Evropský parlament
2019-2024

Dokument ze zasedání

A9-0189/2023

22.5.2023

ZPRÁVA

o vyšetřování údajných porušení a správních pochybení v oblasti provádění právních předpisů Unie týkajících se používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru
(2022/2077(INI))

Vyšetřovací výbor pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru

Zpravodajka: Sophie in ‘t Veld

OBSAH

Strana

NÁVRH VÝSLEDKŮ

vyšetřování údajných porušení a správních pochybení v oblasti provádění právních předpisů Unie týkajících se používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru
(2022/2077(INI))

Evropský parlament,

– s ohledem na článek 226 Smlouvy o fungování Evropské unie (dále jen „SFEU“),

– s ohledem na rozhodnutí Evropského parlamentu ze dne 10. března 2022 o zřízení, vymezení předmětu vyšetřování, působnosti, početního složení a funkčního období vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru,

– s ohledem na články 54 a 208 jednacího řádu,

– s ohledem na zprávu vyšetřovacího výboru o používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru (A9-0189/2023),

Obecný úvod

1. V červenci 2021 zveřejnil kolektiv investigativních novinářů, nevládních organizací a výzkumných pracovníků – projekt Pegasus (*Pegasus Project*) – zprávu na základě seznamu, který měli k dispozici a který obsahoval přibližně 50 000 telefonních čísel, na něž mohl být špionážní software Pegasus zaměřen. Tento špionážní software je hojně využíván autoritářskými i demokratickými vládami po celém světě, a to jak pod soudním dohledem, tak i bez něj, a cílí na novináře, právníky, soudce, aktivisty, politiky a státní úředníky. Lidé se stali terčem špionážního softwaru i v Evropské unii: někteří ze strany subjektů mimo EU a ze strany subjektů v rámci EU, včetně vládních orgánů. Vlády většiny členských států, ne-li všech, zakoupily špionážní software v zásadě pro účely vymáhání práva a bezpečnosti. Existuje však řada důkazů o tom, že špionážní software byl v několika členských státech zneužíván k čistě politickým účelům, k útokům na kritiky a odpůrce vládnoucích stran nebo v souvislosti s korupcí. Zjištění vyšetřování spojují Pegasus a další špionážní software s různými případy porušování lidských práv ze strany vlád, včetně sledování, vydírání, pomlouvačných kampaní, zastrašování a obtěžování. Vyvolává to znepokojení na různých úrovních právního řádu EU, pokud jde o ochranu a soukromí údajů, svobodu projevu, svobodu sdělovacích prostředků, svobodu sdružování, mechanismy nápravy a demokratické procesy a instituce. Ačkoli použití špionážního softwaru může uspět při posouzení nezbytnosti a přiměřenosti v případě hrozby pro národní bezpečnost, jeho zneužívání k politickým účelům je mimořádně znepokojující a vyvolává závažné obavy ohledně procesněprávní a hmotněprávní zákonnosti praktik sledování a úrovně ochrany, již skýtá unijní a vnitrostátní právo. Takové zneužívání špionážního softwaru přímo podrývá základní práva a demokracii, tedy základní hodnoty, na nichž je EU založena. Následné investigativní zprávy médií a dalších zdrojů prokázaly, že špionážní software je ze zemí EU vyvážen do třetích zemí s nedemokratickými režimy a vysokým rizikem porušování lidských práv, což je v příkrém rozporu s pravidly EU pro vývoz. Odvětví špionážního

softwaru je v EU pevně zavedeno a těží z velmi příznivých podmínek pro podniky.

2. V reakci na tento narůstající skandál se Evropský parlament dne 10. března 2022 rozhodl zřídit vyšetřovací výbor podle článku 226 Smlouvy o fungování EU s cílem vyšetřit údajné porušení nebo nesprávný úřední postup při provádění práva Unie v souvislosti s používáním softwaru Pegasus a ekvivalentního špionážního softwaru (dále jen „výbor PEGA“). Zatímco porušením je existence protiprávního jednání, ať už ve smyslu jednání nebo opomenutí v rozporu s právem, ze strany orgánů nebo institucí EU nebo orgánů členských států při provádění a prosazování práva EU, nesprávným úředním postupem se rozumí špatný nebo chybějící správní postup, k němuž dochází například tehdy, nejsou-li dodržovány zásady řádné správy. K příkladům nesprávného úředního postupu patří nesrovnalosti a opomenutí, zneužití moci, nespravedlnost, selhání nebo nezpůsobilost, diskriminace, ale také zpoždění, kterým lze předejít, odmítnutí poskytnout informace, nedbalost a další nedostatky, které znamenají nesprávné uplatňování práva Unie.

3. Pro účely tohoto šetření používal výbor PEGA široký přístup k tomu, co představuje špionážní software, konkrétně sledovací špionážní software, který je instalován do mobilních zařízení zneužitím zranitelností IT. Během šetření byla rovněž použita definice „zboží kybernetického dohledu“ stanovená v nařízení o zboží dvojího užití: definice toto zboží popisuje jako „zboží dvojího užití, které je speciálně navržené k tomu, aby umožňovalo tajné sledování fyzických osob prostřednictvím monitorování, extrakce, shromažďování nebo analýzy dat z informačních a telekomunikačních systémů“. Komise v září 2022 navrhla definici špionážního softwaru ve svém návrhu Evropského aktu o svobodě sdělovacích prostředků jako „špionážní software je jakýkoli produkt s digitálními prvky účelově navržený tak, aby zneužíval zranitelnosti jiných produktů s digitálními prvky a umožňoval skryté sledování fyzických nebo právnických osob prostřednictvím monitorování, získávání, shromažďování nebo analyzování údajů z těchto produktů nebo údajů o fyzických nebo právnických osobách, které tyto produkty používají, zejména formou tajného nahrávání hovorů nebo jiným využíváním mikrofonu zařízení koncového uživatele, natáčením fyzických osob, počítačů nebo jejich okolí, kopírováním zpráv, fotografováním, sledováním aktivity při prohlížení webových stránek, sledováním zeměpisné polohy, shromažďováním jiných údajů ze snímačů nebo sledováním činností na více zařízeních koncového uživatele, aniž by o tom byla dotčená fyzická nebo právnická osoba konkrétním způsobem informována a aniž by k tomu dala výslovný konkrétní souhlas“.

4. Dne 19. dubna 2022 zahájil výbor PEGA svou práci na shromažďování informací prostřednictvím veřejných slyšení, pracovních cest, konzultací s odborníky, žádostí o údaje, důkazů a výzkumu.

5. Během několika veřejných slyšení se vyšetřování zabývalo fungováním špionážního softwaru. Špionážní software je typ malwaru, který špehuje aktivity uživatele bez jeho vědomí a souhlasu. Toto sledování může zahrnovat zaznamenávání kláves, sledování aktivit a shromažďování dat, jakož i další formy krádeží dat. Špionážní software se obvykle šíří jako trojský kůň nebo tím, že zneužívá zranitelnosti softwaru[1]. Špionážní software lze na dálku nainstalovat do mobilních telefonů předem určených osob, a to i za hranicemi. V některých případech se k přenosu spywaru do cílového zařízení

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

používají telekomunikační sítě. Jakmile špionážní software pronikne do systému, deaktivuje ochranné mechanismy a bezpečnostní aktualizace. Infikované zařízení pak přenáší shromážděná data ze zařízení a umožňuje operátorům provádět dohled v reálném čase čtením příchozích textových zpráv, sledováním hovorů a polohy a přístupem ke zvuku a videu a jejich nahráváním prostřednictvím mikrofonu a kamery zařízení.

6. Na rozdíl od běžného odposlechu, který umožňuje pouze sledování komunikace v reálném čase, může špionážní software poskytnout úplný, zpětný přístup k souborům a zprávám vytvořeným v minulosti, heslům a metadatům o minulé komunikaci. V důsledku toho soudní rozhodnutí o datu zahájení a délce trvání sledovací operace neposkytuje účinné záruky, pokud špionážní software poskytuje plný zpětný přístup k údajům. Z technického hlediska je rovněž možné vydávat se za cílovou osobu díky získání přístupu k jejím digitálním údajům a identitě. Pro osobu, na kterou je sledování zacíleno, je velmi obtížné zjistit, zda došlo k průniku spywaru. Špionážní software nezanechává v cílovém zařízení žádné stopy nebo jich zanechává jen velmi málo, a i když je odhalen, je velmi obtížné prokázat, kdo byl za útok zodpovědný.

7. Výbor PEGA obdržel od vnitrostátních orgánů jen minimální nebo žádné odpovědi o pořizování a používání spywaru v jejich členských státech, ani o rozpočtových aspektech. Prodejci a země vydávající vývozní licence (převážně Izrael) o svých zákaznících žádné informace neposkytují. Mnohé orgány členských států neposkytly výboru PEGA smysluplné informace o právních rámcích upravujících používání spywaru nebo o používání spywaru ve svých členských státech nad rámec toho, co již bylo veřejně známo, a to zejména z důvodu vnitrostátních právních požadavků týkajících se utajení a důvěrnosti.

8. Některé členské státy zavedly špionážní software a odmítly se k tomu vyjádřit s odvoláním na národní bezpečnost, která podle čl. 4 odst. 2 Smlouvy o Evropské unii (SEU) „zůstává výhradní odpovědností každého členského státu EU“. Podle judikatury Soudního dvora Evropské unie (SDEU) a Evropského soudu pro lidská práva (ESLP) je však třeba sladit hlediska národní bezpečnosti se základními právy a demokratickými normami pevně zakotvenými v právu EU. Ačkoli je na členských státech, aby vymezily své základní zájmy národní bezpečnosti a přijaly vhodná opatření k zajištění své vnitřní a vnější bezpečnosti, SDEU rozhodl, že „pouhá skutečnost, že vnitrostátní opatření bylo přijato za účelem ochrany národní bezpečnosti, nemůže způsobit nepoužitelnost unijního práva a zprostit členské státy jejich povinnosti dodržovat toto právo“[2] a objasnil kritéria, jimiž se členské státy musí řídit při vymezování záležitostí spadajících do oblasti národní bezpečnosti. Několik členských států tvrdí, že používání spywaru spadá do oblasti národní bezpečnosti a že to vylučuje použitelnost práva EU. Pokud se však členské státy jen odkážou na národní bezpečnost jako takovou, nelze omezení základních práv odůvodnit tím, že spadá pod národní bezpečnost. Musí se použít právo EU se všemi zárukami, které poskytuje. Existuje řada důkazů o zneužívání spywaru z důvodů, které s národní bezpečností vůbec nesouvisejí. Členské státy by neměly mít možnost vyhnout se odpovědnosti za tak závažné zneužití špionážního softwaru pouhým odkazem na národní bezpečnost. Kvůli této nejednoznačnosti bylo obtížné získat dostatečné informace během slyšení a pracovních cest a na základě žádostí o

[2] Rozsudek ze dne 6. října 2020, *Privacy International* v. *Secretary of State for Foreign and Commonwealth Affairs a další*, C-623/17, ECLI:EU:C:2020:790.

informace. Nejednoznačnost definice národní bezpečnosti a příliš široký výklad jejího rozsahu ze strany vnitrostátních orgánů představují problém pro pochopení oprávněnosti používání spywaru.

9. Nicméně díky spojení informací z různých zdrojů byl výbor PEGA schopen rekonstruovat částečný, ale jasný obraz a dokázal identifikovat problémy, které vzbuzují obavy a zasluhují si další šetření.

10. Lze se bezpečně domnívat, že špionážní software určitým způsobem používají orgány ve všech členských státech, přičemž některé legitimně a jiné nelegitimně. Špionážní software může být pořízen přímo nebo prostřednictvím zmocněnců, zprostředkovatelských společností nebo prostředníků. Software lze buďto rovnou zakoupit, ale možné je i sjednání některých specifických služeb. Nabízeny mohou být i doplňkové služby, jako je školení zaměstnanců nebo dodání serverů. Špionážní software nelze vnímat izolovaně, ale jako součást široké škály produktů a služeb nabízených na expandujícím a lukrativním globálním trhu. Je důležité si uvědomit, že nákup a používání spywaru jsou velmi nákladné záležitosti, jejichž cena může dosahovat milionů eur. V mnoha členských státech však tyto výdaje nejsou zahrnuty do řádného rozpočtu, a mohou tak uniknout kontrole.

11. Z informací poskytnutých společností NSO Group víme, že Pegasus byl prodáván nejméně ve čtrnácti zemích EU, přičemž smlouvy se dvěma zeměmi byly později ukončeny. Není známo, o které země se jedná, ale obecně se usuzuje, že šlo o Polsko a Maďarsko. Protože však NSO Group ani izraelská vláda o ukončení smlouvy oficiálně neinformuje, nelze tuto informaci ověřit.

12. Dalším kouskem v mozaice je seznam účastníků veletrhu ISS World (*Intelligence Support Systems*) z roku 2013, kterému se přezdívá „ples odposlouchávačů“. S výjimkou Portugalska a Lucemburska zde byly zastoupeny všechny stávající členské státy EU, a to velkým počtem organizací, včetně místních policejních útvarů[3]. V posledních letech se společnost NSO Group stala hlavním sponzorem této akce, ale na seznamu sponzorů figurují také společnosti Intellexa, Candiru, RCS a mnoho dalších[4].

13. Členské státy nejsou pouze zákazníky komerčních prodejců špionážního softwaru, ale v obchodování se špionážním softwarem hrají i jinou roli. Některé poskytují jeho prodejcům zázemí či jsou oblíbenou destinací finančních a bankovních služeb, jiné zase aktérům tohoto průmyslu nabízejí občanství a povolení k pobytu.

14. V převážné většině členských států jsou zpravodajské služby regulovány právním rámcem, často s ustanoveními o organizaci a fungování těchto služeb, jakož i o jejich mandátech a pravomocích, včetně jejich prostředků činnosti a podmínek pro jejich využívání, a mechanismy dohledu, které zahrnují výkonnou kontrolu, parlamentní dohled, odborné orgány a soudní přezkum. Přesto se objevily obavy ohledně liberálního zpravodajského rámce některých zemí, neúčinných kontrol, laxních postupů dohledu a politického zasahování**.**

15. Je zřejmé, že špionážní software používá také policie, nikoli pouze zpravodajské služby. Panují závažné pochybnosti ohledně přípustnosti takových materiálů jako důkazů u

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

soudu v kontextu policejní a justiční spolupráce EU, a to i v rámci Europolu a Eurojustu, pokud by tyto informace byly získány pomocí vyšetřovacích metod uplatňovaných bez řádné soudní kontroly. V závislosti na vnitrostátních právních předpisech je používání špionážního softwaru ve vyšetřováních legitimní, pokud probíhá pod soudním dohledem.

16. Zneužívání špionážního softwaru ohrožuje demokracii a základní práva jednotlivých občanů. Od odhalení, která přinesl projekt Pegasus, podnikly Spojené státy několik kroků k vyšetřování a regulaci špionážního softwaru. V rámci EU se zatím podniklo jen velmi málo kroků. Je třeba stanovit jasná pravidla pro používání špionážního softwaru a obchod s ním, nejlépe ve spolupráci s dalšími zeměmi, jako jsou USA.

I. Používání špionážního softwaru v EU

I.A Polsko

17. Zástupci ministerstev se s delegací výboru odmítli setkat. V odpovědi na dotazník zaslaný výborem PEGA dne 15. července 2022 polské orgány neodpověděly na všechny otázky a trvaly na tom, že stávající předpisy jsou dostatečné a že postupují striktně v rámci zákona[5]. Ministr vnitra Mariusz Kaminski rovněž odmítl přijmout pozvání výboru PEGA k výměně názorů[6].

18. Pro výbor měla zásadní význam zjišťovací mise výboru PEGA do Polska v září 2022, která mu umožnila shromáždit informace a fakta o používání špionážního softwaru Pegasus. Jednání ve Varšavě vrhla nové světlo na nezákonné používání rušivého sledovacího softwaru proti demokratickým subjektům v Polsku. Poslanci se dozvěděli, jak byl odstraněn systém právních a institucionálních brzd a protivah, aby bylo možné cílit na osoby považované za politické odpůrce pomocí kybernetických zbraní vojenské kvality. V důsledku toho byly hrubě porušeny zásadní demokratické normy a práva občanů zakotvená v právních předpisech EU a Polska. Jde o další rozměr krize právního státu v Polsku.

NÁKUP SYSTÉMU PEGASUS

19. V listopadu 2016 se v domě tehdejšího izraelského premiéra Benjamina Netanjahua konala večeře, na kterou byla pozvána předsedkyně polské vlády a pozdější europoslankyně Beata Szydłová s ministrem zahraničí Witoldem Waszczykowskim[7]. Příštího roku v červenci se Szydłová a Netanjahu setkali s premiéry zemí Visegrádské čtyřky. Jednali prý o „posílení spolupráce v oblasti inovací a pokročilých technologií“ a o „otázkách týkajících se široce chápané bezpečnosti občanů“[8]. Nedlouho poté se uskutečnila schůzka mezi novým polským premiérem Mateuszem Morawieckim, maďarským premiérem Viktorem Orbánem a Benjaminem Netanjahuem, po níž polská vláda zakoupila software Pegasus[9].

---

[5] Odpověď stálého představitele Polska při EU Andrzeje Sadóse výboru PEGA, 7. září 2022.
[6] Odpověď ministra vnitra Mariusze Kaminského dopisem výboru PEGA, 12. července 2022.
[7] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29. ledna 2022.
[8] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29. ledna 2022.
[9] Financieele Dagblad, „*De wereld deze week: het beste uit de internationale pers*,“ 7. ledna 2022.

20. Polská vláda a předseda strany PiS Jarosław Kaczyński zpočátku nákup systému Pegasus popírali[10]. Začátkem ledna 2022 však potvrdili, že polská vláda špionážní software zakoupila[11] [12] [13]. Ve stejném měsíci vyšlo najevo, že klíčové důkazy týkající se nákupu systému Pegasus shromáždil Nejvyšší kontrolní úřad v roce 2018 během kontroly Fondu spravedlnosti, který provozuje ministerstvo spravedlnosti a který byl zřízen na podporu obětí trestných činů. Dne 18. ledna 2022 bývalý ředitel polského Nejvyššího kontrolního úřadu (NIK) a poté i nezávislý senátor Krzysztof Kwiatkowski poskytli svědectví týkající se nákupu softwaru Pegasus mimořádnému výboru Senátu pro případy sledování za použití softwaru Pegasus[14]. Poté, co byl zproštěn povinnosti mlčenlivosti spojené s jeho funkcí, předložil výboru dvě faktury potvrzující nákup špionážního softwaru pro Ústřední protikorupční úřad (CBA) za 25 milionů zlotých z Fondu spravedlnosti spravovaného ministerstvem spravedlnosti[15]. Kwiatkowski vypověděl, že tento úřad objevil účty Polské národní banky potvrzující uvedený převod[16].

21. Faktury vystavila společnost Matic Sp. z o.o., která působila jako zprostředkovatel, jehož prostřednictvím úřad CBA tento nákup realizoval[17]. Matic Sp. z o.o. je IT a bezpečnostní společnost se sídlem ve Varšavě, kterou vlastní a řídí osoby působící v komunitě zpravodajských a bezpečnostních služeb v období komunismu[18].

22. Společnost Matic se stala akciovou společností bezprostředně po koupi špionážního softwaru Pegasus v listopadu 2017 a podle deníku Gazeta Wyborcza provozuje svou činnost na základě licence ministerstva vnitra na obchodování s technologiemi s bezpečnostními službami a policií a na obchodování se zbraněmi[19]. Společnost má rovněž zvláštní osvědčení o licenci vydané Agenturou pro vnitřní bezpečnost, přičemž nejnovější takové osvědčení bylo vydáno v roce 2019, což jí umožňuje zachovat mlčenlivost o určitých důvěrných informacích až do konce tohoto desetiletí[20]. Zástupci společnosti Matic se odmítli s vyšetřovacím výborem sejít a poskytnout mu informace.

23. Podle polských zákonů může být činnost úřadu CBA financována pouze ze státního rozpočtu. Nákup systému Pegasus byl však financován z Fondu spravedlnosti, který

---

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

není součástí státního rozpočtu, ale veřejného fondu určeného pro oběti trestných činů[21]. Nákupem tak byly porušeny polské právní předpisy. Původní předpisy, jimiž se tento fond řídí, neumožňují jeho využití k financování operací zvláštních služeb[22]. V září však Michał Woś, náměstek ministra spravedlnosti[23] a blízký spolupracovník ministra spravedlnosti Zbigniewa Ziobra[24], předložil Výboru Sejmu (dolní komora polského parlamentu) pro veřejné finance návrh na změnu finančního plánu Fondu pro spravedlnost. Poslanci tuto změnu schválili. Když se později ukázalo, že Fond spravedlnosti byl použit na financování softwaru Pegasus pro úřad CBA, poslanci uvedli, že „během zasedání výboru o tom nepadlo ani slovo“[25]. Zdá se tedy, že byli vládou uvedeni v omyl. Přestože Nejvyšší kontrolní úřad podal oficiální oznámení státnímu zastupitelství ohledně porušení zákona v souvislosti s použitím prostředků z Fondu spravedlnosti na nákup softwaru Pegasus v roce 2017, nelze očekávat, že by státní zastupitelství v takové věci vzhledem k současnému institucionálnímu a politickému prostředí podniklo kroky.

24. Woś rovněž požádal ministerstvo financí o souhlas s přerozdělením 25 milionů PLN vynaložených na software Pegasus z Fondu spravedlnosti na „jinou činnost“ zaměřenou na „boj proti následkům trestné činnosti“. Náměstek ministra poté schválil převody z Fondu spravedlnosti na Ústřední protikorupční úřad. Na dotaz z ledna 2022 však Woś nejprve popřel, že by měl nějaké povědomí o samotném nástroji Pegasus, natož o jeho koupi státem, ale později jeho nákup potvrdil. Není jasné, jak jsou financovány provozní náklady na používání daného softwaru.

25. Bylo oznámeno, že NSO Group dosud prodala software Pegasus celkem 14 zemím v Evropě. Připustila však rovněž, že dvěma z těchto zemí licenci odňala[26]. Během své výpovědi ve výboru PEGA společnost NSO Group uvedla, že „problémy“ týkající se používání softwaru Pegasus vyšetřuje pouze tehdy, když obdrží informace od oznamovatelů nebo prostřednictvím médií. Když NSO Group obdrží stížnosti, prošetří je a přezkoumá a následně může odstavit software Pegasus pro subjekty, které jej zneužily[27]. Na základě velkého počtu zpráv ve sdělovacích prostředcích o používání softwaru Pegasus v Polsku je velmi pravděpodobné, že vzhledem k tomu, že Polsko porušilo podmínky jeho používání stanovené společností NSO, bylo zařazeno mezi

---

[21] The Guardian, „*More Polish opposition figures found to have been targeted by Pegasus spyware*“ (Další představitelé polské opozice se stali terčem špionážního softwaru Pegasus), 17. února 2022; The Guardian, „*Polish senators draft law to regulate spyware after anti-Pegasus testimony*“ (Polští senátoři po svědectví proti programu Pegasus navrhují zákon o regulaci spywaru), 24. ledna 2022. Zpráva Komise 2022 o právním státu, kapitola o situaci v oblasti právního státu v Polsku, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, s. 26; Gazeta Wyborcza, https://www.rp.pl/polityka/art19250101-gazeta-wyborcza-jak-kupowano-pegasusa-dla-cba, 3. ledna 2022.

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

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

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

[26] Diskuse se společností NSO Group, pracovní cesta vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru do Izraele, červenec 2022.

[27] Svědectví Chaima Gelfanda, generálního poradce a ředitele pro dodržování předpisů, NSO, ve výboru PEGA, 21. června 2022.

jednu z těchto dvou zemí. To však nebylo potvrzeno.

26. Od prvních náznaků používání systému Pegasus polskými orgány se polský veřejný ochránce práv snažil u úřadů zjistit, zda se tak děje, a mimo jiné prostřednictvím každoročních zpráv pro polský parlament se zasazoval o zlepšení demokratických a lidskoprávních záruk, aby se zabránilo zneužívání sledování. V lednu 2023 zaslala polská veřejná ochránkyně práv ministru vnitra dopis, v němž uvedla, že neexistuje žádný právní základ pro používání špionážního softwaru Pegasus nebo podobného špionážního softwaru v Polsku, přičemž odkázala na judikaturu polského ústavního soudu a na judikaturu ESLP[28].

PRÁVNÍ RÁMEC

27. V roce 2014 posuzoval polský ústavní soud zákon o policii z roku 1990 a jiné zákony upravující sledování občanů[29]. Označil je za odporující ústavě, formuloval konkrétní doporučení a stanovil 18měsíční lhůtu, do níž měly být v zákonech provedeny příslušné změny[30]. Legislativní změny provedla vláda, která vzešla z voleb v roce 2015. Zákon, kterým byl pozměněn zákon o policii z roku 1990 a některé další zákony, však z právní úpravy neodstranil žádné z nedostatků, jejichž nápravu požadoval ústavní soud[31]. Zákon o policii z roku 2016 naopak oslabil existující ustanovení, která sama o sobě dostatečně nechránila práva občanů ani nezajistila řádný dohled.

28. Benátská komise ve svém stanovisku k zákonu o policii z roku 2016 uvedla, že „... procesní záruky a materiální podmínky stanovené v zákoně o policii k tajnému sledování stále nepostačují k tomu, aby zabránily nadměrnému používání a bezdůvodnému zasahování do soukromí občanů“[32]. V rozporu s rozsudky ESLP je navíc také nedostatečná specifikace, pokud jde o dohled, záruky proti zneužívání a kategorie osob a trestných činů, na které se lze při sledování zaměřit[33]. Zejména v rozsudku ve věci *Roman Zacharov* v. Rusko z roku 2015 se ESLP zabýval nutností zajistit jasné podmínky používání špionážního softwaru. Bylo konstatováno, že v souvislosti s tajným sledováním občanů je třeba stanovit přísná kritéria, řádný soudní dohled, okamžité zničení irelevantních údajů, soudní kontrolu naléhavých postupů a požadavek na oznamování obětí[34]. Soud navíc výslovně uvedl, že by bylo „v rozporu se zákonem“, pokud by o tajném sledování rozhodovala výlučně soudní výkonná moc[35]. Zákon o policii z roku 2016, který zůstává v Polsku v platnosti, toto rozhodnutí nijak

[28] Schůze výboru PEGA, 19. ledna 2023.
[29] Stanovisko č. 839/2016 k zákonu ze dne 15. ledna 2016, kterým se mění zákon o policii a některé další zákony, přijaté Benátskou komisí na jejím 107. plenárním zasedání ve dnech 10.–11. června 2016.
[30] https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani.
[31] Zákon ze dne 15. ledna 2016, kterým se mění zákon o policii a některé další zákony v článku 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf .
[32] Stanovisko č. 839/2016 k zákonu ze dne 15. ledna 2016, kterým se mění zákon o policii a některé další zákony, přijaté Benátskou komisí na jejím 107. plenárním zasedání ve dnech 10.–11. června 2016.
[33] Viz mimo jiné *Roman Zacharov* v. *Rusko* [velký senát], č. 47143/06, rozsudek ESLP ze dne 4. prosince 2015; *Klass a další* v. *Německo*, č. 5029/71, rozsudek ESLP ze dne 6. září 1978, bod 40; *Prado Bugallo* v. *Španělsko*, č. 58496/00, rozsudek ESLP ze dne 18. února 2003, bod 30; *Liberty a další* v. *Spojené království*, č. 58243/00, rozsudek ze dne 1. července 2008, bod 62.
[34] *Roman Zacharov* v. *Rusko* [velký senát], č. 47143/06, rozsudek ESLP ze dne 4. prosince 2015.
[35] *Roman Zacharov* v. *Rusko*, [velký senát], č. 47143/06, rozsudek ESLP ze dne 4. prosince 2015, bod 229 a 230; Viz také stanovisko Benátské komise č. 839/2016, červen 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e, s. 11.

nereflektuje. Jeho ustanovení jsou totiž v přímém rozporu s velkou částí rozsudku.

29. Evropský soud pro lidská práva se rovněž jednoznačně vyjádřil ke kritériu nezbytnosti, což znamená, že sledování musí mít dostatečný význam k tomu, aby vyžadovalo takové narušení soukromí. V rozsudku ve věci *Klass a další* v. *Německo* z roku 1978 je tento bod ujasněn, přičemž se v něm uvádí, že nehledě na systém použitý ke sledování, soud musí být přesvědčen, že „proti zneužití [existují] přiměřené a účinné záruky“[36]. Pečlivě zorganizované zničení systému brzd a protivah v Polsku je projevem zjevného vzdoru vládnoucí strany vůči soudům. Navzdory všem těmto skutečnostem vláda vedená PiS trvá na tom, že stávající ustanovení jsou dostatečná a že fungují striktně v mezích zákona[37]. Vláda zároveň odmítá všechny žádosti o dialog a vysvětlení, jak se v Polsku používá sledování.

PROTITERORISTICKÝ ZÁKON Z ROKU 2016

30. Kromě zákona o policii byl v Sejmu v roce 2016 přijat také zákon o sledování zahraničních občanů, označovaný jako „zákon o protiteroristické činnosti“. Podle tohoto zákona mohou být občané jiných států monitorováni bez souhlasu soudu po dobu tří měsíců, pokud existují pochybnosti o jejich totožnosti. Zákon povoluje odposlouchávání telefonů, snímání otisků prstů, pořizování biometrických fotografií a získávání vzorků DNA a stanovuje povinnost registrovat předplacené telefonní karty[38]. Podle článku 9.8 tohoto zákona má Nejvyšší státní zástupce pravomoc nařídit zničení nerelevantních materiálů. Vzhledem k tomu, že současný Nejvyšší státní zástupce Zbigniew Ziobro je zároveň ministrem spravedlnosti, existují vážné obavy, zda je schopen přijímat nezávislá a nestranná rozhodnutí, aniž by byl ovlivňován politickými zájmy vlády, kterou zastupuje[39] [40].

TRESTNÍ ŘÁD

31. V červenci 2015 byla přijata novela polského trestního řádu, kterou bylo zakázáno používat v trestním řízení protizákonně získané důkazy. V březnu 2016 však byl po nástupu strany PiS k moci trestní řád pozměněn znovu, aby zahrnoval článek 168a[41]. Nový článek 168a označuje za přípustné v trestních řízeních i důkazy získané v rozporu se zákonem, nebo jak se někdy říká, „ovoce z otráveného stromu“, tedy i informace opatřené pomocí softwaru Pegasus[42]. Je však třeba dodat, že Nejvyšší soud Polska ve svém rozsudku uvedl, že tento článek nelze použít v rozporu s ustanoveními Evropské úmluvy o lidských právech a Ústavy Polska, která v některých případech omezuje jeho účinné uplatňování[43]. Rovněž byly vydány rozsudky, v nichž byl článek 168a shledán částečně protiústavním[44]. Nicméně přítomnost tohoto ustanovení v právním řádu

[36] *Klass a další* v. *Německo*, 6. září 1978, bod 50, série A č. 28. 40.
[37] Dopis Mariusze Kaminského, ministra vnitra a správy Polska, výboru PEGA, 8. září 2022.
[38] Zákon z 10. června 2016 o protiteroristické činnosti, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf.
[39] Zákon z 10. června 2016 o protiteroristické činnosti, 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. června 2016.
[41] Zákon ze dne 11. března 2016, kterým se mění trestní řád a některé další zákony, 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.
[43] Např. rozsudek Nejvyššího soudu Polska ze dne 26. června 2019, IV KK 328/18.
[44] Např. rozsudek Nejvyššího soudu Polska ze dne 26. června 2019, IV KK 328/18.

vyvolává nejistotu, pokud jde o dodržování základních práv.

ZÁKON O TELEKOMUNIKACÍCH

32. Po změně zákona o telekomunikacích z roku 2004 z roku 2016 obsahuje zákon o telekomunikacích v Polsku ustanovení umožňující policii získat neomezený přístup k metadatům a v některých případech bez účasti zaměstnanců telekomunikačních společností[45]. Tento přístup lze získat na základě velmi širokého odůvodnění „prevence nebo odhalování trestných činů“. Po získání údajů pak o dalším postupu rozhodne nejvyšší státní zástupce. To však nelze považovat za záruku vzhledem k tomu, že kvůli sloučení úlohy ministra spravedlnosti a nejvyššího státního zástupce nelze státní zastupitelství považovat za nezávislé na výkonné moci[46].

33. Výše uvedená změna trestního řádu, která umožňuje využívat „ovoce z otráveného stromu“, měla velký dopad na význam telekomunikačních operátorů a údajů, které společnosti uchovávají. V Polsku jsou největší telekomunikační poskytovatelé fakticky povinni mít specializovaný tým, který reaguje na četné žádosti orgánů o odposlech. Obvykle však nemají příliš velký přehled o obsahu odposlechů ani o operativních detailech jednotlivých případů[47].

AKT, KTERÝM SE PROVÁDÍ SMĚRNICE O PROSAZOVÁNÍ PRÁVA

34. Polsko řádně neprovedlo směrnici o prosazování práva (EU) 2016/680[48], která vyžaduje zvláštní normy pro shromažďování a zpracování osobních údajů policií a jinými službami. Směrnice o prosazování práva byla do polského práva provedena zákonem z roku 2018 o ochraně osobních údajů zpracovávaných v souvislosti s prevencí a potíráním trestné činnosti. Zákon výrazně rozšířil rozsah důvodů stanovených ve směrnici pro odmítnutí oznámit fyzickým osobám zpracování jejich údajů a nerespektoval mechanismus stanovený v článku 17 směrnice, což dává fyzickým osobám možnost vykonávat svou pravomoc prostřednictvím příslušného orgánu dozoru – v Polsku je jím předseda Úřadu pro ochranu osobních údajů. Zákon dále stanoví významnou výjimku pro národní bezpečnost, včetně provádění statutárních úkolů různými složkami bezpečnostních sil[49].

