put primijećeno da bi se poljske vlasti mogle koristiti Pegasusom, poljski pučki pravobranitelj pokušava od vlasti saznati je li uistinu tako te se zalaže za poboljšanje demokratskih zaštitnih mjera i mjera zaštite ljudskih prava kako bi se spriječila zlouporaba nadzora, među ostalim godišnjim izvješćima poljskom parlamentu. U siječnju 2023. poljski pučki pravobranitelj poslao je dopis ministru unutarnjih poslova u kojem navodi da ne postoji pravna osnova za uporabu Pegasusa ili sličnog špijunskog softvera u Poljskoj, pozivajući se na sudsku praksu poljskog Ustavnog suda i sudsku praksu Europskog suda za ljudska prava[28].

PRAVNI OKVIR

27. Ustavni sud proveo je 2014. preispitivanje Zakona o policiji iz 1990. i drugih postojećih zakona kojima se regulira nadzor građana, a koji su se smatrali nespojivima s poljskim Ustavom[29]. Ustavni sud donio je presudu koja je sadržavala konkretne preporuke i 18-mjesečni rok u kojem je trebalo provesti zakonodavne promjene[30]. Nova Vlada uvela je zakonodavne promjene nakon izbora održanih 2015. Međutim, donesenim Zakonom o izmjeni Zakona o policiji iz 1990. i određenih drugih zakona (u daljnjem tekstu: Zakon o policiji iz 2016.) od 15. siječnja 2016. nije otklonjen nijedan nedostatak u zakonu čije je otklanjanje zahtijevao Ustavni sud[31]. Umjesto toga, Zakonom o policiji iz 2016. oslabljene su postojeće odredbe kojima se ne štite prava građana niti se stvara odgovarajući nadzor.

28. U svojem mišljenju o Zakonu o policiji iz 2016. Venecijanska komisija navodi da „postupovna jamstva i bitni uvjeti koji su Zakonom o policiji određeni za provedbu tajnog nadzora nisu dostatni za sprečavanje njegove pretjerane upotrebe i neopravdanog uplitanja u privatan život [...] pojedinaca”[32]. Nadalje, nedostatak konkretnih podataka o nadzoru, jamstvima protiv zlouporabe te kategorijama osoba i kaznenih djela koji bi mogli biti mete također se smatraju kršenjem presude Europskog suda za ljudska prava[33]. Konkretno, u presudi u predmetu *Roman Zakharov* protiv *Rusije* iz 2015. sud se bavio nužnošću jasnoće u pogledu uporabe špijunskog softvera. U pogledu tajnog nadzora građana presuđeno je da postoji potreba za strogim kriterijima, pravilnim sudskim nadzorom, trenutnim uništavanjem nebitnih podataka, sudskim nadzorom nad hitnim postupcima i obvezom obavješćivanja žrtava[34]. Osim toga, sud je izričito naveo da bi bilo „u suprotnosti s vladavinom prava” da se diskrecijsko pravo odlučivanja o

[28] Sastanak odbora PEGA, 19. siječnja 2023.
[29] Mišljenje br. 839/2016 o Zakonu o izmjeni Zakona o policiji i određenih drugih zakona od 15. siječnja 2016., koji je Venecijanska komisija donijela na 107. plenarnoj sjednici od 10. do 11. lipnja 2016.
[30] https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani.
[31] Zakon o izmjeni Zakona o policiji i određenih drugih zakona od 15. siječnja 2016., članak 20.c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf .
[32] Mišljenje br. 839/2016 o Zakonu o izmjeni Zakona o policiji i određenih drugih zakona od 15. siječnja 2016., koji je Venecijanska komisija donijela na 107. plenarnoj sjednici od 10. do 11. lipnja 2016.
[33] Među ostalim vidjeti Roman Zakharov protiv Rusije [GC], br. 47143/06, ESLJP, presuda od 4. prosinca 2015.; Klass i ostali protiv Njemačke, br. 5029/71, ESLJP, presuda od 6. rujna 1978., točka 40.; Prado Bugallo protiv Španjolske, br. 58496/00, ESLJP, presuda od 18. veljače 2003., točka 30.; Liberty i ostali protiv Ujedinjene Kraljevine, br. 58243/00, presuda od 1. srpnja 2008, točka 62.
[34] Roman Zakharov protiv Rusije [GC], br. 47143/06, ESLJP, presuda od 4. prosinca 2015.;

tajnom nadzoru u potpunosti dodijeli izvršnoj vlasti[35]. Zakon o policiji iz 2016. koji je na snazi u Poljskoj ni na koji način ne odražava tu presudu suda. Štoviše, njegove su odredbe u izravnoj suprotnosti s velikim dijelom presude.

29. ESLJP je također iznio nedvojbeno stajalište o testu nužnosti, što znači da nadzor mora biti dovoljno važan da bi takvo narušavanje privatnosti bilo potrebno. U svojoj je presudi u predmetu *Klass i drugi* protiv *Njemačke* iz 1978. jasno istaknuo tu točku te je utvrdio da, bez obzira na sustav nadzora, sud mora biti uvjeren da postoje „odgovarajuća i efikasna jamstva protiv zlouporabe”[36]. Pozorno orkestrirano ukidanje sustava provjere i ravnoteže u Poljskoj pokazuje da vladajuća stranka očito ne poštuje sudove. Unatoč svemu tome, vlada na čelu s PiS-om ustraje u tome da su postojeće odredbe dovoljne i da djeluju potpuno u skladu sa zakonom[37]. Vlada je istodobno odbila sve zahtjeve za dijalog i pojašnjenje o tome kako se nadzor primjenjuje u Poljskoj.

ZAKON O BORBI PROTIV TERORIZMA IZ 2016.

30. Uz Zakon o policiji iz 2016., Sejm je donio zakon kojim se uređuje nadzor stranih državljana, nazvan „Zakon o borbi protiv terorizma”. Tim zakonom dopušta se nadzor stranih državljana bez sudskog odobrenja u razdoblju od tri mjeseca ako je njihov identitet „dvojben”, što uključuje prisluškivanje telefona, prikupljanje otisaka prstiju, biometrijskih fotografija i DNK-a te obvezu registracije telefonskih kartica s unaprijed uplaćenim sredstvima[38]. U skladu s člankom 9. točkom 8. Zakona, glavni javni tužitelj može naložiti uništenje nerelevantnih materijala. S obzirom na činjenicu da je glavni javni tužitelj trenutačno Zbigniew Ziobro, koji je ujedno i ministar pravosuđa, postoji ozbiljan razlog za zabrinutost u pogledu njegove sposobnosti da donosi neovisne i nepristrane odluke bez utjecaja političkih interesa vlade koju zastupa[39] [40].

ZAKON O KAZNENOM POSTUPKU

31. U Poljskoj je u srpnju 2015. donesen Zakon o izmjeni Zakona o kaznenom postupku kako bi se spriječilo uključivanje nezakonito pribavljenih dokaza u kaznene postupke. Međutim, nakon što je PiS došao na vlast, u ožujku 2016. revidirali su Zakon i u njega uključili članak 168.a[41]. Tim se dodanim člankom dokazi pri čijem je prikupljanju prekršen zakon, tzv. „plod otrovnog stabla”, kao što su informacije prikupljene s pomoću Pegasusa, proglašavaju prihvatljivima za iznošenje pred sudom[42]. Međutim, važno je dodati da je Vrhovni sud Poljske u presudi naveo da se taj članak ne može primjenjivati protivno odredbama Europske konvencije o ljudskim pravima i Ustava

[35] Roman Zakharov protiv Rusije [GC], br. 47143/06, ESLJP, presuda od 4. prosinca 2015., točke 229. i 230. Vidjeti i Mišljenje br. 839/2016 Venecijanske komisije iz lipnja 2016., https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e, str. 11.
[36] Klass i ostali protiv Njemačke, 6. rujna 1978., točka 50, serija A, br. 28. 40.
[37] Dopis Mariusza Kaminskog, ministra unutarnjih poslova i uprave Poljske, Odboru PEGA, 8. rujna 2022.
[38] Zakon o borbi protiv terorizma od 10. lipnja 2016., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf.
[39] Zakon o borbi protiv terorizma od 10. lipnja 2016., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf.
[40] EDRi, https://edri.org/our-work/poland-adopted-controversial-anti-terrorism-law/, 29. lipnja 2016.
[41] Zakon o izmjeni Zakona o kaznenom postupku i određenih drugih zakona od 11. ožujka 2016., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000437/T/D20160437L.pdf.
[42] https://palestra.pl/en/palestra/issue/5-2016/article/article-168a-of-the-polish-criminal-procedure-code-as-a-permission-to-use-illegally-obtained-evidence-in-criminal-proceedings.

Poljske, što u nekim slučajevima ograničava njegovu djelotvornu primjenu[43]. Donesene su i presude u kojima je utvrđeno da je članak 168.a djelomično neustavan[44]. Međutim, zbog postojanja te odredbe u pravnom sustavu dovodi se u pitanje poštovanje temeljnih prava.

ZAKON O TELEKOMUNIKACIJAMA

32. Nakon što je 2016. izmijenjen Zakon o telekomunikacijama iz 2004., poljski zakon kojim se uređuju telekomunikacije sadržava odredbe kojima se policiji omogućuje neograničen pristup metapodacima, u određenim slučajevima bez sudjelovanja telekomunikacijskih poduzeća[45]. Takav se pristup odobrava na temelju vrlo širokog tumačenja „sprečavanja ili otkrivanja kaznenih djela". Javni tužitelj odlučuje o daljnjem postupanju nakon primitka tih podataka. Međutim, to se ne može smatrati zaštitnom mjerom jer ulogu ministra pravosuđa i javnog tužitelja ima ista osoba te se državno odvjetništvo ne može smatrati neovisnim o izvršnoj vlasti[46].

33. Spomenuta izmjena Zakona o kaznenom postupku kako bi se omogućilo korištenje dokaza koji su. „plod otrovnog stabla" znatno je utjecala na važnost telekomunikacijskih operatera i podataka koje ta poduzeća pohranjuju. U Poljskoj su najveći pružatelji telekomunikacijskih usluga zapravo dužni imati poseban tim koji odgovara na razne zahtjeve vlasti za prisluškivanje. Međutim, obično nemaju uvid u sadržaj prisluškivanja ili operativne pojedinosti pojedinačnih slučajeva[47].

ZAKON O PROVEDBI DIREKTIVE O ZAŠTITI PODATAKA PRI IZVRŠAVANJU ZAKONODAVSTVA

34. Poljska nije pravilno provela Direktivu (EU) 2016/680 o zaštiti podataka pri izvršavanju zakonodavstva[48], kojom se zahtijevaju posebni standardi za prikupljanje i obradu osobnih podataka koje provode policija i druge službe. Direktiva o zaštiti osobnih podataka pri izvršavanju zakonodavstva prenesena je u poljsko pravo Zakonom o zaštiti osobnih podataka obrađenih u vezi sa sprečavanjem i suzbijanjem kriminala iz 2018. Zakonom je znatno proširenо područje primjene razloga za odbijanje obavješćivanja pojedinaca o obradi njihovih podataka koji je predviđen Direktivom te je prekršen mehanizam predviđen člankom 17. Direktive, kojim se pojedincima daje mogućnost da ostvare svoja prava preko relevantnog nadzornog tijela, a to je u Poljskoj predsjednik Ureda za zaštitu osobnih podataka. Nadalje, Zakonom se predviđa znatno izuzeće za nacionalnu sigurnost, uključujući provedbu zakonom utvrđenih zadaća različitih

[43] Na primjer, presuda Vrhovnog suda Poljske od 26. lipnja 2019., IV KK 328/18.
[44] Na primjer, presuda Vrhovnog suda Poljske od 26. lipnja 2019., IV KK 328/18.
[45] Zakon o telekomunikacijama od 16. srpnja 2004. https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004.
[46] Zakon o izmjeni Zakona o policiji i određenih drugih zakona od 15. siječnja 2016., članak 20.c,https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[47] https://www.europarl.europa.eu/doceo/document/PEGA-CR-736647_EN.pdf; The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, 17. veljače 2022.; https://palestra.pl/en/palestra/issue/5-2016/article/article-168a-of-the-polish-criminal-procedure-code-as-a-permission-to-use-illegally-obtained-evidence-in-criminal-proceedings; https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, str. 16–17.
[48] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.).

agencija snaga sigurnosti[49].

35. Poljska još nije provela Direktivu EU-a o zaštiti zviždača. Nije ispoštovala rok u prosincu 2021. nakon neuspjeha prvotnog nacrta zakonodavstva. Drugi nacrt objavljen je u travnju 2022., ali nije ostvaren daljnji napredak, a predloženo zakonodavstvo sadržava znatno slabije odredbe. Komisija je u siječnju 2022. pokrenula postupak zbog povrede protiv Poljske jer nije u potpunosti provela Direktivu, a u veljači 2023. odlučila je uputiti predmet protiv Poljske Sudu Europske unije[50].

36. Sejm, a posebno članovi PiS-a, trenutačno izrađuje nacrt zakona o elektroničkim komunikacijama. Tim bi se zakonom vlastima olakšao pristup porukama e-pošte i porukama na društvenim mrežama poljskih građana. Pružatelji bi morali pohranjivati e-poštu i poruke na svojim poslužiteljima kako bi relevantni sudovi mogli izdavati naloge za pristup podacima, IP adresama i sadržaju poruka[51].

EX ANTE NADZOR

37. Iako je za nadzor u Poljskoj u pravilu potrebno sudsko odobrenje, u praksi postupak odobravanja ne služi kao mjera zaštite protiv zlouporabe, već kao sredstvo za davanje zakonskog pokrića nadzoru koji se provodi u političke svrhe. Nije izričito razjašnjeno je li ijedna od dosadašnjih meta Pegasusa podvrgnuta špijuniranju uz sudsko odobrenje. Zahtjeve za sudsko odobrenje za operacije nadzora podnose posebne policijske jedinice[52]. Suci pri ocjenjivanju zahtjeva raspolažu samo informacijama koje je naveo podnositelj zahtjeva (tj. posebne policijske jedinice), a javni tužitelj odlučuje o tome koji je materijal relevantan za podnošenje[53]. Podnesene informacije često se svode na sažetak, koji katkad ne sadržava ni osnovne pojedinosti o osobi koja je predmet nadzora (ime, zanimanje, kazneno djelo za koje se osoba sumnjiči), i opis metode nadzora koja će se upotrebljavati.

38. Ako sudac odbije zahtjev, dužan je obrazložiti takvu odluku i protiv nje se može podnijeti žalba[54]. U hitnim slučajevima javni tužitelj može odmah odobriti uporabu metoda presretanja bez odobrenja suca, pod uvjetom da sud to odobri naknadno, u roku od pet dana[55]. To je velika i namjerno ostavljena rupa u poljskom pravnom okviru.

39. Zahtjeve za odobrenje nadzora glavnih agencija, tj. ureda CBA, policije (Policja KGP) i obavještajnih službi (Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, Służba Ochrony Państwa, Biuro

[49] Adam Bodnar i dr., „How to saddle Pegasus: Observance of civil rights in the activities of security services: objectives of the reform', rujan 2019. https://bip.brpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20(OSIOD%C5%81A%C4%86%20PEGAZA).pdf.
[50] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_703.
[51] Euractiv, „Polish government working on controversial surveillance bill", https://www.euractiv.com/section/politics/news/polish-government-working-on-controversial-surveillance-bill/.
[52] Zakon o izmjeni Zakona o policiji i određenih drugih zakona od 15. siječnja 2016., članak 20.c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[53] Zakon o izmjeni Zakona o policiji i određenih drugih zakona od 15. siječnja 2016., članak 20.c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[54] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef.
[55] https://www.lexology.com/library/detail.aspx?g=b3c8b4a9-d10f-4502-a345-b736280977ef.

Nadzoru Wewnętrznego MSWiA i nedavno dodan Inspektorat Służby Więziennej) podnose se gotovo isključivo Okružnom sudu u Varšavi (Sad Okręgowy), gdje se nalazi većina tih agencija.

40. Svaki se dan podnosi nekoliko desetaka zahtjeva za nadzor, čime se umanjuje kapacitet suda da provede detaljno ispitivanje svakog zahtjeva[56]. Sustav kojim se predmeti nasumično dodjeljuju sucima sudova i dalje je tehnički u uporabi u Poljskoj, ali funkcionira samo tijekom radnog vremena. Međutim, s obzirom na to da sud koji odobrava nadzor radi 24 sata dnevno, lako je pronaći priliku da se sustav zaobiđe. Podnošenjem zahtjeva vikendom ili izvan uobičajenog radnog vremena predmet se automatski dodjeljuje dežurnom sucu[57]. Informacije o tome tko je dežurni sudac u određeno vrijeme poznate su tajnim službama, koje tako mogu odabrati „prijateljski nastrojenog suca" kojem će podnijeti zahtjeve za nadzor[58]. Nadalje, nasumičnu dodjelu može zaobići i informatičko osoblje koje ima pristup sustavu i može dodijeliti zahtjeve za odobrenje nadzor „prijateljski nastrojenim sucima"[59]. Sve to ozbiljno umanjuje sposobnost suda da provodi učinkovit sudski nadzor.

EX POST NADZOR

41. Parlamentarni nadzor u Poljskoj praktički ne postoji. Prije 2016. na mjestu predsjednika Odbora za parlamentarni nadzorni odbor nad posebnim jedinicama policije (KSS) izmjenjivali su se članovi vladajuće stranke i oporbenih stranaka. Međutim, PiS je promijenio to parlamentarno pravilo i postavio članove PiS-a Waldemara Andzela na mjesto stalnog predsjednika i Jarosława Krajewskog na mjesto zamjenika predsjednika tog odbora[60]. Stranke koje čine Vladu u tom odboru imaju apsolutnu većinu[61]. Zbog toga je nadzorna funkcija odbora besmislena. Osim toga, vladina većina u Sejmu odbila je pozive na parlamentarnu istragu navoda o nezakonitoj uporabi špijunskog softvera[62] [63] [64] [65] [66]. S druge strane, Senat, u kojem vladine stranke nemaju većinu glasova, početkom 2022. osnovao je istražni odbor. Međutim, odbor Senata nema istražne ovlasti kao Sejm[67], čiji istražni odbor može pozvati svjedoke i saslušati iskaze pod prisegom. U

---

[56] Svjedočanstvo Ewe Wrzosek, posebno saslušanje o Poljskoj, sastanak Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, 15. rujna 2022.
[57] Svjedočanstvo Ewe Wrzosek, posebno saslušanje o Poljskoj, sastanak Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, 15. rujna 2022.
[58] Svjedočanstvo Ewe Wrzosek, posebno saslušanje o Poljskoj, sastanak Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, 15. rujna 2022.
[59] Svjedočanstvo Ewe Wrzosek, posebno saslušanje o Poljskoj, sastanak Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, 15. rujna 2022.
[60] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS.
[61] https://sejm.gov.pl/Sejm9.nsf/agent.xsp?symbol=SKLADKOMST&NrKadencji=9&KodKom=KSS.
[62] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17. siječnja 2022.
[63] Izvješće Europske komisije o vladavini prava za 2022., poglavlje o Poljskoj, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, str. 27.
[64] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosinca 2021.
[65] The Guardian, „Polish senators draft law to regulate spyware after anti-Pegasus testimony", 24. siječnja 2022.
[66] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18. siječnja 2022.
[67] Izvješće Europske komisije o vladavini prava za 2022., poglavlje o Poljskoj, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, str. 27, bilješka 220.

svakom je pokušaju odbor naišao je na otpor vladajuće stranke u Sejmu[68], vladinih dužnosnika i sigurnosnih agencija, koji su odbili surađivati i provesti vlastitu istragu[69].

42. Nadzor i pravni lijekovi drugih neovisnih tijela također su znatno oslabljeni. Vrhovni ured za reviziju ima djelotvorne nadzorne ovlasti, ali njegovi članovi i osoblje neprestano su izloženi ometanju, uznemiravanju i zastrašivanju, što ozbiljno utječe na njegove operativne sposobnosti[70]. Sejm dosad nije imenovao 10 od 19 članova Vijeća NIK-a[71]. Obvezna provjera članova vijeća za koju su zadužene posebne službe, na čelu s ministrom Kaminskim, provodi se vrlo sporo[72].

43. Ako NIK otkrije kršenje zakona, ovlašten je dostaviti obavijest Uredu javnog tužitelja[73]. Međutim, Ured javnog tužitelja odlučuje hoće li pokrenuti postupak na temelju te obavijesti. U slučaju da javni tužitelj ne poduzme mjere, NIK ima vrlo ograničene mogućnosti za daljnje djelovanje. Ako se prijavljeno kršenje odnosi na rad samog Ureda javnog tužitelja, stvara se začarani krug nepreuzimanja odgovornosti. Osim toga, svi predmeti koje NIK prijavi Uredu javnog tužitelja moraju se prijaviti glavnom javnom tužitelju, koji je ujedno i ministar pravosuđa, na čelu ministarstva koje je i kupilo špijunski softver. Glavni javni tužitelj ima ovlasti za prekidanje ili nastavljanje istraga koje je prekinulo državno odvjetništvo. Osim toga, može pokrenuti disciplinske postupke protiv tužitelja za koje smatra da su donijeli pogrešne odluke.

44. Sadašnji pučki pravobranitelj Marcin Wiącek imenovan je 2021. kad su Sejm i Senat postigli dogovor o nestranačkom kompromisnom kandidatu nakon dugotrajne rasprave[74]. Kad je riječ o slučaju senatora Brejze, Wiącek je tvrdio da se pučki pravobranitelj ne treba uključivati u rane faze postupka. Unatoč tome, i bivši i sadašnji pučki pravobranitelji prate situaciju i vrše pritisak u pogledu potrebe za osnivanjem neovisnog nadzornog tijela koje bi pružalo demokratski nadzor nad djelovanjem tajnih

[68] Bloomberg, https://www.bloomberg.com/news/articles/2022-01-03/polish-government-urged-to-probe-spyware-use-as-scandal-grows?leadSource=uverify%20wall#xj4y7vzkg, 3. siječnja 2022.
[69] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17. siječnja 2022.; Izvješće Europske komisije o vladavini prava za 2022., poglavlje o Poljskoj, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, str. 27.; AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosinca 2021.; The Guardian, „Polish senators draft law to regulate spyware after anti-Pegasus testimony", 24. siječnja 2022.; Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18. siječnja 2022.
[70] Reuters, https://www.reuters.com/article/poland-pegasus-idUSL8N2UF596, 4. siječnja 2022.; Rasprava s Vrhovnim uredom za reviziju, misija Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, rujan 2022.
[71] https://www.nik.gov.pl/en/about-us/the-council-of-nik/; Rasprava s Vrhovnim uredom za reviziju, misija Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, rujan 2022.
[72] Rasprava s Vrhovnim uredom za reviziju, misija Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, rujan 2022.
[73] Zakon o Vrhovnom uredu za reviziju od 23. prosinca 1994., https://www.nik.gov.pl/en/about-us/legal-regulations/act-on-the-supreme-audit-office.html, članak 63.
[74] Euractiv, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/, 22. srpnja 2021.

službi[75].

IZVJEŠĆIVANJE

45. Prema Zakonu o policiji iz 2016., policija je obvezna sudovima podnositi izvješća o broju prikupljanja telekomunikacijskih, poštanskih ili internetskih podataka samo dvaput godišnje, zajedno s pravnim razlozima (povezanima sa sprečavanjem ili otkrivanjem kaznenih djela, zaštitom ljudskog života ili zdravlja ili pomoći u operacijama potrage i spašavanja)[76]. Ta se izvješća mogu sastavljati isključivo *ex post* i ne objavljuju se. Ako sud uoči neki problem u vezi s podnesenim izvješćima, podnosi svoje nalaze u roku od 30 dana, ali ne može naložiti uništenje bilo kakvih podataka čak ni ako utvrdi nesukladnosti sa zakonom. Još je važnije to da su te mjere nadzora samo mogućnost i nisu obvezne.

PRAVNA ZAŠTITA

46. Unatoč brojnim dokazima da su počinjena teška kaznena djela, poljski javni tužitelj dosad je odugovlačio s djelovanjem. Čini se da su sudovi pokrenuli postupak samo u slučaju tužiteljice Ewe Wrzosek i Krzysztofa Brejze. Wrzosek je prvotno podnijela svoj predmet Uredu javnog tužitelja. Međutim, nakon što je on službeno odbio pokrenuti postupak, mogla je podnijeti žalbu sudovima. Krajem rujna 2022. Okružni sud u Varšavi (Mokotów) naložio je javnom tužitelju da pokrene istragu. Međutim, javni tužitelj dosad nije poduzeo smislene postupke koji su potrebni za napredak predmeta, kao što je saslušanje iskaza osobe koja je predmet nadzora.

47. Bitno je napomenuti da je Wrzosek mogla podnijeti žalbu sudovima tek nakon što je Ured javnog tužitelja službeno odbio njezin predmet. U mnogim drugim slučajevima javni tužitelj odugovlači s istragom kako bi izbjegao davanje službenog odgovora jer je svjestan da bi time omogućio pokretanje žalbenog postupka pred sudovima.

48. Građani koji su bili predmet nadzora mogu pokrenuti građanski postupak pred sudom, ali sami snose teret dokazivanja da su bili pod nadzorom te je praktički nemoguće dokazati nezakonitu uporabu špijunskog softvera bez suradnje nadležnih tijela. Neprovedba obveze obavješćivanja u Poljskoj, kako je navedeno u presudi u predmetu Klass, znači da mnoge osobe možda nikad ne saznaju da su bile predmet nadzora.

49. Trenutačno se predmeti Pietrzak protiv Poljske i Bychawska-Siniarska i drugi protiv Poljske vode pred ESLJP-om te otvaraju pitanja nedostatka transparentnosti, praćenja, obavješćivanja i pravnih lijekova u pogledu nadzora u Poljskoj. Važno je napomenuti da je sud odlučio održati rijetko saslušanje o tim predmetima, koje je održano 27. rujna 2022. Predmete je pokrenulo petero građana[77] koji su podnijeli pritužbe

[75] Europski parlament. Glavna uprava za usluge parlamentarnog istraživanja, „Europe's PegasusGate: Countering spyware abuse", studija, 6. srpnja 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, str. 22.
[76] Zakon o izmjeni Zakona o policiji i određenih drugih zakona od 15. siječnja 2016., članak 20.c,https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[77] Mikołaj Pietrzak, odvjetnik, predsjednik odvjetničke komore u Varšavi; Dominika Bychawska-Siniarska, članica i zaposlenica Helsinške zaklade za ljudska prava; Barbara Grabowska-Moroz, sveučilišna profesorica i istraživačica te vanjska stručna suradnica Helsinške zaklade za ljudska prava; Wojciech Klicki i Katarzyna Szymielewicz, članovi Zaklade Panoptykon iz Varšave.

ESLJP-u u rujnu 2017. i veljači 2018. Jedanaest subjekata podnijelo je podneske *amicus curiae* u tom slučaju, uključujući Europsku komoru odvjetnika krivičara[78], poljskog pučkog pravobranitelja i posebnog izvjestitelja UN-a o promicanju i zaštiti ljudskih prava i temeljnih sloboda u borbi protiv terorizma[79].

50. Iako je mogućnost podnošenja pritužbe pred ESLJP-om otvorena građanima, upitno je može li se to smatrati djelotvornim pravnim lijekom s obzirom na trajanje postupka. Pet godina nakon podnošenja prve pritužbe u ovom predmetu još uvijek nije donesena sudska odluka.

51. Na temelju članka 227. Zakonika o upravnom postupku tužbe su podnesene početkom 2017. predsjedniku vlade kao i voditeljima policijskih i obavještajnih službi. Među tim su obavještajnim službama CBA, Agencija za unutarnju sigurnost, nacionalna porezna uprava, vojna protuobavještajna agencija, nacionalna policija, granična policija i nacionalna žandarmerija. Njihove su se pritužbe odnosile na činjenicu da je članovima tih policijskih i obavještajnih službi zakonodavstvom omogućeno praćenje telekomunikacija i digitalnih komunikacija bez njihova znanja. Budući da članovi navedenih službi nisu bili dužni obavijestiti podnositelje pritužbi o mogućem nadzoru, oni nisu mogli provjeriti zakonitost te radnje na sudu, što je, prema njihovu mišljenju, protivno poljskom Ustavu.

52. Između lipnja i rujna 2017. voditelji navedenih policijskih i obavještajnih službi poslali su svoje odgovore na podnesene pritužbe. Pozivajući se na članak 8. (pravo na poštovanje privatnog i obiteljskog života) Europske konvencije o ljudskim pravima, podnositelji pritužbe naveli su da tajni sustavi za praćenje telekomunikacija, poštanskih i digitalnih komunikacija te prikupljanje metapodataka, uvedeni Zakonom o policiji i Zakonom o borbi protiv terorizma, krše njihovo pravo na poštovanje privatnog života. Pozivajući se na članak 8. i članak 13. (pravo na djelotvoran pravni lijek), podnositelji pritužbe tvrde da im nije bio dostupan djelotvoran pravni lijek koji bi im omogućio da utvrde jesu li i sami bili podvrgnuti tajnom nadzoru i, prema potrebi, da zakonitost tog nadzora preispita sud.

JAVNI NADZOR

53. Neovisni mediji još su jedan element demokratske provjere i ravnoteže koji vrši javni nadzor. Međutim, poljska javna televizija, koja je u velikoj mjeri pod kontrolom vladajućih stranaka, u slučaju uporabe špijunskog softvera zapravo je postala suučesnikom u skandalu nezakonitog nadzora, objavivši materijale pribavljene s pametnih telefona nekolicine osoba koje su bile predmet nadzora, uključujući oporbenog senatora Krzysztofa Brejzu. Objava informacija dobivenih u okviru operacije nadzora posebnih službi kazneno je djelo samo po sebi, no policija ni javni tužitelj nisu poduzeli nikakve radnje.

[78] https://www.ecba.org/content/index.php/working-groups/human-rights/857-ecba-hr-office-at-the-echr-hearing-in-the-case-pietrzak-v-poland-and-bychawska-siniarska-and-others-v-poland-hearing-29-09-2022.

[79] https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/SR/AmicusBrief_Poland_SRCT_ECHR.pdf.

POLITIČKA KONTROLA

54. Mnoge ključne položaje u cijelom lancu obnašaju članovi vladajućih stranaka ili osobe koje su im odane. Ministar unutarnjih poslova i koordinator posebnih jedinica policije Kaminski osuđen je na tri godine zatvora 2015. zbog zlouporabe ovlasti[80]. Međutim, predsjednik Duda pomilovao ga je odmah po održavanju parlamentarnih izbora 2015. u vrlo nepropisnom postupku koji su među ostalim osudili poljski Vrhovni sud, Sud Europske unije, Venecijanska komisija i Ministarstvo vanjskih poslova SAD-a. Postavilo se pitanje njegove neovisnosti i neutralnosti. Kaminski se odbio sastati ili ozbiljno surađivati s Odborom PEGA[81].

55. Ured CBA u potpunosti je pod kontrolom vladajuće većine i nije neovisan unatoč svojem nazivu i mandatu, koji je uspostavljen Zakonom o Središnjem uredu za borbu protiv korupcije od 9. lipnja 2006.[82], u čijem se članku 1. stavku 1. navodi da je „Središnji ured za borbu protiv korupcije ... osnovan kao posebna služba za borbu protiv korupcije u javnom i gospodarskom životu, posebno u javnim institucijama i institucijama lokalne vlasti te za borbu protiv aktivnosti koje štete gospodarskom interesu države”[83]. U Godišnjem izvješću o vladavini prava za 2022. Komisija je utvrdila da je „neovisnost glavnih institucija za borbu protiv korupcije i dalje problem, posebno uzimajući u obzir podređenost Središnjeg ureda za borbu protiv korupcije izvršnoj vlasti i činjenicu da je ministar pravosuđa ujedno i glavni javni tužitelj”[84].

56. Nastojanja vlade da stekne kontrolu nad pravosuđem opsežno su dokumentirala i potvrdila brojna tijela, uključujući Komisiju, Sud EU-a i Europski sud za ljudska prava.

57. Osim što je stvoren pravni i institucionalni okvir u kojem je omogućen gotovo neograničen nadzor špijunskim softverom, gotovo svi dijelovi postupka također su pod čvrstom kontrolom vladajućih stranaka. Zbog toga zaštitne mjere koje možda postoje na papiru u praksi nemaju nikakav utjecaj ili je njihov utjecaj neznatan.

METE

58. Prvi slučajevi uporabe Pegasusa u Poljskoj dokumentirani su 2018. Jedan od njih bio je slučaj bivšeg zamjenika ministra financija Pawełа Tamborskog, čiji je telefon hakiran Pegasusom u veljači 2018., što su u srpnju 2022. otkrili Amnesty International i Wyborcza. Istog je dana ured CBA pritvorio njega i pet bivših dužnosnika ministarstva i analitičara tržišta, koji su optuženi za podcjenjivanje tržišne vrijednosti društva CIECH za proizvodnju kemikalija u zamjenu za mito. Sud se nije složio s uhićenjem i naložio je njihovo puštanje na slobodu. Meta je bio i glavni izvršni direktor i vlasnik agencije Cross Media PR Andrzej Długosz, koji je hakiran najmanje 61 put između ožujka 2018. i studenoga 2019. Pučki pravobranitelj nakon toga je od vlasti zatražio više informacija,

[80] *Reuters*, https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117, 17 November 2015.
[81] EU Observer, https://euobserver.com/rule-of-law/156063, 15. rujna 2022.
[82] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf.
[83] https://www.cba.gov.pl/ftp/dokumenty_pdf/ACT_on_the_CBA_October_2016.pdf, članak 1. stavak 1.
[84] Izvješće Europske komisije o vladavini prava za 2022., poglavlje o Poljskoj, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, str. 1.

ali bez uspjeha. Vlada je i dalje poricala da je kupila špijunski softver.

59. Istragama koje su proveli istraživači iz organizacija Associated Press i Citizen Lab na Sveučilištu u Torontu utvrđeno je da su najmanje tri osobe bile mete napada špijunskim softverom u Poljskoj 2019.[85], točnije oporbeni senator Krzysztof Brejza, odvjetnik Roman Giertych i tužiteljica Ewa Wrzosek. Iako su neki članovi vladajuće većine potvrdili kupnju softvera od Grupe NSO, vlada nije službeno priznala da je bilo koja određena osoba bila njegova meta. Nijedna od triju meta nije službeno optužena ni za kakvo kazneno djelo niti je pozvana na ispitivanje. Isto tako, zbog ovog slučaja nije podnesen zahtjev za ukidanje imuniteta metama koje obnašaju javnu dužnost.

60. Agencija Citizen Lab otkrila je mnogo slučajeva zaraze u Poljskoj krajem 2017., ali u tom trenutku nije mogla utvrditi koje su osobe bile mete[86].

61. Uporaba špijunskog softvera i pokušaji kontrole građana moraju se promatrati u bliskoj vezi s izbornim sustavom. Nekoliko meta Pegasusa u određenoj je mjeri bilo povezano s izborima: senator Krzysztof Brejza (voditelj izborne kampanje najveće oporbene stranke), Roman Giertych (odvjetnik vođe oporbe i bivšeg predsjednika Europskog vijeća Donalda Tuska), Ewa Wrzosek (tužiteljica koja je istraživala glasovanje poštom na predsjedničkim izborima), Vrhovni ured za reviziju (NIK) (koji je objavio izvješća o glasovanju poštom na predsjedničkim izborima) i Michael Kolodziejczak (osnivač agrarne političke stranke koja se bori za naklonost istog biračkog tijela kao i vladajuće stranke).

62. Istodobno, neovisnost Nacionalnog izbornog povjerenstva dovedena je u pitanje jer ga čine suci koje je izabrao Parlament i sudovi koje kontrolira vladajuća stranka. Nadalje, na Okružnom sudu u Varšavi, nadležnom za registraciju novih političkih stranaka[87], rade brojni „neo-suci” koji su odani vladi i čija bi se neovisnost mogla dovesti u pitanje.

KRZYSZTOF BREJZA

63. Senator Krzysztof Brejza vodio je izbornu kampanju oporbene stranke Građanske platforme na europskim i nacionalnim izborima kada je postao meta hakiranja špijunskim softverom[88]. Njegov telefon napadnut je 33 puta dok je vodio kampanju Građanske platforme 2019. na parlamentarnim izborima. Napadi su počeli 26. travnja 2019. i nastavili se do 23. listopada 2019., nekoliko dana nakon završetka izbornog ciklusa[89].

64. Kao izravna posljedica hakiranja Brejzina telefona tekstualne poruke navodno su

---

[85] The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, 17. veljače 2022.
[86] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosinca 2021.
[87] Zakon o političkim strankama od 27. lipnja 1997., https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970980604/U/D19970604Lj.pdf, članak 11.
[88] Haaretz, https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000, 5. travnja 2022.
[89] The Guardian, „More Polish opposition figures found to have been targeted by Pegasus spyware”, 17. veljače 2022.

ukradene, izmijenjene pa objavljene na državnoj televizijskoj mreži (TVP)[90] tijekom izbora 2019. u okviru navodno orkestrirane kampanje sramoćenja[91]. Zbog toga je senator Brejza doveo u pitanje legitimnost izbora 2019. na kojima je vladajuća stranka PiS pobijedila s malom prednošću[92].

65. Iako PiS-ova vlada priznaje kupnju Pegasusa, oštro osporava navode da ga je rabila u političke svrhe[93]. Kaczynski nije ni potvrdio niti osporio napade na Brejzu, ali je tvrdio da je senator povezan sa „sumnjama na kaznena djela", što Brejza žestoko osporava[94]. Protiv Brejze nikad nije podignuta optužnica i nikad nije bio pozvan na svjedočenje. Po tome se može zaključiti da špijunski softver nije uporabljen za istragu. Impliciranjem da je Brejza povezan s kriminalnim aktivnostima vlada je pokušala službeno opravdati uporabu špijunskog softvera stvaranjem okolnosti u kojima bi poljska vlada mogla rabiti špijunski softver Pegasus zbog jednog od razloga koje Grupa NSO smatra „legitimnim" kad odlučuje o prodaji svojeg softvera vladi, točnije istrage teških kriminalnih aktivnosti[95].

66. Senator Brejza bio je meta kampanje sramoćenja koja je trajala tjednima, a u kojoj je iskorišten materijal pribavljen s pomoću špijunskog softvera Pegasus. Značajno je da je taj materijal objavljen na javnoj televiziji. Neobjašnjivo je kako javna televizijska kuća može dobiti pristup takvim materijalima. Ako je hakiranje senatora Brejze špijunskim softverom Pegasus doista bilo pitanje nacionalne sigurnosti, kao što je to vlada sugerirala, curenje materijala prikupljenog tijekom tajne sigurnosne operacije bilo bi vrlo ozbiljno kazneno djelo. Javna televizijska kuća također je pod kontrolom vladajuće stranke, što uvelike upućuje na kampanju sramoćenja koju su orkestrirale stranke na vlasti.

67. Međutim, u to je vrijeme pokrenuta kaznena istraga protiv oca senatora Brejze, Ryszarda Brejze. Dok je bio gradonačelnik Inowroclawa, grada u središnjoj Poljskoj, Brejza stariji pozvan je na ispitivanje zbog navodnog lošeg upravljanja javnim sredstvima i neispunjavanja dužnosti[96]. To se ispitivanje odvilo neposredno nakon što je Brejza mlađi pokrenuo sudski postupak protiv Kaczynskog zbog klevete. Krzysztof i Ryszard Brejza tvrdili su da su optužbe protiv Brejze starijeg bile odmazda zbog tužbe.

68. Sam Ryszard Brejza od srpnja do kolovoza 2019. primio je 10 tekstualnih poruka koje je sigurnosni laboratorij Amnesty Internationala smatrao sumnjivima i koje su imale

---

[90] Izvješće Europske komisije o vladavini prava za 2022., poglavlje o Poljskoj, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, str. 20.–23.; AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosinca 2021.

[91] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosinca 2021.

[92] Financieele Dagblad, https://fd.nl/politiek/1426857/liberalen-europarlement-eisen-onderzoek-naar-spionagesoftware, 12. siječnja 2022.

[93] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7. siječnja 2022.

[94] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7. siječnja 2022.

[95] BBC, https://www.bbc.com/news/technology-57881364, 19. srpnja 2021.

[96] AP, https://apnews.com/article/technology-business-software-hacking-spyware-8cc528ba7d46a61b378adf1ede9dd00f, 10. siječnja 2022.

obilježja Pegasusa[97]. Osim toga, dok je vodila kampanju senatora Brejze za Europski parlament, u travnju 2019. bivša pomoćnica senatora Brejze Magdalena Losko primila je četiri sumnjive tekstualne poruke koje su, prema forenzičkim ispitivačima Amnesty Internationala, tehnički odgovarale obilježjima špijunskog softvera Pegasus Grupe NSO[98].

ROMAN GIERTYCH

69. Roman Giertych postao je meta špijunskog softvera Pegasus u zadnjim tjednima parlamentarnih izbora u 2019. Od rujna do prosinca 2019. hakiran je čak 18 puta, a većina tih hakerskih napada odigrala se neposredno prije izbornog dana, 13. listopada 2019. Tada je obnašao dužnost odvjetnika vođe oporbene stranke Građanska platforma i bivšeg premijera Donalda Tuska. U tom razdoblju također je zastupao Radeka Sikorskog, bivšeg ministra vanjskih poslova i aktualnog zastupnika u Europskom parlamentu iz redova Europske pučke stranke (EPP). Sikorski je istraživao uključenost Kaczynskog i njegovih suradnika u nezakonito prisluškivanje koje je rezultiralo snimanjem i objavom razgovora Sikorskog[99].

70. Kao i u slučaju senatora Brejze, vlada nije htjela ni potvrditi ni opovrgnuti odgovornost za te napade. Organizacija Associated Press izvijestila je da je javni tužitelj podnio prijedlog za uhićenje Giertycha u pogledu navodne istrage financijskih kaznenih djela, samo nekoliko sati prije nego što je glasnogovornik državne sigurnosti Stanislaw Zaryn odgovorio na pitanja AP-a o hakiranju Giertychova telefona. Giertych oštro osporava te navode. Zaryn je odbio komentirati moguću povezanost tih incidenata. U sličnom incidentu dužnosnici ureda CBA pretresli su i pretražili Giertychov dom 2020.[100]

71. Tijekom tog razdoblja 2019. Giertych je predstavljao i Geralda Birgfellnera, austrijskog nositelja projekta. U trenutku otkazivanja dogovora Birgfellner je bio uključen u građevinski projekt za vođu PiS-a Jarosława Kaczynskog, s kojim ima obiteljske veze. Nakon objave razgovora koji su snimljeni između njih izbio je politički skandal za Kaczynskog, koji je zatim otkazao projekt. Birgfellner tvrdi da nikada nije bio plaćen za svoje usluge te je stoga angažirao Giertycha[101]. Ministar pravosuđa i glavni javni tužitelj Zbigniew Ziobro također je 2021. komentirao da nastoji podnijeti optužnicu protiv Giertycha „uz sumnju na počinjenje kaznenih djela”[102].

EWA WRZOSEK

---

[97] The Guardian, „More Polish opposition figures found to have been targeted by Pegasus spyware”, 17. veljače 2022.; Le Monde, https://www.lemonde.fr/pixels/article/2022/07/18/affaire-pegasus-un-an-apres-le-crepuscule-de-nso-group_6135168_4408996.html, 18. srpnja 2022.

[98] The Guardian, „More Polish opposition figures found to have been targeted by Pegasus spyware”, 17. veljače 2022.

[99] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosinca 2021.

[100] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosinca 2021.

[101] AP, https://apnews.com/article/elections-international-news-jaroslaw-kaczynski-european-parliament-poland-bed5ffc814e649f4bb4d10f82628b4c2, 16. veljače 2019.; TVP World, https://tvpworld.com/41262080/ruling-party-leader-im-no-dictator, 11. veljače 2019.

[102] TVP Info, https://www.tvp.info/57607147/zaryn-ws-senatora-brejzy-falszywe-sa-sugestie-ze-sluzby-nielegalnie-wykorzystuja-kontrole-operacyjna-do-gry-politycznej, 23. prosinca 2021.

72. Javna tužiteljica Ewa Wrzosek bila je žrtva šest hakerskih napada špijunskim softverom Pegasus između 24. lipnja i 19. kolovoza 2020.[103] Wrzosek je članica skupine Lex Super Omnia, udruženja javnih tužitelja koji se zalažu za neovisnost Ureda javnog tužitelja. Istraživala je odluku o održavanju poljskih predsjedničkih izbora 2020. usred globalne pandemije bolesti COVID-19 kad je skinuta s predmeta, koji je nakon toga odbačen. U ovlasti glavnog javnog tužitelja, Zbigniewa Ziobra, i njegove desne ruke, javnog tužitelja Bogdana Święczkowskija, pripada odlučivanje o nepokretanju kaznenog progona u određenim predmetima ili o skidanju podređenih javnih tužitelja s određenih predmeta[104]. Nakon toga javna tužiteljica Wrzosek premještena je u drugi Ured javnog tužitelja smješten u gradu koji se nalazi nekoliko sati od njezina doma, o čemu je obaviještena samo 48 sati unaprijed. Wrzosek je postala meta špijunskog softvera Pegasus kad se vratila u Varšavu. Poljske su vlasti, kao i obično, odbile potvrditi ili zanijekati svoju odgovornost[105] [106].

73. Wrzosek je također pokrenula pravnu pritužbu zbog zaraze Pegasusom njezina mobilnog telefona. Sud je naložio stručno mišljenje agencije Citizen Lab o zarazi Pegasusom, dok je sama Wrzosek zatražila da njezin telefon provjere stručnjaci agencije Citizen Lab. Međutim, javni tužitelj odbio je taj zahtjev i odabrao drugog stručnjaka koji nije mogao povezati ni jednu zarazu s Pegasusom. Osim toga, javni tužitelj zatražio je od telekomunikacijskog operatera da dostavi sve metapodatke koji se odnose na Wrzosek za razdoblje koje nije relevantno za sudske istrage. Wrzosek smatra da je još uvijek pod nadzorom i da je postupak javnog tužitelja usmjeren na pružanje dodatnih dokaza koji bi se mogli upotrijebiti protiv nje u drugim predmetima[107].

74. Kao što je Wrzosek istaknula na sastanku odbora PEGA od 19. siječnja 2023., Ured javnog tužitelja optužuje je za otkrivanje informacija o predmetu koji nije povezan s Pegasusom i za sudjelovanje u političkim aktivnostima. Wrzosek ne može izgraditi svoju pravnu obranu jer Ured javnog tužitelja zabranjuje pristup dokumentima[108]. To ukazuje na očito kršenje prava na pošteno suđenje i stvara se dojam da je jedina svrha predmeta diskreditirati Wrzosek.

DRUGE MOGUĆE METE

VRHOVNI URED ZA REVIZIJU

75. Iako nije meta Pegasusa, poljske su vlasti napale i uznemiravale Vrhovni ured za reviziju (NIK) koji je zadužen za zaštitu javne potrošnje i upravljanje javnim uslugama i koji je objavio račune za „kupnju posebnih tehnoloških sredstava za otkrivanje i sprečavanje kaznenih djela” u ukupnom iznosu od 25 milijuna PLN. Vrijeme napada posebno je važno s obzirom na prirodu istrage koju je NIK provodio. Glasnogovornik

[103] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosinca 2021.
[104] Izvješće Europske komisije o vladavini prava za 2022., poglavlje o Poljskoj, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, str. 16.
[105] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw--8b52e16d1af60f9c324cf9f5099b687e, 21. prosinca 2021.
[106] The Guardian, https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony, 24. siječnja 2022.
[107] Sastanak odbora PEGA, 19. siječnja 2023.
[108] Sastanak odbora PEGA, 19. siječnja 2023.

NIK-a potvrdio je da je u tijeku istraga otkazivanja predsjedničkih izbora 2020. Na temelju rezultata te istrage premijer, članovi njegove vlade i fond Ministarstva pravosuđa primili su obavijesti o kaznenim djelima. Čini se da se time pojačavaju sumnje da se Pegasus u Poljskoj uglavnom upotrebljavao u političke svrhe[109].

SURADNICI STRANKE PIS

76. Čini se da je Pegasus upotrebljavan za „preventivno prisluškivanje” vođa i organizatora uličnih prosvjeda protiv reformi Ustavnog suda koje je provela stranka PiS. Međutim, moguće je da uporaba Pegasusa nije bila ograničena na protivnike vladajuće stranke. Prema izvorima koje navodi Wyborcza, bivši glasnogovornik stranke PiS Adam Hofman špijuniran je 2018. pa je postao jedna od prvih meta nakon kupnje špijunskog softvera. Nakon što je izbačen iz PiS-a, Hofman je osnovao poduzeće za odnose s javnošću pod nazivom R4S[110] [111]. To je navodno uznemirilo vladajuću stranku, pa je Hofman postao meta nadzora. Navodi da su informacije prikupljene o njemu kasnije iskorištene u kampanji sramoćenja usmjerenoj protiv njega.

77. Osim toga, prema navodima informativnog programa Wiadomości, vlada je navodno putem Pegasusa napadala bivšeg zastupnika PiS-a u parlamentu Mariusa Antonija Kaminskia i bivšeg ministra Državne riznice Dawida Jackiewicza[112]. Mariusz A. Kaminski izbačen je iz PiS-a nakon što je umiješan u skandal istodobno s Hofmanom, dok je Jackiewicz i dalje član vladajuće stranke unatoč svojem iznenadnom odstupanju od ministarske funkcije[113].

78. Sličnu kampanju sramoćenja provela je vladajuća stranka u veljači 2018. protiv bivšeg predsjednika udruženja poslodavaca Republike Poljske Andrzeja Malinowskog. Svjedočio je na posebnoj sjednici odbora Senata u travnju 2022. u vezi s hakiranjem njegova telefona Pegasusom kako bi prikupile informacije za to javno diskreditiranje[114]. Istaknuo je da su poruke preuzete iz njegova WhatsAppa i SMS-a koristeći sustav Pegasus te da se strateški upotrebljavaju za širenje mržnje protiv njega na internetu. Taj je napad bio odmazda zbog neslaganja s vladajućom strankom i zahtijevanja alternativnih gospodarskih politika.

ZAKLJUČNE NAPOMENE

79. Zloupotreba Pegasusa u Poljskoj mora se promatrati u punom kontekstu krize vladavine prava u zemlji, koja je započela 2015. kada je vlada, pod vodstvom PiS-a, započela s rušenjem pravosudnog sustava i otada je sustavno preuzimala najvažnije institucije u zemlji, postavljajući osobe odane vladajućim strankama u sve strateške urede. Vladajuća stranka planski je i metodički objedinila pravne, institucionalne i političke

[109] Poljske bilješke, https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/, 7. veljače 2022.
[110] https://wyborcza.pl/7,173236,28015977,polish-state-surveilled-nearly-50-targets-with-pegasus-spyware.html?disableRedirects=true.
[111] Rzeczpospolita, https://www.rp.pl/polityka/art4805251-hofman-usuniety-z-pis-decyzja-w-sprawie-hofmana, 11. listopada 2014.
[112] https://wiadomosci.onet.pl/kraj/pegasus-oto-kolejne-osoby-ktore-mialy-byc-inwigilowane-przez-sluzby-pis/yvt6tym.
[113] https://nextvame.com/dawid-jackiewicz-is-back-jaroslaw-kaczynski-confirms-the-reports/.
[114] https://www.senat.gov.pl/prace/komisje-senackie/przebieg,9668,1.html.

elemente tog sustava kako bi stvorila usklađen i vrlo djelotvoran okvir u kojem je upotreba Pegasusa sastavni i ključni dio sustava za nadzor oporbe i kritičara vlade za ostvarenje političke koristi. Osmišljen je tako da vladajuća većina i vlada ostanu na vlasti.

80. Opseg nadzora u Poljskoj znatno je proširen tijekom proteklih nekoliko godina, čime su oslabljene ili uklonjene zaštitne mjere i odredbe o nadzoru. Tijekom sustavnih i ciljanih zakonodavnih promjena koje je donijela vladajuća većina prava žrtava maksimalno su umanjena, a pravni lijek i pravna zaštita u praksi su postali beznačajni. Učinkovit *ex ante* i *ex post* nadzor, kao i neovisni nadzor, *de facto* su ukinuti. Članovi poljske vlade i osobe odane vladajućim strankama izravno ili neizravno kontroliraju glavne položaje u tom sustavu. Informacije prikupljene s pomoću špijunskog softvera upotrebljavaju se u kampanjama sramoćenja kritičara vlade i pripadnika oporbe koje se provode putem državnih medija pod kontrolom vlade. Činjenica da poljska vlada širi zakone na taj sustavan i ciljani način u skladu s nacionalnim pravom predstavlja pravnu osnovu za nadzor, čime se čvrsto krše pravo EU-a, presuda poljskog Ustavnog suda iz 2014. i temeljna prava poljskih građana. Na taj je način protuzakoniti nadzor kojim se očito krši pravo EU-a i nacionalno pravo u osnovi legaliziran.

I.B Mađarska

81. Mađarska je bila jedna od prvih država upletenih u europski skandal povezan sa špijunskim softverom. Projekt Pegasus 2021. otkrio je, što potvrdio i Amnesty International,[115] da je više od 300 Mađara možda bilo žrtvom zloupotrebe Pegasusa, uključujući političke aktiviste, istraživačke novinare, odvjetnike, poduzetnike, oporbene političare i bivšeg vladinog ministra.

82. U veljači 2023. izaslanstvo odbora PEGA posjetilo je Mađarsku. Zaključilo je da postoje sve naznake da je špijunski softver teško zloupotrijebljen u Mađarskoj i da se objašnjenje vlasti u kojem se kao razlog navodi nacionalna sigurnost smatralo vrlo neuvjerljivim. Čvrsti dokazi upućuju na to da su osobe bile špijunirane u cilju stjecanja još veće političke i financijske kontrole nad javnom sferom i medijskim tržištem.

83. Odbor je uvjeren da su vladavina prava i osnovni demokratski standardi ozbiljno prekršeni u Mađarskoj i da je situacija u toj zemlji među najgorima u EU-u. Kao rezultat godina demokratskog nazadovanja, čini se da državne institucije nisu usmjerene na služenje građanima i zaštitu njihovih prava i sloboda, već na ostvarivanje političkih ciljeva vlade. Odbor je pozvao vlasti da omoguće smislenu istragu zlouporabe.

KUPNJA PEGASUSA

84. Tijekom 2017. Odbor za nacionalnu sigurnost mađarskog parlamenta glasovao je o tome da se obavještajnim službama te zemlje omogući nabava određenih dijelova opreme u skladu s redovnim postupkom javne nabave. Na zahtjev Posebne službe za nacionalnu sigurnost (Nemzetbiztonsági Szakszolgálat, NBSZ) mađarski parlament

[115] Euractiv, „Hungary employed Pegasus spyware in hundreds of cases, says government agency”, *1. veljače 2022.*

podržao je nabavu sofisticiranog špijunskog softvera[116]. Međutim, postupak je bio tajan, a u zahtjevima za odobrenje nije navedena posebna robna marka i vrsta tehnologije[117].

85. Mađarsko Ministarstvo unutarnjih poslova kupilo je Pegasus za 6 milijuna EUR neizravno preko društva Communication Technologies Ltd od društva Grupe NSO u Luksemburgu 2017., nedugo nakon što se premijer Viktor Orbán sastao sa svojim poljskim kolegama Mateuszom Morawieckim i bivšim izraelskim premijerom Benjaminom Netanyahuom[118] [119]. Mađarsko Ministarstvo unutarnjih poslova to je potvrdilo tek u studenome 2021., kad je predsjednik Odbora za obranu i kazneni progon mađarskog parlamenta Lajos Kósa priznao da je Fideszova vlada kupila Pegasus[120]. Međutim, Kósa je i dalje tvrdio da taj špijunski softver nikad nije upotrijebljen protiv mađarskih građana[121].

86. Mađarsko nacionalno tijelo za zaštitu podataka i slobodu informiranja (NAIH) istraživalo je postupak nabave za kupnju špijunskog softvera i dobilo pristup tajnom ugovoru s NSO-om. Tijekom misije odbora PEGA u Budimpešti u veljači 2023. predsjednica NAIH-a Attila Péterfalvi prvotno je izjavila da nije točno da je mogućnost uporabe Pegasusa mađarskim vlastima ukinuta, što bi značilo da Mađarska nije bila jedna od dviju država članica EU-a koja je uklonjena s popisa od 14 zemalja kojima NSO omogućuje uporabu Pegasusa. Péterfalvi je kasnije povukla svoju izjavu tvrdeći da ne raspolaže informacijama o tome je li NSO prestao koristiti Pegasus u Mađarskoj ili ne.

PRAVNI OKVIR

87. U Mađarskoj je okvir za zakonito presretanje komunikacija u kontekstu kaznene istrage propisan Zakonom o policiji. U skladu sa Zakonom o policiji nadzor fizičkih osoba u okviru kaznene istrage može se provoditi samo uz sudsko odobrenje. Međutim, kad je riječ o pitanjima povezanima s terorizmom, u Zakonu o policiji upućuje se na istražni nadzor naveden u Zakonu o nacionalnoj sigurnosti[122]. U skladu s tom odredbom nije potrebno tražiti sudsko odobrenje kako bi se odobrila primjena tih tehnika, već je

---

[116] Studija – „Uporaba Pegasusa i jednakovrijednog špijunskog softvera – postojeći pravni okvir u državama članicama EU-a za nabavu i uporabu Pegasusa i jednakovrijednog špijunskog softvera za nadzor”, Europski parlament, Glavna uprava za unutarnju politiku, Resorni odjel C – prava građana i ustavna pitanja, 5. prosinca 2022., dostupno na adresi: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf. Direkt36, The inside story of how Pegasus was brought to Hungary, https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/.

[117] Misija odbora PEGA u Mađarskoj, sastanak s članovima Odbora za nacionalnu sigurnost mađarskog parlamenta, 20. i 21. veljače 2023.

[118] Financieele Dagblad, De wereld deze week: het beste uit de internationale pers. 7. siječnja 2022.

[119] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 srpnja 2021.

[120] DW, „Hungary admits to using NSO Group’s Pegasus spyware” (Mađarska priznaje uporabu špijunskog softvera Pegasus grupe NSO), 4 studenoga 2021.

[121] DW, „Hungary admits to using NSO Group’s Pegasus spyware” (Mađarska priznaje uporabu špijunskog softvera Pegasus grupe NSO), 4 studenoga 2021.

[122] Agencija Europske unije za temeljna prava (FRA), „National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary” (Nacionalna obavještajna tijela i nadzor u EU-u: mjere zaštite temeljnih prava i pravni lijekovi: Mađarska), 26 rujna 2014.

umjesto toga ministar pravosuđa odgovoran za izdavanje odobrenja[123]. U zahtjevima za odobrenje nadzora ne spominje se vrsta tehnologije koja će se upotrebljavati[124].

88. U skladu sa Zakonom CXXV. iz 1995. interes nacionalne sigurnosti definiran je kao „osiguravanje suverenosti i zaštita zakonitosti Mađarske i u tom okviru”, što je prilično općenita definicija.

89. U značajnom predmetu (Szabó i Vissy protiv Mađarske[125]) Europski sud za ljudska prava (ESLJP) utvrdio je da Zakonom o nacionalnoj sigurnosti nisu predviđene dovoljno precizne, učinkovite i sveobuhvatne zaštitne mjere u pogledu propisivanja, provedbe i mogućeg poboljšanja mjera nadzora. Zakonom o nacionalnoj sigurnosti izostavlja se obveza obavješćivanja predmeta nadzora i izričito se propisuje da stranka koja izdaje ovlaštenje ne smije obavijestiti mete nadzora da ih se špijunira[126]. ESLJP nedvojbeno je utvrdio obvezu obavješćivanja žrtava u predmetu Klass i drugi protiv Njemačke[127]. Osim toga, ne postoje djelotvorne mogućnosti za pravni lijek i pravnu zaštitu u slučaju zlouporabe, kao ni odgovarajući nadzor. Mađarska vlada dosad nije provela nijednu od tih odluka.

EX ANTE NADZOR

90. Prema Zakonu o nacionalnim sigurnosnim službama, nadzor koji provodi Posebna služba za nacionalnu sigurnost (SNSS) s pomoću špijunskog softvera u većini slučajeva ovisi o odobrenju ministra pravosuđa, a u nekim određenim slučajevima o sucu kojeg imenuje predsjednik Gradskog suda u Budimpešti[128] [129]. Protiv tih odluka ne postoji mogućnost žalbe i ne postoji praktički nikakav nadzor nad tim procesom[130] [131].

91. Unatoč ozbiljnosti takve odluke, kada nije u mogućnosti, sadašnja ministrica pravosuđa Judit Varga prenosi odgovornost za odobravanje uporabe špijunskog softvera protiv građana na državnog tajnika Ministarstva pravosuđa, dužnost koju trenutačno obnaša Robert Repassy[132]. To je sam Repassy potvrdio u odgovoru na pismena pitanja o tom

---

[123] Agencija Europske unije za temeljna prava (FRA), „National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary” (Nacionalna obavještajna tijela i nadzor u EU-u: mjere zaštite temeljnih prava i pravni lijekovi: Mađarska), pravna izmjena, 23. listopada 2017.
[124] Misija odbora PEGA u Mađarskoj, 20. i 21. veljače 2023.
[125] Szabó i Vissy protiv Mađarske, zahtjev br. 37138/14, presuda od 12. siječnja 2016., https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}.
[126] Zakon CXXV o nacionalnim sigurnosnim službama iz 1995., http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf.
[127] Klass i ostali protiv Njemačke, 6. rujna 1978., točka 50., serija A, br. 28.
[128] Zakon CXXV o nacionalnim sigurnosnim službama iz 1995., http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf odjeljci 56–58.
[129] Europe’s PegasusGate: Countering Spyware Abuse - – izvješće Službe Europskog parlamenta za istraživanja, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, srpanj 2022., str. 20.
[130] Zakon CXXV o nacionalnim sigurnosnim službama iz 1995.,http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf odjeljci 57 i 58.
[131] Izvješće Europske komisije o vladavini prava za 2022., https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf, str. 26.
[132] https://telex.hu/belfold/2021/12/10/repassy-robert-igazsagugyi-allamtitkar-varga-judit-igazsagugyi-miniszterium; Europe’s PegasusGate: Countering Spyware Abuse, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, srpanj 2022, str. 20.

problemu[133]. Opće je poznato da je Varga redovito prenosila odgovornost na Repassyjeva prethodnika Pála Völnera, koji je u prosincu 2021. bio prisiljen dati ostavku na tu dužnost zbog velikog korupcijskog skandala[134]. Često se navodilo da je prihvatio milijune mađarskih forinti kao mito od niza istaknutih dionika u zamjenu za povoljne odluke i imenovanja na ključne položaje, što je Völner provodio u okviru funkcije državnog tajnika[135].

92. Iako ministar unutarnjih poslova Sándor Pintér ustraje u tome da se taj postupak odobrenja uvijek provodi bez iznimke preko ministra ili sudova[136], slabe pravne odredbe Zakona o nacionalnoj sigurnosti isto tako omogućuju da glavni direktori SNSS-a izdaju privremeno odobrenje za provedbu nadzora bez pristanka sve dok se ne izda službena dozvola. To omogućuje SNSS-u da djeluje bez odgovarajućeg sudskog odobrenja sve dok tvrdi da bi kašnjenje pri dobivanju odobrenja štetilo njegovu radu. U takvim se slučajevima neovlašteni nadzor može nastaviti[137].

93. Zakonski rok od najviše 90 dana za nadzor propisan predmetnim Zakonom može se produljiti za dodatnih 90 dana jednostavno na temelju zahtjeva glavnog direktora upućenog službeniku koji izdaje dozvole[138], što je predviđeno samo radi prisutnosti pravne zaštite.

94. Osim toga, uloga je NAIH-a nadgledati cjelokupni nadzor tajnih službi. Predsjednica NAIH-a Attila Péterfalvi neprestano je tvrdila da se Pegasus koristio u svrhu nacionalne sigurnosti, što je u isključivoj nadležnosti nacionalnih vlada[139]. Međutim, NAIH je provjerio postupak odobrenja samo na temelju tehničkih razloga kako bi ocijenio je li obrada podataka bila zakonita, ali nije ispitao stvaran razlog uporabe Pegasusa. NAIH nije vidio potrebu pozvati mete da svjedoče jer je imao pristup svim relevantnim dokumentima. Istraženi su samo slučajevi koje je odobrio ministar pravosuđa jer NAIH ne može istraživati odobrenja koja je izdao sudac[140].
Prema navodima predsjednice Péterfalvi istraga NAIH-a nije otkrila nezakonite aktivnosti ili nešto što bi bilo protivno uvjetima prodaje Grupe NSO[141].