---

[45] Zákon o telekomunikacích ze dne 16. července 2004 https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004.

[46] Zákon ze dne 15. ledna 2016, kterým se mění zákon o policii a některé další zákony v článku 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.

[47] https://www.europarl.europa.eu/doceo/document/PEGA-CR-736647_CS.pdf; The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, 17. února 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, s. 16-17.

[48] Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (Úř. věst. L 119, 4.5.2016, s. 89).

[49] Adam Bodnar et al., „*How to saddle Pegasus: Observance of civil rights in the activities of security services: objectives of the reform*“ (Jak osedlat Pegase: Dodržování občanských práv při činnosti bezpečnostních služeb: Cíle reformy), září 2019 https://bip.brpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20(OSIOD%C5%81A%C4%86%20PEGAZA).pdf.

35. Polsko dosud neprovedlo směrnici EU o oznamovatelích. Po neúspěchu původního návrhu právního předpisu nedodrželo lhůtu pro prosinec 2021. Druhý návrh byl zveřejněn v dubnu 2022, ale nedošlo k žádnému dalšímu pokroku a navrhované právní předpisy obsahují výrazně slabší ustanovení. V lednu 2022 zahájila Komise řízení o nesplnění povinnosti proti Polsku z důvodu neprovedení směrnice v plném rozsahu a v únoru 2023 se Komise rozhodla obrátit se na Soudní dvůr EU[50].

36. Polský Sejm, zejména členové strany PiS, v současné době připravuje zákon o elektronických komunikacích. Tento zákon by orgánům usnadnil přístup k e-mailům a zprávám polských občanů na sociálních médiích. Poskytovatelé by museli ukládat e-maily a zprávy na svých serverech, aby příslušné soudy mohly nařídit přístup k údajům, IP adresám a obsahu zpráv[51].

PŘEDBĚŽNÁ KONTROLA

37. Ačkoli sledování osob musí být v Polsku v zásadě povoleno soudem, v praxi již povolovací postup neslouží jako záruka, že sledování nebude zneužito, nýbrž jako prostředek k tomu, aby se špionáži pro politické účely dodalo zdání legality. Nebylo ani výslovně sděleno, zda sledování osob pomocí softwaru Pegasus vůbec probíhalo se soudním povolením. Žádosti o povolení ke sledování osob podávají zvláštní útvary[52]. Při posuzování žádostí mají soudci k dispozici pouze informace, které poskytl žadatel (tj. zvláštní služby), a o rozsahu poskytnutých informací rozhoduje státní zástupce[53]. Často se jedná o pouhé shrnutí, někdy bez elementárních detailů o sledované osobě (jméno, povolání, trestný čin, z jehož spáchání je daná osoba podezřelá), a o popis toho, jaké sledovací techniky mají být použity.

38. Pokud soudce zamítne návrh, je povinen toto rozhodnutí odůvodnit a lze se proti němu odvolat[54]. V naléhavých případech může státní zástupce nejprve povolit použití odposlechových metod bez souhlasu soudce, pokud soud následně do pěti dnů vydá povolení[55]. Jedná se o významnou a záměrnou mezeru v polském právním rámci.

39. Žádosti o povolení sledování ze strany hlavních agentur, tj. CBA, policie (Policja KGP) a zpravodajských služeb ((Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, Służba Ochrony Państwa, Biuro Nadzoru Wewnętrznego MSWiA, a a nedávno doplněný Inspektorat Służby Więziennej) jsou předkládány téměř výlučně okresnímu soudu ve Varšavě (Sad Okręgowy), kde je sídlí většina těchto agentur.

40. Každý den je podáno několik desítek žádostí o sledování, což snižuje schopnost soudu

[50] https://ec.europa.eu/commission/presscorner/detail/cs/ip_23_703.
[51] Euractiv, „*Polish government working on controversial surveillance bill*“ (Polská vláda pracuje na kontroverzním návrhu zákona o dohledu), https://www.euractiv.com/section/politics/news/polish-government-working-on-controversial-surveillance-bill/.
[52] Zákon ze dne 15. ledna 2016, kterým se mění zákon o policii a některé další zákony v článku 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf .
[53] Zákon ze dne 15. ledna 2016, kterým se mění zákon o policii a některé další zákony v článku 20c, 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.

provést důkladné posouzení každé žádosti[56]. Systém, který náhodně přiděluje věci soudcům soudů, je v Polsku z technického hlediska stále funkční, ale funguje pouze v úředních hodinách. Avšak vzhledem k tomu, že soud povoluje funkce sledování po dobu 24 hodin, existuje dostatek příležitostí k tomu, aby byl systém obcházen. V případě podání žádosti o víkendu nebo mimo běžnou pracovní dobu bude věc automaticky přidělena soudci, který je v pohotovosti[57]. Informace o tom, kdo je v danou chvíli na příjmu, jsou známy tajným službám, které si tak mohou v podstatě vybrat „spřáteleného soudce“, jemuž mohou předkládat své žádosti o sledování[58]. Náhodné přidělování lze navíc obejít i prostřednictvím pracovníků IT, kteří mají přístup do systému a mohou přidělovat oprávnění ke sledování „spřáteleným soudcům“[59]. To vše vážně narušuje schopnost soudu vykonávat účinný soudní dohled.

NÁSLEDNÁ KONTROLA

41. Parlamentní kontrola v Polsku v podstatě neexistuje. Před rokem 2016 vedl parlamentní výbor pro dohled nad zvláštními službami (KSS) rotující předsednictví vládnoucích a opozičních stran. Strana PiS však změnila toto parlamentní pravidlo a jmenovala členy PiS Waldemar Andzela stálým předsedou a Jarosława Krajewského místopředsedou tohoto výboru[60]. Vládní strany ostatně mají ve výboru absolutní většinu[61]. Kontrolní funkce výboru tak ztrácí smysl. Vládní většina v Sejmu také odmítla výzvy, aby bylo zahájeno parlamentní vyšetřování na základě informací o nezákonném používání špionážního softwaru[62] [63] [64] [65] [66]. Na druhé straně Senát, kde vládní strany nemají většinu, zřídil na začátku roku 2022 vyšetřovací výbor. Senátní výbor však nemá vyšetřovací pravomoci jako Sejm[67], jehož vyšetřovací výbor může předvolávat svědky a vyslechnout přísežné svědectví. Proti výboru se na každém kroku staví vládnoucí strana

[56] Svědectví Ewy Wroszekové, slyšení pro jednotlivé země týkající se Polska, schůze vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, 15. září 2022.
[57] Svědectví Ewy Wroszekové, slyšení pro jednotlivé země týkající se Polska, schůze vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, 15. září 2022.
[58] Svědectví Ewy Wroszekové, slyšení pro jednotlivé země týkající se Polska, schůze vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, 15. září 2022.
[59] Svědectví Ewy Wroszekové, slyšení pro jednotlivé země týkající se Polska, schůze vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, 15. září 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. ledna 2022.
[63] Evropská komise 2022, Zpráva o právním státu, kapitola o situaci v oblasti právního státu v Polsku,https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, s. 27.
[64] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosince 2021.
[65] The Guardian, „*Polish senators draft law to regulate spyware after anti-Pegasus testimony*“ (Polští senátoři po svědectví proti programu Pegasus navrhují zákon o regulaci spywaru), 24. ledna 2022
[66] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18. ledna 2022.
[67] Evropská komise 2022 Zpráva o právním státu, kapitola o situaci v oblasti právního státu v Polsku,https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf na str. 27, poznámka pod čarou č. 220.

v Sejmu[68], vládní úředníci a bezpečnostní agentury, kteří odmítají spolupracovat nebo vést vlastní vyšetřování[69].

42. Kontrola a opravné prostředky, které nabízejí jiné nezávislé subjekty, byly rovněž výrazně oslabeny. Nejvyšší kontrolní úřad má účinné pravomoci dohledu; jeho členové a zaměstnanci jsou však vystaveni neustálým překážkám, obtěžování a zastrašování, což má závažný dopad na jeho provozní kapacitu[70]. Sejmu dosud nejmenoval 10 z 19 členů rady NIK[71]. Požadované prověřování členů rady, které provádějí zvláštní útvary vedené ministrem Kaminskim, je velmi pomalé[72].

43. Pokud NIK zjistí porušení zákona, má pravomoc podat oznámení státnímu zastupitelství[73]. Je však na úřadu státního zástupce, aby zahájil řízení na základě tohoto oznámení. V situacích, kdy státní zástupce nepodnikne žádné kroky, může NIK učinit jen málo. Pokud se oznámené porušení týká činnosti samotného státního zastupitelství, vytváří se začarovaný kruh neodpovědnosti. Kromě toho všechny případy oznámené NIK úřadu státního zástupce musí být nahlášeny nejvyššímu státnímu zástupci, který je rovněž ministrem spravedlnosti, který v první řadě vedl samotné ministerstvo, které spyware zakoupilo. Nejvyšší státní zástupce má pravomoc ukončit nebo obnovit vyšetřování, které bylo ukončeno státním zastupitelstvím. Může také zahájit kárné řízení proti státním zástupcům, u nichž má podezření, že přijali nesprávná rozhodnutí.

44. Současný veřejný ochránce práv Marcin Wiącek byl jmenován v roce 2021, kdy se Sejm a Senát po dlouhém přetahování dohodly na nestranném kompromisním kandidátovi[74]. Pokud jde o případ senátora Brejzy, Wiącek tvrdil, že veřejný ochránce práv by se neměl angažovat v raných fázích případu. Navzdory tomu jak bývalí, tak i stávající veřejní ochránci práv situaci sledovali a vyvíjeli určitý tlak ohledně nutnosti vytvořit nezávislý orgán dohledu, který by zajišťoval demokratickou kontrolu

[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. ledna 2022.
[69] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17. ledna 2022; Evropská komise 2022 Zpráva o právním státu, kapitola o situaci v oblasti právního státu v Polsku, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, s. 27. AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosince 2021; The Guardian, „*Polish senators draft law to regulate spyware after anti-Pegasus testimony*“ (Polští senátoři po svědectví proti programu Pegasus navrhují zákon o regulaci spywaru), 24. ledna 2022. Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18. ledna 2022.
[70] Reuters, https://www.reuters.com/article/poland-pegasus-idUSL8N2UF596, 4. února 2022; Diskuse s Nejvyšším kontrolním úřadem, mise vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, září 2022.
[71] https://www.nik.gov.pl/en/about-us/the-council-of-nik/; Diskuse se zaměstnanci Nejvyššího kontrolního úřadu, mise vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, září 2022.
[72] Diskuse se zaměstnanci Nejvyššího kontrolního úřadu, mise vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, září 2022.
[73] Zákon ze dne 23. prosince 1994 o Nejvyšším kontrolním úřadu https://www.nik.gov.pl/en/about-us/legal-regulations/act-on-the-supreme-audit-office.html, článek 63.
[74] Euractiv, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/, 22. července 2021.

nad fungováním tajných služeb[75].

PODÁVÁNÍ ZPRÁV

45. Podle zákona o policii z roku 2016 je policie sice povinna podávat příslušným soudům dvakrát ročně zprávy o tom, kolik údajů o telekomunikacích, poštovním styku nebo internetovém provozu shromáždila, s příslušným právním zdůvodněním (prevence nebo odhalování trestných činů, ochrana života nebo zdraví osob, pomoc při záchranných operacích)[76]. Tyto zprávy jsou vypracovávány pouze *ex post* a nezveřejňují se. Pokud soud narazí ve zprávě na problém, může do 30 dnů zaslat své připomínky. Nemá však možnost nařídit zničení údajů, a to ani pokud by bylo zjištěno, že byly shromážděny v rozporu se zákonem. Nejdůležitější je však to, že soudní dohled je pouze volitelný, zákon ho neukládá jako povinnost.

ZJEDNÁNÍ NÁPRAVY

46. I přes četné důkazy o tom, že byly spáchány závažné trestné činy, polský státní zástupce dosud jednal velmi zdržujícím způsobem. Zdá se, že soudy se zabývaly pouze případem prokurátorky Ewy Wrzosekové a Krzysztofa Brejzy. Paní Wrzoseková nejprve podala žalobu na státní zastupitelství. Když se však úřad odmítl případem zabývat, mohla se obrátit na soud. Na konci září 2022 varšavský obvodní soud v Mokotówě nařídil státnímu zástupci zahájit vyšetřování. Státní zástupce však dosud neprovedl žádné smysluplné úkony, které jsou nezbytné pro další postup v těchto případech, jako je například získání svědectví osoby, která byla cílem.

47. Je třeba poznamenat, že paní Wrzoseková mohla podat tento opravný prostředek u soudů pouze v důsledku oficiálního zamítnutí ze strany státního zastupitelství. V mnoha jiných případech státní zástupce protahuje vyšetřování, aby nemusel vydat oficiální odpověď, neboť si je vědom toho, že pokud tak učiní, bude vystaven odvolacímu řízení u soudů.

48. Občané, kteří se stali obětí útoku ze strany uvedeného špionážního softwaru, mohou podat občanskoprávní žalobu k soudu, důkazní břemeno pro prokázání, že byli předmětem sledování, však nesou sami a je prakticky nemožné prokázat nezákonné používání špionážního softwaru bez spolupráce příslušných orgánů. Nedostatečné plnění oznamovací povinnosti v Polsku, jak je uvedeno v rozsudku ve věci *Klass*, znamená, že mnoho osob se vůbec nemusí dovědět, že se staly obětí těchto útoků.

49. V současnosti jsou na ESLP podané věci *Pietrzak* v. *Polsko* a *Bychawska-Siniarska*v. *Polsko*, ve kterých se namítá vůči chybějící transparentnosti, dohledu, informování a prostředkům nápravy v souvislosti se sledováním v Polsku. Důležité je, že Soudní dvůr se rozhodl uspořádat v těchto věcech výjimečné jednání, které se konalo dne 27. září 2022. Tyto případy podalo pět občanů[77], kteří podali stížnost k ESLP v září 2017 a v

[75] Evropský parlament. Generální ředitelství pro parlamentní výzkumné služby, „Evropská PegasusGate: Boj proti zneužívání špionážního softwaru“ – studie, 6. července 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, červenec 2022, str. 20.

[76] Zákon ze dne 15. ledna 2016, kterým se mění zákon o policii a některé další zákony v článku 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.

[77] Mikołaj Pietrzak, právník, děkan Varšavské advokátní komory; Dominika Bychawska-Siniarska, členka a zaměstnankyně Helsinské nadace pro lidská práva; Barbara Grabowska-Morozová, vysokoškolská přednášející a

únoru 2018. Jedenáct subjektů předložilo v tomto případě informace *amicus curiae*, včetně Evropské advokátní komory v trestních věcech[78], polského veřejného ochránce práv a zvláštního zpravodaje OSN pro podporu a ochranu lidských práv v rámci boje proti terorismu[79].

50. Ačkoli je tato možnost podání stížnosti k Evropskému soudu pro lidská práva otevřena občanům, je vzhledem k délce řízení sporné, zda se jedná o účinný opravný prostředek. Pět let po podání první stížnosti soud v této věci stále nerozhodl.

51. Na základě článku 227 správního řádu byly stížnosti podány dříve v roce 2017 předsedovi vlády a příslušným vedoucím různých policejních a zpravodajských služeb. Mezi tyto zpravodajské služby patřily Ústřední protikorupční úřad (CBA), Agentura pro vnitřní bezpečnost, Národní daňová správa, vojenská kontrarozvědka, státní policie, pohraniční policie a národní četnictvo. Jejich stížnost se týkala skutečnosti, že právní předpisy umožňovaly příslušníkům těchto policejních a zpravodajských služeb sledovat jejich telekomunikace a digitální komunikaci bez jejich vědomí. Vzhledem k tomu, že členové dotčených služeb nebyli povinni je informovat o možném sledování, nemohli žalobci v důsledku toho nechat přezkoumat legalitu této činnosti soudem, což je podle jejich názoru v rozporu s polskou ústavou.

52. V období od června do září 2017 vedoucí výše uvedených policejních a zpravodajských služeb zaslali své odpovědi na stížnosti žalobců. S odvoláním na článek 8 (právo na respektování soukromého a rodinného života) Evropské úmluvy o lidských právech si žalobci stěžovali, že tajné systémy monitorování telekomunikací, poštovní a digitální komunikace a shromažďování metadat zavedené v rámci uplatňování zákona o policii a zákona o boji proti terorismu narušují jejich právo na respektování jejich soukromého života. S odvoláním na článek 8 ve spojení s článkem 13 (právo na účinný opravný prostředek) žalobci tvrdí, že nemají účinný opravný prostředek, který by jim umožnil zjistit, zda byli sami podrobeni tajnému sledování, a případně nechat přezkoumat zákonnost tohoto sledování soudem.

VEŘEJNÁ KONTROLA

53. Jedním z prvků demokratického systému brzd a protivah jsou nezávislá média, která plní funkci veřejné kontroly. V případě používání špionážního softwaru se však polská veřejnoprávní televize, kterou do značné míry ovládají vládní strany, stala naopak komplicem – zveřejnila totiž materiály získané z telefonů několika obětí, mezi nimiž byl i opoziční senátor Krzysztof Brejza. Zveřejnění informací získaných při sledování speciálními službami je samo o sobě trestným činem, přesto policie ani státní zastupitel nepodnikli žádné kroky.

POLITICKÁ KONTROLA

---

výzkumná pracovnice a externí expertka Helsinské nadace pro lidská práva; Wojciech Klicki a Katarzyna Szymielewicz, členové Nadace Panoptykon se sídlem ve Varšavě.

[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.

54. Řadu klíčových pozic napříč celým řetězcem drží členové či spojenci vládních stran. Ministr vnitra a koordinátor zvláštních útvarů Mariusz Kaminski byl v roce 2015 odsouzen za zneužívání pravomocí ke třem letům vězení[80]. Ovšem ihned po parlamentních volbách v roce 2015 ho prezident Duda omilostnil, a to vysoce nestandardním postupem, který si vysloužil kritiku polského nejvyššího soudu, Soudního dvora EU, Benátské komise, amerického ministerstva zahraničí a dalších. Vyvstávají tak pochybnosti o jeho nezávislosti a neutralitě. Pan Kaminski se rovněž odmítl setkat s výborem PEGA nebo s ním významně spolupracovat[81].

55. Ústřední protikorupční úřad je plně kontrolován vládnoucí většinou a není nezávislý, přestože jeho název a mandát byly stanoveny zákonem ze dne 9. června 2006 o Ústředním protikorupčním úřadu[82], jehož čl. 1 odst. 1 stanoví, že „[ú]střední protikorupční úřad... je zřízen jako zvláštní služba pro boj proti korupci ve veřejném a hospodářském životě, zejména ve veřejných a místních vládních institucích, jakož i pro boj proti činnostem poškozujícím hospodářské zájmy státu“[83]. Ve výroční zprávě o právním státu 2022 Komise konstatuje, že „nezávislost hlavních protikorupčních institucí zůstává problémem, zejména s ohledem na podřízení Ústředního protikorupčního úřadu výkonné moci a ministr spravedlnosti je rovněž nejvyšším státním zástupcem“[84].

56. Snaha vlády získat kontrolu nad soudnictvím byla široce zdokumentována a potvrzena řadou instancí, včetně Komise, Soudního dvora EU a Evropského soudu pro lidská práva.

57. Nejenže byl vytvořen právní a institucionální kontext, který umožňuje téměř neomezené sledování špionážním softwarem, ale téměř všechny části procesu jsou rovněž pevně kontrolovány vládními stranami. Výsledkem je, že záruky, které mohou existovat na papíře, nemají v praxi žádný nebo mají jen malý význam.

CÍLE SLEDOVÁNÍ

58. První zdokumentované případy použití softwaru Pegasus v Polsku pocházejí z roku 2018. Jeden z nich se týkal bývalého náměstka ministra financí Pawła Tamborského, jehož telefon byl v únoru 2018 napaden softwarem Pegasus, jak odhalily Amnesty International a Wyborcza v červenci 2022. Téhož dne Ústřední protikorupční úřad zadržel jeho a pět bývalých úředníků ministerstva a analytiků trhu, kteří byli obviněni z podhodnocení tržní hodnoty chemické společnosti CIECH výměnou za úplatky. Soud s jejich zatčením nesouhlasil a nařídil jejich propuštění. Terčem útoku se stal také generální ředitel a majitel PR agentury Cross Media Andrzej Długosz, jehož zařízení byla od března 2018 do listopadu 2019 napadena nejméně 61krát. Veřejná ochránkyně práv následně požádala příslušné orgány o více informací, ale její úsilí bylo neúspěšné.

[80] *Reuters*, https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117, 17. listopadu 2015.
[81] EU Observer, https://euobserver.com/rule-of-law/156063, 15. září 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, článek 1.1.
[84] Zpráva Komise 2022 o právním státu, kapitola o situaci v oblasti právního státu v Polsku, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, s. 1.

V té době vláda nákup špionážního softwaru stále ještě popírala.

59. Jak víme díky vyšetřování, které vedli novináři z organizace Associated Press a výzkumníci z torontského univerzitního pracoviště Citizen Lab, byl spyware Pegasus v roce 2019[85] v Polsku použit proti nejméně třem osobám. Byli to jmenovitě opoziční senátor Krzysztof Brejza, právník Roman Giertych a státní zástupkyně Ewa Wrzoseková. Někteří poslanci vládnoucí většiny sice potvrdili zakoupení softwaru od NSO Group, vláda však oficiálně nepřiznala, že by ho použila proti konkrétním osobám. Nikdo ze tří uvedených nebyl obviněn ze spáchání trestného činu ani předvolán k výslechu a v případě osob vykonávajících veřejné funkce nebyla v souvislosti s tímto případem podána žádost o zbavení imunity.

60. Organizace Citizen Lab odhalila řadu napadení zařízení v Polsku koncem roku 2017; nebyla však tehdy schopna určit dotčené osoby[86].

61. Na používání špionážního softwaru a úsilí o kontrolu občanů je třeba pohlížet v úzkém spojení s volebním systémem. Několik obětí softwaru Pegasus bylo nějakým způsobem spojeno s volbami: senátor Krzysztof Brejza (lídr volební kampaně největší opoziční strany), Roman Giertych (advokát opozičního lídra a bývalého předsedy Evropské rady Donalda Tuska), Ewa Wrzoseková (prokurátorka vyšetřující korespondenční hlasování v prezidentských volbách), Nejvyšší kontrolní úřad (NIK) (který zveřejnil zprávy o korespondenčním hlasování v prezidentských volbách) a Michael Kolodziejczak (zakladatel agrární politické strany, která se uchází o stejné voliče jako vládnoucí strany).

62. Zároveň byla zpochybněna nezávislost Národní volební komise, a to tím, že je složena ze soudců, které vybírá parlament a soudů, které vládnoucí strana dostala pod svoji kontrolu. Kromě toho byl okresní soud ve Varšavě, jenž je odpovědný za registraci nových politických stran[87], obsazen vládě věrnými „novosoudci“ jejichž nezávislost by mohla být zpochybněna.

KRZYSZTOF BREJZA

63. Senátor Krzysztof Brejza působil jako vedoucí volební kampaně opoziční strany Občanská platforma během vnitrostátních voleb a voleb do Evropského parlamentu, když se stal obětí napadení špionážním softwarem[88]. Jeho telefon byl v době kampaně Občanské platformy ve volbách do parlamentu v roce 2019 napaden 33krát. Útok začal 26. dubna 2019 a pokračoval až do 23. října 2019, skončil tedy několik dní po završení volebního cyklu[89].

64. V přímém důsledku hackerského útoku na telefon senátora Brejzy byly během voleb v

---

[85] The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, *17. února 2022.*
[86] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosince 2021.
[87] Zákon ze dne 27. června 1997 o politických stranách, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970980604/U/D19970604Lj.pdf, článek 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. dubna 2022.
[89] The Guardian, „*More Polish opposition figures found to have been targeted by Pegasus spyware*“ (Další představitelé polské opozice se stali terčem špionážního softwaru Pegasus), 17. února 2022.

roce 2019 prý odcizeny, pozměněny a následně vysílány ve státem kontrolované televizní síti (TVP)[90] v rámci údajné organizované očerňující kampaně jeho textové zprávy[91]. To vedlo senátora Brejzu ke zpochybnění legitimity voleb v roce 2019, které těsně vyhrála vládnoucí strana PiS[92].

65. Ačkoli vláda PiS připouští, že Pegasus získala, důrazně popírá, že by byl použit k politickým účelům[93]. Kaczynski nepotvrdil ani nepopřel sledování Brejzy, ale tvrdil, že tento senátor byl spojen s „podezřením z trestných činů“, což Brejza důrazně popírá[94]. Proti Brejzovi nebylo nikdy vzneseno žádné obvinění a nikdy nebyl předvolán ke svědectví. To naznačuje, že použití špionážního softwaru nesloužilo žádnému vyšetřovacímu účelu. Tím, že měl být Brejza spojen s trestnou činností, pokusila se vláda formálně legitimizovat použití špionážního softwaru vytvořením situace, kdy by polská vláda mohla špionážní software Pegasus použít na základě jednoho z důvodů, které NSO Group považuje za „legitimní“, když zvažuje, zda prodat svůj software nějaké vládě, a sice vyšetřování závažné trestné činnosti[95].

66. Proti senátorovi Krysztofu Brejzovi byla po několik týdnů vedena diskreditační kampaň, při níž byly používány materiály získané pomocí spywaru Pegasus. Je pozoruhodné, že tyto materiály byly zveřejněny ve veřejnoprávní televizi. Nelze vysvětlit, jak mohou veřejné sdělovací prostředky získat k takovým materiálům přístup. Pokud byl telefon senátora Brejzy skutečně sledován z důvodu národní bezpečnosti, jak naznačuje vláda, bylo by zveřejnění těchto materiálů – tedy informací získaných v rámci tajné bezpečnostní operace – velmi závažným trestným činem. Veřejnoprávní televize je rovněž v rukou vládnoucí strany, a to poukazuje na to, že by se skutečně mohlo jednat o diskreditační kampaň pod taktovkou vládních stran.

67. V té době však bylo zahájeno trestní vyšetřování otce senátora Brejzy, Ryszarda Brejzy. V době, kdy byl starostou polského města Inowrocław, byl Brejza starší pozván k výslechu ohledně údajné zpronevěry veřejných finančních prostředků a neplnění povinností[96]. K tomuto výslechu došlo bezprostředně poté, co Brejza mladší zahájil soudní řízení proti Kaczyńskému za pomluvu. Krzysztof Brejza i Ryszard Brejza tvrdí, že obvinění vznesená proti společnosti Brejzovi staršímu byla odvetou za soudní řízení (proti Kaczynskému).

68. Sám Ryszard Brejza obdržel v období od července do srpna 2019 10 textových zpráv, které bezpečnostní laboratoř Amnesty International považovala za podezřelé a

---

[90] Zpráva Komise 2022 o právním státu, kapitola o situaci v oblasti právního státu v Polsku, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, s. 20–23; AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosince 2021.
[91] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23. prosince 2021.
[92] Financieele Dagblad, https://fd.nl/politiek/1426857/liberalen-europarlement-eisen-onderzoek-naar-spionagesoftware, 12. ledna 2022.
[93] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7. ledna 2022.
[94] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7. ledna 2022.
[95] BBC, https://www.bbc.com/news/technology-57881364, 19. července 2021.
[96] AP, https://apnews.com/article/technology-business-software-hacking-spyware-8cc528ba7d46a61b378adf1ede9dd00f, 10. ledna 2022.

odpovídající charakteristickým znakům softwaru Pegasus[97]. Navíc v době, kdy vedla kampaň senátora Brejzy do Evropského parlamentu, obdržela jeho bývalá asistentka Magdalena Losková v dubnu 2019 čtyři podezřelé textové zprávy, které podle forenzních průzkumových výzkumníků Amnesty International technicky odpovídaly špionážnímu softwaru Pegasus společnosti NSO Group[98].

ROMAN GIERTYCH

69. Roman Giertych se stal obětí spywaru Pegasus v posledních týdnech před parlamentními volbami v roce 2019. Od září do prosince 2019 byl jeho telefon napaden dokonce osmnáctkrát, přičemž většina útoků se odehrála těsně před 13. říjnem 2019, kdy se konaly volby. V té době působil jako právník opozičního vůdce a bývalého předsedy vlády Donalda Tuska ze strany Občanská platforma. Současně zastupoval i Radka Sikorského, bývalého ministra zahraničí, nyní europoslance a člena EPP, Sikorski podal podnět k prošetření zapojení Kaczynského a jeho spojenců do případu nezákonného odposlechu a zveřejnění nahrávek jeho telefonních hovorů[99].

70. Stejně jako v případě senátora Brejzy vláda nepotvrdila, ani nepopřela, zda je za tyto útoky odpovědná. Agentura Associated Press uvedla, že státní zástupce podal v souvislosti s údajným vyšetřováním finanční trestné činnosti návrh na zatčení Giertycha pouze několik hodin předtím, než mluvčí státní bezpečnosti Stanislaw Zaryn odpověděl na otázky AP týkající se hackerského útoku na Giertychův telefon. Giertych tato obvinění důrazně odmítá. Mluvčí Zaryn se odmítl vyjádřit k možné souvislosti mezi těmito incidenty. Při podobném incidentu provedli činitelé úřadu CBA v roce 2020 razii v Giertychově domě a prohledali jej[100].

71. V této době v roce 2019 zastupoval Giertych také rakouského developera Geralda Birgfellnera. Birgfellner se podílel na stavebním projektu pro lídra PiS Jaroslawa Kaczynského, s nímž ho pojí rodinné vazby, když tento obchod nevyšel. Po zveřejnění nahraných rozhovorů mezi nimi vypukl pro Kaczynského politický skandál a ten poté projekt zrušil. Birgfellner tvrdí, že nikdy nedostal za své služby zaplaceno, a proto najal Giertycha[101]. Ministr spravedlnosti a nejvyšší státní zástupce Zbigniew Ziobro rovněž v roce 2021 uvedl, že se snaží obžalovat Giertycha „s podezřením ze spáchání trestných činů“[102].

EWA WRZOSEKOVÁ

---

[97] The Guardian, „*More Polish opposition figures found to have been targeted by Pegasus spyware*“ (Další představitelé polské opozice se stali terčem špionážního softwaru Pegasus), 17. února 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. července 2022.
[98] The Guardian, „*More Polish opposition figures found to have been targeted by Pegasus spyware*“ (Další představitelé polské opozice se stali terčem špionážního softwaru Pegasus), 17. února 2022;
[99] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosince 2021.
[100] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosince 2021.
[101] AP, https://apnews.com/article/elections-international-news-jaroslaw-kaczynski-european-parliament-poland-bed5ffc814e649f4bb4d10f82628b4c2, 16. února 2019; TVP World, https://tvpworld.com/41262080/ruling-party-leader-im-no-dictator, 11. února 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. prosince 2021.

72. Státní zástupkyně Ewa Wrzoseková byla obětí hackerského útoku spywarem Pegasus šestkrát, a to mezi 24. červnem a 19. srpnem 2020[103]. Ewa Wrzoseková je členkou Lex Super Omnia, sdružení státních zástupců usilujícího o zaručení nezávislosti státního zastupitelství. Zabývala se vyšetřováním rozhodnutí o pořádání prezidentských voleb v Polsku v roce 2020 uprostřed celosvětové pandemie. Mezi pravomoci nejvyššího státního zástupce Zbigniewa Ziobra a jeho pravé ruky, státního zástupce Bogdana Święczkowského, patří i rozhodnutí nestíhat určité případy nebo konkrétní případy odebrat danému státnímu zástupci[104]. Poté byla státní zástupkyně Wrzoseková s pouhým 48hodinovým předstihem přeložena na jiné státní zastupitelství ve městě, které je několik hodin vzdáleno od jejího domova. Ewa Wrzoseková se po svém návratu do Varšavy stala terčem špionážního softwaru Pegasus. Polské orgány jako obvykle nepotvrdily ani nevyvrátily, že by to byly ony, kdo za útoky stál[105] [106].

73. Paní Wrzoseková rovněž podala žalobu týkající se napadení jejího mobilního telefonu softwarem Pegasus. Soud nařídil, aby pracoviště Citizen Lab vypracovalo znalecký posudek o napadení softwarem Pegasus, a sama paní Wrzoseková požádala, aby byl její telefon znalci Citizen Lab zkontrolován. Státní zástupce však tuto žádost zamítl a vybral jiného znalce, který nebyl schopen spojit žádné napadení se softwarem Pegasus. Státní zástupce kromě toho požádal telekomunikačního operátora, aby předal všechna metadata týkající se paní Wrzosekové za dobu, která je pro soudní vyšetřování irelevantní. Paní Wrzoseková má za to, že je stále pod dohledem a že cílem postupu státního zástupce je poskytnout další důkazy, které by mohly být použity v jiných případech proti ní[107].

74. Jak zdůraznila paní Wrzoseková na schůzi výboru PEGA dne 19. ledna 2023, je v současné době státním zastupitelstvím obviněna z odhalení informací o případu nesouvisejícím se softwarem Pegasus a z účasti na politické činnosti. Paní Wrzoseková nemůže připravovat svou obhajobu, neboť jí státní zastupitelství odepírá přístup k dokumentům[108]. Jedná se o jasné porušení práva na spravedlivý proces a vzbuzuje to dojem, že jediným účelem daného případu je paní Wrzosekovou diskreditovat.

DALŠÍ MOŽNÉ OBĚTI

NEJVYŠŠÍ KONTROLNÍ ÚŘAD

75. Ačkoli Nejvyšší kontrolní úřad (NIK) není cílem softwaru Pegasus, byl polskými úřady napaden a obtěžován, neboť jeho úkolem je ochrana veřejných výdajů a řízení veřejných služeb a zveřejnil faktury za „nákup speciálních technologických prostředků pro odhalování a prevenci trestné činnosti“ v celkové hodnotě 25 milionů PLN. Načasování útoků je obzvláště důležité vzhledem k povaze vyšetřování, které NIK vedl. Mluvčí NIK potvrdil, že vyšetřuje zrušení prezidentských voleb v roce 2020.

---

[103] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21. prosince 2021.
[104] Evropská komise 2022 Zpráva o právním státu, kapitola o situaci v oblasti právního státu v Polsku,https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, s. 16.
[105] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw--8b52e16d1af60f9c324cf9f5099b687e, 21. prosince 2021.
[106] The Guardian, https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony, 24. ledna 2022.
[107] Schůze výboru PEGA, 19. ledna 2023.
[108] Schůze výboru PEGA, 19. ledna 2023.

Výsledkem tohoto průzkumu bylo, že předseda vlády, členové jeho vlády a ministerstvo spravedlnosti obdrželi oznámení o trestných činech. To zřejmě posiluje podezření, že Pegas byl v Polsku využíván převážně k politickým účelům[109].

LIDÉ Z OKRUHU PIS

76. Zdá se, že software Pegasus byl použit k „preventivnímu odposlechu“ vůdců a organizátorů pouličních protestů proti reformám ústavního soudu, které zavedla strana PiS. Oběťmi špionážního softwaru však nejsou vždy jen odpůrci vládnoucí strany. Podle zdrojů listu Wyborcza byl v roce 2018 sledován bývalý mluvčí strany PiS Adam Hofman, který se tak stal jednou z prvních osob, na které se po zakoupení špionážního softwaru zaměřili. Po svém vyloučení z PiS založil Hofman PR agenturu R4S[110] [111]. Strana na to prý reagovala s velkou nelibostí a rozhodla se Hofmana sledovat. Hofman říká, že získané informace byly později použity v diskreditační kampani proti jeho osobě.

77. Kromě toho se vláda podle pořadu Wiadomości prostřednictvím softwaru údajně zaměřovala na bývalého poslance PiS Mariusze Antoniho Kaminského a bývalého ministra financí PiS Dawida Jackiewicze[112]. Mariusz A. Kaminski byl ze strany PiS vyloučen poté, co se zapletl do skandálu ve stejnou dobu jako Hofman, Jackiewicz však zůstává členem vládnoucí strany přesto, že náhle odstoupil ze své pozice ministra[113].

78. Podobnou očerňující kampaň vedla v únoru 2018 vládnoucí strana i proti bývalému předsedovi Zaměstnavatelů Polské republiky Andrzeji Malinowskému. Svědčil před zvláštním zasedáním senátního výboru v dubnu 2022 ohledně hackerského útoku na jeho telefon prostřednictvím softwaru Pegasus, který měl za cíl shromáždit informace k tomu, aby mohl být veřejně odstraněn[114]. Uvedl, že zprávy byly převzaty z jeho aplikace WhatsApp a SMS s využitím softwaru Pegasus a byly strategicky využívány k šíření nenávisti na internetu proti němu. Tento útok byl odvetou za nesouhlas s vládnoucí stranou a za požadování alternativních hospodářských politik.

ZÁVĚREČNÉ POZNÁMKY

79. Na používání softwaru Pegasus v Polsku je třeba nahlížet v plném kontextu krize právního státu v Polsku, která začala v roce 2015, kdy vláda vedená stranou PiS začala demontovat soudní systém a od té doby systematicky převzala nejdůležitější instituce v zemi a instalovala své příznivce do všech strategických úřadů; Vládnoucí strana cílevědomě a metodicky sestavila právní, institucionální a politické stavební kameny tohoto systému tak, aby vytvořila ucelený a vysoce účinný rámec, v němž je využití softwaru Pegasus nedílnou a zásadní součástí systému sledování opozice a kritiků vlády

[109] Sdělení Polska, https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/, 7. února 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. října 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.

za účelem politického zisku. Jejím cílem je udržet vládnoucí většinu a vládu u moci.

80. Rozsah sledování v Polsku se v posledních letech značně rozšířil, čímž se oslabila nebo zrušila ochranná opatření a ustanovení o dohledu. V průběhu těchto systematických a cílených legislativních změn zavedených vládnoucí většinou byla práva obětí minimalizována a opravné a nápravné prostředky byly v praxi zbaveny účinnosti. Předchozí i následná kontrola byla téměř eliminována, stejně jako nezávislý dohled. Hlavní pozice v systému přímo či nepřímo ovládají členové polské vlády a věrní straníci. Informace získané pomocí špionážního softwaru jsou pak využívány k diskreditačním kampaním, které proti kritikům vlády a představitelům opozice vedou státem ovládané sdělovací prostředky. Skutečnost, že polská vláda rozšiřuje stanovy tímto systematickým a cíleným způsobem v rámci vnitrostátního práva zachovává právní základ pro sledování občanů, což důrazně porušuje právní předpisy EU, rozhodnutí polského ústavního soudu z roku 2014 a základní práva polských občanů. Tímto způsobem bylo v podstatě legalizováno nezákonné sledování, které jasně porušuje právo EU a vnitrostátní právo.

I.B. Maďarsko

81. Maďarsko bylo jednou z prvních zemí, které byly do evropské kauzy špionážního softwaru zapleteny. V roce 2021 bylo projektem Pegasus odhaleno a organizací Amnesty International potvrzeno[115], že obětí zneužití softwaru Pegasus se mohlo stát více než 300 maďarských občanů, včetně politických aktivistů, investigativních novinářů, právníků, podnikatelů, opozičního politika a bývalého ministra.

82. V únoru 2023 navštívila delegace výboru PEGA Maďarsko. Dospěla k závěru, že vše nasvědčuje tomu, že v Maďarsku dochází k hrubému zneužívání špionážního softwaru, a vysvětlení úřadů, které se odvolávají na národní bezpečnost, považuje za velmi nepřesvědčivé. Existují pádné důkazy o tom, že lidé byli sledováni s cílem získat ještě větší politickou a finanční kontrolu nad veřejným prostorem a mediálním trhem.

83. Výbor byl přesvědčen, že právní stát a základní demokratické standardy byly v Maďarsku vážně porušeny a že situace v Maďarsku patří k nejhorším v EU. Zdá se, že v důsledku dlouholetého ústupu od demokracie se státní instituce nesnaží sloužit občanům a chránit jejich práva a svobody, ale spíše sledují politické cíle vlády. Výbor vyzval úřady, aby umožnily smysluplné vyšetřování zneužívání.

NÁKUP SYSTÉMU PEGASUS

84. V roce 2017 hlasoval Výbor pro národní bezpečnost maďarského parlamentu o povolení zpravodajským službám země pořizovat určité vybavení v rámci běžného postupu zadávání veřejných zakázek. Maďarský parlament podpořil na žádost Zvláštní služby pro národní bezpečnost (Nemzetbiztonsági Szakszolgálat, NBSZ) pořízení sofistikovaného špionážního softwaru[116]. Postup byl však tajný a v žádostech o

[115] Euractiv, „*Hungary employed Pegasus spyware in hundreds of cases, says government agency*“ (Maďarsko použilo špionážní software Pegasus ve stovkách případů, říká vládní agentura), 1. února 2022.
[116] Studie – „*The use of Pegasus and equivalent spyware – The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware*“ (Používání programu Pegasus a obdobného špionážního softwaru – stávající právní rámec v členských státech EU pro pořizování a používání

schválení nebyla uvedena konkrétní značka a typ technologie[117].

85. Maďarské ministerstvo vnitra koupilo Pegasus za 6 milionů EUR nepřímo prostřednictvím společnosti Communication Technologies Ltd od společnosti NSO Group v Lucembursku v roce 2017 krátce poté, co se premiér Viktor Orbán setkal s polským premiérem Mateuszem Morawieckim a bývalým izraelským premiérem Benjaminem Netanjahuem[118] [119]. Maďarské ministerstvo vnitra tuto informaci nepotvrdilo až do listopadu 2021, kdy předseda bezpečnostního výboru maďarského parlamentu Lajos Kósa přiznal, že vláda Fidesz software Pegasus skutečně zakoupila[120]. Kósa však nicméně trval na tom, že špionážní software nebyl nikdy použit proti maďarským občanům[121].

86. Maďarský Národní úřad pro ochranu údajů a svobodu informací (NAIH) se zajímal o zadávací řízení na nákup špionážního softwaru a získal přístup k tajné smlouvě se společností NSO. Během mise výboru PEGA v Budapešti v únoru 2023 předseda NAIH Attila Péterfalvi nejprve prohlásil, že není pravda, že poskytování softwaru Pegasus maďarským orgánům bylo ukončeno, což by znamenalo, že Maďarsko není jedním ze dvou členských států EU, které byly vyřazeny ze seznamu 14 států, jimž NSO poskytuje program Pegasus. Péterfalvi později své prohlášení odvolal a prohlásil, že nemá žádné informace o tom, zda společnost NSO ukončila používání systému Pegasus v Maďarsku, či nikoli.

PRÁVNÍ RÁMEC

87. V Maďarsku je rámec pro legální odposlech komunikace v rámci vyšetřování trestné činnosti stanoven v policejním zákoně. Podle zákona o policii lze sledování soukromých osob v rámci vyšetřování trestné činnosti provádět pouze se souhlasem soudu. Ve věcech souvisejících s terorismem však zákon o policii odkazuje na vyšetřovací sledování uvedené v zákoně o národní bezpečnosti[122]. Podle tohoto ustanovení není třeba pro schválení použití těchto technik žádat o soudní povolení, ale místo toho je za poskytnutí povolení odpovědný ministr spravedlnosti[123]. V žádostech o

---

špionážního softwaru Pegasus a ekvivalentního sledovacího špionážního softwaru), Evropský parlament, Generální ředitelství pro vnitřní politiku, Politické oddělení C – Práva občanů a ústavní záležitosti, 5. prosince 2022, k dispozici na adrese: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf. Direkt36, Příběh o tom, jak se Pegas dostal do Maďarska, https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/.

[117] Mise výboru PEGA do Maďarska, setkání se členy Výboru pro národní bezpečnost maďarského parlamentu, 20.–21. února 2023.

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

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

[120] DW, „*Hungary admits to using NSO Group's Pegasus spyware*“ (Maďarsko připouští používání špionážního softwaru Pegasus společnosti NSO Group), 4. listopadu 2021.

[121] DW, „*Hungary admits to using NSO Group's Pegasus spyware*“ (Maďarsko připouští používání špionážního softwaru Pegasus společnosti NSO Group), 4. listopadu 2021.

[122] Agentura Evropské unie pro základní práva (FRA), „*National intelligence authorities and surveillance in the EU*: *Fundamental rights safeguards and remedies: Hungary*“ (Vnitrostátní zpravodajské orgány a dohled v EU: záruky základních práv a opravné prostředky: Maďarsko), 26. září 2014.

[123] FRA, „*National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary*“ (Vnitrostátní zpravodajské orgány a dohled v EU: záruky základních práv a opravné prostředky: Maďarsko), právní aktualizace, 23. října 2017.

povolení sledování není uveden typ technologie, která bude použita[124].

88. Podle zákona CXXV z roku 1995 je zájem národní bezpečnosti definován jako „zajištění svrchovanosti a ochrana právního řádu Maďarska a v tomto rámci“, což je poměrně široká definice.

89. V přelomovém případu (*Szabó a Vissy* v. *Maďarsko*[125]) Evropský soud pro lidská práva (ESLP) shledal, že zákon o národní bezpečnosti neposkytuje dostatečně přesné, účinné a komplexní záruky týkající se nařizování, provádění a případné nápravy sledovacích opatření. Zákon o národní bezpečnosti opomíjí povinnost informovat sledovaný subjekt a výslovně stanoví, že cíle povolující strana nesmí cíle informovat, že jsou sledovány[126]. Požadavek informovat oběti jednoznačně stanovil ESLP ve věci *Klass a další* v. *Německo*[127]. Kromě toho neexistují žádné účinné prostředky nápravy a odškodnění v případě zneužití a žádný řádný dohled. Maďarská vláda dosud neprovedla ani jedno z těchto rozhodnutí.

PŘEDBĚŽNÁ KONTROLA

90. Podle zákona o národní bezpečnosti je ke sledování prováděnému zvláštními službami pro národní bezpečnost (SNS) pomocí špionážního softwaru ve většině případů potřebné povolení ministra spravedlnosti a v některých konkrétních případech povolení soudce jmenovaného předsedou budapešťského městského soudu[128] [129]. Proti těmto rozhodnutím není možné se odvolat a nad celým procesem prakticky neexistuje žádný dohled[130] [131].

91. Navzdory závažnosti takového rozhodnutí přenáší současná ministryně spravedlnosti Judit Vargová odpovědnost za povolení používat špionážní software proti občanům na státního tajemníka ministerstva spravedlnosti, což je funkce, kterou v současné době zastává Robert Repassy[132]. Tuto skutečnost potvrdil sám Repassy v odpovědi na písemné otázky týkající se této problematiky[133]. Obecně se uvádí, že Vargová pravidelně přenášela odpovědnost na předchůdce Repassyho Pála Völnera, který byl v

[124] Mise výboru PEGA do Maďarska, 20.–21. února 2023.
[125] Szabó a Vissy v. Maďarsko, stížnost č. 37138/14, rozsudek ze dne 12. ledna 2016, https://hudoc.echr.coe.int/fre#{"itemid":["001-160020"]}.
[126] Zákon CXXV z roku 1995 o národních bezpečnostních službách, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf.
[127] Klass a další v. Německo, 6. září 1978, bod 50, série A č. 28.
[128] Zákon CXXV z roku 1995 o národních bezpečnostních službách, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf viz oddíly 56 až 58.
[129] *Europe's PegasusGate: Countering Spyware Abuse - EPRS Report* (Evropská PegasusGate: Boj proti zneužívání softwaru – zpráva EPRS), https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf , červenec 2022 na s. 20.
[130] Zákon CXXV z roku 1995 o národních bezpečnostních službách, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf viz oddíly 57 až 58.
[131] Zpráva Evropské komise o právním státu 2022, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf na s. 26.
[132] https://telex.hu/belfold/2021/12/10/repassy-robert-igazsagugyi-allamtitkar-varga-judit-igazsagugyi-miniszterium; *Europe's PegasusGate: Countering Spyware Abuse* (Evropská PegasusGate: Boj proti zneužívání softwaru), https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, červenec 2022,na s. 20.
[133] https://telex.hu/belfold/2022/01/27/varga-judithoz-kerulhetett-vissza-a-titkos-megfigyelesek-engedelyezese.

prosinci 2021 v důsledku rozsáhlého korupčního skandálu nucen odstoupit[134]. Obecně se uvádělo, že přijal miliony maďarských forintů v úplatcích od řady vysoce postavených zúčastněných stran výměnou za příznivá rozhodnutí a jmenování do klíčových funkcí státním tajemníkem Völnerem[135].

92. Zatímco ministr vnitra Sándor Pintér trvá na tom, že toto povolovací řízení prostřednictvím ministra nebo soudů je bez výjimky dodržováno[136], slabá právní ustanovení zákona o národní bezpečnosti rovněž umožňují generálním ředitelům SNS udělit prozatímní povolení k provádění sledování bez souhlasu, dokud nebude možné udělit úřední povolení. To v zásadě umožňuje SNSS fungovat bez řádného soudního povolení, pokud tvrdí, že prodlevy při získávání povolení by poškodily jejich operaci. V takových případech může neoprávněné sledování pokračovat[137].

93. Zákonný 90denní limit dnů pro sledování stanovený zákonem lze prodloužit o dalších 90 dnů na základě prosté žádosti podané generálním ředitelem schvalujícímu úředníkovi[138], což je stanoveno pouze pro zdání právní záruky.

94. Kromě toho má úřad NAIH dohlížet na veškeré sledování prováděné tajnými službami. Předseda úřadu NAIH Attila Péterfalvi soustavně tvrdí, že veškeré použití softwaru Pegasus bylo prováděno pro účely národní bezpečnosti, což spadá do výlučné pravomoci vnitrostátních vlád[139]. Úřad NAIH však ověřil postup povolování pouze z technických důvodů, aby zjistil, zda je zpracování údajů zákonné, ale nezkoumal podstatu používání softwaru Pegasus. Úřad NAIH nepovažoval za nutné předvolat cílové osoby k podání svědectví, protože měl přístup ke všem relevantním dokumentům. Byly prošetřeny pouze případy povolené ministrem spravedlnosti, protože NAIH nemůže prošetřovat povolení udělená soudcem[140].
Podle předsedy Péterfalviho šetření úřadu NAIH neodhalilo žádnou protiprávní činnost ani nic, co by bylo v rozporu s podmínkami prodeje NSO Group[141].

95. Vedoucí úřadu NAIH je jmenován předsedou vlády, a proto může být zpochybněna jeho nezávislost[142]. ESLP v této věci rozhodl v září 2022 ve věci *Hüttl* v. *Maďarsko*[143], kterou podal právník Maďarské unie občanských svobod (HCLU) Tivadar Hüttl, když poté, co byl údajně odposloucháván, Výbor pro národní bezpečnost rozhodl, že nezahájí

---

[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. listopadu 2021.
[137] Zákon CXXV z roku 1995 o národních bezpečnostních službách, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, viz oddíl 59.
[138] Zákon CXXV z roku 1995 o národních bezpečnostních službách, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, viz oddíl 58.
[139] HVG, https://hvg.hu/itthon/20111117_Peterfalvi_palyaja_adatvedelem, 21. listopadu 2011.
[140] Mise výboru PEGA do Maďarska, 20. února 2023.
[141] Euractiv, „Maďarsko použilo špionážní software Pegasus ve stovkách případů“, říká vládní agentura, 1. února 2022.
[142] https://hclu.hu/en/pegasus-whats-new.
[143] https://hudoc.echr.coe.int/fre#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-219501%22]}.

další vyšetřování, a nebyly k dispozici žádné další opravné prostředky[144]. ESLP ve svém rozsudku jasně uvedl, že úřad NAIH, ačkoli je oprávněn vyšetřovat jednání tajných služeb, nebyl schopen provádět nezávislý dohled nad používáním sledování. Soudní dvůr rozhodl, že NAIH k tomu nemá nezbytnou pravomoc, jelikož tajné služby jsou oprávněny odepřít přístup k určitým dokumentům na základě utajení[145]. V takovém případě by bylo na ministrovi odpovědném za tajné služby, aby provedl audit, který však nelze v žádném případě považovat za nezávislý dohled[146].

NÁSLEDNÁ KONTROLA

96. V listopadu 2021 byla na naléhání opozice, Výboru pro národní bezpečnost a Výboru pro obranu a bezpečnost uspořádána slyšení, v Národním shromáždění, která se věnovala používání špionážního softwaru v Maďarsku a zejména údajnému politicky motivovanému sledování občanů maďarskou vládou. Vládní strana obsadila 4 ze 6 křesel ve Výboru pro národní bezpečnost a znemožnila jakoukoli smysluplnou a demokratickou kontrolu použití softwaru Pegasus**.** Zástupci vládní strany trvali na tom, že veškeré sledování bylo schváleno příslušnými kanály, ale odmítli se vyjádřit k tomu, zda byli cílem sledování novináři nebo politici. Odmítli se rovněž vyjádřit ke skutečnosti, že povolení byla ministryní spravedlnosti delegována na státního tajemníka Pála Völnera, který je vyšetřován kvůli obviněním z korupce a zneužití pravomoci. Odmítli také žádosti opozičních poslanců o provedení hloubkového vyšetřování a návštěvu bezpečnostních služeb za účelem výslechu jednotlivých agentů. Klíčové cíle, jako jsou Zoltán Varga a Szabolcs Panyi, výbor nevyslechl. V srpnu 2021 bylo provedeno pouze pro forma obecné šetření, protože to byl jediný vzorec, který získal podporu většiny[147]. Co na slyšeních přesně zaznělo, nelze zjistit, protože vládní strana označila zápis z jednání za tajný až do roku 2050[148].

97. Vyšetřování úřadu NAIH bylo zahájeno na základě obvinění vzneseného nejméně deseti právníky, předsedou maďarské advokátní komory a nejméně pěti dotčenými novináři[149]. Výsledná zpráva byla zveřejněna dne 31. ledna 2022 a dospěla k závěru, že spyware Pegasus byl používán výhradně z důvodů národní bezpečnosti.

98. Stejně tak maďarské státní zastupitelství ukončilo vyšetřování dne 15. června 2022 a dospělo k závěru, že nedošlo k žádnému nepovolenému sledování.

99. Vzhledem k tomu, že schvalovací pravomoc náleží ministerstvu spravedlnosti a že nejvyšší státní zástupce Péter Polt za podpory strany Fidesz, byl v roce 2019 znovu zvolen na dalších devět let (již v té době vykonával funkci po dobu 15 let ve dvou

---

[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] Mise výboru PEGA do Maďarska, setkání se členy Výboru pro národní bezpečnost maďarského parlamentu, 20. února 2023.
[148] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4. listopadu 2021.
[149] Zpráva Komise 2022 o právním státu, https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, s. 26.

různých funkčních obdobích), lze zpochybnit skutečný vládní dohled.

100. V maďarském protikorupčním rámci pro to neexistuje žádná opora, neboť ministerstvo vnitra, které původně zakoupilo Pegasus od NSO Group, odpovídá za koordinaci veškeré protikorupční politiky a dohledu[150].

ZJEDNÁNÍ NÁPRAVY

101. Když v Maďarsku vypukl skandál okolo softwaru Pegasus, byli novináři jednou ze skupin, na které se vláda nejvíce zaměřovala. Na začátku roku 2022 proto skupina šesti novinářů a aktivistů podala žalobu k maďarským orgánům, Komisi a ESLP. Pět ze zúčastněných zastupuje maďarská Unie pro občanské svobody (jsou to maďarští novináři Brigitta Csikászová, Dávid Dercsényi, Dániel Németh a Szabolcs Panyi a belgicko-kanadský doktorand a aktivista Adrien Beauduin), šestý člen skupiny se rozhodl zůstat v anonymitě. Unie pro občanské svobody rovněž spolupracuje s izraelským právníkem Eitayem Mackem a snaží se dosáhnout toho, aby izraelské státní zastupitelství zahájilo vyšetřování NSO Group[151].

102. Mnoho technických aspektů tuto věc blokuje u maďarských soudů. Vzhledem k tomu, že v této oblasti neexistuje velké množství judikatury, jsou postupy nejasné. Vyskytly se například otázky týkající se soudní příslušnosti. Tyto kroky a neustálé průtahy jsou vnímány především jako pokusy o zamítnutí případu z technických nebo procesních důvodů.

103. Závažným problémem je také přístup k informacím. Aby bylo možné požádat o přístup ke spisům obsahujícím všechny shromážděné údaje o jednotlivých občanech, je nutné uvést přesný název spisu, k němuž se žádost vztahuje, což je informace, kterou je téměř nemožné získat. Vzhledem k tomu, že žádosti šesti stran zastoupených HCLU byly Nejvyšším soudem nevyhnutelně zamítnuty, domáhala se HCLU u Ústavního soudu rozhodnutí, kterým by byla tato praxe a rozhodnutí maďarského Nejvyššího soudu prohlášeny za protiústavní. Ústavní soud však v roce 2021 podnět HCLU zamítl.

104. Kromě soudních žalob HCLU usilovala i o další způsoby přístupu k údajům svých šesti klientů. Bylo zahájeno a přijato správní řízení podle zákona o utajovaných údajích a zákona o ochraně údajů. Před tím, než budou známy výsledky, však bude Úřad pro ochranu ústavy každý jednotlivý případ zkoumat po dobu jednoho roku[152]. Dále byly špionážní útoky nahlášeny komisaři pro základní práva (veřejnému ochránci práv). Ústavní soud stanovil, že odpovědnost za vyšetřování zneužití ze strany tajných služeb nese veřejný ochránce práv[153].

105. Při dalším pokusu o dosažení určité transparentnosti požádala HCLU v rámci mimosoudního procesu o přístup ke zpracovávaným údajům, které byly získány hackerskými útoky na šest osob. Nárok na tyto informace však existuje pouze tehdy, pokud poskytnutí údajů subjektům údajů neohrožuje národní bezpečnost[154]. To vytváří

[150] Zpráva Komise 2022 o právním státu, https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, s. 10.
[151] The Guardian, https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state, *28. ledna 2022.*
[152] https://hclu.hu/en/pegasus-case-hungarian-procedures.
[153] https://hclu.hu/en/pegasus-whats-new.
[154] https://hclu.hu/en/pegasus-case-hungarian-procedures.

další záminku pro maďarské orgány, aby opět využily důvody národní bezpečnosti[155]. Úřad pro ochranu ústavy dosud zamítl 270 žádostí v souvislosti se svobodou informací předložených HCLU v období od roku 2018 do května 2022[156].

POLITICKÁ KONTROLA

106. Politická kontrola nad sledovacími operacemi je v Maďarsku naprostá. Režim Orbánovy strany Fidesz vytvořil systém, v němž může sledovat právníky, novináře, politické odpůrce a organizace občanské společnosti sledovat.

107. Za nákup špionážního softwaru Pegasus byl v první řadě odpovědný ministr vnitra a ministryně spravedlnosti odpovídá za udělování povolení k jeho používání. Maďarský legislativní rámec týkající se sledování občanů byl opakovaně shledán nedostatečným. Vládnoucí strana však neučiní žádné kroky k jeho změně, protože jí to vyhovuje.

108. Předseda vlády vybírá vedoucího NAIH, což je subjekt odpovědný za nezávislý dohled nad používáním spywaru Pegasus tajnými službami. Vzhledem k tomu, že se jedná o politicky jmenovanou funkci, chybí nezávislý dohled. Maďarsko a vláda Fidesz nejsou pro taková politická jmenování nováčky. Vláda systematicky jmenovala své stoupence do vedoucích funkcí v orgánech, jako je Ústavní soud, Nejvyšší soud, Účetní dvůr, státní zastupitelství, Maďarská národní banka a Národní volební komise[157]. Tím je zajištěno, že žádná instituce ustavená s úmyslem vykonávat dohled nad výkonnou složkou moci nemůže fungovat nezávisle[158].

109. Při praktickém provádění dohledu prostřednictvím špionážního softwaru hrají významnou úlohu telekomunikační společnosti. Existuje řada případů, kdy jsou zařízení dotčených osob nakažena pomocí odkazů zaslaných SMS, a množství údajů, k nimž mají telekomunikační společnosti přístup, je pro subjekty, které chtějí provádět sledování, velmi atraktivním zdrojem informací. V případě Maďarska je situace nebezpečnější, jelikož maďarská vláda nedávno koupila společnost Vodafone Hungary[159]. S podporou maďarské vlády odkoupila společnost 4iG prostřednictvím dceřiné společnosti 51 % společnosti Vodafone. Kromě toho maďarská vláda odkoupila 49 % akcií společnosti Vodafone prostřednictvím jiné společnosti. Vazby mezi 4iG a vládou jsou zřejmé. Současný předseda společnosti byl blízkým spolupracovníkem maďarského oligarchy Lőrinca Mészárose, přítele Viktora Orbána z dětství. Celkové pořizovací náklady činí 1,7 miliardy EUR a vládě umožní snadný a přímý přístup k údajům o více než 3 milionech zákazníků[160]. Navíc bude mít stát díky tomuto nákupu

[155] https://hclu.hu/en/pegasus-whats-new.
[156] https://hclu.hu/en/pegasus-whats-new.
[157] Martin, J. a Ligeti, M., „Hungary. Lobbying, State Capture and Crony Capitalism“, Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. and Harris, P. (eds.), Springer, 2017, s. 177-193, s. 178.
[158] Martin, J. a Ligeti, M., „Hungary. Lobbying, State Capture and Crony Capitalism“, Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. and Harris, P. (eds.), Springer, 2017, s. 177-193, s. 178.
[159] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22. srpna 2022.
[160] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22. srpna 2022; Volkskrant, *Orbán verstevigt met overname Vodafone Hongarije grip op telecommunicatie, critici uiten zorgen*.

přístup k celosvětovému systému zasílání zpráv známému jako SS7[161]. Tento systém umožňuje mobilním operátorům připojit uživatele po celém světě. Maďarský stát si bude moci tento přístupový bod dále pronajmout, jako tomu bylo v případě Rayzone[162].

CÍLE SLEDOVÁNÍ

110. Mezi telefonními čísly na seznamu, který získal projekt Pegasus, figurují čísla více než 300 maďarských občanů[163]. Mezi nimi bylo nejméně pět novinářů, deset právníků, starosta Gödöllő, který je členem opoziční strany, zaměstnanec opoziční strany a také aktivisti a známí podnikatelé[164]. Proti žádné osobě však nebylo vedeno trestní vyšetřování ani nebyl nikdo obviněn. To, že jsou tato telefonní čísla uvedena na seznamu, ještě neznamená, že tyto telefony byly skutečně napadeny. Prozrazuje to však, jak metodicky a systematicky Orbánova vláda postupuje při omezování základních práv a svobody sdělovacích prostředků Mezitím bylo potvrzeno, že řada osob na seznamu z roku 2021 byla skutečně sledována špionážním softwarem. Od chvíle, kdy v Maďarsku vypukl skandál se špionážním softwarem, bylo zcela jasné, že kroky vlády jsou politicky motivované.

SZABOLCS PANYI

111. Zařízení novináře a redaktora Szabolcse Panyiho bylo napadeno v souvislosti s jeho prací v investigativním centru Direkt36. Ten patří k posledním z nezávislých médií v Maďarsku, a jako takový se stal pro vládnoucí stranu důležitým cílem. Je jasné, že známý a renomovaný novinář Panyi měl pro vládu velkou cenu nejen sám o sobě – cenné byly i vedlejší úlovky v podobě kontaktů a jiných zdrojů v jeho telefonu.

112. Amnesty International potvrdila, že telefon pana Panyiho byl v roce 2019 soustavně sledován po dobu sedmi měsíců[165]. Na tyto útoky bylo poukázáno a často k nim docházelo v době, kdy Panyi požádal vládu, aby se k záležitostem vyjádřila. Konkrétní a znepokojivý příklad ilustrující tuto situaci nastal 3. dubna 2019. Panyi kontaktoval vládu s žádostí o vyjádření k svému článku, v němž podrobně popsal přesun ruské banky do maďarského kapitálu, který byl významným příběhem, neboť vyvstávaly otázky ohledně toho, zda dotčená banka ve skutečnosti není předvojem ruských zpravodajských služeb[166]. Amnesty International potvrdila, že Panyiho telefon byl následujícího dne napaden hackery, a dále ověřila, že bezprostředně po podání žádosti o vyjádření Orbánovy vlády došlo k dalším jedenácti hackerským útokům[167]. Jejich počet odpovídá více než polovině Panyiho žádostí podaných v tomto sedmiměsíčním

[161] The Guardian, https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands, 16. prosince 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. července 2021.
[164] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021 a Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. července 2021.
[165] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[166] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[167] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.

období[168].

113. Úřady předstíraly nevědomost, pokud jde o sledování Panyiho, a nepotvrdily, ani nepopřely svou odpovědnost. Vláda však již dříve napadla Panyiho veřejně, přičemž Orbánův mluvčí tvrdil, že je fanatickým politickým aktivistou, a obvinil ho z nenávisti vůči Orbánovi a Maďarsku[169]. Jedná se o očividný pokus diskreditovat Panyiho a jeho zdroje i jeho osobu vylíčit jako „nepřátele“ prostřednictvím státem ovládaných sdělovacích prostředků.

114. Po vyšetřování, které Panyi vedl proti maďarské zprostředkovatelské společnosti Communication Technologies Ltd, jejímž prostřednictvím byl software Pegasus zakoupen, ho společnost zažalovala[170].

ZOLTÁN VARGA

115. Zoltán Varga je ředitelem a předsedou správní rady skupiny Central Media a vlastníkem „24.hu“, největšího ze nezávislých zpravodajských serverů, které ještě v zemi zbývají. Poté, co Orbánova vláda v roce 2020 iniciovala převzetí jeho hlavního konkurenta, serveru Index.hu, zůstal Varga posledním, kdo vládní straně ještě vzdoruje[171].

116. Fidesz již nějakou dobu vede očerňující kampaň proti Vargovi prostřednictvím vládou kontrolovaných sdělovacích prostředků s cílem diskreditovat jak jeho veřejnou osobnost, tak publikaci, a to navzdory popularitě, s více než 7,5 milionu osob za měsíc[172]. Varga tvrdí, že mu bylo při různých příležitostech nabízeno a vyhrožováno, aby prodal, včetně nabídek na štědré státní dotace na reklamu výměnou za najímání vládního výběru redakčního personálu[173]. Varga měl nejprve podezření, že jeho telefon byl nakažen softwarem Pegasus, když začal slyšet přehrávání hovoru v polovině konverzace. Následně v roce 2021 společnost Amnesty International zjistila, že Varga byl s největší pravděpodobností napaden softwarem Pegasus, ale nelze to potvrdit z důvodu, že dotčený telefon byl od té doby vyměněn[174].

117. Kromě toho se znovu zvolený Orbán krátce po volbách v roce 2018 pokusil dostat se k Vargovi nepřímo. Po večeři, kterou pořádá Varga na jaře 2018 a na níž se diskutovalo o převzetí vládních sdělovacích prostředků a jíž se zúčastnili bývalý ministr Fideszu Attila Chikán, nyní kritik Orbána, bylo ověřeno, že všichni přítomní byli zaznamenáni jako kandidáti na sledování[175]. Následně bylo potvrzeno, že zařízení jednoho hosta bylo v době večeře napadeno, zatímco jiné telefony vykazovaly stopy potenciálních útoků

[168] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[169] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[170] Mise výboru PEGA do Budapešti, 20.–21. února 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. července 2020.
[173] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[174] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. července 2021.
[175] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.

softwarem Pegasus, ale bez důkazu o úspěšném napadení[176]. Hackerské útoky byly všechny potvrzeny osobou spřízněnou s vládou, která se zná s panem Vargem, a ta v rozhovoru přímo odkázala na večeři a varoval před socializací s lidmi, kteří by mohli být „nebezpeční“[177].