95. Voditelja NAIH-a imenuje predsjednik vlade te stoga njegova neovisnost može dovesti u pitanje[142]. ESLJP je o tom pitanju donio presudu u rujnu 2022. u predmetu Hüttl

---

[133] https://telex.hu/belfold/2022/01/27/varga-judithoz-kerulhetett-vissza-a-titkos-megfigyelesek-engedelyezese.
[134] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye; https://hungarytoday.hu/444-key-figure-in-volner-corruption-case-gyorgy-schadl-judge-fired-judiciary-obh/.
[135] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye.
[136] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4. studenoga 2021.
[137] Zakon CXXV o nacionalnim sigurnosnim službama iz 1995., http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, odjeljak 59.
[138] Zakon CXXV o nacionalnim sigurnosnim službama iz 1995., http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, odjeljak 58.
[139] HVG, https://hvg.hu/itthon/20111117_Peterfalvi_palyaja_adatvedelem, 21. studenoga 2011.
[140] Misija odbora PEGA u Mađarskoj, 20. veljače 2023.
[141] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1. veljače 2022.
[142] https://hclu.hu/en/pegasus-whats-new.

protiv Mađarske[143] koji je pokrenuo odvjetnik Mađarskog saveza za građanske slobode (HCLU) Tivadar Hüttl kada je, nakon što su ga navodno prisluškivali, Odbor za nacionalnu sigurnost odlučio da neće pokrenuti daljnju istragu i nisu bili dostupni pravni lijekovi[144]. ESLJP u svojoj je presudi naveo da NAIH, iako ima pravo istražiti postupke tajnih službi, nije mogao provoditi neovisan nadzor nad primjenom nadzora. Sud je smatrao da NAIH nije imao potrebnu nadležnost za to, s obzirom da tajne službe imaju pravo uskratiti pristup određenim dokumentima na temelju tajnosti[145]. U tom bi slučaju odgovornost da provede reviziju bila na ministru zaduženom za tajne službe, što se ni na koji način ne bi moglo smatrati neovisnim nadzorom[146].

EX POST NADZOR

96. U prosincu 2021., na insistiranje oporbe, Odbor za nacionalnu sigurnost i Odbor za obranu i sigurnost u Nacionalnoj skupštini provela su saslušanja o uporabi špijunskog softvera u Mađarskoj, a posebno o navodnoj vladinoj politički motiviranoj uporabi tog softvera za nadzor građana. Vladajuća stranka imala je četiri od šest mjesta u Odboru za nacionalnu sigurnost i onemogućila svaki smislen i demokratski nadzor nad uporabom Pegasusa. Predstavnici vladajuće stranke ustrajali su u tvrdnjama da je sav nadzor bio odobren odgovarajućim kanalima, ali su odbili komentirati pitanje jesu li na meti bili novinari ili političari. Također su odbili komentirati činjenicu da je ministar pravosuđa dodijelio odobrenja državnom tajniku Pálu Völneru, koji je pod istragom zbog optužbi za korupciju i zlouporabu ovlasti. Isto su tako odbili zahtjeve članova oporbe da provedu detaljnu istragu i posjete sigurnosne službe kako bi se obavili razgovori s pojedinačnim agentima. Odbor nije saslušao ključne mete, kao što su Zoltán Varga i Szabolcs Panyi. U kolovozu 2021. provedena je samo *pro forma* opća istraga jer je to bila jedina metoda koja je dobila potporu većine[147]. Međutim, nije moguće utvrditi što je točno bilo rečeno, budući da je vladajuća stranka zapisnik sa sastanka označila povjerljivim do 2050.[148]

97. Istraga NAIH-a pokrenuta je na temelju optužbi najmanje deset odvjetnika, predsjednika Mađarske odvjetničke komore i najmanje pet novinara koji su bili mete[149]. Dobiveno izvješće objavljeno je 31. siječnja 2022. i u njemu je zaključeno da je razlog uporabe Pegasusa isključivo nacionalna sigurnost.

98. Slično tome, mađarsko državno odvjetništvo zaključilo je 15. lipnja 2022. istragu o nadziranju, zaključivši da nije proveden nikakav neovlašteni nadzor.

---

[143] https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-219501%22]}.
[144] https://tasz.hu/cikkek/valoszinusithetoen-lehallgattak-pert-nyert-strasbourgban-a-tasz-ugyvedje; https://hudoc.echr.coe.int/fre?i=001-219501.
[145] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere.
[146] https://444.hu/2022/10/12/emberi-jogok-birosaga-az-adatvedelmi-hatosag-alkalmatlan-a-lehallgatasok-ellenorzesere.
[147] Misija odbora PEGA u Mađarskoj, sastanak s članovima Odbora za nacionalnu sigurnost mađarskog parlamenta, 20. veljače 2023.
[148] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4. studenoga 2021.
[149] Izvješće Komisije o vladavini prava za 2022., https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, str. 26.

99. S obzirom na to da ovlast za izdavanje odobrenja imaju Ministarstvo pravosuđa i Péter Polt, glavni javni tužitelj kojeg podupire Fidesz, ponovno je izabran 2019. na dodatnih devet godina (nakon što je do tada obnašao dužnost u kombiniranom razdoblju od 15 godina tijekom dva različita mandata), stvaran nadzor vlade može se dovesti u pitanje.

100. U mađarskom okviru za borbu protiv korupcije ne postoji potpora kao odgovor na to, s obzirom da je Ministarstvo unutarnjih poslova, koje je prvotno kupilo Pegasus od Grupe NSO, odgovorno za koordinaciju svih antikorupcijskih politika i nadzora[150].

PRAVNA ZAŠTITA

101. Kad je u Mađarskoj izbio skandal povezan s Pegasusom, novinari su bili jedna od skupina protiv kojih je vlada najviše upotrijebila taj softver. Zbog toga je skupina od šestero novinara i aktivista u Mađarskoj početkom 2022. pokrenula pravne postupke pred mađarskim vlastima, Komisijom i ESLJP-om. Mađarski savez za građanske slobode (HCLU) predstavlja novinare Brigittu Csikász, Dávida Dercsényija, Dániela Németha i Szabolcsa Panyija, uz Adriena Beauduina, belgijsko-kanadskog doktoranda i aktivista. Šesta stranka u postupku odlučila je ostati anonimna. HCLU također surađuje s Eitayjem Mackom u Izraelu na podnošenju prijave glavnom javnom tužitelju s ciljem pokretanja istrage protiv Grupe NSO[151].

102. Mnoga tehnička obilježja blokiraju put za ovaj predmet na mađarskim sudovima. Budući da u tom području ne postoji dovoljno sudske prakse, postupci su nejasni. Na primjer, pojavila su se pitanja u pogledu nadležnosti. Takvi postupci i neprestana kašnjenja uglavnom se smatraju pokušajima odbacivanja predmeta zbog tehničkog ili postupovnog pitanja.

103. Postoji i ozbiljan problem u pogledu pristupa informacijama. Kako bi se zatražio pristup spisima koji sadržavaju sve podatke prikupljene o svakom pojedincu, potrebno je navesti točan naziv spisa na koji se zahtjev odnosi, koje je gotovo nemoguće pribaviti. Budući da je Vrhovni sud neizbježno odbio zahtjeve šest stranaka koje zastupa HCLU, predmetni je savez zatražio odluku Ustavnog suda kojom se ta praksa proglašava neustavnom, kao i presudu mađarskog Vrhovnog suda. Međutim, Ustavni je sud 2021. odbio prijedlog HCLU-a.

104. Osim tužbama pred sudovima, HCLU se služio i drugim načinima pristupa podacima svojih šest klijenata. Pokrenut je i prihvaćen upravni postupak na temelju Zakona o povjerljivim podacima i Zakona o zaštiti podataka. Međutim, Ured za zaštitu ustavnosti provest će cjelogodišnje preispitivanje u svakom pojedinačnom predmetu prije objave rezultata[152]. Nadalje, napadi špijunskim softverom prijavljeni su povjereniku za temeljna prava (pučki pravobranitelj). Ustavni je sud utvrdio da je odgovornost pučkog

[150] Izvješće Komisije o vladavini prava za 2022., https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, str. 10.
[151] The Guardian, https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state, 28. siječnja 2022.
[152] https://hclu.hu/en/pegasus-case-hungarian-procedures.

pravobranitelja da istraži zlouporabe koje su vršile tajne službe[153].

105. U drugom pokušaju postizanja određene transparentnosti HCLU je zatražio pristup podacima koji se prikupljaju i obrađuju zbog hakiranja šest osoba koje su bile mete u okviru postupka koji se provodi izvansudskim putem. Međutim, pravo na te informacije postoji samo ako takvo pružanje podataka ne utječe na nacionalnu sigurnost[154]. To je još jedan izgovor da se mađarske vlasti ponovno pozovu na razloge povezane s nacionalnom sigurnošću[155]. Do sada je Ured za zaštitu ustavnosti odbio 270 zahtjeva za slobodu informiranja koje je podnio HCLU u razdoblju od 2018. do svibnja 2022[156].

POLITIČKA KONTROLA

106. U Mađarskoj politika ima potpunu kontrolu nad primjenom nadzora. Režim Orbánova Fidesza uspostavio je sustav u kojem mete mogu biti odvjetnici, novinari, politički protivnici i organizacije civilnog društva.

107. Ministar unutarnjih poslova u prvoj je fazi bio odgovoran za kupnju špijunskog softvera Pegasus, a ministar pravosuđa i dalje je nadležan za odobravanje njegove uporabe. U više su navrata utvrđeni nedostaci mađarskog zakonodavnog okvira povezanog s nadzorom njezinih građana. Međutim, vladajuća stranka neće ga mijenjati jer odgovara njezinim potrebama.

108. Predsjednik vlade odabire voditelja NAIH-a, tijela odgovornog za neovisan nadzor nad korištenjem Pegasusa od strane tajnih službi. S obzirom na to da je on imenovan u okviru politike, ne postoji neovisni nadzor. Mađarskoj i Fideszovoj vladi nisu strane te vrste političkih imenovanja. Vlada je sustavno postavljala osobe odane vladajućoj stranki na vodeće položaje u tijelima kao što su Ustavni sud, Vrhovni sud, Revizorski sud, državno odvjetništvo, Mađarska narodna banka i Nacionalno izborno povjerenstvo[157]. Time se osigurava da svaka institucija osnovana s namjerom provođenja nadzora izvršne vlasti ne može obavljati svoju dužnost na neovisan način[158].

109. Kad je riječ o praktičnom dijelu provedbe nadzora uporabom špijunskog softvera, telekomunikacijska poduzeća imaju važnu ulogu. Postoji više slučajeva zaraze uređaja meta putem poveznica koje se šalju SMS-om, a brojni podaci kojima telekomunikacijska poduzeća imaju pristup vrlo su privlačni onima koji žele provoditi nadzor. U slučaju Mađarske situacija je postala opasnija jer je mađarska vlada nedavno kupila pružatelja telekomunikacijskih usluga Vodafone Hungary[159]. Uz potporu mađarske vlade društvo 4iG kupilo je 51 % udjela u društvo Vodafone putem društva

[153] https://hclu.hu/en/pegasus-whats-new.
[154] https://hclu.hu/en/pegasus-case-hungarian-procedures.
[155] https://hclu.hu/en/pegasus-whats-new.
[156] https://hclu.hu/en/pegasus-whats-new.
[157] Martin, J. i Ligeti, M., „Hungary. Lobbying, State Capture and Crony Capitalism", „Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries", Bitonti, A. i Harris, P. (ur.), Springer, 2017., str. 177.–193., str. 178.
[158] Martin, J. i Ligeti, M., „Hungary. Lobbying, State Capture and Crony Capitalism", *Lobbying in Europe:* Public Affairs and the Lobbying Industry in 28 EU Countries", Bitonti, A. i Harris, P. (ur.), Springer, 2017., str. 177.–193., str. 178.
[159] Reuters, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22. kolovoza 2022.

kćeri. Osim toga, mađarska vlada kupila je 49 % udjela društva Vodafone putem drugog društva. Veze između društva 4iG i vlade očite su. Sadašnji predsjednik tog društva bio je bliski suradnik mađarskog oligarha Lőrinca Mészárosa, prijatelja iz djetinjstva Viktora Orbána. Ukupni troškovi nabave iznose 1,7 milijardi EUR i omogućit će vladi jednostavan i izravan pristup podacima za više od 3 milijuna potrošača[160]. Usto, zbog te kupnje država će imati pristupnu točku desetljećima starom globalnom sustavu za razmjenu poruka poznatom pod nazivom SS7[161]. Taj sustav omogućuje mobilnim operaterima da povežu korisnike diljem svijeta. Mađarska će moći dodatno iznajmljivati takvu pristupnu točku, kao što je bio slučaj s grupom Rayzone[162].

METE

110. Prema izvješćima, u nalaze koje je objavio Pegasus Project uključeni su telefonski brojevi preko 300 osoba [163]. Među njima je bilo najmanje pet novinara, deset odvjetnika, gradonačelnik Gödöllőa, koji je član oporbene stranke, zaposlenik oporbene stranke, kao i aktivisti i istaknuti poduzetnici[164]. Međutim, nijedna od tih osoba nije bila predmet kaznene istrage niti je optužena za nešto. Iako prisutnost telefonskih brojeva na tom popisu ne znači nužno da su telefoni zaista hakirani, svejedno pruža znakovit uvid u metodičke i sustavne postupke Orbánove vlade i u njezin stav prema temeljnim pravima i slobodi medija. Od tog trenutka u 2021. potvrđeno je da su brojne mete uspješno hakirane špijunskim softverom. Od trenutka kad je u Mađarskoj izbio skandal povezan sa špijunskim softverom bilo je sasvim jasno da su postupci vlade bili politički motivirani.

SZABOLCS PANYI

111. Telefon novinara i urednika Szabolcsa Panyija hakiran je za vrijeme njegova rada za Direkt36. Kao jedan od malobrojnih preostalih neovisnih izvora vijesti u Mađarskoj, Direkt36 jedna je od najvažnijih meta vladajuće stranke. Panyi je poznat i ugledan novinar, što znači da bi, uz prikupljanje ključnih informacija izravno od samog Panyija, brojni kontakti i izvori iz njegova telefona za Vladu bili dragocjen usputan ulov.

112. Amnesty International potvrdio da je 2019. Panyijev telefon stalno hakiran u razdoblju od sedam mjeseci[165]. Ti su napadi bili ciljani i često su se događali u vrijeme kada je Panyi tražio od vlade da dostavi komentare na ta pitanja. Konkretan i zabrinjavajući primjer takvog napada dogodio se 3. travnja 2019. Panyi se obratio vladi tražeći komentar na članak u kojem je detaljno opisao preseljenje ruske banke u glavni grad

[160] Reuters, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22. kolovoza 2022.; Volkskrant, Orbán verstevigt met overname Vodafone Hongarije grip op telecommunicatie, critici uiten zorgen.
[161] The Guardian, https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands, 16. prosinca 2020.
[162] https://www.haaretz.com/israel-news/tech-news/2020-12-17/ty-article/israeli-spy-tech-firm-tracked-mobile-users-around-the-world-investigation-suggests/0000017f-e76b-da9b-a1ff-ef6f847c0000.
[163]Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.
[164] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021. i Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.
[165] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.

Mađarske, priča koja je medijski bila dosta popraćena, s obzirom na to da se postavljalo pitanje je li banka zapravo bila paravan ruskih obavještajnih službi[166]. Amnesty International potvrdio je da je Panyijev telefon hakiran sljedećeg dana te je dodatno utvrdio još 11 takvih slučajeva hakiranja neposredno nakon zahtjeva za iznošenje komentara Orbánove uprave[167]. Iz toga proizlazi da je više od polovice Panyijevih zahtjeva rezultiralo napadima u tom razdoblju od sedam mjeseci[168].

113. Vlasti su negirale saznanja o napadima na Panyija te nisu htjele ni potvrditi ni opovrgnuti odgovornost za njih. Međutim, vlada je prethodno javno napala Panyija, pri čemu je Orbánov glasnogovornik tvrdio da je on fanatični politički aktivist te ga optužio za orbánofobiju i hungarofobiju[169]. To je očit pokušaj diskreditiranja Panyija i prikazivanja njegovih izvora i njega kao „neprijatelja” putem vladinih državnih medija.

114. Nakon istrage koju je Panyi proveo protiv mađarskog brokerskog društva Communication Technologies Ltd, preko kojeg je kupljen Pegasus, društvo ga je tužilo[170].

ZOLTÁN VARGA

115. Kao glavni izvršni direktor i predsjednik poduzeća Central Media Group, Zoltán Varga vlasnik je posljednjeg preostalog mađarskog neovisnog informativnog portala 24.hu. Nakon što je Orbánova vlada 2020. pokrenula preuzimanje njegovog glavnog konkurenta, portala Index.hu, Varga je ostao „posljednji preživjeli” koji nastavlja pružati otpor vladajućoj stranci[171].

116. Fidesz već neko vrijeme provodi kampanju sramoćenja Varge putem državnih medija pod kontrolom vlade kako bi diskreditirao njegovu javnu osobu i objavljivanje, unatoč svojoj popularnosti, s publikom od više od 7,5 milijuna osoba mjesečno[172]. Varga tvrdi da ga se navodilo na prodaju uz prijetnje u različitim prilikama, uključujući ponude koje uključuju velikodušne državne subvencije za oglašavanje u zamjenu za zapošljavanje uredničkog osoblja po vladinu izboru[173]. Varga je prvi put posumnjao da je njegov telefon zaražen Pegasusom kada je tijekom poziva u pozadini čuo reprodukciju telefonskog razgovora. Nakon toga 2021. Amnesty International otkrio je da je Varga doista najvjerojatnije bio hakiran Pegasusom, ali to se nije moglo potvrditi zbog

[166] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[167] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[168] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[169] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[170] Misija odbora PEGA u Budimpešti, 20. i 21. veljače 2023.
[171] https://www.mapmf.org/alert/25319.
[172] Politico, https://www.politico.eu/article/viktor-orban-bent-on-muzzling-independent-press-hungarian-media-mogul-warns-index-24-hu-news-sites/, 25. srpanj 2020.
[173] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.

činjenice da je telefon kasnije zamijenjen[174].

117. Osim toga, ubrzo nakon izbora 2018. ponovno izabrani Orbán pokušao je neizravno doći do Varge. Nakon večere na kojoj se raspravljalo o vladinom preuzimanju medija, koju je organizirao Varga u proljeće 2018., kojoj je prisustvovao i Attila Chikán, bivši ministar Fideszove vlade koji je postao Orbánov kritičar, potvrđeno je da su svi prisutni bili kandidati za nadzor[175]. Naknadno je potvrđeno da je jedan gost hakiran tijekom večere, dok su se za druge telefone utvrdili tragovi potencijalnih hakerskih napada Pegasusom, ali nije bilo dokaza o uspješnoj zarazi[176]. Hakiranje je gotovo potvrdilo Vargin poznanik, koji je povezan s vladom i koji je u razgovoru izravno spomenuo večeru i upozorio na druženje s osobama koje bi mogle biti „opasne”[177].

118. Varga je isto tako bio podvrgnut tradicionalnom nadzoru. Prisluškivanje u poslovnom okruženju, automobili koji kruže oko njegova doma te helikopteri koji ga oblijeću, kao i nekoliko upada u njegov vrt bili su razlog uspostave cjelodnevnog osiguranja.

119. U listopadu 2022. protiv Varge su pokrenute kaznene prijave. Policija ga je pozvala na ispitivanje, a samo nekoliko minuta kasnije mediji naklonjeni vladi već su izvještavali o tome[178].

ADRIEN BEAUDUIN

120. Adrien Beauduin privukao je pozornost Orbánova režima dok je 2018. dovršavao doktorat iz rodnih studija na Srednjoeuropskom sveučilištu. Tu je ustanovu osnovao George Soros i Vlada ju je u ono vrijeme pokušavala istjerati iz Mađarske, zajedno s čitavim predmetom rodnih studija[179]. Beauduin je uhićen nakon što je prisustvovao prosvjedu u Budimpešti. Njegovo je uhićenje protumačeno kao uvelike politički motiviran potez. Optužen je za napad na policijskog službenika, koji odlučno poriče[180]. Prema izvještajima, protiv Beauduina u osnovi nije bilo nikakvih dokaza, a dokazi koji su podneseni prepisani su od riječi do riječi iz policijskog iskaza u jednom drugom predmetu[181]. Kazneni postupak protiv Adriena Beauduina, kojeg je u predmetu zastupao HCLU, okončan je 2020.

121. Predstavnici vlade javno su osudili takozvanu proimigracijsku mrežu Soros za

---

[174] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.
[175] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[176] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[177] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.
[178] Misija odbora PEGA u Budimpešti, 20. i 21. veljače 2023.
[179] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[180] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[181] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.

organiziranje „nasilnih prosvjeda u Budimpešti”[182]. Nakon toga na Beauduinu telefonu pronađeni su tragovi Pegasusa, ali nije bilo moguće potvrditi je li zaraza bila uspješna.

122. Budući da je Beauduin bio belgijski državljanin koji je u vrijeme tih incidenata živio u Mađarskoj, ključna je i važnost prekogranične dimenzije ovog predmeta. To je bitno jer utječe na suverena prava građana EU-a, kao što su sloboda kretanja i pravo na rad. Komisija ima uspostavljen postupak za podnošenje pritužbi koji svaka osoba može iskoristiti u slučaju povrede njezinih prava iz Povelje. Adrien Beauduin podnio je takvu pritužbu 24. siječnja 2022. Međutim, sedam mjeseci kasnije Komisija je u odgovoru od 17. kolovoza 2022. upućenom njegovu odvjetniku tvrdila da nije nadležna za intervenciju[183].

ILONA PATÓCS

123. Sumnja se da je odvjetnica Ilona Patócs nadzirana s pomoću softvera Pegasus u ljeto 2019. dok je zastupala klijenta optuženog za ubojstvo u jednom eksponiranom i dugotrajnom predmetu[184]. Zbog vrste mobilnog uređaja kojim se koristila nije bilo moguće potvrditi je hakiranje njezinog uređaja bilo uspješno ni kad se točno dogodilo. Njezin klijent István Hatvani već je bio odslužio sedam godina zbog ubojstva, a Patócs tvrdi da je osuđujuća presuda protiv njega bila „politički motivirana”[185]. Iako je neka druga osoba naknadno preuzela odgovornost za to ubojstvo, mađarski Žalbeni sud vratio je Hatvanija u zatvor da odsluži prvobitnu kaznu do kraja. Telefonski brojevi mnogih drugih odvjetnika navedeni su kao moguće mete Pegasusa, uključujući predsjednika Mađarske odvjetničke komore Jánosa Bánátija[186]. Iz toga je posebno razvidno da Vlada očito ne poštuje povjerljivi odnos između odvjetnika i njihovih klijenata.

GYÖRGY GÉMESI

124. György Gémesi, gradonačelnik Gödöllőa, također je bio meta špijunskog softvera Pegasus krajem 2018., upravo dok je bio pod velikim pritiskom vlade te su nepoznate osobe provalile u njegov dom i domove njegove djece. Istodobno s gradonačelnikom oporbe, vladin poznanik Gémesija određen je krajem 2018. kao meta špijunskog softvera. Osim toga, na popisu su se nalazila i dva telefonska broja povezana s kolegama iz njegove stranke i Gémesijevim bivšim zamjenikom gradonačelnika.

BRIGITTA CSIKÁSZ

125. Za vrijeme nadzora Brigitte Csikász, jedne od najiskusnijih mađarskih kriminalističkih novinarki, ona je među ostalim istraživala zlouporabu sredstava Europske unije. Csikászine istrage pokazale su da, unatoč upozorenju Europskog ureda za borbu protiv

[182] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[183] https://tasz.hu/a/files/220816-Complaint-unlawful-surveillance.pdf.
[184] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31. ožujka 2022.
[185] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31. ožujka 2022.
[186] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31. ožujka 2022.

prijevara (OLAF), mađarske vlasti nisu pokazale volju ni sposobnost kaznenog progona sumnjivog trošenja novca EU-a, što je još jednom dokazalo da, iako je kazneni progon *de jure* neovisan i na visokoj hijerarhijskoj razini, glavni je javni tužitelj *de facto* usko povezan s vladajućom strankom i predsjednikom vlade.

126. Mete Pegasusa bili su i predsjednik Mađarske odvjetničke komore, János Bánáti, odvjetnik za kazneno pravo te nekoliko drugih odvjetnika.

DRUGE METE

127. Osobe iz kruga vladajuće stranke također su se našle na meti špijunskog softvera. Neovisna mađarska medijska kuća Direkt36 objavila je u prosincu 2021. da su voditelj službe za zaštitu i osobni tjelohranitelj Jánosa Ádera, predsjednika i Orbánovog bliskog saveznika, hakirani špijunskim softverom Pegasus. Szabolcs Panyi, novinar portala Direkt36, koji je i sam bio žrtva špijunskog softvera, izvijestio je da je takvo špijuniranje uglavnom posljedica sve veće paranoje mađarskog predsjednika Vlade. Cecília Szilas, bivša veleposlanica Mađarske u Kini, bila je meta Pegasusa netom prije nego što je postala viša savjetnica Viktora Orbána. Meta špijunskog softvera Pegasus bio je i Attila Aszódi, državni tajnik Orbánove vlade, odgovoran za izgradnju i razvoj nuklearne elektrane Paks II za čiju granju je zadužen Roszatom. Postao je meta 2018., dok je još bio u vladi, ali je bio u sukobu sa svojim nadređenim, ministrom Jánosom Sülijem.

128. Nadalje, i sin i odvjetnik jednog od Orbánovih najstarijih prijatelja, Lajosa Simicske, hakirani su Pegasusom[187]. Simicska je od Orbánovog bliskog prijatelja postao njegov protivnik. Bio je u postupku prodaje svojeg konzorcija medija koji je poticao velik dio zavade nakon Orbánove pobjede na izborima 2018. kada je došlo do tog relacijskog ciljanja[188]. Sam Simicska nije bio meta iz jednostavnog razloga što se ne koristi pametnim telefonom, zbog čega zaraza špijunskim softverom kao što je Pegasus nije moguća[189]. Ajtony Csaba Nagy, Simicskin odvjetnik, posumnjao je na zarazu kada je tijekom poziva čuo reprodukciju telefonskog razgovora sa Simicskom. Kasnije su te sumnje naizgled potvrđene kada su informacije o tim pozivima objavljene samo u mađarskim medijima[190]. S obzirom na to da je većina medijskih kuća u Mađarskoj u državnom vlasništvu, vjerojatno je da je sama vlada dostavila informacije izravno medijima.

PODUZEĆA KOJA PROIZVODE ŠPIJUNSKI SOFTVER

[187] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.
[188] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.
[189] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.
[190] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. srpnja 2021.

129. Osim što je kupila špijunski softver Pegasus i upotrebljavala ga protiv svojih građana, mađarska vlada dopustila je i drugim poduzećima na obavještajnom tržištu da posluju na teritoriju Mađarske, kao što su Black Cube i Cytrox. Black Cube privatna je izraelska obavještajna agencija koju čine bivši djelatnici Mossada, izraelske vojske i izraelskih obavještajnih službi[191]. Na svojem mrežnom mjestu opisana je kao „kreativna obavještajna služba" koja pronalazi „prilagođena rješenja za složene poslovne i parnične izazove"[192]. Black Cube bio je upleten u brojne javne kontroverze povezane s hakiranjem, među ostalim u SAD-u i Rumunjskoj[193]. Otkrivena je i veza između Grupe NSO te špijunskog softvera Pegasus. Nakon snažnog pritiska javnosti do kojeg je došlo jer je NSO angažirao Black Cube za nadzor svojih protivnika, bivši glavni izvršni direktor NSO-a Shalev Hulio priznao je da je angažirao Black Cube u najmanje jednoj situaciji na Cipru.

130. Black Cube uključio se u slučaj Mađarske tijekom izbora 2018. kada je obilazio razne nevladine organizacije i osobe koje su bile povezane s Georgeom Sorosom te o tome izvještavao Orbána kako bi te aktivnosti iskoristili u kampanji sramoćenja[194]. Među metama je bila odvjetnica i članica vodeće nevladine organizacije za ljudska prava Mađarskog helsinškog odbora, Marta Pardavi[195]. Informacije dobivene nadzorom tih pojedinaca i nevladinih organizacija nisu bile objavljene samo u medijima pod kontrolom mađarske države, već i u Jerusalem Postu[196].

131. Dodatna veza s Mađarskom je društvo Cytrox Holdings Zrt., sa sjedištem registriranim na adresi u Budimpešti. Društvo Cytrox, tvorac špijunskog softvera Predator, izvorno je osnovano u Sjevernoj Makedoniji, prije nego što ga je kupio WiSpear, koji je sada dio grupe Intellexa Alliance kojim upravlja Tal Dilian.

ZAKLJUČNE NAPOMENE

132. Čini se da je uporaba Pegasusa u Mađarskoj dio vladine proračunane i strateške kampanje za narušavanje slobode medija i slobode izražavanja[197]. Vlada se koristila špijunskim softverom kako bi uvela režim uznemiravanja, ucjene, prijetnji i pritiska na neovisne novinare, medije, političke protivnike i organizacije civilnog društva s lakoćom i bez straha od pravnih posljedica. Vladina kontrola nad gotovo svim neinternetskim i internetskim elektroničkim mađarskim medijskim kućama omogućuje joj da i dalje prezentira svoju verziju istine i da u velikoj mjeri spriječi da javni nadzor koji provode neovisni mediji dopre do mađarskih građana.

133. Zakon kojim se dopušta uporaba presretanja u većoj je mjeri instrument za kontrolu i

[191] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7. listopada 2019.
[192] https://www.blackcube.com/.
[193] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.
[194] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. srpnja 2018.
[195] Reuters, https://www.reuters.com/article/meta-facebook-cyber-idCNL1N2T12MC, 16. prosinca 2021.
[196] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. srpnja 2018.
[197] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.

iskazivanje moći vlade nego što je instrument za zaštitu prava i privatnosti građana te je jedan od najslabijih u Europi[198] [199]. Mađarskim se sustavom otvoreno krše europski zahtjevi i standardi u pogledu nadzora građana koji su utvrđeni u Europskoj konvenciji o ljudskim pravima i presudama Europskog suda za ljudska prava[200] unatoč tvrdnjama vlade da je u svim slučajevima postupala zakonito i da u potpunosti poštuje zakon[201] [202]. Iako se vlada stalno poziva na „nacionalnu sigurnost"[203], njezine tvrdnje da su mete prijetnja nacionalnoj sigurnosti nisu vjerodostojne.

I.C Grčka

134. Odbor je u studenome 2022. posjetio Grčku u okviru zajedničke misije u Grčkoj i na Cipru. Članovi su se sastali s državnim tajnikom Giorgosom Gerapetritisom i raspravljali o istaknutim slučajevima nadzora i širem kontekstu medijskog pluralizma i vladavine prava u Grčkoj. Također su se susreli s istraživačkim novinarima, zastupnicima u grčkom parlamentu, predsjednikom Grčkog tijela za zaštitu podataka (HDPA), predstavnicima ADAE-a i nevladinih organizacija te braniteljima ljudskih prava.

135. Posjet je ukazao na činjenicu da se potrebno dodatno potruditi kako bi se osigurala transparentnost. Navodi o zlouporabi nadzora i uporabi špijunskog softvera moraju se temeljito istražiti i prema potrebi sankcionirati. Trebalo bi uspostaviti sve potrebne zaštitne mjere, a reformom bi se trebala poboljšati transparentnost i osigurati odgovarajući sudski nadzor nad primjenom nadzora. Posjetom je potvrđeno i da su potrebna jasna pravila za ograničavanje navođenja nacionalne sigurnosti kao temelja za nadzor, osiguravanje odgovarajućeg sudskog nadzora i jamčenje zdravog i pluralističkog medijskog okruženja.

136. Tijekom 2022. Grčku je potresao niz izvješća o uporabi špijunskog softvera, koji je prema grčkom pravu nezakonit. Nikos Androulakis, zastupnik u Europskom parlamentu i vođa grčke oporbene stranke PASOK, podnio je 26. srpnja 2022. tužbu Uredu javnog tužitelja pri Vrhovnom sudu zbog pokušaja da se njegov mobilni telefon zarazi špijunskim softverom Predator[204]. Taj pokušaj zaraze špijunskim softverom otkriven je dok je informatička služba Europskog parlamenta provjeravala telefon g. Androulakisa[205]. Prema forenzičkoj analizi informatičke službe, pokušaji hakiranja dogodili su se za vrijeme kandidature g. Androulakisa za vođu oporbene stranke. To je otkriće u središte pozornosti dovelo pritužbe koje je prije toga u travnju i svibnju 2022. podnio financijski novinar Thanasis Koukakis, žaleći se da je njegov telefon zaražen

[198] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. srpnja 2021.
[199] DW, 'Pegasus scandal: In Hungary, journalists sue state over spyware", 29. siječnja 2022.
[200] Među ostalim vidjeti Roman Zakharov protiv Rusije [GC], br. 47143/06, ESLJP 2015 39; Klass i ostali protiv Njemačke, 6. rujna 1978., § 50, serija A, br. 28. 40; Prado Bugallo protiv Španjolske, br. 58496/00, § 30, 18. veljače 2003.; Liberty i ostali protiv Ujedinjene Kraljevine, br. 58243/00, § 62, 1. srpnja 2008.
[201] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4. studenoga 2021.
[202] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1. veljače 2022.
[203] Euractiv, Hungary employed Pegasus spyware in hundreds of cases, says government agency, 1. veljače 2022.
[204] Euractiv, EU Commission alarmed by new spyware case against Greek socialist leader.
[205] Tagesspiegel, Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.

Predatorom. Tu zarazu potvrdio je CitizenLab. U rujnu je bivši ministar infrastrukture i zakonodavac iz stranke Syriza, Christos Spirtzis[206], tvrdio da je meta špijunskog softvera Predator. Iako njegov mobilni telefon nije službeno provjeren, g. Spirtzis podijelio je poveznice koje je primio s dva tehničara koji su usmeno potvrdili da je bio meta špijunskog softvera[207]. Nadalje, kasnije tog mjeseca otkriveno je da je grčka Nacionalna obavještajna služba (EYP) navodno upotrijebila špijunski softver za nadzor dvoje vlastitih zaposlenika[208]. Grčki mediji objavili su 5. i 6. studenoga popis na kojem su 33 mete softvera Predator, sve odreda istaknute osobe[209]. Popis, koji ni vlada ni osobe na koje se nadzor odnosi ne potvrđuju niti osporavaju, uključuje imena osoba koje rade u politici i medijima ili je riječ o poduzetnicima u Grčkoj. Učinak navodnog nadzora osoba koje se nalaze na popisu mogao bi biti opsežniji jer bi svi njihovi kontakti i veze mogli neizravno biti „uhvaćeni" u špijunskoj operaciji, uključujući njihove kontakte u tijelima EU-a. Velika raširenost špijunskog softvera navodno je bila razvidna već iz izvješća poduzeća Meta iz 2021., u čijem se prilogu spominje 310 poveznica na lažne mrežne stranice povezane s proizvođačem špijunskog softvera Cytrox, od čega su 42 osnovane s ciljem dovođenja meta u zabludu samo u Grčkoj[210] [211]. Krajem studenoga 2022. grčki dnevnik *Documento* objavio je popis na kojem je 498 URL-ova koji su upotrijebljeni za špijuniranje softverom Predator. Neki od URL-ova bili su istovjetni onima objavljenima u izvješću poduzeća Meta iz 2021[212]. Predsjednik HDPA-e potvrdio je 28. veljače 2023. da je 300 tekstualnih poruka povezanih sa špijunskim softverom Predator poslano na približno 100 uređaja. Predsjednik ADAE-a dodatno je naveo da je ADAE postupio po nekoliko pritužbi i utvrdio dva slučaja uporabe Predatora i jednog bankovnog računa osobe koja stoji iza lažnih tekstualnih poruka. U tijeku je istraga ADAE-a novih pritužbi[213].

137. U kolovozu 2022. grčka vlada priznala je da je EYP doista pratio g. Androulakisa i g. Koukakisa, ali je osporila da je ikada koristila ili kupila špijunski softver Predator. Osim toga, tijekom tog razdoblja otkriveni su i drugi slučajevi nadzora koji provodi EYP, kao što je slučaj novinara Stavrosa Malichoudisa[214]. Do danas nisu objavljeni službeni razlozi za nadzor.

138. Predsjednik vlade Mitsotakis objavio je 8. kolovoza 2022. videoporuku u kojoj je nejasno naveo da je nadzor g. Androulakisa bio „zakonit", ali „politički neprihvatljiv". Nije spomenuo nadzor g. Koukakisa ni druge navodne slučajeve. Također je izjavio da

---

[206] *Reuters*, One more Greek lawmaker files complaint over attempted phone hacking.
[207] https://insidestory.gr/article/predator-perissoteroi-apo-20-oi-stohoi-toy-stin-ellada-symfona-me-tin-arhi-prostasias.
[208] Efsyn, Targeting the disliked.
[209] Documento, Apocalypse: They Watched – This Sunday in Document.
[210] Meta, Threat Report on the Surveillance-for-Hire Industry („Izvješće o prijetnji u industriji nadzora za unajmljivanje").
[211] Inside Story, „Who was tracking the mobile phone of journalist Thanasis Koukakis?".
[212] Documento, 27. studenoga 2022.
[213] Razmjena mišljenja odbora PEGA s Konstantinosom Menoudakosom i Christosom Rammosom, 28. veljače 2023.
[214] Solomon, „Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'" (Novinar Solomona Stavros Malichudis pod nadzorom „zbog nacionalne sigurnosti"); Ekathimerini, slučaj prisluškivanja: Telefonski podaci koji su potaknuli razvoj događaja; EPRS (Služba Europskog parlamenta za istraživanja). Grčki Predatorgate. Najnovije poglavlje u europskom skandalu sa špijunskim softverom?

nije imao saznanja o nadzoru, no da je bio upoznat s tim, to ne bi dopustio[215]. Prema službenoj izjavi glasnogovornika vlade Yiannisa Oikonomoua, čim je predsjednik vlade saznao za „zakonito presretanje" g. Androulakisa, državni tajnik Giorgos Gerapetritis nastojao je u potpunosti privatno obavijestiti g. Androulakisa o razlozima njegova nadzora[216]. G. Androulakis odbio je ponudu o obavješćivanju i naveo da bi takav privatan sastanak biti nezakonit te da je jedini zakoniti način da se to obavi putem grčkog parlamenta. Kasnije, dok je svjedočio pred parlamentom, ministar Gerapetritis izjavio je da nikada nije bio upoznat s razlozima te je zatražio da se sve relevantne informacije drže u tajnosti. EYP je pod izravnom kontrolom premijera Kyriakosa Mitsotakisa nakon zakonodavne izmjene koja je donesena ubrzo nakon što je njegova stranka Néa Dimokratía stupila na vlast 2019[217].

139. Nakon tih otkrića Grigoris Dimitriadis, glavni tajnik vlade odgovoran za suradnju između grčke vlade i EYP-a, i direktor EYP-a Panagiotis Kontoleon podnijeli su ostavku[218].

KUPNJA

140. Krajem 2019. glavni tajnik Dimitriadis bio je u kontaktu s Grupom NSO radi kupnje špijunskog softvera Pegasus. U siječnju 2020. službeni prijedlog koji je podnijela Grupa NSO odnosio se na sporazum između vlada u iznosu od 50 milijuna EUR. Nakon potpisivanja sporazuma na pojedincu je bilo da se povuče, a na EYP-u da preuzme. Predviđeno je da EYP surađuje s Mossadom na instalaciji sustava. Dogovor je naposljetku opozvan[219].

141. EYP i vlada kategorički poriču da su grčke vlasti kupile ili koristile softver Predator[220].142. U nedostatku bilo kakvih dokaza o identitetu kupca i korisnika Predatora u slučajevima u Grčkoj nije moguće sa sigurnošću utvrditi na koji su način Vlada ili neki drugi akter kupili taj softver. Ako za pokušaje hakiranja i hakiranje telefona koji su pripadali g. Koukakisu i g. Androulakisu nije odgovorna grčka vlada, nameće se zaključak da je odgovoran neki nedržavni akter. To bi bilo kazneno djelo prema grčkom pravu koje bi se moralo istražiti. Hipoteza da iza napada softverom Predator stoje privatni akteri osim toga slabo je vjerojatna, jer se njome ne objašnjava izbor meta. Međutim, u načelu nije nemoguće nabaviti ili upotrebljavati špijunski softver i ako ga nisu izravno kupila Vladina tijela. Špijunski softver moguće je kupiti putem opunomoćenika, brokerskih društava ili posrednika, kao što smo vidjeli u drugim slučajevima, a moguće je i s dobavljačima špijunskog softvera dogovoriti pružanje određenih s njime povezanih usluga. Nema nikakve sumnje da su postojale bliske veze i međuovisnosti između određenih osoba i događaja povezanih s Vladom, EYP-om i pružateljima špijunskog softvera, posebno Krikelom, koji je povlašteni dobavljač komunikacijske opreme i opreme za nadzor, među ostalim za policiju i EYP. Krikel je

[215] Reuters, „Greek PM says he was unaware of phone tapping of opposition party leader" (Grčki premijer tvrdi da nije znao za prisluškivanje telefona vođe oporbene stranke).
[216] 1b LIFO, Androulakis je nakon nadzora odbio primiti informacije u privatnosti https://www.lifo.gr/now/politics/o-androylakis-arnithike-idiotiki-enimerosi-apo-ton-gerapetriti-kai-zita-na-toy.
[217] Euractiv, „Another Greek opposition lawmaker victim of Predator".
[218] POLITICO, „PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal".
[219] https://insidestory.gr/article/greek-state-and-spyware-vendor-intellexa-they-are-acquainted-after-all.
[220] EPRS (Služba Europskog parlamenta za istraživanja). Grčki Predatorgate. Najnovije poglavlje u europskom skandalu sa špijunskim softverom?

blisko povezan s osobama iz najužeg kruga predsjednika Vlade Mitsotakisa. Sve je više dokaza o opsežnim odnosima između Intellexe, poduzeća koje je vlasnik špijunskog softvera Predator, i Grčke. Grčko tijelo za zaštitu podataka kaznilo je 16. siječnja 2023. Intellexu novčanom kaznom u iznosu od 50 000 EUR zbog odbijanja suradnje, kao i dostave informacija o svojim klijentima u okviru istrage pokrenute u srpnju 2020. nakon pritužbe g. Androulakisa. Ispitni je postupak i dalje u tijeku[221].

143. Jedna je od mogućnosti da je Predator kupljen preko Ketyaka, Centra za tehnološku potporu, razvoj i inovacije, koji je osnovao bivši glavni direktor EYP-a Kontoleon. Djeluje neovisno o EYP-u[222] i sudjeluje u projektima koji se odnose na istraživanje, inovacije i tehnološki razvoj[223].

METE

GRIGORIS DIMITRIADIS

144. Dimitriadis je nećak predsjednika Vlade Mitsotakisa, koji je do kolovoza 2022. bio zaposlen kao glavni tajnik u njegovu uredu. U toj ulozi bio je zadužen za kontakte između Vlade i EYP-a. Bio je prisiljen podnijeti ostavku 5. kolovoza 2022. nakon što je otkrio da je EYP prisluškivao telefon g. Androulakisa. U početku se njegova ostavka povezivala s toksičnim političkim okruženjem, no kasnije mu je predsjednik vlade pripisao političku odgovornost za prisluškivanje g. Androulakisa i drugih političara[224].

145. Bivši voditelj EYP-a Panagiotis Kontoleon priznao je Grčkom parlamentarnom istražnom odboru svoj „društveni odnos” s g. Dimitriadisom. G. Kontoleona imenovala je vlada Mitsotakisa, no neke su se pravne odredbe morale prilagoditi kako bi se omogućilo njegovo imenovanje[225].

146. G. Dimitriadis također je na nekoliko načina blisko povezan s Felixom Bitziosom i Giannisom Lavranosom. Tri se muškarca osobno poznaju. G. Dimitriadis i g. Lavranos vjenčani su kumovi („Koumbaroi”),[226] dok je g. Dimitriadis kum drugom djetetu g. Lavranosa[227]. G. Dimitriadis također je bio neizravno povezan s g. Bitziosom putem poslovnih transakcija s bratom g. Bitziosa[228].

147. To ga stavlja u središte mreže koja ga poslovno i osobno povezuje s ključnim osobama u Intellexi, Krikelu i EYP-u.

148. G. Dimitriadis navodno poznaje i Andreasa Loverdosa, kandidata za vodstvo saveza stranki PASOK-KINAL 2021.

---

[221] https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-stin-intellexa-ae-gia-mi-synergasia-me-tin-arhi.
[222] https://www.tovima.gr/print/politics/to-trigono-lfpou-egkatestise-lfto-predator-crstin-ypiresia-crpliroforion-crkai-i-lista-crton-xeiriston-tou/.
[223] https://www.nis.gr/en/ketyak.
[224] https://www.iefimerida.gr/politiki/paraitisi-dimitriadi-klima-toxikotitas-ohi-predator?amp, https://primeminister.gr/2022/08/08/29961.
[225] Ieidiseis, nalazi stranki SYRIZA – PASOK o prisluškivanju: I skandal i zataškavanje.
[226] TVXS, Giannis Lavranos: Koumbarias s Tsouvalom i Dimitriadisom.
[227] Ieidiseis, nalazi stranki SYRIZA – PASOK o prisluškivanju: I skandal i zataškavanje.
[228] Reporters United, The Great Nephew and Big Brother.

FELIX BITZIOS

149. Poslovni čovjek Felix Bitzios bio je umješan u ogromni skandal koji je izbio zbog kršenja kontrolâ kapitala u banci Bank of Piraeus. Njegova je imovina zamrznuta do okončanja istrage[229]. G. Bitzios okoristio se zakonodavnom izmjenom koju je predsjednik vlade Mitsotakis donio ubrzo nakon što je došao na vlast 2019. Spornom je izmjenom propisana vremenska granica za zamrzavanje imovine, čime je omogućeno odmrzavanje zamrznute imovine nakon najviše osamnaest mjeseci[230]. Zahvaljujući toj izmjeni koju je donijela Mitsotakisova vlada, imovina g. Bitziosa mogla je biti odmrznuta.

150. M. Bitzios povezan je s Ciprom preko svojeg poduzeća Santinomo, registriranog na Cipru, i svojih veza s Tal Dilianom. Čini se da je g. Bitzios imao ključnu ulogu u prijenosu Intellexe u Grčku[231].

151. G. Bitzios je putem svojeg poduzeća Santinomo bio vlasnik 35 % dionica poduzeća Intellexa. Međutim, 4. kolovoza 2022. prenio je sve svoje dionice na Thalestris, matično poduzeće Intellexe[232]. Datum registracije prijenosa nekoliko je dana nakon što je otkriveno da je Androulakis hakiran. Međutim, sam prijenos navodno je izvršen 28. prosinca 2020., više od 19 mjeseci ranije. G. Bitzios na taj se način retroaktivno distancirao od vlasništva nad trećinom Intellexe. Bez obzira na to, g. Bitzios je s Intellexom bio povezan od ožujka 2020. do lipnja 2021. jer je u tom poduzeću bio zaposlen kao zamjenik upravitelja[233].

GIANNIS LAVRANOS

152. Giannis Lavranos optužen je za utaju poreza, a novinar Koukakis izvještavao je o njegovu predmetu.

INTELLEXA

153. Špijunski softver Predator prodaje se putem poduzeća Intellexa, konzorcija dobavljača špijunskog softvera koji je među ostalim prisutan na Cipru te u Grčkoj, Irskoj i Francuskoj. Tal Dilian, bivši pripadnik izraelskih obrambenih snaga, osnovao je taj konzorcij na Cipru. Njegova druga bivša supruga, poljska državljanka Sara Hamou, središnja je osoba u toj zamršenoj mreži poduzeća. Tal Dilian također je stekao malteško državljanstvo. Grčka vlada izjavila je da su Intellexi odobrene dvije izvozne dozvole, od kojih je jednom ovlašten izvoz u Madagaskar. Osim toga, grčka vlada izdala je dozvolu za izvoz Predatora u Sudan. Nije potvrđeno je li dozvola izdana za Intellexu ili neki drugi subjekt. Intellexa je navodno izvozila svoje proizvode i u Bangladeš.

154. U istražnom izvješću organizacije Lighthouse Reports od 30. studenoga 2022., u suradnji s izraelskim novinama *Haaretz* i grčkom novinskom kućom Inside Story, otkriveno je da su operacije Tala Diliana u vezi s Predatorom u Grčkoj navodno

[229] Lexocology, Cyprus court offers directions to bank on ambit of freezing injunction.
[230] Financial Times, Greek law change viewed as backtracking on money laundering.
[231] Inside Story, Predatorgate: The second shareholder of Intellexa SA.
[232] Inside Story, Predatorgate: The second shareholder of Intellexa SA.
[233] https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae.

povezane s letom zrakoplova tipa Cessna iz Grčke i Cipra u Sudan između travnja i kolovoza 2022. Taj je zrakoplov, navodno, paravojnim postrojbama Snaga za brzu potporu potajno i nezakonito dostavio naprednu nadzornu tehnologiju[234]. Evidencije letova povezale su privatni zrakoplov, koji je letio preko Cipra, s Talom Dilianom, bivšim visoko pozicioniranim operativcem izraelskih obrambenih snaga, koji je 2019. uspostavio konzorcij Intellexa sa sjedištima na Cipru i u Grčkoj. Komisija je 18. veljače 2023. potvrdila da je stupila u vezu s nacionalnim tijelima u Grčkoj i na Cipru radi pojašnjenja tog pitanja. Međutim, Komisija nije zaprimila odgovor[235]. Zamjenik grčkog ministra vanjskih poslova Miltiadis Varvitsiotis potvrdio je 19. travnja 2023. da je grčka vlada odobrila izvoznu dozvolu špijunskog softvera Predator u Sudan. Međutim, ministar poriče bilo kakvu ulogu Predatora u nedavnim sukobima između sudanskih oružanih snaga i paravojnih postrojbi Snaga za brzu potporu u Sudanu[236].

155. U prosincu 2022. grčka vlada objavila je da je 15. studenoga 2021. Intellexi dostavila dvije izvozne dozvole. Prema glasnogovorniku grčkog Ministarstva vanjskih poslova Alexandrosu Papaioannouu, jednom od tih dozvola odobrena je prodaja Predatora Madagaskaru[237]. Dozvola je izdana unatoč lošem stanju ljudskih prava u zemlji[238] i potencijalnom djelovanju u suprotnosti s Uredbom EU-a o dvojnoj namjeni[239]. Glavni tajnik za međunarodne gospodarske odnose Ioannis Smyrlis, koji je odobrio prodaju Predatora Madagaskaru, podnio je ostavku nakon tih otkrića[240] kako bi preuzeo dužnost zamjenika glavnog direktora vladajuće stranke Néa Dimokratía, koja je odgovorna za predstojeće izbore.

156. Osim izvoza špijunskog softvera, u jednom slučaju navodno je zabilježeno da je Grčka organizirala putovanja u svrhu osposobljavanja za uporabu špijunskog softvera. Bangladeš je lipnju 2021. kupio špijunsko vozilo od ciparskog poduzeća Passitora. Prema dokumentima Ministarstva unutarnjih poslova u Bangladešu, osoblje Nacionalnog centra za nadzor telekomunikacija (NTMC) prošlo je osposobljavanje za uporabu špijunskog vozila između 2021. i 2022. Vozilo je u konačnici stiglo u

[234] https://www.lighthousereports.nl/investigation/flight-of-the-predator/; https://www.haaretz.com/israel-news/security-aviation/2022-11-30/ty-article-magazine/.premium/jet-linked-to-israeli-spyware-tycoon-brings-spy-tech-from-eu-to-notorious-sudanese-militia/00000184-a9f4-dd96-ad8c-ebfcd8330000; https://insidestory.gr/article/flight-predator.
[235] https://www.europarl.europa.eu/doceo/document/E-9-2022-003990-ASW_EN.html; Sastanak odbora PEGA, 28. ožujka 2023.
[236] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/; https://www.aa.com.tr/en/africa/greek-government-admits-opposition-s-claim-of-spyware-export-to-sudan/2876824.
[237] The New York Times, 8. prosinca 2022., „How the Global Spyware Industry Spiraled Out of Control” (Kako je globalna industrija špijunskih softvera izmakla kontroli), https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.
[238] The New York Times, 8. prosinca 2022., „How the Global Spyware Industry Spiraled Out of Control” (Kako je globalna industrija špijunskih softvera izmakla kontroli), https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.
[239] Uredba (EU) 2021/821 Europskog parlamenta i Vijeća od 20. svibnja 2021. o uspostavi režima Unije za kontrolu izvoza, brokeringa, tehničke pomoći, provoza i prijenosa robe s dvojnom namjenom (SL L 206, 11.6.2021., str. 1.).
[240] The National Herald, „Top Greek Official Who Authorized Predator Spyware Sale Resigns” (Najviši grčki dužnosnik koji je odobrio prodaju špijunskog softvera Predatora podnio ostavku).

Bangladeš u lipnju 2022[241].

KRIKEL

157. Krikel je povlašteni dobavljač opreme za grčka tijela kaznenog progona i sigurnosna tijela. Usto je grčki zastupnik talijanskog poduzeća RCS Lab, koje se bavi prodajom softvera za nadzor. Osim toga, tvrdi se da je Giannis Lavranos vlasnik udjela od 50 % u Krikelu, preko drugog poduzeća pod nazivom Mexal[242]. Međutim, čini se da nije moguće sa sigurnošću utvrditi tko je krajnji stvarni vlasnik Krikela, unatoč brojnim ugovorima koje to poduzeće ima s državnim tijelima.

158. Poduzeće Ioniki Technologiki u vlasništvu Giannisa Lavranosa prodano je poduzeću Tetra Communications u Londonu 2014. Iste je godine Ioniki Technologiki bilo jedno od triju poduzeća koja su grčkom Ministarstvu zaštite građana donirale Tetra Communications Systems[243]. Kako je otkriveno WikiLeaksom, grčka je vlada 2014. izrazila interes i za RCS Galileo, talijansku marku špijunskog softvera poduzeća Hacking Team, ali taj softver nikad nije nabavljen[244]. Donaciju Tetre olakšalo je poduzeće sa sjedištem na Floridi, omogućivši zaobilaženje uobičajenih postupaka natječaja. Donacija grčkoj vladi prihvaćena je 2017. Krikel je 2018. potpisao ugovor o održavanju i tehničkoj podršci vrijedan10,8 milijuna EUR. Ugovor je u ime Krikela potpisao njegov upravitelj Stanislaw Pelczar, ali se čini da je u pregovorima za cijelog njihovog trajanja neslužbeno sudjelovao Lavranos[245]. Krikel je postao važan dobavljač grčkog Ministarstva zaštite građana. U razdoblju od 2018. to je poduzeće potpisalo sedam ugovora s grčkom vladom, od kojih je šest povjerljivo[246].

159. Osim toga, poduzeće Krikel postalo je lokalni zastupnik talijanskog poduzeća RCS Lab. U lipnju 2021. EYP je od poduzeća RCS Lab navodno kupio sustav za prisluškivanje[247] putem Krikela[248]. U to je vrijeme Dimitriadis bio nadležan za kontakte između Vlade i EYP-a. Neki izvori dokumentirali su da je materijal koji je sadržavao informacije o nadzoru Androulakisa i Koukakisa izgubljen tijekom instalacije tog novog sustava, navodno zbog tehničkog problema[249]. Drugi izvori, međutim, tvrdili su da je Kontoleon

[241] Haaretz, „Israeli Spy Tech Sold to Bangladesh, World's Third-largest Muslim Country, Despite Dismal Human Rights Record" (Izraelska špijunska tehnologija prodana Bangladešu, trećoj muslimanskoj zemlji po veličini u svijetu, unatoč poražavajućem stanju ljudskih prava).
[242] Tu je prisutno nekoliko zanimljivih veza. Lavranos je u travnju 2021. prodao svoj obiteljski dom u Ateni poduzeću Albitrum Properties po cijeni nižoj od tržišne vrijednosti. Tijekom te prodaje poduzeće Albitrum Properties zastupao je Theodoros Zervos, polubrat Felixa Bitziosa. Albitrum je ciparsko poduzeće među čijim je dioničarima Mexal Services Ltd., vlasnik stopostotnog udjela u poduzeću Eneross Holdings Ltd. Eneross Holdings osim toga je vlasnik Krikela. Registrirani ured Giannisa Lavranosa nalazi se na istoj adresi na kojoj su registrirani Eneross Holdings i Mexal Services na Cipru. Vidjeti: Inside Story, 'Predatorgate's invisible privates', i TVXS, 'G.„G. Lavranos iza KRIKELA – Pokušaj prijevare Parlamenta [Osjetljivi dokumenti]".'.
[243] Inside Story, „Nevidljivi privatnici skandala Predatorgate".
[244] Inside Story, „Višegodišnji interes grčkih vlasti za špijunski softver".
[245] Inside Story, „Nevidljivi privatnici skandala Predatorgate".
[246] Inside Story, „Nevidljivi privatnici skandala Predatorgate".
[247] Hellas Posts English, „The EYP supplier contaminates smartphones in Greece as well" (Dobavljač EYP-a kontaminira i pametne telefone u Grčkoj).
[248] TVXS, G.„G. Lavranos iza KRIKELA – Pokušaj prijevare Parlamenta [Osjetljivi dokumenti]".
[249] TVXS, G.„G. Lavranos iza KRIKELA – Pokušaj prijevare Parlamenta [Osjetljivi dokumenti]".

29. srpnja 2022. naredio uništenje tih datoteka[250].

160. Zanimljivo je da su zaposlenici Krikela primijećeni kako rade u Ketyaku, navodno pro bono. Ketyaku je navodno odobreno 40 milijuna EUR iz EU-ova Mehanizma za oporavak i otpornost putem povjerljivog natječajnog postupka temeljenog na tajnoj odluci predsjednika Vlade[251]. Nezakonita uporaba financijskih sredstava EU-a za financiranje nezakonitog špijunskog softvera predstavljala bi ozbiljno kršenje prava Unije i bila bi u nadležnosti brojnih europskih tijela, uključujući Ured europskog javnog tužitelja.

161. Zaposlenici Krikela navodno su posjetili i prostore EYP-a u Agia Paraskevi u prosincu 2021. i siječnju 2022. u svojstvu voditelja osposobljavanja. Te prostore kontrolira grčka vlada i ondje je navodno ugrađen špijunski softver Predator[252].

UMIJEŠANOST BITZIOSA AND LAVRANOSA

162. Bitzios i Lavranos obojica su aktivno sudjelovali u osnivanju Krikela 2017. Zajedno su organizirali imenovanje poljskog odvjetnika Stanislawa Pelczara za upravitelja Krikela u listopadu 2017[253]. Krikel je nakon toga angažirao Bitziosovo poduzeće Viniato Holdings Limited kao konzultanta u razdoblju od siječnja do kolovoza 2018. za naknadu od oko 550 000 EUR (iako je Krikel te godine ostvario promet od samo 840 000 EUR)[254].

163. Bitzios i Pelczar imaju i druge uzajamne poslovne veze. Iz Rajskih dokumenata proizlazi da dijele poduzeće registrirano na Malti pod nazivom Baywest Business[255]. Osim toga, Tal Dilian, osnivač Intellexe, ima malteško (zlatnu) putovnicu[256] i fiktivno poduzeće MNT Investments LTD u toj otočnoj državi[257].

164. Bitzios i Lavranos dvije su ključne osobe u opskrbi državnih tijela kao što su policija i EYP komunikacijskim materijalima i materijalima dobivenim nadzorom. Bitzios je imao središnju ulogu u poduzeću koje prodaje Predator. Obojica su bili bliski Dimitriadisu i obojica su profitirali od unosnih ugovora s Vladom. Također su se okoristili novom zakonodavnom izmjenom Vlade koja je omogućila odmrzavanje

---

[250] Euractiv, 'Greek MEP spyware scandal takes new turn' (Novi zaokret u skandalu sa špijunskim softverom grčkog zastupnika u EP-u).
[251] https://www.flash.gr/politiki/1988373/predator-apokalypseis-gia-to-ketyak-tis-eyp-me-xrimatodotisi-kai-apo-to-tameio-anakampsis.
[252] Inside Story, „Greek State and spyware vendor Intellexa:they are acquainted after all" (Grčka država ipak upoznata s dobavljačem špijunskog softvera Intellexa).
[253] TVXS, G. Lavranos behind KRIKEL – How attempts were made to deceive the Parliament [Revealing documents]'. (G. Lavranos iza KRIKELA – Kako su pokušali zavarati Parlament).
[254] Inside Story, From Koukakis to Androulakis: A new twist in the Predator spyware case'.(Od Koukakisa do Androulakisa: Novi zaplet u priči o špijunskom softveru)
[255] Međunarodni konzorcij istraživačkih novinara, baza podataka Offshore Leaks, Rajski dokumenti – Malteški registar trgovačkih društava.
[256] Vlada Malte, „Persons Naturalised Registered as Citizens of Malta" (Osobe koje su naturalizirane/registrirane kao državljani Malte), Gaz 21.12, https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf.
[257] https://mlt.databasesets.com/company-all/company/73006 https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/.

njihove zamrznute imovine. Imali su motiv za uporabu špijunskog softvera protiv Koukakisa. U toj zamršenoj mreži poslovnih interesa, osobnih odnosa i političkih veza prisutan je vrlo očit i velik rizik od sukoba interesa i korupcije. Osim toga, oni bi mogli pružiti ključne informacije o nabavi i uporabi Predatora u Grčkoj.

165. Međutim, unatoč očitoj važnosti svjedočenja Bitziosa i Lavranosa pred istražnim odborom grčkog parlamenta, većina članova odbora, koju čine članovi stranke Néa Dimokratía, odbila je zahtjeve oporbe da se te pojedince pozove na saslušanje.

EX ANTE NADZOR

166. U Grčkoj je zaraza uređaja špijunskim softverom kazneno djelo, što je utvrđeno u nekoliko članaka grčkog Kaznenog zakona, uključujući članak 292. o kaznenim djelima protiv sigurnosti telefonskih komunikacija, članak 292.B o onemogućavanju rada informacijskih sustava te članak 370. o povredama tajnosti pisama. Osim toga, proizvodnja, prodaja, uporaba, uvoz, posjedovanje i distribucija zloćudnog softvera (uključujući špijunski softver) te opskrba tim softverom također je kazneno djelo, što je utvrđeno u članku 292.C grčkog Kaznenog zakona[258]. Grčka vlada izmijenila je taj članak 9. prosinca 2022.

167. Broj odobrenih prisluškivanja znatno se povećao tijekom godina. Od 4871 u 2015. na 11 680 u 2019. i u konačnici na 15 475 u 2021.[259] Trenutačno se svaki dan mora obraditi oko 60 zahtjeva, a donedavno ih je morao obrađivati samo jedan javni tužitelj. Osim toga, u odredbama EYP-a kojima se zbog razloga povezanih s nacionalnom sigurnošću ukida povjerljivost komunikacija građana ne spominje se ime dotične osobe ni razlog za ukidanje povjerljivosti. Ograničene su na telefonski broj i pozivanje na nacionalnu sigurnost[260].

168. Sudsko odobrenje za nadzor privatnih komunikacija te njegovo produljenje i ukidanje mora odobriti nadležni javni tužitelj. Kako je propisano Zakonom br. 3649/2008, nadležni tužitelj za ukidanje tajnosti i povjerljivosti interni je tužitelj EYP-a. Zakonodavnom izmjenom iz 2018., tijekom drugog mandata predsjednika Vlade Alexisa Tsiprasa, broj javnih tužitelja potrebnih za odobrenje prisluškivanja smanjen je s dva na jedan. Tužitelj nadležan za navedene predmete je Vasiliki Vlachou[261]. Vlachou se nije sastao s misijom odbora PEGA u Grčkoj.