118. Varga byl rovněž předmětem tradičního sledování. Odposlech v podnikatelském prostředí, vozidla stojící u jeho domu a vrtulníky vznášející se nad jeho domem a několik vniknutí do jeho zahrady ho opravňovaly k tomu, aby si najal ochranku na plný úvazek.

119. V říjnu 2022 bylo proti Vargovi zahájeno trestní stíhání. Policie ho předvolala k výslechu a jen o pár minut později už o tom informovala vládě nakloněná média[178].

ADRIEN BEAUDUIN

120. Adrien Beauduin do hledáčku Orbánova režimu dostal v roce 2018, kdy dokončoval doktorské studium na katedře genderových studií Středoevropské univerzity. Tuto instituci založenou Georgem Sorosem se tehdy maďarská vláda pokoušela vypudit ze země a zlikvidovat s ní i genderová studia jako obor[179]. Po účasti na demonstraci v Budapešti byl Adrien Beauduin zatčen a obviněn z útoku na policistu, což on sám důrazně odmítá. Jeho zatčení je považováno za silně politicky motivované[180]. Objevily se zprávy, podle nichž neexistují proti Beauduinovi prakticky žádné důkazy; jediné předložené důkazy byly doslova zkopírovány z výpovědi policisty v úplně jiném případu[181]. V roce 2020 bylo trestní řízení proti Adrienu Beauduinovi, který byl ve věci zastoupen HCLU, zastaveno.

121. Zástupci vlády veřejně odsoudili tzv. proimigrační síť Soros za organizaci „násilných demonstrací v Budapešti“[182]. Následně byly na telefonu Beauduina nalezeny stopy softwaru Pegasus, ale nebylo možné potvrdit, zda došlo k úspěšnému napadení.

122. Vzhledem k tomu, že Beauduin byl v době těchto incidentů belgickým občanem žijícím v Maďarsku, nelze význam přeshraničního rozměru tohoto případu přeceňovat. Má zásadní význam, neboť ovlivňuje svrchovaná práva občanů EU, jako je svoboda pohybu a právo pracovat. Komise má zaveden postup pro podávání stížností, který může kdokoli využít, pokud byla porušena jeho práva vyplývající z Listiny. Adrien Beauduin podal takovou stížnost 24. ledna 2022. nicméně o sedm měsíců později v odpovědi ze 17. srpna 2022 adresované jeho právníkovi Komise uvedla, že nemá pravomoc

[176] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[177] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. července 2021.
[178] Mise výboru PEGA do Budapešti, 20.–21. února 2023.
[179] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[180] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18. července 2021.*
[181] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18. července 2021.*
[182] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, *18. července 2021.*

zasáhnout[183].

ILONA PATÓCSOVÁ

123. Právnička Ilona Patócsová se pravděpodobně stala obětí softwaru Pegasus v létě 2019, kdy zastupovala významného klienta v dlouhotrvajícím procesu týkajícím se vraždy[184]. Vzhledem k typu mobilního zařízení, které používala, nebylo možné potvrdit, zda bylo napadení úspěšné ani kdy přesně k němu došlo. Její klient István Hatvani strávil sedm let ve vězení za atentát, za který byl odsouzen v procesu, který Patócsová označuje za „politicky motivovaný“[185]. Přestože se k atentátu později přihlásil někdo jiný, maďarský odvolací soud poslal Hatvaniho zpět do vězení, aby si odpykal i zbytek trestu. Jako potenciální cíle softwaru Pegasus byly uvedeny také telefony mnoha dalších právníků, mezi nimiž byl i předseda maďarské advokátní komory János Bánáti[186]. Tento výběr potenciálních cílů jasně ukazuje, že vláda naprosto nebere ohled na privilegovaný vztah mezi advokáty a jejich klienty.

GYÖRGY GÉMESI

124. György Gémesi, starosta města Gödöllő, se koncem roku 2018 také stal terčem špionážního softwaru Pegasus, a to v době, kdy byl pod silným tlakem vlády a kdy se neznámé osoby vloupaly do jeho domu i do domu jeho dětí. Ve stejnou dobu jako opoziční starosta, tedy na konci roku 2018, byl za cíl špionáže vybrán i Gémesiho známý z vlády. Kromě toho se na seznamu objevila rovněž dvě telefonní čísla spojená s jeho spolustraníky a bývalým Gémesiho místostarostou.

BRIGITTA CSIKÁSZOVÁ

125. Během svého sledování Brigitta Csikászová, jedna z nejzkušenějších maďarských zločineckých reportérů, vyšetřovala mimo jiné zneužívání finančních prostředků Evropské unie. Vyšetřování Csikászové odhalila, že navzdory tomu, že Evropský úřad pro boj proti podvodům (OLAF) bije na poplach, maďarské orgány postrádají vůli nebo schopnost stíhat podezřelé vynakládání prostředků EU, což opět dokazuje, že i když je trestní stíhání de iure nezávislé a vysoce hierarchické, hlavní státní zástupce je de facto úzce propojen s vládní stranou a předsedou vlády.

126. Předseda maďarské advokátní komory János Bánáti, obhájce trestního práva a několik dalších právníků byli také terčem softwaru Pegasus.

DALŠÍ SLEDOVANÉ OSOBY

127. Špionážní software byl použit také proti lidem z užšího okruhu samotné vládní strany. Nezávislý maďarský server Direkt36 v prosinci 2021 informoval, že vedoucí ochranné

[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. března 2022.
[185] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31. března 2022.
[186] Direkt36, https://www.direkt36.hu/en/pegasus-celpontta-valt-a-vedougyved-amikor-fordulat-allt-be-magyarorszag-egyik-leghirhedtebb-gyilkossagi-ugyeben/, 31. března 2022.

služby a osobní strážce prezidenta a Orbánova blízkého spojence Jánose Ádera byl napaden špionážním softwarem Pegasus. Novinář ze serveru Direkt26 Szabolcs Panyi, který byl sám obětí špionážního softwaru, napsal, že tento druh sledování je do značné míry důsledkem rostoucího stihomamu maďarského premiéra. Cecília Szilasová, bývalá velvyslankyně Maďarska v Číně, byla napadena softwarem Pegasus, krátce předtím, než se stala hlavní poradkyní Viktora Orbána. Attila Aszódi, státní tajemník Orbánovy vlády, odpovědný za výstavbu a rozvoj jaderné elektrárny Paks II, která má být postavena Roszatomem, byl také terčem špionážního softwaru Pegasus. Terčem se stal v roce 2018, kdy byl součástí vlády, ale měl konflikty se svým nadřízeným, ministrem Jánosem Sülim.

128. Kromě toho, byli softwarem Pegasus napadeni i syn a právník jednoho z Orbánových nejstarších přátel, Lajose Simicsky[187]. Z blízkého přítele se Simicska stal Orbánovým soupeřem. Právě prodával své mediální konsorcium, které po Orbánově volebním vítězství v roce 2018 podnítilo velkou část sporů, když došlo k tomuto zacílení na příbuzné[188]. Sám Simicska nebyl cílem z toho prostého důvodu, že nepoužívá chytrý telefon, což znemožňuje napadení špionážním softwarem, jako je Pegasus[189]. Ajtony Csaba Nagy, Simicskův právník, pojal podezření na napadení, když během telefonátu slyšel přehrávku svého rozhovoru s panem Simicskou. Později se tato podezření zdánlivě potvrdila, když se v maďarských médiích objevily informace, o nichž se hovořilo pouze v těchto hovorech[190]. Vzhledem k tomu, že většinu médií v Maďarsku vlastní stát, je pravděpodobné, že informace médiím poskytla sama vláda.

SPOLEČNOSTI ZABÝVAJÍCÍ SE ŠPIONÁŽNÍM SOFTWAREM

129. Maďarská vláda nejenže zakoupila a používá špionážní software Pegasus proti svým občanům, ale také poskytuje zázemí dalším společnostem působícím na trhu zpravodajských služeb, jako jsou Black Cube a Cytrox. Black Cube je izraelská soukromá zpravodajská služba, kterou tvoří bývalí zaměstnanci Mosadu, izraelské armády a izraelských zpravodajských služeb[191]. Na svých vlastních internetových stránkách se označuje za „kreativní zpravodajskou službu“, která nalézá „řešení složitých obchodních a soudních problémů podle potřeb konkrétních zákazníků“[192]. Byla zapojena do řady veřejně známých hackerských skandálů, mimo jiné v USA a Rumunsku[193]. Byly také odhaleny kritické vazby na společnost NSO Group a na špionážní software Pegasus. Po velkém tlaku veřejnosti na NSO Group, která najímala Black Cube na sledování svých odpůrců, se bývalý generální ředitel NSO Shalev Hulio

[187] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. července 2021.
[188] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. července 2021.
[189] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. července 2021.
[190] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19. července 2021.
[191] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7. října 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. dubna 2022.

přiznal, že najal Black Cube přinejmenším v jedné situaci na Kypru.

130. Společnost Black Cube se v Maďarsku angažovala během voleb v roce 2018, kdy sledovala různé nevládní organizace a osoby, které byly jakkoli spojeny s Georgem Sorosem, a podávala o tom zprávy Orbánovi, aby mohl jejich aktivity využít v pomlouvačné kampani[194]. Mezi napadenými byla i právnička a členka přední nevládní organizace na ochranu lidských práv Maďarský helsinský výbor Marta Pardaviová[195]. Výsledné informace ze sledování těchto osob a nevládních organizací se objevily nejen v maďarských státem kontrolovaných médiích, ale také v deníku Jerusalem Post[196].

131. Dalším spojením s Maďarskem je společnost Cytrox Holdings Zrt., která je registrována na adrese v Budapešti. Společnost Cytrox, tvůrce spywaru Predator, byla původně založena v Severní Makedonii, a poté ji koupila společnost WiSpear, která je nyní součástí aliance Intellexa, kterou provozuje Tal Dilian.

ZÁVĚREČNÉ POZNÁMKY

132. Používání softwaru Pegasus v Maďarsku se zdá být součástí plánované a strategické kampaně na ničení svobody sdělovacích prostředků a svobody projevu vládou[197]. Vláda využívá tento špionážní software k tomu, aby snadno a bez obav zavedla režim obtěžování, vydírání, vyhrožování a nátlaku vůči nezávislým novinářům, médiím, politickým oponentům a organizacím občanské společnosti. Vláda ovládá téměř všechna maďarská offline i vysílací média, což jí umožňuje nadále prosazovat svou vlastní verzi pravdy a bránit tomu, aby se k maďarským občanům dostala velká část veřejné kontroly, kterou provádí nezávislé sdělovací prostředky.

133. Zákon povolující používání odposlechu je mnohem více nástrojem kontroly a výkonu moci vlády než ochranou práv a soukromí občanů a je jedním z nejslabších v Evropě[198] [199]. Systém je zcela zjevně v rozporu s evropskými požadavky a normami pro sledování občanů, jak jsou formulovány Evropské úmluvě o lidských právech, a s rozsudky ESLP[200], přestože vláda trvá na tom, že ve všech případech postupovala v souladu se zákonem a plně jej dodržuje[201] [202]. Ačkoli se vláda soustavně odvolává na „národní bezpečnosti“[203], její tvrzení, že cíle sledování představují hrozbu pro národní

[194] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. července 2018.
[195] *Reuters*, https://www.reuters.com/article/meta-facebook-cyber-idCNL1N2T12MC, 16. prosince 2021.
[196] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. července 2018.
[197] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[198] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18. července 2021.
[199] DW, „*Pegasus scandal: In Hungary, journalists sue state over spyware*“ (Skandál Pegasus: V Maďarsku novináři žalují stát kvůli špionážnímu softwaru), 29. ledna 2022.
[200] Viz mimo jiné Roman Zacharov v. Rusko [velký senát], č. 47143/06, ESLP 2015 39, Klass a další v. Německo, 6. září 1978, bod 50, série A č. 28. 40; Prado Bugallo v. Španělsko, č. 58496/00, bod 30, 18. února 2003; Liberty a další v. Spojené království, č. 58243/00, bod 62, 1. července 2008.
[201] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4. listopadu 2021.
[202] Euractiv, „*Hungary employed Pegasus spyware in hundreds of cases, says government agency*“ (Maďarsko použilo špionážní software Pegasus ve stovkách případů“, říká vládní agentura), 1. února 2022.
[203] Euractiv, „*Hungary employed Pegasus spyware in hundreds of cases, says government agency*“ (Maďarsko použilo špionážní software Pegasus ve stovkách případů“, říká vládní agentura), 1. února 2022.

bezpečnost, nejsou přesvědčivá.

I.C. Řecko

134. Výbor navštívil Řecko v listopadu 2022 v rámci společné mise do Řecka na Kypr. Poslanci se setkali se státním tajemníkem Georgem Gerapetritisem a projednali významné případy sledování a širší kontext plurality sdělovacích prostředků a právního státu v Řecku. Setkali se také s investigativními novináři, poslanci řeckého parlamentu, předsedou řeckého úřadu pro ochranu údajů (HDPA), zástupci ADAE a nevládních organizací a obránci lidských práv.

135. Návštěva poukázala na skutečnost, že je třeba zvýšit úsilí o zajištění transparentnosti. Obvinění ze zneužití sledování a používání špionážního softwaru musí být důkladně prošetřeno a v případě potřeby sankcionováno. Měly by být zavedeny všechny nezbytné záruky a reformy by měly zvýšit transparentnost a zajistit odpovídající soudní dohled nad používáním dohledu. Návštěva rovněž potvrdila, že je třeba stanovit jasná pravidla pro omezení využívání národní bezpečnosti jako důvodu pro sledování, zajistit řádný soudní dohled a zaručit zdravé a pluralitní mediální prostředí.

136. V roce 2022 Řeckem otřásla řada zpráv o používání špionážního softwaru, který je podle řeckých zákonů nelegální. Poslanec Evropského parlamentu a předseda řecké opoziční strany PASOK Nikos Androulakis podal dne 26. července 2022 stížnost k úřadu státního zástupce při nejvyšším soudu, v níž tvrdí, že se někdo pokoušel nainstalovat na jeho mobilní telefon špionážní software Predator[204]. Pokus odhalila kontrola telefonu pana Androulakise, kterou provádělo IT oddělení Evropského parlamentu[205]. Podle forenzní analýzy IT oddělení se do jeho telefonu někdo pokusil proniknout v době, kdy pan Androulakis kandidoval na předsedu opoziční strany. Díky tomuto odhalení se do popředí pozornosti dostaly i stížnosti, jež v souvislosti s napadením svého telefonu programem Predator podal již v dubnu a květnu 2022 novinář Thanasis Koukakis, který se věnuje finančním tématům. Jeho napadení potvrdila organizace Citizen Lab. Bývalý ministr infrastruktury a zákonodárce strany Syriza, Christos Spirtzis[206] v září také tvrdil, že se stal terčem špionážního softwaru Predator. Ačkoli jeho mobilní telefon nebyl oficiálně kontrolován, pan Spirtzis se o obdržené odkazy podělil se dvěma techniky, kteří ústně potvrdili, že byl cílem[207]. Později v září dále vyšlo najevo, že Národní zpravodajská služba Řecka (EYP) měla údajně použít spyware ke sledování dvou svých zaměstnanců[208]. Ve dnech 5. a 6. listopadu řecké sdělovací prostředky odhalily seznam 33 cílů softwaru Predator, z nichž všechny byly významné osobnosti[209]. Seznam, který vláda ani sledované osoby nepotvrdily ani nepopřely, obsahuje jména osob působících v politice, byznysu a médiích v Řecku. Dopad údajného sledování osob, které se na seznamu objevily, by mohl být rozsáhlejší, protože všechny jejich kontakty a vazby by mohly být nepřímo „zachyceny“ v rámci špionážní operace, včetně jejich kontaktů v orgánech EU. Vysoký

[204] *EU Commission alarmed by new spyware case against Greek socialist leader* (Evropská komise je znepokojena novým případem špionážního softwaru proti řeckému socialistickému vůdci).
[205] Tagesspiegel, *Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not*.
[206] *Reuters*, *One more Greek lawmaker files complaint over attempted phone hacking.* (Další řecký zákonodárce podal stížnost kvůli pokusu o hackerské útoky na telefony.)
[207] https://insidestory.gr/article/predator-perissoteroi-apo-20-oi-stohoi-toy-stin-ellada-symfona-me-tin-arhi-prostasias.
[208] Efsyn, Zaměření na neoblíbence.
[209] Documento, Apokalypsa:Dívali se – tuto neděli v Documento.

výskyt špionážního softwaru byl údajně patrný již ve zprávě společnosti Meta z roku 2021, která ve své příloze uvádí 310 falešných odkazů na webové stránky související se spywarovou společností Cytrox, z nichž 42 bylo vytvořeno za účelem klamání cílů jen v Řecku[210] [211]. Koncem listopadu 2022, zveřejnil řecký deník *Documento* seznam 498 URL adres, které byly použity ke sledování špionážním softwarem Predator. Některé URL adresy jsou totožné s těmi, které byly zveřejněny ve zprávě Meta z roku 2021[212]. Dne 28. února 2023 předseda HDPA potvrdil, že na přibližně 100 zařízení bylo odesláno 300 textových zpráv souvisejících se špionážním softwarem Predator. Předseda úřadu ADAE dále uvedl, že úřad jednal na základě několika stížností a zjistil dva případy použití programu Predator a jedno číslo bankovního účtu osoby, která stojí za falešnými textovými zprávami. Probíhá šetření nových stížností ze strany ADAE[213].

137. V srpnu 2022 řecká vláda připustila, že služba EYP skutečně sledovala pana Androulakise a pana Koukakise, ale popřela, že by kdy použila nebo zakoupila špionážní software Predator. Kromě toho se během tohoto období objevily další případy sledování ze strany EYP, například novináře Stavrose Malichudise[214]. K dnešnímu dni nebyly oficiální důvody sledování zveřejněny.

138. Dne 8. srpna 2022 vydal premiér Mitsotakis videozprávu, v níž nejednoznačně uvedl, že sledování pana Androulakise bylo „legální“, ale „politicky nepřijatelné“. O sledování pana Koukakise ani o dalších údajných případech se nezmínil. Rovněž uvedl, že o sledování nevěděl, ale kdyby o něm věděl, nedovolil by ho[215]. Podle oficiálního prohlášení mluvčího vlády Yiannise Oikonomoua se státní ministr Giorgos Gerapetritis, jakmile se premiér dozvěděl o „zákonném odposlechu“ pana Androulakise, snažil pana Androulakise v soukromí plně informovat o důvodech jeho sledování[216]. Pan Androulakis odmítl být informován s tím, že takovéto soukromé informování by bylo nezákonné a že jediný zákonný postup je prostřednictvím řeckého parlamentu. Později při výpovědi před parlamentem ministr Gerapetritis prohlásil, že o důvodech nikdy nevěděl, a požádal, aby veškeré relevantní informace byly přísně utajeny. EYP je pod přímou kontrolou premiéra Kyriakose Mitsotakise na základě legislativní změny, která byla přijata krátce po nástupu jeho strany Néa Dimokratía k moci v roce 2019[217].

139. Po odhaleních rezignovali Grigoris Dimitriadis, vládní generální tajemník odpovědný za

[210] Meta, *Threat Report on the Surveillance-for-Hire Industry.* (Zpráva o hrozbách v odvětví nájemního sledování.)
[211] Inside Story, *Who was tracking the mobile phone of journalist Thanasis Koukakis?* (Kdo sledoval mobilní telefon novináře Thanasise Koukakise?).
[212] Documento, 27. listopadu 2022.
[213] Výměna názorů výboru PEGA s Konstantinosem Menoudakosem a Christosem Rammosem, 28. února 2023.
[214] Solomon, *Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'* (Reportér Solomonu Stavros Malichudis je pod dohledem z „důvodu národní bezpečnosti“); Ekathimerini, Případy odposlechů: Telefonní údaje, které vyvolaly další události; EPRS. *Greece's Predatorgate. The latest chapter in Europe's spyware scandal?* (Řecká Predatorgate: Nejnovější kapitola evropského skandálu se špionážním softwarem?).
[215] *Reuters*, „*Greek PM says he was unaware of phone tapping of opposition party leader*“. (Řecký premiér tvrdí, že o odposlechu telefonu předsedy opoziční strany nevěděl).
[216] 1b LIFO, Androulakis v soukromí popřel informace o svém sledování 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*“. (Další řecký opoziční zákonodárce obětí softwaru Predator).

spolupráci mezi řeckou vládou a EYP, a ředitel EYP Panagiotis Kontoleon[218].

NÁKUP

140. Na konci roku 2019 byl generální tajemník Dimitriadis v kontaktu se společností NSO Group za účelem nákupu špionážního softwaru Pegasus. V lednu 2020 předložila NSO Group oficiální návrh, který se týkal mezivládní dohody ve výši 50 milionů EUR. Po podpisu dohody by dotyčný ustoupil do pozadí a kontrolu by převzala EYP. EYP by na instalaci systému spolupracovala s Mosadem. Dohoda byla nakonec zrušena[219].

141. Jak EYP, tak vláda kategoricky popírají, že software Predator byl někdy zakoupen nebo používán řeckými orgány[220]. Vzhledem k absenci jakýchkoli důkazů o totožnosti kupujícího a uživatele softwaru Predator v řeckých případech, nelze ani s jistotou určit, zda a jak vláda nebo jiný subjekt tento software získali. Pokud to nebyla řecká vláda, nezbývá než konstatovat, že za (pokus o) napadení telefonů pana Koukakise a pana Androulakise je odpovědný nestátní subjekt. To by podle řeckého práva představovalo trestný čin, který by musel být vyšetřen. Hypotéza, že za útoky napadením softwarem Predator stojí soukromé subjekty, je navíc velmi nepravděpodobná, protože by nevysvětlovala výběr cílů sledování. V zásadě však není nemožné získat nebo využívat špionážní software, aniž by státní orgány tento software skutečně přímo zakoupily. Spyware může být nakoupen prostřednictvím zástupců, zprostředkovatelských společností nebo prostředníků, jak jsme viděli v jiných případech, nebo mohou být uzavřeny dohody s dodavateli špionážního softwaru o poskytování určitých služeb souvisejících se tímto typem softwaru. Není pochyb o tom, že mezi některými osobami a událostmi souvisejícími s vládou, EYP a dodavateli špionážního softwaru, zejména společností Krikel, která je přednostním dodavatelem komunikačního a sledovacího vybavení mj. pro policii a EYP, existovaly úzké vazby a vzájemné závislosti. Společnost Krikel je úzce napojena na osoby z okolí premiéra Mitsotakise. Přibývá důkazů o rozsáhlých vazbách mezi společností Intellexa, která vlastní špionážní software Predator, a řeckým státem. Dne 16. ledna 2023 uložil řecký úřad pro ochranu osobních údajů společnosti Intellexa pokutu ve výši 50 000 EUR za to, že nespolupracovala a odmítla předat informace o své klientele v rámci vyšetřování zahájeného v červenci 2020 na základě stížnosti pana Androulakise. Vyšetřování stále probíhá[221].

143. Jednou z možností je, že společnost Predator byla získána prostřednictvím společnosti Ketyak, Centra pro technologickou podporu, vývoj a inovace, které založil bývalý generální ředitel EYP Kontoleon. Funguje nezávisle na EYP[222] a podílí se na projektech týkajících se výzkumu, inovací a vývoje technologií[223].

SLEDOVANÉ OSOBY

---

[218] POLITICO, *PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal*. (Premiér Mitsotakis pociťuje napětí, když v souvislosti se špionážním skandálem skončili dva vysocí řečtí úředníci).
[219] https://insidestory.gr/article/greek-state-and-spyware-vendor-intellexa-they-are-acquainted-after-all.
[220] EPRS. *Greece's Predatorgate. The latest chapter in Europe's spyware scandal?* (Řecká Predatorgate: Nejnovější kapitola evropského skandálu se špionážním softwarem?)
[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.

GRIGORIS DIMITRIADIS

144. Dimitriadis je synovcem premiéra Mitsotakise a do srpna 2022 pracoval v jeho kanceláři jako generální tajemník. V rámci této funkce odpovídal za kontakty vlády s EYP. Dne 5. srpna 2022 byl nucen rezignovat poté, co bylo odhaleno, že EYP odposlouchávala telefon pana Androulakise. Zpočátku byla jeho rezignace přičítána toxickému politickému prostředí, později mu však premiér připsal politickou odpovědnost za odposlechy pana Androulakise a dalších politiků[224].

145. Bývalý šéf EYP Panagiotis Kontoleon přiznal řeckému parlamentnímu vyšetřovacímu výboru „společenskou známost“ s panem Dimitriadisem. Pana Kontoleona vybrala Mitsotakisova vláda, ale musela být upravena některá ustanovení zákona, aby mohl být jmenován[225].

146. Pan Dimitriadis je také v několika ohledech úzce spojen s Felixem Bitziosem a Giannisem Lavranosem. Tito tři muži se osobně znají. Pan Dimitriadis a pan Lavranos si byli navzájem svatebními svědky („koumbaroi“)[226] a pan Dimitriadis je kmotrem druhého dítěte pana Lavranose[227]. Pan Dimitriadis má také nepřímou vazbu na pana Bitziose skrze obchodní transakce s Bitziosovým bratrem[228].

147. To ho staví do středu sítě, která ho profesně i osobně spojuje s klíčovými osobami ve společnostech Intellexa, Krikel a EYP.

148. Pan Dimitriadis se údajně také zná s Adreasem Loverdosem, kandidátem do vedení strany PASOK-KINAL z roku 2021.

FELIX BITZIOS

149. Podnikatel Felix Bitzios byl zapleten do rozsáhlého skandálu s porušováním kontrol pohybu kapitálu ze strany Piraeus Bank. Po dobu vyšetřování byl panu Bitziosovi zmrazen majetek[229]. Premiér Mitsotakis však krátce po svém nástupu k moci v roce 2019 prosadil kontroverzní legislativní změnu, která panu Bitziosovi pomohla. Spočívala v zavedení maximální doby, po kterou může být majetek zmrazen, stanovené na 18 měsíců[230]. Díky tomuto zásahu Mitsotakisovy vlády tak mohl být majetek pana Bitziose znovu uvolněn.

150. Pan Bitzios je spojen s Kyprem prostřednictvím své společnosti Santinomo, registrované na Kypru, a vazbou na Tala Diliana. Zdá se, že pan Bitzios napomohl převodu společnosti Intellexa do Řecka[231]

151. Pan Bitzios prostřednictvím své firmy Santinomo vlastnil 35% podíl ve společnosti

---

[224] https://www.iefimerida.gr/politiki/paraitisi-dimitriadi-klima-toxikotitas-ohi-predator?amp, https://primeminister.gr/2022/08/08/29961.
[225] *Ieidiseis*, SYRIZA – PASOK zjištění o odposleších: Skandál i zástěrka.
[226] TVXS, Giannis Lavranos: *The koumbarias with Tsouvala and Dimitriadis*.
[227] Ieidiseis, SYRIZA – PASOK zjištění o odposleších: Skandál i zástěrka.
[228] Reporters United, *The Great Nephew and Big Brother*. (Velký synovec a velký bratr).
[229] Lexocology, *Cyprus court offers directions to bank on ambit of freezing injunction.* (Kyperský soud dal bance pokyny ohledně rozsahu příkazu k zmrazení majetku).
[230] Financial Times, *Greek law change viewed as backtracking on money laundering.* (Změna řeckého zákona je vnímána jako ústup od praní peněz).
[231] Inside Story, Predatorgate: Druhý akcionář společnosti Intellexa SA.

Intellexa. Dne 4. srpna 2022 však nechal zaregistrovat převod všech svých akcií na mateřskou společnost Intellexy Thalestris[232]. Registrace převodu se uskutečnila několik dní po odhalení hackerského útoku na pana Androulakise. Samotný převod se však údajně uskutečnil 28. prosince 2020, tedy o více než 19 měsíců dříve. Pan Bitzios se tak retroaktivně distancoval od třetinového podílu v Intellexe. S touto společností byl ale spojen i jinak – od března 2020 do června 2021 v Intellexe působil jako zástupce správce[233].

GIANNIS LAVRANOS

152. Giannis Lavranos byl obviněn z daňových úniků a novinář pan Koukakis o jeho případu psal.

INTELLEXA

153. Špionážní software Predator prodává společnost Intellexa, což je konsorcium prodejců špionážního softwaru, které je zastoupeno mj. v na Kypru, v Řecku, Irsku a Francii. Na Kypru jej založil Tal Dilian, který byl dříve důstojníkem izraelské armády. Klíčovou postavou v této složité síti společností je jeho bývalá druhá manželka, Polka Sara Hamouová. Tal Dilian získal také občanství Malty. Řecká vláda prohlásila, že společnosti Intellexa byly uděleny dvě vývozní licence, z nichž jedna povoluje vývoz na Madagaskar. Kromě toho řecká vláda vydala licenci pro vývoz softwaru Predator do Súdánu. Nebylo potvrzeno, komu byla licence vydána, zda společnosti Intellexa nebo jinému subjektu. Společnost Intellexa údajně vyvážela své výrobky také do Bangladéše.

154. Dne 30. listopadu 2022 odhalila vyšetřovací zpráva Lighthouse Reports ve spolupráci s izraelskými novinami *Haaretz* a řeckým serverem Inside Story, že operace Predator Tala Diliana v Řecku byly údajně spojeny s letadlem Cessna, které v období od dubna do srpna 2022 létalo z Řecka a Kypru do Súdánu. Údajně tento letoun tajně a nelegálně dodal špičkovou technologii sledování milice rychlé podpory (RSF)[234]. Záznamy o letu propojily tento soukromý letoun, který letěl tam i zpět přes Kypr, s Talem Dilianem, bývalým vysoce postaveným příslušníkem izraelských obranných sil, který v roce 2019 založil společnost Intellexa Alliance s pobočkami na Kypru a v Řecku. Dne 18. února 2023 Komise potvrdila, že se obrátila na vnitrostátní orgány v Řecku a na Kypru, aby tuto záležitost objasnily. Odpověď však Komise neobdržela[235]. Dne 19. dubna 2023 potvrdil řecký náměstek ministra zahraničních věcí Miltiadis Varvitsiotis, že řecká vláda schválila licenci na vývoz špionážního softwaru Predator do Súdánu. Ministr však popírá jakoukoli roli softwaru Predator v nedávných střetech mezi súdánskými ozbrojenými silami a milicemi RSF v Súdánu[236].

---

[232] Inside Story, Predatorgate: Druhý akcionář společnosti Intellexa SA.
[233] https://insidestory.gr/article/predatorgate-o-deyteros-metohos-tis-intellexa-ae.
[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; Schůze výboru PEGA, 28. března 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.

155. V prosinci 2022 řecká vláda oznámila, že společnosti Intellexa udělila dne 15. listopadu 2021 dvě vývozní licence. Podle mluvčího řeckého ministerstva zahraničí Alexandrose Papaioannouho jedna z těchto licencí povolila prodej softwaru Predator Madagaskaru[237]. Licence byla udělena navzdory špatnému stavu lidských práv v této zemi[238] a potenciálně je v rozporu s nařízením EU o dvojím užití[239]. Generální tajemník pro mezinárodní hospodářské vztahy Ioannis Smyrlis, který schválil prodej softwaru Predator na Madagaskar, podal po těchto odhaleních demisi[240] a nastoupil na místo zástupce generálního ředitele vládnoucí strany Néa Dimokratía, která je zodpovědná za nadcházející volby.

156. Kromě vývozu špionážního softwaru se v jednom případě údajně v Řecku konala školení o používání tohoto typu softwaru. V červnu 2021 koupil Bangladéš špionážní vozidlo od kyperské společnosti Passitora. Podle dokumentů bangladéšského ministerstva vnitra byli pracovníci Národního střediska pro sledování telekomunikací (NTMS) vyškoleni v Řecku v letech 2021 až 2022, aby mohli špionážní vozidlo používat. Vozidlo nakonec dorazilo do Bangladéše v červnu 2022[241].

KRIKEL

157. Společnost Krikel je jedním z hlavních dodavatelů vybavení pro řecké policejní a bezpečnostní orgány. V Řecku také zastupuje italskou společnost RCS Lab, která prodává sledovací software. Kromě toho se má za to, že 50% podíl společnosti Krikel vlastní Giannis Lavranos, a to prostřednictvím jiné společnosti s názvem Mexal[242]. Avšak skutečného vlastníka společnosti Krikel, navzdory četným smlouvám, které společnost uzavřela se státními orgány, zřejmě nelze s jistotou určit.

158. V roce 2014 byla společnost Giannise Lavranose Ioniki Technologiki prodána londýnské společnosti Tetra Communications. V témže roce Ioniki Technologiki spolu s dalšími dvěma společnostmi darovala komunikační systémy Tetra řeckému ministerstvu

---

[237] The New York Times, 8. prosince 2022, „*How the Global Spyware Industry Spiraled Out of Control*“ (Jak se světový průmysl špionážního softwaru vymkl kontrole), https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[238] The New York Times, 8. prosince 2022, „*How the Global Spyware Industry Spiraled Out of Control*“ (Jak se světový průmysl špionážního softwaru vymkl kontrole), https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[239] Nařízení Evropského parlamentu a Rady (EU) 2021/821 ze dne 20. května 2021, kterým se zavádí režim Unie pro kontrolu vývozu, zprostředkování, technické pomoci, tranzitu a přepravy zboží dvojího užití (Úř. věst. L 206, 11.6.2021, s. 1).

[240] The National Herald, „*Top Greek Official Who Authorized Predator Spyware Sale Resigns*“ (Vrcholný řecký představitel, který povolil prodej spywaru Predator, rezignoval na svou funkci).

[241] Haaretz, „*Israeli Spy Tech Sold to Bangladesh, World's Third-largest Muslim Country, Despite Dismal Human Rights Record*“ (Prodej izraelské špionážní techniky do Bangladéše, třetí největší muslimské země na světě, navzdory špatným výsledkům v oblasti lidských práv).

[242] Je zde několik zajímavých souvislostí. Lavranos prodal v dubnu 2021 svůj rodinný dům v Aténách za cenu nižší, než je jeho tržní hodnota, společnosti Albitrum Properties. Zástupcem Albitrum Properties během prodeje byl nevlastní bratr Felixe Bitziose Theodoros Zervos. Albitrum je kyperská společnost a jejím akcionářem je Mexal Services Ltd. Mexal Services vlastní 100 % společnosti Eneross Holdings Ltd. Eneross Holdings navíc vlastní společnost Krikel. Úřední adresa Giannise Lavranose je stejná jako sídlo Eneross Holdings a Mexal Services na Kypru. Viz: Inside Story, „*Predatorgate's invisible privates*“ (Neviditelné soukromí Predatorgate) a TVXS, „*G. Lavranos behind KRIKEL – How the deception of the Parliament was attempted [Revealing documents]*“ (G. Lavranos v pozadí společnosti KRIKEL – Jak došlo k pokusu o podvod na Parlament [Dokumenty z odhalení]).

vnitra[243]. V roce 2014 projevila řecká vláda zájem o italský spyware RCS Galileo od společnosti Hacking Team, jak odhalily WikiLeaks, ale tento software nebyl nikdy získán[244]. Darování společnosti Tetra zprostředkovala společnost se sídlem na Floridě, což umožnilo obejít běžná výběrová řízení. Řecká vláda dar přijala v roce 2017. V roce 2018 byla se společností Krikel podepsána smlouva na údržbu a technickou podporu v hodnotě10,8 milionu EUR. Smlouvu za Krikel podepsal Stanislaw Pelczar, ale na celý průběh jednání podle všeho neoficiálně dohlížel Lavranos[245]. Společnost Krikel se stala významným dodavatelem řeckého ministerstva vnitra. Od roku 2018 podepsala s řeckou státní správou sedm smluv, z toho šest tajných[246].

159. Společnost Krikel rovněž získala obchodní zastoupení italské společnosti RCS Lab v Řecku. V červnu 2021 údajně koupila řecká zpravodajská služba (EYP) od společnosti RCS Lab[247] systémy pro odposlech, a to právě prostřednictvím společnosti Krikel[248]. V té době odpovídal za smlouvy mezi státní správou a EYP pan Dimitriadis. Podle některých zdrojů to bylo právě v době instalace tohoto nového systému, kdy se měl ztratit materiál obsahující informace o sledování Androulakise a Koukakise, údajně kvůli technickému problému[249]. Jiné zdroje však uvádějí, že materiál byl dne 29. července 2022 zničen na příkaz Kontoleona[250].

160. Zajímavé je, že ve společnosti Keytak byli spatřeni zaměstnanci společnosti Krikel, kteří tam měli údajně pracovat bez nároku na odměnu. Společnost Ketyak údajně získala 40 milionů EUR z nástroje EU pro obnovu a odolnost prostřednictvím důvěrného výběrového řízení na základě tajného rozhodnutí předsedy vlády[251]. Nezákonné využívání finančních prostředků EU k financování nezákonného špionážního softwaru by představovalo závažné porušení práva Unie a spadalo by do pravomoci řady evropských orgánů, včetně úřadu evropského žalobce.

161. Zaměstnanci společnosti Krikel údajně v prosinci 2021 a lednu 2022 rovněž navštívili zařízení EYP v Agia Paraskevi v pozici „školitelů“. Tato zařízení jsou řízena řeckou vládou a jsou údajně místem, kde byl instalován špionážní software Predator[252].

ZAPOJENÍ PÁNŮ BITZIOSE A LAVRANOSE

162. Pánové Bitzios i Lavranos se v roce 2017 aktivně podíleli na založení společnosti

[243] Inside Story, „*Predatorgate's invisible privates*“ (Neviditelné soukromí Predatorgate).
[244] Inside Story, „*The timeless interest of the Greek authorities in spyware*“ (Nadčasový zájem řeckých úřadů o špionážní software).
[245] Inside Story, „*Predatorgate's invisible privates*“ (Neviditelné soukromí Predatorgate).
[246] Inside Story, „*Predatorgate's invisible privates*“ (Neviditelné soukromí Predatorgate).
[247] Hellas Posts English, „*The EYP supplier contaminates smartphones in Greece as well*“(Dodavatel služby EYP kontaminuje chytré telefony i v Řecku).
[248] TVXS, ‘G. *Lavranos behind KRIKEL – How the deception of the Parliament was attempted [Revealing documents]*“ (G. Lavranos v pozadí společnosti KRIKEL – Jak došlo k pokusu o podvod na Parlament [Dokumenty z odhalení]).
[249] TVXS, ‘G. *Lavranos behind KRIKEL – How the deception of the Parliament was attempted [Revealing documents]*“ (G. Lavranos v pozadí společnosti KRIKEL – Jak došlo k pokusu o podvod na Parlament [Dokumenty z odhalení]).
[250] Euractiv, „*Greek MEP spyware scandal takes new turn*“ (Skandál řeckého europoslance se špionážním softwarem nabírá nový směr).
[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*“ (Řecký stát a prodejce špionážního softwaru Intellexa: přeci jen se navzájem znají).

Krikel. Společně rozhodli o tom, že administrátorem této společnosti bude v říjnu 2017 jmenován polský právník Stanislaw Pelczar[253]. Následně byla najata společnost pana Bitziose Viniato Holdings Limited, aby pro společnost Krikel vykonávala v období leden až srpen 2018 poradenské služby, a to za odměnu ve výši přibližně 550 000 EUR (ačkoli společnost Krikel měla v daném roce obrat pouze 840 000 EUR)[254].

163. Pánové Bitzios a Pelczar mají i další vzájemné obchodní vazby. Z Paradise Papers vyplývá, že mají společnou společnost registrovanou na Maltě pod názvem Baywest Business[255]. Kromě toho je Tal Dilian, zakladatel společnosti Intellexa, držitelem maltského (zlatého) pasu[256] a v ostrovním státě má také schránkovou společnost MNT Investments LTD[257].

164. Pánové Bitzios a Lavranos jsou dva klíčoví aktéři v oblasti dodávek telekomunikačního a sledovacího materiálu státním orgánům, jako je policie a EYP. Pan Bitzios byl ústřední postavou ve společnosti, která prodává software Predator. Oba měli úzké vztahy s panem Dimitriadisem a oba získávali lukrativní státní zakázky. Ze změny legislativy, kterou prosadila nová vláda, měli prospěch, protože jejich zmrazený majetek byl uvolněn. Ke sledování pana Koukakise měli motiv. Jestliže jsou takto propojeny obchodní zájmy, osobní vztahy a politické vazby, je zcela jasné, že vzniká vysoké riziko střetu zájmů a korupce. Oby by navíc zcela jistě mohli poskytnout zásadní informace o pořizování a používání systému Predator v Řecku.

165. Přestože bylo zřejmé, že svědectví pánů Bitziose a Lavranose před vyšetřovacím výborem řeckého parlamentu je důležité, většina poslanců strany Néa Dimokratía ve výboru odmítla žádosti opozice o předvolání těchto osob k výslechu.

PŘEDBĚŽNÁ KONTROLA

166. Napadení zařízení špionážním softwarem je v Řecku trestným činem podle hned několika článků řeckého trestního zákoníku. Je to např. článek 292 o trestných činech narušujících bezpečnost telefonické komunikace, článek 292B o narušování fungování informačních systémů a článek 370 o porušování listovního tajemství. Kromě toho je podle článku 292C řeckého trestního zákoníku trestným činem také výroba, prodej, dodávání, používání, dovoz, vlastnění a distribuce škodlivého softwaru (což zahrnuje i špionážní software)[258]. Tento článek řecká vláda dne 9. prosince 2022 změnila.

167. Počet povolení k odposlechům se v průběhu let výrazně zvýšil. Z 4 871 v roce 2015 na 11 680 v roce 2019 a 15 475 v roce 2021[259]. V současnosti se každý den musí zpracovat

[253] TVXS, "G. Lavranos behind KRIKEL – How attempts were made to deceive the Parliament [Revealing documents]".
[254] Inside Story, „*From Koukakis to Androulakis*: *A new twist in the Predator spyware case*" (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).
[255] International Consortium of Investigative Journalists, Offshore Leaks Database, Paradise Papers – Malta Corporate Registry.
[256] Maltská vláda, Persons Naturalised Registered as Citizens of Malta, 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/.
[258] International Comparative Legal Guide, *Cybersecurity Laws and Regulation Greece 2022*. (Zákony a regulace kybernetické bezpečnosti Řecko 2022)
[259] Ekathimerini, Odposlechy a „národní bezpečnost".

asi 60 žádostí, přičemž donedávna přicházely pouze od jednoho státního žalobce. Kromě toho ustanovení EYP, která ruší důvěrnost komunikace občanů z důvodů národní bezpečnosti, neuvádějí jméno dotyčné osoby ani důvod zrušení důvěrnosti. Omezují se na telefonní číslo a zdůvodnění národní bezpečností[260].

168. Soudní povolení ke sledování soukromé komunikace, jakož i prodloužení a ukončení platnosti takového povolení musí schválit příslušný státní zástupce. Jak je stanoveno v zákoně č. 3649/2008, příslušným státním zástupcem pro zrušení utajení a důvěrnosti je interní státní zástupce EYP. Legislativní změna z roku 2018 za druhé vlády premiéra Tsiprase snížila počet státních zástupců potřebných pro povolení odposlechu ze dvou na jednoho. Státní zástupkyní, která se těmito případy zabývá, je Vasiliki Vlachouová[261]. Paní Vlachouová se s členy výboru PEGA, kteří přicestovali do Řecka, nesetkala.

NAŘÍZENÍ S MOCÍ ZÁKONA

169. Po aféře se sledováním navrhl premiér Mitsotakis změny právního rámce pro fungování EYP. Jedna z těchto změn spočívala v tom, že vláda dne 9. srpna 2022 zavedla nařízení s mocí zákona. Došlo k úpravě znění odstavce 2 článku 9 zákona 3649/2008. Nyní je k jmenování ředitele EYP vyžadováno stanovisko Stálého výboru pro instituce a transparentnost[262]. Avšak vzhledem k tomu, že absolutní většinu ve Stálém výboru pro instituce a transparentnost má nyní vládní strana, novým ředitelem EYP byl po schválení tímto výborem jmenován pan Demiris, přestože všechny ostatní opoziční strany byly proti[263]. Stejně tak se druhým zástupcem velitele EYP stal bývalý člen kabinetu předsedy vlády Dionysis Melitsiotis[264] a zástupcem ředitele zase Anastasios Mitsialis, který dříve působil ve vedení strany Néa Dimokratía[265].

170. Kromě toho zákon znovu zavedl povolování žádostí o sledování dvěma státními zástupci[266]. Článek 5 zákona 3649/2008 o ustanovení o zrušení důvěrnosti komunikace ze strany EYP je doplněn o předložení ke schválení příslušnému odvolacímu státnímu zástupci a následné schválení státním zástupcem odvolacího soudu[267].

NÁSLEDNÁ KONTROLA

171. Od roku 2019 je činnost EYP pod přímou kontrolou premiéra Kyriakose Mitsotakise. Umožnila to změna zákona schválená po vítězství strany Néa Dimokratía v roce

---

[260] Reporters United, „*Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*“ (Nepřítel státu: Dokazujeme, že Mitsotakisova vláda sledovala novináře Thanase Koukakise).
[261] Reporters United, „*Enemy of the State*: *We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*“ (Nepřítel státu: Dokazujeme, že Mitsotakisova vláda sledovala novináře Thanase Koukakise).
[262] EfSyn, „*What (does not) change with the Act of Legislative Content for EYP?*“ (Co se (ne)mění se zákonem o legislativním obsahu pro EYP).
[263] Ekathimerini, „Themistoklis Demiris:Jeho jmenování do vedení EYP bylo schváleno většinou“.
[264] Ekathimerini, „Národní bezpečnost v centru pozornosti“.
[265] Greek City Times, „*Greek PM appoints new security and intelligence chiefs*“ (Řecký premiér jmenoval nové šéfy bezpečnostních a zpravodajských služeb).
[266] At a Glance, „*Greece's Predatorgate: The latest chapter in Europe's spyware scandal?*“(Řecká Predatorgate: Nejnovější kapitola evropského skandálu se špionážním softwarem) Evropský parlament, Generální ředitelství pro parlamentní výzkumné služby, 8. září 2022.
[267] EfSyn, „*What (does not) change with the Act of Legislative Content for EYP?*“ (Co se (ne)mění se zákonem o legislativním obsahu pro EYP).

2019[268].

172. Parlamentní kontrolu vykonává Stálý výbor pro instituce a transparentnost. Výbor dohlíží na činnost EYP a má pravomoc shromažďovat dokumenty, vyslýchat osoby a předvolávat generálního ředitele ke slyšení[269]. Absolutní většinu ve složení výboru má vládní strana.

173. Řecký úřad pro bezpečnost komunikace a soukromí (ADAE) zajišťuje ochranu důvěrnosti pošty a všech ostatních druhů komunikace[270]. Statut úřadu mu přiznává správní autonomii[271]. Úřad ADAE může provádět šetření v zařízeních, databázích a archivech a také šetření technického vybavení a dokumentů EYP[272].

174. Důvěrnost komunikace je chráněna zákonem 2225/1994, v němž se uvádí, že této důvěrnosti může být zproštěna pouze v případech ohrožení národní bezpečnosti a z důvodu vyšetřování závažných trestných činů. Článek 5 dále stanoví, že po zrušení důvěrnosti může úřad ADAE uvědomit sledované osoby o probíhajícím vyšetřování, avšak pouze v případě, že tím není ohrožen účel vyšetřování[273]. Právo jednotlivce na přístup k informacím o tom, zda byl předmětem sledování, upravuje zákon 2472/1997[274]. Když však v březnu 2021 úřad ADAE upozornil EYP na to, že Koukakis má právo být informován, vláda okamžitě zareagovala a dne 31. března 2021 podala pozměňovací návrh 826/145, kterým úřadu ADAE zakázala informovat občany o zrušení důvěrnosti komunikace[275]. To de facto zbavuje jednotlivce práva na informace. Uvedená novela byla přijata velmi nestandardním způsobem, Byla připojena ke zcela nesouvisejícímu zákonu (o opatřeních proti COVID-19), a nebyly dodrženy ústavou stanovené lhůty ústavou[276] [277] [278]. V žádném případě tady proto nelze hovořit o řádném konzultačním procesu.

175. Zákonem o obsahu právních předpisů chtěl Mitsotakis posílit transparentnost a odpovědnost. Zákon však nezrušuje novelu 826/145.

176. Dne 9. prosince 2022 přijala řecká vláda zákon č. 5002/2022 s cílem aktualizovat a vytvořit účinný právní rámec pro ochranu osobních údajů, komunikačního tajemství a posílení kybernetické bezpečnosti. Zákon však zavádí několik ustanovení, která oslabují záruky, kontrolu a odpovědnost. Jak je stanoveno v čl. 4 odst. 7[279], každou žádost

---

[268] Euractiv, „Another Greek opposition lawmaker victim of Predator“.
[269] Centrum pro evropské ústavní právo, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies* (Vnitrostátní zpravodajské orgány a sledování v EU: Záruky základních práv a opravné prostředky).
[270] ADAE, *Prezentace*.
[271] ADAE*, Regulační rámec.*
[272] Centrum pro evropské ústavní právo, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies* (Vnitrostátní zpravodajské orgány a sledování v EU: Záruky základních práv a opravné prostředky).
[273] Constitutionalism, „Rozpor článku 87 zákona č. 4790/2021 se zárukami EÚLP na ochranu důvěrnosti komunikace“.
[274] Řecký úřad pro ochranu osobních údajů (DPA), Zákon 2472/1997 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů.
[275] https://www.reportersunited.gr/8646/eyp-koukakis/.
[276] Řecký parlament, Ústava.
[277] Řecký parlament, Jednací řád Sněmovny.
[278] Govwatch, „Violation of the legislative process for amendments in law 4790/2021“ (Porušení legislativního procesu pro změny zákona 4790/2021).
[279] https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022.

jednotlivců o informace o tom, zda byli sledováni z důvodů národní bezpečnosti, posoudí tříčlenný výbor složený z ředitele EYP, státního zástupce při EYP a vedoucího úřadu ADAE. To znamená, že většinu nesou ti, kteří sledování nařídili (ředitel EYP) a povolili (státní zástupce). Kromě toho prakticky znemožňuje, aby byly osoby, které jsou sledovány z důvodů národní bezpečnosti, náležitě informovány *ex post*, neboť zákon stanoví, že mohou podat příslušnou žádost až tři roky po ukončení sledování. To je neslučitelné s příslušnou judikaturou Evropského soudu a Evropskou úmluvou o lidských právech[280] a nezajišťuje to systém institucionálních brzd a protivah pro zajištění řádného fungování státní moci. Úřad ADAE vyjádřil svůj nesouhlas s tříčlenným orgánem. K dnešnímu dni neexistuje žádný operační rámec pro tripartitní výbor, což znamená, že de facto nefunguje[281]. Kromě toho nový zákon kriminalizuje používání špionážního softwaru jednotlivci nebo soukromými společnostmi a poprvé legalizuje nákup špionážního softwaru veřejnými orgány, přičemž vládu zmocňuje k zavedení tohoto postupu prostřednictvím prezidentského dekretu. Neexistuje žádné ustanovení o soudním dohledu nad používáním špionážního softwaru ani o zadávání odposlechů soukromým subjektům.

177. Poskytování špionážního softwaru soukromými subjekty je nezákonné pouze tehdy, pokud je takový software uveden na orientačním seznamu „zakázaného špionážního softwaru“, který je každých šest měsíců aktualizován ředitelem EYP. Opravňuje EYP k legálnímu pořizování špionážního softwaru, protože kritické relevantní otázky budou řešeny výhradně prostřednictvím sekundárních právních předpisů (tj. prezidentský dekret). Aktualizovaná verze stávajícího špionážního softwaru bude proto považována za legální, dokud nebude zařazena na výše uvedený seznam. Definice „národní bezpečnosti“ v zákoně je velmi široká a vágní, což je v rozporu s čl. 19 odst. 1 Ústavy, který vyžaduje úzký výklad. Úřadu ADAE je dále bráněno v jeho úsilí vykonávat svou ústavně určenou úlohu při kontrole procesu odtajňování. Úloha nezávislého orgánu, který přispěl k odhalení skandálu týkajícího se sledování, je v novém zákoně zlehčována, a to navzdory příslušným ústavním zárukám.

178. Možnosti následné kontroly byly oslabeny skutečností, že Řecku trvalo dlouho, než plně provedlo směrnici EU o oznamovatelích[282]. Dne 27. ledna 2022 zahájila Komise řízení o nesplnění povinnosti zasláním výzvy Řecku. Dne 15. července 2022[283] zaslala Komise odůvodněné stanovisko s dvouměsíční lhůtou pro odpověď. Řecký parlament nakonec 11. listopadu 2022 odhlasoval zákon č. 4990/2022, kterým byla směrnice EU o oznamovatelích provedena do řeckého práva.

---

[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.

[281] Výměna názorů výboru PEGA s Konstantinosem Menoudakosem a Christosem Rammosem, 28. února 2023.

[282] https://ec.europa.eu/commission/presscorner/detail/CS/inf_22_3768.

[283] https://ec.europa.eu/commission/presscorner/detail/CS/inf_22_3768.

VEŘEJNÁ KONTROLA

179. Řecko se v žebříčku světového indexu svobody tisku za rok 2022 umístilo ze všech zemí EU nejhůř, a sice na 108. místě ze 180 zemí[284]. V roce 2021 byl zavražděn novinář Giorgos Karaivaz. Jeho vražda dosud nebyla objasněna. Novináři čelí zastrašování a strategickým žalobám proti účasti veřejnosti (SLAPP). Grigoris Dimitriadis[285] podal žalobu na zpravodajská média Reporters United a *Efimerida ton Syntakton* (EfSyn)[286] poté, co byl přinucen rezignovat. Ministr Oikonomou se zase snažil zdiskreditovat reportérku média *Politico* Nektariu Stamouliovou tvrzením, že její články o skandálu se špionážním softwarem jsou politicky motivované[287]. Pánové Koukakis a Malichudis, dva cíle sledování, skutečně kriticky informovali o případech korupce a podvodů a špatném zacházení s migranty. O skandálu se špionážním softwarem informovali také Athanasios Telloglou a Eliza Triantafillouvá a byli údajně sledováni[288]. Řecký nejvyšší státní zástupce Isidoros Dogiakos navíc zdiskreditoval média, která kritizovala řecké justiční orgány za nedostatečné řešení skandálu s odposlechy. Dokonce se pokusil zastrašit média vyšetřující skandál tím, že požadoval selektivní daňové kontroly jejich vlastníků[289].

ZJEDNÁNÍ NÁPRAVY

NÁRODNÍ ÚŘAD PRO TRANSPARENTNOST

180. Jak je stanoveno v článku 82 zákona č. 4622/2019, má Národní úřad pro transparentnost (EAD) odpovědnost za posílení odpovědnosti, transparentnosti a integrity opatření prováděných vládními orgány, státními orgány, správními orgány a veřejnými organizacemi. Kromě toho by měl EAD předcházet podvodům a korupci ze strany veřejných a soukromých subjektů, odhalovat je a řešit. Podle tohoto zákona převzal úřad EAD veškeré odpovědnosti, práva a povinnosti od těchto veřejných subjektů: Generální sekretariát pro boj proti korupci; orgán auditorů-inspektorů veřejné správy; úřad generálního inspektora veřejné správy; orgán inspektorů zdravotních a sociálních služeb; orgán inspektorů veřejných prací; a orgán inspektorů-auditorů dopravy[290]. Zatímco nezávislost úřadu ADAE je zakotvena v ústavě, EAD není nezávislým orgánem.

181. Úřad EAD začal dne 22. července 2022 prošetřovat údajný nákup špionážního softwaru Predator ministerstvem vnitra a EYP. Audit se zaměřil na řeckou policii, EYP a společnosti Intellexa a Krikel. Svou zprávu úřad dokončil 10. července 2022, ale musel ji předložit EYP ke schválení. Oficiální zpráva, která byla 22. července zaslána panu Koukakisovi, se zmiňovala jen o částech celého auditu, který úřad provedl. Pod záminkou ochrany osobních údajů byla ze zprávy odstraněna některá jména, včetně jmen auditorů z EAD, státního zástupce EYP, který původní zprávu úřadu EAD

[284] https://rsf.org/en/index.
[285] Tagesspiegel.
[286] EUobserver, „*Greece accused of undermining rule of law in wiretap scandal*“ (Řecko obviněno z podkopávání právního státu ve skandálu s odposlechy).
[287] https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/.
[288] Heinrich-Böll-Stiftung, „V podmínkách absolutní osamělosti.“
[289] Novinářské odbory ESIEA odsuzují výhrůžky ze strany nejvyššího státního zástupce, https://www.esiea.gr/oi-dimosiografikes-enoseis-gia-tis-di/.
[290] https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019.

kontroloval, a jmen právníků a účetních právnických osob, které byly do případu zapleteny[291].

182. Zpráva úřadu EAD nakonec dospěla k závěru, že ani EYP, ani ministerstvo vnitra žádnou smlouvu se společností Intellexa a dalšími řeckými společnostmi, kterých se případ týkal, neuzavřely. A dále že nezakoupily, ani nepoužívaly špionážní software Predator[292]. Úřad ovšem nezkontroloval bankovní účty společností Intellexa a Krikel ani jejich přidružených offshorových společností. Kromě toho úřad EAD navštívil kanceláře společností Intellexa a Krikel až po dvou měsících od prvního zveřejnění informací o používání softwaru Predator v Řecku, kdy zaměstnanci pracovali doma kvůli COVID-19. EAD se dále nesetkal s právními zástupci dotčených společností[293].

183. Nad nezávislostí vedení úřadu EAD se vznášejí otazníky. Současný ředitel, bývalý zaměstnanec pana Mitsotakise, zastává tuto funkci dočasně od léta 2022. Není jasné, proč nebylo zahájeno výběrové řízení. Ředitel EAD se s výborem PEGA během jeho mise v listopadu 2022 nesetkal. Dne 7. března 2023 se ředitel setkal s delegací výboru LIBE, kde byly vzneseny otázky týkající se špionážního softwaru v Řecku.

ŘECKÝ ÚŘAD PRO BEZPEČNOST KOMUNIKACE A SOUKROMÍ (ADAE)

184. V červenci 2022 podal Nikos Androulakis stížnost k úřadu státního zástupce při nejvyšším soudu, v níž tvrdí, že se někdo pokoušel nainstalovat na jeho mobilní telefon špionážní program Predator dne 21. září 2021. Na základě této stížnosti úřad ADAE zahájil v srpnu 2022 šetření, přičemž si nejdříve vyžádal informace od telekomunikačního operátora pana Androulakise.

185. Špionážní software Predator zanechává jen málo stop, které by poskytovatelům telekomunikací umožnily zjistit napadení přístroje. Úřad ADAE však zjistil, že mobilní telefon Androulakise byl řeckou tajnou službou sledován[294] a že její interní státní zástupkyně Vasiliki Vlachouová povolila sledování a zásah do důvěrnosti v září 2021, a to v časové shodě s údajným napadením softwarem Predator.

186. Na základě výsledků šetření úřadu ADAE Grigoris Dimitriadis a Panagiotis Kontoleon odstoupili ze svých pozic ve vládě[295]. Pan Kontoleon uvedl, že sledování pana Androulakise bylo zahájeno na žádost zahraničních orgánů – konkrétně zpravodajských agentur Arménie a Ukrajiny – vzhledem k jeho účasti ve Výboru Evropského parlamentu pro obchodní vztahy mezi Evropskou unií a Čínou[296]. Ukrajina a Arménie

[291] Inside Story, „*From Koukakis to Androulakis: A new twist in the Predator spyware case*“ (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).
[292] Inside Story, „*From Koukakis to Androulakis: A new twist in the Predator spyware case*“ (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).
[293] Inside Story, „*From Koukakis to Androulakis: A new twist in the Predator spyware case*“ (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).
[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*“ (Premiér Mitsotakis je pod tlakem, protože v souvislosti se špionážním skandálem skončili dva vysocí řečtí úředníci).
[296] https://www.kathimerini.gr/politics/561988786/ypothesi-parakoloythiseon-ta-dedomena-poy-pyrodotisan-tis-exelixeis/.

tato tvrzení odmítly[297].

187. Dne 15. prosince 2022 orgán na žádost novináře Tasose Tellogloua a poslance EP Giorgose Kyrtsose prověřoval, zda je EYP sledovala. Při auditu provedeném ADAE v telekomunikační společnosti Cosmote bylo zjištěno, že jak Telloglou, tak Kyrtsos byli skutečně sledováni[298]. Společnost Cosmote informovala Nejvyšší soud a zpochybnila zákonnost vyšetřování vedené úřadem ADAE[299]. ADAE zřídil zvláštní tým pro kontrolu poskytovatelů telekomunikačních služeb, který měl za úkol pátrat po dalších žádostech EYP o zásah do důvěrnosti[300].

188. Vláda se pokusila nahradit členy správní rady úřadu ADAE. Řecký nejvyšší státní zástupce Dogiakos oficiálně vydal stanovisko dne 10. ledna 2023, ve kterém rozhodl, že úřad ADAE nemůže procházet záznamy telekomunikačních poskytovatelů, aby v nich pátral po případech zásahů do důvěrnosti komunikace. Podle tohoto stanoviska by v případě, že úřad ADAE zahájí tyto audity, mohly být uplatněny trestní sankce[301]. Toto stanovisko, které je v rozporu s předchozími stanovisky nejvyššího státního zástupce, zjevně porušuje nezávislost úřadu ADAE[302] a snaží se mu bránit v provádění vyšetřování. Na zasedání výboru PEGA dne 28. února 2023 Rammos prohlásil, že stanovisko pana Dogiakose není závazné a úkoly ADAE mohou pokračovat jako obvykle[303].

189. Úřad ADAE potvrdil, že EYP sledovala také šéfa řeckých ozbrojených sil Konstantinose Florose, ministra ve funkci, několik důstojníků, kteří se zabývají případy zbraní, a bývalého poradce pro národní bezpečnost. Vzhledem k tomu, že úřad ADAE v současné době není schopen informovat cílové osoby, hodlal svá zjištění předložit výboru pro transparentnost řeckého parlamentu a jeho orgánům parlamentu[304]. Pan Christos Rammos zaslal řeckému parlamentu dopis s žádostí o tuto prezentaci. Předseda se zpočátku vyhýbal předložení této otázky k diskusi s tím, že si během svých jmenin nenašel čas na přečtení dopisu pana Rammose. Nakonec většina strany Néa Dimokratía ve Výboru pro instituce a transparentnost jeho žádost zamítla. Dne 24. ledna 2023 mluvčí vlády napadl úřad ADAE a jejího předsedu za vyšetřování[305], přičemž tvrdil, že pan Rammos provádí „aktivismus“ a „překračuje“ svůj mandát, což vyšetřování

---

[297] At a Glance, „*Greece's Predatorsgate: The latest chapter in Europe's spyware scandal?*“(Řecká Predatorgate: Nejnovější kapitola evropského skandálu se špionážním softwarem) Evropský parlament, Generální ředitelství pro parlamentní výzkumné služby, 8. září 2022.

[298] Euractiv, „*Exclusive: Another MEP and journalist the latest victims of "Greek Watergate"*“ (Exkluzivně: další poslanec EP a novinář nejnovějšími oběťmi řecké Watergate).

[299] International Press Institute, „*Greece*: *MFRR alarmed by latest revelations of spying on journalists*“ (Organizace MFRR je znepokojena nejnovějšími odhaleními o sledování novinářů).

[300] Euractiv, „*Exclusive: Another MEP and journalist the latest victims of "Greek Watergate"*“ (Exkluzivně: další poslanec EP a novinář nejnovějšími oběťmi řecké Watergate).

[301] Euractiv, „*Chief prosecutor puts Greece's rule of law to the test*“ (Vrchní státní zástupce podrobuje řecký právní stát zkoušce).

[302]http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bdilosi-toy-proedroy-tis-adae-christoy-rammoy-gia-tin-g/.

[303] Výměna názorů výboru PEGA s Konstantinosem Menoudakosem a Christosem Rammosem, 28. února 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/.

prováděnému ADAE neprospívá. Dne 25. ledna 2023 lídr strany SYRIZA Alexis Tsipras v řeckém parlamentu veřejně jmenoval osoby uvedené ve zprávě a potvrdil, že šéf ozbrojených sil, bývalý šéf řecké armády, ministr práce, bývalý poradce premiéra pro národní bezpečnost a dva poradci z ředitelství pro vybavení ozbrojených sil byli sledováni EYP. Vzhledem k závažnosti zjištění se odmítnutí umožnit úřadu ADAE podat zprávu řeckému parlamentu a diskreditace tohoto orgánu rovná bránění odpovědnosti a transparentnosti[306].

190. Kromě toho Rammos uvedl, že změny právního rámce ADAE vyvolaly nejistotu, což vedlo k výměně dopisů s ministerstvy s cílem vyjasnit operační rámec úřadu pro stížnosti a vyšetřování. Pan Rammos zmínil, že úřad ADAE obdrží přibližně 10 stížností denně[307].

VÝBOR PRO INSTITUCE A TRANSPARENTNOST

191. V červenci 2022 byli pan Kontoleon a ředitel úřadu ADAE Christos Rammos předvolání ke slyšení v parlamentním Výboru pro instituce a transparentnost. Během slyšení pan Kontoleon připustil, že Thanasis Koukakis byl sledován řeckou tajnou službou sledován z důvodů národní bezpečnosti, avšak tvrdil, že o pokusu o napadení telefonu pana Androulakise softwarem Predator nevěděl. Mluvčí vlády Giannis Oikonomou prohlásil, že řecké orgány software Predator nezískaly, ani nepoužívaly[308].

192. Ačkoli jsou schůze neveřejné[309], ani pan Kontoleon, ani pan Dimitriadis nebyli ochotni poskytnout podstatné důkazy, a to s odvoláním na důvody ochrany státního tajemství[310]. Nový šéf služby EYP Demiris odepřel výboru přístup ke zprávě obsahující informace o údajném zničení údajů o sledování[311]. To ve skutečnosti znamená, že EYP odmítá odpovědnost a řecký parlament nemůže vykonávat svůj mandát parlamentního dohledu.

193. Dne 30. srpna 2022 výbor předvolal devět osob na slyšení za zavřenými dveřmi, včetně státní zástupkyně Vasiliki Vlachouové, bývalého generálního tajemníka Grigorise Dimitriadise a bývalého šéfa EYP Kontoleona. Všichni se dovolávali důvěrnosti a během slyšení ve výboru se vyhýbali zodpovězení otázek[312].