ZAKON O ZAKONODAVNOM SADRŽAJU

169. Nakon otkrića o nadzoru, predsjednik Vlade Mitsotakis predložio je izmjene EYP-ova okvira rada. Jedna od tih izmjena je uvođenje Zakona o zakonodavnom sadržaju, koji je Vlada uvela 9. kolovoza 2022. Članak 9. stavak 2. Zakona br. 3649/2008 ažuriran je na

---

[258] International Comparative Legal Guide, *Cybersecurity Laws and Regulation Greece 2022*.(Zakoni i propisi o kibersigurnosti u Grčkoj 2022.).
[259] Ekathimerini, „Wiretapping and ‚national security'" (Prisluškivanje i „nacionalna sigurnost").
[260] Reporters United, „Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis" (Neprijatelj države: Dokazujemo da je vlada Mitsotakisa pratila novinara Thanasisa Koukakisa).
[261] Reporters United, „Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis" (Neprijatelj države: Dokazujemo da je vlada Mitsotakisa pratila novinara Thanasisa Koukakisa).

način da se sada zahtijeva mišljenje Stalnog odbora za institucije i transparentnost o imenovanju direktora EYP-a[262]. Međutim, budući da vladajuća stranka trenutačno ima apsolutnu većinu u Posebnom stalnom odboru Parlamenta za institucije i transparentnost, taj je odbor podržao nominaciju g. Demirisa za novog direktora EYP-a, iako su se sve oporbene stranke protivile[263]. Usput, drugi zamjenik direktora EYP-a je Dionysis Melitsiotis[264], bivši član privatnog ureda predsjednika Vlade, a jedan od zamjenika direktora je i Anastasios Mitsialis, bivši dužnosnik stranke Néa Dimokratía[265].

170. Osim toga, zakonom je ponovno uvedeno odobrenje dvaju tužitelja za zahtjeve za nadzor[266]. Članak 5. Zakona br. 3649/2008, koji se odnosi na odredbu o EYP-ovu ukidanju povjerljivosti komunikacija, dopunjen je zahtjevom za odobrenje nadležnog tužitelja, nakon čega se zahtijeva odobrenje javnog tužitelja na Prizivnom sudu[267].

EX POST NADZOR

171. Od 2019. djelovanje EYP-a pod izravnom je kontrolom predsjednika Vlade Kyriakosa Mitsotakisa nakon izmjene zakona koja je izvršena nakon pobjede stranke Néa Dimokratía 2019.[268]

172. Parlamentarni nadzor provodi Stalni odbor za institucije i transparentnost. Taj odbor nadzire djelovanje EYP-a i ovlašten je prikupljati dokumente, ispitivati osobe i pozvati glavnog direktora na saslušanje[269]. Vladajuća stranka ima apsolutnu većinu u sadašnjem sastavu odbora.

173. Grčko tijelo za sigurnost i privatnost komunikacija (ADAE) osigurava zaštitu povjerljivosti pošte i svih drugih vrsta komunikacija[270]. Statut ADAE-a osigurava njegovu administrativnu neovisnost[271]. ADAE može provoditi istrage u prostorima, bazama podataka i arhivima EYP-a te istrage njegove tehničke opreme i dokumenata[272].

174. U Zakonu br. 2225/1994 utvrđuje se da se povjerljivost komunikacija može ukinuti isključivo u slučajevima nacionalne sigurnosti i istraga teških kaznenih djela. U članku 5. navedenog zakona utvrđuje se da nakon ukidanja povjerljivosti ADAE može o

---

262 EfSyn, „Što se (ne) mijenja Zakonom o zakonodavnom sadržaju za EYP?".
263 Ekathemirini,„Themistoklis Demiris:Njegovo imenovanje u upravu EYP-a odobreno većinom glasova".
264 Ekathimerini, „National security takes center stage" (Nacionalna sigurnost preuzima glavnu ulogu).
265 Greek City Times, 'Greek PM appoints new security and intelligence chiefs' (Grčki premijer imenuje nove voditelje sigurnosnih i obavještajnih službi).
266 At a Glance, „Greece's Predatorgate: The latest chapter in Europe's spyware scandal?" (Grčki Predatorgate: najnovije poglavlje u europskom skandalu sa špijunskim softverom?), Europski parlament, Glavna uprava za usluge parlamentarnih istraživanja, 8. rujna 2022.
267 EfSyn, „Što se (ne) mijenja Zakonom o zakonodavnom sadržaju za EYP?".
268 Euractiv, 'Another Greek opposition lawmaker victim of Predator'. (Još jedan grčki parlamentarni zastupnik oporbe žrtva Predatora).
269 Centar za europsko ustavno pravo, „National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies" (Nacionalna obavještajna tijela i nadzor u EU-u: zaštita temeljnih prava i pravna sredstva).
270 ADAE, *Presentation* (Predstavljanje).
271 ADAE*, Regulatory framework* (Regulatorni okvir).
272 Centar za europsko ustavno pravo, „National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies" (Nacionalna obavještajna tijela i nadzor u EU-u: zaštita temeljnih prava i pravna sredstva).

tome obavijestiti mete istraga, pod uvjetom da se time neće ugroziti svrha istrage[273]. Pravo pojedinca na pristup informacijama o tome je li taj pojedinac predmet nadzora uređuje se Zakonom br. 2472/1997[274]. Međutim, kad je ADAE u ožujku 2021. obavijestio EYP o Koukakisovu pravu da bude obaviješten, Vlada je odmah 31. ožujka 2021. podnijela Izmjenu br. 826/145 kojom je ADAE-u ukinuta mogućnost da obavijesti građane o ukidanju povjerljivosti komunikacija[275]. Time se pojedincu de facto ukida pravo na informacije. Postupak donošenja navedene izmjene bio je vrlo nepropisan. Dodana je zakonu koji s time nema nikakve veze (prijedlogu zakona o mjerama za sprečavanje širenja bolesti COVID-19), uz nepoštovanje rokova utvrđenih Ustavom[276] [277] [278]. Stoga nije proveden propisan postupak savjetovanja.

175. Zakonom o zakonodavnom sadržaju Mitsotakis je nastojao ojačati transparentnost i odgovornost. Međutim, zakonom se ne opoziva izmjena 826/145.

176. Grčka vlada donijela je 9. prosinca 2022. Zakon br. 5002/2022 u cilju ažuriranja i stvaranja učinkovitog pravnog okvira za zaštitu osobnih podataka, tajnost komunikacija i jačanje kibersigurnosti. Međutim, zakonom se uvodi nekoliko odredaba kojima se oslabljuju zaštitne mjere, nadzor i odgovornost. U skladu s člankom 4. stavkom 7.[279], svaki zahtjev pojedinaca za informacije o tome jesu li bili predmet nadzora iz razloga povezanih s nacionalnom sigurnošću ispitat će tročlani odbor sastavljen od direktora EYP-a, tužitelja EYP-a i predsjednika ADAE-a. To znači da većinu čine oni koji su naredili (direktor EYP-a) i odobrili (tužitelj) nadzor. Osim toga, time se praktički onemogućuje da pojedinci koji su pod nadzorom iz razloga povezanih s nacionalnom sigurnošću budu na odgovarajući način naknadno obaviješteni jer je zakonom propisano da relevantni zahtjev mogu podnijeti tek tri godine nakon završetka nadzora. To nije u skladu s relevantnom sudskom praksom Suda Europske unije i Europskom poveljom o ljudskim pravima[280] te se navedenim zakonom ne predviđaju institucionalni sustavi provjere i ravnoteže kako bi se osiguralo pravilno funkcioniranje državnih ovlasti. ADAE je izrazio svoje neslaganje s tročlanim tijelom. Zasad ne postoji operativni okvir

[273] Constitutionalism, „Proturječnost članka 87. Zakona br. 4790/2021 s jamstvima EKLJP-a za zaštitu povjerljivosti komunikacija”.
[274] Grčko tijelo za zaštitu podataka (DPA), Zakon br. 2472/1997 o zaštiti pojedinaca u vezi s obradom osobnih podataka.
[275] https://www.reportersunited.gr/8646/eyp-koukakis/.
[276] Grčki parlament, Ustav.
[277] Grčki parlament, Poslovnik Parlamenta.
[278] Govwatch, ‘Violation of the legislative process for amendments in law 4790/2021’. (Kršenje zakonodavnog postupka za izmjene u Zakonu br. 4790/2021).
[279] https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022.
[280] https://www.dsa.gr/%CE%B4%CE%B5%CE%BB%CF%84%CE%AF%CE%B1-%CF%84%CF%8D%CF%80%CE%BF%CF%85/%CE%B1%CF%80%CE%BF%CF%86%CE%AC%CF%83%CE%B5%CE%B9%CF%82-%CE%B4%CF%83/%CE%B1%CF%80%CF%8C%CF%86%CE%B1%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%BF%CE%B9%CE%BA%CE%B7%CF%84%CE%B9%CE%BA%CE%BF%CF%8D-%CF%83%CF%85%CE%BC%CE%B2%CE%BF%CF%85%CE%BB%CE%AF%CE%BF%CF%85-%CF%84%CE%BF%CF%85-%CE%B4%CF%83%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7-%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B5%CE%B9%CF%83%CE%B1%CE%B3%CE%B3%CE%B5%CE%BB.

za tripartitni odbor, što znači da on de facto ne funkcionira[281]. Osim toga, novim je zakonom pojedincima i privatnim poduzećima zabranjeno upotrebljavati špijunski softver, a javna tijela prvi put mogu zakonito kupovati špijunski softver, čime se Vladi odobrava uspostava postupka na temelju predsjedničke odluke. Ne postoji odredba o sudskom nadzoru nad uporabom špijunskog softvera ili o podugovaranju prisluškivanja privatnim subjektima.

177. Isporuka špijunskog softvera koju obavljaju privatni subjekti nezakonita je samo ako se takav softver nalazi na indikativnom popisu „zabranjenog špijunskog softvera" koji direktor EYP-a ažurira svakih šest mjeseci. Njime se EYP ovlašćuje za zakonitu nabavu špijunskog softvera jer će se ključna relevantna pitanja rješavati isključivo sekundarnim zakonodavstvom (tj. predsjedničkom odlukom). Stoga će se ažurirana verzija postojećeg špijunskog softvera smatrati zakonitom dok se ne uvrsti na navedeni popis. Definicija „nacionalne sigurnosti" u zakonu iznimno je široka i nejasna te je stoga u suprotnosti s člankom 19. stavkom 1. Ustava, koji zahtijeva usko tumačenje. ADAE je dodatno spriječen u izvršavanju svoje ustavom određene uloge u kontroli postupka deklasifikacije. Važnost uloge neovisnog tijela koje je bilo ključno za otkrivanje skandala s nadzorom umanjena je u novom zakonu, unatoč relevantnim ustavnim jamstvima.

178. Mogućnosti *ex post* nadzora oslabljene su zbog toga što je Grčkoj trebalo dugo vremena da u potpunosti provede Direktivu EU-a o zaštiti zviždača[282]. Komisija je 27. siječnja 2022. pokrenula postupak zbog povrede prava upućivanjem službene opomene Grčkoj. Komisija je 15. srpnja 2022.[283] poslala obrazloženo mišljenje s rokom od dva mjeseca za odgovor. Grčki parlament u konačnici je 11. studenoga 2022. glasovao o Zakonu br. 4990/2022 kojim se Direktiva EU-a o zaštiti zviždača prenosi u grčko zakonodavstvo.

JAVNI NADZOR

179. Grčka je na Svjetskom indeksu slobode medija za 2022. najniže pozicionirana od svih država članica EU-a, 108. od 180.[284] Novinar Giorgos Karaivaz ubijen je 2021. Njegovo ubojstvo još nije riješeno. Novinari se suočavaju sa zastrašivanjem i strateškim tužbama protiv javnog sudjelovanja (eng. SLAPP). Grigoris Dimitriadis[285] podnio je takve tužbe protiv medijskih kuća Reporters United i *Efimerida ton Syntakton* (EfSyn)[286] nakon što je bio prisiljen podnijeti ostavku. Ministar u Vladi Oikonomou pokušao je diskreditirati Nektariju Stamouli, novinarku portala *Politico*, implicirajući da su njezini članci o skandalu povezanom sa špijunskim softverom bili politički motivirani[287]. Naime, dvije mete nadzora, Koukakis i Malichoudis, kritički su izvještavale o slučajevima korupcije i prijevare te o zlostavljanju migranata. Athanasios Telloglou i Eliza Triantafillou

[281] Odbor PEGA, Razmjena gledišta s Konstantinosom Menoudakosom i Christosom Rammosom, 28. veljače 2023.
[282] https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768.
[283] https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_3768.
[284] https://rsf.org/en/index.
[285] Tagesspiegel.
[286] EUobserver, 'Greece accused of undermining rule of law in wiretap scandal'. (Grčka optužena za ugrožavanje vladavine prava u skandalu prisluškivanja).
[287] https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/.

izvještavali su o skandalu povezanom sa špijunskim softverom i navodno su stavljeni pod nadzor[288]. Osim toga, grčki tužitelj pri Vrhovnom sudu Isidoros Dogiakos diskreditirao je medijske kuće koje su kritizirale grčka pravosudna tijela jer nisu na odgovarajući način rješavala skandal prisluškivanja u Grčkoj. Čak je pokušao zastrašiti medije koji istražuju skandal zatraživši selektivne porezne revizije njihovih vlasnika[289].

PRAVNA ZAŠTITA

NACIONALNO TIJELO ZA TRANSPARENTNOST

180. Kako je utvrđeno člankom 82. Zakona br. 4622/2019, Nacionalno tijelo za transparentnost (EAD) odgovorno je za jačanje odgovornosti, transparentnosti i integriteta mjera koje poduzimaju Vladina tijela, državna tijela, upravna tijela i javne organizacije. Osim toga, EAD bi trebao sprječavati, otkrivati i rješavati slučajeve prijevare i korupcije koje provode javna i privatna tijela. U skladu s tim zakonom EAD je preuzeo sve odgovornosti, prava i obveze od sljedećih javnih tijela: Glavnog tajništva za borbu protiv korupcije, Tijela revizora i inspektora javne uprave, Ureda glavnog inspektora javne uprave, Tijela inspektora zdravstvene i socijalne skrbi, Tijela inspektora javnih radova i Tijela inspektora i revizora prometa[290]. Iako je neovisnost ADAE-a propisana Ustavom, EAD nije neovisno tijelo.

181. EAD je 22. srpnja 2022. pokrenuo istragu o navodnoj kupnji špijunskog softvera Predator od strane Ministarstva zaštite građana i EYP-a. Revizijom su obuhvaćeni grčka policija, EYP i poduzeća Intellexa i Krikel. EAD je svoje izvješće zaključio 10. srpnja 2022., ali ga je podnio EYP-u na prethodno odobrenje. Službeno izvješće poslano Koukakisu 22. srpnja sadržavalo je samo dijelove cjelokupne revizije koju je proveo EAD. Iz revizije je pod izlikom zaštite osobnih podataka izostavljeno nekoliko imena, uključujući imena revizora iz EAD-a, ime tužitelja iz EYP-a koji je pregledao EAD-ovo prvobitno izvješće te imena odvjetnika i računovođa uključenih pravnih osoba[291].

182. Naposljetku, u izvješću EAD-a zaključeno je da EYP i Ministarstvo zaštite građana nisu zaključili ugovore s Intellexom ni drugim s njome povezanim nacionalnim poduzećima. Također nisu kupili ni upotrebljavali špijunski softver Predator[292]. Međutim, istragom EAD-a nisu bili obuhvaćeni bankovni računi poduzeća Intellexa i Krikel, kao ni s njima povezanih offshore poduzeća. Osim toga, EAD je posjetio urede poduzeća Intellexa i Krikel tek dva mjeseca nakon prve objave o uporabi Predatora u Grčkoj, kad su njihovi zaposlenici radili od kuće zbog pandemije bolesti COVID-19. Nadalje, EAD nije održao

[288] Heinrich-Böll-Stiftung, „U uvjetima apsolutne usamljenosti".

[289] Novinarski sindikat ESIEA osuđuje prijetnje tužitelja Vrhovnog suda, https://www.esiea.gr/oi-dimosiografikes-enoseis-gia-tis-di/.

[290] https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019.

[291] Inside Story, From Koukakis to Androulakis: A new twist in the Predator Spyware case'.(Od Koukakisa do Androulakisa: Novi zaplet u priči o špijunskom softveru).

[292] Inside Story, From Koukakis to Androulakis: A new twist in the Predator Spyware case'.(Od Koukakisa do Androulakisa: Novi zaplet u priči o špijunskom softveru).

sastanke sa zakonskim zastupnicima dotičnih poduzeća[293].

183. Neovisnost vodstva EAD-a je upitna. Sadašnji direktor, bivši Mitsotakisov zaposlenik, obnaša dužnost na privremenoj osnovi od ljeta 2022. Nije jasno zašto postupak zapošljavanja nije pokrenut. Direktor EAD-a nije se sastao s predstavnicima odbora PEGA tijekom misije u studenome 2022. Direktor se 7. ožujka 2023. sastao s izaslanstvom odbora LIBE, gdje su postavljena pitanja o špijunskom softveru u Grčkoj.

GRČKO TIJELO ZA SIGURNOST I PRIVATNOST KOMUNIKACIJA (ADAE)

184. Nikos Androulakis potvrdio je u srpnju 2022. da je podnio pritužbu Uredu javnog tužitelja pri Vrhovnom sudu, tvrdeći da se navodno našao na meti špijunskog softvera Predator 21. rujna 2021. ADAE je nakon Androulakisove pritužbe u kolovozu 2022. pokrenuo istragu, koja je započela pribavljanjem informacija od Androulakisova telekomunikacijskog operatera.

185. Špijunski softver Predator ostavlja malo tragova zaraze kod pružatelja telekomunikacijskih usluga. Međutim, ADAE je utvrdio da je EYP nadzirao Androulakisov mobilni telefon[294] te da je interni tužitelj EYP-aVasiliki Vlachou odobrio nadzor i ukidanje tajnosti u rujnu 2021., što se podudara s navodnim napadom Predatorom.

186. Na temelju nalaza istrage ADAE-a, Grigoris Dimitriadis i Panagiotis Kontoleon dali su ostavke na svoje položaje u Vladi[295]. Kontoleon je izjavio da je nadzor Androulakisa pokrenut na zahtjev stranih tijela, konkretno obavještajnih agencija Armenije i Ukrajine, s obzirom na sudjelovanje Androulakisa u Odboru Europskog parlamenta za međunarodnu trgovinu, koji se bavi trgovinskim odnosima između EU-a i Kine[296]. I Ukrajina i Armenija odbacile su te tvrdnje[297].

187. Tijelo je 15. prosinca 2022. odgovorilo na zahtjeve novinara Tasosa Tellogloua i zastupnika u Europskom parlamentu Giorgosa Kyrtsosa za informacije o tome jesu li bili na meti EYP-a. Revizijom koju je ADAE proveo nad poduzećem za telekomunikacije Cosmote utvrđeno je da su i Telloglou i Kyrtsos doista stavljeni pod nadzor[298]. Cosmote je obavijestio Vrhovni sud i doveo u pitanje zakonitost istrage ADAE-a[299]. ADAE je uspostavio poseban tim za nadzor pružatelja telekomunikacijskih

[293] Inside Story, „From Koukakis to Androulakis: A new twist in the Predator Spyware case'.(Od Koukakisa do Androulakisa: Novi zaplet u priči o špijunskom softveru).
[294] https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf.
[295] Politico, „PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal" (Predsjednik Vlade Mitsotakis pod pritiskom nakon ostavki dvaju vodećih grčkih dužnosnika u špijunskom skandalu).
[296] https://www.kathimerini.gr/politics/561988786/ypothesi-parakoloythiseon-ta-dedomena-poy-pyrodotisan-tis-exelixeis/.
[297] At a Glance, „Greece's Predatorgate: The latest chapter in Europe's spyware scandal?" (Grčki Predatorgate: najnovije poglavlje u europskom skandalu sa špijunskim softverom?), Europski parlament, Glavna uprava za usluge parlamentarnih istraživanja, 8. rujna 2022.
[298] Euractiv, „Exclusive: Another MEP and journalist the latest victims of 'Greek Watergate'" (Ekskluzivno: Još jedan zastupnik u EP-u i novinar najnovije žrtve „grčkog Watergatea").
[299] Međunarodni institut za medije, „Greece: MFRR alarmed by latest revelations of spying on journalists" (Grčka: MFRR uznemiren najnovijim otkrićima špijuniranja novinara).

usluga, posebno tražeći daljnje zahtjeve EYP-a za ukidanje povjerljivosti[300].

188. Vlada je pokušala zamijeniti članove upravnog odbora ADAE-a. Osim toga, glavni grčki tužitelj Dogiakos 10. siječnja 2023. službeno je izdao mišljenje u kojem je presudio da ADAE ne može provoditi istrage o evidencijama pružatelja telekomunikacijskih usluga kako bi istražio ukidanje povjerljivosti komunikacija. Prema navedenom mišljenju, kaznene sankcije mogle bi se primjenjivati nakon što ADAE započne takve revizije[301]. Tim se mišljenjem, koje je u suprotnosti s prethodnim mišljenjima glavnog državnog odvjetnika, jasno krši neovisnost ADAE-a[302] i pokušava ga se spriječiti u provođenju istraga. Na sastanku odbora PEGA 28. veljače 2023. Rammos je izjavio da Dogiakosovo mišljenje nije obvezujuće i da se zadaće ADAE-a mogu nastaviti izvršavati bez promjena[303].

189. ADAE je potvrdio da je EYP špijunirao i zapovjednika grčkih oružanih snaga Konstantinosa Florosa, trenutačno obnašajućeg ministra, nekoliko časnika koji se bave slučajevima o oružju i bivšeg savjetnika za pitanja nacionalne sigurnosti. Zbog trenutačne nemogućnosti da obavijesti mete istraga, ADAE je namjeravao predstaviti nalaze Odboru za transparentnost grčkog parlamenta i institucijama grčkog parlamenta[304]. Christos Rammos poslao je pismo grčkom parlamentu kako bi zatražio tu prezentaciju. Isprva je predsjednik izbjegavao pokrenuti raspravu o tome navodeći da nije imao vremena pročitati Rammosovo pismo na svoj imendan. Naposljetku je većina Odbora za institucije i transparentnost, koju čine članovi stranke Néa Dimokratía, odbila njegov zahtjev. Glasnogovornik Vlade napao je 24. siječnja 2023. ADAE i njegova predsjednika zbog istraga[305], tvrdeći da Rammos provodi „aktivizam" i „prekoračuje" svoje ovlasti, što nije pomoglo istragama koje provodi ADAE. Vođa stranke SYRIZA Alexis Tsipras 25. siječnja 2023. javno je, u grčkom parlamentu, prozvao osobe navedene u izvješću i time potvrdio da su zapovjednik oružanih snaga, bivši zapovjednik grčke vojske, ministar rada, bivši savjetnik premijera za pitanja nacionalne sigurnosti te dva savjetnika iz Uprave za opremu oružanih snaga stavljeni pod nadzor EYP-a. S obzirom na ozbiljnost nalaza, odbijanje da se ADAE-u dopusti izvješćivanje grčkog parlamenta i diskreditiranje tog tijela predstavlja ometanje odgovornosti i transparentnosti[306].

190. Osim toga, Rammos je naveo da su izmjene pravnog okvira ADAE-a stvorile nesigurnost, što je dovelo do razmjene pisama s ministarstvima kako bi se pojasnio

---

[300] Euractiv, „Exclusive: Another MEP and journalist the latest victims of 'Greek Watergate'" (Ekskluzivno: Još jedan zastupnik u EP-u i novinar najnovije žrtve „grčkog Watergatea").
[301] Euractiv, „Chief prosecutor puts Greece's rule of law to the test" (Glavni tužitelj stavlja grčku vladavinu prava na kušnju).
[302]http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bdilosi-toy-proedroy-tis-adae-christoy-rammoy-gia-tin-g/.
[303] Odbor PEGA, Razmjena gledišta s Konstantinosom Menoudakosom i Christosom Rammosom, 28. veljače 2023.
[304]https://www.protothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/.
[305] https://www.protothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/.
[306]Newsbomb, *ΣΥΡΙΖΑ: «Κυκλώνει» μέσω ΑΔΑΕ το Μαξίμου – Τι βλέπει πίσω από το «μπλόκο» ΝΔ σε Ράμμο* (SYRIZA: Maximos „kruži" kroz ADAE – ND „blokira" Rammosa, što to znači za Maximosa).

operativni okvir tog tijela za pritužbe i istrage. Rammos je spomenuo da ADAE prima otprilike 10 pritužbi dnevno[307].

ODBOR ZA INSTITUCIJE I TRANSPARENTNOST

191. Odbor za institucije i transparentnost pozvao je u srpnju 2022. Kontoleona i predsjednika ADAE-a Christosa Rammosa na parlamentarno saslušanje. Tijekom tog saslušanja Kontoleon je navodno priznao da je EYP špijunirao Thanasisa Koukakisa iz razloga povezanih s nacionalnom sigurnošću, ali je naveo da nema saznanja o pokušajima hakiranja Androulakisova uređaja softverom Predator. Glasnogovornik Vlade Giannis Oikonomou ustvrdio je da grčke vlasti nisu ni nabavile ni upotrebljavale špijunski softver Predator[308].

192. Iako su sastanci zatvoreni za javnost[309], navodno ni Kontoleon ni Dimitriadis nisu bili voljni pružiti bitne dokaze pozivajući se razloge povezane s nacionalnom sigurnošću[310]. Novi direktor EYP-a Demiris uskratio je odboru pristup izvješću koje sadržava informacije o navodnom uništenju nadzornih podataka[311]. To zapravo znači da EYP odbija odgovornost, a grčki parlament ne može izvršavati svoju ovlast za parlamentarni nadzor.

193. Odbor je 30. kolovoza 2022. pozvao devet osoba na saslušanje iza zatvorenih vrata, uključujući javnog tužitelja Vasilikija Vlachoua, bivšeg glavnog tajnika Grigorisa Dimitriadisa i bivšeg direktora EYP-a Kontoleona. Svi su se pozvali na povjerljivost i izbjegavali odgovaranje na pitanja tijekom tog saslušanja pred odborom[312].

PARLAMENTARNI ISTRAŽNI ODBOR

194. Za prijedlog stranke PASOK-KINAL o uspostavi odbora koji će istražiti navodnu uporabu špijunskog softvera[313] glasala su 142 zastupnika iz oporbe, dok je 157 zastupnika iz stranke Néa Dimokratía bilo suzdržano[314]. Međutim, ND je imao apsolutnu većinu u istražnom odboru. Pozivi na uspostavu dvostranačkog odbora odbijeni su. ND je utvrdio program rada i popis svjedoka koje će odbor pozvati te je odbio nekoliko svjedoka koje su predložile oporbene stranke. Odbor je uspostavljen 29. kolovoza 2022. Započeo je s radom 7. rujna 2022., a svoj je rad zaključio 10. kolovoza 2022.

195. Vladina većina u odboru odbila je pozvati na svjedočenje g. Bitziosa i g Lavranosa, ali

---

[307]Odbor PEGA, Razmjena gledišta s Konstantinosom Menoudakosom i Christosom Rammosom, 28. veljače 2023.
[308] Reuters. „Greek intelligence service admits spying on journalist - sources" (Grčka obavještajna služba priznaje špijuniranje novinara – izvori).
[309] Ekathimerini, „Transparency committee to hold closed-door meeting on phone hacking allegation" (Odbor za transparentnost održat će sastanak zatvoren za javnost o navodima o hakiranju telefona).
[310] Tovima, „In combat positions for eavesdropping" (U borbenim položajima zbog prisluškivanja).
[311] Tovima, „In combat positions for eavesdropping" (U borbenim položajima zbog prisluškivanja).
[312]Ieidiseis, „Nalazi SYRIZA-PASOK-a o prisluškivanju: Skandal i zataškavanje", https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi.
[313] Tovina. „Prisluškivanje:Istražni odbor za nadzor nad Androulakisom – detaljni pregled prijedloga stranke PASOK".
[314] Tovina. *„Parlament:Istraga o nadzoru iz 2016. izglasana sa 142 glasa za".*

je pozvala Stamatisa Tribalisa, aktualnog direktora Krikela, i Saru Hamou. Tribalis je pred parlamentarnim odborom svjedočio 22. rujna. G. Tribalis pritom je iznio bjelodano neistinite informacije o uključenosti Bitziosa i Lavranosa u Krikel, tvrdeći, među ostalim, da je vlasnik Krikela[315].

196. Svjedokinja Sara Hamou iz Intellexe tvrdila je da se ne može osobno pojaviti pred odborom (iako živi na Cipru) te joj je bilo dopušteno da svoje odgovore dostavi pismenim putem. Nije bilo moguće donijeti zajedničke zaključke zbog ozbiljne polarizacije političkog okruženja. Vladina većina odlučila je označiti oznakom tajnosti oko 5500 stranica dokumenata, uključujući zapisnik i iskaz koji je dala Hamou te glavne nalaze stranaka, iako je skidanje te oznake i omogućavanje pristupa tim informacijama u cijelosti u nadležnosti parlamenta. Stoga nije pripremljen javni sažetak. Samo je završna rasprava na plenarnoj sjednici grčkog parlamenta bila javna, a nalaze stranaka PASOK i SYRIZA objavile su same stranke.

197. Oporba je predložila druge svjedoke, kao što su Koukakis, Mitsotakis, Dimitriadis, Vlachou, Lavranos i Bitzios, no odbor ih je naposljetku odbio pozvati. Odbor je 10. listopada 2022. završio svoje istrage, a političke stranke podnijele su završna izvješća[316].

GRČKO TIJELO ZA ZAŠTITU PODATAKA

198. Grčko tijelo za zaštitu podataka neovisno je tijelo koje nadzire primjenu Opće uredbe o zaštiti podataka[317] (GDPR), drugih propisa i nacionalnih zakona o zaštiti osobnih podataka u Grčkoj[318]. Zakonom br. 4624/2019 nacionalna sigurnost isključena je iz nadležnosti Grčkog tijela za zaštitu podataka, iako je bila uključena od zakona iz 1997[319]. Nakon pritužbe Nikosa Androulakisa u srpnju 2022., tijelo je u srpnju 2022. pokrenulo istragu o instalaciji špijunskog softvera na mobilne telefone te o prikupljanju i obradi osobnih podataka koji su uslijedili. Tijelo je provelo reviziju u uredu Intellexe u Chalandriju i u objektu Intellexe u Ellinikou. Međutim, Intellexa nije dostavila ključne informacije, a na upitnike je odgovorila sa znatnim kašnjenjem, čime je narušila reviziju koju je to tijelo provodilo[320].

199. Grčko tijelo za zaštitu podataka izreklo je 16. siječnja 2023. novčanu kaznu poduzeću Intellexa S.A. u iznosu od 50 000 EUR[321]zbog ometanja i odbijanja suradnje tijekom revizije na temelju članka 31. Opće uredbe o zaštiti podataka.

200. Nakon mjere koju je poduzelo Grčko tijelo za zaštitu podataka, Intellexa je predala

---

[315] TVXS. *G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament* (G. Lavranos iza KRIKELA – Kako su pokušali zavarati Parlament).
[316] Ieidiseis. „Nalazi SYRIZA-PASOK-a o prisluškivanju: Skandal i zataškavanje”.
[317] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (SL L 119, 4.5.2016., str. 1.).
[318] Grčko tijelo za zaštitu podataka. *Personal data* (Osobni podaci).
[319] Službeni list Helenske Republike.
[320] Grčko tijelo za zaštitu podataka. „Imposition of a fine on Intellexa S.A. for non-cooperation with the HDPA” (Izricanje novčane kazne poduzeću Intellexa S.A. zbog nesuradnje s Grčkim tijelom za zaštitu podataka).
[321] Grčko tijelo za zaštitu podataka. „Imposition of a fine on Intellexa S.A. for non-cooperation with the HDPA” (Izricanje novčane kazne poduzeću Intellexa S.A. zbog nesuradnje s Grčkim tijelom za zaštitu podataka).

dokumente, ali ih tijelo još uvijek razmatra. Prema navodima predsjednika Grčkog tijela za zaštitu podataka g. Menoudakosa, nadležno tijelo otkrilo je nazive domena koji možda pripadaju poduzećima koja surađuju s Intellexom unutar i izvan EU-a. Istraga Grčkog tijela za zaštitu podataka još je u tijeku[322].

201. Na sastanku odbora PEGA 28. veljače 2023. predsjednik Grčkog tijela za zaštitu podataka spomenuo je da su u istrazi razmotrene internetske aplikacije za slanje tekstualnih poruka. Prema g. Menoudakosu, poduzeća su se koristila tim internetskim aplikacijama za slanje tekstualnih poruka povezanih sa špijunskim softverom Predator. Grčko tijelo za zaštitu podataka trenutačno pokušava utvrditi mete, ali je dosad potvrdilo da je 300 tekstualnih poruka poslano otprilike 100 primatelja primjenom te metode. Tijelo je poduzećima naložilo da čuvaju te podatke i naglasilo da ta poduzeća, ako nemaju pravnog zastupnika u EU-u, krše Opću uredbu o zaštiti podataka[323].

METE

THANASIS KOUKAKIS

202. EYP je prisluškivao novinara Thanasisa Koukakisa u ljeto 2020. On je u to vrijeme izvještavao o financijskim temama, uključujući skandal Piraeus/Libra, u koji je bio upleten Felix Bitzios, kao i navodnu utaju poreza koju je počinio grčki biznismen Yiannis Lavranos i kontroverzne zakone o bankarstvu koje je donijela grčka vlada, a kojima se ometa kazneni progon pranja novca i drugih financijskih malverzacija (zbog njegovog retroaktivnog učinka zapravo je odbačeno 12 predmeta koji su bili u tijeku)[324]. G. Koukakis također je istraživao nabavu novih osobnih iskaznica, u kojoj su g. Lavranos i g. Bitzios imali poslovni interes. Otprilike u vrijeme Koukakisova prvog svjedočenja pred odborom PEGA, natječaj je iznenada povučen, a odgovorni glavni tajnik podnio je ostavku.

203. Direktor EYP-a Panagiotis Kontoleon 29. srpnja 2022. izjavio je da je EYP nadzirao telefon g. Koukakisa iz „razloga povezanih s nacionalnom sigurnošću”.

204. EYP je 1. lipnja 2020. podnio prvi zahtjev za ukidanje povjerljivosti telefonskog broja g. Koukakisa na dva mjeseca, do 1. kolovoza 2020. EYP je podnio zahtjev za produljenje za dodatna dva mjeseca[325], tj. do 1. listopada 2020. Tužitelj Prizivnog suda Vasiliki Vlachou odobrio je sve te zahtjeve iz razloga povezanih s nacionalnom sigurnošću[326].

205. Međutim, dvanaest dana nakon toga, 12. kolovoza 2020., EYP je iznenada podnio zahtjev za prekid ukidanja povjerljivosti telefonskog broja g. Koukakisa, tj. mjesec i pol ranije nego što je to predviđeno prvotnim zahtjevom. To se dogodilo istog dana kad je

[322] Odbor PEGA, Razmjena gledišta s Konstantinosom Menoudakosom i Christosom Rammosom. 28.2.2023.
[323] Odbor PEGA, Razmjena gledišta s Konstantinosom Menoudakosom i Christosom Rammosom. 28.2.2023.
[324] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?*. (Tko je nadzirao mobilni telefon novinara Thanasisa Koukakisa?).
[325] Reporters United. *„Neprijatelj države:Dokazujemo da je vlada Mitsotakisa pratila novinara Thanasisa Koukakisa”*.
[326] Reporters United. „Neprijatelj države: Dokazujemo da je vlada Mitsotakisa pratila novinara Thanasisa Koukakisa”; Inside Story. „Who was tracking journalist Thanasis Koukakis' cell phone?” (Tko je nadzirao mobilni telefon novinara Thanasisa Koukakisa?).

Koukakis pristupio ADAE-u sa zahtjevom da mu se pruže informacije o mogućem nadzoru njegovih dvaju mobilnih telefona i fiksne telefonske linije.

206. ADAE je 10. ožujka 2021. tužitelja EYP-a izvijestio o mogućnosti da se Koukakisa obavijesti o nadzoru njegova mobilnog telefona. Međutim, 31. ožujka grčka je vlada donijela Izmjenu br. 826/145 kojom je ADAE-u ukinuta mogućnost da obavijesti građane o ukidanju povjerljivosti komunikacija s retroaktivnim učinkom[327]. Predsjednik ADAE-a Christos Rammos i druga dva člana ADAE-a protivili su se toj izmjeni i u jednom osvrtu istaknuli da se izmjenom krši pravo na poštovanje privatnog i obiteljskog života iz Europske konvencije o ljudskim pravima (EKLJP) i zaštita povjerljivosti komunikacija kako je zajamčena Ustavom[328].

207. Od 12. srpnja 2021. do 14. rujna 2021. telefon g. Koukakisa bio je zaražen špijunskim softverom Predator[329]. Kako navodi g. Koukakis, primio je tekstualnu poruku s poveznicom na internetsku stranicu s financijskim vijestima[330]. Organizacija Citizen Lab 28. ožujka 2022. službeno je otkrila da je mobilni telefon bio zaražen[331].

208. G. Koukakis nekoliko je puta pokušao dobiti pravnu zaštitu zbog pokušaja nadzora. Podnio je dvije pritužbe ADAE-u. Prvu je podnio 6. travnja 2022. te je njome zatražio temeljitu istragu zbog zaraze svojeg mobilnog telefona Predatorom, dok je drugu podnio 13. svibnja 2022. zbog novih otkrića koja su objavili InsideStory i Reporters United. Osim toga, g. Koukakis je 4. svibnja 2022. podnio pritužbu EAD-u, kojom je zatražio istragu pozadine presretanja koje je izvršio EYP i napada Predatora[332].

209. Istraga koju je 21. srpnja 2022. provelo Nacionalno tijelo za transparentnost (EAD) u uredima atenske podružnice Intellexe, dobavljača špijunskog softvera Predator, bila je ograničena i površna unatoč tomu što je postojala mogućnost pronalaska ključnih informacija o kaznenom djelu napada softverom Predator. Nije se zaplijenio niti osigurao ni jedan server, računalni hardver ni administrativni dokumenti. Provjera financijskog upravljanja bila je ograničena na 2020[333]. Podružnice Intellexe u Cipru i Irskoj nisu uopće bile pod istragom[334]. Istrage nisu uključivale informacije o bankovnim

[327] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis (Neprijatelj države: Dokazujemo da je vlada Mitsotakisa pratila novinara Thanasisa Koukakisa): https://www.reportersunited.gr/8646/eyp-koukakis/ Inside Story. Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?* (Tko je nadzirao mobilni telefon novinara Thanasisa Koukakisa?).
[328] Constitutionalism. „Proturječnost članka 87. Zakona br. 4790/2021 s jamstvima EKLJP-a za zaštitu povjerljivosti komunikacija”: https://www.constitutionalism.gr/2021-04-07-rammos-gritzalis-papanikolaou-aporrito-epikinonion/.
[329] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?* (Tko je nadzirao mobilni telefon novinara Thanasisa Koukakisa?).
[330] Europski parlament. Saslušanje održano 8. rujna 2022.
[331] Inside Story. „Who was tracking journalist Thanasis Koukakis' cell phone?” (Tko je nadzirao mobilni telefon novinara Thanasisa Koukakisa?).
[332] Avgi. *Thanasis Koukakis / Filed a lawsuit for the Predator – Who and why was watching him* (Thanasisi Koukakis podnio tužbu zbog Predatora – Tko ga je pratio i zašto).
[333] InsideStory. *From Koukakis to Androulakis:A new twist in the Predator spyware case* (Od Koukakisa do Androuakisa: novi zaplet u priči o špijunskom softveru Predator)
[334] InsideStory. „From Koukakis to Androulakis: A new twist in the Predator spyware case” (Od Koukakisa do Androuakisa: novi zaplet u priči o špijunskom softveru Predator).

računima Intellexe ni njezinih podružnica[335]. G. Koukakis je 27. srpnja 2022. podnio žalbu Europskom sudu za ljudska prava[336].

210. G. Koukakis je 5. listopada 2022. tužiteljima u Ateni podnio kaznenu prijavu protiv poduzeća Intellexa Alliance, posebno Tala Diliana i Sare Hamou[337] zbog povrede povjerljivosti njegovih komunikacija[338].

NIKOS ANDROULAKIS

211. Nikos Androulakis, vođa stranke lijevog centra PASOK-KINAL i zastupnik u Europskom parlamentu, našao se na meti špijunskog softvera Predator 21. rujna 2021. kad je na njegov telefon poslana zlonamjerna poveznica[339]. G. Androulakis je primio tekstualnu poruku u kojoj je pisalo: „Uozbiljimo se malo, čovječe, ovo nam može biti jako korisno". Poruka je sadržavala i poveznicu za instalaciju špijunskog softvera Predator na njegov telefon, ali g. Androulakis, za razliku od g. Koukakisa, nije kliknuo poveznicu koja mu je poslana[340]. Na sastanku odbora PEGA 28. veljače 2023. g. Androulakis naveo je da je grčko tijelo za zaštitu podataka (HDPA) utvrdilo s kojeg je računa kreditne kartice plaćena tekstualna poruka koja mu je poslana. Ta je informacija proslijeđena relevantnom tužitelju[341].

212. U rujnu 2021. g. Androulakis objavio je svoju kandidaturu u utrci za vođu stranke[342]. Prema istrazi ADAE-a u tom je razdoblju mobilni telefon g. Androulakisa bio pod nadzorom EYP-a posredstvom pružatelja telekomunikacijskih usluga[343]. Tužitelj EYP-a Vasiliki Vlachou odobrio je ukidanje tajnosti telefona g. Androulakisa zbog razloga „nacionalne sigurnosti". Odobrenje se vremenski podudaralo i s nadziranjem Predatorom i kandidaturom g. Androulakisa.

213. Kad je g. Androulakis izabran za vođu stranke u prosincu 2021., „službeno" nadziranje koje je provodio EYP iznenada je završeno[344] unatoč tomu što ponovno odobrenje za njegov nadzor od dva mjeseca još nije bilo isteklo.

214. Glavna uprava Europskog parlamenta za inovacije i tehnološku podršku (DG ITEC) 28. lipnja 2022. provjerila je mobilni telefon g. Androulakisa i otkrila dokaze o

---

[335] InsideStory. „From Koukakis to Androulakis: A new twist in the Predator spyware case" (Od Koukakisa do Androuakisa: novi zaplet u priči o špijunskom softveru Predator).
[336] BBC. *„Greece wiretap and spyware claims circle around PM Mitsotakis" (Tvrdnje o prisluškivanju i špijunskom softveru u Grčkoj vode do zastupnika u Parlamentu g. Mitsotakisa)*.
[337] Vijesti 24 7. Skandal s prisluškivanjem: Lawsuit against Intellexa by Thanasis Koukakis (Skandal s prisluškivanjem: Thanasis Koukakis podnio tužbu protiv Intellexe).
[338] Heinrich Boll Stiftung. *A State of Absolute Solitude*(Stanje potpune samoće).
[339] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.(Od Koukakisa do Androuakisa: novi zaplet u priči o špijunskom softveru Predator).
[340] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader*.(Komisija Europske unije zabrinuta zbog novog slučaja špijuniranja vođe socijalističke stranke u Grčkoj)
[341] Razmjena gledišta odbora PEGA s Konstantinosom Menoudakosom i Christosom Rammosom. 28.2.2023.
[342] Tovima. Androulakis lashes out at PM, ND spokesman says Pasok leader should say why his phone was tapped (Androulakis kritizira premijera, glasnogovornik stranke ND navodi da bi vođa stranke Pasok trebao reći zašto je njegov telefon prisluškivan).
[343] Kathimerini. *Surveillance case:the data that triggered the developments* (Slučaj nadzora: podaci koji su pokrenuli događaje).
[344] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader*.(Komisija Europske unije zabrinuta zbog novog slučaja špijuniranja vođe socijalističke stranke u Grčkoj).

pokušaju hakiranja Predatorom iz rujna 2021. te je o tome obavijestila g. Androulakisa[345]. G. Androulakis je 26. srpnja 2022. podnio kaznenu prijavu Uredu javnog tužitelja pri Vrhovnom sudu[346].

215. Nakon nekoliko dana, 29. srpnja, g. Androulakis je ADAE-u iznio informacije o napadu Predatorom. Istog je dana Stalni odbor za institucije i transparentnost saslušao ravnatelja EYP-a Panagiotisa Kontoleona i predsjednika ADAE-a Christosa Rammosa u prisutnosti ministra digitalnog upravljanja i državnog tajnika. Sastanak se održao iza zatvorenih vrata[347].

216. G. Androulakis je 8. rujna 2022. od ADAE-a zatražio da mu preda dosjee o njegovu prisluškivanju[348]. Međutim, istog je dana dnevnik Ta Nea prenio službenu vijest ADAE-a, u kojoj je navedeno da je EYP uništio dosjee koji se odnose na g. Androulakisa i g. Koukakisa[349]. Nedvojbena je činjenica da su uništeni, ali i dalje nije jasno zašto. S jedne strane, neki izvori uništenje dosjea pripisuju promjeni elektroničkih sustava EYP-a 2021.[350] Ta je promjena elektroničkih sustava na novi sustav sastavljanja pravnih dokumenata navodno uzrokovala tehnički problem koji je doveo do uništenja dosjea. S druge strane, drugi izvori tvrde da je g. Kontoleon izdao naredbu za uništenje tih dosjea 29. srpnja 2022., istog dana kad je Androulakis obavijestio ADAE-a o pokušajima nadzora[351]. Na sastanku odbora PEGA, predsjednik ADAE-a g. Rammos nije potvrdio niti zanijekao uništenje zapisa[352].

217. G. Kontoleon i G. Dimitriadis dali su 5. kolovoza ostavke na svoje položaje. G. Mitsotakis je 8. kolovoza dao izjavu za televiziju i potvrdio prisluškivanje g. Androulakisa te ponovio da nije znao za nadzor[353].

218. EYP je za sada odbio objaviti razloge nadzora. EYP je ponudio da privatno obavijesti g. Androulakisa o razlozima nadzora. To bi bilo nezakonito. G. Androulakis zatražio je da se njegov dosje o nadzoru podnese Odboru za institucije i transparentnost, ali je odbijen.

219. G. Androulakis je 7. prosinca 2022. podnio pritužbu Europskom sudu za ljudska prava zbog toga što ga je EYP prisluškivao i zbog nedostatka službenih informacija o njegovu

---

345 Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader (Komisija Europske unije zabrinuta zbog novog slučaja špijuniranja vođe socijalističke stranke u Grčkoj).
346 News 247. Nikos Androulakis: Near-Victim of Predator Software - Filed a Lawsuit (Nikos Androulakis zamalo je bio žrtva softvera Predator te je podnio tužbu).
347 Avgi. *Predator scandal / EYP dragged to Parliament over surveillance*(Skandal sa softverom Predator / EYP pred Parlamentom zbog nadzora).
348 Ekathimerini. Androulakis asks ADAE for his wiretapping file (Androulakis traži od ADAE-a svoj dosje o prisluškivanju).
349 TaNea*. The archive of the surveillance of Nikos Androulakis destroyed (Arhiva nadzora Nikosa Androulakisa uništena).*
350 TVXS. *„G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament" (G. Lavranos iza KRIKELA – Kako su pokušali zavarati Parlament).*
351 Ieidiseis*. „SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up" (Nalazi o prisluškivanju SYRIZA-PASOK: skandal i zataškavanje).*
352 Europski parlament. Saslušanje 8. rujna 2022.
353 Reuters*. „Greek PM says he was unaware of phone tapping of opposition party leader" (Grčki premijer tvrdi da nije znao za prisluškivanje telefona vođe oporbene stranke).*

slučaju[354].

220. Podvrgavanje političara nadzoru vrlo je neuobičajeno, a grčkim Ustavom predviđena je posebna zaštita za političare. EYP poriče bilo kakvo sudjelovanje u nadzoru s pomoću špijunskog softvera Predator. Vlada je u početku sugerirala da su prisluškivanje g. Androulakisa navodno naručile strane sile ili da bi razlog prisluškivanja moglo biti njegovo članstvo u odboru Europskog parlamenta zaduženom za odnose s Kinom. Nijedna od tih hipoteza nije bila pretjerano vjerodostojna. Prisluškivanje se dogodilo u političkom kontekstu nadolazećih izbora. U tom slučaju PASOK bi bio preferirani koalicijski partner. U jesen 2021. PASOK je održavao izbore za novo stranačko vodstvo, a četvero kandidata imalo je različite stavove o takvoj koaliciji. Za g. Androulakisa se tvrdilo da bi bio otvoren za takvu ideju, ali ne dok je g. Mitsotakis predsjednik vlade. Jedan od preostalih kandidata, Andreas Loverdos, već je jednom bio ministar u koalicijskoj vladi koju su činili Néa Demokratía i PASOK te se smatralo da je skloniji toj ideji. Usto je poznavao g. Dimitriadisa. Popis drugih navodnih meta koji je objavio Documento doprinosi sumnji da je nadzor bio motiviran političkim razlozima. Za nijednu od tih hipoteza nema dokaza, ali je od ključne važnosti da se te sumnje istraže i po mogućnosti isključe.

GIORGOS KYRTSOS

221. ADAE-ovom revizijom poduzeća za telekomunikacije Cosmote 15. prosinca 2022. potvrđeno je da je član Europskog parlamenta Giorgos Kyrstos bio pod nadzorom EYP-a[355]. Prisluškivali su mu se i mobilni telefon i fiksna telefonska linija. Nadzor je prema izvješću produljen devet puta[356] na puno razdoblje od 18 mjeseci.

222. Giorgios Kyrtsos bivši je član stranke Néa Demokratía i Europske pučke stranke. U veljači 2022. ND je izbacio g. Kyrtsosa iz vladajuće grčke stranke jer nije odobravao postupke vlade povezane s pandemijom bolesti COVID-19, ograničenjima slobode medija i pristupom skandalu s poduzećem Novartis[357]. Nakon što je izbačen, g. Kyrtsos je postao član kluba zastupnika Renew Europe.

STAVROS MALICHOUDIS

223. Dnevni list EFSYN otkrio je 13. studenoga 2021. da EYP navodno prisluškuje nekolicinu novinara koji su izvještavali o slučajevima izbjeglica. EYP-ov interni dokument pokazao je da je EYP naredio nadzor i prikupljanje podataka o grčkom novinaru Stavrosu Malichoudisu[358,359]. Malichoudis je pisao o dvanaestogodišnjem djetetu iz Sirije koje je bilo prisiljeno nekoliko mjeseci živjeti u kampu za zadržavanje

---

[354] Ekathimerini. *„Socialist leader appeals to European Court over tapping" (Vođa socijalističke stranke podnosi tužbu Europskom sudu zbog prisluškivanja).*
[355] Euractiv. „Another MEP and journalist the latest victims of 'Greek Watergate" (Još jedan zastupnik u Europskom parlamentu i novinar najnovije žrtve „grčkog Watergatea").
[356] Politico. *„Greek prosecutor slams unflattering comparisons to Belgium's Qatargate probe" (Grčki tužitelj odbija neugodne usporedbe s belgijskom istragom Qatargate).*
[357] Euractiv. *„Renew Europe welcomes first Greek MEP who left EPP" (Renew Europe pozdravlja prvog grčkog zastupnika Europskog parlamenta koji je napustio Europsku pučku stranku).*
[358] Efsyn. *Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ.*
[359] Solomon. *Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'* (Novinar Solomona Stavros Malichudis pod nadzorom zbog „nacionalne sigurnosti").

na grčkom otoku Kosu[360].

224. Glasnogovornik Vlade Giannis Oikonomou 15. studenog 2021. neizravno je potvrdio tvrdnje. Izjavio je da EYP može prisluškivati pojedince ako postoji opasnost za nacionalnu sigurnost zbog „unutarnjih ili vanjskih prijetnji”[361]. Međutim, 24. studenog i 17. prosinca 2021. državni tajnik George Gerapetritis porekao je bilo kakvo nadziranje novinara u Grčkoj, uključujući g. Malouchidisa, ali prema medijskoj kući Solomon nije potvrdio niti porekao autentičnost internih dokumenata EYP-a[362].

225. Na saslušanju pred odborom PEGA u vezi Grčke 8. rujna 2022. g. Malichoudis je izjavio da je prisluškivanjem njegova telefona EYP mogao prikupljati informacije i od kolega i novinara s kojima je u to vrijeme bio u kontaktu[363]. EYP je navodno mogao prisluškivati razgovore koje je g. Malichoudis vodio s Međunarodnom organizacijom za migracije (IOM)[364], čime se ističe da je to opasno za ostale, takozvane „usputne ulove” prisluškivanja pojedinca. Usto, g. Malichoudis je za vrijeme saslušanja pokazao dokaze da se EYP zanimao za njegov rad i izvore, ali da je razlog nadzora obuhvaćen „nacionalnom sigurnošću’[365].

CHRISTOS SPIRTZIS

226. Christos Spirtzis, bivši ministar infrastrukture i zakonodavac iz stranke Syriza, tvrdio je 9. rujna 2022. da je bio žrtva napada špijunskim softverom Predator na svoj mobilni telefon[366]. Spirtzis je 15. studenoga 2021. postavio važna parlamentarna pitanja vladi o zadacima EYP-a u pogledu nadzora. Istog je dana primio poruku[367] sličnu poruci koju je dobio Nikos Androulakis. Christosu Spirtzisu poslana je druga poruka 19. studenoga koja je sadržavala poveznicu na članak medijske kuće Efimerida ton Syntakton[368]. Iako CitizenLab nije provjerio te poruke, Spirtzis je proslijedio poveznice koje je primio dvama stručnjacima, koji su usmeno potvrdili da je bio žrtva napada[369]. Spirtzis je 9. rujna 2022. podnio pritužbu tužitelju Vrhovnog suda[370]. Spirtzis je osoba od povjerenja vođe stranke Alexisa Tsiprasa te sudjeluje u sastancima vodstva stranke na

---

[360] BalkanInsight. *Greek Intelligence Service Accused of ‘Alarming’ Surveillance Activity* (Grčka obavještajna služba optužuje se zbog „zabrinjavajućih” aktivnosti nadzora).
[361] BalkanInsight. „Greek Intelligence Service Accused of ‘Alarming’ Surveillance Activity” (Grčka obavještajna služba optužuje se zbog „zabrinjavajućih” aktivnosti nadzora).
[362] Solomon, „Solomon’s reporter Malichudos under surveillance for national security reasons” (Novinar Solomona Malichudis pod nadzorom zbog nacionalne sigurnosti).
[363] Europski parlament. Saslušanje 8. rujna 2022.
[364] BalkanInsight. *„Greek Intelligence Service Accused of ‘Alarming’ Surveillance Activity” (Grčka obavještajna služba optužuje se zbog „zabrinjavajućih” aktivnosti nadzora).*
[365] Europski parlament. Saslušanje 8. rujna 2022.
[366] Ekathimerini. Former SYRIZA minister says he was targeted by Predator (Bivši ministar stranke SYRIZA tvrdi da je bio žrtva napada softverom Predator).
[367] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware* (Pokušaj hakiranja oporbenog člana Parlamenta Christosa Spirtzisa ilegalnim špijunskim softverom Predator).
[368] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware* (Pokušaj hakiranja oporbenog člana Parlamenta Christosa Spirtzisa ilegalnim špijunskim softverom Predator).
[369] Inside story, *Predator: More than 20 targets in Greece according to the Data Protection Authority.* (Predator: više od 20 žrtava u Grčkoj prema nacionalnoj tijelu za zaštitu podataka).
[370] Reuters. *„One more Greek lawmaker files complaint over attempted phone hacking” (Još jedan zakonodavac podnosi pritužbu zbog pokušaja hakiranja telefona); Euractiv. „Another Greek opposition lawmaker victim of Predator” (Još jedan oporbeni zakonodavac u Grčkoj žrtva Predatora).*

visokoj razini.

TASOS TELLOGLOU, ELIZA TRIANTAFYLLOU I THODORIS CHONDROGIANNOS

227. Tasos Telloglou i Eliza Triantafyllou navodno su bili špijunirani za vrijeme svojeg istraživačkog rada za medijsku kuću Inside Story. U članku za Heinrich-Böll-Stiftung od 24. listopada 2022. Telloglou je podijelio svoja iskustva nadzora i zastrašivanja iz vremena kad je istraživao skandal s nadzorom u Grčkoj. U skladu s tim iskustvima, smatra da je bio pod nadzorom između svibnja i kolovoza 2022[371].

228. Usto, izvor iz sigurnosne službe u lipnju 2022. obavijestio je Tellogloua da su i on i njegovi kolege Eliza Triantafyllou (InsideStory) i Thodoris Chondrogiannos (Reporters United) bili pod nadzorom vlasti kako bi se procijenilo s kojim se izvorima sastaju[372]. U vrijeme izrade ovog nacrta izvješća, grčka Vlada još nije odgovorila na te navode.

229. ADAE-ovom revizijom poduzeća za telekomunikacije Cosmote 15. prosinca 2022. potvrđeno je da je Telloglou bio pod nadzorom EYP-a. Razlozi nadzora nisu otkriveni zbog „nacionalne sigurnosti”[373].

DRUGE METE

230. Dana 29. listopada 2022. objavljeno je da su se na meti špijunskog softvera Predator našli i drugi političari, uključujući jednog ministra u vladi koji nije bio u dobrim odnosima s predsjednikom vlade. Osim toga, još jedan član stranke Néa Demokratía navodno je primio poveznicu za instalaciju Predatora[374]. Glasnogovornik vlade g. Oikonomou naveo je da u članku nedostaju konkretni dokazi[375].

231. Documento je 5. i 6. studenoga 2022. izvijestio o popisu na kojem se nalazilo 33 imena osoba koje su se našle na meti špijunskog softvera Predator[376]. Popis je obuhvaćao brojne istaknute političare, uključujući članove aktualne vlade, bivšeg predsjednika vlade Samarasa i bivšeg povjerenika EU-a Avramopoulosa, kao i glavnog urednika nacionalnih novina naklonjenih vladi te osobe bliske Vangelisu Marinakisu, brodovlasniku, medijskom mogulu i vlasniku nogometnih klubova Olympiakos i Nottingham Forest. ADAE je potvrdio da je EYP nadzirao neke od osoba s popisa u okviru konvencionalnog prisluškivanja. Imena su uključivala zastupnika u Europskom parlamentu Giorgosa Kyrtsosa[377], zapovjednika grčkih oružanih snaga generala

---

[371] Heinrich-Böll-Stiftung. *A State of Absolute Solitude* (Stanje potpune samoće).
[372] MapMF, „Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations” (Tri grčka novinara navodno nadzirana i praćena u vezi s istraživanjem skandala o špijunskom softveru).
[373] Euractiv, Another MEP and journalist the latest victims of ‘Greek Watergate’ (Još jedan zastupnik u Europskom parlamentu i novinar najnovije žrtve „grčkog Watergatea”).
[374] Ta Nea, *Four illegal manipulations by suspicious center* (Četiri ilegalne manipulacije sumnjivog centra).
[375] Politico, *Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes* (Operativni protokol iz Bruxellesa: Lula odnosi pobjedu u Brazilu – Trik ili trgovina – Problemi sa zelenim planom).
[376] Documento, 6. studenoga 2022.
[377] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*.

Konstantinosa Florosa[378], zapovjednika grčke vojske Haralambosa Lalousisa[379], ministra rada i socijalne skrbi Kostisa Hatzidakisa[380], bivše generalne direktore Uprave za opremu i ulaganja u obrani Theodorosa Lagiosa i Aristidesa Alexopoulosa[381], bivšeg savjetnika za sigurnosna pitanja Alexandrosa Diakopoulosa[382] i grčkog istraživačkog novinara Tasosa Tellogloua[383].

232. Osim toga, bivša voditeljica politike kibersigurnosti tvrtke Meta Artemis Seaford također se nalazila na popisu 33 osobe te je potvrđeno da ju je EYP istovremeno prisluškivao i špijunirao upotrebom softvera Predator. EYP je prisluškivao Seaford od srpnja 2021. do ljeta 2022., što znači da je odobrenje za prisluškivanje uređaja gđe Seaford bilo obnovljeno šest puta, a za svaku je obnovu u načelu bilo potrebno odobrenje tužitelja iz EYP-a Vasilikija Vlachoua. CitizenLab je potvrdio da je njezin mobilni telefon isto tako zaražen Predatorom najmanje dva mjeseca od rujna 2021. To znači da se zaraza Predatorom dogodila približno jedan do dva mjeseca nakon početka konvencionalnog prisluškivanja. Gđa Seaford izjavila je da su informacije o njezinu terminu za cijepljenje protiv bolesti COVID-19 dobivene pristupanjem njezinim tekstualnim porukama putem konvencionalnog prisluškivanja. Te su informacije naknadno upotrijebljene za izradu sofisticiranog automatiziranog SMS-a, koji je bio istog općeg izgleda kao i službeni termin, uz zahtjev za potvrđivanje termina s pomoću poveznice. Klikom na tu poveznicu uređaj je zaražen špijunskim softverom Predator. SMS poruke sadržavale su točne i detaljne informacije iz njezina spisa o cijepljenju te su poslane u razmaku od samo nekoliko minuta od stvarnih, službenih poruka, što znači da je osoba koja je poslala poruke imala pristup sadržaju i razdoblju slanja SMS poruka, što bi EYP imao putem konvencionalnog prisluškivanja.

233. Prisluškivanje i/ili nadzor privatne osobe neobični su, posebno kad se u takvom slučaju ne može valjano pozvati na nacionalnu sigurnost. Time se postavlja pitanje koji su drugi motivi mogli imati ulogu u odabiru te mete. Do nadzora je došlo dok je gđa Seaford radila u poduzeću Meta, koje je objavilo izvješće o prijetnji koju predstavlja industrija nadzora za najam i na svojoj platformi zabranilo više poduzeća koja proizvode špijunski softver, uključujući Cytrox. No ne čini se vjerojatnim da je njezina uloga u Meti bila razlog za nadzor. Izvješće o prijetnji tvrtke Meta objavljeno je tek u prosincu 2021., nekoliko mjeseci nakon razdoblja u kojemu je uređaj gđe Seaford prisluškivan, a nijedna druga osoba koja je sudjelovala u izradi izvješća nije bila ciljana. Osim toga, gđa Seaford navela je[384] da je samo djelomično sudjelovala u tim aktivnostima i da je poduzeće Meta vrlo diskretno kad je riječ o otkrivanju imena svojih zaposlenika.

234. U ožujku 2021. časopis Marie-Claire objavio je članak koji uključuje isječak iz zbirke knjiga koje je napisala gđa Seaford. U članku se navode iskustva gđe Seaford sa

[378] https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyp-toy-mitsotakiAvgi,
[379] *https://www.avgi.gr/politiki/437362_ayta-einai-ta-6-prosopa-poy-parakoloythoyse-i-eyp-toy-mitsotaki.*
[380] https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/.
[381] *https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/.*
[382] *https://balkaninsight.com/2023/01/25/greece-motion-of-no-confidence-filed-the-opposition-against-the-government/.*
[383] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*.
[384] Sastanak odbora PEGA, 20. travnja 2023.

svakodnevnim seksizmom i uznemiravanjem u Grčkoj te je posebno opisan slučaj u kojemu ju je seksualno uznemiravao jedan „političar”[385]. Nadzor je započeo nekoliko mjeseci nakon toga. Jedno moguće objašnjenje je da je dotični političar pročitao članak i da se pribojavao da bi njegovo ime moglo biti otkriveno u javnosti. Drugo objašnjenje moglo bi biti da je netko drugi prepoznao o kojem se političaru radi iz opisa u članku te je htio prikupiti dodatne informacije o toj osobi iz političkih razloga. Neovisno o tome koji je motiv, vrlo je malo osoba koje imaju ovlasti predati službeni zahtjev za prisluškivanje EYP-u te dogovoriti upotrebu špijunskog softvera Predator. Kombinacija EYP-ova nadzora i upotrebe špijunskog softvera Predator potvrđena je i u drugim slučajevima.

235. Važno je da se te mogućnosti dodatno istraže, posebno pitanje tko je zatražio nadzor EYP-a. Gđa Seaford podnijela je zahtjev ADAE-u i pritužbu sudu u Grčkoj. No, istraga još traje. Ona je prva državljanka SAD-a za koju se zna da je bila žrtva u EU-u[386][387].