PARLAMENTNÍ VYŠETŘOVACÍ VÝBOR

194. Návrh strany PASOK-KINAL na ustanovení vyšetřovacího výboru, který by prošetřil údajné použití špionážního softwaru[313], byl přijat 142 hlasy opozičních poslanců, zatímco 157 poslanců strany Néa Dimokratía se hlasování zdrželo[314]. Absolutní většinu ve vyšetřovacím výboru však měla nakonec právě Néa Dimokratía. Návrhy, aby v

---

[306]Newsbomb, „*SYRIZA: Maximos circles" through ADAE – What he sees behind the "blockade" of ND in Rammos*" (SYRIZA: „Maximos krouží" skrz ADAE – Co vidí za „blokádou" ND v panu Rammosovi).
[307]Výměna názorů výboru PEGA s Konstantinosem Menoudakosem a Christosem Rammosem, 28. února 2023.
[308] Reuters. *Greek intelligence service admits spying on journalist – sources* (Řecká zpravodajská služba přiznala špehování novináře – zdroje).
[309] Ekathimerini, „Výbor pro transparentnost se sejde za zavřenými dveřmi kvůli obvinění z hackerství".
[310] Tovima, „V bojových pozicích pro odposlech".
[311] Tovima, „V bojových pozicích pro odposlech".
[312] Ieidiseis, SYRIZA – PASOK zjištění o odposleších: Skandál i zástěrka", https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi.
[313] Tovima. Odposlechy: Vyšetřovací výbor ke sledování Androulakise – podrobný návrh strany Pasok.
[314] Tovima. *Parlament: Vyšetřování sledování v roce 2016 bylo schváleno 142 hlasy.*

předsednictvu nebyla zastoupena jen jedna strana, byly zamítnuty. Néa Dimokratía rozhodovala o pracovním programu i seznamu svědků, kteří mají být předvoláni, a odmítla několik svědků, které chtěla předvolat opozice. Výbor byl zřízen dne 29. srpna 2022 a svou činnost vykonával od 7. září 2022 do 10. října 2022.

195. Poslanci vládní strany, kteří měli ve výboru většinu, rozhodli o tom, že pánové Bitzios ani Lavranos předvolání nebudou. Zato však předvolali stávajícího manažera společnosti Krikel Stamatise Tribalise a Sarah Hamouovou. Tribalis před parlamentním výborem vypovídal dne 22. září. Pan Tribalis předložil zjevně nepravdivé informace o zapojení pánů Bitziose a Lavranose do společnosti Krikel a mimo jiné tvrdil, že je majitelem společnosti Krikel[315].

196. Další svědkyně, Sarah Hamouová ze společnosti Intellexa, tvrdila, že se nemůže dostavit osobně (ačkoli žije na Kypru), a tak ji bylo umožněno, aby na dotazy odpověděla písemně. Kvůli silné polarizaci politické scény nebylo možné dospět ke společným závěrům. Vládní většina rozhodla o utajení přibližně 5 500 stran dokumentů, včetně protokolů a výpovědi paní Hamouové a hlavních zjištění stran, ačkoli je zcela v pravomoci Parlamentu tyto informace odtajnit a zpřístupnit. Proto nebylo vypracováno žádné veřejné shrnutí. Veřejná byla pouze závěrečná rozprava na plénu řeckého parlamentu a závěry PASOKu i SYRIZY zveřejnily samy strany.

197. Opozice navrhla další svědky, například pány Koukakise, Mitsotakise, Dimitriadise, paní Vlachouovou, pány Lavranose a Bitziose, ale výbor je nakonec odmítl pozvat. Dne 10. října 2022 výbor dokončil svá šetření a jednotlivé politické strany předložily své závěrečné zprávy[316].

ŘECKÝ ÚŘAD PRO OCHRANU ÚDAJŮ.

198. Řecký úřad pro ochranu osobních údajů (HDPA) je nezávislý orgán, jehož úkolem je dohlížet na uplatňování obecného nařízení o ochraně osobních údajů[317] (GDPR), dalších nařízení a vnitrostátních zákonů týkajících se ochrany osobních údajů v Řecku[318]. Zákon 4624/2019 vyjmul národní bezpečnost z působnosti úřadu HDPA, zatímco od zákona z roku 1997 do něj spadala[319]. Po stížnosti, kterou v červenci 2022 předložil Nikos Androulakis, zahájil úřad šetření týkající se instalace špionážního softwaru na mobilních telefonech a následného shromažďování a zpracování osobních údajů. Úřad provedl audit v kanceláři společnosti Intellexa v Chalandri a v závodě společnosti Intellexa v Elliniko. Společnost Intellexa však neposkytla klíčové informace a odpověděla na dotazník se značným zpožděním, což úřadu bránilo v provádění auditu[320].

199. Dne 16. ledna 2023 uložil úřad HDPA společnosti Intellexa S.A. pokutu ve výši 50 000 EUR[321] za obstrukce a neochotu spolupracovat během auditu na základě článku

---

[315] TVXS. *G. Lavranos v pozadí KRIKEL – Jak se pokoušeli oklamat Parlament*.
[316] Ieidiseis. *Zjištění SYRIZA-PASOK o odposleších: Skandál i zástěrka*.
[317] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Úř. věst. L 119, 4.5.2016, s. 1).
[318] Řecký úřad pro ochranu údajů. *Osobní údaje*.
[319] Vládní věstník Řecké republiky.
[320] Řecký úřad pro ochranu údajů. Uložení pokuty společnosti Intellexa S.A. za nespolupráci s HDPA.
[321] Řecký úřad pro ochranu údajů. Uložení pokuty společnosti Intellexa S.A. za nespolupráci s HDPA.

31 nařízení GDPR.

200. V návaznosti na opatření přijatá úřadem HDPA společnost Intellexa předala dokumenty, ale úřad je stále prověřuje. Podle předsedy HDPA pana Menoudakose úřad objevil doménová jména, která pravděpodobně patří společnostem spolupracujícím se společností Intellexa v rámci EU i mimo ni. Úřad HDPA stále pokračuje ve vyšetřování[322].

201. Během zasedání výboru PEGA dne 28. února 2023 se předseda úřadu HDPA zmínil, že se šetření HDPA zabývalo internetovými aplikacemi pro zasílání textových zpráv. Podle pana Menoudakose společnosti využívaly tyto internetové aplikace k doručování textových zpráv souvisejících se špionážním softwarem Predator. HDPA se v současné době snaží identifikovat cíle, ale zatím potvrdila, že touto metodou bylo odesláno 300 textových zpráv přibližně 100 příjemcům. Úřad HDPA nařídil společnostem, aby tyto údaje uchovávaly, a zdůraznil, že pokud tyto společnosti nemají v EU právního zástupce, porušují GDPR[323].

CÍLE SLEDOVÁNÍ

THANASIS KOUKAKIS

202. V létě 2020 novináře Thanasise Koukakise odposlouchávala řecká tajná služba. V té době pracoval na reportážích s finanční tematikou, mimo jiné o skandálu Piraeus/Libra, do něhož byl zapleten Felix Bitzios, údajných daňových únicích řeckého podnikatele Yiannise Lavranose a kontroverzních zákonech o bankovnictví, které přijala řecká vláda a které ztěžovaly stíhání finančních deliktů jako praní peněz (zpětný účinek vedl k zastavení dvanácti trestních stíhání)[324]. Pan Koukakis se rovněž zabýval zakázkou na výrobu nových průkazů totožnosti, o niž měli zájem pánové Lavranos a Bitzios. Přibližně v době, kdy pan Koukakis poprvé předstoupil před výbor PEGA, byl tendr najednou zrušen a generální tajemník, který za věc odpovídal, odstoupil z funkce.

203. Dne 29. července 2022 prohlásil ředitel EYP Panagiotis Kontoleon prohlásil, že EYP odposlouchává telefon pana Koukakise s ohledem na důvody „národní bezpečnosti“.

204. Dne 1. června 2020 předložila EYP první žádost o zásah do důvěrnosti komunikace probíhající na telefonním čísle pana Koukakise na dva měsíce, tedy do 1. srpna 2020. EYP předložila žádost o prodloužení o další dva měsíce[325], tj. do 1. října 2020. Státní zástupkyně odvolacího soudu – Vasiliki Vlachouová – schválila všechna tato ustanovení z důvodu ochrany národní bezpečnosti[326].

205. O dvanáct dní později, 12. srpna 2020, však EYP náhle požádala o ukončení zrušení utajení telefonního čísla pana Koukakise, tedy o měsíc a půl dříve, než se předpokládalo v původní žádosti. Stalo se tak ve stejný den, kdy se pan Koukakis obrátil na úřad

[322] Výměna názorů výboru PEGA s Konstantinosem Menoudakosem a Christosem Rammosem. 28.2.2023.
[323] Výměna názorů výboru PEGA s Konstantinosem Menoudakosem a Christosem Rammosem. 28.2.2023.
[324] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis*? (Kdo sledoval mobilní telefon novináře Thanasise Koukakise?).
[325] Reporters United. *Nepřítel státu: Dokazujeme, že Mitsotakisova vláda sledovala novináře Thanasise Koukakise*.
[326] Reporters United. *Nepřítel státu: Dokazujeme, že Mitsotakisova vláda sledovala novináře Thanasise Koukakise*; Inside Story. *Kdo sledoval mobilní telefon novináře Thanasise Koukakise?*.

ADAE s žádostí, aby byl informován o možném sledování svých dvou mobilních telefonů a pevné linky.

206. Dne 10. března 2021 úřad ADAE informoval státního zástupce při EYP o možnosti informovat pana Koukakise o sledování jeho mobilního telefonu. Dne 31. března však řecká vláda schválila novelu č. 826/145, který zbavuje úřad ADAE možnosti informovat občany o zrušení důvěrnosti sdělení se zpětnou platností[327]. Předseda úřadu ADAE Christos Rammos a další dva členové úřadu ADAE se proti této novele ohradili a ve vydavatelské poznámce poukázali na to, že novela porušuje právo na respektování soukromého a rodinného života zakotvené v Evropské úmluvě o lidských právech (EÚLP) a ochranu důvěrnosti komunikace zaručenou ústavou[328].

207. V období od 12. července 2021 do 14. září 2021 byl telefon pana Koukakise napaden spywarem Predator[329]. Pan Koukakis obdržel dle svého tvrzení textovou zprávu s odkazem na webovou stránku s finančními informacemi[330]. Dne 28. března 2022 organizace Citizen Lab napadení oficiálně odhalila[331].

208. Pan Koukakis se několikrát pokusil dosáhnout nápravy v souvislosti s těmito pokusy o sledování. Podal dvě stížnosti u úřadu ADAE. První dne 6. dubna 2022, kdy požádal o důkladné prošetření napadení svého mobilního telefonu softwarem Predator; druhou dne 13. května 2022, a to v souvislosti s novými odhaleními, která zveřejnily organizace InsideStory a Reporters United. Kromě toho pan Koukakis podal 4. května 2022 stížnost k úřadu EAD, v níž požádal o prošetření pozadí odposlechů ze strany EYP a útoku programu Predator[332].

209. Vyšetřování Národního úřadu pro transparentnost (EAD), které proběhlo 21. července 2022 v aténských kancelářích společnosti Intellexa, dodavatele špionážního softwaru Predator, bylo omezené a povrchní, přestože mohly být zjištěny zásadní informace o útocích programu Predator, což je trestný čin. Nebyly zabaveny a zajištěny žádné servery, IT hardware ani správa. Ověřování finanční správy bylo omezeno na rok 2020[333]. Kyperské a irské dceřiné společnosti Intellexa nebyly vyšetřovány vůbec[334]. Šetření nezahrnovalo informace o bankovních účtech společnosti Intellexa a jejích dceřiných společností[335]. Pan Koukakis se 27. července 2022 obrátil na Evropský soud

---

[327] Reporters United. *Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis*“ (Nepřítel státu: Dokazujeme, že Mitsotakisova vláda sledovala novináře Thanasise Koukakise). https://www.reportersunited.gr/8646/eyp-koukakis/ Inside Story. Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis*? (Kdo sledoval mobilní telefon novináře Thanasise Koukakise?).
[328] Constitutionalism. Rozpor článku 87 zákona č. 4790/2021 se zárukami EÚLP na ochranu důvěrnosti sdělení: 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*? (Kdo sledoval mobilní telefon novináře Thanasise Koukakise?).
[330] Evropský parlament. Slyšení 8. září 2022.
[331] Inside Story. *Who was tracking journalist Thanasis Koukakis' cell phone?* (Kdo sledoval mobilní telefon novináře Thanasise Koukakise?).
[332] Avgi. *Thanasis Koukakis / Podal žalobu za software Predator – Kdo a proč ho sledoval*.
[333] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case"* (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).
[334] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case"* (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).
[335] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case"* (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).

pro lidská práva[336].

210. Dne 5. října 2022 podal pan Koukakis u aténského státního zastupitelství stížnost na společnost Intellexa Alliance, zejména na Tala Diliana a Saru Hamouovou[337] za porušení důvěrnosti jeho komunikace[338].

NIKOS ANDROULAKIS

211. Dne 21. září 2021 se předseda středolevé strany PASOK-KINAL a poslanec Evropského parlamentu Nikos Androulakis stal obětí hackerského útoku, kdy byl do jeho telefonu prostřednictvím podvodného odkazu nainstalován špionážní software Predator[339]. Androulakis obdržel textovou zprávu, v níž stálo: „Začni to brát vážně, máme toho na tebe dost.“ Zpráva kromě toho obsahovala odkaz. Zpráva kromě toho obsahovala odkaz. Po kliknutí na něj by se na jeho telefon nainstaloval špionážní software Predator, ale pan Androulakis na rozdíl od pana Koukakise takto neučinil[340]. Na zasedání výboru PEGA dne 28. února 2023 pan Androulakis uvedl, že HDPA identifikovala účet kreditní karty, z něhož byly zaplaceny textové zprávy, které mu byly zaslány. Tyto informace byly sděleny příslušnému státnímu zástupci[341].

212. V září 2021 pan Androulakis oznámil svou kandidaturu v boji o post předsedy strany[342]. Podle šetření úřadu ADAE byl v té době mobilní telefon pana Androulakise monitorován službou EYP prostřednictvím telekomunikačních operátorů[343]. Státní zástupkyně při EYP Vasiliki Vlachouová schválila zrušení utajení telefonu pana Androulakise z důvodu „národní bezpečnosti“. Schválení se časově shodovalo se zacílením softwarem Predator i s Androulakisovou kandidaturou.

213. Když byl pan Androulakis v prosinci 2021 zvolen do čela strany, „oficiální“ sledování ze strany EYP bylo náhle ukončeno[344] navzdory skutečnosti, že dvouměsíční povolení k jeho sledování ještě nevypršelo.

214. Dne 28. června 2022 GŘ ITEC Evropského parlamentu zkontrolovalo telefon pana Androulakise a našlo důkazy o pokusu o hackerský útok programu Predator ze září 2021 a pana Androulakise o tom informovalo[345]. Pan Androulakis podal 26. července 2022 trestní oznámení státnímu zastupitelství Nejvyššího soudu[346].

---

[336] BBC. *Greece wiretap and spyware claims circle around PM Mitsotakis. (Tvrzení o odposleších a špionáži v Řecku se točí kolem premiéra Mitsotakise).*
[337] News 24 7. Případ odposlechů: Žaloba na společnost Intellexa podaná Thanasisem Koukakisem.
[338] Heinrich Boll Stiftung. *A State of Absolute Solitude*(Stav absolutní samoty).
[339] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*. (Od Koukakise k Androulakisovi: Nový zvrat v případu špionážního softwaru Predator).
[340] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader* (Evropská komise je znepokojena novým případem špionážního softwaru proti řeckému socialistickému vůdci).
[341] Výměna názorů výboru PEGA s Konstantinosem Menoudakosem a Christosem Rammosem. 28.2.2023.
[342] Tovima. Androulakis se obořil na premiéra, podle mluvčího ND by měl předseda Pasoku říci, proč byl jeho telefon odposloucháván.
[343] Kathimerini. *Případ odposlechů: Telefonní data, která spustila další vývoj*.
[344] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader* (Evropská komise je znepokojena novým případem špionážního softwaru proti řeckému socialistickému vůdci).
[345] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader* (Evropská komise je znepokojena novým případem špionážního softwaru proti řeckému socialistickému vůdci).
[346] News 247. Nikos Androulakis: Téměř oběť softwaru Predator – podal žalobu.

215. O několik dní později, 29. července, předložil pan Androulakis úřadu ADAE informace o napadení softwarem Predator. Stálý výbor pro instituce a transparentnost vyslechl ve stejný den šéfa EYP Panagiotise Kontoleona a Christose Rammose, předsedu ADAE, za přítomnosti ministrů pro digitální správu a stát. Schůzka se konala za zavřenými dveřmi[347].

216. Dne 8. září 2022 požádal pan Androulakis úřad ADAE o předání svých odposlechových spisů[348]. Téhož dne však deník Ta Nea informoval o oficiální zprávě ADAE, v níž se uvádí, že EYP zničila spisy pana Androulakise i pana Koukakise[349]. Zničení je jednoznačným faktem, avšak příběh, který za ním stojí, zůstává nejasný. Na jedné straně některé zdroje viní ze zničení spisů změnu elektronických systémů EYP v roce 2021[350]. Tato změna v novém systému zákonného shromažďování údajně způsobila technický problém, který vedl ke zničení. Na druhou stranu jiné zdroje tvrdí, že pan Kontoleon vydal příkaz ke zničení dne 29. července 2022, tedy ve stejný den, kdy pan Androulakis informoval úřad ADAE o pokusech o sledování[351]. Během slyšení ve výboru PEGA předseda ADAE, pan Rammos, zničení záznamů ani nepotvrdil, ani nevyvrátil[352].

217. Dne 5. srpna pánové Kontoleon a Dimitriadis odstoupili ze svých funkcí. Dne 8. srpna pan Mitsotakis v televizním prohlášení přiznal, že pan Androulakis byl odposloucháván, ale zopakoval, že o sledování nevěděl[353].

218. EYP dosud odmítala sdělit důvody sledování. Nabídla panu Androulakisovi, že ho o důvodech bude informovat soukromě. To by bylo nezákonné. Pan Androulakis požádal o předložení svého sledovacího spisu Výboru pro instituce a transparentnost, ale tato žádost byla zamítnuta.

219. Dne 7. prosince 2022 podal pan Androulakis stížnost k Evropskému soudu pro lidská práva kvůli jeho odposlechům službou EYP a nedostatku oficiálních informací o jeho případu[354].

220. Sledování politiků je velmi neobvyklé a řecká ústava obsahuje zvláštní ustanovení na jejich ochranu. EYP popírá, že by se na sledování prostřednictvím Predatoru jakkoli podílela. Vláda na začátku přišla s teorií, že o odposlech pana Androulakise mohly požádat nějaké zahraniční subjekty nebo že důvodem sledování mohlo být jeho členství ve výboru EP, který se zabývá vztahy s Čínou. Žádná z těchto hypotéz se však nepotvrdila. K sledování došlo v politickém kontextu blížících se voleb. Strana PASOK by byla přijatelným koaličním partnerem. Na podzim 2021 se o post předsedy této strany ucházeli čtyři kandidáti, každý z nich měla na případnou koalici jiný názor. O panu Androulakisovi se říkalo, že by proti koalici nic neměl, ale premiérem by nesměl být pan Mitsotakis. Další kandidát, Andreas Loverdos, už dříve zastával post ministra v koaliční vládě stran Néa Dimokratía a PASOK a předpokládalo se tedy, že by myšlence

[347] Avgi. *Skandál Predator / EYP předvedena před Parlament kvůli sledování.*
[348] Ekathimerini. Androulakis požádá ADAE o spis s odposlechy.
[349] TaNea. *Archiv sledování Nikose Androulakise zničen.*
[350] TVXS. *G. Lavranos v pozadí KRIKEL – Jak se pokoušeli oklamat Parlament.*
[351] Ieidiseis. *Zjištění SYRIZA-PASOK o odposleších: Skandál i zástěrka.*
[352] Evropský parlament. Slyšení ze dne 8. září 2022.
[353] Reuters. *Greek PM says he was unaware of phone tapping of opposition party leader (Řecký premiér tvrdí, že o odposlechu telefonu předsedy opoziční strany nevěděl).*
[354] Ekathimerini. *Předseda socialistů se kvůli odposlechům obrátil na Evropský soudní dvůr.*

koalice byl více nakloněn. Představili jej panu Dimitriadisovi. Seznam dalších údajných obětí sledování zveřejněný listem Documento jen potvrzuje podezření, že sledování mělo politický motiv. Pro žádnou z uvedených hypotéz neexistují důkazy, ale podstatné je, že se tyto možnosti prověřují a případně vylučují.

GIORGOS KYRTSOS

221. Dne 15. prosince 2022 audit úřadu ADAE v telekomunikační společnosti Cosmote potvrdil, že poslanec Evropského parlamentu Giorgos Kyrtsos byl sledován EYP[355]. Jeho mobilní telefony i pevná linka byly odposlouchávány. Sledování bylo údajně devětkrát prodlužováno[356] po dobu 18 měsíců.

222. Giorgios Kyrtsos je bývalým členem strany Néa Dimokratía a Evropské lidové strany. V únoru 2022 vyloučila Néa Dimokratía pana Kyrtsose z řecké vládní strany kvůli jeho nesouhlasu s postupem vlády v souvislosti s pandemií COVID-19, omezováním svobody médií a přístupem ke skandálu Novartis[357]. Pan Kyrtsos se po svém vyloučení připojil ke skupině Renew Europe.

STAVROS MALICHUDIS

223. Dne 13. listopadu 2021 řecký deník EFSYN informoval o tom, že EYP údajně odposlouchávala telefony několika novinářů, kteří psali o uprchlické krizi. Z interního dokumentu EYP vyplývá, že nařídila sledovat řeckého novináře Stavrose Malichudise a shromažďovat o něm údaje[358][359]. Pan Malichudis je autorem článku o dvanáctiletém syrském chlapci, který byl nucen několik měsíců pobývat v detenčním táboře na ostrově Kos[360].

224. Dne 15. listopadu 2021 vládní mluvčí Giannis Oikonomou tato tvrzení nepřímo potvrdil. Uvedl, že EYP může odposlouchávat jednotlivce, pokud existuje riziko pro národní bezpečnost v důsledku „vnitřních nebo vnějších hrozeb“[361]. Státní ministr George Gerapetritis však 24. listopadu a 17. prosince 2021 popřel jakékoli sledování novinářů v Řecku, včetně sledování pana Malichudise, ale podle média Solomon pravost interních dokumentů EYP ani nepotvrdil, ani nevyvrátil[362].

225. Během slyšení výboru PEGA k Řecku dne 8. září 2022 pan Malichudis uvedl, že díky odposlechu jeho telefonu mohla EYP shromažďovat také informace od kolegů a novinářů, s nimiž byl v té době v kontaktu[363]. EYP mohla údajně odposlouchávat

---

[355] Euractiv. *Another MEP and journalist the latest victims of "Greek Watergate"* (Další poslanec EP a novinář nejnovějšími oběťmi řecké Watergate).
[356] Politico. *Řecký státní zástupce odmítá nelichotivá srovnání s belgickým vyšetřováním kauzy Qatargate.*
[357] Euractiv. *Renew Europe welcomes first Greek MEP who left EPP (Renew Europe vítá prvního řeckého europoslance, který opustil EPP).*
[358] Efsyn. *Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ.*
[359] Solomon. *Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'*(Reportér Solomonu Stavros Malichudis je pod dohledem z důvodu „národní bezpečnosti“).
[360] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.* (Řecká zpravodajská služba obviněna ze „znepokojivé“ sledovací činnosti).
[361] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.* (Řecká zpravodajská služba obviněna ze „znepokojivé“ sledovací činnosti).
[362] Solomon, Solomon's reporter Malichudis under surveillance for national security reasons.
[363] Evropský parlament. Slyšení ze dne 8. září 2022.

rozhovory pana Malichudise s Mezinárodní organizací pro migraci (IOM)[364], přičemž poukázal na nebezpečí, které odposlouchávání jednotlivce představuje pro ostatní, tzv. „vedlejší odposlechy“. Kromě toho Malichudis během slyšení poskytl důkazy o tom, že se EYP zajímala o jeho práci a zdroje, ale tvrdil, že důvod sledování je kryt „národní bezpečností“[365].

CHRISTOS SPIRTZIS

226. Dne 9. září 2022 prohlásil bývalý ministr infrastruktury a poslanec za stranu Syriza Christos Spirtzis, že se jeho mobilní telefon stal terčem špionážního softwaru Predator[366]. Pan Spirtzis předložil dne 15. listopadu 2021 vládě kritické parlamentní otázky týkající se úkolů EYP v oblasti sledování. Téhož dne obdržel podobnou zprávu[367] jako Nikos Androulakis. Dne 19. listopadu byla Christosi Spirtzisovi zaslána druhá zpráva, která obsahovala odkaz na článek serveru Efimerida ton Syntakton[368]. Ačkoli organizace Citizen Lab tyto zprávy neověřila, pan Spirtzis se o obdržené odkazy podělil se dvěma techniky, kteří ústně potvrdili, že se stal terčem[369]. Dne 9. září 2022 podal Spirtzis stížnost státnímu zástupci Nejvyššího soudu[370]. Spirtzis je důvěrníkem předsedy strany Tsiprase a účastní se schůzek vedení strany na vysoké úrovni.

TASOS TELLOGLOU, ELIZA TRIANTAFILLOUOVÁ A THODORIS CHONDROGIANNOS

227. Novináři Tasos Telloglou a Eliza Triantafillouová byli údajně sledováni během své práce pro nový magazín Inside Story. V článku pro nadaci Heinrich-Böll-Stiftung z 24. října 2022 se Telloglou podělil o své zkušenosti se sledováním a zastrašováním při vyšetřování skandálů se sledováním v Řecku. Podle této výpovědi je přesvědčen, že byl sledován v období od května do srpna 2022[371].

228. Kromě toho Tellogloua zdroj z bezpečnostních služeb v červnu 2022 informoval, že jeho poloha a poloha jeho kolegů Elizy Triantafillouové (InsideStory) a Thodorise Chondrogiannose (Reporters United) je sledována úřady, aby zjistily, s jakými zdroji se setkávají[372]. V době psaní tohoto textu řecká vláda na tato obvinění ještě nereagovala.

229. Dne 15. prosince 2022 audit úřadu ADAE v telekomunikační společnosti Cosmote potvrdil, že Telloglou byl sledován EYP. Důvody sledování nebyly kvůli „národní

---

[364] BalkanInsight. *Greek Intelligence Service Accused of ‘Alarming’ Surveillance Activity. (Řecká zpravodajská služba obviněna ze „znepokojivé“ sledovací činnosti).*
[365] Evropský parlament. Slyšení ze dne 8. září 2022.
[366] Ekathimerini. Bývalý ministr SYRIZY tvrdí, že se stal terčem softwaru Predator.
[367] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware* (Pokus o hacknutí opozičního poslance Christose Spirtzise pomocí nelegálního spywaru Predator).
[368] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware* (Pokus o hacknutí opozičního poslance Christose Spirtzise pomocí nelegálního spywaru Predator).
[369] Inside story, *Predator:Více než 20 cílů v Řecku, uvádí Úřad pro ochranu osobních údajů.*
[370] Reuters. *One more Greek lawmaker files complaint over attempted phone hacking (Další řecký zákonodárce podal stížnost kvůli pokusu o hackerské útoky na telefon); Euractiv. Another Greek opposition lawmaker victim of Predator (Další řecký opoziční zákonodárce terčem softwaru Predator).*
[371] Heinrich-Böll-Stiftung. *A State of Absolute Solitude*(Stav absolutní samoty).
[372] MapMF, *Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations.* (Tři řečtí novináři byli údajně sledováni a monitorováni v souvislosti s vyšetřováním skandálu se špionážním softwarem).

bezpečnosti“ zveřejněny[373].

DALŠÍ SLEDOVANÉ OSOBY

230. Dne 29. října 2022 vyšel článek o sledování dalších politiků pomocí špionážního softwaru Predator, mimo jiné jednoho ministra, který nemá dobré vztahy s předsedou vlády. Kromě toho obdržel ještě jeden člen strany Néa Dimokratía odkaz k instalaci softwaru Predator[374]. Mluvčí vlády pan Oikonomou však uvedl, že článek není podložen žádnými konkrétními důkazy[375].

231. Dne 5. a 6. listopadu 2022 noviny Documento zveřejnily seznam 33 osob sledovaných pomocí špionážního softwaru Predator[376]. Seznam uváděl i jména mnoha vysoce postavených politiků včetně členů současné vlády, bývalého premiéra Samarase, bývalého člena Evropské komise Avramopoulose, šéfredaktora jednoho provládního deníku a osob kolem Vangelise Marinakise, rejdaře, mediálního magnáta a majitele fotbalových klubů Olympiakos a Nottingham Forest. Úřad ADAE potvrdil, že některá jména na seznamu EYP monitorovala prostřednictvím běžných odposlechů. Mezi tato jména patří poslanec Evropského parlamentu Giorgos Kyrtsos[377], náčelník spojených štábů generál Konstantinos Floros[378], velitel řecké armády Haralambos Lalousis[379], ministr práce a sociálních věcí Kostis Hatzidakis[380], bývalí generální ředitelé pro obranné vybavení a investice Theodoros Lagios a Aristides Alexopoulos[381], bývalý bezpečnostní poradce Alexandros Diakopoulos[382] a řecký investigativní novinář Tasos Telloglou[383].

232. Kromě toho se na seznamu 33 jmen objevila také bývalá manažerka společnosti Meta pro politiku kybernetické bezpečnosti Artemis Seafordová, u níž bylo potvrzeno, že byla současně odposlouchávána EYP a sledována pomocí softwaru Predator. Seafordová byla odposlouchávána EYP od července 2021 do léta 2022, což znamená, že povolení k odposlechu zařízení paní Seafordové bylo šestkrát prodlouženo, což v zásadě vyžaduje souhlas interního státní zástupkyně EYP Vasiliki Vlachouové. Organizace Citizen Lab potvrdila, že i její mobilní telefon byl od září 2021 nejméně dva měsíce infikován programem Predator. K nákaze softwarem Predator tedy došlo přibližně jeden až dva měsíce po zahájení běžného odposlechu. Paní Seafordová uvedla, že informace o jejím očkování vakcínou COVID-19 byly získány z jejích textových

---

[373] Euractiv „*Another MEP and journalist the latest victims of ‘Greek Watergate’*“ (Další poslanec EP a novinář nejnovějšími oběťmi řecké Watergate).
[374] Ta Nea, *Čtyři nezákonné manipulace ze strany podezřelého centra.*
[375] Politico, *Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.* (Bruselská příručka: Lula vítězí v Brazílii – Podvod nebo obchod – Potíže s obchodem s obilím)-
[376] Documento, 6. listopadu 2022.
[377] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*.
[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/*.

zpráv prostřednictvím běžného odposlechu. Tyto informace byly následně použity k vytvoření sofistikované automatické SMS zprávy, která používala stejnou osnovu jako oficiální schůzka, s žádostí o potvrzení schůzky prostřednictvím odkazu. Kliknutím na tento odkaz bylo zařízení infikováno spywarem Predator. SMS zprávy obsahovaly přesné a podrobné informace z jejího očkovacího spisu a byly odeslány jen několik minut po skutečných, oficiálních zprávách, což naznačuje, že ten, kdo zprávy odeslal, měl přístup k obsahu a načasování SMS zpráv, které by měla EYP k dispozici prostřednictvím běžného odposlechu.

233. Odposlouchávání a/nebo sledování soukromé osoby je neobvyklé, zejména pokud se v takovém případě nelze legitimně odvolávat na národní bezpečnost. Nabízí se otázka, jaké další motivy mohly hrát roli při výběru cíle. Ke sledování došlo v době, kdy paní Seafordová pracovala ve společnosti Meta, která zveřejnila zprávu o hrozbách v odvětví námezdního sledování a zakázala na své platformě přístup několika společnostem zabývajícím se spywarem, včetně společnosti Cytrox. Je však velmi nepravděpodobné, že by důvodem sledování byla její role ve společnosti Meta. Zpráva o hrozbách Meta byla zveřejněna až v prosinci 2021, tedy o několik měsíců později, než kdy došlo k napadení zařízení paní Seafordové, a nikdo z dalších lidí, kteří se na psaní zprávy podíleli, se sám nestal terčem útoku. Kromě toho paní Seafordová uvedla[384], že se na těchto aktivitách podílela pouze částečně a že společnost Meta je velmi diskrétní, pokud jde o sdělování jmen svých zaměstnanců.

234. V březnu 2021 vyšel v časopise Marie-Claire článek obsahující úryvek z knižní série napsané paní Seafordovou. Článek zmiňuje její zkušenosti s každodenním sexismem a obtěžováním v Řecku a popisuje zejména případ sexuálního obtěžování ze strany „jednoho politika“[385]. Sledování začalo o několik měsíců později. Jedním z vysvětlení může být, že dotyčný politik si článek přečetl a obával se, že by jeho jméno mohlo být zveřejněno. Dalším vysvětlením může být, že někdo jiný poznal politika podle popisu v článku a chtěl o něm z politických důvodů získat více informací. Ať už je to jakkoli, jen velmi málo osob by mělo pravomoc podat oficiální žádost o odposlech u EYP a zároveň zajistit použití špionážního softwaru Predator. Kombinace sledování pomocí EYP a spywaru Predator byla potvrzena i v dalších případech.

235. Je důležité, aby tyto možnosti byly dále prošetřeny, zejména otázka, kdo si vyžádal sledování ze strany EYP. Paní Seafordová podala žádost u ADAE a podala stížnost u soudu v Řecku. Vyšetřování však stále probíhá. Je první známou americkou občankou, která se stala terčem útoku v EU[386][387].

236. Dalšími jmény na seznamu, která nebyla oficiálně potvrzena, jsou bývalý ministr školství a náboženských záležitostí Andreas Loverdos, bývalý premiér Antonis Samaras, státní ministr George Gerapetritis, bývalý komisař Dimitris Avramopoulos, ministr Nikos Dendias, ministryně školství Niki Kerameusová, ministr Akis Skertsos, ministr investic Nikos Papathanasis, bývalý ministr pro ochranu občanů Mihalis

[384] Schůze výboru PEGA, 20. dubna 2023.
[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] Schůze výboru PEGA, 20. dubna 2023.

Chrysochoidis, Náměstek ministra obrany Řecké republiky Nikos Hardalias, Aristotelia Peloniová, poslanec Christos Spirtzis, bývalá ministryně ochrany občanů Olga Gerovasiliová, šéf řecké policie Michalis Karamalakis, vedoucí úřadu hospodářského prokurátora Christos Barkadis, interní prokurátorka EYP Eleni Vlachouová, mluvčí vlády Giannis Oikonomou, zástupce šéfa EYP Vassilis Grizis; tato odhalení na seznamu jsou nanejvýš znepokojivá nejen proto, že se jedná o známé osobnosti, ale i proto, že zneužívání špionážního softwaru je zřejmě systematické a rozsáhlé.