236. Ostala imena na popisu koja nisu službeno potvrđena uključuju bivšeg ministra obrazovanja i vjerskih pitanja Andreasa Loverdosa, bivšeg premijera Antonisa Samarasa, državnog tajnika Georgea Gerapetritisa, bivšeg povjerenika EU-a Dimitrisa Avramopoulosa, ministra Nikosa Dendiasa, ministricu obrazovanja Niki Kerameus, ministra Akisa Skertsosa, ministra ulaganja Nikosa Papathanasisa, bivšeg ministra zaštite građana Mihalisa Chrysochoidisa, zamjenika grčkog ministra obrane Nikosa Hardaliasa, Aristoteliju Peloni, zastupnika u Parlamentu Christosa Spirtzisa, bivšu ministricu zaštite građana Olgu Gerovasili, ravnatelja grčke policije Michalisa Karamalakisa, načelnika ureda tužitelja za gospodarska pitanja Christosa Bardakisa, tužiteljicu iz EYP-a Eleni Vlachou, glasnogovornika vlade Giannisa Oikonomoua, zamjenika ravnatelja EYP-a Vassilisa Grizisa. Otkrića povezana s popisom izrazito su uznemirujuća, ne samo zbog imena osoba visokog profila, nego i zbog sustavne i opsežne zlouporabe špijunskog softvera.

237. ADAE je 2023. izvijestio da je EYP prisluškivao ministra koji trenutačno obnaša dužnost, nekoliko časnika koji su se bavili slučajevima koji uključuju oružje i bivšeg savjetnika za pitanja nacionalne sigurnosti[388].

ZAKLJUČNE NAPOMENE

238. Prisutni su obrasci koji upućuju na to da grčka vlada omogućuje upotrebu špijunskog softvera protiv novinara, političara i osoba iz poslovnog svijeta. Isto tako dozvoljava izvoz špijunskog softvera u zemlje s lošim stanjem u pogledu ljudskih prava i omogućuje osposobljavanje dionika iz zemalja koje nisu članice EU-a koji žele saznati više o špijunskom softveru. Iako je upotreba špijunskog softvera u Grčkoj protuzakonita, istrage o podrijetlu napada špijunskim softverom dobile su zamah tek u ljeto 2022. Politička većina navodno se upotrebljava za promicanje pojedinačnih

[385] https://www.marieclaire.gr/art-lifestyle/artemis-seaford-i-chiroteri-morfi-katapiesis-ine-afti-pou-den-katalavenis-oti-ifistase/.

[386] *https://www.nytimes.com/2023/03/20/world/europe/greece-spyware-hacking-meta.html#:~:text=Artemis%20Seaford%2C%20a%20dual%20U.S.,of%20illicit%20snooping%20in%20Europe*.

[387] Sastanak odbora PEGA, 20. travnja 2023.

[388] Politico. *Brussels Playbook: Globalization's sanatorium - Vestager rings alarm - S(upended & D(dumped) (Operativni protokol iz Bruxellesa: Sanatorij globalizacije – Vestager upozorava – Suspendirani i odbačeni).*

interesa umjesto općeg interesa, posebno imenovanjem suradnika i pristaša na ključne položaje u organizacijama kao što su EYP, EAD (Nacionalno tijelo za transparentnost) i Krikel (poduzeće specijalizirano za elektroničke sigurnosne sustave). Najviše političko vodstvo u zemlji upotrebljava špijunski softver kao instrument političke moći i kontrole, u nekim slučajevima istodobno ili nakon zakonitog presretanja. Grčka u načelu ima prilično čvrst pravni okvir. Međutim, ključne mjere zaštite oslabljene su zakonskim izmjenama, a politička imenovanja na ključne položaje prepreka su nadzoru i odgovornosti. Mehanizmi *ex ante* i *ex post* nadzora namjerno su oslabljeni, a transparentnost i odgovornost se izbjegavaju. Novinari koji kritički izvještavaju ili dužnosnici koji se bore protiv korupcije i prijevare suočavaju se sa zastrašivanjem i ometanjem. Sustav zaštitnih mjera i nadzor nad praćenjem općenito nisu primjereni da bi se građani zaštitili od zlouporabe za koju su odgovorne državne agencije i privatni akteri. Potrebno je učiniti više kako bi se riješio taj problem. Osim toga, izgovor „nacionalne sigurnosti” navodi se kao opravdanje za prisluškivanje pojedinaca.

239. Špijuniranje iz političkih razloga nije novost u Grčkoj, ali nove tehnologije špijunskog softvera znatno olakšavaju nezakonit nadzor, posebno u kontekstu znatno oslabljenih zaštitnih mjera. Za razliku od drugih slučajeva, na primjer Poljske, čini se da zlouporaba špijunskog softvera u Grčkoj nije dio integrirane autoritarne strategije, već instrument koji se ad hoc upotrebljava za ostvarenje političkih i financijskih koristi. Međutim, njime se u istoj mjeri potkopavaju demokracija i vladavina prava te se ostavlja prostor za korupciju u ovim burnim vremenima koja iziskuju pouzdano i odgovorno vodstvo.

I.D Cipar

240. Odbor je posjetio Cipar u studenome 2022. u okviru zajedničke misije u Grčkoj i Cipru. Članovi su se susreli s ministricom energetike, trgovine i industrije, drugim vladinim službenicima i članovima Zastupničkog doma koji sudjeluju u radu relevantnih odbora kako bi se raspravilo o aktualnom pravnom okviru primjenjivom na špijunski softver. Čuli su i mišljenja pravnih stručnjaka, predstavnika nevladinih organizacija i novinara koji su Odboru predali dokumentaciju o nadzoru i korupciji. Odbor je istaknuo da bi se trebale poduzeti dodatne mjere u pogledu registara stvarnih vlasnika, koji nisu dovoljno transparentni iako su osmišljeni kako bi se razjasnila ta pitanja.

241. Za razliku od drugih država članica, ne postoji mnogo informacija o uporabi špijunskog softvera u Cipru. Nema službeno potvrđenih slučajeva osoba koje su nezakonite mete špijunskog softvera ili su bile mete takvog softvera. Međutim, ciparska vlada navodno je u veljači 2018. pratila novinara Makariosa Drousiotisa primjenom tehnika prisluškivanja i špijunskog softvera[389]. Na papiru postoji snažan pravni okvir, uključujući pravila EU-a, ali je Cipar u praksi atraktivno mjesto za poduzeća koja prodaju tehnologije za nadzor. No vlada to poriče i ukazuje na smanjenje broja registriranih poduzeća koja proizvode špijunski softver u zemlji. Međutim, nedavni skandali nanijeli su štetu ugledu te države te se očekuje da će skup novih zakonodavnih inicijativa kojima se pooštrava zakonodavni okvir za izvoz i poboljšava usklađenost biti dovršen u 2023.

242. Između Cipra i Grčke postoje bliske veze u pogledu špijunskog softvera. Intellexa, poduzeće Tala Diliana, ima sjedište u Grčkoj, a njegov špijunski softver Predator

[389] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/.

upotrebljavao se u grčkim skandalima s hakiranjem. Obje su zemlje sudjelovale i u nezakonitom izvozu softvera Predator sudanskoj paravojnoj postrojbi Snage za brzu potporu[390]. Grčka je izdala izvoznu dozvolu, dok je materijal otpremljen u Sudan iz zračne luke Larnaca[391].

243. Osim što omogućuje izvoz špijunskog softvera izvan EU-a, Cipar omogućuje i trgovanje podsustavima i tehnologijama špijunskog softvera s državama članicama. Poduzeće UTX Technologies, koje je registrirano u Cipru i koje je kupio izraelski tehnološki div Verint, pojavljuje se na računima zajedno s njemačkim, francuskim i poljskim poduzećima za otpremanje tehnologije Gi2 i sustava nadzora[392].

244. Na papiru postoji pravni okvir kojim se uređuje zaštita privatnih komunikacija, obrada osobnih podataka i pravo pojedinca na informiranje. Međutim, u slučaju pozivanja na nacionalnu sigurnost u praksi ne postoje jasno određena pravila kojima se uređuje uporaba uređaja za presretanje i zaštita ustavnih prava građana.

PRAVNI OKVIR

UREDBA O ROBI S DVOJNOM NAMJENOM

245. Čini se da Cipar blisko surađuje s Izraelom u području tehnologija nadzora. Cipar se savjetovao s Izraelom i SAD-om o reformi svojeg pravnog okvira i sustava za kontrolu izvoza robe s dvojnom namjenom. Cipar je popularno odredište brojnih izraelskih poduzeća koja se bave špijunskim softverom.

246. Odjel za dozvole za izvoz strateške robe Ministarstva energetike, trgovine i industrije regulira izvoz robe s dvojnom namjenom[393]. U odgovoru na upitnik koji je odbor PEGA dostavio svim državama članicama, Cipar je izjavio da sve zahtjeve za izvoznom dozvolom za robu s dvojnom namjenom nadzire i ocjenjuje pojedinačno u potpunosti u skladu s relevantnim režimima sankcija. Ti su režimi sankcija globalni režim sankcija EU-a u području ljudskih prava kao i Uredba EU-a o robi s dvojnom namjenom, koji se vode kriterijima iz relevantnog Zajedničkog stajališta vijeća (2008/944/CFSP)[394]. Odbor PEGA primjećuje da Cipar nije potpisnik Sporazuma iz Wassenaara o kontroli izvoza konvencionalnog oružja te robe i tehnologije dvojne namjene. Za vrijeme misije odbora PEGA navedeno je da je Turska blokirala članstvo Cipra u tom sporazumu. Međutim, ciparska Vlada izjavljuje da se pridržava istih standarda.

247. Ministarstvo energetike, trgovine i industrije može se savjetovati s takozvanim savjetodavnim odborom u vezi s odobravanjem izvozne dozvole. Taj se odbor sastoji od predstavnika Ministarstva obrane, Ministarstva pravosuđa i javnog reda i Ministarstva vanjskih poslova te Odjela za carinu i trošarine i drugih odjela[395]. Ciparska vlada tvrdi da se redovito savjetuje s tim Odborom pri razmatranju zahtjeva za izvoz. Izvoz robe s dvojnom namjenom u treće zemlje nekoliko je puta odbijen zbog negativnog mišljenja

[390] LightHouse Reports. Flight of the Predator (Let Predatora).
[391] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/.
[392] Philenews. Cyprus is a pioneer in software exports (documents) (Cipar je predvodnik u izvozu softvera, dokumenti).
[393] http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument.
[394] Odgovor Cipra na upitnik Europskog parlamenta.
[395] Lelaw, „Export Controls for dual-use products" (Kontrola izvoza proizvoda s dvojnom namjenom).

Odbora[396]. Gospodarska komora obično ne pruža informacije o broju odobrenih i odbijenih dozvola za stavljanje softvera na tržište[397].

248. Za vrijeme misije odbora PEGA u Cipru 1. i 2. studenoga 2022. sudionici misije sastali su se s Ministarstvom energetike, trgovine i industrije te zamjenikom ministra za istraživanja, inovacije i digitalnu politiku. Na sastanku su ministri Natasa Pilides i Kyriacos Kokkinos izjavili su da je broj aktivnih poduzeća koji se bave špijunskim softverom u Cipru naglo pao. Registrirana su 32 poduzeća, no ministar navodi da ih je u trenutku posjeta bilo aktivno samo 8 do 10, pri čemu samo tri ili četiri proizvode špijunski softver[398]. Međutim, priznali su i da se suočavaju s tehničkim poteškoćama pri nadziranju i kontroli trgovačkih društava sa sjedištem u Cipru koja neovisno prodaju pojedinačne špijunske softvere.

249. Cipar je u praksi navodno prilično popustljiv pri izdavanju izvoznih dozvola poduzećima koja proizvode špijunski softver[399]. Poduzeća upotrebljavaju tehnike kojima zaobilaze pravila i šalju fizički hardver proizvoda u zemlju primateljicu bez ugrađenog softvera[400]. Nakon toga se u zemlju primateljicu na odvojenom USB uređaju za pohranu podataka šalje aktivacijski softver (koji se naziva i „licencni ključ”)[401]. Drugi je način da se navodi da se proizvod izvozi isključivo u demonstracijske svrhe iako se prilaže detaljan opis proizvoda[402]. Osim toga, u obrascu za izvoz radi dobivanja izvozne dozvole navodi se nejasan opis špijunskog softvera, što onemogućuje odgovarajuće carinske provjere.

250. Nekoliko je ciparskih poduzeća navodno pribavilo izvozne dozvole za prodaju „robe s dvojnom namjenom” zemljama koje nisu članice EU-a. Ta su poduzeća UTX Technologies, Coralco Tech, Prelysis i Passitora[403].

251. UTX Technologies bio je uključen u prodaju špijunskog softvera državama članicama Eu-a, ali i zemljama nečlanicama. Između 2013. i 2014. UTX je spomenut na računima njemačkih (Syborg Informationsysteme), francuskih (COFREXPORT) i poljskih (Verint) poduzeća za trgovanje sustavima nadzora i tehnologijom Gi2[404].

252. Ciparska služba za trgovinu omogućila je podružnici poduzeća Cognyte, poduzeću UTX

---

[396] Odgovor Cipra na upitnik Europskog parlamenta.
[397] Inside Story, „Who signs the exports of spyware from Greece and Cyprus?” (Tko potpisuje izvozne dozvole za špijunski softver iz Grčke i Cipra?).
[398] Sastanak s gđom Natasom Pilides, ministricom energetike, trgovine i industrije, i Kyriacosom Kokkinosom, zamjenikom ministra za istraživanja, inovacije i digitalnu politiku u vrijeme misije odbora PEGA 2. studenoga 2022.
[399] InsideStory, „Who signs the exports of spyware from Greece and Cyprus?” (Tko potpisuje izvozne dozvole za špijunski softver iz Grčke i Cipra?).
[400] InsideStory, „Who signs the exports of spyware from Greece and Cyprus?” (Tko potpisuje izvozne dozvole za špijunski softver iz Grčke i Cipra?).
[401] Philenews, „This is how interception patents are exported from Cyprus” (Kako se patenti za presretanje izvoze iz Cipra)
[402] Philenews, „Export of monitoring software confirmed” (Potvrđen izvoz softvera za praćenje).
[403] Philenews, „Cyprus is a pioneer in software exports (documents)” (Cipar pionir u izvozu softvera (dokumenti)); Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record” (Izraelska špijunska tehnologija prodana Bangladešu usprkos izrazito lošem stanju u pogledu ljudskih prava).
[404] Philenews, „Cyprus is a pioneer in software exports (documents)” (Cipar je predvodnik u izvozu softvera, dokumenti).

Technologies, privremene izvozne dozvole za prodaju softvera za nadzor Meksiku, Ujedinjenim Arapskim Emiratima, Nigeriji, Izraelu, Peruu, Kolumbiji, Brazilu i Južnoj Koreji[405]. UTX Technologies navodno je imao i ugovor s Tajlandom za prodaju podsustava nadzora za 3 milijuna USD. U opisu tih podsustava spominjala se i vrsta s „dvojnom namjenom" i „algoritmom za analizu govora" te „metapodataka i glasa". U ugovoru je bilo posebno spomenuto i poduzeće iz Litve. S obzirom na to da ciparske vlasti nisu htjele izdati izvoznu dozvolu, nadležnost Ministarstva energetike, trgovine i industrije mogla se zaobići posredstvom poduzeća UAB Communication Technologies koje je registrirano u Litvi[406]. Rusko-izraelski građanin Anatoly Hurgin vlasnik je tog poduzeća i usto ima malteško putovnicu[407]. Osim toga, UTX je 2019. osigurao ugovor s Bangdalešom za internetski obavještajni sustav vrijedan 2 milijuna USD, a 2021. za sustav za praćenje mobilnih telefona vrijedan 500 000 USD[408].

253. Povijest izvoza iz Cipra pokazuje i da je poduzeće Coralco Tech, koje je izvorno iz Singapura, ali je registrirano i u Izraelu i u Nikoziji, poslalo opremu za nadzor u vrijednosti 1,6 milijuna USD bangladeškoj vojsci nakon natječajnog postupka u 2018. Vlasnik poduzeća Coralco Tech je Izraelac Eyal Almog[409].

254. Unutarnja obavještajna agencija Bangdaleša (NSI) kupila je 2019. softver za presretanje Wi-Fi-ja za ukupno 3 milijuna USD od poduzeća Prelysis (registriranog u Cipru). Kobi Naveh, osnivač i direktor tvrtke Prelysis, radio je za izraelsku tvrtku Verint do 2014. Verint je tvrtka koja je kupila tvrtku UTX Technologies registriranu u Cipru[410].

255. U ljeto 2021. Bangladeš je od poduzeća Passitora (prethodno WiSpear) vlasnika Tala Diliana dodatno kupio i špijunsko vozilo. Švicarsko poduzeće Toru Group Limited, registrirano na Britanskim Djevičanskim Otocima, bilo je posrednik za ugovore s Dilianovim poduzećem Passitora[411].

256. Dana 4. listopada 2022. otkriveno je da je nizozemsko Ministarstvo obrane u studenome 2019. namjeravalo potpisati ugovor s WiSpearom, poduzećem u vlasništvu Tala Diliana, koje je prije toga preuzelo Cytrox, proizvođača špijunskog softvera Predator[412]. Prema medijskim izvješćima i izjavama predsjednika stranke DISY (Dimokratikós Sinagermós) poduzeće WiSpear poslalo je e-poštu vladajućoj stranci DISY i Ministarstvu energetike, trgovine i industrije u kojoj moli za pomoć u provedbi ugovora s nizozemskim Ministarstvom obrane[413]. Nije poznato je li taj ugovor potpisan i je li nizozemskom Ministarstvu obrane isporučen bilo kakav špijunski softver.

---

[405] Philenews, „Cyprus is a pioneer in software exports (documents)" (Cipar je predvodnik u izvozu softvera, dokumenti).
[406] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
[407] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
[408] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record" (Izraelska špijunska tehnologija prodana Bangladešu usprkos izrazito lošem stanju u pogledu ljudskih prava)
[409] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record" (Izraelska špijunska tehnologija prodana Bangladešu usprkos izrazito lošem stanju u pogledu ljudskih prava)
[410] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record" (Izraelska špijunska tehnologija prodana Bangladešu usprkos izrazito lošem stanju u pogledu ljudskih prava)
[411] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record" (Izraelska špijunska tehnologija prodana Bangladešu usprkos izrazito lošem stanju u pogledu ljudskih prava)
[412] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/.
[413] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/

257. Ti primjeri pokazuju da je industrija nadzora vrlo aktivna u Cipru i uključuje iste aktere koji su se pojavili u skandalu povezanom sa špijunskim softverom koje istražuje odbor PEGA.

258. Brojna izraelska poduzeća dolaze u Cipar kako bi ondje započela svoju djelatnost u Europi[414]. Osim toga, različiti izvori izvijestili su da u toj državi posluje oko 29 izraelskih poduzeća[415]. Neki izvori ukazuju na blisku vezu između trgovine špijunskim softverom i diplomatskih odnosa. Cipar je navodno omogućio licence izraelskim poduzećima i zauzvrat dobio neke od proizvoda koje ta poduzeća razvijaju i izvoze, kao što su špijunski softver Pegasus grupe NSO[416] i materijali povezani sa špijunskim softverom poduzeća WiSpear[417]. Cipar služi kao uporište za trgovanje izraelskim špijunskim softverom na unutarnjem tržištu EU-a te za izvoz špijunskog softvera u treće zemlje.

EX ANTE NADZOR

259. Zakonom 92(I)/1996 o zaštiti povjerljivosti privatnih komunikacija utvrđuje se da glavni državni odvjetnik Sudu može podnijeti zahtjev za izdavanje sudskog naloga kojim se autoriziranoj osobi odobrava ili produljuje presretanje privatnih komunikacija. Za taj zahtjev glavnog državnog odvjetnika Sudu potreban je pismeni zahtjev ravnatelja policije, zapovjednika ciparske obavještajne službe ili istražnog suca. Međutim, odredbe o odobrenju ili suglasnosti mogu se poništiti u slučajevima u kojima je presretanje privatnih komunikacija od sigurnosnih interesa Cipra ili kako bi se kaznena djela spriječila, istražila ili kazneno progonila[418].

260. Nakon podnošenja zahtjeva, ravnatelj policije, u dogovoru sa zamjenikom ravnatelja policije i zapovjednikom ciparske obavještajne službe, daje zaposlenicima svoje službe ili zaposlenicima koji izvršavaju zadatke za službu pismeno odobrenje za presretanje privatnih komunikacija i/ili pristup opremi za nadzor radi tehničkog rada[419].

261. Usto, člankom 4. stavkom 2. Zakona 92(I)/1996 kako je izmijenjen 2020.[420] utvrđuje se da ako je uređaj ili stroj prvenstveno osmišljen, proizveden ili prilagođen radi omogućavanja ili pojednostavljivanja presretanja ili nadzora privatne komunikacije, nikome nije dopušteno uvoziti, proizvoditi, oglašavati, prodavati ili na bilo koji drugi način distribuirati takve uređaje ili strojeve. Kršenje tog članka može dovesti do novčane kazne od 50 000 EUR ili do pet godina zatvora[421]. Te odredbe se ne primjenjuju ako je dobavljač o tome obavijestio središnju obavještajnu službu (KYP), policiju i povjerenika te dobio njihovo odobrenje. Te se odredbe ne primjenjuju ni na

---

[414] Philenews. Revelations in Greece: Predator came from Cyprus (Otkrića u Grčkoj: Predator je došao iz Cipra).
[415] Makarios Drousiotis. Κράτος Μαφία. Poglavlje 6. Objavljeno 2022.
[416] Makarios Drousiotis. Κράτος Μαφία. Poglavlje 6. Objavljeno 2022.
[417] Inside Story, „Predator: the 'spy' who came from Cyprus'." (Predator: „špijun" koji je došao iz Cipra).
[418] CyLaw, Zakon o zaštiti povjerljivosti privatnih komunikacija (presretanje i pristup snimljenom sadržaju privatnih komunikacija) 1996 (92(I)/1996).
[419] CyLaw, Zakon o zaštiti povjerljivosti privatnih komunikacija (presretanje i pristup snimljenom sadržaju privatnih komunikacija) 1996 (92(I)/1996).
[420] CyLaw. E.U. Stavak J(J) zakona 13(J)/2020.
[421] Odgovor Cipra na upitnik Europskog parlamenta.

sustave nadzora koje upotrebljava ravnatelj policije i zapovjednik KYP-a[422].

EX POST NADZOR

262. U Cipru je Zakonom o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka iz 2018. uređeno da ako se upotrebljavaju osobni podaci ili ako je pojedinac predmet obrade, dotični pojedinac ima pravo da ga se o tome obavijesti[423]. To se pravo može zaobići ako povjerenik za zaštitu osobnih podataka odluči drukčije primjerice zbog razloga nacionalne sigurnosti[424].

263. Nadalje, u Zakonu o zaštiti povjerljivosti privatnih komunikacija donesenom 1996. navodi se da je u slučaju da agencije kaznenog progona presreću privatne komunikacije, glavni državni odvjetnik obvezan o tome obavijestiti dotičnog pojedinca. Pojedinac mora biti obaviješten najkasnije 90 dana od početnog datuma sudskog naloga[425] ili najkasnije 30 dana od izvršavanja tog sudskog naloga. Glavni državni odvjetnik dotičnom pojedincu mora dostaviti izvješće s detaljima izdavanja sudskog naloga, datumom izdavanja sudskog naloga i činjenicom da je u tom razdoblju došlo do presretanja privatnih komunikacija ili pristupanja njima. Ta se obveza može privremeno odgoditi ako glavni državni odvjetnik odluči da je, među ostalim, uskraćivanje tih informacija u sigurnosnom interesu Cipra[426]. Isto tako, Sud može zahtijevati neotkrivanje informacija zbog sigurnosnih interesa Cipra[427].

264. Povreda zaštite privatnih komunikacija je de iure kazneno djelo. De facto se ta nezakonitost često prikriva pozivanjem na nacionalnu sigurnost[428]. Ne postoji zakonodavstvo kojim bi se regulirao način na koji se policija ili druge obavještajne službe služe uređajima za presretanje, kao niti tko regulira postupke presretanja i na koji se način jamči zaštita ustavnih prava građana. Mjerodavni propisi i protokoli trenutačno čekaju raspravu i odobrenje Zastupničkog doma. Zasad se ta aktivnost nastavlja bez kontrole[429].

PRAVNA ZAŠTITA

265. Zakonitost djelovanja ciparske obavještajne službe ocjenjuje tročlani odbor kako je utvrđeno u Zakonu 74(I)/2016 o ciparskoj obavještajnoj službi. Tripartitni odbor

---

[422]Odgovor Cipra na upitnik Europskog parlamenta.
[423] Zakon 125(I) iz 2018. https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf.
[424] Agencija Europske unije za temeljna prava, Nadzor koji provode obavještajne službe: Nadzor koji provode obavještajne službe: mjere zaštite temeljnih prava i pravni lijekovi u EU-u) – svezak II. Perspektive s terena i pravne novosti.
[425] CyLaw, Zakon o zaštiti povjerljivosti privatnih komunikacija (presretanje i pristup snimljenom sadržaju privatnih komunikacija) 1996 (92(I)/1996).
[426] Agencija Europske unije za temeljna prava, Nadzor koji provode obavještajne službe: Nadzor koji provode obavještajne službe: mjere zaštite temeljnih prava i pravni lijekovi u EU-u) – svezak II. Perspektive s terena i pravne novosti.
[427] CyLaw, Zakon o zaštiti povjerljivosti privatnih komunikacija (presretanje i pristup snimljenom sadržaju privatnih komunikacija) 1996 (92(I)/1996).
[428] Makarios Drousiotis, „Κράτος Μαφία", poglavlje 6., 2022.
[429] Philenews. „Legal but uncontrolled interceptions" (Legalna, ali nekontrolirana presretanja)

imenuje Vijeće ministara na temelju preporuke Predsjednika Republike[430].

266. Zakon 92(I)/1996 izmijenjen je 2020., čime se ojačao nadzorni okvir Republike, posebno u pogledu odredaba o Tripartitnom odboru. U okviru svojih ovlasti Odbor može pokrenuti *ex officio* istrage te istrage prostora, tehničke opreme i arhiviranih materijala KYP-a. Kako je navedeno u članku 17.A stavku 1. Zakona 92(I)/1996 i kako je izmijenjeno Zakonom 13(I)/2020, Odbor može pokrenuti istrage prostora, tehničke opreme i arhiviranog materijala policije. S obzirom na takve istrage, Odbor može proslijediti predmet glavnom državnom odvjetniku, povjereniku za zaštitu osobnih podataka ili povjereniku za elektroničke komunikacije i regulaciju poštanskih usluga radi daljnjeg djelovanja. Odbor Predsjedniku Republike dostavlja i godišnje izvješće, u kojemu opisuje svoje aktivnosti, iznosi zapažanja i preporuke te utvrđuje propuste[431].

267. Ciparski predsjednik ima značajan utjecaj na sastav odbora koji može pokrenuti kritičke istrage o djelovanju KYP-a. Osim toga, godišnja izvješća o nalazima tog odbora prvo se šalju predsjedniku[432]. U vrijeme izrade ovog dokumenta nema informacija o točom sastavu odbora, njegovu radu ni nadzoru koji obavlja[433].

KLJUČNE OSOBE U INDUSTRIJI ŠPIJUNSKOG SOFTVERA

268. Tal Dilian imao je ključnu ulogu u brojnim događajima u Cipru i Grčkoj. Stekao je malteško državljanstvo 2017.[434] Tal Dilian obnašao je razne vodeće položaje u izraelskim obrambenim snagama 25 godina dok se nije povukao u mirovinu iz vojske 2002.[435] Započeo je karijeru „obavještajnog stručnjaka, graditelja zajednice i serijskog poduzetnika" u Cipru, a zatim je pokrenuo poduzeće Aveledo Ltd., koje će kasnije postati poznato pod nazivom Ws WiSpear Systems Ltd., a nakon toga kaoPassitora Ltd[436].

269. Dilian je u Cipru uspostavio bliske veze s Abrahamom Sahakom Avnijem. Avni je nekad radio za posebne snage izraelske policije kao posebni detektiv[437]. U studenome 2015. stekao je ciparsko državljanstvo i zlatnu putovnicu uloživši 2,9 milijuna EUR u nekretnine[438]. Avni je osnovao NCIS Intelligence Services Ltd.[439], ciparsko poduzeće koje je navodno surađivalo s najmoćnijim tehnološkim poduzećima na svijetu[440]. Poduzeće NCIS Intelligence and Security Services isporučilo je sigurnosni softver stožeru policije između 2014. i 2015. te je obučavalo zaposlenike Ureda za analizu kaznenih djela i statistiku između 2015. i 2016.[441]. Među klijentima tog

---

[430] Odgovor Cipra na upitnik Europskog parlamenta.
[431] Odgovor Cipra na upitnik Europskog parlamenta; CyLaw. E.U. Stavak J(J) zakona 13(J)/2020.
[432] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[433] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[434] Malteška Vlada. Registar naturaliziranih osoba, Gaz 21.12
https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf.
[435] https://taldilian.com/about/.
[436] Opencorporates, Passitora ltd.
[437] ShahakAvni. O Shahaku Avniju.
[438] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[439] Philenews, „FILE: The state insulted Avni and Dilian" (Predmet: Država je uvrijedila Avnija i Diliana).
[440] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[441] Philenews, „FILE: The state insulted Avni and Dilian" (Predmet: Država je uvrijedila Avnija i Diliana).

poduzeća je i vladajuća stranka DISY. Avni je navodno instalirao sigurnosnu opremu u uredima stranke[442]. Uz Avnijevu sigurnosnu opremu, Dilianovi materijali prodani su ciparskoj agenciji za suzbijanje droga i ciparskoj policiji[443].

270. U nekom je trenutku stožer odjela policije za kriminalističke istrage pronašao povrede povjerljivosti privatnih komunikacija povezanih s Avnijevim poduzećem. Policija je odlučila zatvoriti slučaj[444].

271. Između Diliana i Avnija postoje brojne veze. Dilianovo poduzeće WiSpear dijelilo je s Avnijem zgradu u Lacarni i dio osoblja[445]. Njih su dvojica 2018. pokrenula poduzeće Poltrex, koje je kasnije preimenovano u Alchemycorp Ltd. Poltrex ima urede u zgradi Novel Tower, u kojoj se nalazi i Avni[446], a Poltrex je usto i dio grupacije Intellexa Alliance. Dilian je navodno zahvaljujući Avnijevim odnosima sa strankom DISY imao testni poligon za svoje proizvode[447].

DILIANOV KOMBI SA ŠPIJUNSKIM SOFTVEROM

272. Nakon prodaje poduzeća Circles Technologies i osnivanja WiSpeara Tal Dilian je 2019. pokrenuo i poduzeće Intellexa Alliance, koje je na vlastitoj mrežnoj stranici opisano kao poduzeće sa sjedištem u EU-u i usklađeno sa zakonima EU-a čija je svrha razvoj i integracija tehnologija koje osnažuju obavještajne agencije[448]. Pod nazivom Intellexa Alliance posluju različiti dobavljači proizvoda za nadzor kao što su Cytrox, WiSpear (kasnije preimenovan u Passitora Ltd.), Nexa Technologies i Poltrex Ltd. Ti različiti dobavljači koji djeluju unutar Dilianove grupacije omogućuju Intellexi da svojim klijentima ponudi širok raspon softvera za nadzor i usluga nadzora te njihovih kombinacija[449]. Detaljnije informacije o toj korporativnoj strukturi nalaze se u poglavlju o industriji špijunskog softvera.

273. Dilian je 5. kolovoza 2019. dao intervju za časopis Forbes o crnom kombiju poduzeća WiSpear i pohvalio se različitim mogućnostima špijunskog softvera koji njegova grupacija nudi. Kombijem u vrijednosti od 9 milijuna EUR moglo se hakirati uređaje u radijusu od 500 metara[450]. Pozornost javnosti koju je privukao intervju s časopisom Forbes[451] dovela je do toga da su ciparske vlasti pokrenule istragu. Odvjetnik Elias Stefanou imenovan je neovisnim istražiteljem kaznenog djela za tu istragu. U toj su istrazi vlasti otkrile još jedno Dilianovo poduzeće koje je poslovalo iz međunarodne

[442] Tovima, „The unknown ‘bridge’ between Greece and Cyprus for the eavesdropping system” (Nepoznati „most” između Grčke i Cipra za sustav prisluškivanja).
[443] Inside Story, „Predator:the ‘spy’ who came from Cyprus” (Predator: „špijun” koji je došao iz Cipra).
[444] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[445] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[446] CyprusMail, „Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal” (Akel tvrdi da je pronašao nepobitni dokaz koji povezuje Cipar s grčkim skandalom špijuniranja).
[447] Inside Story, „Predator:the ‘spy’ who came from Cyprus” (Predator: „špijun” koji je došao iz Cipra).
[448] https://intellexa.com/.
[449] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire” (Dok Izrael smanjuje svoju industriju kiberoružja, bivši obavještajac gradi novo carstvo).
[450] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire” (Dok Izrael smanjuje svoju industriju kiberoružja, bivši obavještajac gradi novo carstvo).
[451] Forbes, „A Multimillionaire Surveillance Dealer Steps Out Of The Shadows ... And His $9 Million Whatsapp Hacking Van” (Multimilijunaš dobavljač proizvoda za nadzor izlazi iz sjene ... kao i njegov kombi za hakiranje Whatsappa vrijedan 9 milijuna USD)

zračne luke Larnaca[452].

274. Tal Dilian je 16. lipnja 2019. navodno sklopio izvanugovorni dogovor sa zračnim lukama Hermes za upotrebu njegove opreme WiSpear radi navodnog poboljšanja Wi-Fi signala za putnike međunarodne zračne luke Larnaca, nakon čega su postavljene tri antene za Wi-Fi[453]. Iako nije registrirano na Cipru, i izraelsko poduzeće Go Networks bilo je uključeno u pregovorima koji su prethodili dogovoru[454]. Pravi razlog dogovora bio je, međutim, ispitivanje tehnologije za presretanje poduzeća WiSpear. Presretani podaci putnika spremali su se na poslužitelje u sobi zračne luke za poslužitelje, koja se nalazi blizu ureda poduzeća WiSpear u međunarodnoj zračnoj luci Larnaca koji dijeli s Avnijem[455]. U vremenskom razdoblju u kojem su antene bile u pogonu, presretani podaci preuzeti su s 9 507 429 mobilnih uređaja[456].

275. Nakon pritužbi podnesenih protiv Diliana izraelsko poduzeće Go Networks navodno je povezano s Intellexom putem zajedničkog korporativnog vlasništva u Irskoj. Bivši višerangirani predstavnici izraelskog poduzeća Go Networks navodno su postavljeni na najviše položaje u Intellexi[457]. Osim toga, policijskom istragom utvrđeno je da su WiSpearu izdane izvozne dozvole za „opremu za presretanje namijenjenu izdvajanju glasa ili podataka koji se prenose radiosučeljem”[458] [459]. Kao što je izjavila gospodarska komora, Dilianova poduzeća nisu dobila izvozne dozvole u zadnje dvije godine. U vrijeme izrade ovog dokumenta nije poznato tko je odobrio te izvozne dozvole[460].

276. Elektronički podaci izdvojeni iz zaplijenjene opreme u okviru istrage dostavljeni su na forenzično ispitivanje na tri razine, koje su proveli policija, akademski stručnjak i Europol[461]. Kombi je zadržan u policiji, ali nije jasno što se dogodilo s opremom za nadzor. Navodno je vraćena Dilianu, ali čini se da za to ne postoji potvrda.

277. Predmet protiv WS WiSpear Systems Ltd. pokrenut je 15. studenoga 2021. pred kaznenim sudom, a optuženici su bili Tal Dilian i druga dva zaposlenika poduzeća WiSpear. U konačnici, glavni državni odvjetnik George Savvides prihvatio je predmet protiv poduzeća WiSpear, ali kazneni postupci protiv Diliana i zaposlenika su odbačeni[462]. Razlozi za tu odluku su tajni. Međutim, glavni državni odvjetnik mogao je u bilo kojem trenutku odlučiti ponovno otvoriti predmet protiv tri pojedinca.

---

[452] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire” (Dok Izrael obuzdava svoju industriju kibernetičkog oružja, bivši obavještajni časnik gradi novo carstvo).
[453] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire” (Dok Izrael obuzdava svoju industriju kibernetičkog oružja, bivši obavještajni časnik gradi novo carstvo).
[454] Makarios Drousiotis, „Κράτος Μαφία”, poglavlje 6., 2022.
[455] Makarios Drousiotis, „Κράτος Μαφία”, poglavlje 6., 2022.
[456] Makarios Drousiotis, „Κράτος Μαφία”, poglavlje 6., 2022.
[457] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire (Dok Izrael smanjuje svoju industriju kiberoružja, bivši obavještajac gradi novo carstvo).
[458] Makarios Drousiotis. Κράτος Μαφία. Poglavlje 6. Objavljeno 2022.
[459] Philenews. Export of tracking software from Cyprus (Izvoz softvera za praćenje iz Cipra).
[460] Inside Story, „Who signs the exports of spyware from Greece and Cyprus?” (Tko potpisuje izvozne dozvole za špijunski softver iz Grčke i Cipra?).
[461] Priopćenje za medije zamjenika glavnog državnog odvjetnika od 10. kolovoza 2022. pribavljeno tijekom misije odbora PEGA u Cipru 2. studenoga 2022.
[462] Financial Mirror, „Anger after ‘spy van’ charges dropped” (Ljutnja nakon odustajanja od kaznenog progona za „špijunski kombi”)

278. Poduzeće WiSpear priznalo je krivnju za 42 optužbe i dobilo novčanu kaznu od 76 000 EUR na sudu za teža kaznena djela 22. veljače 2022.[463] Poduzeće WiSpear priznalo je optužbe nezakonitog nadzora privatnih komunikacija i kršenje zaštite podataka[464]. Sud je objavio konačnu odluku i naveo sljedeće: „Sud za teška kaznena djela napomenuo je i odredio da povreda koja se pripisuje poduzeću nije uključivala namjeru, hakiranje [ili] prisluškivanje i izjavljuje da nikad nije bilo pokušaja ili potrebe za personalizacijom podataka. Sud je naglasio da nikakva šteta nije prouzročena ni jednom pojedincu.”[465]. Uz novčanu kaznu koju je izrekao sud za teška kaznena djela, povjerenica za zaštitu osobnih podataka Irini Loizidou Nicolaidou poduzeću WiSpear izrekla je novčanu kaznu od 925 000 EUR zbog kršenja Opće uredbe o zaštiti podataka[466]. Iako je navedeno da je epizoda s crnim kombijem povezana s pitanjima od nacionalnog interesa i kritične infrastrukture, kazne za počinitelje bile su vrlo blage. Ovaj incident možda ima politički značaj koji nadilazi kršenje privatnosti putnika. S obzirom na to da se Cipar na više načina nalazi na sjecištu puteva, postoji nekoliko zemalja koje nisu članice EU-a koje bi potencijalno moglo zanimati posjedovanje uvida u kretanje putnika kroz zračnu luku Larnaka, a te su zemlje primjerice Turska, Izrael, Rusija i SAD.

279. Oporbena stranka AKEL izrazila je ogorčenje zbog odbacivanja predmeta protiv Diliana i njegova osoblja te je glavnog državnog odvjetnika zbog te odluke optužila za pokušaj zataškavanja[467]. Na kraju krajeva, ciparska vlada navodno je kupila opremu od Dilianova poduzeća, a jedan od optuženih zaposlenika navodno je radio za NSO te obučavao KYP za upotrebu špijunskog softvera Pegasus[468]. Odbacivanjem optužbi zajamčeno je da će informacije o vezama između Dilianova poduzeća i ciparske Vlade ostati zaštićene[469]. Glavni državni odvjetnik odbio je predati zaključke istrage iako je to od njega zatražio odbor PEGA tijekom svoje službene misije u Cipru. Taj primjer pokazuje da prava pojedinaca na zaštitu od kršenja privatnosti njihovih osobnih podataka opremom za masovni nadzor nisu u potpunosti zajamčena. Iako pravni lijek postoji na papiru, na ishode sudskih postupaka mogu utjecati vladine intervencije, zbog čega su pojedinačne žrtve nezaštićene. Istragom se dodatno pokazalo da Cipar omogućuje poduzećima sa sjedištem u Cipru da provode pokuse s opremom za nadzor.

PRESELJENJE U GRČKU

280. Nakon epizode s kombijem i tužbom, g. Dilian premjestio je poslovanje Intellexe u

[463] Makarios Drousiotis, „Κράτος Μαφία”, poglavlje 6., 2022.; Priopćenje za medije zamjenika glavnog državnog odvjetnika od 10. kolovoza 2022. pribavljeno tijekom misije odbora PEGA u Cipru 2. studenoga 2022.
[464] Financial Mirror, „Spy van company fined €76,000” (Proizvođač špijunskog kombija kažnjen novčanom kaznom od 76 000 funti).
[465] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire” (Dok Izrael obuzdava svoju industriju kibernetičkog oružja, bivši obavještajni časnik gradi novo carstvo).
[466] CyprusMail. Israeli company that deployed ‘spy van’ fined €925,000 for data violations (Izraelsko poduzeće koje je stavilo na tržište „špijunski kombi” dobilo novčanu kaznu od 925 000 EUR zbog kršenja zakonodavstva o podacima); Financial Mirror, „Anger after ‘spy van’ charges dropped” (Ljutnja nakon odustajanja od kaznenog progona za „špijunski kombi”).
[467] Financial Mirror. Anger after ‘spy van’ charges dropped (Ljutnja nakon odustajanja od kaznenog progona za „špijunski kombi”).
[468] Makarios Drousiotis. Κράτος Μαφία.. Poglavlje 6. Objavljeno 2022.
[469] Makarios Drousiotis. Κράτος Μαφία. Poglavlje 6. Objavljeno 2022.

Grčku, iako sam nije napustio Cipar. Navodno se planira vratiti u Tel Aviv[470]. Neizravne veze među nekoliko fizičkih i pravnih osoba registriranih u Cipru i Grčkoj otkrivaju da je poslovanje Dilianovih poduzeća premješteno u Atenu[471]. Slijede neka od imena koja su dio veza između Cipra i Grčke iako će se glavna uloga poduzeća Intellexa SA u Grčkoj dodatno objasniti u poglavlju o Grčkoj.

281. Sudske istrage dovele su do prijenosa aktivnosti g. Avnijna i g. Diliana u Poltrexu na Yarona Levgorena. G. Levgoren ima stalno boravište u Kanadi. Postao je dioničar kao i direktor i tajnik Poltrexa. Levgoren je isto tako povezan s poduzećem Intellexa u Grčkoj[472]. Prema njegovu profilu na LinkedInu trenutačno je predstavnik tvrtke Apollo Technologies, podružnice Intellexe s nastanom u Grčkoj.

PODUZEĆA KOJA PROIZVODE ŠPIJUNSKI SOFTVER I CIPAR

282. Uz poduzeće Intellexa Alliance, u Cipru je navodno poslovala i Grupa NSO. Tal Dilian je 2010. pokrenuo poduzeće Circles Technologies zajedno s Boazom Goldmanom i Ericom Banounom, specijalizirano za prodaju sustava koji iskorištavaju nedostatke mreža SS7[473]. Šest godina kasnije Circles Technologies prodan je poduzeću Francisco Partners za nešto manje od 130 milijuna USD, od čega je Dilianu išlo 21,5 milijuna USD. To privatno društvo za kapitalna ulaganja sa sjedištem u Kaliforniji na sličan je način steklo udio od 90 % u Grupi NSO, što je dovelo do spajanja poduzeća Circles Technologies i Grupe NSO u poduzeće L.E.G.D Company Ltd., koje se od 29. ožujka 2016. naziva Q Cyber Technologies Ltd.[474].

283. Prema odgovoru ciparske vlade odboru PEGA, u odjelu za registraciju poduzeća i intelektualnog vlasništva nije registriran pravni subjekt Grupe NSO. Grupa NSO nema dionice ni jednog pravnog subjekta na Cipru. Međutim, pojedinačni članovi uprave grupe NSO osnovali su ili kupili šest poduzeća. Usto, čini se da špijunski softver Pegasus nije razvijen u Cipru niti se službeno izvozi s Cipra[475].

284. Širenje u vlasništvu poduzeća Francisco Partners između 2014. i 2019. uključivalo je šest ciparskih poduzeća. Francisco Partners dopunjen je poduzećem ITOA Holdings Ltd., registriranim na Cipru i roditeljskim poduzećem poduzeća CS-Circles Solutions Ltd., Global Hubcom Ltd., te poduzećem MS Magnet Solutions. Poduzeće MS Magnet Solutions vlasnik je poduzeća Mi Compass Ltd. Osim toga, poduzeće CS-Circles Solutions Ltd. vlasnik je poduzeća CI-Compass Ltd. Uz subjekte u Cipru, poduzeće CS-Circles Solutions Ltd. vlasnik je i subjekata u Bugarskoj. Grupa NSO izjavila je da „bugarska poduzeća na temelju ugovora pružaju usluge istraživanja i razvoja svojim dotičnim ciparskim podružnicama te izvoze mrežne proizvode za vladinu uporabu”[476].

---

[470] Intelligence Online, Israeli cyber tsar Tal Dilian plans Tel Aviv return (Izraelski kibermogul Tal Dilian planira povratak u Tel Aviv).

[471] *Haaretz*, As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire (Dok Izrael smanjuje svoju industriju kiberoružja, bivši obavještajac gradi novo carstvo).

[472] Philenews, How the spyware scandal in Greece is related to Cyprus. (Kako je skandal sa špijunskim softverom u Grčkoj povezan s Ciprom).

[473] Amnesty International, Operating from the Shadows (Poslovanje iz sjene).

[474] Amnesty International, Operating from the Shadows (Poslovanje iz sjene).

[475] Odgovor Cipra na upitnik Europskog parlamenta.

[476] Amnesty International, Operating from the Shadows (Poslovanje iz sjene).

285. Ciparska vlada poriče izvoz i razvoj softvera Pegasus. No, dužnosnik NSO-a Chaim Gelfad izjavio je 21. lipnja 2022. da se NSO-ova poduzeća u Cipru i Bugarskoj bave softverom koji pruža obavještajne usluge[477]. Prema dokumentu koji je oporbena stranka AKEL dostavila Europskom parlamentu, Grupa NSO navodno je izvezla špijunski softver Pegasus poduzeću u Ujedinjenim Arapskim Emiratima putem jedne od svojih podružnica na Cipru. Navodno je jedna od podružnica izdala fakturu na iznos od 7 milijuna USD za usluge pružene dotičnom poduzeću[478]. Međutim, te informacije nije moguće potvrditi.

286. U okviru Grupe NSO u Cipru je navodno također djelovalo poduzeće koje je navodno vodilo centar za usluge kupcima. Dužnosnici Grupe NSO sastali su se 2017. s kupcima iz Saudijske Arabije u hotelu Four Seasons u Limassolu. Na tom su im sastanku predstavili najnovije mogućnosti treće inačice špijunskog softvera Pegasus. Ta je verzija imala novu mogućnost da zarazi uređaj bez potrebe za klikanjem poveznice, na primjer putem propuštenog poziva u aplikaciji WhatsApp. Klijenti iz Saudijske Arabije odmah su kupili tu tehnologiju za iznos od 55 milijuna USD[479] [480]. Trebalo bi napomenuti da je godinu dana kasnije, 2. listopada 2018., saudijski režim ubio Jamala Khashoggija u saudijskim konzulatu u Turskoj nakon što su nadzirali njegove bližnje s pomoću Pegasusa. NSO niječe taj navod.

287. Prema Citizen Labu, 25 državnih aktera bili su 2020. klijenti poduzeća Circles Technologies. Među tim državnim akterima bili su Belgija, Danska, Estonija i Srbija[481]. Grupa NSO zatvorila je 2020. ured poduzeća Circles Technologies u Cipru. U vrijeme izrade ovog dokumenta nije poznato koje je od poduzeća Circles i dalje aktivno[482].

288. Izraelsko poduzeće QuaDream još je jedno poduzeće koje je navodno povezano s izvozom špijunskog softvera Reign iz Cipra. Mediji su u travnju 2023. izvijestili da poduzeće QuaDream zatvara svoje urede u Izraelu[483]. Proizvodi poduzeća QuaDream neizravno su se prodavali kupcima posredstvom poduzeća InReach, registriranog u Cipru od 2017., i tako izbjegavali izraelske kontrole izvoza. Ta su dva poduzeća u pravnom sporu koji je u tijeku[484].

289. Na položaju direktora i tajnika poduzeća InReach trenutačno je društvo A.I.L. Nominee Services Ltd. To je poduzeće već 2010. bilo registrirano u Cipru, a njegov dioničar osnivač bio je sadašnji zamjenik glavnog državnog odvjetnika Savvas Angelides[485]. G. Angelides prodao je svoje udjele u poduzeću A.I.L. Nominee Services Christosu

---

[477] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[478] Izvješće AKEL-a, misija odbora PEGA u Cipru.
[479] Makarios Drousiotis, Κράτος Μαφία, poglavlje 6., objavljeno 2022.
[480] Haaretz, Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals (Haaretz otkriva da je izraelsko kiberpoduzeće dogovorilo prodaju proizvoda s naprednim mogućnostima za napad sa Saudijcima).
[481] Citizen Lab. Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles (Kretanje u krug. Otkrivanje klijenata poduzeća za kibernetičko špijuniranje Circles).
[482] Amnesty International, Operating from the Shadows (Poslovanje iz sjene).
[483] https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadream-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000.
[484] Amnesty International, Operating from the Shadows (Poslovanje iz sjene).
[485] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://opencorporates.com/companies/cy/HE373827.

Ioannidesu 16. veljače 2018., nekoliko tjedana prije nego što je postao ministar obrane[486]. Međutim, A.I.L. Nominee Services i dalje je direktor i tajnik poduzeća InReach[487], što znači da posluje s poduzećem koje izvozi proizvode poduzeća QuaDream trećim zemljama.

290. Abraham Sahak Avni je 2011. osnovao poduzeće s Michaelom Angelidesom, bratom bivšeg ministra i aktualnog zamjenika glavnog državnog odvjetnika Savvasa Angelidesa. Njihovo poduzeće S9S registrirano je u Registru trgovačkih društava 10. studenoga 2011.[488] uz pomoć bivšeg odvjetničkog društva Savvasa Angelidesa[489]. Usto, A.I.L. Nominee Services Ltd. na položaju je tajnika poduzeća S9S. U tom razdoblju Savvas Angelides i dalje je glavni dionika poduzeća A.I.L. Nominee Services[490]. Međutim, partnerstvo između Michaela Angelidesa i g. Avnija prekinuto je 2012. Savvas Angelides postao je glavni državni odvjetnik 2020. i on je bio zadužen za istragu g. Avnija i g. Diliana u slučaju špijunskog kombija[491]. U priopćenju za medije od 10. kolovoza 2022. zamjenik glavnog državnog odvjetnika izjavio je da ni on ni bilo tko u njegovoj široj obitelji nema nikakve veze s Talom Dilianom. Kad je riječ o partnerstvu između Michaela Angelidesa i g. Avnija, naveo je da je „profesionalna suradnja bila neuspješna od samog početka uz činjenicu da poduzeće koje je registriralo njegovo bivše odvjetničko društvo na uputu njegova rođaka nikad nije aktivirano" te da stoga nikada nije stvaralo „prepreku njegovu sudjelovanju u odluci u predmetu o ‚crnom kombiju'"[492]. No u priopćenju za medije ne spominje se poduzeće A.I.L Nominee Services Ltd. Savvasa Angelidesa, koje je aktivirano u srpnju 2010.[493], ni uloga poduzeća kao tajnika u partnerstvu između njegova rođaka i g. Avnija u poduzeću S9S.

CRNA KOCKA

291. Black Cube je poduzeće u kojem su zaposleni bivši časnici izraelskih obavještajnih agencija kao što je Mosad. Poduzeće se služi operativcima s lažnim identitetima. Kako navodi časopis *New Yorker*, Shalev Hulio, bivši glavni izvršni direktor Grupe NSO, angažirao je Black Cube nakon što su troje odvjetnika, Mazen Masri, Alaa Mahajna i Christiana Markou, tužili NSO i jednu povezanu podružnicu u Izraelu i Cipru[494]. Tri su odvjetnika 2018. primila nekoliko poruka od takozvanih poznanika određenih poduzeća i pojedinaca koji su predlagali sastanke u Londonu. Hulio je izjavio da se „u tužbi u

[486] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.
[487] https://opencorporates.com/companies/cy/HE373827.
[488] Politis, „Interceptions" file: Classified Police Report (2016) shows he knew everything about Avni (Dosje „Presretanja": tajno policijsko izvješće (2016.) pokazuje da je znao sve o Avniju).
[489] Priopćenje za medije zamjenika glavnog državnog odvjetnika od 10. kolovoza 2022. pribavljeno tijekom misije odbora PEGA u Cipru 2. studenoga 10. kolovoza 2022.
[490] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://b2bhint.com/en/company/cy/s9s-ltd--%CE%97%CE%95%20296578; https://i-cyprus.com/company/433750.
[491] Izvješće Fanisa Makridisa, Misija odbora PEGA u Cipru 1. studenoga 2022.
[492] Priopćenje za medije zamjenika glavnog državnog odvjetnika od 10. kolovoza 2022. pribavljeno tijekom misije odbora PEGA u Cipru 2. studenoga 2022.
[493] https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=271194&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1.
[494] The New Yorker, How Democracies Spy on their Citizens (Kako demokracije špijuniraju svoje građane).

Cipru Black Cube jednom umiješao" jer je tužba „bila iznenadna i želi je razumjeti"[495]. Black Cube bio je izložen skandalima povezanima sa špijuniranjem u Mađarskoj i Rumunjskoj.

KUPNJA I UPORABA SOFTVERA OD STRANE CIPRA

292. Osim što je poduzećima koja se bave špijunskim softverom omogućila povoljnu izvoznu klimu, ciparska vlada i sama je kupovala takav softver. Također se navodno i sama koristila sustavima nadzora. U vrijeme izrade ovog dokumenta ostaje nejasno u kojim se slučajevima Cipar poslužio konvencionalnim metodama nadzora ili špijunskim softverom.

293. Nakon izbora 2013. Andreas Pentaras imenovan je za voditelja ciparske obavještajne službe, a stručnjak za nadzor Andreas Mikellis bio je odgovoran za zaštitu komunikacija predsjednika Anastasiadesa. Iste je godine g. Mikellis navodno posjetio sajam industrije nadzora ISS u Pragu, gdje je navodno pregovarao s poduzećem Hacking Team o kupnji takozvanog softvera DaVinci[496]. Softver DaVinci mogao je zaraziti aplikacije mobilnog telefona i stoga nije zadovoljio službene zahtjeve za ukidanjae privatnosti[497].

294. Kako je otkriveno WikiLeaksom, objavljene informacije o kontaktu Mikellisa i Hacking Teama upućivale su na zaobilaženje postupaka natječaja i nedostatak odgovarajućeg preispitivanja kupljenog sustava nadzora. Početkom 2014. softver je navodno instaliran i na osposobljavanju su bila četiri zaposlenika KYP-a, uključujući g. Mikellisa[498].

295. Kad je WikiLeaksom otkrivena kupnja Hacking Teamova softvera za nadzor, iz KYP-a je potvrđeno da se taj sustav upotrebljavao samo za nacionalne potrebe[499]. Unatoč kontaktu g. Mikellisa s Hacking Teamom[500], voditelj KYP-a Andreas Pentaras bio je taj koji je dao ostavku kad su ta otkrića isplivala na površinu[501]. G. Pentarasa zamijenio je Kyriakos Kouros.

296. Prema WikiLeaksu još je jednu policijsku upravu navodno zanimala kupnja sustava za nadzor komunikacija od Hacking Teama. Ta je policijska uprava pokušala osigurati taj sustav preko Sahaka Avnija[5021a]. Međutim, nije poznato o kojoj se policijskoj upravi radi**.**

META MAKARIOS DROUSIOTIS

297. Ciparska vlada navodno je špijunirala istraživačkog novinara Makariosa Drousiotisa od veljače 2018. upotrebom tehnika prisluškivanja i špijunskog softvera[503]. To je

[495] The New Yorker*,* How Democracies Spy on their Citizens (Kako demokracije špijuniraju svoje građane).
[496] Makarios Drousiotis, Κράτος Μαφία, poglavlje 6., objavljeno 2022.
[497] Inside Story*,* Predator: The 'spy' who came from Cyprus (Predator: „špijun" koji je došao iz Cipra).
[498] Makarios Drousiotis, Κράτος Μαφία, poglavlje 6., objavljeno 2022.
[499] Inside Story*,* Predator: The 'spy' who came from Cyprus (Predator: „špijun" koji je došao iz Cipra).
[500] Makarios Drousiotis, Κράτος Μαφία, poglavlje 6., objavljeno 2022.
[501] CyprusMail*,* Intelligence chief resigns after spy tech revelations (Šef obavještajne službe daje ostavku nakon otkrića o špijunskoj tehnologiji). https://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/.
[502] Inside Story, Predator: The 'spy' who came from Cyprus (Predator: „špijun" koji je došao iz Cipra).
[503] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/
184 Makarios Drousiotis, Κράτος Μαφία, poglavlje 5., obavljeno 2022.

špijuniranje navodno započelo dok je g. Drousiotis bio pomoćnik povjerenika EU-a za humanitarnu pomoć i upravljanje krizama, Cipranina Christosa Stylianidesa te je trajala tijekom njegove istrage financijskih veza između predsjednika Anastasiadesa i Rusa kao što je oligarh Dmitri Rybolovlev. Prema navodima g. Drousiotisa prvi pokušaj nadzora bio je potaknut njegovom potonjom ulogom[504].

298. Za vrijeme istrage ruskih veza koju je provodio g. Drousiotis, u međunarodnim medijskim izvorima počela su se pojavljivati otkrića da Grupa NSO posluje iz Cipra, uključujući otkriće o prezentaciji Pegasusa 3 u hotelima Four Seasons. Nadalje, CitizenLab je sumnjao da je Cipar jedna od zemalja koja upotrebljava tehnologije Grupe NSO radi presretanja komunikacija računalnih sustava britanskog Ministarstva vanjskih poslova[505]. Tad se g. Drousiotis počeo prisjećati nekoliko znakova da je njegov mobitel infiltriran špijunskim softverom Pegasus, uključujući propušteni poziv na WhatsAppu, brzo pražnjenje baterije i često pregrijavanje njegova uređaja iako ga nije upotrebljavao[506]. S obzirom na te događaje, g. Drousiotis smatra da se ciparska vlada, točnije ciparska obavještajna služba, nalazi iza zaraze njegova telefona.

299. U svibnju 2019. g. Drousiotis poslao je pismo predsjedniku Anastasiadesu u kojem izražava zabrinutost zbog nadzora njegova telefona i opisuje moguće razloge tog nadzora te da predsjednika smatra osobno odgovornim za sve što bi mu se moglo dogoditi nakon špijuniranja. G. Anastasiades proslijedio je pismo aktualnom voditelju ciparske obavještajne službe, Kyriakosu Kourosu. G. Anastasiades i g. Kouros opovrgnuli su navodno nadziranje softverom Pegasus i ponovili da Grupa NSO nije ni bila registrirana u Cipru[507].

300. U mjesecima koji su uslijedili dogodilo se nekoliko pokušaja zastrašivanja, uključujući nestanak dokaza s njegova računala, isključivanje sigurnosnih kamera u domu g. Drousiotisa i činjenicu da su ga pratile nepoznate osobe. Nakon što je sa svojom pričom izašao u javnost i podnio pritužbu ciparskoj policiji, g. Drousiotis kontaktirao je Lambrosa Katsonisa, voditelja odjela tehničke podrške poduzeća Panda Security, ciparskog poduzeća specijaliziranog za antivirusnu opremu. Međutim, g. Drousiotis nije znao da i ciparska vlada upotrebljava taj antivirusni softver za vlastite uređaje. Imajući to u vidu, čini se da je Katsonis poslan u dom g. Drousiotisa na prijevaru, možda bi kako bi dodatno infilltrirao uređaje g. Drousiotisa po nalogu KYP-a[508].

301. G. Drousiotis je 2019. postao svjestan sumnjivih ulazaka u njegov mobilni telefon sa sustavom Android te se javio podršci za korisnike Google One kako bi potvrdio prirodu tih ulazaka. Međutim, Google općenito ne odgovara na pitanja povezana s nadzorom i dotičnog je korisnika usmjerio na nacionalne agencije kaznenog progona.1a Iako nije imao povjerenja u policiju, g. Drousiotis pristao je predati svoje uređaje na forenzično ispitivanje[509].

---

[504] Makarios Drousiotis, Κράτος Μαφία, poglavlje 5., objavljeno 2022.
[505] BBC, No 10 network targeted with spyware, says group (Grupacija tvrdi da je mreža ureda premijera bila meta špijunskog softvera).
[506] Makarios Drousiotis, Κράτος Μαφία, poglavlje 5., objavljeno 2022.
[507] Makarios Drousiotis, Κράτος Μαφία, poglavlje 5., objavljeno 2022.
[508] Makarios Drousiotis. Κράτος Μαφία, poglavlje 5., objavljeno 2022.
[509] Makarios Drousiotis. Κράτος Μαφία, poglavlje 5., objavljeno 2022.

302. Na Cipru postoji snažan pravni okvir za zaštitu osobnih podataka i privatnosti, odobravanje nadzora i izvoz. Međutim, čini se da je u praksi pravila lako zaobići te da postoje bliske veze između političara, sigurnosnih agencija i industrije nadzora. Čini se da je upravo zbog blage primjene pravila Cipar tako atraktivno mjesto za trgovinu špijunskim softverom. Potrebna je bolja provedba postojećih pravila. Cipar je također mjesto od znatnog strateškog interesa za Rusiju, Tursku i SAD. Nadalje, čini se da su bliski odnosi s Izraelom posebno obostrano korisni u pogledu trgovine špijunskim softverom. Izvozne dozvole za špijunski softver postale su valuta u diplomatskim odnosima.

I.E Španjolska

303. Na poziv odbora PEGA španjolske vlasti prisustvovale su saslušanju 29. studenoga 2022. kako bi, u mjeri koju im omogućuju njihove pravne obveze, izvijestile o uporabi špijunskog softvera za nadzor u Španjolskoj. Zbog navedenih „pravnih ograničenja” odgovori dani odboru bili su ograničeni, a većina pitanja ostala je otvorena.

304. Odbor PEGA posjetio je Madrid u ožujku 2023. Delegacija se sastala s državnim tajnikom za europske poslove i osobama koje su prema Citizen Labu bile na meti špijunskog softvera, odnosno predsjednikom katalonske regionalne vlade, katalonskom regionalnom ministricom vanjske politike i članom gradskog vijeća Barcelone. Sastala se i s članovima Istražnog odbora katalonskog parlamenta za Pegasus, predstavnikom ureda ombudsmana, nevladinim organizacijama koje djeluju u području temeljnih prava i novinarima.

305. Otkrića koja je objavio Pegasus Project u srpnju 2021. pokazala su da je u Španjolskoj na meti tog softvera navodno bio velik broj osoba. Međutim, čini se da su bili mete različitih aktera i iz različitih razloga. U izvješću koje je dnevni list *The Guardian* objavio u svibnju 2022. navedeno je da je Maroko možda špijunirao više od 200 španjolskih mobilnih telefona. Španjolska je vlada potvrdila da su predsjednik vlade Pedro Sánchez, ministrica obrane Margarita Robles i ministar unutarnjih poslova Fernando Grande-Marlaska bili zaraženi špijunskim softverom Pegasus te da se ministar poljoprivrede Luis Planas našao na meti špijuniranja, ali nije bio zaražen[510]. Navedeno je i da je špijuniran i mobilni telefon tadašnje ministrice vanjskih poslova Aranche González Laya, ali nije bilo moguće utvrditi ni izvor kibernapada ni je li mobilni telefon bio ugrožen softverom Pegasus. Druga skupina žrtava bila je meta špijunskog softvera u aferi pod nazivom „CatalanGate”[511]. U toj su skupini katalonski zastupnici u parlamentu, zastupnici u Europskom parlamentu, odvjetnici, novinari, članovi organizacija civilnog društva, članovi akademske zajednice te članovi obitelji meta i s njima povezano osoblje[512], što se može nazvati „neizravnim” ili „relacijskim” ciljanjem.

[510] Le Monde, https://www.lemonde.fr/en/international/article/2022/05/10/spain-fires-head-of-intelligence-services-over-pegasus-phone-hacking_5982990_4.html, 10. svibnja 2022.
[511] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022.
[512] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18. travnja 2022.* str. 1.