237. V roce 2023 úřad ADAE oznámil, že EYP také odposlouchávala ministra ve službě, několik důstojníků, kteří se zabývali případy zbraní, a bývalého poradce pro národní bezpečnost[388].

ZÁVĚREČNÉ POZNÁMKY

238. Existují vzorce, které naznačují, že řecká vláda umožňuje používání špionážního softwaru proti novinářům, politikům a podnikatelům. Umožňuje také vývoz špionážního softwaru do zemí se špatným stavem lidských práv a poskytuje školicí středisko pro agenty ze zemí mimo EU, kteří se chtějí o špionážním softwaru něco dozvědět. Ačkoli je používání špionážního softwaru v Řecku nezákonné, vyšetřování původu napadení tímto typem softwaru nabralo na intenzitě až v létě 2022. Politická většina je údajně využívána spíše k prosazování konkrétních než obecných zájmů, zejména jmenováním spolupracovníků a loajálních osob na klíčové pozice, jako například v EYP, EAD (Národní úřad pro transparentnost) a společnosti Krikel (společnost specializující se na elektronické bezpečnostní systémy). Nejvyšší politické vedení země používá špionážní software jako nástroj politické moci a kontroly, v některých případech souběžně nebo po legálním odposlechu. Řecko má v zásadě poměrně pevný právní rámec. Avšak v důsledku některých legislativních změn byly oslabeny klíčové záruky a k zajištění kontroly a odpovědnosti nepřispívají ani politická jmenování do klíčových funkcí. Dochází k záměrnému oslabování kontrolních mechanismů *ex ante* i *ex post*, nedodržují se zásady transparentnosti a odpovědnosti. Nepohodlní novináři nebo úředníci bojující proti korupci a podvodům jsou vystaveni zastrašování a obstrukcím. Systém záruk a dohledu nad sledováním je celkově nedostatečný pro ochranu občanů před zneužitím ze strany státních orgánů a soukromých subjektů. Pro řešení tohoto problému je třeba udělat více. Kromě toho je odposlouchávání osob odůvodňováno záminkou „národní bezpečnosti“.

239. Sledování osob za politickým účelem není v Řecku ničím novým, avšak díky novým špionážním technologiím je nelegitimní sledování daleko snazší, zejména jsou-li výrazně oslabeny související záruky. Na rozdíl od jiných zemí, například Polska, není zneužívání špionážního softwaru v Řecku podle všeho součástí celkové autoritářské strategie, ale spíše nástrojem používaným ad hoc k dosažení konkrétních politických a finančních cílů. Nicméně demokracii a právní stát narušuje i tak a ponechává velký prostor pro korupci, přestože tato neklidná doba vyžaduje spolehlivé a odpovědné vedení.

I.D. Kypr

240. Výbor navštívil Kypr v listopadu 2022 v rámci společné mise do Řecka a na Kypr. Členové se setkali s ministrem energetiky, obchodu a průmyslu, dalšími vládními

[388] Politico. *Brussels Playbook: Globalization’s sanatorium - Vestager rings alarm - S(upended & D(dumped).*

úředníky a členy Sněmovny reprezentantů zasedajícími v příslušných výborech, aby projednali současný právní rámec pro špionážní software. Vyslechli také právní experty, zástupce nevládních organizací a novináře, kteří výboru předložili dokumentaci o dohledu a korupci. Výbor zdůraznil, že by se mělo více pracovat na registrech skutečných vlastníků, které nejsou dostatečně transparentní, ačkoli jsou navrženy tak, aby tyto otázky osvětlovaly.

241. Na rozdíl od jiných členských států není o používání špionážního softwaru na Kypru mnoho informací. Neexistují žádné oficiálně potvrzené případy osob, které jsou nebo byly nelegálně napadeny špionážním softwarem. Kyperská vláda však v únoru 2018 údajně sledovala novináře Makariose Drousiotise pomocí odposlouchávacích technik i špionážního softwaru[389]. Vývoz tohoto zboží se zde teoreticky řídí přísnou právní úpravou, jejíž součástí jsou i právní předpisy EU, avšak v praxi je Kypr pro prodejce sledovacích technologií velmi atraktivní. Vláda to však popírá a poukazuje na pokles počtu registrovaných spywarových společností v zemi. Pověst Kypru utrpěla nedávnými skandály a nyní se očekává, že v roce 2023 bude dokončeno několik legislativních iniciativ, které mají právní úpravu vývozu zpřísnit a zlepšit její dodržování.

242. Kypr a Řecko jsou v oblasti špionážního softwaru úzce propojeny. Společnost Intellexa Tala Diliana je usazena v Řecku a její špionážní software Predator byl použit v řeckých hackerských skandálech. Obě země se také podílely na nelegálním vývozu špionážního softwaru Predator súdánským milicím Jednotky rychlé podpory (RSF)[390]. Řecko vydalo vývozní licenci, zatímco materiál byl do Súdánu odeslán z letiště v Larnace[391].

243. Kromě vývozu špionážního softwaru mimo EU Kypr rovněž usnadňuje obchod se subsystémy a technologiemi špionážního softwaru do členských států. Jméno společnosti UTX Technologies – registrované na Kypru a převzaté izraelským technologickým gigantem Verint – se objevilo na fakturách německých, francouzských a polských společností, které dodávaly technologie a monitorovací systémy Gi2[392].

244. Právní rámec formálně zaručuje ochranu soukromé komunikace a zpracovávaných osobních údajů a právo osob na informace. Neexistují však jasná pravidla pro regulaci odposlouchávacích zařízení a ochranu ústavních práv občanů, pokud se orgány odvolávají na ochranu ústavních práv občanů.

PRÁVNÍ RÁMEC

NAŘÍZENÍ O ZBOŽÍ DVOJÍHO UŽITÍ

245. Zdá se, že Kypr velmi úzce spolupracuje s Izraelem v oblasti sledovacích technologií. Kypr konzultoval s Izraelem a USA reformu svého právního rámce a systému kontroly vývozu zboží dvojího užití. Kypr je i oblíbenou destinací mnoha izraelských společností, které prodávají špionážní software.

246. Odbor ministerstva energetiky, obchodu a průmyslu pro udělování licencí na vývoz strategického materiálu reguluje vývoz zboží dvojího užití[393]. V odpovědi na dotazník

[389] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/.
[390] LightHouse Reports. *Flight of the Predator* (Únik predátora).
[391] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/.
[392] Philenews. *Cyprus is a pioneer in software exports* (Kypr je průkopníkem ve vývozu softwaru), dokumenty.
[393] http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument.

výboru PEGA, který byl zaslán všem členským státům, Kypr uvedl, že sleduje a posuzuje všechny žádosti o vývozní licence na zboží dvojího užití případ od případu v plném souladu s příslušnými sankčními režimy. Těmito režimy jsou globální režim sankcí Evropské unie v oblasti lidských práv a nařízení EU o dvojím použití, které se řídí kritérii příslušného společného postoje Rady (2008/944/SZBP)[394]. Výbor PEGA konstatuje, že Kypr není smluvní stranou Wassenaarského ujednání o kontrole vývozu konvenčních zbraní a zboží a technologií dvojího užití. Bylo konstatováno, že Turecko během mise výboru PEGA zablokovalo účast Kypru na ujednání. Vláda však prohlašuje, že dodržuje stejné normy.

247. Ministerstvo energetiky, obchodu a průmyslu může udělování vývozních licencí konzultovat s tzv. poradním výborem. Tento výbor se skládá mimo jiné ze zástupců ministerstva obrany, ministerstva spravedlnosti a veřejného pořádku, ministerstva zahraničních věcí, ministerstva cel a spotřebních daní[395]. Podle kyperské vlády je tento výbor pravidelně konzultován při posuzování žádostí o vývoz. V několika případech byl vývoz zboží dvojího užití do třetích zemí zamítnut na základě negativního stanoviska tohoto výboru[396]. Hospodářská komora obvykle neposkytuje informace o počtu schválených a zamítnutých licencí na uvádění softwaru na trh[397].

248. Během mise výboru PEGA na Kypr ve dnech 1. a 2. listopadu 2022 se účastníci mise setkali s ministerstvem energetiky, obchodu a průmyslu a náměstkem ministra pro výzkum, inovace a digitální politiku. Ministři Natasa Pilidesová a Kyriacos Kokkinos uvedli, že na Kypru došlo k prudkému poklesu počtu společností působících v oblasti špionážního softwaru. Bylo zaregistrováno 32 společností, ale podle ministra bylo v době návštěvy aktivních pouze 8 až 10, přičemž tři nebo čtyři vyráběly špionážní software[398]. Uznali však také technické problémy při dohledu a kontrole společností se sídlem na Kypru, které samostatně prodávají jednotlivé složky špionážního softwaru.

249. V praxi Kypr údajně přistupuje k vydávání vývozních licencí pro špionážní software spíše shovívavě[399]. Společnosti používají k obcházení pravidel různé technologie. Fyzický hardware produktu je odeslán do země příjemce bez nahraného softwaru[400]. Poté je aktivační software (označovaný také jako „licenční klíč“) zaslán samostatně na paměťovém zařízení USB do cílové země[401]. Jiným způsobem je uvést, že daný výrobek vyváží pouze pro předváděcí účely, ačkoli je k němu připojen podrobný popis[402]. Kromě toho jsou ve vývozním formuláři pro vývozní licence vyplněny nejasné popisy špionážního softwaru, což brání příslušným celním kontrolám.

250. Několik kyperských společností údajně získalo vývozní licence na prodej „zboží dvojího užití“ do zemí mimo EU. Jedná se o společnosti UTX Technologies, Coralco

---

394 Odpověď na dotazník Evropského parlamentu obdržený od Kypru.
395 Lelaw, „*Export Controls for dual-use products*“.(Vývozní kontroly pro zboží dvojího užití).
396 Odpověď Kypru na dotazník Evropského parlamentu.
397 Inside Story, „*Who signs the exports of spyware from Greece and Cyprus?*“ (Kdo podepisuje vývoz spywaru z Řecka a Kypru).
398 Setkání s Natasou Pilidesovou, ministryní energetiky, obchodu a průmyslu, a Kyriacosem Kokkinosem, náměstkem ministra pro výzkum, inovace a digitální politiku, během mise výboru PEGA 2. února 2022.
399 InsideStory, „Kdo podepisuje vývoz spywaru z Řecka a Kypru?“
400 InsideStory, ‘Kdo podepisuje vývoz spywaru z Řecka a Kypru?“.
401 Philenews, „Takto se z Kypru vyvážejí patenty na odposlechy“.
402 Philenews, „Vývoz monitorovacího softwaru potvrzen“.

Tech, Prelysis a Passitora[403].

251. Společnost UTX Technologies se podílela na prodeji špionážního softwaru členským státům EU i zemím mimo EU. V letech 2013 a 2014 byla společnost UTX uvedena na fakturách německým společnostem (Syborg Informationsysteme), francouzským společnostem (COFREXPORT) a polským společnostem (Verint), které se zabývají obchodem s monitorovacími systémy a technologií Gi2[404].

252. Kyperská obchodní agentura udělila dceřiné společnosti UTX Technologies dočasné vývozní licence na prodej sledovacího softwaru do Mexika, Spojených arabských emirátů, Nigérie, Izraele, Peru, Kolumbie, Brazílie a Jižní Koreje[405]. Společnost UTX Technologies údajně také uzavřela s Thajskem smlouvu na prodej sledovacích subsystémů za 3 miliony USD. V popisu tohoto subsystému se uvádí typ „dvojího užití“ s „algoritmem analýzy řeči“ a „metadaty a hlasem“. Dohoda rovněž obsahovala konkrétní odkaz na litevskou společnost. Vzhledem k tomu, že kyperské úřady by vývozní licenci nevydaly, bylo možné obejít ministerstvo energetiky, obchodu a průmyslu prostřednictvím litevské registrované společnosti UAB Communication Technologies[406]. Tuto společnost vlastní rusko-izraelský občan Anatolij Hurgin, který je navíc držitelem maltského pasu[407]. Kromě toho společnost UTX také v roce 2019 získala dohodu s Bangladéšem na webový zpravodajský systém za 2 miliony USD v a na buňkový sledovací systém za 500 000 USD v roce 2021[408].

253. Kyperská exportní historie také ukazuje, že společnost Coralco Tech – původem ze Singapuru, ale registrovaná také v Izraeli a Nikósii – dodala v roce 2018 po výběrovém řízení bangladéšské armádě monitorovací zařízení za 1,6 milionu USD. Majitelem společnosti Coralco Tech je Izraelec Eyal Almog[409].

254. V roce 2019 zakoupila bangladéšská vnitřní zpravodajská služba (NSI) od společnosti Prelysis, která je registrována na Kypru, software pro odposlech Wi-Fi za celkem 3 miliony USD. Kobi Naveh – zakladatel a ředitel společnosti Prelysis – pracoval do roku 2014 pro izraelskou společnost Verint. Společnost Verint je také společností, která získala na Kypru registrovanou společnost UTX Technologies[410].

255. V létě 2021 Bangladéš navíc koupil špionážní vozidlo od firmy Passitora Tala Diliana (dříve WiSpear). Švýcarská společnost Toru Group Limited, registrovaná na Britských Panenských ostrovech, sloužila jako zprostředkovatel dohod uzavřených s Dilianovou

[403] „*Cyprus is a pioneer in software exports*“ (Kypr je průkopníkem ve vývozu softwaru), dokumenty. Haaretz, „*Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record*“ (Izraelská špionážní technika prodána Bangladéši navzdory špatným výsledkům v oblasti lidských práv).
[404] „*Cyprus is a pioneer in software exports*“ (Kypr je průkopníkem ve vývozu softwaru), dokumenty.
[405] „*Cyprus is a pioneer in software exports*“ (Kypr je průkopníkem ve vývozu softwaru), dokumenty.
[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*“ (Izraelská špionážní technika prodána Bangladéši navzdory špatným výsledkům v oblasti lidských práv).
[409] Haaretz, „*Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record*“ (Izraelská špionážní technika prodána Bangladéši navzdory špatným výsledkům v oblasti lidských práv).
[410] Haaretz, „*Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record*“ (Izraelská špionážní technika prodána Bangladéši navzdory špatným výsledkům v oblasti lidských práv).

společností Passitora[411].

256. Dne 4. října 2022 bylo odhaleno, že v listopadu 2019 se nizozemské ministerstvo obrany chystalo podepsat dohodu se společností WiSpear, kterou vlastní Tal Dilian a kterou předtím zakoupila společnost Cytrox, výrobce špionážního softwaru Predator[412]. Podle zpráv v médiích a prohlášení předsedy strany DISY (Dimokratikós Sinagermós) poslala společnost WiSpeare-mail vládní straně DISY a ministerstvu energetiky, obchodu a průmyslu s žádostí o pomoc při provádění dohody s nizozemským ministerstvem obrany[413]. Zda byla smlouva podepsána a zda byl jakýkoli špionážní software nizozemskému ministerstvu obrany dodán, není jasné.

257. Tyto příklady ukazují, že na Kypru probíhá rozsáhlá činnost sledovacího průmyslu, do níž jsou zapojeni stejní aktéři, kteří se objevují ve skandálu se špionážním softwarem, který vyšetřuje výbor PEGA.

258. Mnoho izraelských společností přichází na Kypr proto, aby mohly začít působit na evropském trhu[414]. Navíc je podle různých zdrojů na Kypru registrováno asi 29 izraelských společností[415]. Některé zdroje poukazují na úzkou souvislost mezi obchodem se špionážním softwarem a diplomatickými vztahy. Za to, že mají na Kypru jednodušší přístup k licencím, izraelské společnosti údajně poskytují Kypru některé produkty, které vyvíjejí a vyvážejí, například špionážní software Pegasus společnosti NSO Group[416] a špionážní materiál firmy WiSpear[417]. Kypr slouží jako opěrný bod pro obchodování s izraelským špionážním softwarem na vnitřním trhu EU a pro vývoz špionážního softwaru do třetích zemí.

PŘEDBĚŽNÁ KONTROLA

259. Zákon 92(I)/1996 o ochraně důvěrného charakteru soukromé komunikace stanoví, že generální prokurátor může podat soudu žádost o vydání soudního příkazu, který povoluje nebo rozšiřuje odposlech soukromých komunikací oprávněnou osobou. Tato žádost generálního prokurátora k soudu vyžaduje písemnou žádost policejního ředitele, velitele kyperské zpravodajské služby nebo vyšetřujícího soudce. Ustanovení o povolení nebo schválení však mohou být zrušena v případech, kdy je odposlech soukromé komunikace v bezpečnostním zájmu Kypru nebo za účelem prevence, vyšetřování nebo stíhání trestných činů[418].

260. Po podání žádosti vydá policejní ředitel po dohodě se zástupcem policejního ředitele a velitelem kyperské zpravodajské služby písemné povolení zaměstnancům své služby nebo zaměstnancům, kteří plní úkoly pro svou službu, k odposlechu soukromé

[411] Haaretz, „*Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record*“ (Izraelská špionážní technika prodána Bangladéši navzdory špatným výsledkům v oblasti lidských práv).
[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/
[414] Philenews. *Revelations in Greece:Predator came from Cyprus.* (Odhalení v Řecku: Predator pochází z Kypru.
[415] Makarios Drousiotis. Κράτος Μαφία. Kapitola 6. Vydáno v roce 2022.
[416] Makarios Drousiotis. Κράτος Μαφία. Kapitola 6. Vydáno v roce 2022.
[417] Inside Story, „Predator: špion, který přišel z Kypru“.
[418] CyLaw, Zákon o ochraně soukromí soukromých komunikací (odposlech a přístup k obsahu zaznamenaných soukromých komunikací) z roku 1996 (92(I)/1996).

komunikace a/nebo k přístupu k monitorovacímu zařízení za účelem technické práce[419].

261. Kromě toho čl. 4 odst. 2 zákona 92(I)/1996 ve znění z roku 2020[420] stanoví, že pokud bylo zařízení nebo přístroj primárně navrženo, vyrobeno nebo upraveno tak, aby umožňovalo nebo usnadňovalo odposlech nebo sledování soukromé komunikace, nesmí nikdo takové zařízení nebo přístroj dovážet, vyrábět, propagovat, prodávat nebo jinak distribuovat. Porušení tohoto článku může vést až k pokutě 50 000 EUR a/nebo k trestu odnětí svobody až na 5 let[421]. Tato ustanovení se nepoužijí, pokud poskytovatel informoval Ústřední zpravodajskou službu (KYP), policii a komisaře a získal jejich souhlas. Tato ustanovení se nevztahují na sledovací systémy používané náčelníkem policie a velitelem KYP[422].

NÁSLEDNÁ KONTROLA

262. Na Kypru zákon o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů z roku 2018 stanoví, že pokud jsou osobní údaje používány nebo pokud byla fyzická osoba předmětem zpracování, má dotyčná osoba právo být informována[423]. Toto právo lze obejít, jakmile komisař pro ochranu osobních údajů rozhodne jinak, mimo jiné z důvodů národní bezpečnosti[424].

263. Zákon o ochraně důvěrnosti soukromé komunikace přijatý v roce 1996 navíc upřesňuje, že v případě odposlechu soukromé komunikace orgány činnými v trestním řízení je generální prokurátor povinen informovat dotyčnou osobu. Fyzická osoba musí být vyrozuměna nejpozději do 90 dnů od data zahájení soudního příkazu[425] nebo ve lhůtě nejvýše 30 dnů od provedení tohoto soudního příkazu. Generální prokurátor musí dotyčné osobě poskytnout zprávu s podrobnostmi o vydání soudního příkazu, datu vydání soudního příkazu a skutečnosti, že v tomto období došlo k odposlechu nebo přístupu k soukromým komunikacím. Tato povinnost může být dočasně odložena, pokud generální prokurátor rozhodne, že je neposkytnutí těchto informací mimo jiné v zájmu bezpečnosti Kypru[426]. Soud může rovněž nařídit nezveřejnění informací s ohledem na bezpečnostní zájmy Kypru[427].

264. Podle právních předpisů je porušení ochrany soukromé komunikace trestným činem. Nezákonné sledování se však často zastírá ochranou národní bezpečnosti[428]. Neexistuje žádný právní předpis, který by upravoval způsob, jakým policie nebo jiné zpravodajské

---

[419] CyLaw, Zákon o ochraně soukromí soukromých komunikací (odposlech a přístup k obsahu zaznamenaných soukromých komunikací) z roku 1996 (92(I)/1996).
[420] CyLaw. E.U. odst. J(J) ZÁKONA 13(J)/2020.
[421] Odpověď na dotazník Evropského parlamentu obdržený od Kypru.
[422] Odpověď na dotazník Evropského parlamentu obdržený od Kypru.
[423] Zákon 125(I) z roku 2018.
https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf.
[424] Agentura Evropské unie pro základní práva, Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii – díl II: aktuální přehled právní úpravy a pohled z praxe.
[425] CyLaw, Zákon o ochraně soukromí soukromých komunikací (odposlech a přístup k obsahu zaznamenaných soukromých komunikací) z roku 1996 (92(I)/1996).
[426] Agentura Evropské unie pro základní práva, Sledování zpravodajskými službami: záruky ochrany základních práv a prostředky nápravy v Evropské unii – díl II: aktuální přehled právní úpravy a pohled z praxe.
[427] CyLaw, Zákon o ochraně soukromí soukromých komunikací (odposlech a přístup k obsahu zaznamenaných soukromých komunikací) z roku 1996 (92(I)/1996).
[428] Makarios Drousiotis, „Κράτος Μαφία“, Kapitola 6, 2022.

služby používají odposlouchávací zařízení, kdo upravuje postupy odposlouchávání nebo jak je zaručena ochrana ústavních práv občanů. Příslušné právní předpisy a protokoly v současné době čekají na projednání a schválení v parlamentu. Prozatím tato činnost pokračuje bez kontroly[429].

ZJEDNÁNÍ NÁPRAVY

265. Zákonnost činnosti kyperské zpravodajské služby posuzuje tříčlenný výbor, jak je uvedeno v zákoně o kyperské zpravodajské službě 74(I)/2016. Tento tříčlenný výbor je jmenován Radou ministrů na doporučení prezidenta republiky[430].

266. Zákon 92(I)/1996 byl v roce 2020 novelizován a posílil rámec dohledu nad republikou, zejména ustanovení týkající se tříčlenného výboru. V rámci svého mandátu může výbor zahájit šetření z moci úřední a může zahájit vyšetřování zařízení, technického vybavení a archivních materiálů z KYP. Jak je uvedeno v čl. 17A odst. 1 zákona 92(I)/1996 ve znění zákona 13(I)/2020, může výbor rovněž zahájit vyšetřování zařízení, technického vybavení a archivních materiálů policie. Na základě těchto šetření může výbor věc postoupit generálnímu prokurátorovi, komisaři pro ochranu osobních údajů nebo komisaři pro elektronické komunikace a poštovní předpisy, aby přijali další opatření. Výbor rovněž předkládá prezidentu republiky výroční zprávu, v níž popisuje svou činnost, formuluje připomínky a doporučení a upozorňuje na opomenutí[431].

267. Kyperský prezident má značný vliv na složení výboru, který je oprávněn zahájit klíčová vyšetřování činnosti zpravodajské služby KYP. Prezident je také tím, kdo jako první dostává výroční zprávy se zjištěními výboru[432]. V době, kdy zpráva vznikala, nebyly k dispozici žádné informace o přesném složení výboru, jeho práci nebo kontrole, kterou provádí[433].

KLÍČOVÉ POSTAVY V ODVĚTVÍ ŠPIONÁŽNÍCH TECHNOLOGIÍ

268. Jednou z klíčových postav vývoje špionážních technologií na Kypru a v Řecku je Tal Dilian. V roce 2017 získal maltské občanství[434]. Před svým odchodem do armádní výslužby v roce 2002 působil Tal Dilian 25 let na různých vedoucích pozicích v izraelských obranných složkách[435]. Na Kypru začal pracovat jako „zpravodajský expert, odborník na rozvoj komunit a zakladatel mnoha podniků“ a poté založil společnost Aveledo Ltd., později známou jako Ws WiSpear Systems Ltd, a poté ještě společnost Passitora Ltd[436].

269. Tal Dilian začal na Kypru úzce spolupracovat s Avrahamem Shahakem Avnim, který

---

[429] Philenews. 'Legální, ale nekontrolované odposlechy.
[430] Odpověď na dotazník Evropského parlamentu obdržený od Kypru.
[431] Odpověď na dotazník Evropského parlamentu obdržený od Kypru; CyLaw. E.U. odst. J(J) ZÁKONA 13(J)/2020.
[432] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[433] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[434] Vláda Malty Persons Naturalised Registered 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.

předtím působil jako zvláštní detektiv v izraelských speciálních policejních složkách[437]. Shahak Avni získal v roce 2015 kyperské občanství a zlatý pas za investice do nemovitostí ve výši 2,9 milionů EUR[438]. Založil také kyperskou společnost NCIS Intelligence Services Ltd[439], která údajně spolupracuje s nejmocnějšími technologickými společnostmi na světě[440]. Jeho firma v roce 2014 a 2015 prodala bezpečnostní software policejnímu ředitelství a v letech 2015 až 2016 poskytovala školení zaměstnancům Úřadu pro kriminalistické analýzy a statistiky[441]. Ke klientům jeho společnosti patří i vládní strana DISY. Objevily se zprávy, že Shahak Avni v kancelářích strany údajně instaloval bezpečnostní zařízení[442]. Kromě Avniho bezpečnostního vybavení koupil Dilianovy produkty také kyperský protidrogový úřad a kyperská policie[443].

270. Oddělení vyšetřování trestné činnosti policejního ředitelství v jednu chvíli zjistilo porušení důvěrnosti soukromé komunikace týkající se společnosti Avni. Policie se rozhodla případ uzavřít[444].

271. Mezi pány Dilianem a Avnim existuje mnoho vazeb. Dilianova společnost WiSpear sdílela s Avnim kromě budovy v Larnace i některé pracovníky[445]. Oba muži v roce 2018 založili společnost Poltrex, která byla později přejmenována na Alchemycorp Ltd. Společnost má kanceláře v budově Novel Tower, stejně jako pan Avni[446], a patří pod značku Intellexa Alliance. Kontakty pana Avniho na stranu DISY údajně připravily půdu pro testování Dilianových produktů[447].

DILIANŮV ŠPIONÁŽNÍ VŮZ

272. Tal Dilian po prodeji společnosti Circles Technologies a založení společnosti WiSpear založil v roce 2019 také společnost Intellexa Alliance, který je podle svých internetových stránek „regulovanou společností se sídlem v EU, jejímž cílem je vyvíjet a integrovat technologie pro posílení práce zpravodajských služeb“[448]. Pod marketingovou značku Intellexa Alliance spadají různí dodavatelé sledovacích systémů, například Cytrox, WiSpear (později přejmenovaný na Passitora Ltd.), Nexa technologies a Poltrex Ltd. Tito různí dodavatelé v Dilianově skupině společností umožňují společnosti Intellexa dodávat a kombinovat široký sortiment dohledového softwaru a služeb pro své zákazníky[449]. Více informací o této korporátní struktuře lze

[437] ShahakAvni. O Shahaku Avnim.
[438] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[439] Philenews, „SPIS: Stát urazil Avniho a Diliana“.
[440] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[441] Philenews, „SPIS:Stát urazil Avniho a Diliana“.
[442] Tovima, „Neznámý „most“ mezi Řeckem a Kyprem pro systém odposlechů“.
[443] Inside Story, „Predator: špion, který přišel z Kypru“.
[444] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[445] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[446] CyprusMail, „*Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal*“ (Akel tvrdí, že našel „kouřící zbraň“ spojující Kypr s řeckým špionážním skandálem).
[447] Inside Story, „Predator: špion, který přišel z Kypru“.
[448] https://intellexa.com/.
[449] Haaretz, „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Bývalý důstojník izraelské tajné služby buduje nové impérium, zatímco Izrael omezuje svůj kybernetický zbrojní průmysl).

nalézt v kapitole o odvětví špionážního softwaru.

273. Dne 5. srpna 2019 poskytl Dilian časopisu Forbes rozhovor o své černé dodávce WiSpear, v němž ukázal různé možnosti špionážního softwaru, které jeho společnost nabízí. Tato dodávka v hodnotě 9 milionů EUR byla schopna napadnout zařízení v dosahu 500 metrů[450]. Pozornost veřejnosti, kterou rozhovor pro Forbes vyvolal, vedla k vyšetřování kyperskými úřady[451]. Nezávislým vyšetřovatelem byl pro toto vyšetřování jmenován právník Elias Stefanou. Během tohoto vyšetřování odhalily úřady další Dilianův podnik, který působil na mezinárodním letišti v Larnace[452].

274. Dne 16. června 2019 Tal Dilian údajně uzavřel se společností Hermes Airports mimosmluvní ujednání o použití svého zařízení WiSpear za účelem údajného posílení Wi-Fi signálu pro cestující na mezinárodním letišti v Larnace, kde byly nainstalovány tři WiFi antény[453]. Ačkoli izraelská společnost Go Networks není registrována na Kypru, podílela se na jednáních, která vedla k uzavření dohody[454]. Skutečným důvodem dohody však bylo otestování odposlechové technologie společnosti WiSpear. Zachycené údaje o cestujících byly uloženy na serverech v serverové místnosti letiště v blízkosti pobočky společnosti WiSpear v Larnace, kterou sdílí s panem Avnim[455]. Během doby, kdy byly antény v provozu, byla zachycena data z 9 507 429 mobilních zařízení[456].

275. V návaznosti na stížnosti proti společnosti Dilian byla izraelská společnost Go Networks údajně spojena se společností Intellexa prostřednictvím sdíleného vlastnictví společnosti v Irsku. Bývalí vysocí zástupci Go Networks byli údajně obsazeni do nejvyšších řídících pozic ve společnosti Intellexa[457]. Policejní vyšetřování kromě toho dospělo k závěru, že společnost WiSpear získala vývozní licence na „odposlouchávací zařízení k extrakci hlasu nebo dat přenášených přes vzdušné rozhraní“[458] [459]. Dilianovy společnosti, jak uvedla obchodní komora, neobdržely v posledních dvou letech žádné vývozní licence. V době, kdy tato zpráva vznikala, nebylo jasné, kdo tyto vývozní licence povolil[460].

276. Elektronická data získaná ze zabaveného zařízení byla pro účely vyšetřování předložena k třístupňovému forenznímu zkoumání, které provedla policie, akademický expert a

---

[450] Haaretz, „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Bývalý důstojník izraelské tajné služby buduje nové impérium, zatímco Izrael omezuje svůj kybernetický zbrojní průmysl).

[451] Forbes, „*A Multimillionaire Surveillance Dealer Steps Out Of The Shadows ... And His $9 Million Whatsapp Hacking Van*“ (Multimilionářský obchodník se sledovacími zařízeními vystoupil ze stínu... a ze své dodávka za 9 milionů dolarů pro hackování Whatsappu).

[452] Haaretz, „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Zatímco Izrael omezuje kybernetický zbrojní průmysl, bývalý důstojník tajné služby buduje nové impérium).

[453] Haaretz, „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Zatímco Izrael omezuje kybernetický zbrojní průmysl, bývalý důstojník tajné služby buduje nové impérium).

[454] Makarios Drousiotis, „Κράτος Μαφία“, Kapitola 6, 2022.

[455] Makarios Drousiotis, „Κράτος Μαφία“, Kapitola 6, 2022.

[456] Makarios Drousiotis, „Κράτος Μαφία“, Kapitola 6, 2022.

[457] Haaretz. „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Zatímco Izrael omezuje kybernetický zbrojní průmysl, bývalý důstojník tajné služby buduje nové impérium).

[458] Makarios Drousiotis. Κράτος Μαφία. Kapitola 6. Vydáno v roce 2022.

[459] Philenews. Vývoz sledovacího softwaru z Kypru.

[460] Inside Story, „*Who signs the exports of spyware from Greece and Cyprus?*“ (Kdo podepisuje vývoz spywaru z Řecka a Kypru).

Europol[461]. Dodávka zůstala v policejní úschově, ale není jasné, co se stalo se sledovacím zařízením. Údajně bylo vráceno panu Dilianovi, ale patrně neexistuje žádné potvrzení.

277. Dne 15. listopadu 2021 byl případ předložen trestnímu soudu, kde byli obžalováni společnost WS WiSpear Systems ltd., Tal Dilian a dva další zaměstnanci společnosti WiSpear. Generální prokurátor George Savvides nakonec potvrdil obvinění společnosti WiSpear, ale trestní řízení proti Dilianovi a zaměstnancům bylo zastaveno[462]. Důvody tohoto rozhodnutí jsou tajné. Generální prokurátor se však může kdykoli rozhodnout, že případ proti těmto třem osobám znovu otevře.

278. Společnost WiSpear se přiznala ke 42 obviněním a 22. února 2022 jí byla u porotního soudu uložena pokuta ve výši 76 000 EUR[463]. Společnost WiSpear se přiznala k obvinění z nezákonného sledování soukromé komunikace a porušování ochrany údajů[464]. Soud zveřejnil svůj konečný rozsudek, v němž uvedl, že: „Porotní soud konstatoval a kvalifikoval, že porušení, které je společnosti přičítáno, nikdy nezahrnovalo žádný úmysl, hackerský útok [nebo] odposlech, a uvedl, že nikdy nedošlo k pokusu nebo záměru personalizovat jakékoli údaje. Soud zdůraznil, že žádné osobě nevznikla újma“[465]. Komisařka pro ochranu osobních údajů Irini Loizidou Nicolaidouová uložila společnosti WiSpear kromě pokuty uložené porotním soudem také pokutu ve výši 925 000 EUR za porušení nařízení GDPR[466]. Přestože se tvrdilo, že se epizoda s černou dodávkou týkala záležitostí národního zájmu a kritické infrastruktury, sankce pro pachatele byly velmi mírné. Tento incident může mít politický význam i nad rámec narušení soukromí cestujících. Vzhledem k tomu, že Kypr leží v mnoha ohledech na křižovatce cest, existuje několik zemí mimo EU, které by mohly mít zájem získat přehled o pohybu cestujících přes letiště Larnaka: například Turecko, Izrael, Rusko a USA.