Za skandal s nadzorom, prozvan „CatalanGate”, prvi se put doznalo 2020. nakon istrage koju su zajedno proveli dnevnici *The Guardian* i *El País*[513], ali su njegovi razmjeri postali poznati tek nakon što je Citizen Lab u travnju 2022. dovršio svoju dubinsku istragu. Rezultati te istrage pokazali su da se na meti špijuniranja našlo najmanje 65 osoba[514]. Treba napomenuti da je Citizen Lab u prosincu 2022. naveo da je jedna zaraza bila pogrešno pripisana zbog pogreške u označivanju inicijalima[515], premda je ukupan broj katalonskih meta ostao nepromijenjen. Španjolske vlasti priznale su u svibnju 2022. da su nadzirale 18 pojedinaca uz odobrenje suda[516], iako nalozi za te predmete nisu javno objavljeni. Bivša voditeljica španjolskog Nacionalnog obavještajnog centra Paz Esteban pojavila se pred Odborom za službene tajne parlamenta na sastanku koji je bio zatvoren za javnost kako bi obrazložila nadzor tih 18 osoba.

306. Španjolska vlada zasad je dala ograničene informacije o svojoj ulozi u tom špijuniranju pozivajući se na potrebu povjerljivosti zbog razloga nacionalne sigurnosti i pravnih razloga. Međutim, na temelju niza pokazatelja[517], od kojih su neki potvrđeni na prethodno navedenom sastanku Odbora za službene tajne, pretpostavlja se da su nadzor katalonskih meta provele španjolske vlasti.

307. Detaljna analiza nadzora pokazuje jasan obrazac. Većina presretanja iz afere CatalanGate podudara se i povezana je s ključnim političkim događajima, pitanjima ili osobama, kao što je dopuštenost zakona o odcjepljenju koje je odobrio katalonski parlament, sudski predmeti protiv katalonskih separatista, javni skupovi koje je organizirao Tsunami Democràtic i komunikacija s katalonskim separatistima koji žive izvan Španjolske[518]. Takav nadzor uključuje, primjerice, komunikaciju između odvjetnika i klijenta separatista u zatvoru večer prije njegova suđenja, kontakte između supružnika ili komunikaciju povezanu s preuzimanjem dužnosti u Europskom parlamentu. Kad je riječ o preostalih 47 predmeta uporabe špijunskog softvera, nije bilo moguće procijeniti kako bi mete mogle izravno utjecati na nacionalnu sigurnost ili integritet države ili kako su bile izravna prijetnja nacionalnoj sigurnosti ili integritetu države te o tome nisu pružene informacije[519]. Iako su protiv nekih osoba postojale kaznene optužbe prije nego što su postale predmet špijuniranja, protiv nijedne od 18 osoba nisu podignute kaznene optužbe kao posljedica nadzora špijunskim softverom[520].

KUPNJA ŠPIJUNSKOG SOFTVERA

308. Španjolske vlasti prethodno su priznale kupnju alata za presretanje telekomunikacija i

---

[513] https://www.theguardian.com/world/2020/jul/16/two-catalan-politicians-to-take-legal-action-targeting-spyware

[514] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18. travnja 2022.* str. 1.

[515] Citizen Lab, *Correcting a case* (Ispravak predmeta), izvješće o aferi CatalanGate, https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/, 22. prosinca 2022.

[516] *El National*, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. svibnja 2022.

[517] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022. str. 1+3.

[518] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022.

[519] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022.

[520] Misija u Španjolsku.

nabavu Sustava za zakonito presretanje telekomunikacija (SITEL) 2001. Priznale su i da su Ministarstvo unutarnjih poslova, Nacionalni obavještajni centar i španjolska nacionalna policija 2010. sklopili ugovor s poduzećem Hacking Team za usluge povezane sa špijunskim softverom kao dio provedbe integriranog sustava presretanja telekomunikacija, što je pružilo operativnim jedinicama snaga državne sigurnosti (FCSE) sredstva za presretanje i snimanje elektroničkih komunikacija koji su odobreni sudskim nalogom[521]. Od njegova pribavljanja španjolske vlasti upotrijebile su SITEL, među ostalim, u operacijama za borbu protiv droga, za pronalazak džihadističke ćelije koja je počinila napade u Madridu 11. ožujka 2004. i za borbu protiv slučajeva političke korupcije. Citizen Lab je također izvijestio o sumnji da je Španjolska kupila Finfisher[522]. Španjolski dnevnik *El Pais* izvijestio je 2020. da je Španjolska poslovala s Grupom NSO i da CNI rutinski upotrebljava Pegasus[523]. Španjolska vlada navodno je taj špijunski softver kupila u prvoj polovini 2010-tih godina, a prema procjenama za njega je platila oko 6 milijuna EUR[524] [525]. Kupnju SITEL-a potvrdila je bivša potpredsjednica vlade de la Vega 2009.[526], a sklapanje ugovora za usluge Hacking Teama priznao je Nacionalni obavještajni centar u komentaru za portal El Confidencial 2015.[527] Osim toga, jedan bivši zaposlenik NSO-a potvrdio je da Španjolska ima račun kod tog poduzeća[528], iako su to španjolske vlasti odbile komentirati ili potvrditi[529].

309. Prema Googleovoj Skupini za analizu prijetnji (TAG) poduzeće za špijunski softver Variston IT ima sjedište u Barceloni i navodno je povezano s okvirom koji iskorištava nedostatke „n-day" u programu Microsoft Defender i internetskim preglednicima Chrome i Firefox te instalira špijunski softver na uređaje koji su meta napada. Ti su nedostaci popravljeni 2021. i početkom 2022.[530] Prema njegovu web-mjestu Variston nudi „rješenja za informacijsku sigurnost po mjeri"[531].

---

[521] Ministarstvo unutarnjih poslova, Secretaría de Estado de Seguridad, Centro Tecnológico de Seguridad, Projekt domovinske sigurnosti, scetse.ses.mir.es/publico/cetse/en/proyectosEuropeos/fondoISF/marcoFinanciero-2021-2027/proyectosEuISF

[522] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 5.

[523] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 5.

[524] Politico, https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/, 20. travnja 2022.

[525] El País, https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html, 20. travnja 2022.

[526] Newtral, https://www.newtral.es/sitel-programa-espia-guardia-civil-policia-espana/20220509/, 9. svibnja 2022.

[527] El Confidencial, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/, 6. srpnja 2015.

[528] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.

[529] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.

[530] Skupina za analizu prijetnji. *„New details on commercial spyware vendor Variston"* (Nove pojedinosti o dobavljaču komercijalnog špijunskog softvera Varistonu)*; Techcrunch. „Spyware vendor Variston exploited Chrome, Firefox and Windows zero-days, says Google"* (Google tvrdi da je dobavljač špijunskog softvera Variston iskorištavao ranjivosti nultog dana u internetskim preglednicima Chrome i Firefox te operativnom sustavu Windows).

[531] *https://variston.net/*

PRAVNI OKVIR

310. Pravo na privatnost zaštićeno je člankom 18. španjolskog Ustava iz 1978., što uključuje pravo na tajnost komunikacija, točnije jamči se tajnost „poštanskih, telegrafskih i telefonskih komunikacija”[532]. Uporabom softvera kao što su Pegasus i Candiru kršio bi se članak 18. bez sudskog naloga, ali moguće ga je dobiti u skladu sa španjolskim zakonodavstvom[533]. Ustavom se utvrđuju i dodatne iznimke od tih prava u dijelu I., odjeljku 55., gdje se navodi da se neka prava mogu privremeno ukinuti „uz sudjelovanje sudova i odgovarajuću parlamentarnu kontrolu” ako je dogovoreno proglašenje izvanrednog stanja ili opsade u skladu s uvjetima predviđenima u Ustavu ili u slučaju pojedinaca koji su pod istragom zbog aktivnosti povezanih s oružanim skupinama ili terorističkim organizacijama[534]. Isto tako, članak 55. sadržava demokratske zaštitne mjere kako bi se osiguralo utvrđivanje kaznene odgovornosti za „neosnovano korištenje ili zlouporabu” navedenih ovlasti.

311. Za aktivnosti koje mogu utjecati na nepovredivost doma i tajnost komunikacija člankom 18. španjolskog Ustava zahtijeva se sudski nalog. Člankom 8. Europske konvencije o ljudskim pravima zahtijeva se da je svako uplitanje javne vlasti u ostvarivanje tog prava u skladu sa zakonom i da je to mjera koja je u demokratskom društvu nužna za nacionalnu sigurnost, javnu sigurnost, gospodarski interes države, zaštitu javnog reda i sprečavanje kriminala, zaštitu zdravlja ili morala te zaštitu prava i sloboda drugih.

312. Dodatne pojedinosti o izuzećima od prava na privatnost iz članka 18. navedene su u Zakonu o kaznenom postupku[535 , 536]. Člankom 588. tog zakona posebno se ograničava uporaba istražnih mjera u istrazi onih činjenica koje, zbog svoje posebne ozbiljnosti, opravdavaju ograničavanje temeljnih prava. Ipak, iz te su odredbe izuzeti slučajevi navedeni u: a) Organskom zakonu 2/2002 od 6. svibnja kojim se regulira prethodni sudski nadzor Nacionalnog obavještajnog centra; b) Organskom zakonu 4/1981 od 1. lipnja o stanju uzbune, izvanrednom stanju i opsadnom stanju; i c) Organskom zakonu 2/1989 od 13. travnja o vojnom postupku, koji sadržava dodatne odredbe primjenjive na Zakon o kaznenom postupku. Člankom 588. tog zakona zahtijeva se odobrenje suca za presretanje telefonskih i telematskih komunikacija ako su predmet istrage teška kaznena djela kao što su terorizam ili kaznena djela počinjena računalnim instrumentima ili drugom informatičkom ili komunikacijskom tehnologijom ili komunikacijskom uslugom. Usto, ograničenja mora odobriti pravosudno tijelo. Na odobrenja se primjenjuju četiri načela. Prvo načelo je načelo posebnosti (nadzor treba biti povezan s određenim kaznenim djelom). Drugo načelo je načelo prikladnosti

[532] Španjolski ustav iz 1978., https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx,odjeljak 18.
[533] Španjolski ustav iz 1978., https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, odjeljak 18.
[534] Španjolski ustav iz 1978., https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, odjeljak 55.
[535] Zakon o kaznenom postupku iz 2016., https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf

[536] Kraljevski dekret od 14. rujna 1882. kojim se odobrava Zakon o kaznenom postupku, https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20220907

(utvrđuje trajanje, cilj i subjektivni opseg). Treće načelo je načelo proporcionalnosti (jačina dostupnih dokaza, ozbiljnost predmeta i traženi rezultat), a četvrto načelo je načelo iznimne prirode i nužnosti (nema drugih dostupnih mjera i bez njega bi bilo uplitanja u istragu)[537]. Člankom 588.f (točke (a), (b) i (c)) posebno se utvrđuju uvjeti pretraga računala na daljinu. Nadležni sudac može na temelju članka 588.f odobriti instalaciju softvera i omogućiti telematsku istragu na daljinu bez znanja vlasnika ili korisnika ako je to povezano s istragom određenih kaznenih djela. U tu svrhu mjera je strogo ograničena na trajanje od jednog mjeseca, koje se može produljiti na razdoblja od mjesec dana do najviše tri mjeseca.

313. Člankom 197. Kaznenog zakona predviđena je zatvorska kazna u trajanju od 12 mjeseci do četiri godine i novčana kazna u trajanju od 12 mjeseci do 24 mjeseca za osobe koje oduzmu ili presretnu, među ostalim, elektroničku poštu i telekomunikacije bez ispravnog dopuštenja[538]. Člankom 264. Kaznenog zakona dodatno se regulira kazneno djelo brisanja podataka i dopušta se pristup podacima u situacijama u kojima je nadležno tijelo dalo potrebno odobrenje[539].

314. Zahtjevi za sudski nadzor su sljedeći: a) pravosudna policija mora obavijestiti suca istrage o provedbi i rezultatima mjere; b) sudac u sudskoj odluci kojom odobrava nadzor utvrđuje učestalost i oblik u kojem ga pravosudna policija mora obavijestiti o provedbi mjere; c) pravosudna policija sucu mora do utvrđenih rokova staviti na raspolaganje dva različita digitalna spisa, jedan s transkriptom odlomaka koji se smatraju važnima i drugi s potpunim snimkama; d) na snimkama mora biti naznačen izvor i odredište svake komunikacije; e) pravosudna policija mora naprednim sustavom elektroničkog pečaćenja ili potpisa ili dovoljno pouzdanim sustavom upozorenja osigurati autentičnost i cjelovitost informacija prenesenih sa središnjeg računala na digitalne medije na kojima su komunikacije snimljene, i; f) pravosudna policija mora izvijestiti o rezultatima mjere kad provedba mjere završi.

315. Španjolska obavještajna služba sastoji se od tri glavne agencije. Prva je Nacionalni obavještajni centar, koji provodi svoje misije prikupljanjem informacija u Španjolskoj i inozemstvu pod nadzorom i kontrolom izvršne, zakonodavne i sudske vlasti i dio je Ministarstva obrane[540]. Direktora CNI-ja predlaže ministar obrane i on obnaša dužnost glavnog savjetnika predsjednika Vlade za obavještajna i protuobavještajna pitanja[541]. Drugo tijelo je domaća obavještajna agencija pod nazivom Obavještajni centar za suzbijanje terorizma i organiziranog kriminala (CITCO). Treće tijelo je Obavještajni centar španjolskih oružanih snaga (CIFAS). I CIFAS je pod izravnim nadzorom

[537] . Zakon o kaznenom postupku iz 2016., https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf
[538] Kazneni zakon iz 1995., https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, članak 197.
[539] Kazneni zakon iz 1995., https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, članak 264.
[540] Nacionalni obavještajni centar, https://www.cni.es/
[541] https://www.cni.es/en/intelligence

Ministarstva obrane[542] [543]. Nacionalni obavještajni centar osnovan je Zakonom 11/2002 od 6. svibnja 2002., kojim ga se ovlašćuje za provođenje „sigurnosnih istraga”[544]. Španjolska policija i tijela kaznenog progona, poznata kao „Guardia Civil”, imaju „vojnu prirodu” i isto odgovaraju Ministarstvu obrane[545].

316. Zakonom o službenim tajnama donesenim 1968. obuhvaćeni su povjerljivi dokumenti u Španjolskoj i nije navedeno razdoblje za deklasifikaciju nakon kojeg službena tajna istječe[546]. Takvi dokumenti ostaju tajni osim ako vlada posebno naredi njihovu objavu, tj. da ministarstvo ili neko drugo službeno tijelo provede brzu deklasifikaciju dokumenta. Španjolska vlada trenutačno preispituje taj zakon i iako nije utvrđen rok za njegovo donošenje, preliminarni nacrt zakona o povjerljivim podacima odobren je 1. kolovoza 2022. Njime se propisuje da će povjerljivi podaci morati biti objavljeni unutar razdoblja od 4 godine do 50 godina, iako se ono može produljiti.

EX ANTE NADZOR

317. Misija je Nacionalnog obavještajnog centra pružati španjolskoj vladi informacije i obavještajne podatke potrebne za sprečavanje i izbjegavanje bilo kakve opasnosti ili prijetnje neovisnosti i integritetu države, nacionalnim interesima i stabilnosti pravne države i njezinih institucija. Velik dio nadzora u Španjolskoj provodio je CNI. Nacionalni obavještajni centar osnovan je Zakonom 11/2002 od 6. svibnja, kojim mu se daju ovlasti za provođenje „sigurnosnih istraga osoba ili subjekata”[547]. Međutim, sredstva za provođenje takvih djelatnosti i njihova ograničenja slabo su razjašnjeni[548] jer su djelatnosti Nacionalnog obavještajnog centra, njegova organizacija i unutarnja struktura, sredstva i postupci, osoblje, prostori, baze podataka i podatkovni centri, izvori informacija te informacije i podaci koji mogu dovesti do saznanja o prethodno navedenim pitanjima povjerljivi podaci s odgovarajućim stupnjem tajnosti[549]. Zakonom 11/2002 ujedno je uspostavljen parlamentarni, izvršni i zakonodavni nadzor nad Nacionalnim obavještajnim centrom[550]. Parlamentarni nadzor provodi Odbor za upotrebu i nadzor kredita dodijeljenih tajnim fondovima (takozvani Odbor za službene tajne) španjolskog parlamenta, koji je uspostavljen 1995.[551] Odbor za službene tajne zbog kašnjenja u svojem sastavljanju tijekom 14. saziva španjolskog parlamenta (izabran u prosincu 2019.) nije podnio godišnje izvješće o aktivnostima Nacionalnog obavještajnog centra kako je propisano zakonom. Do travnja 2023. nije podneseno

[542] https://emad.defensa.gob.es/en/?__locale=en
[543]Izvješće Ženevskog centra za upravljanje sigurnosnim sektorom za 2020.,https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf, str. 40.
[544] Zakon 11/2002 od 6. svibnja, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, članak 5.5.
[545] https://www.guardiacivil.es/es/institucional/Conocenos/index.html
[546] El Pais, https://english.elpais.com/spanish_news/2021-04-05/spanish-government-begins-reform-of-franco-era-official-secrets-law.html, 5. travnja 2021.; Zakon o službenim tajnama iz 1968.
[547] Zakon 11/2002 od 6. svibnja, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, članak 5.5.
[548] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. svibnja 2022.
[549] Zakon 11/2002 od 6. svibnja kojim se regulira Nacionalni obavještajni centar, članak 5.1.
[550] Zakon 11/2002 od 6. svibnja, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, članak 11.
[551] Zakon 11/1995 od 11. svibnja, https://www.boe.es/eli/es/l/1995/05/11/11/con

godišnje izvješće tijekom ovog parlamentarnog saziva. Vladin delegirani odbor za obavještajne poslove koordinira obavještajne aktivnosti svih španjolskih obavještajnih i informacijskih službi[552]. Konačno, Odbor za obranu Kongresa zastupnika provodi zakonodavni nadzor nad CNI-jem[553]. Godišnjom Obavještajnom direktivom utvrđuju se obavještajni prioriteti Nacionalnog obavještajnog centra.

318. Sudski nadzor djelovanja Nacionalnog obavještajnog centra omogućen je Organskim zakonom 2/2002 od 6. svibnja[554, 555], kojim se nadopunjuje Zakon 11/2002 od 7. svibnja kojim se regulira Nacionalni obavještajni centar. Točnije, tim se zakonom zahtijeva da kad Nacionalni obavještajni centar želi provesti nadzor, državni tajnik direktor Nacionalnog obavještajnog centra obvezan je u skladu s Organskim zakonom o pravosuđu od nadležnog suca Vrhovnog suda zatražiti odobrenje za donošenje mjera koje utječu na nepovredivost doma i tajnost komunikacija[556] ako su takve mjere potrebne da bi Nacionalni obavještajni centar izvršio svoje funkcije. Njime je propisano i da operacije nadzora ne mogu trajati dulje od tri mjeseca i da produljenje tog razdoblja mora imati primjereno opravdanje. Međutim, te su odredbe stupile na snagu u vrijeme kad je tehnologija za nadzor bila mnogo manje napredna, a špijunski softveri kao Pegasus i Candiru nisu postojali. Stoga postoji rizik da su pravna jamstva zastarjela i da građanima ne pružaju dostatnu zaštitu. Stoga je izvršna vlast najavila reformu pravnog okvira Nacionalnog obavještajnog centra, ali još nisu podneseni prijedlozi te reforme.

EX POST NADZOR

319. Zakonima kojima je osnovan Nacionalni obavještajni centar ujedno je uspostavljen Odbor za obranu Kongresa zastupnika, koji je odgovoran za dodjelu tajnih financijskih sredstava Nacionalnom obavještajnom centru i izradu godišnjeg izvješća o Nacionalnom obavještajnom centru. Iznosi koji se dodjeljuju tajnim fondovima utvrđeni su u španjolskom Zakonu o općem proračunu za svaku financijsku godinu[557]. Sva tijela koja imaju zadaću nadziranja Nacionalnog obavještajnog centra, kao što su Odbor za obranu, Odbor za službene tajne ili ombudsman, imaju pristup potrebnim informacijama za ocjenjivanje jesu li operacije izvršene zakonito i ispravno. Vlada godišnje Obavještajnom direktivom određuje i odobrava ciljeve Nacionalnog obavještajnog centra, koji su tajni[558, 559]. Direktor Nacionalnog obavještajnog centra ima isključivu nadležnost za odlučivanje o svrsi i odredištu dodijeljenih sredstava i treba redovito izvještavati predsjednika vlade o njihovoj uporabi. Odbor za službene tajne obavješćuje se o obavještajnim ciljevima i ima pravo na podnošenje godišnjeg izvješća o

[552] Zakon 11/2002 od 6. svibnja, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, članak 6.
[553] Zakon 11/2002 od 6. svibnja, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html, članak 11.
[554] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. svibnja 2022.
[555] Organski zakon 2/2002 od 6. svibnja, https://www.global-regulation.com/translation/spain/1451142/law-2-2002%252c-6-may%252c-regulating-the-prior-judicial-control-of-the-national-intelligence-center.html
[556] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. svibnja 2022.
[557] Zakon 11/1995 od 11. svibnja kojim se regulira uporaba i nadzor kredita dodijeljenih tajnim fondovima, članak 2., https://www.boe.es/eli/es/l/1995/05/11/11/con
[558] Zakon 11/2002 od 6. svibnja kojim se regulira Nacionalni obavještajni centar, članak 3.
[559] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 2.

aktivnostima obavještajnih službi[560]. Ima i pristup izvješću o ocjeni aktivnosti, statusa i stupnja ispunjenja ciljeva koje jednom godišnje sastavlja direktor Nacionalnog obavještajnog centra. Međutim, španjolskim se zakonom ne utvrđuje da će se omogućiti javni pristup dokumentima ili informacijama koji se odnose na rad obavještajnih službi. Takva obveza ne postoji ni u pravnom okviru Zakona o transparentnosti[561]. S obzirom na tu tajnost nije moguće sa sigurnošću utvrditi je li španjolska vlada sklopila ugovore s Grupom NSO ni je li kupila i upotrebljavala Pegasus. Osobe koje su se našle na meti špijuniranja ne znaju razloge, opseg ni posljedice presretanja njihovih komunikacija[562].

320. Zbog otkrića da je Nacionalni obavještajni centar upotrijebio Pegasus i Candiru španjolski ombudsman najavio je *ex officio* istragu[563]. Španjolski ombudsman u svojoj je službenoj izjavi od 18. svibnja 2022. potvrdio da mu je Vijeće ministara dalo potpuni pristup povjerljivim dokumentima i nije iskoristilo svoje isključivo pravo predviđeno člankom 22. Organskog zakona 3/1981 o ombudsmanu. Međutim, ta je istraga obuhvaćala samo 18 osoba za koje su španjolske vlasti potvrdile da su bile meta špijuniranja uz odobrenje suda[564] [565]. Zaključak istrage bio je da su presretanja provedena u skladu sa zakonom jer je utvrđeno da ih je odobrio sud i da je odobrenje bilo praćeno potrebnim obrazloženjem[566]. Međutim, ombudsman nema nadležnost za ocjenjivanje proporcionalnosti, koju može utvrditi samo sudac[567]. Osim toga, nije stupio u kontakt ni razgovarao s osobama koje su bile meta špijuniranja ni njihovim odvjetnicima. Ombudsman je preporučio reviziju postojećih pravnih odredaba i po potrebi uvođenje reformi kako bi se uzela u obzir modernizacija sustava nadzora[568]. Povodom toga španjolska je vlada u svibnju 2022. najavila da će se provesti revizija Zakona o službenim tajnama iz 1968. i Organskog zakona 2/2002[569] [570], ali nije utvrđen rok za donošenje te revizije.

321. Odbor za službene tajne obvezan je podnositi godišnje izvješće o aktivnostima obavještajnih službi. Sazvan je 5. svibnja 2022. zbog aktivnosti nadzora koji je provodio Nacionalni obavještajni centar, ali to je bio prvi sastanak tog tijela u više od tri godine zbog prekida parlamentarne aktivnosti uzrokovanog pandemijom bolesti COVID-19.

---

[560] Zakon 11/1995 od 11. svibnja kojim se regulira uporaba i nadzor kredita dodijeljenih tajnim fondovima, članak 7.4.
[561] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 2.
[562] Amnesty International, „10 medidas que garanticen la no repeticion de violaciones des Derechos Humanos".
[563] https://www.reuters.com/article/us-spain-politics-catalonia-spying-idCAKCN2MG0A6, 24. travnja 2022.
[564] The Guardian, https://www.theguardian.com/world/2022/may/05/catalans-demand-answers-after-spanish-spy-chief-confirms-phone-hacking, 5. svibnja 2022.
[565] https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/
[566] La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. svibnja 2022.

[567] Informacije iz misije u Španjolsku.
[568] https://www.defensordelpueblo.es/noticias/defensor-del-pueblo-verifica-la-actuacion-del-cni-se-ha-realizado-conforme-la-constitucion-la-ley-los-casos-examinados/
[569] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. svibnja 2022.
[570] https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. svibnja 2022.

Voditeljica Nacionalnog obavještajnog centra Paz Esteban pojavila se pred Odborom i priznala nadzor 18 vođa separatističkog pokreta. Ujedno je Odboru podnijela sudske naloge za tih 18 predmeta[571, 572]. Međutim, to je saslušanje u skladu s člankom 5.5. Zakona 11/2002 provedeno iza zatvorenih vrata, a osobama koje su mu prisustvovale nije bilo dopušteno unijeti elektroničke uređaje[573]. Nisu objavljene nikakve službene informacije osim broja predmeta. Prema glasnogovornicima koji su bili prisutni na saslušanju, ono je gotovo isključivo bilo usmjereno na katalonske mete, a ne na Pedra Sáncheza, Margaritu Robles i navodnih 3 GB podataka koji su preuzeti s njihovih uređaja plaćeničkim špijunskim softverom[574]. Robles je opetovano ustrajala u tome da je špijuniranje 18 katalonskih meta bilo opravdano.

322. Sánchez je o problemu govorio i u španjolskom parlamentu, gdje je još jednom ponovio da je sve učinjeno u skladu sa zakonom i da je nacionalna sigurnost predmet nadzora španjolskog parlamenta i drugih vladinih tijela[575]. To da je uporaba Pegasusa bila u potpunosti zakonita tvrdio je i bivši glavni izvršni direktor Grupe NSO Shalev Hulio, koji je za *New Yorker* rekao da je španjolska uporaba Pegasusa bila zakonita s obzirom na to da Španjolska izrazito poštuje vladavinu prava i obvezu odobrenja Vrhovnog suda[576].

323. Španjolski kongres glasao je 3. svibnja 2022. protiv prijedloga za uspostavu istražnog odbora za ispitivanje uporabe Pegasusa. Katalonski parlament osnovao je 21. rujna 2022. istražni odbor za ispitivanje špijunaže koju je Kraljevina Španjolska provela nad političkim predstavnicima, aktivistima, novinarima i njihovim članovima obitelji s pomoću programa Pegasus i Candiru.

JAVNI NADZOR

324. Uporaba špijunskog softvera protiv članova španjolske vlade i pristaša neovisnosti Katalonije privlači veliku pažnju javnosti otkad je otkrivena u travnju 2022. Španjolski mediji i medijske kuće iz cijelog svijeta provodili su opsežna istraživanja sustava nadzora u Španjolskoj u suradnji s organizacijama civilnog društva i zauzimali se za temeljna prava osoba koje su se našle na meti špijuniranja. Nasuprot tomu, neki španjolski političari pokušali su diskreditirati Citizen Lab, sugerirajući da se ta organizacija služi nepouzdanim metodama ili da je politički motivirana.

PRAVNA ZAŠTITA

325. Sudski postupak u slučaju nadzora špijunskim softverom predsjednika vlade Pedra

[571] *El National*, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. svibnja 2022.
[572] *El País*, https://elpais.com/espana/2022-05-05/la-directora-del-cni-da-explicaciones-sobre-el-espionaje-de-pegasus-ante-el-escepticismo-de-los-partidos.html, 21. svibnja 2022.
[573] *El National*, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. svibnja 2022.
[574] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. svibnja 2022.
[575] . La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. svibnja 2022.
[576] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.

Sáncheza i ministrice obrane Margarite Robles pokrenuo je glavni državni odvjetnik[577] pred Španjolskim nacionalnim sudom, koji se naziva Audiencia Nacional, u Madridu. Nadležnost Španjolskog nacionalnog suda propisana je člankom 65. stavkom 1. točkom (a) Organskog zakona 6/1985 o pravosuđu, na temelju koje iznesene činjenice spadaju pod nadležnost Španjolskog nacionalnog suda jer utječu na osobe u visokim nacionalnim tijelima, kao što su predsjednik vlade i ministrica obrane. Postupak je u tijeku, a za njega je odgovoran sudac José Luis Calama, voditelj Središnjeg istražnog suda br. 4[578]. Sudac Calama dostavio je 13. listopada 2022. ministrici Robles i ministru Grande-Marlaska upitnik koji je sadržavao zahtjev da obrazlože kako su utvrđeni slučajevi zaraze Pegasusom, koji su trebali potvrditi zakoniti izvori. Ured tužitelja i Ured državnog odvjetnika također su uputili pitanja ministrima[579].

326. Pojedinci koji su izravno ili neizravno povezani s pokretom za neovisnost Katalonije podnijeli su pred Istražnim sudom u Barceloni pravne pritužbe u vezi s nadzorom špijunskim softverom. Istrage su u tijeku, iako sporo napreduju. Prvu pritužbu podnijeli su 2020. bivši predsjednik katalonskog parlamenta i aktualni ministar gospodarstva i rada Katalonije Roger Torrent te bivši ministar vanjske politike, institucionalnih odnosa i transparentnosti Katalonije i aktualni predsjednik Republikanske ljevice Katalonije (ERC) u gradskom vijeću Barcelone Ernest Maragall[580, 581]. Predmet je dodijeljen Istražnom sudu br. 32 u Barceloni, koji je privremeno zatvorio predmet. Andreu Van Den Eynde, i sam meta Pegasusa, jedan je od odvjetnika koji zastupaju Torrenta i Maragalla u tom predmetu. Van Den Eynde je kritizirao sudove zbog stalnog odgađanja postupaka i „praktičkog paraliziranja" predmeta[582]. I organizacija Omnium Cultural, Narodna skupština Katalonije (ANC) i stranka Kandidatura narodnog jedinstva (CUP) podnijele su nekoliko kaznenih prijava pred istim sudom u Barceloni, ali još nije pokrenuta istraga. Istražni sud br. 32 u Barceloni odbio je zahtjev za objedinjenje tužbi, stoga ih sada rješavaju različiti sudovi i suci. Pritužbe organizacije Òmnium Cultural i stranke Kandidatura narodnog jedinstva dodijeljene su u travnju 2022. Istražnom sudu br. 21, a pritužbe Narodne skupštine Katalonije dodijeljene su 26. srpnja 2022. Istražnom sudu br. 23. Nastavak postupka u vezi s pritužbama još nije u potpunosti odobren niti je dogovoreno pokretanje istraga, stoga se nijedan od tih predmeta trenutačno ne istražuje. Većinu predmeta suci su privremeno obustavili dok se ne prikupi više dokaza jer ključni dokazi – navodno zaraženi mobilni telefoni – nisu bili u posjedu tužitelja[583]. Suci mogu odlučiti prihvatiti izvješća Citizen Laba kao stručne dokaze u predmetu. Međutim, ako suci to ne dopuste, osobama koje su bile meta

[577] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. svibnja 2022.
[578] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. svibnja 2022.
[579] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. svibnja 2022.
[580] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. svibnja 2022.
[581] El Diario, https://www.eldiario.es/catalunya/juez-archiva-investigacion-espionaje-pegasus-torrent-maragall_1_9030414.html, 30. svibnja 2020.
[582] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30. svibnja 2022.
[583] El País, https://elpais.com/espana/catalunya/2022-05-30/el-juez-de-barcelona-archiva-de-forma-provisional-la-causa-por-el-espionaje-con-pegasus-a-torrent-y-maragall.html, 30. svibnja 2022.

špijuniranja bit će teško dokazati svoje tvrdnje[584].

327. Budući da Španjolski nacionalni sud ima nadležnost nad cijelom Španjolskom za predmete koji se odnose na najteža kaznena djela, javni tužitelj mogao bi zatražiti objedinjenje svih predmeta povezanih s Pegasusom[585]. Drugim riječima, svi predmeti meta španjolske vlade i meta u aferi CatalanGate rješavali bi se pred Španjolskim nacionalnim sudom u Madridu. Odvjetnici koji zastupaju katalonske mete tvrde da između tih predmeta ne postoji nikakva veza, osim ako se dokaže da je počinitelj isti u svim slučajevima nadzora[586].

328. Sa 65 katalonskih meta povezano je nekoliko drugih sudskih predmeta koji su u tijeku. Jedan od njih je predmet koji je odvjetnik i meta Pegasusa Gonzalo Boye pokrenuo u ime najmanje 19 meta protiv NSO-a, njegove trojice osnivača Niva Karmija, Shaleva Hulija i Omrija Lavieja, poduzeća Q Cyber Technologies i poduzeća OSY, podružnice sa sjedištem u Luksemburgu[587, 588]. Bivši predsjednik Katalonije Quim Torra i bivši potpredsjednik katalonskog parlamenta Josep Costa podnijeli su pritužbu Vrhovnom sudu, ali godinu dana poslije pravosuđe još nije odlučio bi li se predmet trebao iznijeti pred Vrhovnim sudom ili Španjolskim nacionalnim sudom. U međuvremenu se nije odvila nikakva istraga. I u Francuskoj, Belgiji, Švicarskoj, Njemačkoj i Luksemburgu u tijeku su sudski postupci zbog nadzora katalonskih separatista u egzilu[589].

METE

329. Članovi pokreta koji zagovara neovisnost Katalonije, njihovi članovi obitelji i s njima povezano osoblje navodno su bili na meti špijunskog softvera još od 2015., od špijuniranja tadašnjeg predsjednika Narodne skupštine Katalonije Jordija Sáncheza nedugo nakon velikih demonstracija u Barceloni. Prema izvješću Citizen Laba iz travnja 2022. najmanje 65 osoba bilo je na meti špijunskog softvera u razdoblju od 2017. do 2020. U slučaju 63 osobe bio je upotrijebljen Pegasus, u slučaju četiri osobe Candiru, a u slučaju najmanje dvije osobe oba spomenuta softvera[590]. Uspješno su zaraženi uređaji najmanje 51 pojedinca[591]. Među navodnim metama, izravnim ili neizravnim, bile su političke ličnosti zagovaratelji neovisnosti Katalonije, kao što su ministar gospodarstva i rada i bivši predsjednik katalonskog parlamenta Roger Torrent, aktualni predsjednik Republikanske ljevice Katalonije u gradskom vijeću Barcelone i bivši ministar vanjske politike, institucionalnih odnosa i transparentnosti Katalonije Ernest Maragall te četiri zastupnika u Europskom parlamentu. S obzirom na to da je od početka hakiranja do tih

[584] Misija u Španjolsku.
[585] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. svibnja 2022.
[586] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. svibnja 2022.
[587] El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html, 3. svibnja 2022.
[588] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19. travnja 2022.
[589] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19. travnja 2022.
[590] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 5.
[591] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 5.

otkrića proteklo dosta vremena, velik broj meta nije bilo moguće utvrditi ili dalje istraživati zbog različitih čimbenika, uključujući taj da su brojne mete bacile hakirane telefone[592].

330. Španjolski predsjednik vlade Pedro Sánchez, ministrica obrane Margarita Robles i ministar unutarnjih poslova Fernando Grande-Marlaska bili su na meti Pegasusa između svibnja i lipnja 2021.[593] Zasad je o pojedinostima tog hakiranja dostupno vrlo malo informacija. Informacije koje su poznate objavila je vlada i one nisu rezultat istrage koju su proveli Citizen Lab ili bilo koja druga slična istraživačka organizacija ili istraživački novinari te su još dio istrage u tijeku. Sánchez i Robles čelnici su dvaju ogranaka Vlade koji nadziru CNI, tijelo nadležno za provođenje nadzora u Španjolskoj. Zaražene uređaje koji su pripadali Sánchezu i Robles izdala im je Vlada i povremeno su provjeravani kako bi se utvrdila moguća prisutnost špijunskog softvera[594]. U slučaju Grande-Marlaske zaražen je bio njegov privatni uređaj[595]. Ministar poljoprivrede Luis Planas, koji je prethodno bio diplomat u Maroku, također je bio meta špijunskog softvera, ali pokušaj zaraze u njegovu slučaju nije uspio. Pojavila su se izvješća da bi za taj pokušaj mogla biti odgovorna marokanska vlada. Međutim, ta informacija nije potvrđena[596].

331. Za 18 predmeta od njih 65 potvrđeno je da su nadzor provele španjolske vlasti, ali vlada nije komentirala preostalih 47 osoba[597]. Ostaje nejasno jesu li drugi pojedinci bili mete nadzora Nacionalnog obavještajnog centra na temelju sudskog naloga odnosno je li neko drugo tijelo dobilo sudski nalog da ih zakonito nadzire. Unatoč sudskim nalozima za uporabu špijunskog softvera na 18 osoba, one poslije nisu optužene za kazneno djelo u vezi s nalogom kojim je odobrena uporaba špijunskog softvera. Među metama za koje je odobren nadzor su aktualni predsjednik Katalonije Pere Aragonès, bivši predsjednik i aktualni zastupnik u Europskom parlamentu Carles Puigdemont i drugi političari zagovaratelji neovisnosti Katalonije i njihovi suradnici[598]. Podložno zahtjevima tajnosti i povjerljivosti sadržanima u zakonu ministrica obrane Robles pozvala se na Zakon o službenim tajnama kako bi obrazložila razloge nadziranja tih konkretnih meta[599]. Većina od 65 katalonskih meta u nekom je trenutku bila u kontaktu s članovima pokreta koji zagovara neovisnost Katalonije koji žive izvan Španjolske. Neke osobe koje su se našle na meti napada u trenutku zaraze nalazile su se izvan Španjolske, među ostalim u Belgiji, Švicarskoj, Njemačkoj i Francuskoj. Takav digitalni nadzor bio bi nezakonit u Njemačkoj, osim ako ga savezna tijela izričito dopuste.

---

[592] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022. str. 5.
[593] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. svibnja 2022.
[594] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7. svibnja 2022.
[595] La Razon, https://www.larazon.es/espana/20220510/gwxedc4drzhali5bqi4vbhk7kq.html
[596] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7. svibnja 2022.
[597] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. svibnja 2022.
[598] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. svibnja 2022.
[599] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html 5. svibnja 2022.

332. Otkriveno je da su katalonski zastupnici u Europskom parlamentu koji zagovaraju neovisnost Katalonije bili jedna od glavnih skupina koja se našla na meti špijunskog softvera. Svatko od njih izravno je ili neizravno hakiran špijunskim softverom postupkom koji Citizen Lab naziva „relacijskim ciljanjem" (engl. *relational targeting*)[600]: Diana Riba i Giner, Jordi Solé, Carles Puigdemont i Clara Ponsatí. Mobilni telefon bivše akreditirane asistentice Clare Ponsatí uspješno je zaražen Pegasusom. U slučaju Antonija Comína, koji je tijekom saslušanja pred odborom PEGA optužio španjolsku državu da ga je špijunirala, Citizen Lab je priznao da mu je zaraza pogrešno pripisana zbog pogreške u označivanju inicijalima.

333. Telefon Diane Ribe i Giner, zastupnice u Europskom parlamentu iz Republikanske ljevice Katalonije, izravno je zaražen špijunskim softverom 28. listopada 2019., samo tri mjeseca nakon što je preuzela dužnost u Parlamentu. Dok je telefonom razgovarala s asistenticom komunikacija je prekinuta i članica njezina osoblja čula je snimku razgovora koji je upravo vodila s Ribom i Giner. Ta se zaraza izravno podudarala s ključnom sudskom presudom u vezi s katalonskim separatistima, među kojima je i Raül Romeva, suprug Ribe i Giner koji je u konačnici dobio dvanaestogodišnju kaznu[601]. Riba i Giner navela je na saslušanju pred odborom PEGA u Parlamentu da se u to vrijeme većina njezinih telefonskih poziva odnosila na taj sudski predmet, kao i da je prisustvovala brojnim sastancima i često odlazila na sud. Stoga je usputni ulov u tom slučaju bio iznimno važan jer je uključivao Romevu i druge povezane s tim značajnim predmetom[602].

334. Za zastupnika u Europskom parlamentu Jordija Soléa, također iz Republikanske ljevice Katalonije, prema istraživanju Citizen Laba izvorno se tvrdilo da je hakiran 11. i 27. lipnja 2020.[603] Međutim, poslije je otkriveno pet dodatnih napada u istom razdoblju[604]. Solé je slučajno otkrio da se našao na meti Pegasusa, davši svoj telefon na provjeru u sklopu snimanja dokumentarnog filma nakon što je primio neke potencijalno sumnjive poruke[605]. Kao i u slučaju njegove kolegice, važno je istaknuti vrijeme tog napada. On se dogodio tijekom važnih političkih rasprava o slobodnom mjestu u Europskom parlamentu Oriola Junquerasa, koji nije dobio dopuštenje da preuzme dužnost kao zastupnik dok se nalazio u zatvoru u Španjolskoj[606], i samo mjesec dana prije nego što je Solé imenovan na to mjesto u srpnju 2020. Osim toga, u vrijeme zaraza aktualne su bile rasprave o strategiji stranke i međunarodnim sporovima u vezi s

[600] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 6.
[601] Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor, iskaz zastupnice u Europskom parlamentu Diane Ribe i Giner, Strasbourg, 6. listopada 2022.
[602] Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor, iskaz zastupnice u Europskom parlamentu Diane Ribe i Giner, Strasbourg, 6. listopada 2022.
[603] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 7.
[604] Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor, iskaz zastupnika u Europskom parlamentu Jordija Soléa, Strasbourg, 6. listopada 2022.
[605] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.
[606] Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor, iskaz zastupnika u Europskom parlamentu Jordija Soléa, Strasbourg, 6. listopada 2022.

članovima stranke koji su se nalazili u zatvoru ili u egzilu[607].

335. Europski zastupnik u Parlamentu iz stranke JUNTS i bivši predsjednik Katalonije Carles Puigdemont bio je meta špijuniranja preko svoje supruge Marcele Topor, članova osoblja i nekoliko suradnika[608]. Citizen Lab je izvijestio da se na meti špijuniranja našlo do 11 pojedinaca u bliskom kontaktu s Puigdemontom, što je uključivalo barem dvije zaraze Toporina uređaja 7. listopada 2019. i 4. srpnja 2020.[609]

336. Europska zastupnica u Parlamentu iz stranke JUNTS i bivša ministrica obrazovanja Katalonije Clara Ponsatí bila je relacijska meta. Potvrđeno je da je član osoblja u Europskom parlamentu Pol Cruz zaražen 7. srpnja 2020.[610]

337. Svi predsjednici Katalonije od 2010. bili su mete špijunskog softvera tijekom ili nakon njihovih mandata[611]. Među spomenutih 65 meta bilo je čak 12 članova Republikanske ljevice Katalonije, uključujući glavnu tajnicu stranke Martu Roviru, koja je prema navodima Citizen Laba hakirana najmanje dvaput u lipnju 2020. Vrlo je značajno da su i Gabriel i Rovira živjele u Švicarskoj u vrijeme dok su bile nadzirane poslije sukoba do kojih je došlo nakon referenduma održanog 2017.

CIVILNE METE, UKLJUČUJUĆI NOVINARE, ODVJETNIKE I PREDSTAVNIKE CIVILNOG DRUŠTVA

338. Jordi Domingo bio je 2020. jedan od prvih katalonskih aktivista za koje se tvrdilo da su bili mete špijunskog softvera. Iako je Domingo pristaša neovisnosti Katalonije i član Narodne skupštine Katalonije, *The Guardian* je izvijestio kako sam Domingo smatra da se na meti špijunskog softvera našao greškom. S obzirom na to da u događajima koji su se odigrali 2017. nije imao značajnu ulogu, smatra da je ciljana meta bio odvjetnik istoga imena koji je sudjelovao u sastavljanju mogućeg ustava neovisne Katalonije[612].

339. Narodna skupština Katalonije (ANC), katalonska organizacija civilnog društva koja podupire neovisnost Katalonije, bila je jedna od prvih organizacija meta prije katalonskog referenduma, a otada je izložena opsežnim napadima[613]. Šest meta Narodne skupštine Katalonije uključuju njezino dvoje bivših predsjednika, Jordija Sancheza (2015.–2017.) i Elisendu Paluzie (2018.–2022.), čiji je nadzor špijunskim softverom odobren sudskim nalogom, baš kao i nadzor stručnjaka za digitalno glasanje i decentralizaciju Jordija Bayline, dviju članica njezina Nacionalnog odbora (Arià Bayè i Sònia Urpí) i jednog člana lokalne podružnice (Jordi Domingo).

---

[607] Politico, https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/, 9. siječnja 2020.
[608] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 7.
[609] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 8.
[610] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 7.
[611] Artur Mas (nakon odlaska s dužnosti), Carles Puigdemont (relacijsko ciljanje), Joaquim Torra (dok je bio na dužnosti), Pere Aragones (zaraza se dogodila dok je bio Torrin potpredsjednik). https://catalonia.citizenlab.ca/.
[612] The Guardian, https://www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware, 13. srpnja 2020.
[613] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

340. Zaraženi su uređaji pojedinaca bliskih Jordiju Cuixartu, predsjedniku organizacije Òmnium Cultural (do veljače 2022.), jer se on u to vrijeme nalazio u zatvoru. To je uključivalo potpredsjednika te nevladine organizacije Marcela Maurija, za kojega je nadzor špijunskim softverom odobren sudskim nalogom.

341. U veljači 2021. Citizen Lab je otkrio aktivnu zarazu softverom Candiru na laptopu Joana Matamale, poduzetnika i aktivista blisko povezanog s katalonskim političarima zagovarateljima neovisnosti Katalonije[614]. Matamalin nadzor špijunskim softverom bio je odobren sudskim nalogom. Candiru je znatno teže otkriti od Pegasusa, stoga je to otkriće aktivne zaraze omogućilo istraživačima u Citizen Labu da bolje razumiju njegove obrasce. Nakon toga je otkriveno 16 drugih zaraza na Matamalinu uređaju[615]. Microsoft je popravio ranjivosti ažuriranjima, ali nemoguće je znati koliko zaraza softverom Candiru nije otkriveno[616].

342. Najmanje tri poznata programera otvorenog koda i poduzetnika našla su se na meti Pegasusa, uključujući Xaviera Vivesa i Paua Escricha, tvorce protokola otvorenog koda Vocdoni temeljenog na ethereum blockchainu za sigurno digitalno glasanje otporno na cenzuru. Za špijuniranje Vivesa upotrijebljen je zloćudni softver Candiru, a za špijuniranje Escricha upotrijebljeni su i Pegasus i Candiru[617]. Vivesov and Escrichov nadzor špijunskim softverom bio je odobren sudskim nalogom.

343. Gonzalo Boye odvjetnik je bivših predsjednika Puigdemonta i Torre[618]. Boye je tijekom pet mjeseci, između siječnja i svibnja 2020., čak 18 puta bio meta tekstualnih poruka koje su izgledale kao tvitovi organizacija civilnog društva ili istaknutih medijskih kuća[619]. Citizen Lab je potvrdio da je zaraza špijunskim softverom u njegovu slučaju uspjela barem jednom, 30. listopada 2020. Do zaraze je došlo samo 48 sati nakon što je jedan od njegovih klijenata uhićen[620]. Nadziranjem Boyea otvorilo se pitanje zakonitosti kršenja povjerljivog odnosa odvjetnika i klijenta.

344. Međunarodna predstavnica organizacije Òmnium Cultural Elena Jimenez i odvjetnik zadužen za institucionalne odnose te organizacije Jordi Bosch našli su se na meti Pegasusa dok su bili u pravnom timu Jordija Cuixarta. Jimenez je bila u stalnom kontaktu s cijelim Cuixartovim pravnim timom, uključujući međunarodni tim koji je pripremao pritužbu Europskom sudu za ljudska prava. Citizen Lab je dosad pregledao samo Jimenezin najnoviji mobilni telefon, ali potvrdio je da je u veljači 2020. došlo do uspješne zaraze bez potrebe za klikanjem poveznice. Bosch, član pravnog tima manje poznat javnosti, bio je meta u srpnju 2020., manje od tjedan dana prije nego što je Cuixartu odobren blaži oblik zadržavanja i istoga dana kad se prvi put pojavio na

[614] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.
[615] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.
[616] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.
[617] https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/#finding-catalans-targeted-with-candiru
[618] https://catalonia.citizenlab.ca/.
[619] https://catalonia.citizenlab.ca/.
[620] https://catalonia.citizenlab.ca/.

katalonskoj televiziji u ime organizacije Òmnium.

345. Andreu van den Eynde i Adroer uspješno je zaražen Pegasusom 14. svibnja 2020.[621] Do hakiranja je došlo dok je kao odvjetnik zastupao Raula Romevu i Oriola Junquerasa u njihovom predmetu pred Vrhovnim sudom.

346. Slično tomu, uređaj odvjetnika Jaumea Alonso-Cuevillasa također je zaražen dok je predstavljao ključne osobe iz Katalonije, poput Carlesa Puigdemonta. Međutim, Citizen Lab nije uspio odrediti točan datum kad je došlo do uspješne zaraze.

ISTRAGE I PRAVNE REFORME

347. Nakon što su 22. travnja 2022. otkriveni navodi iz slučaja CatalanGate, španjolske institucije pokrenule su postupak provjere kako bi se osiguralo da su smjernice o nadzoru bile ispravno primijenjene. Te su mjere uključivale pozivanje direktorice Nacionalnog obavještajnog centra Paz Esteban pred Odbor za službene tajne 5. svibnja, koje je najavio ministar predsjedništva Félix Bolaños, sesiju parlamentarnog nadzora vlade i ministrice obrane 26. i 27. travnja i neovisnu procjenu koju je proveo ombudsman, pokrenutu 26. travnja i završenu 18. svibnja. Premda se na nju primjenjivala obveza čuvanja tajnosti iz Zakona o službenim tajnama, ministrica obrane Margarita Robles natuknula je da su mjere poduzete kao odgovor na djelovanje onih koji „krše Ustav, preuzimaju javnu infrastrukturu, stvaraju javne nerede i [onih koji] imaju veze s političkim vođama zemlje koja vrši invaziju na Ukrajinu”[622]. Vladajuća stranka (PSOE) i tri glavne oporbene stranke (PP, Vox i Ciudadanos) izvijestile su da je direktorica na zadovoljavajući način objasnila nužnost i zakonitost mjera nadzora špijunskim softverom[623] [624].

348. Španjolski ombudsman zaključio je da je velik dio nadzora koji je Nacionalni obavještajni centar proveo u Španjolskoj bio potpuno u skladu s pravnim postupcima. Kao posljedica njegovih preporuka u pogledu prikladnosti parlamentarnog i sudskog nadzora te kako bi se ažuriralo zakonodavstvo, ojačala jamstava pravosudnog nadzora i osiguralo maksimalno poštovanje temeljnih prava pojedinaca, izvršna vlast Španjolske obvezala se:

1. pokrenuti unutarnju istragu u Nacionalnom obavještajnom centru;

2. pokrenuti istragu unutar Odbora za upotrebu i nadzor kredita dodijeljenih tajnim fondovima španjolskog kongresa i održati saslušanje na kojem će se pojaviti direktorica Nacionalnog obavještajnog centra;

3. otkriti Odboru za upotrebu i nadzor kredita dodijeljenih tajnim fondovima španjolskog kongresa; 18 naloga Vrhovnog suda kojima su odobreni upadi; i

[621] Citizen Lab, izvješće o aferi CatalanGate, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. travnja 2022., str. 10.
[622] El País, https://elpais.com/espana/2022-04-27/margarita-robles-sobre-el-espionaje-que-tiene-que-hacer-un-estado-cuando-alguien-declara-la-independencia.html, 27. travnja 2022.
[623] La Vanguardia, https://www.lavanguardia.com/politica/20220505/8245084/cni-aporta-autorizaciones-judiciales-parte-espionaje-catalangate.html, 5. svibnja 2022.
[624] El Periódico de España, https://www.epe.es/es/politica/20220505/frente-comun-pp-vox-cs-13614030, 5. svibnja 2022.

deklasificirati na zahtjev suca dokumente Nacionalnog obavještajnog centra koji se odnose na nadzirane članove pokreta koji zagovara neovisnost Katalonije;

4. reformirati španjolski Zakon o službenim tajnama iz 1968.[625];

5. reformirati pravni okvir Nacionalnog obavještajnog centra[626];

6. odobriti novu Obavještajnu direktivu, u kojoj će se utvrditi obavještajni ciljevi Nacionalnog obavještajnog centra; i

7. ažurirati strategiju nacionalne sigurnosti iz 2021. i plan kibersigurnosti.

349. Španjolski Visoki sud[627] otvorio je vlastitu istragu nakon što je vlada izjavila da je softver Pegasus korišten za špijuniranje ministara, uključujući predsjednika vlade Sancheza. Sud je u sklopu takozvane istražne komisije za ispitivanje špijuniranja pozvao glavnog izvršnog direktora Grupe NSO, izraelskog poduzeća koje proizvodi špijunski softver Pegasus, i ministra Félixa Bolañosa da svjedoče. Istražni sudac razgovarao je i s bivšom direktoricom Nacionalnog obavještajnog centra Paz Esteban[628] [629] te s ministricom obrane i ministrom unutarnjih poslova, čiji su uređaji isto hakirani. Sud[630] je izraelskoj vladi poslao službeni zahtjev za međunarodnu pravosudnu pomoć tražeći informacije o „različitim aspektima softverskog alata”. Visoki sud ujedno je ukinuo tajnost dokumenata povezanih s predmetom i ukinuo zabranu istraživanja prisluškivanja mobilnih telefona predsjednika vlade Pedra Sáncheza i ministrice obrane Margarite Robles.

ZAKLJUČNE NAPOMENE

350. Španjolska ima neovisan pravosudni sustav s dostatnim zaštitnim mjerama. Međutim, nakon otkrića dviju kategorija meta u Španjolskoj ostaju neka pitanja, na koja bi se moglo odgovoriti donošenjem brzih i temeljitih reformi i njihovom djelotvornom provedbom. Španjolska vlada radi na izmjenama kako bi uklonila nedostatke. Dana 26. svibnja 2022. španjolska vlada najavila je namjeru reformiranja pravnog okvira Nacionalnog obavještajnog centra, ali prijedlog reforme još nije podnesen. Vlada je 1. kolovoza 2022.[631] podnijela zakonodavne izmjene Zakona o službenim tajnama i trenutačno čeka mišljenje Državnog vijeća.

351. Razlozi i opseg špijuniranja Pegasusom i akteri koji stoje iza njega nisu poznati 47

[625] El País, „El Gobierno inicia la reforma de la ley franquista de secretos oficiales”, 5. travnja 2021.
[626] La Moncloa, „Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías”, 26. svibnja 2022.
[627] https://www.reuters.com/world/spanish-court-calls-ceo-israels-nso-group-testify-case-spying-with-pegasus-2022-06-07
[628] https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html
[629] https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations
[630] https://www.theguardian.com/world/2022/may/10/spains-spy-chief-paz-esteban-sacked-after-pegasus-spyware-revelations.
[631] https://www.mpr.gob.es/servicios/participacion/Documents/MAIN%20APL%20Informaci%C3%B3n%20Clasificada.pdf

osoba koje su se našle na meti špijuniranja spomenutih u izvješću Citizen Laba, za koje ostaje nejasno jesu li bile mete nadzora Nacionalnog obavještajnog centra na temelju sudskog naloga odnosno je li neko drugo tijelo dobilo sudski nalog da ih zakonito nadzire. Te bi osobe trebale imati pristup pravdi i trebala bi se pokrenuti istraga kako bi se ti slučajevi razjasnili.

352. Kad je riječ o 18 predmeta u kojima je izdan sudski nalog, ombudsman je provjerio i potvrdio njihovu zakonitost, ali njihovu posebnost, prikladnost, iznimnu prirodu, proporcionalnost i nužnost[632] može potvrditi samo sud.

353. U širem smislu, sudski postupci koje su pokrenuli nadzirani pojedinci ne odvijaju se onoliko brzo koliko bi trebali kako bi se osigurala transparentnost i pristup značajnom pravnom lijeku. Za to je ključna suradnja nadležnih tijela. Kako bi se zajamčila veća jasnoća i doprinos u obliku tehničke stručnosti, mogao bi se pozvati Europol. Uz njegovu bi se podršku osiguralo da se slijedi pravilan forenzički postupak.

I.F Ostale države članice

NIZOZEMSKA

354. U koalicijskom sporazumu nizozemske vlade iz 2017. stoji da nizozemskoj policiji nije dopušteno nabavljati špijunski softver od pružatelja usluga koji svojim proizvodima opskrbljuju „dvojbene režime”, koji se poslije definiraju kao „države koje su počinile teška kršenja ljudskih prava ili međunarodnog humanitarnog prava”. Nizozemska policija obvezna je prije bilo kakve nabave špijunskog softvera zatražiti od pružatelja informaciju je li isporučivao špijunski softver zemljama pod sankcijama EU-a ili UN-a te provjeriti ima li zemlja u kojoj pružatelj ima sjedište mehanizam za kontrolu izvoza u kojem se tijekom postupka izdavanja izvozne dozvole procjenjuju ljudska prava. Ta se procjena periodički ponavlja. Treba napomenuti kako se čini da se to ograničenje primjenjuje samo na slučajeve kada špijunski softver nabavlja policija. Obavještajne službe nisu izričito spomenute. Prema navodima vlade policija upotrebljava softver za hakiranje od 2019., iako vlasti nisu navele koju vrstu softvera upotrebljava[633]. Čini se da Grupa NSO i njezin proizvod, špijunski softver Pegasus, ne zadovoljavaju prethodno navedene standarde. U svakom ih slučaju nisu zadovoljavali prije pooštravanja izvoznog režima u Izraelu u prosincu 2021.[634] Nisu objavljeni podaci o izdacima policije i obavještajnih službi za kupnju i uporabu sustava špijunskog softvera.

355. U Nizozemskoj je 2018. s radom počelo novo tijelo (Toetsingscommissie Inzet Bevoegdheden, TIB) čiji je cilj unaprijed procijeniti zakonitost odobrenja koje vlada daje obavještajnim agencijama za primjenu tehnika nadzora. Nadzor se ne može nastaviti ako TIB utvrdi da je odobrenje nezakonito. TIB nadopunjuje rad glavnog nadzornog tijela, Odbora za reviziju rada obavještajnih i sigurnosnih službi (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD). CTIVD nadzire tekuće aktivnosti nadzora obavještajnih službi nakon što im je izdano odobrenje i

[632] Poglavlje IV., članak 588.a, točka i. Zakona o kaznenom postupku.
[633] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/06/23/ntwoorden-op-kamervragen-over-het-gebruik-van-hacksoftware-zoals-pegasus-in-nederland
[634] https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021

rješava pritužbe.

356. Treba napomenuti da je Grupa NSO mogla poslovati od studenoga 2014. do prosinca 2016. zahvaljujući dvama poduzećima, Shapes 1 BV i Shapes 2 BV, osnovanima u Nizozemskoj u sektoru financijskih holdinga i sektoru inženjerstva i drugog tehničkog dizajna i savjetovanja. Oba su poduzeća likvidirana nakon dvije godine rada[635].

357. Dana 4. listopada 2022. otkriveno je da se nizozemsko Ministarstvo obrane u studenome 2019. spremalo potpisati ugovor s WiSpearom, poduzećem u vlasništvu Tala Diliana, koje je prije toga preuzelo Cytrox, proizvođača špijunskog softvera Predator[636]. WiSpear je pobijedio na natječaju koji je izdalo ministarstvo Nizozemske. Iz razmjene e-poruka nije jasno odnosi li se na Predator ili neki drugi proizvod. Iz objavljenih e-poruka koje su razmijenili ciparsko Ministarstvo energetike, trgovine i industrije i WiSpear postaje jasno da je predstavnik nizozemskog Ministarstva obrane u razdoblju od 13. do 15. studenoga 2019. stupio u kontakt s ciparskim Ministarstvom trgovine kako bi dobio jamstva u pogledu WiSpeara, samo nekoliko dana prije nego što je otkrivena priča o Dilianovu „kombiju sa špijunskim softverom”. Dilian je rekao predstavnici ciparskog Ministarstva trgovine da bi cijenio njezinu brzu pomoć u tom pitanju jer se približava rok za potpisivanje ugovora[637]. Nije jasno je li taj ugovor potpisan i je li nizozemskom Ministarstvu obrane isporučen ikakav špijunski softver.

358. U Nizozemskoj sjedište ima i podružnica poduzeća Cognyte, registrirana kao Cognyte Netherlands B.V. Kao što je vidljivo u izvatku nizozemskog Ministarstva trgovine, jedini dioničar te nizozemske podružnice je poduzeće UTX Technologies sa sjedištem u Cipru. Kao što je opisano u poglavlju „Cipar i industrija špijunskog softvera”, UTX Technologies ima povijest izvoza obavještajnih sustava i sustava za praćenje u Bangladeš i slanja sustava nadzora u države članice EU-a. Uz to, izraelsko poduzeće Verint, u čijem je vlasništvu Cognyte također bio prije nego što se 2021. odvojio, bilo je glavni dobavljač sustava nadzora za nizozemsku policiju[638]. Veze između policije i tog izraelskog dobavljača postale su još jasnije kad je bivši policijski službenik Robert van Bosbeek 2014. preuzeo ulogu direktora poduzeća Cognyte Netherlands B.V.[639] Još jedan direktor te nizozemske podružnice, David Abadi, glavni je financijski direktor izraelskog poduzeća Cognyte Software Ltd, koje je povezano s prodajom špijunskog softvera za presretanje u Mjanmar[640].

359. Mediji su 2. lipnja 2022. izvijestili da je nizozemska obavještajna služba Algemene Inlichtingen- en Veiligheidsdienst (AIVD) koristila Pegasus pri pomaganju policiji da pronađe osumnjičenika za teško kazneno djelo, Ridouana T., koji je postao glavni osumnjičenik za nekoliko ubojstava povezanih s organiziranim kriminalom, trgovinom droge i vođenjem kriminalne organizacije te je uhićen 16. prosinca 2022. u Dubaiju[641].

---

[635] Amnesty International, „Operating from the Shadows: Inside NSO Group’s Corporate Structure” (Rad iz sjene: unutar korporativne strukture Grupe NSO), https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[636] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
[637] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/
[638] „Volkskrant: Achterdeur in het nationale aftapsysteem van de politie, Israëli’s konden meeluisteren”.
[639] Kamer van Koophandel: Bedrijfsprofiel - Cognyte Netherlands B.V. (34139430).
[640] Reuters: „Israel’s Cognyte won tender to sell intercept spyware to Myanmar before coup, documents show” (Dokumenti pokazuju da je izraelsko poduzeće Cognyte pobijedilo na natječaju za prodaju špijunskog softvera za presretanje prije državnog udara).
[641] https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/

Nizozemska vlada odbila je to komentirati. To je značajan slučaj kojem je potrebno posvetiti veću pozornost. Curenja informacija dogodila su se u vrijeme kad su Pegasus i Grupa NSO privlačili mnoštvo kritika javnosti, a uvrštavanje na crnu listu američkog Ministarstva trgovine financijski je naštetilo Grupi NSO. Nizozemska priča o uspješnom hvatanju pojedinca koji je bio jedan od najtraženijih kriminalaca posljednjih godina za to je poduzeće bila dobrodošla pozitivna poruka. Medijsko izvješće temelji se na izjavama četiriju izvora iz AIVD-a. U izvješću se ne spominje njihov motiv za curenje informacija, a čini se i da nije provedena istraga tih curenja, zbog čega se javlja pitanje je li ih odobrila uprava AIVD-a. Međutim, malo je vjerojatno da bi AIVD dopustio da takva priča izađe u javnost bez znanja i odobrenja izraelskih vlasti.

BELGIJA

360. Bivši izraelski obavještajac otkrio je u intervjuu za *The New Yorker* da se belgijska policija u svojem radu služi Pegasusom[642]. Belgijska je policija u svojoj reakciji navela da „ne bi otkrila informacije ni o kakvim tehničkim i/ili tehnološkim sredstvima kojima se služi u svojim istragama i misijama”. Ministar pravosuđa Vincent Van Quickenborne spomenuo je u rujnu 2021. da obavještajne službe „mogu zakonito upotrebljavati Pegasus”, ali je odbio potvrditi da je belgijska obavještajna služba klijent NSO-a ili da se služi bilo kakvim špijunskim softverom protiv počinitelja kaznenih djela[643].

361. Branitelj ljudskih prava iz Zapadne Sahare koji živi u Belgiji El Mahjoub Maliha i kći ruandskog političkog aktivista Paula Rusesabagine Carine Kanimba također su špijunirani softverom Pegasus dok su se nalazili u Belgiji, pa čak i tijekom sastanaka s dužnosnicima belgijske vlade. Napade špijunskim softverom najvjerojatnije su izvršile marokanske odnosno ruandske vlasti. Ruanda je optužena i da je koristila softver Pegasus za špijuniranje kritičara koji žive u egzilu u Belgiji, uključujući istaknute oporbene ličnosti Placidea Kayumbu i Davida Batengu[644]. Belgijska vojna obavještajna služba ADIV otkrila je i da je Ruanda vrlo vjerojatno instalirala Pegasus na pametni telefon belgijskog novinara Petera Verlindena, kritičara ruandskog predsjednika Kagamea, i njegove supruge Marie Bamutese[645]. Ostale belgijske mete uporabe špijunskog softvera uključuju bivšeg predsjednika vlade Charlesa Michela i njegova oca Louisa Michela (tadašnji zastupnik u Europskom parlamentu i bivši povjerenik i ministar vanjskih poslova). Prema navodima belgijskih medija iza napada je stajala marokanska vlada[646].

NJEMAČKA

362. Njemačka tijela koja se služe ili su se služila hakiranjem uključuju Saveznu obavještajnu službu (Bundesnachrichtendienst, BND), vojsku, carinu i policiju. Savezna obavještajna služba je agencija koja se najviše služi hakiranjem te je 2009. već ostvarila

[642] https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens
[643] https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spionagetool-pegasus/10329450.html
[644] https://www.ft.com/join/licence/88bec95c-78fd-4030-9526-a95fbdeb9da8/details?ft-content-uuid=d9127eae-f99d-11e9-98fd-4d6c20050229
[645] https://www.vrt.be/vrtnws/nl/2021/09/17/pegasus-spionageware-op-de-telefoon-van-journalist-peter-verlind/
[646] https://www.knack.be/nieuws/wereld/belgisch-slachtoffer-van-pegasus-spyware-mijn-leven-is-in-gevaar/; https://www.knack.be/nieuws/pegasus-project-macron-en-michel-in-het-vizier-van-marokko/.

nadzor nad 2 500 uređaja[647].

363. U Njemačkoj je uspostavljen pravni okvir koji regulira uporabu špijunskog softvera. Njemačkim saveznim zakonom policiji su od 2008. dodijeljene ovlasti hakiranja pod pokroviteljstvom države u slučajevima međunarodnog terorizma i za sprečavanje terorističkih napada[648], a 2017. stupio je na snagu novi zakon kojim je svakom tijelu kaznenog progona dopušteno da se služi hakiranjem pod pokroviteljstvom države za 42 kaznena djela. Ta kaznena djela među ostalim uključuju podnošenje lažnih zahtjeva za azil, utaju poreza i kaznena djela povezana sa zlouporabom droga[649]. Njemački parlament donio je 2021. nacrt zakona savezne vlade „o prilagodbi zakona za zaštitu ustava". Tom se promjenom ozakonjuje provedba hakiranja pod pokroviteljstvom države u svih 19 njemačkih obavještajnih službi[650] i propisuje obveza pružatelja komunikacijskih usluga da surađuju s državom u aktivnostima hakiranja[651].

364. Zakoni o hakiranju u Njemačkoj često se opravdavaju u svjetlu slučajeva kaznenih djela protiv seksualnog samoodređenja, dječje pornografije, osnivanja kriminalnih organizacija i ubojstva. Međutim, većina istraga u kojima je policija upotrijebila alate za hakiranje nije bila povezana s prethodno navedenim kaznenim djelima[652]. Najnoviji podaci iz 2020. pokazuju da je njemačka policija dobila odobrenja za 48 hakiranja. Provela je samo 22 hakiranja, od kojih nijedno nije bilo povezano s borbom protiv terorizma i ubojstvima[653].

365. U rujnu 2021. objavljeno je da je Njemački savezni ured kriminalističke policije (BKA) nabavio Pegasus krajem 2020. Važno je napomenuti da se u njemačkom pravu razlikuju dva oblika uporabe špijunskog softvera[654]: pristup svim informacijama (Online-Durchsuchung[655]) i pristup samo komunikaciji koja se odvija uživo (Quellen-TKÜ[656]). Budući da je izvorni softver Pegasus imao mogućnost pristupa svim informacijama na uređaju, a ne samo komunikacijama koje se odvijaju uživo, Njemački savezni ured kriminalističke policije bi uporabom tog softvera kršio zakon. Od značajne presude njemačkog Saveznog ustavnog suda donesene 2008. svaki špijunski softver kojim se koristi policija mora ispunjavati standarde za nadzor telekomunikacija i internetski

---

[647] Europski parlament, saslušanje Njemačke; https://www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html.

[648] https://web.archive.org/web/20171008044948/https://www.gesetze-im-internet.de/bkag_1997/__20k.html

[649] https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0528

[650] https://www.bundestag.de/dokumente/textarchiv/2021/kw23-de-verfassungsschutzrecht-843408

[651] https://netzpolitik.org/2020/staatstrojaner-provider-sollen-internetverkehr-umleiten-damit-geheimdienste-hacken-koennen/

[652] Europski parlament, saslušanje Njemačke.

[653] Quellen-TKÜ (članak 100.a Zakona o kaznenom postupku) odobren je 25 puta i proveden 14 puta, a Online-Durchsuchung (članak 100.b Zakona o kaznenom postupku) odobren je 23 puta i proveden 8 puta. Podaci preuzeti s: https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_TKUE_2020.pdf?__blob=publicationFile

[654] https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html

[655] https://www.gesetze-im-internet.de/stpo/__100b.html

[656] https://www.gesetze-im-internet.de/stpo/__100a.html

nadzor utvrđene za Njemački savezni ured kriminalističke policije[657] [658]. Stoga je Njemački savezni ured kriminalističke policije zatražio od Grupe NSO da napiše izvorni kod kojim bi Pegasus imao pristup samo onim informacijama koje su dopuštene zakonom. NSO je to u početku odbio[659]. Pristao je tek nakon novih pregovora, pa je BKA nabavio izmijenjenu inačicu softvera[660]. Iako to nije javno potvrđeno, tadašnja potpredsjednica Njemačkog saveznog ureda kriminalističke policije Martina Link potvrdila je kupnju izmijenjene inačice na sastanku iza zatvorenih vrata Odbora za unutarnje poslove u njemačkom parlamentu[661]. Ona je navodno u uporabi od ožujka 2021. U inačici koju je kupio Njemački savezni ured kriminalističke policije određene su funkcije bile blokirane radi sprečavanja zlouporabe, iako nije jasno kako to funkcionira u praksi. BKA je sastavio izvješće o toj izmijenjenoj inačici, međutim, ono je i dalje označeno kao povjerljivo[662]. Njemački savezni ured kriminalističke policije je organizacijama civilnog društva uskratio pristup ugovorima s poduzećima koja se bave špijunskim softverom dok ih sud na to nije prisilio, no čak je i tada omogućio pristup samo znatno redigiranim verzijama ugovora[663]. Unatoč dvama pozivima odbora PEGA Njemački savezni ured kriminalističke policije nije mogao prisustvovati nijednom saslušanju zbog preklapanja s rasporedom.

366. U listopadu 2021. otkriveno je i da je njemačka vanjska obavještajna služba, Savezna obavještajna služba (Bundesnachrichtendienst, BND), kupila izmijenjenu inačicu Pegasusa, iako je ta kupnja bila povjerljiva[664]. Savezna vlada je u odgovoru na parlamentarno pitanje navela da je uporaba Pegasusa dopuštena samo u pojedinim predmetima i da mora biti u skladu sa strogim pravnim uvjetima utvrđenima u njemačkom Zakonu o kaznenom postupku (StPO), Zakonu o ograničenjima tajnosti pošte i telekomunikacija (Zakon G-10) i Zakonu o Njemačkom saveznom uredu kriminalističke policije (BKAG), ali nije mogla dodatno komentirati njegovu uporabu zbog sigurnosnih razloga (Geheimhaltungsbedürftigkeit)[665].

UPORABA ŠPIJUNSKOG SOFTVERA

367. Njemački savezni ured kriminalističke policije i berlinska policija kupili su 2012. i 2013. neovisno jedno o drugome softver FinSpy od poduzeća FinFisher. Njemački savezni ured kriminalističke policije je i u ovom slučaju, kao i u slučaju Pegasusa, naložio proizvođaču da razvije špijunski softver FinFisher tako da on ne može pristupiti

[657] „The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware”, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf
[658] *Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung*, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf?__blob=publicationFile
[659] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197
[660] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197
[661] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197
[662] https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-prufbericht-zur-pegasus-software/
[663] Iskaz Andrea Meistera, saslušanje Njemačke, sastanak Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor u Poljskoj, 14. studenoga 2022. https://netzpolitik.org/2022/finfisher-vertrag-wir-haben-das-bka-verklagt-und-gewonnen/

[664] https://www.sueddeutsche.de/politik/pegasusprojekt-nso-pegasus-bundesnachrichtendienst-1.5433974
[665] https://dserver.bundestag.de/btd/19/322/1932246.pdf

svim podacima na uređaju, već samo komunikacijama koje se odvijaju uživo, kako bi bio usklađen s njemačkim pravom. Njemački savezni ured kriminalističke policije nastavio je testirati nove inačice špijunskog softvera FinFishera kako bi se on upotrebljavao samo na „pravno siguran i tehnički čist način” te je Savezno ministarstvo unutarnjih poslova odobrilo njegovu uporabu tek 2018. Iste je godine otkrivena i uporaba softvera FinFisher protiv oporbenih stranaka u Turskoj, iako Njemačka od 2015. nije izdala izvoznu dozvolu za izvoz softvera za nadzor u treće zemlje[666]. Međutim, ugovor između FinFishera i berlinske policije dotad je već istekao, stoga ona nikad nije upotrijebila taj softver. Njemački savezni ured kriminalističke policije nije dodatno komentirao uporabu softvera FinFisher u svojim operacijama ni je li ugovor i dalje valjan[667].

368. Savezni ministar unutarnjih poslova osnovao je 2017. Središnji ured za informacijsku tehnologiju u sigurnosnom sektoru (ZITiS) radi olakšavanja vladina istraživanja i razvoja alata za hakiranje te kupnje alata za hakiranje od komercijalnih dobavljača[668]. Dana 6. travnja 2022. objavljeno je da je Središnji ured za informacijsku tehnologiju u sigurnosnom sektoru u potrazi za drugim dostupnim tehnologijama nakon što je osramoćeni proizvođač špijunskog softvera FinFisher proglasio stečaj[669]. Među ostalim, objavljeno je da se od 2019. pet puta sastao[670] s talijanskim poduzećem za nadzor RCS Lab, ali kupnja alata od tog poduzeća nije dokazana[671]. Središnji ured za informacijsku tehnologiju u sigurnosnom sektoru sastao se i s austrijskim poduzećem DSIRF[672] i izraelskim poduzećima Quadream[673] i Candiru[674] te je ocijenio njihove proizvode špijunskog softvera.

369. U siječnju 2023. u televizijskoj emisiji *Tagesschau* objavljeno je da je Središnji ured za informacijsku tehnologiju u sigurnosnom sektoru u kontaktu i s poduzećem Intellexa ili njegovom podružnicom Cytrox, premda nije jasno je li špijunski softver Predator u konačnici i kupljen. Bivši koordinator tajnih službi Bernd Schmidbauer navodno je djelovao kao predstavnik za proizvode Intellexe. Schmidbauer je prema e-porukama iz studenoga 2021. bio u kontaktu s bivšim predsjednikom Saveznog ureda za informacijsku sigurnost Arneom Schönbohmom kako bi dogovorio sastanak s Intellexom. U veljači 2022. Schmidbauer je stupio u kontakt i s predsjednikom Središnjeg ureda za informacijsku tehnologiju u sigurnosnom sektoru radi prezentacije Intellexe. Osim toga, Schmidbauer je komunicirao i s potpredsjednikom Saveznog ureda za zaštitu ustava (BfV), uslijed čega je Intellexa početkom srpnja 2022. navodno održala prezentaciju osoblju te institucije. Vlada nije komentirala sastanke koji su bili

[666] „The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware”, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf
[667] https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/
[668] https://www.zitis.bund.de/DE/Home/home_node.html
[669] https://www.intelligenceonline.com/surveillance--interception/2022/04/06/after-finfisher-s-demise-berlin-explores-cyber-tool-options,109766000-art
[670] Odgovor na parlamentarno pitanje zastupnice iz Stranke ljevice Martine Renner, https://dserver.bundestag.de/btd/20/038/2003840.pdf
[671] https://netzpolitik.org/2022/rcs-lab-hackerbehoerde-trifft-sich-mehrmals-mit-staatstrojaner-hersteller/
[672] https://dserver.bundestag.de/btd/20/001/2000175.pdf#page=12
[673] https://dserver.bundestag.de/btd/20/001/2000104.pdf#page=29
[674] https://dserver.bundestag.de/btd/20/003/2000327.pdf

posljedica Schmidbauerovih kontroverznih aktivnosti lobiranja[675]. Schmidbauer se 2021. sastao i s Janom Marsalekom, koji je povezan s poduzećem DSIRF[676].

MALTA

370. Nekoliko ključnih osoba trgovine špijunskim softverom registriralo je poduzeća na Malti ili ishodilo malteške putovnice, no čini se da zapravo ne borave ondje i da njihova poduzeća nisu aktivna. Dosad je identificirano nekoliko ključnih osoba trgovine špijunskim softverom.

371. Tal Dilian je izraelski državljanin i bivši izraelski vojnik. Osnivač je poduzeća Intellexa i živi u Cipru. Ishodio je malteško putovnicu 2017.[677] Ujedno je suvlasnik poduzeća MNT Investments LTD na Malti[678].

372. Anatoly Hurgin je rusko-izraelski državljanin i bivši izraelski vojni inženjer. Ishodio je malteško putovnicu 2015.[679] Osnivač je poduzeća Ability Ltd, koje je surađivalo s Grupom NSO na Pegasusu te je upravljalo mrežnom stranom operacija NSO-a[680]. U trenutku predaje zahtjeva za malteško putovnicu već je bio predmet istrage američkih i izraelskih vlasti zbog raznih zločina[681]. Istraživačka novinarka Daphne Caruana Galizia, koja je ubijena u listopadu 2017., pisala je o njemu u kolovozu 2016.[682] Komisija za vrijednosne papire i burzu SAD-a istraživala je 2017. poduzeće Ability Ltd zbog navodnog laganja o stanju financija te je ono skoro isključeno iz kotacije burze NASDAQ[683]. Hurgin je navodno vlasnik poduzeća pod nazivom UAB „Communication technologies" u Litvi, koje pruža „usluge veza i telekomunikacijske usluge"[684].

373. Felix Bitzios je direktor poduzeća Baywest Business Europe Ltd sa sjedištem u Malti[685]. Bivši je vlasnik i zaposlenik Intellexe te je bio uključen u slučaj prijevare

[675] https://www.tagesschau.de/investigativ/swr/predator-spionage-software-101.html. https://dserver.bundestag.de/btd/20/050/2005061.pdf
[676] https://www.tagesschau.de/investigativ/swr/wirecard-marsalek-schmidbauer-101.html
[677] Registar naturaliziranih/registriranih državljana Malte 2017., objavljeno 21. prosinca 2018., https://www.gov.mt/en/Government/DOI/Government%20Gazette/Government%20Notices/PublishingImages/Pages/2018/12/GovNotices2112/Persons%20naturalised%20registered%20Gaz%2021.12.pdf
[678] https://mlt.databasesets.com/company-all/company/73006; https://happenednow.gr/to-neo-logismiko-kataskopias-predator-kai-oi-douleies-stin-ellada/.
[679] https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429
[680] https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=543a981a3997; https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/.
[681] https://www.euractiv.com/section/all/short_news/mep-calls-out-malta-for-selling-passport-to-man-linked-to-pegasus-spyware/
[682] https://daphnecaruanagalizia.com/2016/08/owner-israeli-phone-surveillance-hacking-software-intelligence-operation-buys-maltese-passporteu-citizenship/
[683] https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/.
[684] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
[685] https://offshoreleaks.icij.org/nodes/55071906

Piraeus/Libra[686].

374. Stanislaw Szymon Pelczar pravni je zastupnik poduzeća Baywest Business Europe Ltd, registriranog u Malti, i bivši upravitelj poduzeća Krikel. Spomenut je u Rajskim dokumentima[687].

375. Peter Thiel američki je državljanin rođen u Njemačkoj koji je 2011. ishodio novozelandsko državljanstvo unatoč tome što nije boravio ondje. Podnio je zahtjev za malteško zlatnu putovnicu 2022. (nedugo nakon što su Kurz i Hulio najavili osnivanje zajedničkog novoosnovanog poduzeća)[688]. Osnivač je PayPala i kontroverznog poduzeća Palantir (povezanog sa skandalom Cambridge Analytica). Sponzor je Donalda Trumpa i prvi vanjski ulagač u Facebook. Angažirao je Sebastiana Kurza (koji je nedavno osnovao poduzeće sa Shalevom Hulijem, bivšim direktorom NSO-a) kao stratega[689].

FRANCUSKA

METE U FRANCUSKOJ

376. Pegasus Project otkrio je 2021. nekoliko slučajeva pokušaja hakiranja špijunskim softverom Pegasus u Francuskoj[690]. Skup podataka koji je procurio uključivao je telefonski broj predsjednika Emmanuela Macrona i telefonske brojeve 14 članova njegova ureda[691] [692]. Nalazi forenzičkih analiza francuskih državnih obavještajnih službi potvrdili su da su telefoni ministra obrazovanja Jean-Michela Blanquera, ministrice teritorijalne kohezije Jacqueline Gourault, ministra poljoprivrede Juliena Denormandieja, ministrice stanovanja Emmanuelle Wargon i ministra vanjskih poslova Sébastiena Lecornua bili zaraženi špijunskim softverom Pegasus[693]. Bio je zaražen i telefon člana parlamenta Adriena Quatennensa[694].

377. Registar u koji je Pegasus Project ostvario uvid navodno je sadržavao i telefonske brojeve drugih francuskih državljana, među ostalim novinara, bivših političara i njihovih članova obitelji. Francuska agencija za računalnu sigurnost (Agence nationale de la sécurité des systèmes d'information) potvrdila je zaraze Pegasusom mobilnih uređaja direktora pariške radiopostaje TSF Jazz Brune Delporta, bivšeg ministra

---

[686] https://www.haaretz.com/israel-news/tech-news/2022-04-19/ty-article/israeli-predator-spyware-found-in-phone-of-top-greek-investigative-reporter/00000180-6565-dc5d-a1cd-757f069c0000
[687] https://offshoreleaks.icij.org/nodes/55071906
[688] https://www.nytimes.com/2022/10/15/technology/peter-thiel-malta-citizenship.html
[689] https://www.politico.eu/article/austria-former-chancellor-sebastian-kurz-palantir-technologies-silicon-valley-peter-thiel/
[690] The Guardian, „Pegasus spyware found on journalists' phones, French intelligence confirms" (Francuska obavještajna služba potvrdila je da je špijunski softver Pegasus nađen na telefonima novinara).
[691] The Guardian, Spyware 'found on phones of five French cabinet members'. (Špijunski softver „nađen na telefonima pet francuskih ministara").
[692] Euractiv, France's Macron targeted in project Pegasus spyware case. (Francuski predsjednik Macron bio je meta u slučaju špijuniranja softverom Pegasus).
[693] The Guardian, „Spyware ‚found on phones of five French cabinet members'" (Špijunski softver „nađen na telefonima pet francuskih ministara").
[694] https://www.google.com/url?q=https://www.bfmtv.com/politique/cible-par-le-logiciel-espion-pegasus-le-depute-insoumis-adrien-quatennens-annonce-deposer-plainte_AV-202107210122.html&sa=D&source=docs&ust=1674591349575339&usg=AOvVaw2rgujnaWzoVapS7ZbiH4-r

Arnauda Montebourga, istraživačkih novinara Edwyja Plenela i Lénaïg Bredoux te neimenovanog novinara televizijske kuće France 24[695]. Na meti Pegasusa našla se i Claude Mangin, supruga političkog zatvorenika pripadnika naroda Sahrawi u Maroku Naâme Asfarija[696], i pariški odvjetnik Joseph Breham, branitelj nekoliko aktivista pokreta Polisario Front za neovisnost Zapadne Sahare[697].

378. Čini se da Maroko stoji iza brojnih napada na novinare i političare u Francuskoj[698], među ostalim na marokanske novinare koji ondje žive u egzilu, točnije istraživačkog novinara Hichama Mansourija, koji je 2016. pobjegao od neprekidnog maltretiranja marokanskih vlasti, i neovisnog novinara Aboubakra Jamaïja, koji je napustio Maroko 2007.[699]

379. Francuska je navodno 2021. i sama trebala kupiti softver Pegasus. U vrijeme završnih pregovora s Grupom NSO otkrića da se njezin špijunski softver navodno upotrebljava protiv dužnosnika francuske vlade dovela su do nagle obustave prodaje[700]. Francusko Ministarstvo vanjskih poslova zanijekalo je da je vodilo razgovore s Grupom NSO[701].

380. Predsjednik Nacionalnog odbora za kontrolu obavještajnih tehnika Serge Lasvignes izjavio je na sastanku odbora PEGA održanom 9. siječnja 2023. da je odluka o tome da se uporaba Pegasusa neće odobriti u Francuskoj bila donesena prije otkrića koja je objavio Pegasus Project. Prema Lasvignesu francuske obavještajne službe upotrebljavaju samo proizvode za nadzor izrađene u Francuskoj kako bi se izbjeglo da strani proizvođači špijunskog softvera dobiju pristup informacijama. Međutim, Lasvignes je naveo da tehnička uprava koja proizvodi francuski špijunski softver uvozi određene dijelove iz poduzeća koja se nalaze izvan Francuske[702].

381. Zahtjeve za odobrenje nadzora pojedinaca u Francuskoj najprije treba odobriti glavni direktor službe, a zatim ministar unutarnjih poslova. U konačnici sve zahtjeve mora odobriti predsjednik vlade. Trenutačno se u Francuskoj pod nazorom nalazi 23 000 osoba, a svaku je operaciju odobrio predsjednik vlade. Ako meta želi otkriti je li sada ili nekad u prošlosti bila pod nadzorom, pristup spisu odbija se zbog razloga nacionalne sigurnosti. Osoba može zatražiti potvrdu suca. Međutim, sudac samo može odlučiti je li nadzor bio zakonit, ali ne može obavijestiti metu nadzora o tome jer je to povjerljivo pitanje zbog razloga nacionalne sigurnosti[703]. To znači da je pravo na pravni lijek u praksi beznačajno jer teret dokaza snosi pojedinac i gotovo je nemoguće dobiti ikakve

---

[695] Haaretz, „The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware” (Spis o NSO-u: potpuni (ažurirani) popis pojedinaca koji su se našli na meti špijunskog softvera Pegasus).
[696] Haaretz, „The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware” (Spis o NSO-u: potpuni (ažurirani) popis pojedinaca koji su se našli na meti špijunskog softvera Pegasus).
[697] https://www.middleeasteye.net/fr/entretiens/pegasus-espionnage-maroc-france-macron-sahara-occidental-breham-avocat-mangin-algerie
[698] Radio France, Projet Pegasus: le gouvernement et toute la classe politique française dans le viseur du Maroc.
[699] https://forbiddenstories.org/journaliste/hicham-mansouri/; https://forbiddenstories.org/journaliste/aboubakr-jamai/.
[700] MIT Technology Review, „NSO was about to sell hacking tools to France. Now it’s in crisis” (NSO je Francuskoj trebao prodati alate za hakiranje. Sad je u krizi.).
[701] MIT Technology Review, „NSO was about to sell hacking tools to France. Now it’s in crisis” (NSO je Francuskoj trebao prodati alate za hakiranje. Sad je u krizi.).
[702] Saslušanje pred odborom PEGA, 9. siječnja 2022.
[703] Saslušanje pred odborom PEGA, 9. siječnja 2022.

dokaze od vlasti.

382. Prema brošuri sajma ISS World iz 2013. francusko Ministarstvo unutarnjih poslova, Ministarstvo obrane, Interpol i Veleposlanstvo Toga u Francuskoj sudjelovali su na sajmu ISS World održanom 2012., poznatom i kao „Bal prisluškivača”. Osim toga, popis dobavljača i integratora tehnologije ISS-a pokazuje da su na tom događanju bila prisutna i sljedeća francuska poduzeća koja se bave špijunskim softverom: Advantech, Amesys-Bull, AQSACOM France, Bertin Technologies, BreakingPoint, BULL, COFREXPORT, DataDirect Networks, Ercom, EXFO NetHawk, HALY3, Intersec, IP Solutions, OLEA Partners France, Scan & Target, Thales Communications & Security, Utimaco, VUPEN Security i WAHOUE AND PARTNERS[704].

PODUZEĆA KOJA SE BAVE ŠPIJUNSKIM SOFTVEROM U FRANCUSKOJ

383. U Francuskoj se nalaze različita poduzeća koja se bave špijunskim softverom, a najistaknutija su Nexa Technologies i Amesys. Nexa Technologies, poduzeće koje posluje u okviru grupacije Intellexa Alliance Tala Diliana, francusko je poduzeće za kibernetičku obranu i obavještajne djelatnosti, osnovano 2000.[705] Vode ga bivši voditelji Amesysa. Amesys je osnovan 1979.[706], a poznat je po prodaji programa pod nazivom Cerebro, koji ima mogućnost praćenja elektroničkih komunikacija svojih meta, kao što su e-adrese i telefonski brojevi[707].

384. Amesys je 2007. navodno prodao tu tehnologiju za nadzor telekomunikacija Libiji te ju je Gaddafijev režim upotrebljavao za uhićenje i mučenje kritičara režima. Prema navodima tjednog lista *Telerama* Nexa je osnovana kako bi se provelo rebrendiranje softvera za nadzor i nastavila prodaja Amesysa egipatskom režimu[708]. Poduzeće Nexa Technologies navodno je 2014. egipatskom režimu prodalo sustav za presretanje pod nazivom Eagle. Taj je sustav korišten u vezi sa zadržavanjem i mučenjem političkih protivnika Al-Sisijeva režima[709]. Amesys je uvodio i održavao Eagle od 2007. do 2011.[710]

385. Podneseno je nekoliko pritužbi protiv poduzeća Amesys i Nexa Technologies. Međunarodni savez za ljudska prava (FIDH) i Liga za ljudska prava (LDH) podnijeli su u listopadu 2011. tužbu protiv Amesysa na Visokom sudu u Parizu zbog navodne prodaje proizvoda Libiji[711]. Pet libijskih meta saslušano je u ljeto 2013., a jedna libijska meta saslušana je u prosincu 2015. Kao posljedica novih dokaza da je Gaddafijev režim upotrebljavao Amesysovu tehnologiju za nadzor Amesysu je službeno dodijeljen status osumnjičenika za suučesništvo u mučenju od 2007. do 2011.[712]

---

[704] ISS World, raspored programa za 2013.
[705] Bloomberg, Nexa Technologies Inc.
[706] PitchBook, Amesys.
[707] Le Monde, Vente de matériel de cybersurveillance à l'Egypte : la société Nexa Technologies mise en examen.
[708] ZDNet, „Amesys and Nexa Technologies executives indicted” (Podignuta je optužnica protiv direktora poduzeća Amesys i Nexa Technologies).
[709] Trial International, Amesys (Nexa Technologies).
[710] ZDNet, „Amesys and Nexa Technologies executives indicted” (Podignuta je optužnica protiv direktora poduzeća Amesys i Nexa Technologies).
[711] Trial International, Amesys (Nexa Technologies).
[712] Trial International, Amesys (Nexa Technologies).

386. Francusko računalno poduzeće Bull preuzelo je Amesys 2010. Poduzeće Atos, koje je u to vrijeme vodio Thierry Breton, preuzelo je 2014. Bull, a time je steklo i Amesys[713]. U vrijeme preuzimanja sumnjive aktivnosti Amesysa u smislu trgovine s autoritarnim režimima već su bile dobro poznate. Štoviše, već je bila podnesena i pritužba.

387. U istraživačkom medijskom izvješću objavljenom 2017. otkriveno je da je poduzeće Nexa Technologies 2014. prodalo Egiptu sustave za nadzor, zbog čega su Međunarodni savez za ljudska prava, Liga za ljudska prava i Institut u Kairu za studije ljudskih prava (CIHRS) podnijeli pritužbu protiv tog poduzeća[714, 715].

388. Nakon što je zaprimio nekoliko pritužbi organizacija za ljudska prava, Sud u Parizu podignuo je u lipnju 2021. optužnice protiv četiri direktora poduzeća Amesys i Nexa Technologies zbog prodaje tehnologije za nadzor vladama Libije i Egipta[716]. Zabrinjavajuće je to što je od podnošenja prve pritužbe do pokretanja sudskog predmeta prošlo punih 10 godina. Amesys je u međuvremenu mogao neometano nastaviti svoju djelatnost, uključujući prethodno navedenu prodaju tehnologije za nadzor Egiptu.

389. Unatoč tim kontroverzama francuska agencija Agence Nationale des Titres Sécurisés (ANTS) potpisala je u listopadu 2016. ugovor s Amesysom vrijedan više od 5 milijuna EUR za tehničko upravljanje bazom podataka TES (koja sadržava osobne i biometrijske podatke svih francuskih državljana). Odluka francuskih vlasti da u takav projekt uključe Amesys, koji je tada već bio poznat po svojim praksama, naišla je na kritike. Iako Amesys ne bi imao potpunu kontrolu nad sustavima korištenima za kontroverzni spis baze podataka TES, pomagao bi voditeljima projekata agencije koji rade sa spisom TES, stoga se ne može isključiti da bi imao pristup osobnim podacima. Međutim, direktorica ANTS-a smatrala je da ne postoji pravni prigovor za poslovanje s Amesysom[717].

390. Izdavanje izvoznih dozvola u Francuskoj kontrolira Služba za robu s dvojnom namjenom (SBDU) pri Ministarstvu gospodarstva, industrije i digitalne tehnologije. Uz to, Međuministarska komisija za robu s dvojnom namjenom, kojom predsjeda Ministarstvo europskih i vanjskih poslova, ispituje osjetljiviju robu s dvojnom namjenom. U vrijeme sastavljanja ovog izvješća nisu bile dostupne informacije tome da je francuska vlada izdala izvozne dozvole poduzeću Nexa Technologies.

IRSKA

391. Zbog svojih financijskih propisa Irska je postala država članica u kojoj su registrirana neka od vodećih poduzeća u industriji špijunskog softvera koja su bila umiješana u skandale. *The Currency*, irska internetska izdavačka kuća koja se bavi istraživačkim novinarstvom, otkrila je 20. rujna 2022. da Thalestris Limited, matično društvo Intellexe, kao i sama Intellexa, imaju sjedište u Irskoj i registrirani su u odvjetničkom

[713] L'Obs, „Amesys file un coup de main à l'agence en charge du fichier monstre".
[714] Le Monde, Vente de matériel de cybersurveillance à l'Egypte : la société Nexa Technologies mise en examen.
[715] ZDNet, „Amesys and Nexa Technologies executives indicted" (Podignuta je optužnica protiv direktora poduzeća Amesys i Nexa Technologies).
[716] Amnesty, „Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture" (Podignuta je optužnica protiv direktora poduzeća za nadzor Amesys i Nexa Technologies zbog suučesništva u mučenju).
[717] L'Obs, „Amesys file un coup de main à l'agence en charge du fichier monstre".

društvu u gradu Balbrigganu. Znakovito je da je zahtjev za osnivanje poduzeća Thalestris Limited u Irskoj podnio stručnjak za osnivanje poduzeća u studenome 2019., samo 12 dana nakon što je objavljeno da ciparske vlasti provode kaznenu istragu protiv Diliana i njegovog poduzeća WiSpear. Sam Tal Dilian, glavni izvršni direktor Intellexe, nije naveden u dokumentima irskog poduzeća, ali je njegova druga supruga Sara Hamou navodno navedena kao direktorica i Thalestrisa i Intellexe[718].

392. U objavljenim financijskim izvještajima Thalestrisa za razdoblje do 31. prosinca 2020. navedeno je da postoji 10 drugih podružnica u Grčkoj, Cipru, Švicarskoj i Britanskim Djevičanskim Otocima te da Thalestris nije obvezan plaćati porez na dobit. Primjenjivao je niz fiskalnih odredbi koje primjenjuju i multinacionalna poduzeća koja posluju u Irskoj i stoga je tehnički poslovao s gubitkom[719].

393. Irska vlada odbila je odgovoriti na pitanje jesu li Thalestris ili Intellexa stupili u kontakt s njom ili tijelima kaznenog progona i jesu li se vlada ili tijela kaznenog progona ikad koristili uslugama tih poduzeća, navodeći da „zbog opravdanih operativnih razloga i razloga nacionalne sigurnosti ne bi bilo primjereno komentirati pojedinosti nacionalnih sigurnosnih mjera ni objaviti mjere kibersigurnosti koje primjenjuju vlada ili državni uredi, agencije i tijela koja spadaju pod nadležnost vlade”. Irska vlada odbila je komentirati i irske poveznice sa špijunskim softverom koji proizvode Thalestris i Intellexa[720]. Ne postoje javno poznati dokazi zlouporabe špijunskog softvera u Irskoj.

394. Dnevni list *Haaretz* otkrio je da je korporativno vlasništvo u Irskoj imalo i poduzeće pod nazivom GoNet Systems, koje je sudjelovalo u pružanju usluga Wi-Fi infrastrukture u zračnoj luci Larnaca i koje je bilo povezano s Dilianovim poduzećem WiSpear, a zatvoreno je 2022.[721]

395. U siječnju 2023., nakon primitka pisma zastupnika u Europskom parlamentu Barryja Andrewsa, objavljeno je da će Odbor za pravosuđe irskog parlamenta ispitati postojanje poduzeća u Irskoj koja su uključena u proizvodnju špijunskog softvera. Odbor je izjavio da je razmotrio to pitanje na privatnom sastanku 18. siječnja te je pristao dodati tu temu u svoj program rada za 2023.[722]

396. Treba napomenuti da se irsko pravo trgovačkih društava redovito preispituje i ažurira kako bi se povećala transparentnost poslovnih struktura. Primjeri uključuju Zakon o trgovačkim društvima (Zakon o osnivanju tijela za provedbu zakonodavstva o trgovačkim društvima) iz 2021., kojim je ažuriran provedbeni režim, ažuriranu inačicu tog zakona koja se očekuje 2023. i Zakon o raznim odredbama (Zakon o

---

[718] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-inside-the-predators-irish-lair/

[719] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/

[720] https://thecurrency.news/articles/95068/an-address-in-north-dublin-e20m-in-spyware-sales-and-no-tax-insidethe-predators-irish-lair/

[721] https://www.haaretz.com/israel-news/security-aviation/2022-09-20/ty-article-magazine/.highlight/as-israel-reins-in-its-cyberarms-industry-an-ex-intel-officer-is-building-a-new-empire/00000183-5a07-dd63-adb3-da173af40000?lts=1667755247674

[722] https://www.irishtimes.com/politics/oireachtas/2023/01/29/justice-committee-to-investigate-controversial-spyware-technology-group-with-links-to-ireland/

transparentnosti i registraciji društava s ograničenim partnerstvom i imenima poduzeća) iz 2023. Osim toga, irska vlada najavila je daljnja ulaganja u Nacionalni kibersigurnosni centar (NCSC) radi povećanja njegove sposobnosti aktivnog otkrivanja i uklanjanja kiberprijetnji koje su različitim sredstvima usmjerene na kritičnu infrastrukturu i kritične mreže. Sposobnost Nacionalnog kibersigurnosnog centra da prati i odgovara na incidente povećat će se razvojem Zajedničkog centra za sigurnosne operacije (JSOC) i proširenim analitičkim sposobnostima i sposobnostima izvješćivanja. U tijeku je i rad na izradi tehnološke strategije za Nacionalni kibersigurnosni centar u suradnji s vanjskim savjetnicima[723].

LUKSEMBURG

397. Kako je otkrio Amnesty International u lipnju 2021. i potvrdio luksemburški ministar vanjskih poslova Jean Asselborn, u Luksemburgu se nalazi devet subjekata koji su izravno povezani s Grupom NSO[724]. Činjenica da imena tih devet poduzeća (kao što su Triangle Holdings SA, Square 2 SARL i Q Cyber Technologies SARL), okupljenih pod krovnim društvom za upravljanje i kapitalna ulaganja Novalpina Capital, ne otkrivaju odmah vezu s Grupom NSO pokazuje da netransparentne poslovne strukture u Luksemburgu omogućuju poduzećima da djeluju potpuno izvan javnog pogleda.

398. Nakon što je Amnesty u lipnju 2021. otkrio postojanje devet subjekata NSO-a u Luksemburgu, ministar vanjskih poslova Jean Asselborn svakome je od njih poslao pismo u kojem ih je pozvao da se suzdrže od donošenja odluka koje bi mogle dovesti do nezakonite uporabe robe i tehnologija koje stavljaju na raspolaganje kupcima. Kako navodi LuxTimes, Grupa NSO je odgovorila da izvozi špijunski softver iz Izraela samo uz pristanak izraelske vlade, ali Asselborn je u listopadu 2021. izjavio da to nije mogao potvrditi[725]. U svakom slučaju, prema navodima ministra nijedan od devet subjekata nije imao odobrenje za izvoz proizvoda za kibernadzor iz Luksemburga jer Luksemburg nije izdao nikakve izvozne licence[726]. „Luksemburg ni pod kojim okolnostima neće tolerirati djelatnosti izvoza iz Luksemburga koje pridonose kršenjima ljudskih prava u trećim zemljama te će po potrebi osigurati poduzimanje nužnih mjera kako bi se ispravila kršenja ljudskih prava i spriječila njihova buduća kršenja”, izjavio je Asselborn[727]. Međutim, Grupa NSO još uvijek može poslovati zahvaljujući subjektima sa sjedištem u Luksemburgu, kao što je poduzeće Q Cyber Technologies, koje je odgovorno za pitanja povezana s računima, ugovorima i plaćanjem kupaca njezina softvera[728]. Dana 24. kolovoza 2022. otkriveno je da je u prethodne dvije godine Grupa NSO dogovorila više od polovine prodaja svojih proizvoda u Luksemburgu, što jasno ukazuje na činjenicu da Luksemburg funkcionira kao važno poslovno središte Grupe

[723] https://www.kildarestreet.com/wrans/?id=2022-12-15a.199&s=cyber+security#g201.r
[724] https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[725] https://www.luxtimes.lu/en/luxembourg/government-cannot-verify-pegasus-export-claims-616eead9de135b9236b1efcc
[726] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e
[727] https://delano.lu/article/nine-nso-entities-in-luxembour
[728] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e

NSO[729].

399. U listopadu 2021. predsjednik vlade Xavier Bettel potvrdio je da je Luksemburg kupio i upotrebljavao Pegasus „zbog razloga državne sigurnosti”[730].

ITALIJA

400. Dosad nije bilo nikakvih navoda o mogućoj kupnji špijunskog softvera od strane talijanskih vlasti. Nema prijavljenih slučajeva špijuniranja na visokoj razini iako je telefonski broj bivšeg predsjednika Vlade i predsjednika Komisije Romana Prodija bio na popisu koji je objavio Pegasus Project[731]. Prodi je mogao biti zanimljiva meta za Maroko kao bivši posebni izaslanik UN-a za područje Sahela, s obzirom na njegovu moguću mrežu istaknutih osoba u Zapadnoj Sahari i Alžiru.

401. Poduzeća koja se bave špijunskim softverom Tykelab i RCS Lab odabrala su Italiju kao bazu za poslovanje.

402. Drugo poduzeće koje je nudilo agresivni softver za neovlašteni ulazak iz Italije najmanje od 2012. bilo je Hacking Team, a danas se zove Memento Labs. Poduzeće je postalo poznato nakon hakiranja koje je otkrilo prodaju u nekoliko autoritarnih zemalja koje su nastavile koristiti RCS špijunski softver za napad na političke disidente, novinare i branitelje ljudskih prava. Istraga koju su pokrenule nevladine organizacije i istražitelji UN-a o izvozu RCS špijunskog softvera u Sudan konačno je navela talijanske vlasti da nametnu odredbu „primjenjivu na sve” prema talijanskom zakonu o izvozu zbog zabrinutosti za ljudska prava, pa je poduzeće moralo zatražiti pojedinačnu dozvolu za svaki izvoz. Ne samo da je Hacking Team odbio surađivati tijekom istrage, nego je i iskoristio svoje bliske odnose s višim dužnosnicima u vladi, obavještajnim službama i organima za provođenje zakona u Italiji kako bi se pozicionirao kao sredstvo nacionalne sigurnosti, te je na kraju izvršio pritisak na Ministarstvo gospodarskog razvoja da mu ponovno odobri opću dozvolu za izvoz[732].

AUSTRIJA

403. U odgovoru na pismena pitanja koja je postavio austrijski parlament, Austrijska Savezna Vlada navela je da Austrija nije NSO-ov klijent[733]. Međutim, bivši austrijski kancelar Sebastian Kurz blisko je povezan s osnivačem Grupe NSO, a DSIRF, veliki pružatelj špijunskog softvera, ima sjedište u Austriji.

404. Nakon ostavke, g. Kurz je kasnije angažiran kao globalni strateg za Thiel Capital, u

---

[729] https://www.luxtimes.lu/en/business-finance/pegasus-firm-nso-booked-most-sales-through-luxembourg-6303754ade135b9236e0870b

[730] https://www.luxtimes.lu/en/luxembourg/tax-voting-rights-housing-watch-bettel-video-highlights-6176e835de135b923682378d

[731] https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.

[732] **1a** https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/;
https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/.

[733] Odgovori bivšeg ministra unutarnjih poslova Karla Nehammera zastupniku u Nacionalnom vijeću Nikolausu Scheraku, 22. rujna 2021., referentni br. 2021-0.580.421.

vlasništvu milijardera Petera Thiela[734]. G. Kurz i Shalev Hulio (osnivač Grupe NSO) pokrenuli su u listopadu 2022. poduzeće za kibernetičku sigurnost pod nazivom Dream Security[735]. Iako je g. Hulio odstupio s mjesta izvršnog direktora Grupe NSO u kolovozu 2022., Dream Security i NSO usko su povezani kroz razne osobne i poslovne veze. Jedan od njegovih ulagača, Adi Shalev, također je bio rani ulagač u NSO. Gil Dolev još je jedan od članova osnivača poduzeća Dream Security. Dolevova sestra Shiri Dolev predsjednica je Grupe NSO. Shalev Hulio prethodno je kupio jedno od poduzeća[736] Gila Doleva.

405. Operateri su u srpnju 2022. upotrebljavali špijunski softver austrijske tvrtke DSIRF za hakiranje odvjetničkih društava, banaka i konzultantskih tvrtki u Austriji, Panami i Ujedinjenom Kraljevstvu. Prema Microsoftovim istraživačima, DSIRF-ov alat „Subzero" upotrebljavao je napad iskorištavanjem ranjivosti nultog dana za pristup povjerljivim informacijama, kao što su lozinke i druge vjerodajnice[737]. U listopadu 2022. Savezno ministarstvo rada i gospodarstva reklo je da nije upoznato s bilo kakvim zahtjevima DSIRF-a za izvozne dozvole i da u posljednjih 10 godina nije podnesen nijedan zahtjev za izvoz „softvera za neovlašteni ulazak"[738]. Budući da nije izdana izvozna dozvola za DSIRF-ov softver, Ured javnog tužitelja u Beču pokrenuo je preliminarnu istragu zbog sumnje na nezakoniti pristup računalnom sustavu prema austrijskom zakonu.

ESTONIJA

406. Estonija je navodno isto tako bila zainteresirana za kupnju špijunskog softvera Pegasus od Grupe NSO. Početni pregovori između Estonije i Grupe NSO odigrali su se 2018., nakon čega je Estonija uplatila predujam za dogovoreni posao sa softverom za nadzor, vrijedan 30 milijuna USD[739].

407. Međutim, godinu dana kasnije, ruski dužnosnik iz resora obrane obavijestio je Izrael o namjeri Estonije da koristi špijunski softver Pegasus na ruskim telefonskim brojevima. Ova informacija navela je izraelsko Ministarstvo obrane da onemogući Estoniju da špijunira bilo koji ruski uređaj u cijelom svijetu, navodeći da bi dogovoreni posao bio štetan za izraelsko-ruske odnose[740]. Slučaj Estonije naglašava da špijunski softver Pegasus nije samo oružje za nadzor, već služi i kao politička valuta u diplomatskim odnosima.

LITVA

[734] https://www.bloomberg.com/news/articles/2021-12-30/billionaire-thiel-gives-austria-s-former-wunderkind-a-job.
[735] https://www.spiegel.de/netzwelt/web/sebastian-kurz-und-ex-nso-chef-gruenden-it-sicherheitsfirma-dream-security-a-4482132c-9faf-4be3-927a-86560ba28670.
[736] https://www.timesofisrael.com/former-nso-ceo-ex-chancellor-of-austria-establish-new-cybersecurity-startup/.
[737] U studiji pod nazivom „Pegasus i vanjski odnosi EU-a", Europski parlament, Glavna uprava za unutarnju politiku, Resorni odjel C – prava građana i ustavna pitanja, 25. siječnja 2023., str. 52; Microsoft (2022), Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits.
[738] https://www.parlament.gv.at/dokument/XXVII/AB/11698/imfname_1473647.pdf.
[739] The New York Times, „Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia", 23. ožujka 2022.
[740] The New York Times, „Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia", 23. ožujka 2022.

408. Poduzeće iz Litve, UAB Communication Technologies, koje posluje u djelatnosti „usluga veza i telekomunikacijskih usluga” u vlasništvu je Anatolya Hurgina, rusko-izraelskog državljanina i bivšeg izraelskog vojnog inženjera koji je razvio Pegasus zajedno s NSO-om[741]. Osim toga, Hurgin je ishodio malteško zlatnu putovnicu 2015[742].

BUGARSKA

409. U Bugarskoj Ministarstvo gospodarstva, konkretnije Međuministarska komisija za kontrolu izvoza i neširenje oružja masovnog uništenja, kontrolira izvoz i izvozne dozvole za proizvode koji su klasificirani kao proizvodi „s dvojnom namjenom” u Uredbi EU-a o robi s dvojnom namjenom[743]. Nikola Stojanov trenutačni je ministar gospodarstva i industrije[744]. Bugarske vlasti da su izdale izvozne dozvole Grupi NSO ili njezinim podružnicama.[745]. Međutim, Novalpina Capital, bivši privatni vlasnik udjela u Grupi NSO, naglasio je da se NSO-ovi proizvodi izvoze iz EU-a i iz Cipra i iz Bugarske[746] [747] [748]. Te su dvije tvrdnje proturječne. Nadalje, u medijima su objavljene tvrdnje da se neki od poslužitelja mrežne infrastrukture preko kojih napada Pegasus nalaze u bugarskom podatkovnom centru u vlasništvu bugarskog poduzeća. Vlasnici poduzeća su Grupa NSO, Circles Bulgaria i Magnet Bulgaria, koji su od vlasti dobili izvozne dozvole. Ta podružnica Grupe NSO iz Bugarske pruža usluge istraživanja i razvoja ciparskim podružnicama, a izvozi mrežne proizvode za vlade[749]. Poduzeće Magnet trenutno nije aktivno, ali poduzeće Circles još uvijek je aktivno i dobilo je izvoznu dozvolu koja vrijedi do 25 travnja 2023[750].

410. Ured državnog odvjetnika Grada Sofije pokrenulo je istragu u veljači 2022. kako bi utvrdio jesu li državne službe nezakonito koristile špijunski softver Pegasus za nadziranje bugarskih građana. Istraga je u tijeku[751]. U predmetu *Ekimdzhiev i dr. protiv Bugarske*, ESLJP je utvrdio u siječnju 2022. da postojeći zakoni u Bugarskoj o tajnom nadzoru, zadržavanju i pristupu komunikacijama ne ispunjavaju zahtjeve kvalitete prava iz Konvencije i zatražio je da vlada izvrši potrebne izmjene domaćeg zakona kako bi se prekinulo kršenje[752].

I.G Institucije EU-a

---

[741] https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
[742] https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.
[743] Republika Bugarska, Ministrarstvo gospodarstva i industrije, Međuministarska komisija za kontrolu izvoza i neširenje oružja masovnog uništenja.
[744] Vijeće ministara Republike Bugarske.
[745] Politico, „Pegasus makers face EU grilling. Here’s what to ask them”, 21. lipnja 2022.
[746] Amnesty International, „Novalpina Capital’s response to NGO coalition’s open letter”, 18. veljače 2019.
[747] Access Now, „Is NSO Group’s infamous Pegasus spyware being traded through the EU?’”, 12. rujna 2019.
[748] https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/.
[749] Amnesty International, „Operating From the Shadows: Inside NSO Group’s Corporate Structure”.
[750] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuseruploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK.
[751] https://bnr.bg/en/post/101599684/sofia-city-prosecutor-s-office-investigates-possible-use-of-pegasus-spyware-in-bulgaria.

[752] Ekimdzhiev i dr. protiv Bugarske, Zahtjev br. 70078/12, presuda od 11. siječnja 2022, koja je dostupna na: https://hudoc.echr.coe.int/fre?i=001-214673.

411. Reuters je 11. travnja 2022. izvijestio da su povjerenik za pravosuđe Didier Reynders i najmanje četvero članova osoblja Komisije bili mete softvera Pegasus u rujnu 2021.[753] Apple je 23. studenoga 2021. poslao službene obavijesti na uređaje povjerenika Reyndersa i „dodatnih članova osoblja Komisije" u kojima ih obavještava da su bili „mete napadača koje sponzorira država" i da su njihovi uređaji možda ugroženi[754].

412. Nakon ovih otkrića, povjerenik Reynders pozvan je da razgovara s Odborom PEGA 30. svibnja 2022., a odgovorio na njegova pitanja i pisanim putem. Nakon otkrića koja su objavili Forbidden Stories i Amnesty International, Komisija je još 19. srpnja 2021. oformila „posebni tim internih stručnjaka za provođenje interne istrage" kako bi „provjerio jesu li uređaji osoblja Komisije i članova Kolegija bili na meti napada Pegasusom"[755]. Osim toga, Komisija je u rujnu 2021. na sve službene telefone uvela mobilno rješenje za „prepoznavanje krajnjih točaka i odgovor" (eng. endpoint detection and response (EDR)).

413. Komisija je tijekom istrage priopćila da, „ni ... prije ni nakon ovog datuma [23. studenoga 2021.]' ove provjere nisu potvrdile da su osobni ili službeni uređaji povjerenika Reyndersa bili ugroženi. Nadležne službe Komisije pregledale su i uređaje ostalih djelatnika koji su isti dan primili slične obavijesti od Applea, ali „jednako tako niti jedan od pregledanih uređaja nije potvrdio Appleove sumnje"[756].

414. Međutim, u svojem pismu od 9. rujna 2022., Komisija je priznala da je tijekom tekuće istrage o tome je li Komisija na meti napada Pegasusom, „nekoliko provjera uređaja dovelo do otkrića pokazatelja ugroženosti". Komisija još nije pojasnila dosadašnje nalaze istrage javno ili unutar Odbora PEGA jer bi se time „njezinim protivnicima otkrile Komisijine metode i mogućnosti istrage, čime bi sigurnost institucije bila ozbiljno ugrožena"[757]. Komisija nije potvrdila neslužbena izvješća o više od 50 otkrivenih zaraza.

415. U odgovoru na pitanje Odbora PEGA koji bi akter ili akteri mogli stajati iza ovih napada, Komisija je odgovorila da je „nemoguće je pripisati te pokazatelje određenom počinitelju s potpunom sigurnošću". Međutim, vladavina prava je zajedničko sveobuhvatno pitanje kojim se bavi dvoje dužnosnika Komisije za koje znamo da su bili mete špijunskog softvera, povjerenik Reynders i članica ureda povjerenice Věre Jourove[758]. U odgovoru na pitanje odbora PEGA o mogućoj vezi, Komisija odbija podijeliti dodatne informacije o broju odjela koji su mogli biti ugroženi, o zanimanjima pogođenog osoblja ili bilo koje dodatne informacije koje bi bile od interesa za rad odbora PEGA i kojima bi se moglo utvrditi podrijetlo napada te navodi da „ne raspolaže s dovoljno informacija da bi mogla donositi definitivne zaključke o vezi između

[753] https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/.
[754] Odgovor povjerenika Hahna i Reyndersa izvjestiteljici od 25. srpnja 2022.; Odgovor povjerenika Hahna i Reyndersa odboru PEGA od 9. rujna 2022.
[755] Odgovor povjerenika Hahna i Reyndersa izvjestiteljici od 25. srpnja 2022.
[756] Odgovor povjerenika Hahna i Reyndersa odboru PEGA od 9. rujna 2022.
[757] https://pro.politico.eu/news/148627.
[758] https://pro.politico.eu/news/148627.

geolokacije i mogućeg pokušaja zaraze uređaja putem Pegasusa”[759].

416. S obzirom na prethodno navedeno, može se utvrditi nekoliko problema. Prvo, Komisija nije pokazala dovoljnu svijest i razumijevanje golemih političkih rizika uključenih u činjenicu da je netko meta špijunskog softvera. Svaki pokušaj hakiranja Komisije ili njezinog člana, bez obzira na to je li bio uspješan ili ne, vrlo je ozbiljna politička činjenica koja utječe na integritet postupka demokratskog odlučivanja. Komisija je u komunikaciji s odborom PEGA opetovano objašnjavala da hakiranje uređaja povjerenika Reyndersa softverom Pegasus nije uspjelo. Međutim, kao što je sama Komisija spomenula, „nekoliko provjera uređaja [osoblja] dovelo je do otkrića pokazatelja ugroženosti”, o čemu nije bilo daljnje komunikacije. To naizgled ukazuje na to da Komisija umanjuje ozbiljnost činjenice da je napadnuta Institucija EU-a.

417. Drugo, čini se da nije bilo dovoljno kapaciteta IT-a i sposobnosti za zaštitu povjerenika i osoblja od napada ili za nadzor i provjeru njihove kibernetičke sigurnosti. Iako je Komisija uvela nove mjere, kao što je rješenje EDR, na svim telefonima Komisije i kontinuirano surađuje sa CERT-EU-om[760], zbog nedostatka informacija koje je odbor PEGA dobio od Komisije, nije jasno koliko su mjere Komisije za analizu prethodnih napada špijunskog softvera bile su uspješne i u u kojem će opsegu provedene mjere biti dostatne u budućnosti.

418. Treće, Komisija nije službeno izvijestila o obavijestima ili pokazateljima ugroženosti belgijskoj policiji radi daljnje istrage, već je samo bila u kontaktu s belgijskom policijom u vezi s „tehničkim detaljima” u sklopu svoje „redovne suradnje”. Komisija je izjavila da „relevantni IT odjeli Komisije primaju više puta svakog dana takve obavijesti” i da one stoga ne zahtijevaju službenu prijavu policiji. Prema Komisiji, budući da Appleova obavijest nije signalizirala „definitivnu zarazu, već mogući pokušaj zaraze odgovarajućeg uređaja zlonamjernim softverom”, Komisija nije poduzela daljnje korake s tijelima za provođenje zakona[761].
Međutim, u drugim slučajevima, primjerice u Španjolskoj i Francuskoj, pokrenuta je kaznena istraga o korištenju špijunskog softvera protiv ministara i šefova država. Špijunski softver uglavnom koriste državni akteri, navodeći razloge nacionalne sigurnosti. Komisija tvrdi da su „neki aspekti povezani s nacionalnom sigurnošću izvan nadležnosti Komisije”[762], ali ne uspijeva objasniti kako bi povjerenici i osoblje Komisije zaista mogli predstavljati rizik za nacionalnu sigurnost.

419. Četvrto, činjenica da Komisija nije odboru PEGA dala značajne informacije, bilo iza zatvorenih vrata, o tome da je na meti, ili, općenito, bilo kakve osnovne informacije u vezi s istragom, znači da Parlament nije mogao ispravno vršiti demokratski nadzor. Komisija bi trebala ponovno procijeniti koje informacije može otkriti kako bi omogućila smislen parlamentarni nadzor.

ČLANOVI EUROPSKOG PARLAMENTA, VIJEĆA I KOMISIJE NA METI ŠPIJUNSKOG SOFTVERA

420. Ne samo da su na meti bili jedan sadašnji član Komisije i drugo osoblje Komisije, već

[759] Odgovor povjerenika Hahna i Reyndersa odboru PEGA od 9. rujna 2022.
[760] Odgovor povjerenika Hahna i Reyndersa odboru PEGA od 9. rujna 2022.
[761] Odgovor povjerenika Hahna i Reyndersa odboru PEGA od 9. rujna 2022.
[762] Odgovor povjerenika Hahna i Reyndersa izvjestiteljici od 25. srpnja 2022.

su i vladini čelnici, ministri i bivši povjerenik također navodno bili meta špijunskog softvera iz područja izvan i unutar Unije.

421. Telefonski broj francuskog predsjednika Macrona pojavio se na popisu potencijalnih meta inicijative Pegasus Project, a španjolska vlada potvrdila je da su telefoni španjolskog premijera Pedra Sancheza, ministrice obrane Margarite Robles i ministra unutarnjih poslova Fernanda Grande-Marlaske bili zaraženi Pegasusovim špijunskim softverom, navodno iz područja izvan Unije.

422. Prema grčkom dnevniku Documento, koji je objavio opsežan popis osoba na čijim su uređajima navodno pronađeni tragovi Predatora[763], na meti špijunskog softvera bili su Dimitris Avramopoulos, europski povjerenik u razdoblju 2014. 2019. i nekoliko aktualnih ministara u Vladi, uključujući ministre vanjskih poslova i financija. . Nije jasno je li Avramopoulos bio meta navodnih pokušaja hakiranja u vrijeme dok je bio član Komisije niti je jasno tko je stajao iza njih. Međutim, dug popis osoba koje su bile na meti uključuje brojne grčke političare kako iz vladajuće stranke tako i iz oporbe.432.
Ove potvrđene i navodne infekcije i pokušaji hakiranja pokazuju da je moguće da su sadašnji vladini čelnici i ministri, te sadašnji ili bivši povjerenici, uključujući njihovu komunikaciju s kolegama, meta s područja izvan ili unutar Unije dok su članovi Europskog vijeća, Vijeća i Komisije. Stoga bi jedan zaraženi telefon također mogao ozbiljno ugroziti informacije koje posjeduju institucije, uključujući informacije koje se dijele tijekom sastanaka Komisije i Vijeća u stvarnom vremenu.

I.H Treće zemlje

423. Sljedeći odjeljak će istaknuti opseg u kojem je upotreba Pegasusa ili jednakovrijednog špijunskog softvera za nadzor, koji izravno ili neizravno uključuje subjekte povezane s EU-om, pridonijela nezakonitom špijuniranju novinara, političara, službenika tijela kaznenog progona, diplomata, odvjetnika, poslovnih ljudi, aktera civilnog društva, branitelja ljudskih prava ili drugih aktera u trećim zemljama. To uključuje opseg u kojem je primjena špijunskog softvera dovela do kršenja ljudskih prava koja izazivaju ozbiljnu zabrinutost u pogledu ciljeva zajedničke vanjske i sigurnosne politike EU-a te je li uporaba špijunskog softvera bila u suprotnosti s vrijednostima sadržanima u članku 21. UEU-a i u Povelji, uz dužno poštovanje i vodećih načela Ujedinjenih naroda o poslovanju i ljudskim pravima i drugim pravima sadržanim u međunarodnom pravu o ljudskim pravima.

424. Od trećih zemalja povezanih sa špijunskim softverom, Izrael i Maroko dobili su posebnu pozornost odbora PEGA, sa saslušanjem i misijom u Izraelu u srpnju 2022. i sastankom posvećenom Maroku u veljači 2023. tijekom saslušanja na temu geopolitike špijunskog softvera. Osim toga, saslušanje u kolovozu 2022. bilo je djelomično posvećeno Ruandi, uz izjavu Carine Kanimbe, koja je bila meta Pegasusa.

IZRAEL

425. Odbor PEGA posjetio je Izrael u srpnju 2022. Glavni cilj putovanja bio je susret s

[763] Documento, izdanje od 6. studenoga 2022.

proizvođačem špijunskog softvera Pegasus, Grupe NSO, poduzeća sa sjedištem u Izraelu. Izaslanstvo odbora PEGA saznalo je da je Grupa NSO prodala špijunski softver 14 vlada EU-a, koristeći izvozne dozvole koje je izdala izraelska vlada. Razgovarali su o zloporabama plaćeničkoga alata za nadzor i njihovom utjecaju na demokraciju, vladavinu prava i temeljna prava u EU-u. Odbor se sastao i s predstavnicima vlade, Knesseta, stručnjaka i civilnog društva. Ovaj je posjet naglasio neučinkovitost postojećih zaštitnih mjera protiv zlouporabe špijunskog softvera i potrebu za mnogo strožom regulativom Europske unije o prodaji, kupnji i upotrebi špijunskog softvera. Obavještajne podatke u području kibernetike treba učinkovito regulirati kako bi se spriječila zlouporaba špijunskog softvera u budućnosti.

426. Geopolitička i sigurnosna situacija u Izraelu potaknula je njegovu vladu i privatni sektor da razviju alate za prikupljanje obavještajnih podataka koji bi proširili sposobnosti u pogledu kibersigurnosti zemlje, a posebno u pogledu obrane. Tijekom godina, Izrael je postao jedan od vodećih svjetskih proizvođača naprednih tehnologija nadzora i špijunskog softvera, jer raspolaže stručnim znanjem za razvoj alata za prikupljanje obavještajnih podataka. Industrija izvozi svoje proizvode po cijelom svijetu. U studiji koju je naručio Europski parlament, objavljenoj 2023. pod naslovom „Pegasus i vanjski odnosi EU-a” istaknuto je da „za zemlje izvoznice industrija špijunskog softvera može biti unosan izvor prihoda i sredstvo diplomatskog utjecaja”[764]. To potvrđuju i novinski izvještaji, pri čemu stručnjaci ističu korisnost Pegasusa u uspostavljanju diplomatskih odnosa, npr. sa zaljevskim zemljama[765].

427. Uz domaće strateške razloge, Izrael se uspješno promovirao kao inovativna start-up nacija, s poduzećima s najsofisticiranijom tehnologijom u tom području, kao što su NSO, Cellebrite, Candiru, QuaDream te Intellexa. Procjenjuje se da ukupna prodaja industrije iznosi najmanje 1 milijardu USD godišnje[766], što iznosi oko 0,6 % izraelskog izvoza[767]. Izraelske obrambene snage i obavještajna agencija, posebice njezin odjel za kibernetičku sigurnost Unit 8200, odigrali su bitnu ulogu u uspješnoj izraelskoj špijunskoj industriji, a poduzeća imaju bliske odnose s entitetom. Prema studiji iz 2018., 80 % od 2 300 ljudi koji su osnovali 700 izraelskih kompanija za kibernetičku sigurnost bivši su zaposlenici obavještajnih jedinica izraelskih obrambenih snaga. Jedna od najistaknutijih osoba u industriji je Tal Dilian, vlasnik i osnivač poduzeća Intellexa (pogledajte odjeljak o poduzeću Intellexa i Tal Dilianu)[768].

428. Izraelska poduzeća koja proizvode špijunski softver prodala su tehnologiju nadzora u cijelom svijetu, uključujući zemlje članice EU-a i autoritarne zemlje Zaljeva. Prema dnevniku Haaretz, prodaja Pegasusa korištena je kao diplomatski pregovarački instrument, a olakšala je pregovore za uspostavljanje formalnih diplomatskih odnosa s

[764] „Pegasus i vanjski odnosi EU-a”, Europski parlament, Glavna uprava za unutarnju politiku, Resorni odjel C – prava građana i ustavna pitanja, 25. siječnja 2023.
[765] https://www.france24.com/en/livenews/20210719-pegasus-scandal-showsrisk-of-israel-s-spy-tech-diplomacyexperts.
[766] https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.
[767] https://en.globes.co.il/en/article-israels-exports-rise-sharply-in-2022-1001433699#:~:text=According%20to%20a%20conservative%20estimate,a%20then%20record%20%24144%20billion.
[768] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106.

Marokom, Bahreinom i, formalno, Ujedinjenim Arapskim Emiratima u skladu s Abrahamovom sporazumu[769]. Prodaja špijunskog softvera autoritarnim režimima bila je kritizirana, osobito nakon inicijative Pegasus Project. Kao rezultat toga, izraelska je vlada u prosincu 2021. postrožila izvozna pravila za opremu za kibernetičko ratovanje. S obzirom na planirane reforme pravosuđa u Izraelu, Grčka, Cipar i Portugal navodno nude poticaje mnogim izraelskim tehnološkim tvrtkama da presele svoje poslovanje u te zemlje. Prema medijskim izvješćima, te tri zemlje navodno nude izraelskim tehnološkim poduzećima porezne olakšice, dok Grčka navodno daje državljanstvo po ubrzanom postupku[770].

429. Prema riječima stručnjaka, spremnost Izraela da testira nove sustave nadzora na Palestincima na okupiranim teritorijima stvara poticaje za poslovni model u industriji nadzora, od čega je i NSO imao koristi[771]. Kao rezultat toga, zemlje koje od Izraela nabavljaju špijunski softver „obučen na terenu" pridonose kršenju ljudskih prava u gore navedenim regijama. Države članice EU-a, kao neki od najprestižnijih klijenata NSO-a, stoga su u izravnoj suprotnosti s programom vanjske i sigurnosne politike EU-a u pogledu podrške ljudskim pravima i demokraciji[772].

430. Meta NSO-ovog špijunskog softvera Pegasus bilo je palestinsko civilno društvo, uključujući šest palestinskih branitelja ljudskih prava[773]. Čini se da je upotreba špijunskog softvera za nadzor u slučaju Ubaija Al-Aboudija, izvršnog direktora Centra za istraživanje i razvoj Bisan, i Salaha Hammourija, koji ima dvojno francusko-palestinsko državljanstvo, odvjetnika i terenskog istraživača u Udruzi za podršku zatvorenicima i ljudskim pravima Addameer, rezultiralo njihovim administrativnim pritvorom. Nadzor svih šest osoba podudara se s vrlo kontroverznim proglašenjem šest palestinskih organizacija za ljudska prava „terorističkim", što je izazvalo međunarodni protest koji je osudio odluku izraelske vlade. Ovaj primjer nadzora palestinskih branitelja ljudskih prava još je jedan dokaz nedostatka provedbe NSO-ove politike ljudskih prava[774], koju je poduzeće upotrebljavalo za jačanje svog legitimiteta i vjerodostojnosti pri prodaji državama članicama EU-a.

431. Treba napomenuti da je Komisija surađivala s izraelskim vlastima povezano s izvješćima o zlouporabi NSO-ovog špijunskog softvera Pegasus čime se krše ljudska prava. U pismu odboru PEGA od 9. rujna 2022., Komisija je odgovorila da je s izraelskim izvoznim tijelima razgovarala o zabrinutostima zbog moguće zlouporabe i „tražila naznake o svim povezanim mjerama ublažavanja koje bi nadležna izraelska

[769] Haaretz (2022) „Netanyahu Used NSO's Pegasus for Diplomacy", https://www.haaretz.com/israelnews/2022-02-05/tyarticle/.premium/netanyahu-used-nsospegasus-for-diplomacy-now-he-blames-itfor-his-downfall/0000017f-e941-dc91- a17f-fdcd55c80000.
[770] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106.
[771] Misija odbora PEGA u Izraelu, od 18. do 20. srpnja 2022.
[772] U skladu s većinom nalaza godišnjeg izvješća Komisije za 2021. o primjeni Povelje EU-a o temeljnim pravima, pod naslovom „Zaštita temeljnih prava u digitalnom dobu", EU je dužan olakšati rad branitelja ljudskih prava na internetu.
[773] https://www.frontlinedefenders.org/en/statement-report/statement-targetingpalestinian-hrds-pegasus; https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/.
[774] https://www.amnesty.org/en/latest/researc h/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/.

tijela za kontrolu izvoza mogla poduzeti u budućnosti”. U vrijeme pisma, Komisija nije primila takve naznake od nadležnih izraelskih tijela za kontrolu izvoza, ali se namjeravala „vratiti na pitanje mogućih mjera ublažavanja na sljedećem sastanku Pododbora za industriju, trgovinu i usluge Sporazuma o pridruživanju između EU-a i Izraela”.

MAROKO

432. U brojnim novinskim izvješćima dokumentirana je navodnu raširenu upotrebu špijunskog softvera u Maroku. S licencom za oko 100 000 telefonskih brojeva, Maroko se može smatrati jednim od NSO-ovih najvećih klijenata za Pegasus[775]. Maroko je opovrgnuo optužbe vezane uz Pegasus Project navodeći da su „pogrešne”. U izvješću organizacije Citizen Lab iz prosinca 2020. otkriveno je da je Maroko jedan od 25 kupaca podružnice grupe NSO Circles[776].

433. Otkrića su pokazala i da je unutar zemlje nadzor sa špijunskim softverom navodno upotrebljavan za hakiranje i naknadno zastrašivanje novinara i aktivista[777]. U nedavnoj rezoluciji o nadzoru i zatvaranju istraživačkog novinara Omara Radija, Europski parlament osudio je kontinuirano pravosudno uznemiravanje novinara koje provodi marokanska vlada i pozvao je marokanske vlasti da „prestanu s nadzorom novinara, uključujući i putem NSO-ovog špijunskog softvera Pegasus”[778]. Jedan od ciljanih pojedinaca, Ignacio Cembrero, istraživački novinar španjolskog dnevnika El Confidential, pojavio se pred odborom PEGA 29 studenog 2022. Postao je svjestan da mu je telefon hakiran nakon što su SMS poruke između njega i španjolske vlade objavljene u marokanskom dnevniku. Kad je španjolski sud zatražio suradnju izraelskih vlasti, odbile su pružiti dodatne informacije koje bi pomogle slučaju.

434. Maroko je također progonio marokanske novinare Hichama Mansourija i Aboubakra Jamaima[779], koji su u egzilu u Francuskoj, kao i pristaše Zapadne Sahare, uključujući odvjetnika obrane Josepha Brehama koji živi u Parizu i branitelja ljudskih prava iz Sahravija El Mahjouba Malihu koji živi u Belgiji[780].

435. Maroko je pokrenuo nekoliko sudskih postupaka kao odgovor na optužbe o umiješanosti u upotrebu Pegasusa u Francuskoj, Španjolskoj i Njemačkoj. U Francuskoj su marokanske vlasti podnijele tužbe zbog klevete protiv nekoliko medijskih kuća i organizacija civilnog društva, uključujući Le Monde, Forbidden Stories, Radio France, Mediapart, L’Humanité i Amnesty International. Pariški Kazneni sud odbacio je predmete kao nedopuštene 25. ožujka 2022., a marokanske vlasti podnijele su žalbu na odluku. U Španjolskoj su marokanske vlasti pokrenule postupak protiv novinara Ignacia Cembrera na temelju srednjovjekovne klauzule u Kaznenom zakonu, optužujući ga za „radnju hvaljenja”. Predmet je u tijeku, a osuđen je kao pokušaj da se Cembrero i drugi

[775] https://www.npr.org/2022/05/11/1098368201/a-spying-scandal-and-the-fate-of-western-sahara.
[776] https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.
[777] https://daraj.media/en/76202/.
[778] Rezolucija Europskog parlamenta od 19. siječnja 2023. o položaju novinara u Maroku, posebno o slučaju Omara Radija, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0014_HR.html.
[779] Forbidden Stories. https://forbiddenstories.org/journaliste/hicham-mansouri/, https://forbiddenstories.org/journaliste/aboubakr-jamai/.
[780] https://www.middleeasteye.net/fr/entretien s/pegasus-espionnage-maroc-francemacron-sahara-occidental-brehamavocat-mangin-algerie.

odvrate od izvještavanja o upotrebi špijunskog softvera u Maroku[781].

436. Prema novinskom izvješću, prije široke upotrebe Pegasusa, Maroko je osim toga bio klijent najmanje tri europska dobavljača špijunskog softvera, a to su francuska poduzeća Amesys i Vupen[782] te talijansko poduzeće Hacking Team. Prema povjerljivim dokumentima, Maroko je bio treći najveći klijent talijanskog poduzeća i platio je više od 3 milijuna EUR tijekom šest godina za kupnju RCS softvera poduzeća Hacking Team za svoje domaće Vrhovno vijeće za nacionalnu obranu (CSDN) i Upravu za teritorijalni nadzor (DST)[783]. Više UN-ovih odjela i službi na visokoj razini nadzirano je pomoću špijunskog softvera.

437. Maroko ne samo da je nabavio špijunski softver u EU-u, već mu je Europska komisija pružila i tehnološku i financijsku potporu. Prema platformi Der Spiegel, Maroko je od EU-a primio dva špijunska sustava za špijuniranje pojedinaca u svrhu granične kontrole (špijunski softver XRY francusko-libanonskog poduzeća MSAB i špijunski softver Detective američkog poduzeća Oxygen Forensics)[784]. Osim toga, Agencija Europske unije za osposobljavanje u području izvršavanja zakonodavstva (CEPOL) poslana je u Maroko kako bi provela obuku uživo o tome kako koristiti špijunski softver i naučiti policiju kako izvući informacije s profila društvenih medija putem društvenog hakiranja[785]. Za razliku od Pegasusa, navedeni špijunski softver može samo fizički ući u uređaje i ne ostavlja nikakve tragove upotrebe. Izvješće opisuje više slučajeva u kojima su pametni telefoni oduzeti metama, među kojima su novinari i aktivisti, te vraćeni s nagovještajima o mogućoj zarazi. Iako nije moguće provjeriti jesu li treće strane pravilno koristile špijunski softver, nije bilo naznaka da je Komisija provjerila ispravnu upotrebu dostavljenih tehnologija. Odražavajući sličnu situaciju opisanu u pritužbi pučkom pravobranitelju EU-a o financiranju tehnologija nadzora u okviru programa EUTFA (vidjeti relevantni odjeljak u nastavku), Komisija nije provela procjenu učinka kako bi mapirala moguću zlouporabu isporučenih tehnologija. Komisija je izjavila da je na korisniku, Maroku, da postavi špijunski softver odgovorno i u skladu s ugovornim sporazumom (tj. samo u svrhe navedene u ugovoru)[786].

OSTALE TREĆE ZEMLJE

438. Na globalnoj razinie najmanje 75 zemalja kupilo je i/ili upotrebljavalo špijunski softver, uključujući represivne režime[787]. Organizacije za ljudska prava dokumentirale su brojne incidente u kojima je špijunski softver zloupotrijebljen za nadziranje političara, novinara, odvjetnika, branitelja ljudskih prava i drugih aktivista civilnog društva koji

[781] https://www.middleeastmonitor.com/20220705-morocco-files-lawsuit-against-spain-journalist-who-reported-use-of-pegasus-spyware/.
[782] https://moroccomail.fr/2022/09/21/morocco-used-hacking-team-to-spy-on-the-un/.
[783] https://privacyinternational.org/blog/1394 /facing-truth-hacking-team-leak-confirms-moroccan-government-use-spyware; https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.
[784] https://www.spiegel.de/ausland/marokkowie-die-eu-rabatsueberwachungsapparat-aufruestet-ad3f4c00e-4d39-41ba-be6c-e4f4ba65035; https://disclose.ngo/en/article/how-the-eu-supplied-morocco-with-phone-hacking-spyware.
[785] https://privacyinternational.org/longread/4289/revealed-eu-training-regimeteaching-neighbours-how-spy.
[786] https://disclose.ngo/en/article/how-theeu-supplied-morocco-with-phonehacking-spyware.
[787] Carnegie Endowment for International Peace, „Global Inventory of Commercial Spyware & Digital Forensics", 11. siječnja 2023, https://carnegieendowment.org/programs/democracy/commercialspyware.

promiču ljudska prava, prava žena i zaštitu okoliša[788].

SUDIONIŠTVO DRŽAVA ČLANICA EU-A, KAO KLIJENATA NSO GRUPE, U ZLOUPORABI PEGASUSA U TREĆIM ZEMLJAMA

439. Vlasti 14 zemalja koje nisu članice EU najvjerojatnije su odgovorne za mnoge slučajeve u kojima su nadzirane osobe identificirane, a zaraza je tehnički dokazana. U pitanju su Salvador, Meksiko, Tajland, Maroko, Indija, Ruanda, Saudijska Arabija, Bahrein, Jordan, Kazahstan, Togo, UAE, Izrael i Azerbajdžan[789].

440. Pegasus Project, suradnja više od 80 novinara iz 17 medijskih kuća, dokumentirao je kako su Pegasus upotrebljavale represivne vlade kako bi ušutkale novinare, napale aktiviste i ugušile neslaganje. Istrage koje je proveo Pegasus Project pokazale su da su članovi obitelji saudijskog novinara Jamala Khashoggija bili na meti špijunskog softvera Pegasus prije i nakon što su ga saudijski agenti ubili u Istanbulu 2. listopada 2018., unatoč opetovanom poricanju NSO grupe. Security Lab organizacije Amnesty International utvrdio je da je špijunski softver Pegasus uspješno instaliran na telefon Khashoggijeve zaručnice Hatice Cengiz samo četiri dana nakon njegova ubojstva. Njegova supruga Hanan Elatr također je više puta bila meta špijunskog softvera između rujna 2017. i travnja 2018., kao i njegov sin Abdullah, koji je odabran kao meta zajedno s drugim članovima obitelji u Saudijskoj Arabiji i UAE[790].

441. Nadalje, Pegasus Project dokumentirao je da su novinari česte mete Pegasus špijunskog softvera. U Meksiku je telefon novinara Cecilija Pinede odabran za nadzor samo nekoliko tjedana prije njegova ubojstva 2017. Pegasus je upotrebljavan i u Azerbajdžanu, zemlji u kojoj je ostalo samo nekoliko neovisnih medija. Prema istrazi, više od 40 azerbajdžanskih novinara odabrano je kao potencijalne mete. Security Lab organizacije Amnesty International otkrio je da je telefon Sevinca Vaqifqizija, slobodnog novinara neovisnog medija Meydan TV, bio zaražen u razdoblju od dvije godine zaključno sa svibnjem 2021. U Indiji je najmanje 40 novinara iz gotovo svih velikih medija u zemlji odabrano kao potencijalne mete između 2017. i 2021. Forenzički testovi otkrili su da su telefoni Siddhartha Varadarajana i MK Venua, suosnivača neovisnog internetskog medija The Wire, bili zaraženi špijunskim softverom Pegasus još u lipnju 2021.[791]

442. Branitelji ljudskih prava i dalje su česte mete, uključujući i vlasti sljedećih zemalja: Meksiko, Salvador, Maroko, Ruanda, Izrael, Jordan, Saudijska Arabija, Bahrein, Ujedinjeni Arapski Emirati, Indija, Kazahstan, Indonezija i Bjelarus[792]. Frontline

[788] Forensic Architecture, Amnesty International i The Citizen Lab, „Digital Violence”, https://www.digitalviolence.org/#/.
[789] https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.
[790] Amnesty International, „Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally”, 19. srpnja 2021., https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/.
[791] Amnesty International, „Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally”, 19. srpnja 2021., https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/.
[792] https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/; https://www.amnesty.org/en/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/.

Defenders objavio je 2021. izvješće u kojem je dokumentiran ciljani nadzor branitelja ljudskih prava u raznim zemljama uključujući Indiju. 16 branitelja ljudskih prava zatvoreno je u lipnju 2018. u skladu s indijskim protuterorističkim zakonodavstvu u predmetu nazvanom Bhima Koregaon, a odnosi na nasilje koje se dogodilo u Bhima Koregaonu. Jedan od branitelja ljudskih prava, 84-godišnji isusovački svećenik Stan Swamy, umro je u pritvoru u srpnju 2021.[793] Istraga digitalne forenzike otkrila je da su „dokazi" na koje se tužiteljstvo oslanjalo protiv grupe bili podmetnuti pomoću špijunskog softvera Pegasus na uređaje koji pripadaju braniteljima ljudskih prava Roni Wilson i Surendri Gadling te da nema dokaza da su branitelji ljudskih prava bili u interakciji[794].

II. Industrija špijunskog softvera

443. Europska unija privlačno je mjesto za trgovinu tehnologijama za nadzor i uslugama nadzora, uključujući alate špijunskog softvera. S jedne strane, potencijalni su kupci vlade država članica. S druge strane, pojam usklađenosti s propisima EU-a služi kao referentna vrijednost koja može dobro doći na globalnom tržištu. Unutarnje tržište EU-a nudi slobodu kretanja i povoljne nacionalne porezne sustave. Pravila kojima se regulira nabava mogu se izbjeći pozivanjem na nacionalnu sigurnost, a vlade se mogu koristiti opunomoćenicima ili posrednicima, zbog čega je javnim tijelima vrlo teško otkriti i dokazati kupnju špijunskog softvera. EU ima stroga pravila izvoza, ali odnedavna postoji trend da ih države članice zaobilaze i nastoje ostvariti konkurentsku prednost nepravilnom nacionalnom provedbom. Nadalje, Europska komisija ih je često neodgovarajuće provodila. Zapravo, svaki put kad je u Izraelu pooštren režim izvoznih dozvola, nekoliko poduzeća preselilo je svoje izvozne odjele u Europu, posebno na Cipar[795] [796]. Osim toga, nekoliko osoba iz industrije špijunskog softvera steklo je državljanstvo neke od država članica EU-a kako bi mogle slobodno poslovati unutar EU-a i iz njega.

444. Nadalje, kao što je Claudio Guarnieri, direktor organizacije Amnesty Tech posvjedočio pred odborom PEGA, europska poduzeća poput njemačkog poduzeća FinFisher i talijanskog poduzeća Hacking Team bila su pioniri u industriji plaćeničkog špijunskog softvera. Prva izvješća o ulogama tih poduzeća u praćenju novinara i gušenju neslaganja pojavila su se prije više od deset godina kada su, s pojavom prosvjedničkih pokreta poznatih kao Arapsko proljeće, iz ureda tajne policije počeli izlaziti ugovori s tim poduzećima[797].

445. Industrija špijunskog softvera ima zamršenu strukturu, izgrađenu na složenoj mreži osoba, lokacija, veza, vlasničkih struktura, fiktivnih trgovačkih društava, korporativnih naziva koji se neprestano mijenjaju, tokova novca, državnih opunomoćenika i

[793] Frontline Defenders (2. prosinca 2021.): Action needed to address targeted surveillance of human rights defenders https://www.frontlinedefenders.org/en/stat ement-report/action-needed-addresstargeted-surveillance-human-rightsdefenders.
[794] The Wire, Rona Wilson's iPhone Infected With Pegasus Spyware, Says New Forensic Report, 17. prosinca 2021., https://thewire.in/rights/rona-wilsonpegasus-iphone-arsenal.
[795] Makarios Drousiotis, „Državna mafija", 2022., Šesto poglavlje.
[796] Haaretz. „Cyprus, Cyberspies and the Dark Side of Israeli Intel".
[797] Saslušanje odbora PEGA 30. kolovoza 2022. o utjecaju špijunskog softvera na građane EU-a, https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/.

posrednika, tajkuna i vlada.

446. U mnogim slučajevima čini se da je oznaka „plaćenički špijunski softver” točna. Kao što pokazuje broj osoba koje su nezakonite mete, mnoga poduzeća zaostaju u pogledu etičkih standarda, jer često prodaju diktaturama i bogatim nedržavnim akterima, a nastavljaju to činiti čak i nakon otkrića inicijative Pegasus Project. Cellebrite je 2021. objavio da će prestati prodavati svoje proizvode ruskoj vladi nakon što se saznalo da je njegov špijunski softver upotrijebljen za nadziranje aktivista koji se protive Putinu. Međutim, u listopadu 2022. postojali znakovi da se ruske vlasti i dalje služe Cellebriteom[798]. To je unosno i neodređeno tržište. Unatoč tomu, oni svoje proizvode mogu prodavati demokratskim vladama u SAD-u i EU-u, što im daje privid respektabilnosti. Unatoč tvrdnjama da je uporaba špijunskog softvera posve zakonita i potrebna, vlade nevoljko priznaju da ga posjeduju. Katkad pribjegavaju angažiranju opunomoćenika, posrednika ili brokera za kupnju špijunskog softvera kako ne bi ostavile tragove. Sajam ISS World Fair, poznat i pod nadimkom „Bal prisluškivača”, veliki je godišnji događaj na kojem se okuplja industrija špijunskog softvera. Godišnje europsko izdanje tog događaja održava se u Pragu. Izlagači na sajmu ISS World Fair u velikoj se mjeri preklapaju sa izlagačima na sajmovima vojne industrije.

447. Osim „službenih kanala”, postoji i crno tržište za ove proizvode. Iako mnogi dobavljači tvrde da prodaju samo vladama, čini se da pokušavaju poslovati i s nedržavnim subjektima. Vrlo je teško pronaći čvrste dokaze, jer ova trgovina ostavlja malo tragova. Grčki dnevnik Documento tvrdi da ima dokaze da se softver prodaje na crnom tržištu i to u iznosu do 50 milijuna USD, ne samo vladama i agencijama za borbu protiv terorizma, već i privatnim osobama[799]. Drugi grčki dnevnik, To Vima, izvijestio je da je Predator kupilo 34 kupaca iz Grčke[800]. Dokumenti koji su procurili pokazuju da je piratska verzija proizvoda koja se službeno prodavala samo vladama bila dostupna po cijeni od 8 milijuna USD, iznos koji je uključivao obuku agenata koji će koristiti program, 24-satnu tehničku podršku i praćenje računa društvenih mreža mete[801].

448. Industrija nudi širok raspon proizvoda i usluga za nadzor i obavještavanje, a ne samo špijunski softver kao jedan proizvod. Špijunski softver samo je jedan alat u kompletu alata hakerskih poduzeća.

Nedostaci

449. Bez nedostataka softvera ne bi bilo moguće instalirati i upotrebljavati špijunski softver. Stoga je za regulaciju špijunskog softvera potrebno regulirati i otkrivanje, dijeljenje i iskorištavanje tih nedostataka[802]. Unatoč tomu što se revidiranom Direktivom o sigurnosti mrežnih i informacijskih sustava (NIS2) i prijedlogom Akta o kiberotpornosti zahtijeva i potiče jačanje obrane digitalnih sustava, gotovo je nemoguće razvijati

---

[798] https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000.
[799] Documento, „Documento’s ‚Predator’ revelations on Euractiv – Europol’s intervention calls for Dutch MEP”.
[800] To Vima, Interceptions „Spy software has 34 customers”.
[801] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/.
[802] Ot van Daalen, intervencija u odboru PEGA, 27. listopada 2022.;
Dokument organizacije EDRi: „Breaking encryption will doom our freedoms and rights”, https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-Encryption.pdf;
https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu.

sustave bez nedostataka.

450. Ranjivosti se stoga moraju otkriti i popraviti što je prije moguće. Međutim, trenutni zakon EU-a potiče suprotno od otkrivanja podataka. Prema Direktivi o kibernetičkom kriminalu i Direktivi o autorskim pravima, istraživači informacijske sigurnosti mogu se suočiti s građanskom i kaznenom odgovornošću kada istražuju ranjivosti i dijele svoje rezultate. Nadalje, istraživači nisu obavezni dijeliti svoje nalaze o ranjivostima. Istraživači bi stoga mogli odlučiti prodati svoje znanje o ranjivosti privatnom posredniku u zamjenu za visoku naknadu.

451. Ova praksa je stvorila živahnu i unosnu trgovinu ranjivostima. Međutim, nisu samo posrednici u ranjivostima nultog dana ti koji traže ranjivosti. Sigurnosna tijela i tijela kaznenog progona jednako tako skupljaju ranjivosti: neke su pronašli njihovi vlastiti stručnjaci, a neke su im pribavili posrednici. Ako se ranjivosti ne prijave, one se ne zakrpaju, ostavljajući IT sustave oslabljene, a korisnike nezaštićene. To omogućuje nastavak upotrebe špijunskog softvera.

Telekomunikacijske mreže

452. Pružatelji telekomunikacijskih usluga imaju značajnu ulogu u procesu špijuniranja, kako zakonitog tako i nezakonitog. Živimo u modernom dobu umjetne inteligencije, tehnologije velikih podataka i kvantnog računalstva, ali istovremeno upotrebljavamo međunarodni komunikacijski protokol pod nazivom Signalling System No 7 (SS7) i u velikoj mjeri ovisimo o njemu. Taj je protokol razvijen 1975. te je i danas u upotrebi. Radi se o sustavu koji kontrolira način na koji se telefonski pozivi usmjeravaju i naplaćuju te omogućuje napredne značajke poziva i SMS-a (usluge kratkih poruka)[803]. Putem mreže SS7 moguće je presretati telefonske pozive i SMS poruke, utvrditi geolokaciju i zaraziti metu špijunskim softverom poput Pegasusa ili Predatora[804].

453. Rizik da pružatelji telekomunikacijskih usluga zlouporabe pristup tim mrežama je visok. Postoji nekoliko dokumentiranih slučajeva zlouporabe, gdje su pristupne točke (eng. global titles) iznajmljene tvrtkama koje su nadzirale i presretale komunikaciju meta korištenjem napada „preko posrednika”. Prikupili su i geolokacijske podatke i metapodatke u vlastite gospodarske svrhe. Global title je adresa koja se upotrebljava za usmjeravanje poruka unutar SS7. Može se usporediti s IP adresom, jer je global title adresa unutar telekomunikacijskog sustava[805]. Prema zviždaču, to je razlog zašto je NSO bio toliko zainteresiran za pristup mreži SS7 u SAD-u da je pokušao kupiti pristup od njihovog poduzeća[806]. Pružatelji telekomunikacijskih usluga namjerno drže niske standarde industrije kako bi omogućili lakši pristup lokalnim nacionalnim agencijama kaznenog progona.

Grupa NSO

454. Grupa NSO proizvođač je špijunskog softvera Pegasus. Osnovali su je 2010. Shalev

[803] https://www.techtarget.com/searchnetworking/definition/Signaling-System-7#:~:text=SS7 was first adopted as, up to and including 5G.
[804] https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/.
[805] https://www.gms-worldwide.com/glossary/global-title/.
[806] https://www.theguardian.com/news/2022/feb/01/nso-offered-us-mobile-security-firm-bags-of-cash-whistleblower-claims.

Hulio, Omri Lavie i Niv Karmi, a bavi se razvojem tehnologije za pomoć licenciranim vladinim agencijama i agencijama kaznenog progona u otkrivanju i sprečavanju terorizma i kriminala[807]. Špijunski softver Pegasus najpoznatiji je proizvod Grupe NSO. Na globalno tržište izbačen je 2011[808] [809].

455. Od svog pokretanja 2010., Grupa NSO bila je korporativno prisutna u Izraelu, Ujedinjenoj Kraljevini, Luksemburgu, Kajmanskim otocima, Cipru, SAD-u, Nizozemskoj, Bugarskoj i Britanskim Djevičanskim otocima. Još uvijek nedostaju mnoge informacije o ulogama različitih korporativnih subjekata, a neka od tih društava već su likvidirana. Međutim, Grupa NSO u svom je izvješću o transparentnosti i odgovornosti za 2021. navela da su Bugarska i Cipar izvozna središta[810]. Amnesty International navodi da su nizozemski subjekti (likvidirani 22. prosinca 2016.) djelovali su u sektoru financijskih holdinga, dok je Q Cyber Technologies sa sjedištem u Luksemburgu bio aktivan kao komercijalni distributer odgovoran za izdavanje računa, potpisivanje ugovora i primanje uplata od kupaca . Nadalje, poduzeće Westbridge Technologies registrirano u SAD-u možda je poduzeću olakšalo prodaju u SAD-u[811].

456. NSO je navodno imao prihod od 243 milijuna USD u 2020.[812] Međutim, nakon otkrića koja je objavio Pegasus Project, poduzeće se suočilo s nekoliko poteškoća. Tužbe koje su podnijeli Apple[813] i Meta[814] protiv poduzeća, to što je Ministarstvo trgovine SAD-a stavilo NSO na crnu listu, pooštravanje izraelskog izvoznog režima, kritičko ispitivanje u nekoliko zemalja i unutarnje napetosti unutar fonda privatnog kapitala koji stoji iza NSO grupe doveli su do ozbiljnog pada dobiti. U jednom trenutku dug Grupe NSO navodno je bio čak 6,5 puta veći od svojih normalnih godišnjih prihoda[815].

457. Odbor PEGA imao je dva sastanka s NSO grupom, od kojih je jedan održan u Bruxellesu, a jedan u Izraelu. Špijunski softver Pegasus isprva je prodan 22 krajnja korisnika u 14 država članica EU-a, koristeći marketinške i izvozne dozvole koje je izdao Izrael. Ugovori s krajnjim korisnicima u dvije države članice naknadno su raskinuti[816]. Nije potvrđeno koje su države članice uključene u popis od 14 država, niti koje su dvije zemlje uklonjene. Međutim, moglo bi se pretpostaviti da su to Poljska i Mađarska.

KORPORATIVNA STRUKTURA, TRANSPARENTNOST I DUBINSKA ANALIZA

458. Grupa NSO pokrenula je svoje prvo poduzeće 25. siječnja 2010. u Izraelu. To je poduzeće registrirano pod nazivom NSO Group Technologies Limited. Grupa NSO naziv je prvog registriranog poduzeća i krovni naziv za različita poduzeća osnovana u

[807] Grupa NSO. „About us".
[808] The New York Times „The Battle for the World's Most Powerful Cyberweapon".
[809] Hulio S., „NSO Never Engaged in Illegal Mass Surveillance", The Wall Street Journal, 24. veljače 2022.
[810] NSO Group, „Transparency and Responsibility Report 2021".
[811] Amnesty International „Operating From the Shadows – inside NSO Group's Corporate Structure".
[812] Haaretz, „NSO Is Having a Bad Year – and It's Showing".
[813] Apple „Apple sues NSO Group to curb the abuse of state–sponsored spyware".
[814] Bloomberg Law, NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware".
[815] Bloomberg, „Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop".
[816] Odgovori koje je Grupa NSO dostavila tajništvu odbora PEGA nakon saslušanja, 20 srpnja 2022.

drugim nadležnostima. Prvo osnovano poduzeće vlasnik je žiga NSO Group[817].

459. Fond privatnog vlasničkog kapitala Francisco Partners dobio je u ožujku 2014. udio od 70 % u Grupi NSO. U okviru poduzeća Francisco Partners grupa je proširila svoje subjekte na različita područja nadležnosti, uključujući Cipar, Bugarsku, SAD, Nizozemsku i Luksemburg. Tijekom godina pod poduzećem Francisco Partners (2014.–2019.) fond je sustavno revidirao prodaju proizvoda Grupe NSO u okviru Odbora za poslovnu etiku (BEC). Prema poduzeću Francisco Partners, Odbor za poslovnu etiku uskratio je desetke milijuna dolara prodaje koja bi inače bila odobrena u skladu s pravnim zahtjevima[818].

460. Francisco Partners prodao je 14. veljače 2019. cijeli vlasnički udio, uključujući udio u podružnicama, poduzeću Novalpina Capital. Tim otkupom od strane uprave promijenili su se standardi upravljanja, a Odbor za poslovnu etiku zamijenio je Odbor za upravljanje, rizike i usklađenost (GRCC) radi preispitivanja stanja ljudskih prava potencijalnih kupaca[819].

461. U skladu s certifikatom o krajnjoj uporabi/krajnjem korisniku, nakon pooštravanja izraelskog izvoznog režima Grupa NSO uvela je politiku o ljudskim pravima i postupak dubinske analize u području ljudskih prava. Kako je opisano u izvješću o transparentnosti i odgovornosti Grupe NSO za 2021., Grupa NSO zahtijeva da svi ugovori s kupcima uključuju klauzule o poštovanju ljudskih prava i klauzule u kojima se opisuje privremeni ili trajni prestanak uporabe proizvoda Grupe NSO u slučaju zlouporabe povezane s ljudskim pravima. U pisanom podnesku odboru PEGA Grupa NSO potvrdila je da je raskinula ugovore s državama članicama EU-a[820] koje su navodno prekršile klauzule o ljudskim pravima. Grupa NSO nije pojasnila je li ispitala nadzorne dnevnike i jesu li predmetni kupci pristali na ispitivanje. Stoga nije poznato postoji li još uvijek bilo kakav dokaz o zlouporabi, može li Grupa NSO na bilo koji način sačuvati te dokaze niti imaju li izraelske vlasti ikakve dokaze.

462. Prema organizaciji Amnesty International, u izvješću o transparentnosti Grupe NSO nedostaje odgovarajuća korektivna politika za osobe koje su mete nezakonitog nadzora te nema informacija o tužbama koje su u tijeku protiv Grupe NSO[821]. Špijunski softver Grupe NSO i dalje se otkriva na uređajima novinara i kritičara autoritarnih režima, što je u suprotnosti s politikom Grupe NSO o ljudskim pravima i postupkom dubinske analize u području ljudskih prava[822].

NADZOR IZVOZA

463. Budući da je špijunski softver Pegasus klasificiran kao tehnologija s dvojnom

---

[817] Amnesty International, „*Operating from the shadows - inside NSO Group's corporate structure*" (Rad iz sjene – unutar korporativne strukture Grupe NSO).
[818] Amnesty International, „Operating from the shadows - inside NSO Group's corporate structure" (Rad iz sjene – unutar korporativne strukture Grupe NSO).
[819] Saslušanje odbora PEGA s Grupom NSO, 21. lipnja 2022.
[820] Saslušanje odbora PEGA s Grupom NSO, 21. lipnja 2022.
[821] Amnesty International, „NSO Group's new transparency report is ‚another missed opportunity'" (Novo izvješće o transparentnosti Grupe NSO je „još jedna propuštena prilika"), priopćenje za medije, 1. srpnja 2021.
[822] The New York Times, „U.S. Blacklists Israeli Firm NSO Group Over Spyware" (SAD stavlja izraelsku Grupu NSO na crnu listu zbog špijunskog softvera).

namjenom, za njega je potrebna izvozna dozvola. Poduzeća u okviru Grupe NSO pribavljaju izvozne dozvole u Izraelu i Bugarskoj te na Cipru[823]. Grupa NSO sama je to potvrdila, ali poriče da se špijunski softver Pegasus izvozi iz Cipra i Bugarske[824]. Ciparska i bugarska vlada općenito su uskratile izdavanje izvoznih dozvola poduzećima Grupe NSO. Drugi su izvori to osporili navodeći da se podružnice Grupe NSO često skrivaju iza drugog imena u nacionalnim poslovnim registrima. Međutim, jedna od podružnica Grupe NSO na Cipru, koja je poslovala pod imenom „Circles", zatvorila je svoje urede 2020.[825] Dozvole izdaju i izraelske vlasti[826]. Izrael ne sudjeluje u Wassenaarskom aranžmanu, ali navodi da je neke njegove elemente ugradio u nacionalni Zakon br. 5766 o kontroli izvoza proizvoda povezanih s obranom iz 2007.[827] Za izdavanje dozvola za stavljanje na tržište i izvoznih dozvola nadležna je Agencija za kontrolu izvoza proizvoda povezanih s obranom Ministarstva obrane[828]. Nakon otkrića koja je objavio Pegasus Project i uvrštavanja NSO-a na crnu listu, popis država koje ispunjavaju uvjete sužen je sa 102 na 37 država, uz obvezu da svaka od njih potpiše certifikat o krajnjoj uporabi/krajnjem korisniku[829]. Izrael u postupku dubinske analize automatski smatra da su sve države članice EU-a usklađene sa standardima EU-a i ne provodi dodatne procjene za pojedinačne države. Međutim, čini se da odluka o raskidu ugovorâ s dvama državama članicama EU-a upućuje na to da se EU više ne smatra jedinstvenom cjelinom za potrebe dubinske analize.

NEETIČKO POSTUPANJE KOJE JE REZULTIRALO TUŽBAMA, UVRŠTAVANJEM NA CRNU LISTU I SUKOBIMA ULAGAČA

464. Sukob između triju suosnivača poduzeća Novalpina Capital u srpnju 2021. počeo je utjecati na poslovanje Grupe NSO, zbog čega su ulagači konačno odlučili oduzeti kontrolu tom privatnom društvu za kapitalna ulaganja[830]. Berkeley Research Group (BRG), društvo za poslovno savjetovanje iz SAD-a, preuzelo je taj fond privatnog vlasničkog kapitala 27. kolovoza 2021. i pokrenulo kritičke istrage kako bi utvrdilo zakonitost aktivnosti Grupe NSO i njezinu usklađenost s crnim listama SAD-a. Uprava Grupe NSO opstruirala je istragu koju je u svibnju 2022. provodio BRG[831]. Izvršni direktor iz BRG-a naveo je da suradnja s Grupom NSO „praktički više ne postoji" jer Grupa NSO vrši pritisak da se nastavi prodaja proizvoda državama u kojima je stanje

[823] Amnesty International, „Operating from the shadows– inside NSO Group's corporate structure" (Rad iz sjene – unutar korporativne strukture Grupe NSO), str. 62.
[824] Amnesty International, „Operating from the shadows– inside NSO Group's corporate structure" (Rad iz sjene – unutar korporativne strukture Grupe NSO).
[825] VICE, „NSO Group Closes Cyprus Office of Spy Firm" (Grupa NSO zatvara ciparski ured špijunskog poduzeća).
[826] Amnesty International, „Operating from the shadows– inside NSO Group's corporate structure" (Rad iz sjene – unutar korporativne strukture Grupe NSO).
[827] Služba Europskog parlamenta za istraživanja, „Europe's PegasusGate – countering spyware abuse" (Europski PegasusGate – Suzbijanje zlouporabe špijunskog softvera).
[828] Amnesty International, Odgovor poduzeća Novalpina Capital na pismo skupine nevladinih organizacija (15. travnja 2019.) i na pismo organizacije Citizen Lab (6. ožujka 2019.).
[829] Služba Europskog parlamenta za istraživanja, „Europe's PegasusGate – countering spyware abuse" (Europski PegasusGate – Suzbijanje zlouporabe špijunskog softvera).
[830] Financial Times, „Private equity owner of spyware group NSO stripped of control of €1bn fund" (Privatni vlasnik udjela Grupe NSO za špijunski softver izgubio kontrolu nad fondom od 1 milijarde EUR).
[831] Financial Times, „NSO Group keeping owners 'in the dark", manager says" (Grupa NSO drži vlasnike u neznanju, kaže upravitelj).

ljudskih prava sporno[832]. Dvojica bivših glavnih partnera Novalpine podigla su 25. travnja 2022. tužbu protiv BRG-a pred sudom u Luksemburgu, tražeći da se Novalpina Capital ponovno postavi za glavnog partnera i da se suspendiraju sve odluke koje je donio BRG[833]. Sud u Luksemburgu odbacio je te zahtjeve i BRG i dalje upravlja fondom koji kontrolira Grupu NSO[834].

465. Uz sukobe oko vlasništva Ministarstvo trgovine SAD-a uvrstilo je 3. studenoga 2021. Grupu NSO na crnu listu zbog neusklađenosti njezinih aktivnosti s pitanjima vanjske politike i nacionalne sigurnosti SAD-a. Vlada SAD-a zabranjuje izvoz tehnologije Grupi NSO i njezinim podružnicama, što *de facto* znači da nijedno američko poduzeće ne može s njom surađivati[835].

466. Kao odgovor na crnu listu SAD-a Credit Suisse, jedan od vjerovnika Grupe NSO, navodno je natjerao poduzeće da nastavi prodavati špijunski softver Pegasus novim kupcima. U pismu koje je BRG-u uputio Willkie Farr & Gallagher nekoliko je vjerovnika izjavilo da je zabrinuto da BRG sprječava Grupu NSO da „traži i stječe nove klijente". Iako to nije izričito navedeno u pismu, dva stručnjaka za to pitanje navela su da je jedan od vjerovnika Credit Suisse. BRG je odgovorio zajmodavcima da je duboko zabrinut zbog toga što od Grupe NSO zahtijevaju prodaju[836].

467. Nekoliko dana nakon što je SAD uvrstio Grupu NSO na crnu listu, Žalbeni sud Sjedinjenih Američkih Država potvrdio je da se tužba protiv NSO-a koju je podnijela Meta može nastaviti. Odmah nakon toga Apple je podnio pritužbu protiv NSO-a saveznom sudu[837]. Jedan okružni sud u SAD-u odbacio je u lipnju 2022. zahtjev za imunitetom Grupe NSO u tužbi koju je podnio Apple[838]. U vrijeme pisanja ovog dokumenta, tužba koju je Apple podnio protiv Grupe NSO još je u tijeku.

468. Unatoč tome što je SAD uvrstio Grupu NSO na crnu listu, Bidenova administracija navodno je u listopadu 2022. imenovala bivšeg savjetnika NSO-a Jeremyja Basha članom savjetodavnog odbora za obavještajne aktivnosti. Pod okriljem poduzeća Beacon Global Strategies Bash je navodno angažiran za savjetovanje Grupe NSO preko poduzeća Francisco Partners. Prema Guardianu, bio je jedan od osam članova Odbora za poslovnu etiku NSO-a, što mu je navodno omogućilo glasovanje o predloženim prodajama NSO-a. Beacon Global Strategies prekinuo je svoj rad s NSO-om nakon što je grupa nastavila s prodajom Saudijskoj Arabiji[839].

469. Na sličan je način Grupa NSO pogođena odlaskom osoblja. Od ubojstva Jamala Khashoggija i zbog sve veće zabrinutosti u pogledu uloge koju je Pegasus imao u tome,

---

[832] The New Yorker, „How democracies spy on their citizens" (Kako demokracije špijuniraju svoje građane).
[833] Pismo g. Jeroenu Lenaersu i njegovim potpredsjednicima.
[834] Luxembourg Times, „Top five stories you may have missed" (Pet priča koje ste možda propustili).
[835] The New York Times, „U.S. Blacklists Israeli Firm NSO Group Over Spyware" (SAD stavlja izraelsku Grupu NSO na crnu listu zbog špijunskog softvera).
[836] Financial Times, „Credit Suisse pushed for spyware sales at NSO despite US blacklisting" (Credit Suisse tražio prodaju špijunskog softvera u NSO-u unatoč uvrštavanju na crnu listu SAD-a).
[837] The New York Times, „Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones" (Apple tuži izraelskog proizvođača špijunskog softvera i želi blokirati njegov pristup pametnim telefonima iPhone).
[838] https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/35/.
[839] The Guardian, „Biden intelligence advisor previously vetted deals for Israeli NSO Group" (Bidenov obavještajni savjetnik prethodno provjeravao prodaje za izraelsku Grupu NSO).

mnogi zaposlenici napustili su Grupu NSO. Istog je mjeseca suosnivač Shalev Hulio odstupio s dužnosti glavnog izvršnog direktora Grupe NSO i zamijenio ga je Yaron Shohat[840]. Grupa NSO promijenila je politiku i sada je usmjerena samo na članice NATO-a[841]. U ožujku 2023. objavljeno je da su dionice NSO-a prenesene na investicijsko društvo Dufresne Holding suosnivača Omrija Lavieja[842].

470. Pritisak na Grupu NSO stvorio je potražnju za drugim poduzećima koja se bave špijunskim softverom. Financial Times je 31. ožujka 2023. izvijestio da Vlada Indije navodno traži mogućnost kupnje alternativnog komercijalnog špijunskog softvera sa sličnim funkcijama kao kontroverzni špijunski softver Pegasus te da uzima u obzir i špijunski softver Predator poduzeća Intellexa[843].

471. U listopadu 2022. Shalev Hulio i bivši austrijski kancelar Sebastian Kurz pokrenuli su novo poduzeće za kibersigurnost pod nazivom Dream Security. Kurz je odstupio s mjesta kancelara nakon korupcijskog skandala u listopadu 2021. i počeo raditi za investicijsko društvo Petera Thiela dva mjeseca kasnije. Poduzeće će proizvoditi rješenja u području kibernetičkih incidenata s naglaskom na umjetnoj inteligenciji te će prodaju usmjeriti na europsko tržište[844]. Suradnja između Kurza i Hulia predstavlja neizravnu, ali alarmantnu vezu između industrije špijunskog softvera te Petera Thiela i njegova poduzeća Palantir.

472. Poduzeće Dream Security prikupilo je 20 milijuna USD od nekoliko ulagača, kao što je Adi Shalev, koji je ulagao i u NSO. Ostali ulagači uključuju Yevgenyja Dibrova[845], koji predstavlja „novi ruski glas” u onome što naziva „rusko-izraelski tehnološki ekosustav”[846]. To pokazuje da, unatoč turbulencijama i gospodarskim izazovima s kojima se suočila Grupa NSO, ista imena i dalje pokreću nova poduzeća koja se bave špijunskim softverom unutar EU-a i izvan njega.

CRNA KOCKA

473. Black Cube je privatna izraelska obavještajna agencija koju čine bivši djelatnici Mossada, izraelske vojske i izraelskih obavještajnih službi[847]. Na svojem mrežnom mjestu opisana je kao „kreativna obavještajna služba” koja pronalazi „prilagođena

---

[840] The Washington Post, CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup (Glavni izvršni direktor izraelskog poduzeća NSO za špijunski softver odstupio uslijed preustroja); Calcalist, After cutbacks and CEO departure, what's next for the controversial NSO? (Što je sljedeće za kontroverzni NSO nakon rezova i odlaska glavnog izvršnog direktora?).
[841] The Guardian, „CEO of Israeli Pegasus spyware firm NSO to step down” (Glavni izvršni direktor izraelskog poduzeća NSO povezanog sa špijunskim softverom Pegasus odstupa).
[842] The Guardian, „NSO Group co-founder emerges as new majority owner” (Suosnivač Grupe NSO postaje novi većinski vlasnik).
[843] https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9.
[844] Projekt izvješćivanja o organiziranom kriminalu i korupciji, „Former Austrian Chancellor and ex-NSO Chief Start Cybersecurity Firm” (Bivši austrijski kancelar i bivši direktor NSO-a otvorili poduzeće za kibersigurnost); The Times, „Former NSO CEO and ex-Austrian Chancellor found startup” (Bivši direktor NSO-a i bivši austrijski kancelar osnovali start-up poduzeće).
[845] The Times, „Former NSO CEO and ex-Austrian Chancellor found startup” (Bivši direktor NSO-a i bivši austrijski kancelar osnovali start-up poduzeće).
[846] Calcalist, „From Russia, With Coding Skills” (Iz Rusije, s vještinama programiranja).
[847] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7. listopada 2019.

rješenja za složene poslovne i parnične izazove”[848]. Black Cube bio je upleten u brojne javne kontroverze povezane s hakiranjem, među ostalim u SAD-u i Rumunjskoj[849]. Točnije, čelnici Black Cubea priznali su da su špijunirali bivšu glavnu tužiteljicu rumunjske Državne uprave za borbu protiv korupcije Lauru Kövesi[850]. Kövesi trenutačno obnaša dužnost glavne europske tužiteljice, odnosno voditeljice Ureda europskog javnog tužitelja (EPPO). Bivši rumunjski tajni agent Daniel Dragomir navodno je angažirao Black Cube za taj posao[851].

474. Ključno je što je otkrivena veza između Black Cubea te Grupe NSO i špijunskog softvera Pegasus. Nakon snažnog pritiska javnosti do kojeg je došlo jer je NSO angažirao Black Cube za nadzor svojih protivnika, bivši glavni izvršni direktor NSO-a Shalev Hulio priznao je da je angažirao Black Cube u najmanje jednoj situaciji u Cipru.

475. Black Cube je radio u Mađarskoj tijekom izbora 2018. godine, kad je špijunirao razne nevladine organizacije i osobe koje su bile na bilo koji način povezane s Georgeom Sorosom i izvještavao Viktora Orbána kako bi mogao prilagoditi prikazivanje svojih aktivnosti u kampanji ocrnjivanja[852]. Informacije dobivene nadzorom tih pojedinaca i nevladinih organizacija pojavile su se ne samo u mađarskim medijima pod kontrolom države, već i u izraelskom dnevnom listu Jerusalem Post[853].

INTELLEXA ALLIANCE

476. Tal Dilian osnovao je Intellexu na Cipru 2019. Dilian je obnašao razne vodeće položaje u izraelskim obrambenim snagama prije nego što je počeo karijeru „obavještajnog stručnjaka, graditelja zajednice i serijskog poduzetnika”[854]. Intellexa Alliance na svojoj se stranici opisuje kao poduzeće sa sjedištem u EU-u i usklađeno s propisima EU-a čiji je cilj razvijati i integrirati tehnologije za osnaživanje obavještajnih agencija. Dobavljači proizvoda za nadzor koji su pod nazivom Intellexa Alliance uključuju Cytrox, WiSpear (kasnije preimenovan u Passitora Ltd.), Nexa Technologies (kojim upravljaju bivši menadžeri Amesysa) i Poltrex.

477. Svi ti dobavljači omogućuju različite sustave. Dok je Cytrox dobar u izvlačenju podataka iz mobilnih telefona, Nexa Technologies nudi iskorištavanje globalnih mobilnih komunikacijskih sustava. WiSpear može izvući podatke iz Wi-Fi mreža. Različiti dobavljači u okviru Dilianove grupacije stoga pružaju širok asortiman softvera i usluga koje Intellexa može ponuditi, pojedinačno ili kombinirano, svojim klijentima

[848] https://www.blackcube.com/.
[849] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. travnja 2022.
[850] Balkan Insight, „Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case” (Šefovi obavještajne tvrtke izjasnili se krivima u slučaju nadzora u Rumunjskoj).
[851] Haaretz. „Black Cube CEO Suspected of Running Crime Organisation – Revealed:The Romania Interrogation” (Glavni izvršni direktor Black Cubea osumnjičen za vođenje zločinačke organizacije – Otkriveno: Ispitivanje u Rumunjskoj).
[852] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. srpnja 2018.
[853] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. srpnja 2018.
[854] Tal Dilian. „About” (Biografija).

unutar i izvan EU-a[855].

478. Matično društvo grupacije Intellexa Alliance, Thalestris Limited, ima različite podružnice s korporativnom prisutnošću u Irskoj, Grčkoj, Britanskim Djevičanskim otocima, Švicarskoj i Cipru. Sara Aleksandra Hamou, navodno druga bivša supruga Tala Diliana, direktorica je poduzeća Thalestris Limited i glavna direktorica podružnice sa sjedištem u Grčkoj[856]. Hamou je rođena u Poljskoj i posjeduje ciparsku putovnicu koju je izdalo Veleposlanstvo Republike Poljske u Cipru[857].

WiSpear i Cytrox

479. Tal Dilian pokrenuo je 2013. poduzeće registrirano u Cipru pod nazivom Aveledo Ltd., koje će kasnije biti preimenovano u Ws WiSpear Systems Ltd., a nakon toga u Passitora Ltd.[858] Sjedište WiSpeara je u Limassolu u Cipru, a poduzeće se uglavnom bavi prodajom opreme i softvera za lociranje i praćenje pojedinaca putem njihovih mobilnih telefona. Dilian je opisao mogućnosti WiSpearova softvera u intervjuu koji je dao časopisu Forbes, pokazavši crni kombi vrijedan 9 milijuna USD koji može hakirati uređaje u krugu od 500 metara. Osim toga, WiSpear posjeduje opremu koja ima mogućnost presretanja podataka iz Wi-Fi mreža[859]. Javni skandali povezani s tim proizvodima potaknuli su Intellexu da svoje glavne poslovne aktivnosti preseli s Cipra u Grčku.

480. Poduzeće Cytrox Holdings Zrt. osnovao je 2017. u Sjevernoj Makedoniji Ivo Malinkovski. Međutim, Cytrox je zapravo nastao u Tel Avivu, a Malinkovski je bio samo paravan. Nakon otkrića o projektu Pegasus Malinkovski je pokušao izbrisati sve tragove koji su ga povezivali s Cytroxom.

481. Cytrox je razvio špijunski softver Predator. Za razliku od špijunskog softvera Pegasus Predator zahtijeva da meta klikne poveznicu za instalaciju softvera[860]. Kad je Cytrox bio na rubu bankrota, Tal Dilian ga je spasio, a akvizicija je koštala skoro 5 milijuna USD[861]. Cytrox je kasnije spojen s Dilianovim WiSpearom[862]. Tom je akvizicijom softver Predator postao dio arsenala tehnologija društva Intellexa. Kao što je izvijestila organizacija Lighthouse Reports, u suradnji s novinama Haaretz i Inside Story, Intellexa je tajno i ilegalno isporučila softver Predator sudanskoj paravojnoj postrojbi Snage za brzu potporu koristeći privatni zrakoplov Cessna[863].

482. Prema Citizen Labu dva poduzeća Cytrox registrirana su u Izraelu (Cytrox EMEA Ltd. i

---

[855] Haaretz, „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire" (Dok Izrael obuzdava svoju industriju kibernetičkog oružja, bivši obavještajni časnik gradi novo carstvo).
[856]Thalestris Limited, Godišnje izvješće i konsolidirani financijski izvještaji za razdoblje od 28. studenoga 2019. do 31. prosinca 2020.
[857]ReportersUnited, „The Great Nephew and Big Brother" (Veliki nećak i veliki brat).
[858] Open Corporates, Passitora Ltd., https://opencorporates.com/companies/cy/HE318328.
[859] Haaretz, 'As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire' (Dok Izrael obuzdava svoju industriju kibernetičkog oružja, bivši obavještajni časnik gradi novo carstvo).
[860]Služba Europskog parlamenta za istraživanja, „Greece's Predatorgate. The latest chapter in Europe's spyware scandal?" (Afera Predatorgate u Grčkoj. Najnovije poglavlje u europskom skandalu sa špijunskim softverom?)
[861] BalkanInsight, „Wine, Weapons and Whatsapp: A Skopje Spyware Scandal" (Vino, oružje i Whatsapp: Skandal sa špijunskim softverom u Skoplju).
[862] PitchBook, Pregled Cytroxa.
[863] https://www.lighthousereports.nl/investigation/flight-of-the-predator/.

Cytrox Software Ltd.) i jedno u Mađarskoj (Cytrox Holdings Zrt.)[864]. Sve dionice poduzeća Cytrox Holdings Zrt. i Cytrox EMEA Ltd., kasnije preimenovanog u Balinese Ltd., prenesene su u poduzeće Aliada Group Inc., sa sjedištem na Britanskim Djevičanskim otocima. Aliada Group je i vlasnik poduzeća WiSpear. Glavni su dioničari poduzeća Aliada Group Dilian, Oz Liv, Meir Shamir i Avi Rubinstein. Rubinstein je u prosincu 2020. podnio pritužbu protiv svojih kolega dioničara poduzeća Aliada Group zbog nezakonitog razvodnjavanja njegovih dionica. Prema tužbi premještanje dionica na Britanske Djevičanske otoke i kasnije u Irsku zaobišlo je izraelske i inozemne zakone o kontroli izvoza[865].

483. Citizen Lab objavio je 16. prosinca 2021. izvješće u kojem se navodi da su vjerojatni kupci Predatora pronađeni u Armeniji, Egiptu, Grčkoj, Indoneziji, Madagaskaru, Omanu, Saudijskoj Arabiji i Srbiji[866].

AMESYS I NEXA TECHNOLOGIES

484. Amesys i Nexa Technologies, poduzeća koja su također u sastavu grupacije Intellexa Alliance, i sama su bila upetljana u određene kontroverze, kao što je opisano u dijelu o Francuskoj.

POLTREX

485. Poltrex je pokrenut u listopadu 2018., a jedini njegov dioničar bilo je poduzeće Intellexa Ltd., registrirano na Britanskim Djevičanskim Otocima. U rujnu 2019. kao direktor Poltrexa registriran je Izraelac Shahak Avni, osnivač ciparskog poduzeća NCIS Intelligence Services Ltd.[867] i suradnik Tala Diliana. Avni i Dilian postali su sudirektori u listopadu 2019., a naziv Poltrex promijenjen je u Alchemycorp Ltd. Bez obzira na promjenu naziva, uredi Poltrexa i dalje su bili u zgradi Novel Tower, na istoj adresi kao i uredi WiSpeara[868].

486. Dok su istrage o Dilianovu kombiju sa špijunskim softverom bile u tijeku, vlasništvo nad poduzećem Alchemycorp Ltd. preneseno je na Yarona Levgorena, zaposlenika poduzeća Cytrox Holdings[869]. Na Levgorenovu LinkedIn profilu stoji da on trenutačno zastupa poduzeće Apollo Technologies iz grupacije Intellexa, sa sjedištem u Grčkoj[870].

---

[864] Citizen Lab, „Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (Pegasus protiv Predatora: Disidentov dvostruko zaraženi iPhone pokazao prisutnost Cytroxova plaćeničkog špijunskog softvera).
[865] Citizen Lab, „Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (Pegasus protiv Predatora: Disidentov dvostruko zaraženi iPhone pokazao prisutnost Cytroxova plaćeničkog špijunskog softvera).
[866] Citizen Lab, „Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware" (Pegasus protiv Predatora: Disidentov dvostruko zaraženi iPhone pokazao prisutnost Cytroxova plaćeničkog špijunskog softvera) https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.
[867] Philenews, „FILE: The state insulted Avni and Dilian" (Predmet: Država je uvrijedila Avnija i Diliana).
[868] CyprusMail, 'Akel says found 'smoking gun' linking Cyprus to Greek spying scandal'(Akel navodno pronašao dokaze koji povezuju Cipar sa špijunskim skandalom u Grčkoj).
[869]Philenews, „How the spyware scandal in Greece is related to Cyprus" (Kako je skandal sa špijunskim softverom u Grčkoj povezan s Ciprom).
[870] https://ca.linkedin.com/in/yaron-levgoren-116948101.

VERINT/COGNYTE

487. Verint je izraelsko-američko kiberpoduzeće s brojnim podružnicama diljem svijeta. Samo je u Europi Verint registriran u Bugarskoj, Nizozemskoj, Cipru, Njemačkoj i Francuskoj (stanje 2021.). Verint je imao i društva kćeri koja su poslovala pod nazivom Cognyte. Te podružnice posluju neovisno od 2021., kad je Verint dovršio izdvajanje svoje obavještajne i kiberdjelatnosti u Cognyte[871]. Europske podružnice poduzeća Cognyte registrirana su u Cipru (UTX Technologies), Bugarskoj (Cognyte Bulgaria EOOD), Nizozemskoj (Cognyte Netherlands B.V.), Njemačkoj (Syborg GmbH, Syborg Grundbesitz GmbH i Syborg Informationsysteme b.h. OHG) i Rumunjskoj (Cognyte Romania S.R.L.)[872].

488. Verint je prodao alate za nadzor nekoliko represivnih vlada, među ostalim vladi Azerbajdžana, Indonezije i Južnog Sudana. U potonjem je slučaju Služba za nacionalnu sigurnost Južnog Sudana (NSS) upotrijebila je Verintovu opremu za presretanje protiv boraca za ljudska prava i novinara u razdoblju od ožujka 2015. do veljače 2017. Prema Amnesty Internationalu lokalni mobilni operater Vivacell Network of the World omogućio je NSS-u da prisluškuje sve telekomunikacije u zemlji[873]. Verint nije odgovorio na pitanja Amnestyja, ali je objavio izjavu u kojoj navodi da je Verintova neovisna jedinica Cognyte zapravo obrambena jedinica, dok se Verint bavi isključivo uključenošću kupaca. Verint tvrdi da je podjela s Cognyteom bila na snazi godinama prije službenog izdvajanja 2021., čime se distancirao od navodnog izvoza opreme za nadzor u zemlje u kojima je stanje ljudskih prava loše[874].

489. I Cognyte ima povijest izvoza u zemlje u kojima je stanje ljudskih prava loše. Meta je u istrazi iz 2021. identificirala kupce u Izraelu, Srbiji, Kolumbiji, Keniji, Maroku, Meksiku, Jordanu, Tajlandu i Indoneziji[875]. Cognyteova podružnica UTX Technologies, sa sjedištem u Cipru, navodno je dobila dozvole za izvoz softvera za praćenje u Meksiko, Ujedinjene Arapske Emirate, Nigeriju, Izrael, Peru, Kolumbiju, Brazil, Južnu Koreju i Tajland u razdoblju od rujna 2014. do ožujka 2015.[876] U Metinom izvješću iz 2021. za četiri je zemlje utvrđeno da su bile i Cognyteovi kupci. Usto, UTX Technologies je 2019. osigurao ugovor s Bangladešom za internetski obavještajni sustav vrijedan 2 milijuna USD, a 2021. sustav za praćenje mobilnih telefona vrijedan 500 000 USD.[877]

490. Mediji su 15. siječnja 2023. izvijestili da je izraelsko poduzeće Cognyte Software Ltd. pobijedilo na natječaju za prodaju špijunskog softvera za presretanje Mjanmaru mjesec

[871] Calcalistech, „Verint completes spin-off of its defense activities into new company Cognyte Software" (Verint dovršio izdvajanje obrambene djelatnosti u novo poduzeće Cognyte Software).
[872] https://www.sec.gov/Archives/edgar/data/1824814/000182481421000007/exhibit81.htm.
[873] Haaretz, „Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds" (Istraga otkrila – Izraelsko kiberpoduzeće prodalo špijunsku tehnologiju Južnom Sudanu); Amnesty International, „South Sudan: rampant abusive surveillance by NSS instils climate of fear" (Južni Sudan: NSS-ova neobuzdana zlouporaba nadzora stvara ozračje straha).
[874] Haaretz, „Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds" (Istraga otkrila – Izraelsko kiberpoduzeće prodalo špijunsku tehnologiju Južnom Sudanu).
[875] Meta, „Threat Report on the Surveillance-for-Hire Industry" (Izvješće o prijetnjama o tzv. „surveillance-for-hire" industriji praćenja i nadzora ciljanih osoba po narudžbi").
[876] Philenews, „Cyprus is a pioneer in software exports" (dokumenti) (Cipar pionir u izvozu softvera).
[877] Haaretz, „Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Records" (Izraelska špijunska tehnologija prodana u Bangladeš unatoč lošem stanju ljudskih prava).

dana prije vojnog udara u veljači 2021. Mjanmar je službeno kupio Cognyteov špijunski softver 30. prosinca 2020.[878]

491. Osim što Cognyte izvozi u treće zemlje, olakšao je i prijevoz opreme za praćenje u države članice. Preko poduzeća UTX Technologies registriranog u Cipru, tehnologija Gi2 isporučena je u drugu Cognyteovu podružnicu u Njemačkoj, Syborg Informationsysteme[879]. Tehnologija Gi2 navodno je poslana i u Verintovu podružnicu u Poljskoj „u svrhu demonstracije". Gi2 tehnologija može pristupiti određenom uređaju i čak može imitirati vlasnika i slati lažne poruke putem tog istog uređaja[880]. Te su pošiljke izvršene od 2013. do 2014. U to vrijeme Verint i Cognyte još su bili dio iste strukture poduzeća.

492. UTX Technologies prodao je i sustave za praćenje 2013. francuskom poduzeću za izvoz pod nazivom COFREXPORT[881]. Ta je tvrtka je prestala s radom i zatvorena je u vrijeme pisanja.

493. Kao i mnogi drugi dobavljači špijunskog softvera Cognyte ima vrlo složenu strukturu poduzeća zbog promjena naziva, podjela i izdvajanja tijekom vremena. Međutim, Cognyteove podružnice pokazuju da se države članice EU-a ne koriste samo kao baze iz koji se izvozi oprema za nadzor, već služe i kao uporišta za prodaju i slanje opreme za nadzor unutar Europe. Stoga izraelska poduzeća koja se bave špijunskim softverom iskorištavaju pogodnosti unutarnjeg tržišta EU-a, koje olakšava prijevoz njihove opreme u vlastite podružnice i u nova poduzeća registrirana u državama članicama EU-a.

QUADREAM

494. QuaDream je izraelsko poduzeće koje su osnovali bivši visoki dužnosnik izraelske vojne obavještajne službe Ilan Dabelstein i bivši zaposlenici NSO-a Guy Geva i Nimrod Rinsky. Poduzeće je najpoznatije po svojem špijunskom softveru Reign, koji navodno koristi exploitove koji ne zahtijevaju klikanje i ima značajku samouništenja koja briše sve tragove zaraze. Ta vrsta špijunskog softvera ima različite funkcionalnosti, kao što su snimanje zvuka, praćenje lokacija, traženje datoteka i fotografiranje objema kamerama.[882]

495. Prema Citizen Labu i Microsoftovoj analizi Saznanja o prijetnjama („Threat Intelligence"), sustavi QuaDream djeluju iz Bugarske, Češke, Mađarske, Rumunjske, Gane, Izraela, Meksika, Singapura, Ujedinjenih Arapskih Emirata i Uzbekistana. Osim toga, identificirano je najmanje pet meta iz civilnog društva u Sjevernoj Americi,

---

[878] Reuters, „Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup" (dokumenti) (Izraelski Cognyte pobijedio na natječaju za prodaju špijunskog softvera za presretanje Mjanmaru prije državnog udara).
[879] https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex81.htm.
[880] Philenews, „Cyprus is a pioneer in software exports" (dokumenti) (Cipar pionir u izvozu softvera).
[881] Philenews, „Cyprus is a pioneer in software exports" (dokumenti) (Cipar pionir u izvozu softvera).
[882] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/; https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000?lts=1681386702066.

središnjoj Aziji, jugoistočnoj Aziji, Europi i na Bliskom istoku[883].

496. U 2017. poduzeće je registrirano u Cipru pod nazivom InReach. To je poduzeće osnovano isključivo za promociju proizvoda QuaDream kao što je Reign izvan Izraela. QuaDream je navodno koristio InReach za prodaju svojih proizvoda kopcima kako bi zaobišao izraelsku kontrolu izvoza. Mnogi su od ključnih zaposlenika obaju poduzeća radili za Grupu NSO, Verint i UT-X Technologies.[884]

497. Nakon izvješća Citizen Laba i Microsoftove analize Saznanja o prijetnjama 16. travnja 2023. objavljeno je da je QuaDream prestao s radom u Izraelu. Prema Haaretzu poduzeće je u prethodnim mjesecima imalo problema s padom prodaje i odlaskom zaposlenika[885].

CANDIRU

498. Candiru je još jedan proizvođač špijunskog softvera registriran u Izraelu. Poduzeće su 2014. osnovali Ya'acov Weitzman i Eran Shorer. Oba osnivača radila su u vojnoj obavještajnoj jedinici 8200 izraelskih obrambenih snaga i obojica su bivši zaposlenici Grupe NSO[886]. Isaac Zack, bivši ulagač u Grupu NSO, postao je najveći dioničar Candirua. To poduzeće prodaje špijunski softver za hakiranje računala i poslužitelja[887]. Informacije objavljene o prijedlogu projekta pokazuju da Candiru svoju opremu prodaje na temelju broja istodobnih zaraza, tj. broja uređaja koji mogu biti meta špijunskog softvera u bilo kojem trenutku. Na primjer, za cijenu od 16 milijuna USD kupac dobiva neograničen broj pokušaja zaraze špijunskim softverom, ali može istodobno napasti samo deset uređaja. Za dodatnih 1,5 milijuna USD kupac može kupiti kapacitete za napad 15 dodatnih uređaja[888].

499. Prema istraživanju novina TheMarker, Candiru sad nudi i špijunski softver za provaljivanje u mobilne uređaje[889]. Svoj špijunski softver prodaje samo vladama i ima klijentelu u Europi, bivšem Sovjetskom Savezu, Perzijskom zaljevu, Aziji i Latinskoj

---

[883] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/.

[884] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/; https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/; https://www.haaretz.com/israel-news/tech-news/2021-06-08/ty-article/.highlight/the-secret-israeli-cyber-firm-selling-spy-tech-to-saudia-arabia/0000017f-df07-d856-a37f-ffc724f80000?lts=1681386702066.

[885] https://www.haaretz.com/israel-news/security-aviation/2023-04-16/ty-article/.premium/offensive-israeli-cyber-firm-quadream-closes-and-fires-all-employees/00000187-8b5c-d484-adef-ebdc048c0000.

[886] Haaretz „'We're on the U.S. Blacklist Because of You': The Dirty Clash Between Israeli Cyberarms Makers'.(„Zbog vas smo na crnoj listi SAD-a": Prljavi sukob među izraelskim proizvođačima kibernetičkog oružja).

[887] Haaretz, „Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed'. (Hakiranje mobilnih telefona i milijunski poslovi u Zaljevu: Otkriveno unutarnje funkcioniranje najtajnijeg izraelskog poduzeća za kibernapade).

[888] Citizen Lab, „Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus'.(Upecana velika riba Candiru: Još jedan dobavljač plaćeničkog špijunskog softvera u središtu pozornosti).

[889] Haaretz, „Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed" (Hakiranje mobilnih telefona i milijunski poslovi u Zaljevu: Otkriveno unutarnje funkcioniranje najtajnijeg izraelskog poduzeća za kibernapade).

Americi[890]. U dijelu o Španjolskoj navodi se da je 65 osoba bilo meta špijunskog softvera, od toga su četiri bile meta Candirua, a najmanje dvije bile su meta i Candirua i Pegasusa[891].

500. Kao i kod drugih dobavljača špijunskog softvera, korporativno prikrivanje koda glavna je praksa tog poduzeća, koje je posljednjih godina nekoliko puta promijenilo naziv. Poduzeće je promijenilo ime u DF Associates Ltd. 2017., u Grindavik Solutions Ltd. 2018., u Taveta Ltd. 2019. i, konačno, u Saito Tech Ltd. 2020.[892] Radi jasnoće u ovom se izvješću to poduzeće naziva Candiru.

501. Baš kao što se dogodilo Grupi NSO, Ministarstvo trgovine SAD-a uvrstilo je Candiru na crnu listu SAD-a u studenome 2021. Nagađa se da je razlog za uvrštavanje Candirua na crnu listu to što je glavni izvršni direktor Grupe NSO Shalev Hulio navodno bio tajni partner u Candiruu i što je predstavio poduzeće važnim posrednicima u obavještajnom svijetu. Navodno je Hulio čak tvrdio da je Candiruov proizvod zapravo prepakirani Pegasus[893]. Istraživači u području sigurnosti identificirali su 1. srpnja 2022. nov napad iskorištavanjem ranjivosti nultog dana u Chromeu koji je Candiru koristio za napad na pojedince u Libanonu, Palestini, Jemenu i Turskoj[894]. Google je poduzeo odgovarajuće mjere za taj exploit, a otad ga krpaju i Microsoft i Apple[895].

TYKELAB I RCS LAB

502. Organizacija Lighthouse Reports izvijestila je u kolovozu 2022. da se Tykelab, poduzeće sa sjedištem u Rimu u vlasništvu RCS Laba, koristi desecima telefonskih mreža koje se često nalaze na otocima u južnom Pacifiku za slanje desetaka tisuća tajnih „paketa za praćenje” po cijelom svijetu. Na njegovoj meti našle su se osobe u Italiji, Grčkoj, Sjevernoj Makedoniji, Portugalu, Libiji, Kostarici, Nikaragvi, Pakistanu, Maleziji, Iraku, Maliju i drugim državama. Tykelab iskorištava nedostatke u svjetskim telefonskim mrežama koji omogućuju trećim stranama da vide lokacije korisnika telefona te da potencijalno presreću njihove pozive, a da na samim uređajima pritom ne ostane nikakav trag koji bi ukazivao na to da su ugroženi[896]. To je poduzeće u lipnju 2022. u samo dva dana ispitalo mreže u gotovo svim državama svijeta[897]. Tykelab na svojoj mrežnoj stranici navodi da „spaja dvadeset godina iskustva u dizajniranju,

[890] Citizen Lab, „Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus” (Upecana velika riba Candiru: Još jedan dobavljač plaćeničkog špijunskog softvera u središtu pozornosti).
[891] Citizen Lab, „CatalanGate. Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru” (KatalonGate: Opsežne operacije plaćeničkih špijunskih softvera protiv Katalonaca koji se koriste Pegasusom i Candiruom).
[892] Citizen Lab, „Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus” (Upecana velika riba Candiru: Još jedan dobavljač plaćeničkog špijunskog softvera u središtu pozornosti).
[893] Haaretz, „’We’re on the U.S. Blacklist Because of You’: The Dirty Clash Between Israeli Cyberarms Makers” („Zbog vas smo na crnoj listi SAD-a”: Prljavi sukob među izraelskim proizvođačima kibernetičkog oružja).
[894] TechCrunch, „Spyware maker Candiru linked to Chrome zero-day targeting journalists” (Proizvođač špijunskog softvera Candiru povezan s napadom iskorištavanjem ranjivosti nultog dana u Chromeu čija su meta bili novinari).
[895] The HackerNews, „Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists” (Špijunski softver Candiru uhvaćen u napadu iskorištavanjem ranjivosti nultog dana u Googleovom Chromeu čija su meta bili novinari).
[896] https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[897] https://euobserver.com/digital/155849.

provedbi i održavanju rješenja Core Network Telco s opsežnim stručnim znanjima u isporuci upravljanih servisa, integraciji sustava zasnovanih na kupcima i razvoju mobilnih aplikacija”[898].

503. U istrazi organizacije Lighthouse Reports istaknuta je i uloga telekomunikacijske industrije s obzirom na to da iznajmljivanje pristupnih točaka telefonskih mreža ili „globalnih adresa” omogućuje da se takva zlouporaba nastavi. Prema industrijskoj organizaciji GSM Association, koja predstavlja operatore pokretnih mreža diljem svijeta, telefonski operateri ne mogu uvijek identificirati izvor i svrhu prometa koji teče kroz njihove mreže, što otežava zaustavljanje tih praksi[899].

504. Tykelab je dio RCS Laba, talijanske tvrtke poznate po aktivnostima presretanja u Italiji i inozemstvu. To je otkriveno u objavi trećeg poduzeća, Cy4Gate, koje je kupilo RCS Lab. RCS Lab ima ogranke u Francuskoj, Njemačkoj i Španjolskoj[900], kao i još jednu prikrivenu podružnicu, Azienda Informatica Italiana, koja izrađuje softver za presretanje Android i iPhone uređaje[901].

ŠPIJUNSKI SOFTVER HERMIT

505. RCS Lab razvio je špijunski softver pod nazivom Hermit, koji se može upotrijebiti za daljinsko aktiviranje mikrofona ciljanog telefona, kao i za snimanje poziva te pristup porukama, zapisnicima poziva, popisima kontakata i fotografijama[902]. Googleova Skupina za analizu prijetnji (Threat Analysis Group) otkrila je u lipnju 2022. da su akteri koji su imali potporu vlada s pomoću RCS Labova špijunskog softvera onemogućavali svojim metama mobilne podatkovne veze u suradnji s njihovim pružateljima usluga pristupa interneta. Nakon što bi veza bila onemogućena, napadač bi SMS-om poslao meti zlonamjernu poveznicu s uputom da instalira aplikaciju kako bi obnovila podatkovnu vezu. Google vjeruje da je zato većina tih aplikacija lažno predstavljena kao aplikacije mobilnih operatera. U slučajevima kada sudjelovanje pružatelja usluga pristupa interneta nije bilo moguće, aplikacije su lažno predstavljene kao aplikacije za razmjenu poruka. Žrtve napada izvršenih s pomoću RCS Labova špijunskog softvera nalazile su se u Italiji i Kazahstanu[903], a softver je otkriven i u Rumunjskoj[904].

506. Justin Albrecht, istraživač koji se bavi saznanjima o prijetnjama za poduzeće Lookout koje se bavi kibersigurnosti, rekao je da, iako je Hermitova instalacijska metoda manje sofisticirana od metode koju koristi Pegasus, njegove su mogućnosti slične. Da bi Hermit napao uređaj, korisnik telefona mora kliknuti zaraženu poveznicu[905].

507. Prema RCS Labu „svaka prodaja ili implementacija proizvoda obavlja se tek nakon službenog odobrenja nadležnih nacionalnih tijela. Proizvodi koji se isporučuju kupcima

[898] http://www.tykelab.it/wp/about/.
[899] https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[900] https://euobserver.com/digital/155849.
[901] https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[902] https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[903] https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/.

[904] https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[905] https://euobserver.com/digital/155849.

instaliraju se u njihovim objektima, a osoblju RCS Laba ni u kojem slučaju nije dopušteno obavljanje operativnih aktivnosti kao potpora kupcu kao ni pristup obrađenim podacima. Zbog obvezujućih ugovora o povjerljivosti RCS Lab ne smije otkriti nikakve pojedinosti o svojim kupcima. Grupa Cy4gate, čiji je RCS Lab član, pridržava se Globalnog sporazuma UN-a i stoga osuđuje sve oblike kršenja ljudskih prava. Proizvodi RCS Lab-a imaju jasnu, specifičnu i isključivu namjenu, a to je pružanje potpore agencijama kaznenog progona u sprečavanju i suzbijanju gnusnih kaznenih djela”[906]. Međutim, nije moguće provjeriti poštuje li Grupa Cy4gate, uključujući RCS Lab, vlastite standarde koje navodi.

508. Prema istrazi Lighthouse Reportsa objavljenoj u kolovozu 2022. Tykelabov alat za nadzor Hermit korišten je za ciljanje pojedinaca diljem svijeta, među ostalim u Libiji, Nikaragvi, Maleziji, Kostarici, Iraku, Maliju, Grčkoj i Portugalu, kao i u Italiji[907].

DECISION SUPPORTING INFORMATION RESEARCH AND FORENSIC (DSIRF)

509. Poduzeće DSIRF GmbH (LLC) nedavno je postalo predmet kaznenog postupka koji vodi austrijsko Ministarstvo pravosuđa[908]. DSIRF je austrijsko poduzeće osnovano 2016. sa sjedištem u Beču, a matično joj je poduzeće u Lihtenštajnu. Tvrdi da pruža „multinacionalnim korporacijama u tehnološkom, maloprodajnom, energetskom i financijskom sektoru usluge prilagođene pojedinim misijama u područjima istraživanja informacija, forenzike i obavještavanja temeljenog na podacima”[909]. DSIRF očito svoje proizvode prodaje nedržavnim akterima.

510. DSIRF je razvio špijunski softver pod nazivom Subzero/KNOTWEED, koji se može implementirati s pomoću ranjivosti nultog dana u sustavu Windows i softveru Adobe Reader, a koji se, prema vlastitom oglašavanju, može potajno instalirati na ciljani uređaj. Nakon instalacije Subzero preuzima „potpunu kontrolu nad ciljanim računalom” i pruža „potpun pristup svim podacima i lozinkama”. Kupci softvera SubZero mogu izvlačiti lozinke, snimati snimke zaslona, pregledavati trenutačne i prethodne lokacije te „pristupiti, preuzeti, izmijeniti i učitati datoteke na ciljano računalo” putem internetskog sučelja. DSIRF promiče Subzero kao „novu generaciju kiberratovanja”, navodeći da je alat „dizajniran za kiber-vrijeme”[910]. DSIRF je 2020. procijenio vrijednost svog softvera Subzero na 245 milijuna EUR.

511. Povezanost s Rusijom postaje jasna iz veza nekoliko visokopozicioniranih zaposlenika DSIRF-a. Vlasnik DSIRF-a je Peter Dietenberger, „čovjek s odličnim vezama u Kremlju” koji „otvora vrata zapadnim tvrtkama u Putinovu carstvu”[911]. Dietenberger je živio u Rusiji nekoliko godina i imao je rusko poduzeće i nekoliko ruskih poslovnih partnera. Jedan od njegovih ruskih poslovnih partnera, Boris Vasilyev, bio je i u

[906] https://euobserver.com/digital/155849.
[907] Lighthouse Reports, „Revealing Europe’s NSO” (Otkrivanje europskog NSO-a), https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[908] DSIRF je pokrata za „Decision Supporting Information Research and Forensic”.
[909] https://dsirf.eu/about/.
[910] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/.
[911] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html.

upravnom odboru DSIRF-a. DSIRF navodi nekoliko referenci za svoje poduzeće i proizvode: Michael Harms (glavni izvršni direktor njemačkog Istočnog poslovnog udruženja), Stephan Fanderl (predsjednik upravnog odbora Galerije Karstadt Kaufhof, koji je želio dovesti Walmart u Rusiju), Christian Kremer (bivši predsjednik BMW-a u Rusiji i glavni izvršni direktor poduzeća Russian Machines, koje je pod sankcijama SAD-a od 2018.) i Florian Schneider (partner u velikom odvjetničkom društvu Dentons u Moskvi, koje se bavi poslovnim pravom)[912]. Russian Machines, poduzeće u vlasništvu oligarha Olega Deripaske, navodno se koristi uslugama DSIRF-a. Moćni lokalni poduzetnik Siegfried „Sigi" Wolf, koji je savjetovao bivšeg kancelara Sebastiana Kurza o gospodarskim pitanjima, smatra se Deripaskovom osobom od povjerenja[913]. Uključen je i Jan Marsalek, navodni zločinac za kojeg Interpol izdao nalog za uhićenje zbog optužbi za prijevaru u gospodarskom poslovanju tešku milijarde eura, među ostalim financijskim i gospodarskim kaznenim djelima. U kolovozu 2018. primio je e-poruku od Floriana Stermanna (glavnog tajnika Rusko-austrijskog društva prijateljstva, za kojeg se u istragama državnog odvjetništva smatralo da je osoba od povjerenja stranke FPÖ)[914], koja je sadržavala prezentaciju poduzeća DSIRF. Marsalek je 2013. navodno pokušao prodati Grenadi špijunski softver koji je proizvelo talijansko poduzeće Hacking Team. Navodno se trenutačno skriva u Moskvi pod nadzorom FSB-a, ruske tajne službe[915].

512. U srpnju 2022. Microsoft je otkrio da je Subzero korišten tijekom neovlaštenih, zlonamjernih aktivnosti za napade na odvjetnička društva, banke i strateška konzultantska društva u Austriji, Ujedinjenoj Kraljevini i Panami[916]. Austrija trenutačno nema pravnu osnovu za neovlašteno korištenje špijunskog softvera kao što je Subzero od strane javnih tijela, a također bi bilo nezakonito da ga jedno privatno poduzeće koristi protiv drugog. Nakon Microsoftove objave austrijska nevladina organizacija za digitalna prava Epicenter.works podnijela je 28. srpnja 2022. kaznenu prijavu protiv DSIRF-a Državnom odvjetništvu u Beču zbog nezakonitog pristupa računalnom sustavu, oštećivanja podataka, ometanja funkcioniranja računalnih sustava, zlouporabe obrade podataka, zločinačkog udruživanja i kršenja Zakona o vanjskoj trgovini i plaćanjima u pogledu robe s dvojnom namjenom[917]. Austrijsko Savezno ministarstvo rada i gospodarstva izjavilo je 7. listopada 2022. da nije izdalo izvoznu dozvolu DSIRF-u[918] te je, prema austrijskom Saveznom ministarstvu pravosuđa, Državno odvjetništvo u Beču pokrenulo kaznenu istragu o DSIRF-u[919]. Korištenje špijunskog softvera Subzero

[912] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/.
[913] https://www.derstandard.at/story/2000131301583/causa-marsalek-die-verbindungen-einer-spionagefirma-werfen-fragen-auf.
[914] https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html.
[915] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/; https://www.dw.com/en/wanted-wirecard-executive-jan-marsalak-reportedly-hiding-in-moscow/a-61440213.
[916] https://www.microsoft.com/en-us/security/blog/2022/07/27/untangling-knotweed-european-private-sector-offensive-actor-using-0-day-exploits/./
[917] https://en.epicenter.works/document/4236.
[918] Odgovor austrijskog saveznog ministra za digitalizaciju i gospodarstvo Martina Kochera na pisana parlamentarna pitanja Stephanie Krisper, 7. listopada 2022., referentni broj, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml.
[919]Odgovor savezne ministrice pravosuđa Alme Zadić na pisana parlamentarna pitanja Stephanie Krisper, 7. listopada 2022., referentni broj 2022-0.575.216, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml.

protiv meta u Austriji znači da je privatno ili javno tijelo u Austriji nezakonito upotrijebilo softver, da je softver upotrijebio strani subjekt i da je DSIRF prekršio ograničenja izvoza, ili da je softver izvezen u drugu državu članicu i da se iz nje upotrebljavao, zakonito ili nezakonito, protiv austrijske mete. Ispitni je postupak i dalje u tijeku.

FINFISHER

513. Valja spomenuti u ovom izvješću i kriminalnu istragu poduzeća FinFisher i njegova bankrota, bivšeg poduzeća za špijunski softver sa sjedištem u Münchenu u Njemačkoj. FinFisher je osnovan 2008. i izvorno je bio snažno povezan s britanskom mrežom poduzeća koja su poslovala pod robnom markom Gamma. FinFisher je svoj špijunski softver reklamirao kao „potpun portfelj informatičkih sredstava za upad”, a upotrebljavali su ga deseci država diljem svijeta[920], uključujući 11 država članica EU-a[921] i 13 „neslobodnih” država[922].

514. FinFisherov proizvod FinSpy pojavio se 2017. u Turskoj na lažnoj verziji internetske stranice za mobilizaciju za tursku oporbu. Softver je bio prerušen u aplikaciju za preuzimanje koja se preporučivala sudionicima protuvladinih demonstracija[923], dok je FinFisher oglašavao svoje proizvode isključivo u svrhu borbe protiv kriminala. Kaznenu prijavu protiv FinFishera podnijeli su 2019. organizacija Gesellschaft für Freiheitsrechte, Reporteri bez granica, blog netzpolitik.org i Europski centar za ustavna i ljudska prava zbog izvoza špijunskog softvera bez potrebne izvozne dozvole njemačkog Saveznog ureda za gospodarstvo i kontrolu izvoza. Stoga je time prekršena Uredba EU-a o robi s dvojnom namjenom i odgovarajuće njemačko nacionalno zakonodavstvo. Nakon kaznene prijave Državno odvjetništvo u Münchenu istražilo je poduzeće FinFisher, a u listopadu 2020. pretražilo je 15 poslovnih prostora grupe FinFisher u Njemačkoj i Rumunjskoj te privatne stambene prostore. Okružni sud u Münchenu odobrio je 2021. da Državno odvjetništvo zaplijeni bankovne račune FinFishera kako bi se osiguralo oduzimanje nezakonito stečene dobiti u slučaju da se FinFisher osudi. Međutim, FinFisher je u veljači 2022. proglasio nesolventnost. Poduzeće je prestalo s radom, ured je zatvoren, a svih 22 zaposlenika je otpušteno[924]. Kaznene istrage osoba odgovornih za FinFisherove aktivnosti još su u tijeku.

III. Sposobnost odgovora Europske unije

515. Neke vlade upotrebljavaju moćan i vrlo invazivan i intruzivan špijunski softver za nadzor građana EU-a, zloupotrebljavajući svoje pravo na nadzor u slučaju rizika za

---

[920] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; https://wikileaks.org/spyfiles4/customers.html.

[921] Belgija, Češka, Estonija, Njemačka, Mađarska, Italija, Nizozemska, Rumunjska, Slovačka, Slovenija i Španjolska.

[922] Angola, Bahrein, Bangladeš, Egipat, Etiopija, Gabon, Jordan, Kazahstan, Mjanmar, Oman, Katar, Saudijska Arabija i Turska.

[923] https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/.

[924] https://netzpolitik.org/2022/nach-pfaendung-staatstrojaner-hersteller-finfisher-ist-geschlossen-und-bleibt-es-auch/; https://edri.org/our-work/criminal-complaint-against-illegal-export-of-surveillance-software-is-making-an-impact-the-finfisher-group-of-companies-ceases-business-operations-after-its-accounts-are-seized-by-public-prosecutor/; https://netzpolitik.org/wp-upload/2022/03/2022-02-08_AG-Muenchen_Insolvenzbekanntmachung_FinFisher-Labs-GmbH.txt.

nacionalnu sigurnost. To predstavlja prijetnju demokraciji, vladavini prava i temeljnim pravima građana. EU ima ograničene ovlasti za djelovanje protiv tih prijetnji i loše je opremljen protiv potencijalnih kriminalnih aktivnosti nacionalnih tijela, čak i ako one utječu na EU. U skladu s Ugovorima nacionalna sigurnost ostaje u isključivoj nadležnosti država članica, ali njihovo djelovanje i dalje mora biti u skladu s temeljnim pravima i demokratskim normama sadržanima u pravu EU-a. Osim toga, politički čimbenici ograničavaju ovlasti EU-a za djelovanje. Europska komisija, kao čuvarica Ugovorâ EU-a, nije uložila maksimalne napore u provedbu prava EU-a primjenom pravnih instrumenata koji su joj na raspolaganju. Komisija naginje vrlo uskom tumačenju svojih ovlasti, prema kojemu je gotovo isključivo nadležna za pravilno prenošenje prava Unije u nacionalno pravo. Komisija smatra da je rješavanje problema kršenja prava Unije isključiva odgovornost nacionalnih tijela. Takav stav, koji se ne temelji na Ugovorima EU-a, postaje vrlo problematičan u slučaju teškog kršenja vladavine prava i temeljnih prava. Iako supsidijarnost i podjela nadležnosti čine stup prava Unije, one ne bi smjele dovesti do nekažnjavanja vlada koje upotrebljavaju špijunski softver za nadzor građana EU-a u političke svrhe. U nastavku ćemo razmotriti ovlasti koje institucije EU-a imaju na raspolaganju. Parlament, Komisija i Vijeće imaju ovlast i dužnost djelovati kao zakonodavci, regulatori i provoditelji zakona i to moraju činiti energično i ambiciozno, pri čemu obrana naše demokracije mora imati prednost pred kratkoročnim političkim razlozima.

Europska komisija

516. Nakon novinskih izvješća o uporabi špijunskog softvera u državama članicama i pitanja odbora PEGA, Komisija je u svojem odgovoru na skandal sa špijunskim softverom isprva samo pismenim putem zatražila pojašnjenja od vlada Poljske, Mađarske, Španjolske, Grčke, Cipra i Francuske. Međutim, čini se da nakon te opomene koju je uputila Komisija nisu uslijedila daljnja postupanja. Točno je da Komisija, strogo uzevši, nema ovlasti za djelovanje u području nacionalne sigurnosti. Međutim, kao što sama Komisija navodi u tim pismima, „nacionalnu sigurnost” ne bi trebalo tumačiti kao sredstvo za neograničeno izuzeće od zakona i ugovora EU-a i ona ne bi smjela postati prostor bezakonja. Međutim, na državama članicama je da „dokažu da bi nacionalna sigurnost bila ugrožena u predmetnom slučaju”. Kao odgovor na pitanje koje će mjere Komisija poduzeti ako nacionalna tijela ne ispitaju temeljito bilo kakve navode o nezakonitom špijuniranju, Komisija samo upućuje na Sud Europske unije i članak 47. Povelje, kojim se dodjeljuje pravo na djelotvoran pravni lijek pred sudom. Čini se da nema političke spremnosti za djelovanje.

517. Nadalje, Komisija je 21. prosinca 2022. poslala opći dopis svim državama članicama u kojem je zatražila informacije o uporabi špijunskog softvera od strane nacionalnih tijela i o pravnom okviru kojim se uređuje takva uporaba u svrhu „pregleda stanja u državama članicama” i ispitivanja „međudjelovanja s pravom Unije”[925]. Komisija je postavila konkretna pitanja o, među ostalim, svrsi uporabe špijunskog softvera, tijelima ovlaštenima za njegovo uvođenje, nacionalnoj definiciji nacionalne sigurnosti, relevantnom zakonodavstvu kojim se uređuje obrada podataka za potrebe nacionalne sigurnosti, zaštitnim mjerama, prethodnom odobrenju suda ili neovisnog upravnog tijela, nadzoru i obavješćivanju, pri čemu je rok za odgovor 31. siječnja 2023.

[925] Pismo Glavne uprave JUST državama članicama. Ref. Ares(2022)8885417, 21. prosinca 2022.

Povjerenik Reynders izjavio je 28. ožujka 2023. odboru PEGA da je velika većina država članica odgovorila, ali da je Komisija još uvijek u postupku prikupljanja odgovora država članica u okviru postupka utvrđivanja stanja te da će „pažljivo ocijeniti” odgovore. Na temelju utvrđenog stanja Komisija će razmotriti svoje opcije u pogledu uporabe špijunskog softvera u državama članicama. Međutim, za procjenu Komisije nije predviđen točan datum završetka „s obzirom na promjenjivu i osjetljivu prirodu procjene”. Osim toga, Komisija je spomenula da će pomno pratiti nalaze odbora PEGA.

518. Za razliku od SAD-a, koji je na otkrića odgovorio uvrštavanjem poduzeća na crnu listu, provedbom istraga, među ostalim na području EU-a, i izdavanjem izvršnog naloga kojim se saveznim tijelima SAD-a zabranjuje stjecanje komercijalnog špijunskog softvera, Komisija dosad nije provela analizu situacije ni procjenu poduzeća koja posluju na tržištu špijunskih softvera u EU-u. Ne postoji očiti pravni prigovor koji bi sprečavao provedbu takve analize. Znakovito je da velika količina dokaza još uvijek nije potaknula Komisiju da poduzme smislene mjere. Komisija zbog svoje inercije sudjeluje u kršenju ljudskih prava i zanemaruje dužnosti.

519. EU ima nekoliko zakona koji bi mogli poslužiti kao regulatorni instrumenti s obzirom na špijunski softver. Uz zakone kojima se štite prava građana, poput zakona o zaštiti podataka i privatnosti komunikacija (Opća uredba o zaštiti podataka, Direktiva o privatnosti i elektroničkim komunikacijama[926]), postoje zakoni o izvozu (Uredba o robi s dvojnom namjenom) i nabavi. Međutim, Komisija kao čuvarica Ugovorâ slabo provodi te zakone i ne ostvaruje svoj puni potencijal. Obično se ograničava na provjeru je li neka država članica ispravno prenijela zakone EU-a u svoje nacionalno pravo. Međutim, to ne otkriva gotovo ništa o stvarnom stanju na terenu. Tako se čini da Komisija u svojem izvješću[927] o provedbi Uredbe o robi s dvojnom namjenom zaključuje da provedba dobro napreduje, iako postoji obilje dokaza da je njezina provedba u praksi slaba i rascjepkana te da je to u nekim državama čak namjerno. Provedba Direktive o privatnosti i elektroničkim komunikacijama i sudske prakse koja iz nje proizlazi nije dobra. Komisija upućuje na to da su države članice odgovorne za provedbu i izvršenje, ali ne poduzima mjere ako države članice ne ispune te zadaće. Bez odgovarajuće i konkretne provedbe zakoni EU-a postaju neučinkoviti i ostavljaju širok prostor za nezakonitu uporabu špijunskog softvera.

520. Svrha Direktive o zaštiti podataka pri izvršavanju zakonodavstva bila je pružiti visoke standarde zaštite podataka i osigurati slobodan protok podataka u sektoru provedbe zakona i kaznenog pravosuđa. Direktivu je bilo potrebno prenijeti u nacionalno pravo, uz široke diskrecijske ovlasti dodijeljene državama članicama. Danas je očito da se provedba razlikuje među državama članicama, posebno u području prava ispitanika. Komisija bi hitno trebala procijeniti provedbu u svim državama članicama i utvrditi najozbiljnije nedostatke. Trebala bi izraditi konkretne smjernice za države članice o provedbi Direktive kako bi se osiguralo poštovanje standarda EU-a u cijeloj Uniji. Nadalje, Komisija bi, prema potrebi, trebala pokrenuti postupke zbog povrede prava u slučajevima kada Direktiva nije pravilno prenesena, a država članica nije voljna to

[926] Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (SL L 201, 31.7.2002., str. 37.).
[927] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

ispraviti.

Europski parlament

521. Europski parlament osnovao je istražni odbor PEGA koji marljivo i djelotvorno radi u okviru svojih ovlasti i svojeg mandata. Međutim, taj odbor nema ovlast pozivati svjedoke niti ih saslušavati pod zakletvom, a nema ni pristup podacima zaštićenim oznakom tajnosti. Nedostaju mu potpune istražne ovlasti koje ima većina nacionalnih parlamenata. Osim toga, u raspravama u odboru PEGA često su prisutni utjecaji nacionalnih vlada, što katkad predstavlja prepreku temeljitim, potpuno neovisnim i objektivnim istraživanjima. Prilično je uznemirujuće što Europski parlament nema pune istražne ovlasti, s obzirom da su neki njegovi zastupnici bili mete špijunskog softvera.

Europsko vijeće i Vijeće ministara

522. Iako nacionalne vlade tvrde da je skandal povezan sa špijunskim softverom isključivo nacionalno pitanje, o njemu se ipak raspravljalo na Vijeću Europske unije i nacionalne su vlade odlučile skupno odgovoriti na upitnik Europskog parlamenta[928]. Na taj su način u potpunosti priznale da je to pitanje kojim bi se trebalo baviti Vijeće.

523. Javna ili značajna reakcija Europskog vijeća na skandal povezan sa špijunskim softverom sve je do danas izostala. Neke od njegovih članica imaju u tome određeni interes jer su možda same sudionici u nezakonitom hakiranju ili jednostavno žele da EU u tom području ostane slab i bez ovlasti.

524. Čak i ako se nezakonito ili kažnjivo ponašanje u konačnici dokaže, ne bi bilo moguće opozvati članove nacionalnih vlada niti ih prisiliti da daju ostavke na svoje položaje u EU-u. To znači da osobe koje su odgovorne za takve postupke mogu nastaviti nekažnjeno sjediti u tijelima EU-a i donositi odluke koje utječu na sve europske građane.

Europol

525. Europol nema nikakve autonomne operativne ovlasti i ne može djelovati bez pristanka i suradnje dotične države članice ili dotičnih država članica, u skladu s člankom 88. stavkom 3. UFEU-a, dok je primjena prisilnih mjera isključiva odgovornost nadležnih nacionalnih tijela. To predstavlja problem u slučajevima kad postoje jasni dokazi o kriminalnim radnjama, kao što su kiberkriminal, korupcija i iznuđivanje, ali nacionalne vlasti ne provedu istragu. Europol je nedavno dobio nove ovlasti koje mu omogućuju da proaktivno predloži istragu, čak i ako se ona odnosi na kazneno djelo koje je počinjeno u samo jednoj državi članici[929], ali dosad nije iskoristio te ovlasti.

526. Odbor PEGA uputio je Europolu pismo 28. rujna 2022.[930], pozivajući ga da iskoristi

[928] Nacrt pisma glavnog tajništva Vijeća delegacijama država članica, 26. rujna 2022.
[929] Uredba (EU) 2022/991 Europskog parlamenta i Vijeća od 8. lipnja 2022. o izmjeni Uredbe (EU) 2016/794 u pogledu suradnje Europola s privatnim stranama, obrade osobnih podataka koju provodi Europol radi potpore kaznenim istragama i uloge Europola u području istraživanja i inovacija (SL L 169, 27.6.2022., str. 1.).
[930] https://twitter.com/EP_PegaInquiry/status/1576855144574377984.

nove ovlasti koje su mu dane člankom 6. Uredbe o Europolu[931]. U svojem odgovoru od 13. listopada 2022.[932] Europol je naveo da je kontaktirao s pet država članica kako bi utvrdio „jesu li na nacionalnoj razini dostupne relevantne informacije za Europol i je li kaznena istraga u tijeku ili je predviđena (ili postoji neka druga istraga u skladu s primjenjivim odredbama nacionalnog prava)". U pismu odboru PEGA 11. travnja 2023. Europol je naveo da su njegova pisma poslana Grčkoj, Mađarskoj, Bugarskoj, Španjolskoj i Poljskoj. Nakon odgovora pet država članica na njegova pisma Europol je spomenuo da nijedna od njih nije imala „dostupne relevantne informacije za Europol". Do listopada 2022. jedna od pet država članica potvrdila je Europolu da su „pokrenute kaznene istrage pod nadzorom nadležnih pravosudnih tijela, što je potvrdio i Eurojust". Do prosinca 2022. druga država članica obavijestila je Europol da je „pokrenut jedan kazneni postupak u vezi s navodnom nezakonitom uporabom softvera Pegasus, koji su u međuvremenu okončala nadležna pravosudna tijela u toj zemlji". Treća država članica obavijestila je Europol da je „u jednom slučaju pokrenut predsudski postupak na regionalnoj razini" i postavila pitanje „ima li Europol informacije o uporabi softvera Pegasus u predmetnoj zemlji, koje su relevantne za predsudski postupak". Četvrta država članica obavijestila je Europol da „ne postoji kaznena istraga koja je u tijeku ili se predviđa", ali da su „pokrenute sudske istrage". Do travnja 2023. peta država članica objasnila je Europolu da „nakon savjetovanja s nadležnim tijelima u toj zemlji ne postoje relevantne informacije za Europol o nezakonitoj uporabi intruzivnog softvera za nadzor i presretanje, uz upućivanje na prethodne postupke ureda javnog tužitelja". Nije poznato odnose li se prethodno navedeni kazneni postupci dviju država članica, predsudski postupci jedne države članice, sudske istrage jedne države članice i prethodni postupci ureda javnog tužitelja u još jednoj državi članici na zlouporabu špijunskog softvera od strane vlada država članica EU-a ili trećih zemalja.

527. Ispada da je EU poprilično nemoćan protiv potencijalnih kriminalnih aktivnosti nacionalnih tijela, čak i ako one utječu na EU.

528. Paradoksalno je da SAD, za razliku od Europola, aktivno istražuje uporabu špijunskog softvera u EU-u. Dana 5. studenoga 2022. objavljeno je da je FBI posjetio Atenu kako bi istražio „raširenost nezakonitog nadzora i osobe koje su ga prodavale"[933]. Nadalje, u ožujku 2023. američki predsjednik Biden izdao je izvršni nalog kojim se saveznim tijelima SAD-a zabranjuje uporaba špijunskog softvera. Nekoliko dana kasnije druge zemlje, uključujući Francusku i Dansku, istaknule su svoju predanost međunarodnoj suradnji u tom području.

Europsko pravosuđe

529. Sud EU-a i ESLJP imaju važnu ulogu u obrani demokracije, vladavine prava i temeljnih prava. Međutim, oni mogu djelovati tek po podnošenju tužbe ili pitanja koje prethodi sudskom postupku. Njihovi su postupci vrlo dugotrajni i pružaju slabe konkretne pravne lijekove u pojedinačnim slučajevima. Ti su sudovi tijekom godina stvorili vrlo opsežnu

[931] „Ako izvršni direktor smatra da bi trebalo pokrenuti kaznenu istragu u pogledu određenog kaznenog djela koje se odnosi samo na jednu državu članicu, ali utječe na zajednički interes obuhvaćen politikom Unije, izvršni direktor može nadležnim tijelima dotične države članice predložiti, putem njezine nacionalne jedinice, da pokrenu, vode ili koordiniraju takvu kaznenu istragu."
[932] Spis br. 1260379.
[933] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ.

mjerodavnu sudsku praksu, na primjer, kojom se utvrđuju standardi za nadzor. Međutim, ti sudovi nemaju načina da osiguraju provedbu svojih presuda. Dosad je Europskom sudu za ljudska prava podnesena jedna tužba koja se odnosi na nezakonitu uporabu špijunskog softvera[934]. Međutim, put koji vodi do sudova u Strasbourgu i Luksemburgu često je dug, skup i kompliciran jer se prvo moraju iscrpiti sve mogućnosti u nacionalnim sudskim postupcima. To posebno vrijedi za slučajeve u kojima nacionalni tužitelji ili suci ne prihvate neki predmet ili ga odbiju. Granica za prolazak na testu prihvatljivosti visoka je.

Ombudsman

530. Ombudsmanica EU-a zaključila je 28. studenoga 2022. da Komisija nije u dovoljnoj mjeri procijenila rizike za ljudska prava prije pružanja potpore afričkim zemljama u razvoju kapaciteta za nadzor, posebno u kontekstu Kriznog uzajamnog fonda EU-a za Afriku (EUTFA). Zaključci su uslijedili nakon pritužbe nekoliko organizacija civilnog društva. U Nigeru je iz Fonda dodijeljeno 11,5 milijuna EUR za nabavu opreme za nadzor, uključujući softver za nadzor, centar za prisluškivanje i uređaj za presretanje međunarodne oznake pokretnog pretplatnika[935], unatoč represiji nad aktivistima u zemlji. Kako bi uklonila nedostatke koje je utvrdila, ombudsmanica je predložila poboljšanja kako bi se osigurala provedba procjene učinka na ljudska prava prije budućih projekata Kriznog uzajamnog fonda EU-a za Afriku.

Druga tijela EU-a

531. Europski odbor za zaštitu podataka, Europski nadzornik za zaštitu podataka, Europski revizorski sud i Eurojust imaju vrlo malo nadležnosti za nadziranje nezakonite uporabe špijunskog softvera ili trgovine takvim softverom od strane vlada država članica ili za intervenciju u takvim slučajevima. Neki od njihovih članova možda su čak upleteni u skandale u svojim državama članicama. To može imati utjecaj na funkcioniranje i integritet navedenih tijela EU-a. Ured europskog javnog tužitelja mogao bi potencijalno intervenirati u slučajevima u koje su na bilo koji način uključena financijska sredstva EU-a.

[934] Koukakisova žalba Europskom sudu za ljudska prava, 27. srpnja 2022.

[935] https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf.

OBRAZLOŽENJE

Europski Watergate

U ljeto 2021. Pegasus project, skupina istraživačkih novinara, nevladinih organizacija i istraživača, objavio je popis od 50 000 osoba koje su se našle na meti plaćeničkog špijunskog softvera. Među njima su novinari, odvjetnici, tužitelji, aktivisti, političari, pa čak i šefovi država. Najdramatičniji slučaj mogao bi biti slučaj Jamala Khashoggija, saudijskog novinara koji je 2018. brutalno ubijen zbog kritike saudijskog režima. Međutim, na popisu su bile i brojne europske mete. Neke su bile mete aktera izvan EU-a, dok su druge bile mete vlastitih nacionalnih vlada. Otkrića su izazvala zgražanje diljem svijeta.

Skandalu je ubrzo dodijeljen naziv „europski Watergate”. Međutim, umjesto političkog trilera „All the President's Men” (Svi predsjednikovi ljudi) o provali u kompleks zgrada Watergate 1972., današnji skandal povezan sa špijunskim softverom podsjeća na zastrašujući film „Das Leben der Anderen” (Život drugih), koji prikazuje nadzor totalitarnog komunističkog režima nad građanima. Današnja digitalna provala špijunskim softverom mnogo je sofisticiranija i invazivnija te gotovo uopće ne ostavlja traga. Uporaba špijunskog softvera znatno nadilazi konvencionalni nadzor osobe. Njime se akterima špijunaže omogućuje potpuni pristup i kontrola. Za razliku od klasičnog prisluškivanja, špijunski softver ne omogućuje samo nadzor u stvarnom vremenu, već i potpuni, retroaktivni pristup datotekama i porukama stvorenima u prošlosti, kao i metapodacima o prošlim komunikacijama. Nadzor se može provoditi čak i na daljinu, iz bilo koje zemlje u svijetu. Špijunski softver u principu se može upotrebljavati za preuzimanje kontrole nad pametnim telefonom i izdvajanje njegova cjelokupnog sadržaja, uključujući dokumente, slike i poruke. Materijal dobiven na taj način može se upotrebljavati za promatranje radnji, ali i za ucjenjivanje, diskreditiranje, manipuliranje i zastrašivanje žrtava. Pristup sustavu žrtve može se manipulirati i može se podmetnuti izmišljeni sadržaj. Mikrofon i kamera mogu se aktivirati na daljinu i time pretvoriti uređaj u špijuna. Žrtva pritom ničega nije svjesna. Špijunski softver ostavlja vrlo malo tragova na uređaju žrtve, a čak i ako se otkrije, gotovo je nemoguće dokazati tko je odgovoran za napad.

Zlouporabom špijunskog softvera ne krši se samo pravo na privatnost pojedinaca. Ona prikriveno ugrožava i demokraciju i demokratske institucije. Ušutkava oporbu i kritičare, ukida nadzor i ima odvraćajući učinak na slobodu tiska i civilno društvo. Osim toga, služi za manipuliranje izborima. Pojam „plaćenički špijunski softver” vrlo dobro odražava prirodu proizvoda i industrije. Čak i neuspjeli pokušaji zaraze pametnog telefona špijunskim softverom imaju političke posljedice i mogu naštetiti pojedincu i demokraciji. Sudjelovanje u javnom životu postaje nemoguće ako osobi nije zajamčeno da je slobodna i da nije pod nadzorom.

Skandal povezan sa špijunskim softverom nije niz izoliranih nacionalnih slučajeva zlouporabe, već posvemašnja europska afera. Vlade država članica EU-a upotrebljavaju špijunski softver na svojim građanima u političke svrhe te za prikrivanje korupcije i kriminalnih aktivnosti. Neki su otišli korak dalje i ugradili špijunski softver u sustav koji je namjerno osmišljen za autoritarnu vladavinu. Vlade drugih država članica možda nisu zloupotrijebile špijunski softver, ali su olakšale njegovu prikrivenu trgovinu. Europa je postala privlačno mjesto za plaćenički špijunski softver. Europa je postala izvozno čvorište za

diktature i represivne režime, kao što su Libija, Egipat i Bangladeš, gdje se špijunski softver upotrebljavao protiv aktivista za ljudska prava, novinara i kritičara vlade.

Zlouporaba špijunskog softvera ozbiljno je kršenje svih vrijednosti Europske unije, koje stavlja na kušnju otpornost demokratske vladavine prava u Europi. Posljednjih je godina EU vrlo brzo izgradio svoje kapacitete za odgovor na vanjske prijetnje našoj demokraciji, bilo da je riječ o ratu, kampanjama dezinformiranja ili političkom upletanju. Za razliku od toga, sposobnost odgovora na unutarnje prijetnje demokraciji još uvijek nije dovoljno razvijena. Antidemokratske tendencije mogu se slobodno širiti poput gangrene po cijelom EU-u jer se nacionalne vlade ne kažnjavaju za prijestupe. EU nije u stanju nositi se s takvim unutarnjim napadom na demokraciju. S jedne strane, EU je u velikoj mjeri političko tijelo koje je uređeno nadnacionalnim zakonima i kojim upravljaju nadnacionalne institucije, s jedinstvenim tržištem, otvorenim granicama, putovanjem bez putovnica, građanstvom Unije te jedinstvenim područjem sigurnosti, slobode i pravde. Međutim, unatoč svečanim obećanjima u pogledu europskih vrijednosti, u praksi se te vrijednosti i dalje smatraju nacionalnim pitanjem. Skandal povezan sa špijunskim softverom nemilosrdno razotkriva nezrelost i slabost EU-a kao „demokratskog” tijela. Što se tiče demokratskih vrijednosti, EU se temelji na „pretpostavci sukladnosti” nacionalnih vlada, no u praksi se ona pretvorila u „lažnu sukladnost”. Scenarij u kojem nacionalne vlade namjerno zanemaruju i krše zakone EU-a jednostavno nije predviđen u upravljačkim strukturama EU-a. EU nije opremljen instrumentima za takve slučajeve. Tijela EU-a imaju malo ovlasti, a još manje sklonosti, da se u slučaju prijestupa suprotstavljaju nacionalnim tijelima, a posebno ne u osjetljivom području „nacionalne sigurnosti”. Prema međuvladinoj logici institucije EU-a podređene su nacionalnim vladama. Međutim, bez djelotvornih i smislenih nadnacionalnih provedbenih mehanizama, novo zakonodavstvo bit će beskorisno. Za rješavanje problema bit će potrebne i regulatorne mjere i reforme upravljanja.

SAD nije pošteđen unutarnjih napada na demokraciju, kao što je Watergate ili opsada Kongresa 6. siječnja 2021., ali je opremljen za snažan odgovor. Ima ovlasti suprotstaviti se čak i najvišim političkim čelnicima ako ne poštuju zakon i Ustav.

Naime, nakon otkrića o špijunskom softveru iz 2021. Sjedinjene Američke Države reagirale su brzo i odlučno na otkrića koja je objavio Project Pegasus. Ministarstvo trgovine SAD-a brzo je uvrstilo Grupu NSO na crnu listu, Ministarstvo pravosuđa pokrenulo je istragu, a u pripremi su i strogi propisi za trgovinu špijunskim softverom. FBI je čak došao u Europu kako bi istražio napad špijunskim softverom na osobu s dvojnim državljanstvom SAD-a i Europe. Tehnološki divovi kao što su Apple i Microsoft pokrenuli su pravne postupke protiv poduzeća koja se bave špijunskim softverom. Žrtve su podnijele pravne pritužbe, tužitelji istražuju, a pokrenute su i parlamentarne istrage.

Za razliku od toga, uz iznimku Europskog parlamenta, druge institucije EU-a uglavnom se nisu oglasile i ostale su pasivne, tvrdeći da je riječ isključivo o nacionalnom pitanju.

Europsko vijeće i nacionalne vlade provode „zakon šutnje” (*omertà*). Europsko vijeće nije službeno odgovorilo na skandal. Vlade država članica u velikoj su mjeri odbile poziv na suradnju s odborom PEGA. Neke vlade izričito su odbile surađivati, dok su druge bile prijateljske i uljudne, ali zapravo nisu podijelile smislene informacije. Čak ni jednostavan upitnik poslan svim državama članicama o pojedinostima njihova nacionalnog pravnog okvira za uporabu špijunskog softvera nije dobio gotovo nikakve značajne odgovore. Uoči objave

ovog nacrta izvješća odbor PEGA primio je zajednički odgovor država članica preko Vijeća, koji također nije bio sadržajan.

Europska komisija izrazila je zabrinutost i od vlada nekoliko država članica zatražila pojašnjenja, ali samo u onim slučajevima u kojima je skandal već izbio na nacionalnoj razini. Komisija je nevoljko i fragmentarno objavila informacije o napadima špijunskim softverom na vlastite službenike.

Europol je dosad odbio iskoristiti svoje nove ovlasti za pokretanje istrage. Tek nakon što je Europski parlament izvršio pritisak na nju, Komisija je uputila pismo pet država članica u kojem ih je priupitala je li policijska istraga započela i može li im pružiti pomoć.

Naglasak na Europi

Zlouporaba špijunskog softvera uglavnom se promatra kroz prizmu nacionalne politike. Tim uskim nacionalnim stajalištem zasjenjuje se cjelovita slika. Samo sagledavanjem šire slike postaje jasno da se u svim aspektima radi o istinski europskom pitanju.

Iako to nije službeno potvrđeno, možemo sa sigurnošću pretpostaviti da su sve države članice EU-a kupile jedan ili više komercijalnih proizvoda špijunskog softvera. Samo jedno poduzeće, Grupa NSO, prodalo je svoje proizvode dvadeset dvama krajnjim korisnicima u najmanje četrnaest država članica, među kojima su Poljska, Mađarska, Španjolska, Nizozemska i Belgija. U najmanje četiri države članice, Poljskoj, Mađarskoj, Grčkoj i Španjolskoj, došlo je do nezakonite uporabe špijunskog softvera, a sumnja se i u njegovu uporabu na Cipru. Dvije države članice, Cipar i Bugarska, služe kao izvozna čvorišta špijunskog softvera. Jedna država članica, Irska, nudi povoljne porezne propise za velikog dobavljača špijunskog softvera, a Luksemburg je bankarsko čvorište za mnoge sudionike u industriji špijunskog softvera. U Pragu u Češkoj Republici održava se godišnji europski sajam industrije špijunskog softvera, tzv. sajam ISS (Intelligence Support Systems) World, koji ima nadimak „Bal prisluškivača”. Čini se da je Malta popularno odredište za određene protagoniste te industrije. Nekoliko nasumičnih primjera načina na koji industrija špijunskog softvera iskorištava Europu bez granica: Intellexa je prisutna u Grčkoj, na Cipru te u Irskoj, Francuskoj i Mađarskoj, a njezin glavni izvršni direktor ima malteško putovnicu i (fiktivno) poduzeće. NSO je prisutan na Cipru i u Bugarskoj, a svoje financijsko poslovanje obavlja preko Luksemburga. DSIRF prodaje svoje proizvode iz Austrije, Tykelab iz Italije, a FinFisher iz Njemačke (prije njegova zatvaranja).

Trgovina špijunskim softverom ostvaruje korist od unutarnjeg tržišta EU-a i slobodnog kretanja. Određene zemlje EU-a privlačne su kao izvozna čvorišta jer je, unatoč ugledu EU-a kao strogog regulatora, provedba izvoznih propisa slaba. Naime, kad su postrožena pravila o izvozu iz Izraela, EU je dobavljačima postao privlačniji. Oni oglašavaju svoje poslovanje kao „usklađeno s propisima EU-a”, iskorištavajući svoju prisutnost u EU-u kao oznaku kvalitete. „EU” osigurava respektabilnost. Članstvo u EU-u korisno je i za vlade koje žele kupiti špijunski softver. Države članice EU-a izuzete su od pojedinačne procjene učinka ljudskih prava koja je potrebna za ishođenje izvozne dozvole od izraelskih vlasti jer se članstvo u EU-u smatra dovoljnim jamstvom usklađenosti s najvišim standardima.

Iako je prodajna strana trgovine špijunskim softverom netransparentna i nedostižna, istovremeno je unosna i u punom zamahu. Strukture poduzeća prikladno su, ako ne i

namjerno, složene kako bi se prikrile nepoželjne aktivnosti i veze, među ostalim s vladama EU-a. Sektor je na papiru uređen, ali u praksi uspijeva zaobići mnoga pravila, među ostalim zbog toga što je špijunski softver proizvod koji može služiti kao politička valuta u međunarodnim odnosima. Poduzeća koja se bave špijunskim softverom imaju poslovni nastan u nekoliko zemalja, ali mnoge su osnovali bivši izraelski vojni i obavještajni službenici. Većina dobavljača tvrdi da prodaje samo državnim akterima, iako neki od njih iza kulisa prodaju i nedržavnim akterima. Gotovo je nemoguće dobiti bilo kakve informacije o tim kupcima ili o ugovornim uvjetima i usklađenosti.

Trgovina špijunskim softverom i njegova uporaba izravno su obuhvaćeni područjem primjene prava i sudske prakse EU-a. Kupnja i prodaja špijunskog softvera uređena je, među ostalim, pravilima o javnoj nabavi i izvozu, kao što je Uredba o robi s dvojnom namjenom. Uporaba špijunskog softvera mora biti u skladu sa standardima Opće uredbe o zaštiti podataka, Uredbe o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ, Direktive o zaštiti podataka pri izvršavanju zakonodavstva i Direktive o privatnosti i elektroničkim komunikacijama. Prava osoba koje su predmet nadzora utvrđena su u Povelji o temeljnim pravima te u međunarodnim konvencijama, posebno pravo na privatnost i pravo na pošteno suđenje, te u propisima EU-a o pravima osumnjičenika i optuženika. Zlouporaba špijunskog softvera u mnogim će slučajevima predstavljati kiberkriminalitet i može podrazumijevati kaznena djela korupcije i iznude, od kojih su sva u nadležnosti Europola. Europski javni tužitelj ima mandat za djelovanje ako su uključena europska financijska sredstva. Zlouporaba špijunskog softvera može utjecati i na policijsku i pravosudnu suradnju, posebno na razmjenu informacija i provedbu europskog uhidbenog i dokaznog naloga.

Zlouporaba špijunskog softvera izravno i neizravno utječe na EU i njegove institucije. Određeni zastupnici u Europskom parlamentu te članovi Europske Komisije i Vijeća također su bili mete špijunskog softvera. Drugi su bili pogođeni kao „usputni ulov” ili neizravne mete. S druge strane, i neki „počinitelji” su članovi Europskog vijeća. Osim toga, manipulacija nacionalnim izborima uporabom špijunskog softvera izravno utječe na sastav institucija EU-a i političku ravnotežu u njegovim upravljačkim tijelima. Četiri ili pet vlada koje su optužene za zlouporabu špijunskog softvera čine gotovo četvrtinu stanovništva EU-a te su stoga od velike važnosti u Vijeću.

Špijunski softver kao dio sustava

Špijunski softver nije samo tehnički alat koji se upotrebljava ad hoc i u izoliranim slučajevima. Upotrebljava se kao sastavni dio sustava. U načelu je njegova uporaba ugrađena u pravni okvir i popraćena potrebnim zaštitnim mjerama, mehanizmima nadzora i kontrole te pravnim sredstvima. Istraga pokazuje da su te zaštitne mjere često slabe i neprimjerene. To je uglavnom nenamjerno, ali u nekim je slučajevima sustav, djelomično ili u cijelosti, namjerno prilagođen ili osmišljen kako bi služio kao sredstvo političke moći i kontrole. U tim slučajevima nezakonita uporaba špijunskog softvera nije incident, već dio namjerne strategije. Vladavina prava pretvara se u pravo vladara. Pravna osnova za nadzor može se sastaviti na nejasan i neprecizan način kako bi se legalizirala široka i neometana uporaba špijunskog softvera. *Ex ante* nadzorom u obliku sudskog odobrenja za nadzor može se lako manipulirati i lišiti ga značenja, posebno u slučaju politizacije pravosuđa ili zarobljavanja države. Vladajuće stranke mogu održavati mehanizme nadzora slabima i staviti ih pod svoju kontrolu. Pravni

lijek i građanska prava mogu postojati na papiru, ali prestaju važiti uslijed ometanja od strane vladinih tijela. Podnositeljima pritužbi odbija se pristup informacijama, čak i u vezi s optužbama protiv njih kojima se navodno opravdava njihov nadzor. Tužitelji, suci i policija odbijaju provoditi istragu i često stavljaju teret dokazivanja na žrtvu, od koje očekuju da dokaže da se našla na meti špijunskog softvera. Posljedično, žrtva se nalazi u paradoksalnoj situaciji jer joj je uskraćen pristup potrebnim informacijama. Vladajuće stranke mogu pojačati svoju moć nad javnim institucijama i medijima kako bi se onemogućio smisleni nadzor. Javni ili komercijalni mediji bliski vladi mogu poslužiti kao kanal za kampanje ocrnjivanja s pomoću materijala dobivenih špijunskim softverom. „Nacionalna sigurnost" često se navodi kao izgovor za uklanjanje transparentnosti i odgovornosti. Svi ti elementi zajedno tvore sustav osmišljen za kontrolu i ugnjetavanje. Takva situacija ne samo da potpuno izlaže pojedinačne žrtve i ostavlja ih bespomoćnima protiv svemoćne vlade, već znači i da su svi ključni sustavi provjere i ravnoteže demokratskog društva onemogućeni.

Neke su vlade već dosegnule tu točku, a druge su na pola puta. Srećom, većina europskih vlada neće tako postupiti. Međutim, kada je to slučaj, EU u svojem trenutačnom institucionalnom i političkom ustroju nije opremljen za sprečavanje ili suzbijanje te situacije. Špijunski softver je pokazatelj moguće opasnosti koji razotkriva opasne ustavne nedostatke u EU-u.

Tajnost

Tajnost je velika prepreka u otkrivanju i istraživanju nezakonite uporabe špijunskog softvera.

Većina žrtava ne može dobiti informacije o svojem predmetu od nadležnih tijela. U mnogim slučajevima nadležna tijela opravdavaju tajnost navodeći razloge povezane s nacionalnom sigurnošću, a u drugim slučajevima jednostavno opovrgavaju postojanje spisa ili se spisi uništavaju. Tužitelji pritom često odbijaju istraživati te slučajeve tvrdeći da žrtve nemaju dovoljno dokaza. To je začarani krug koji ostavlja žrtve bez pravnog lijeka.

Vlade najčešće odbijaju objaviti jesu li kupile špijunski softver i koju vrstu softvera su nabavile. Dobavljači špijunskog softvera također odbijaju otkriti tko su njihovi klijenti. Vlade često pribjegavaju posrednicima, opunomoćenicima ili osobnim vezama za nabavu komercijalnog špijunskog softvera ili usluga povezanih sa špijunskim softverom kako bi prikrile svoje sudjelovanje. Zaobilaze pravila javne nabave i proračunske postupke kako ne bi ostavile nikakve tragove.

Izrael je važno središte poduzeća koja se bave špijunskim softverom i odgovoran je za izdavanje dozvola za stavljanje na tržište i izvoznih dozvola. Iako su Izrael i Europa bliski saveznici, Izrael državama članicama EU-a ne daje nikakve informacije o izdavanju (ili ukidanju) dozvola za špijunski softver, unatoč tome što se on upotrebljava za kršenje prava europskih građana i ugrožavanje naše demokracije.

Novinari na temelju zahtjeva za slobodan pristup informacijama dobivaju malo informacija ili ih uopće ne dobivaju. I posebna tijela za kontrolu i nadzor, kao što su tijela za zaštitu podataka ili revizorski sudovi, imaju poteškoća s dobivanjem informacija. Neovisni nadzor nad tajnim službama iznimno je slab, a često se ni ne provodi. Vladajuće stranke često otežavaju i sprečavaju rad parlamentarnih istražnih odbora. Sudske istrage usmjerene su na hakiranje trećih zemalja, a ne na vlade EU-a koje nezakonito upotrebljavaju špijunski softver.

Novinari koji izvještavaju o tom pitanju suočavaju se sa strateškim tužbama protiv javnog sudjelovanja (eng. SLAPP), verbalnim napadima političara ili kampanjama ocrnjivanja. Hrabri i marljivi novinari koji otkrivaju činjenice povezane sa skandalom zaslužuju naše poštovanje i zahvalnost. Oni su europski ekvivalenti istraživačkih novinara Woodwarda i Bernsteina. Nadalje, zviždači još uvijek nisu na odgovarajući način zaštićeni u svim državama članicama. U nekim slučajevima žrtve napada špijunskim softverom ostaju suzdržane jer ne žele izložiti tko se krije iza napada zbog straha od odmazde ili posljedica otkrivanja kompromitirajućeg materijala.

Sljedeći koraci

U trenutku kad su europske vrijednosti pod napadom vanjskog agresora, još je važnije ojačati našu demokratsku vladavinu prava protiv unutarnjih napada. Rezultati istrage odbora PEGA šokantni su i trebali bi uznemiriti svakog europskog građanina. Očito je da bi trgovina špijunskim softverom i njegova uporaba trebale biti strogo regulirane. Odbor PEGA izradit će niz preporuka u tu svrhu. Međutim, jednako tako trebale bi postojati i inicijative za institucionalne i političke reforme koje bi EU-u omogućile da stvarno provodi i poštuje ta pravila i standarde, čak i ako ih same države članice krše. EU mora brzo razviti svoje linije obrane protiv unutarnjih napada na demokraciju.

INFORMACIJE O USVAJANJU U NADLEŽNOM ODBORU

Datum usvajanja	8.5.2023.
Rezultat konačnog glasovanja	+: 30 –: 3 0: 4
Zastupnici nazočni na konačnom glasovanju	Bartosz Arłukowicz, Vladimír Bilčík, Karolin Braunsberger-Reinhold, Saskia Bricmont, Anna Júlia Donáth, Cornelia Ernst, Giorgos Georgiou, Sylvie Guillaume, Hannes Heide, Ivo Hristov, Sophia in ‘t Veld, Assita Kanko, Beata Kempa, Moritz Körner, Jeroen Lenaers, Juan Fernando López Aguilar, Hannah Neumann, Carles Puigdemont i Casamajó, Diana Riba i Giner, Sándor Rónai, Ernő Schaller-Baross, Birgit Sippel, Dominik Tarczyński, Róża Thun und Hohenstein, Dragoş Tudorache, Lucia Vuolo, Jörgen Warborn, Juan Ignacio Zoido Álvarez
Zamjenici nazočni na konačnom glasovanju	Andrzej Halicki, Gabriel Mato, Thijs Reuten, Jordi Solé, Yana Toom
Zamjenici nazočni na konačnom glasovanju prema čl. 209. st. 7.	Aurélia Beigneux, Theresa Bielowski, Franc Bogovič, Catherine Griset, Andreas Schieder

KONAČNO GLASOVANJE POIMENIČNIM GLASOVANJEM U NADLEŽNOM ODBORU

30	+
EPP	Bartosz Arłukowicz, Vladimír Bilčík, Franc Bogovič, Karolin Braunsberger-Reinhold, Andrzej Halicki, Jeroen Lenaers, Gabriel Mato, Lucia Vuolo, Jörgen Warborn, Juan Ignacio Zoido Álvarez
Renew Europe	Anna Júlia Donáth, Sophia in 't Veld, Moritz Körner, Róża Thun und Hohenstein, Yana Toom, Dragoş Tudorache
S&D	Theresa Bielowski, Sylvie Guillaume, Hannes Heide, Ivo Hristov, Juan Fernando López Aguilar, Thijs Reuten, Sándor Rónai, Andreas Schieder
GUE/NGL	Cornelia Ernst, Giorgos Georgiou
Zeleni/ESS	Saskia Bricmont, Hannah Neumann, Diana Riba i Giner, Jordi Solé

3	-
ECR	Beata Kempa, Dominik Tarczyński
Nezavisni zastupnici	Ernő Schaller-Baross

4	0
ECR	Assita Kanko
Klub zastupnika Identitet i demokracija	Aurélia Beigneux, Catherine Griset
Nezavisni zastupnici	Carles Puigdemont i Casamajó

Legenda:
+ : glasovali „za”
- : glasovali „protiv”
0 : suzdržan