279. Opoziční strana AKEL vyjádřila rozhořčení nad zastavením vyšetřování Tala Diliana a jeho zaměstnanců a příslušné právní rozhodnutí kritizovala jako pokus generálního prokurátora o krytí skandálu[467]. Kyperská vláda přesto od Dilianovy společnosti údajně nakoupila zařízení a jeden z obviněných zaměstnanců společnosti NSO údajně školil zpravodajskou službu KYP v používání špionážního softwaru Pegasus[468]. To, že bylo vyšetřování zastaveno, znamená, že vazby mezi Dilianovou společností a kyperskou vládou zůstanou utajeny[469]. Generální prokurátor odmítl předat závěry vyšetřování, přestože si je výbor PEGA vyžádal během své oficiální mise na Kypru. Tento příklad

---

[461] Tisková zpráva náměstka generálního prokurátora ze dne 10. srpna 2022 získaná na základě mise výboru PEGA na Kypru ze dne 2. listopadu 2022.
[462] Financial Mirror, „Anger after ‘spy van’ charges dropped“ (Hněv po zrušení obvinění za špionážní dodávku).
[463] Makarios Drousiotis, „Κράτος Μαφία“, Kapitola 6, 2022. Tisková zpráva náměstka generálního prokurátora ze dne 10. srpna 2022 získaná na základě mise výboru PEGA na Kypru ze dne 2. listopadu 2022.
[464] Financial Mirror, „*Spy van company fined €76,000*“ (Společnost vyrábějící špionážní dodávky dostala pokutu 76 000 EUR).
[465] Haaretz, „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Zatímco Izrael omezuje kybernetický zbrojní průmysl, bývalý důstojník tajné služby buduje nové impérium).
[466] CyprusMail. *Israeli company that deployed ‘spy van’ fined €925,000 for data violations* (Izraelská společnost, která nasadila „špionážní dodávku“, dostala pokutu 925 000 EUR za porušování ochrany osobních údajů)*;* Financial Mirror, „*Anger after ‘spy van’ charges dropped*“ (Hněv po zrušení obvinění za špionážní dodávku).
[467] Financial Mirror. Anger after ‘spy van’ charges dropped (Hněv po zrušení obvinění za špionážní dodávku).
[468] Makarios Drousiotis. Κράτος Μαφία. Kapitola 6. Vydáno v roce 2022.
[469] Makarios Drousiotis. Κράτος Μαφία.. Kapitola 6. Vydáno v roce 2022.

ukazuje, že neexistují úplné právní záruky práv na ochranu údajů jednotlivců prostřednictvím zařízení pro hromadné sledování. Zákony sice formálně zajišťují opravné prostředky, ale na rozhodnutí soudů mívá vliv vláda, takže oběti zůstávají bez ochrany. Šetření dále ukázalo, že Kypr se stal místem, kde kyperské společnosti samy experimentují se sledovacími zařízeními.

PŘESUN AKTIVIT DO ŘECKA

280. Tal Dilian po epizodě se špionážním vozem a trestním stíhání přesunul činnost společnosti Intellexa do Řecka, on sám však Kypr neopustil. Údajně plánuje návrat do Tel Avivu[470]. Nepřímé vazby s několika fyzickými a právnickými osobami registrovanými na Kypru a v Řecku odhalují přesun obchodní činnosti pana Diliana do Atén[471]. Níže jsou uvedena některá jména, která jsou součástí kypersko-řeckých vazeb, ačkoli hlavní role společnosti Intellexa SA v Řecku je dále vysvětlena v kapitole o Řecku.

281. Soudní vyšetřování vedlo k převedení aktivit pánů Avniho a Diliana ve společnosti Poltrex na Yarona Levgorena. Pan Levgoren má trvalý pobyt v Kanadě. Stal se akcionářem, ředitelem a tajemníkem společnosti Poltrex. Pan Levgoren je napojen také na společnost Intellexa v Řecku[472]. Podle jeho profilu na Linkedin v současné době zastupuje řeckou společnost Intellexa Apollo Technologies.

SPOLEČNOSTI ZABÝVAJÍCÍ SE ŠPIONÁŽNÍM SOFTWAREM A KYPR

282. Kromě společnosti Intellexa Alliance měla na Kypru údajně sídlo také společnost NSO Group. V roce 2010 Tal Dilian založil společně s Boazem Goldmanem a Erikem Banounem společnost Circles Technologies, která se specializovala na prodej systémů, jež využívají slabin protokolu SS7[473]. Šest let poté byla společnost Circles Technologies prodána kalifornské investiční firmě Francisco Partners za necelých 130 milionů USD, z nichž 21,5 milionu inkasoval pan Dilian. Tato soukromá kapitálová společnost se sídlem v Kalifornii podobným způsobem získala 90 % společnosti NSO Group, což vedlo ke sloučení společností Circles Technologies a NSO Group pod společnost L.E.G.D Company Ltd., která od 29. března 2016 působí pod názvem Q Cyber Technologies Ltd[474].

283. Podle odpovědi kyperské vlády výboru PEGA není v rejstříku společností a duševního vlastnictví zapsána právnická osoba společnosti NSO Group. NSO Group nevlastní akcie žádné právnické osoby registrované na Kypru. Jednotliví členové představenstva NSO Group však založili nebo koupili šest společností. Kromě toho se nezdá, že by špionážní software Pegasus byl vyvinut na Kypru, ani že by byl z Kypru oficiálně

[470] Intelligence Online, *Israeli cyber tsar Tal Dilian plans Tel Aviv return* (Izraelský kybernetický car Tal Dilian plánuje návrat do Tel Avivu).
[471] Haaretz, *As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire* (Bývalý důstojník izraelské tajné služby buduje nové impérium, zatímco Izrael omezuje svůj kybernetický zbrojní průmysl).
[472] Philenews, Jak skandál se spywarem v Řecku souvisí s Kyprem.
[473] Amnesty International, *Operating from the Shadows* (Aktivita ze zákulisí).
[474] Amnesty International, *Operating from the Shadows* (Aktivita ze zákulisí).

vyvezen[475].

284. Expanze v rámci společnosti Francisco Partners v letech 2014 až 2019 zahrnovala šest kyperských společností. Společnost Francisco Partners byla doplněna o společnost ITOA Holdings Ltd., registrovanou na Kypru, společnost Global Hubcom Ltd., která je mateřskou společností společnosti CS-Circles Solutions Ltd., a společnost MS Magnet Solutions. Společnost Mi Compass Ltd. vlastní společnost Ms Magnet Solutions. Společnost CS-Circles Solutions Ltd. dále vlastní společnost CI-Compass Ltd. Kromě kyperských subjektů vlastní společnost CS-Circles Solutions Ltd. také bulharské subjekty. NSO Group uvedla, že „Bulharské společnosti poskytují na základě smlouvy výzkumné a vývojové služby svým příslušným kyperským pobočkám a vyvážejí síťové produkty pro vládní použití“[476],

285. Kyperská vláda popírá vývoz a vývoj softwaru Pegasus. Dne 21. června 2022 manažer NSO Chaim Gelfad prohlásil, že se společnosti NSO Group na Kypru a v Bulharsku podílejí na vývoji softwaru pro zpravodajské služby[477]. Podle dokumentu, který opoziční strana AKEL předala Evropskému parlamentu, NSO Group údajně prostřednictvím jedné z kyperských dceřiných společností prodala špionážní software Pegasus určité společnosti ze Spojených arabských emirátů. Jedna z dceřiných firem NSO Group údajně vystavila této společnosti fakturu ve výši 7 milionů USD[478]. Tuto informaci však nelze potvrdit.

286. Podle dostupných informací měla mít NSO Group na Kypru také firmu, která údajně poskytovala klientské služby. V roce 2017 proběhla v hotelu Four Seasons v Limassolu schůzka mezi manažery společnosti NSO a zákazníky ze Saúdské Arábie, kde jim byla představena nejnovější verze špionážního softwaru Pegasus 3. Tato verze byla vybavena novou funkcí tzv. nulového kliknutí, která dokázala telefon napadnout, aniž by bylo nutné kliknout na zavirovaný odkaz, např. pomocí zmeškaného hovoru na aplikaci WhatsApp. Klienti ze Saúdské Arábie tuto technologii okamžitě zakoupili za 55 milionů USD[479] [480]. V této souvislosti je třeba poznamenat, že rok poté, dne 2. října 2018, zavraždili agenti saúdskoarabského režimu na konzulátu v Turecku Džamála Chášukdžího, a to poté, co několik osob v jeho okruhu sledovali pomocí softwaru Pegasus. To NSO zpochybňuje.

287. Podle organizace Citizen Lab bylo v roce 2020 klienty Circles Technologies 25 státních subjektů. Mezi tyto státní subjekty patřily Belgie, Dánsko, Estonsko a Srbsko[481]. Od roku 2020 uzavřela NSO Group kancelář své společnosti Circles na Kypru. V době vzniku této zprávy není jasné, které společnosti patřící pod společnost Circles zůstávají v provozu[482].

288. Izraelská společnost QuaDream je další společností, která je údajně spojována s

---

[475] Odpověď Kypru na dotazník Evropského parlamentu.
[476] Amnesty International, *Operating from the Shadows* (Aktivita ze zákulisí).
[477] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[478] Zpráva strany Akel, mise výboru PEGA na Kypru.
[479] Makarios Drousiotis, Κράτος Μαφία, kapitola 6, vydáno v roce 2022.
[480] Haaretz, *Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals* (Izraelská kybernetická firma jednala se Saúdy o prodeji pokročilých útočných schopností, odhalil Haaretz).
[481] Citizen Lab. *Running in Circles*. *Uncovering the Clients of Cyberespionage Firm Circles* (Začarovaný kruh. Odhalování klientů kyberšpionážních firemních kruhů).
[482] Amnesty International, *Operating from the Shadows* (Aktivita ze zákulisí).

vývozem svého spywarového produktu „Reign“ z Kypru. V dubnu 2023 média informovala, že společnost QuaDream uzavírá své izraelské pobočky[483]. Prostřednictvím společnosti InReach, která je od roku 2017 registrovaná na Kypru, byly výrobky QuaDream nepřímo prodávány zákazníkům, a tím byly obcházeny izraelské vývozní kontroly. Obě společnosti vedou soudní spor[484].

289. Současným ředitelem a tajemníkem společnosti InReach je A.I.L. Nominee Services Ltd. Tato společnost byla na Kypru zaregistrována již v roce 2010 a jejím zakládajícím akcionářem byl současný náměstek generálního prokurátora Savvas Angelides[485]. Pan Angelides prodal své akcie společnosti A.I.L. Nominee Services panu Christosu Ioannidesovi dne 16. února 2018, několik týdnů předtím, než se stal ministrem obrany[486]. Společnost A.I.L. Nominee Services však zůstává ředitelem a tajemníkem společnosti InReach[487], a tedy v obchodním vztahu se společností vyvážející výrobky QuaDream do třetích zemí.

290. V roce 2011 založil Abraham Sahak Avni spolu s Michaelem Angelidesem, bratrem bývalého ministra a současného zástupce generálního prokurátora Savvase Angelidese, společnost S9S. Jejich společnost S9S byla zapsána do obchodního rejstříku dne 10. listopadu 2011[488] za pomoci bývalé advokátní kanceláře Savvase Angelidese[489]. Kromě toho byla za tajemníka společnosti S9S označena společnost A.I.L. Nominee Services ltd. V té době byl Savvas Angelides stále hlavním akcionářem společnosti A.I.L. Nominee Services[490]. Partnerství mezi Michaelem Angelidesem a panem Avnim však bylo v roce 2012 ukončeno. Savvas Angelides se v roce 2020 stal náměstkem generálního prokurátora a byl osobou pověřenou vyšetřováním pana Avniho a pana Diliana v případu sledovací dodávky[491]. V tiskovém prohlášení ze dne 10. srpna 2022 náměstek generálního prokurátora prohlásil, že on ani jeho příbuzní nemají žádné spojení s Talem Dilianem. O partnerství mezi Michaelem Angelidesem a panem Avnim se zmínil, že „profesionální spolupráce selhala od samého počátku, spolu se skutečností, že společnost registrovaná mou bývalou advokátní kanceláří na pokyn mého příbuzného nebyla nikdy aktivována“, a proto nikdy netvořila „překážku pro mou účast na rozhodnutí týkajícím se případu „černé dodávky“[492]. V tiskovém prohlášení však není žádná zmínka o společnosti Savvase Angelidese A.I.L Nominee Services Ltd., jejíž činnost byla zahájena v červenci 2010[493], ani o úloze této společnosti jako tajemníka v

[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* (Aktivita ze zákulisí).
[485] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/ ; https://opencorporates.com/companies/cy/HE373827.
[486] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.
[487] https://opencorporates.com/companies/cy/HE373827.
[488] Politis, složka „Odposlechy“: Z utajované policejní zprávy (2016) vyplývá, že o Avnim věděl vše.
[489] Tisková zpráva náměstka generálního prokurátora ze dne 10. srpna 2022 získaná během mise výboru PEGA na Kypru dne 2. listopadu 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] Zpráva Fanise Makridise, mise výboru PEGA na Kypru 1. listopadu 2022.
[492] Tisková zpráva náměstka generálního prokurátora ze dne 10. srpna 2022 získaná během mise výboru PEGA na Kypru dne 2. listopadu 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.

partnerství mezi jeho příbuzným a panem Avnim v S9S.

BLACK CUBE

291. Ve společnosti Black Cube pracují i bývalí důstojníci izraelských výzvědných služeb, např. Mosadu. Společnost používá agenty s falešnou totožností. Podle listu *New Yorker* najal bývalý výkonný ředitel NSO Group Shalev Hulio společnost Black Cube poté, co tři právníci – Mazen Masri, Alaa Mahajna a Christiana Markouová – podali žalobu na NSO Group a její přidruženou dceřinou společnost v Izraeli a na Kypru[494]. V roce 2018 obdrželi tito tři právníci několik zpráv od takzvaných známých osob určitých firem a osob, které jim navrhovaly schůzky v Londýně. Hulio prohlásil: „Na žalobě na Kypru se podílela společnost Black Cube“, protože žaloba „přišla z ničeho nic a chci to pochopit“[495]. Společnost Black Cube byla také odhalena ve špionážních skandálech v Maďarsku a Rumunsku.

NÁKUP A POUŽÍVÁNÍ ŠPIONÁŽNÍHO SOFTWARU KYPERSKÝMI ORGÁNY

292. Kyperská vláda nejen vytváří příznivé prostředí pro vývoz špionážních technologií, ale sama spyware i nakoupila. Údajně také sama používala systémy pro sledování osob. V době, kdy zpráva vznikala, nebylo možné určit, ve kterých případech Kypr použil běžné metody sledování a kdy se uchýlil k nasazení špionážních technologií.

293. Po volbách v roce 2013 byl Andreas Pentaras jmenován šéfem kyperské zpravodajské služby, zatímco odborník na sledování Andreas Mikellis byl zodpovědný za ochranu komunikace prezidenta Anastasiadese. V témže roce Mikellis údajně navštívil veletrh sledovacích technologií ISS v Praze, kde údajně jednal se společností Hacking Team o nákupu takzvaného softwaru DaVinci[496]. Software DaVinci dokázal napadnout aplikace mobilního telefonu, a proto nesplňoval oficiální požadavky na zrušení ochrany osobních údajů[497].

294. Zveřejněné informace o kontaktu mezi společnostmi Mikellis a Hacking Team, které odhalil server WikiLeaks, naznačují obcházení výběrových řízení a nedostatečnou kontrolu pořízeného sledovacího systému. Na začátku roku 2014 byl údajně software nainstalován a byli proškoleni čtyři zaměstnanci KYP, včetně Mikellise[498].

295. Když WikiLeaks odhalil nákup sledovacího softwaru společnosti Hacking Team, KYP potvrdila, že tento systém byl používán pouze pro vnitrostátní účely[499]. Navzdory Mikellisovu kontaktu se společností Hacking Team[500] to byl právě šéf KYP Andreas Pentaras, který nakonec po těchto odhaleních odstoupil[501]. Pana Pentarase nahradil Kyriakos Kouros.

---

[494] The New Yorker, How Democracies Spy on their Citizens (Jak demokracie špehují své občany).
[495] The New Yorker, How Democracies Spy on their Citizens (Jak demokracie špehují své občany).
[496] Makarios Drousiotis, Κράτος Μαφία, kapitola 6, vydáno v roce 2022.
[497]Inside Story, „Predator: špion, který přišel z Kypru“.
[498] Makarios Drousiotis, Κράτος Μαφία, kapitola 6, vydáno v roce 2022.
[499]Inside Story, „Predator: špion, který přišel z Kypru“.
[500] Makarios Drousiotis, Κράτος Μαφία, kapitola 6, vydáno v roce 2022.
[501] CyprusMail, *Intelligence chief resigns after spy tech revelations.* (Šéf zpravodajské služby rezignuje po odhalení špionážních technologií).https://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/.

296. Podle serveru WikiLeaks mělo o nákup systému pro sledování komunikace od společnosti Hacking Team zájem ještě jedno policejní oddělení. Toto oddělení se snažilo zajistit tento systém prostřednictvím Sahaka Avniho[5021a]. Není však jasné, o které policejní oddělení se jedná.

SLEDOVÁNÍ MAKARIOSE DROUSIOTISE

297. V únoru 2018 začal být kyperskou vládou údajně sledován investigativní novinář Makarios Drousiotis, a to za použití odposlouchávacích zařízení i špionážního softwaru[503]. V té době byl pan Drousiotis asistentem kyperského člena Komise Christose Stylianidese odpovědného za humanitární pomoc a řešení krizí a pracoval na rozkrývání finančních vazeb mezi prezidentem Anastasiadesem a ruskými prominenty, například oligarchou Dmitrijem Rybolovlevem. Podle Drousiotise souvisel první pokus o sledování s jeho investigativní činností[504].

298. V průběhu vyšetřování ruských kontaktů prováděného panem Drousiotisem se v mezinárodních sdělovacích prostředcích začala objevovat odhalení o NSO Group operující z Kypru, včetně představení systému Pegas 3 v hotelech Four Seasons. Organizace Citizen Lab navíc podezřívá Kypr, že je jednou ze zemí, které využívají technologie NSO k odposlechu komunikace počítačových systémů britského ministerstva zahraničí[505]. V tomto okamžiku si pan Drousiotis začal vzpomínat na několik příznaků infiltrace špionážního softwaru Pegasus do svého telefonu, včetně zmeškaného hovoru v aplikaci WhatsApp, rychlého vybíjení baterie a častého přehřívání zařízení, aniž by ho používal[506]. Vzhledem k těmto událostem se Drousiotis domnívá, že za napadením jeho telefonu stojí kyperská vláda, konkrétně kyperská zpravodajská služba.

299. V květnu 2019 zaslal pan Drousiotis prezidentu Anastasiadesovi dopis, v němž vyjádřil své obavy ze sledování svého telefonu a uvedl možné motivy tohoto sledování a také to, že prezident je osobně odpovědný za vše, co se mu po špionáži může stát. Pan Anastasiades předal dopis současnému šéfovi kyperské zpravodajské služby Kyriakosu Kourosovi. Pánové Anastasiades i Kouros údajné sledování pomocí softwaru Pegasus vyvrátili a zopakovali, že NSO Group ve skutečnosti nebyla na Kypru ani registrována[507].

300. V následujících měsících došlo k několika pokusům o zastrašování, včetně zmizení důkazů z jeho počítače, odpojení bezpečnostních kamer v domě pana Drousiotise a sledování cizími osobami. Poté, co pan Drousiotis svůj příběh zveřejnil a podal stížnost na kyperské policii, spojil se s Lambrosem Katsonisem, vedoucím oddělení technické podpory kyperské společnosti Panda Security, která se specializuje na antivirová zařízení. Pan Drousiotis si však nebyl vědom skutečnosti, že kyperská vláda tento antivirový software používá i pro svá vlastní zařízení. V této souvislosti se zdá, že pan Katsonis byl vyslán do domu pana Drousiotise pod falešnou záminkou, pravděpodobně

[502]Inside Story, „Predator: špion, který přišel z Kypru“.
[503] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/
184 Makarios Drousiotis, Κράτος Μαφία, kapitola 5, vydáno v roce 2022.
[504] Makarios Drousiotis, Κράτος Μαφία, kapitola 5, vydáno v roce 2022.
[505] BBC, Síť No. 10 byla napadena spywarem, tvrdí skupina.
[506] Makarios Drousiotis, Κράτος Μαφία, Chapter 5, vydáno v roce 2022.
[507] Makarios Drousiotis, Κράτος Μαφία, Chapter 5, vydáno v roce 2022.

s cílem dále infiltrovat zařízení pana Drousiotise podle pokynů KYP[508].

301. V roce 2019 se pan Drousiotis dozvěděl o podezřelých záznamech ve svém telefonu se systémem Android a obrátil se na podporu společnosti Google One, aby potvrdila povahu těchto záznamů. Společnost Google však obecně na záležitosti týkající se sledování nereaguje a dotyčného zákazníka odkázala na vnitrostátní orgány činné v trestním řízení. Ačkoli pan Drousiotis neměl k policii důvěru, souhlasil s předáním svých zařízení k forenznímu zkoumání[509].

ZÁVĚREČNÉ POZNÁMKY

302. Právní úprava, kterou se řídí ochrana osobních údajů a soukromí a udílení povolení ke sledování osob a pro vývoz sledovacích technologií, je na Kypru velmi přísná. Nicméně ve skutečnosti se tato pravidla zřejmě dají snadno obcházet a mezi politiky, bezpečnostními agenturami a prodejci sledovacích technologií patrně existují úzké vazby. Zdá se, že v praxi jsou zákony uplatňovány dost laxně, a tak je Kypr pro obchodníky se špionážními zařízeními velmi atraktivní zemí. Je třeba lépe provádět stávající pravidla. O Kypr také jeví velký strategický zájem Rusko, Turecko a USA. Kypr kromě toho pravděpodobně využívá úzké vztahy s Izraelem k oboustranně velmi výhodnému obchodování se špionážním softwarem. Vývozní licence na toto zboží se staly důležitým prvkem v diplomatických vztazích.

I.E. Španělsko

303. Na základě výzvy výboru PEGA byly španělské orgány pozvány na slyšení dne 29. listopadu 2022, aby v rámci svých zákonných povinností poskytly informace o používání sledování pomocí špionážního softwaru ve Španělsku. Vzhledem k uvedeným „právním omezením“ byly odpovědi poskytnuté výboru omezené a většina otázek zůstala otevřená.

304. Výbor PEGA navštívil Madrid v březnu 2023. Delegace se setkala se státním tajemníkem pro evropské záležitosti a s osobami, které byly podle Citizen Lab terčem špionážního softwaru, konkrétně s předsedou katalánské regionální vlády, katalánským regionálním ministrem zahraničních věcí a radním barcelonské městské rady. Setkala se také s členy vyšetřovacího výboru katalánského parlamentu pro software Pegasus, se zástupcem úřadu veřejného ochránce práv, nevládními organizacemi činnými v oblasti základních práv a novináři.

305. V červenci 2021 vyšlo na základě zjištění projektu Pegasus najevo, že ve Španělsku byl sledován velký počet osob. Tyto osoby však zřejmě byly sledovány různými subjekty a z různých pohnutek. V květnu 2022 přinesl deník *The Guardian* zprávu o tom, že Maroko pravděpodobně špehovalo více než 200 španělských mobilních telefonů. Španělská vláda potvrdila, že předseda vlády Pedro Sánchez, ministryně obrany Margarita Roblesová a ministr vnitra Fernando Grande-Marlaska byli napadeni špionážním softwarem Pegasus, zatímco ministr zemědělství Luis Planas byl sledován, ale nebyl napaden[510]. Údajně byl sledován také mobilní telefon tehdejší ministryně

[508] Makarios Drousiotis. Κράτος Μαφία. Kapitola 5. Vydáno v roce 2022.
[509] Makarios Drousiotis. Κράτος Μαφία. Kapitola 5. Vydáno v roce 2022.
[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. května 2022.

zahraničí Aranchi González Layiové, ačkoli původ kybernetického útoku ani to, zda byla napaden softwarem Pegasus, nebyly ověřeny. Druhý špionážní skandál vstoupil do povědomí jako „CatalanGate“[511]. Mezi sledovanými byli katalánští poslanci, poslanci Evropského parlamentu, právníci, novináři, členové organizací občanské společnosti, akademičtí pracovníci a někteří rodinní příslušníci a spolupracovníci těchto obětí[512], což lze označit jako „nepřímé“ zacílení nebo „zacílení na základě vztahů“. První zprávy o aféře CatalanGate se objevily už v roce 2020 po společném vyšetřování deníky *The Guardian* a *El País*[513], ale celý rozsah sledování vyšel najevo až v dubnu 2022, kdy byl zveřejněn důkladný výzkum organizace Citizen Lab. Podle výsledku výzkumu bylo sledováno nejméně 65 osob[514]. Je třeba poznamenat, že od prosince 2022 Citizen Lab uznala, že jedna infekce byla nesprávně připsána v důsledku chyby v označování iniciál[515], ačkoli celkový počet katalánských cílů zůstal nezměněn. V květnu 2022 španělské orgány přiznaly, že se zaměřily na 18 osob se soudním povolením[516], ačkoli zatykače k těmto případům nebyly zveřejněny. Bývalá ředitelka španělského Národního zpravodajského centra (CNI) Paz Estebanová vystoupila na neveřejném zasedání parlamentního výboru pro úřední tajemství, aby sledování těchto 18 osob zdůvodnila.

306. Španělská vláda zatím poskytla jen málo informací o své roli v tomto zásahu s odvoláním na nutnost zachování důvěrnosti z důvodu národní bezpečnosti a z právních důvodů. Na základě řady ukazatelů[517], z nichž některé byly uznány na výše zmíněném výboru pro úřední tajemství, se však předpokládá, že sledování katalánských cílů prováděly španělské orgány.

307. Podrobná analýza sledování ukazuje jasný vzorec. Většina odposlechů v rámci CatalanGate se shoduje s klíčovými politickými událostmi, tématy nebo osobnostmi a souvisí s nimi, například s přípustností zákonů katalánského parlamentu o odpojení, soudními procesy proti katalánským separatistům, veřejnými shromážděními organizovanými Tsunami Democràtic a komunikací s katalánskými separatisty žijícími mimo Španělsko[518]. Takové sledování zahrnuje například komunikaci mezi právníkem a klientem, vězněným separatistou, v předvečer jeho soudního procesu, kontakty mezi manželi nebo komunikaci týkající se obsazování křesel v Evropském parlamentu. Pokud jde o zbývajících 47 případů špionážního softwaru, nebylo možné posoudit, jak by tyto cíle bezprostředně ovlivnily národní bezpečnost nebo integritu státu nebo jak by je bezprostředně ohrožovaly, a nebyly o tom poskytnuty žádné informace[519]. Ačkoli

[511]Zpráva organizace Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022.
[512]Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18. dubna 2022*, s. 1.
[513] https://www.theguardian.com/world/2020/jul/16/two-catalan-politicians-to-take-legal-action-targeting-spyware
[514]Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18. dubna 2022*, s. 1.
[515] Citizen Lab*, Correcting a case,* CatalanGate report (Oprava případu. Zpráva o CatalanGate) https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/ 22. prosince 2022.
[516] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. května 2022.
[517]Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 1 a 3.
[518]Zpráva organizace Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022.
[519] Zpráva organizace Citizen Lab, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022.

některé osoby, které se staly terčem útoku, čelily obvinění z trestného činu již předtím, než se staly terčem útoku, proti žádné z 18 osob, které se staly terčem útoku v důsledku sledování špionážním softwarem, nebylo vzneseno trestní obvinění[520].

NÁKUP ŠPIONÁŽNÍHO SOFTWARU

308. Španělské orgány již dříve přiznaly nákup nástrojů pro odposlech telekomunikací a akvizici společnosti SITEL (systémy pro zákonný odposlech telekomunikací) v roce 2001. Rovněž přiznaly, že služby špionážního softwaru si od společnosti Hacking Team v roce 2010 objednaly ministerstvo vnitra, španělská zpravodajská služba (CNI) a španělská národní policie v rámci zavádění integrovaného systému odposlechu telekomunikačního provozu, který poskytl operačním jednotkám Státní bezpečnosti a Sboru (FCSE) prostředky pro odposlech a záznam elektronické komunikace povolené soudním příkazem[521]. Od akvizice společnosti SITEL ji španělské úřady využívaly mimo jiné při protidrogových operacích, při pátrání po členech džihádistické buňky, která stála za útoky v Madridu 11. března 2004, a v boji proti případům politické korupce. Organizace Citizen Lab již dříve informovala také o podezření, že Španělsko koupilo sledovací software FinFisher[522]. V roce 2020 informoval španělský deník *El País* o tom, že Španělsko uzavřelo obchod se společností NSO Group a že španělská zpravodajská služba běžně používá špionážní software Pegasus[523]. Španělská vláda tento špionážní software údajně zakoupila někdy v období 2010 až 2015 za asi 6 milionů EUR[524] [525]. Nákup společnosti SITEL potvrdil bývalý viceprezident de la Vega v roce2009[526], zatímco nákup služeb od společnosti Hacking Team potvrdila služba CNI v komentáři pro deník *El Confidencial* v roce 2015[527]. Jeden bývalý zaměstnanec NSO kromě toho potvrdil, že Španělsko má u této společnosti účet[528], ačkoli španělské orgány se k tomu odmítají vyjádřit nebo to potvrdit[529].

309. Podle skupiny pro analýzu hrozeb (TAG) společnosti Google je společnost Variston IT se sídlem v Barceloně údajně spojena s rámcem, který využívá n-denní zranitelnosti v aplikacích Microsoft Defender, Chrome a Firefox a instaluje spyware do cílových zařízení. Slabá místa byla opravena v roce 2021 a na začátku roku 2022[530]. Podle svých

---

[520] Mise do Španělska.
[521] Ministerio del Interior, Secretaría de Estado de Seguridad, Centro Tecnológico de Seguridad, Homeland Security Project, scetse.ses.mir.es/publico/cetse/en/proyectosEuropeos/fondoISF/marcoFinanciero-2021-2027/proyectosEuISF.
[522] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 5.
[523] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 5.
[524] Politico, https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/, 20. dubna 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. dubna 2022.
[526] Newtral, https://www.newtral.es/sitel-programa-espia-guardia-civil-policia-espana/20220509/, 9. května 2022.
[527] El Confidencial, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/, 6. července 2015.
[528] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 2022.
[529] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 2022.
[530] Threat Analysis Group. *Nové podrobnosti o komerčním dodavateli spywaru Variston.; Techcrunch. Výrobce spywaru Variston zneužil nulové dny v prohlížečích Chrome, Firefox a Windows, tvrdí Google.*

webových stránek nabízí společnost Variston „řešení informační bezpečnosti na míru“[531].

PRÁVNÍ RÁMEC

310. Právo na soukromí je chráněno článkem 18 španělské ústavy z roku 1978, včetně práva na komunikační tajemství, a zejména chrání „listovní, telegrafní a telefonickou komunikaci“[532]. Používání špionážního softwaru Pegasus a Candiru by bylo v rozporu s článkem 18, pokud by bylo prováděno bez soudního příkazu, což je možnost uznaná španělským právem[533]. Ústava v části I článku 55 rovněž stanoví další výjimky z těchto práv, když, že některá práva mohou být pozastavena za „účasti soudů s náležitou parlamentní kontrolou“, pokud bylo dohodnuto vyhlášení výjimečného stavu nebo stavu obležení za podmínek stanovených ústavou nebo v případě osob vyšetřovaných pro činnost související s ozbrojenými skupinami nebo teroristickými organizacemi[534]. Kromě toho článek 55 obsahuje demokratické záruky, které zajišťují, že „neoprávněné použití nebo zneužití“ těchto pravomocí povede k trestní odpovědnosti.

311. Pro činnosti, které mohou ovlivnit nedotknutelnost obydlí a komunikační tajemství, vyžaduje článek 18 španělské ústavy soudní příkaz. Článek 8 EÚLP vyžaduje, aby jakýkoli zásah do uplatňování tohoto práva ze strany veřejného orgánu byl v souladu se zákonem a představoval opatření, které je v demokratické společnosti nezbytné pro národní bezpečnost, veřejnou bezpečnost, hospodářský zájem země, ochranu veřejného pořádku a předcházení trestné činnosti, ochranu zdraví nebo morálky a ochranu práv a svobod jiných osob.

312. Další podrobnosti o výjimkách z práva na soukromí podle článku 18 jsou uvedeny v trestním řádu [535] [536]. Článek 588 tohoto zákona výslovně omezuje použití vyšetřovacích opatření na vyšetřování skutečností, které vzhledem ke své zvláštní závažnosti odůvodňují omezení základních práv. Nicméně z tohoto ustanovení jsou vyloučeny případy uvedené níže: a) organický zákon č. 2/2002 ze dne 6. května 2002, „který upravuje předběžnou soudní kontrolu Národního zpravodajského střediska“; b) organický zákon č. 4/1981 ze dne 1. června „o stavu ohrožení, výjimečném stavu a nouzovém stavu“; a c) organický zákon č. 2/1989 ze dne 13. dubna o vojenském řízení, který obsahuje doplňující ustanovení použitelná k trestnímu řádu. Článek 588 zákona vyžaduje, aby soudce vydal povolení k odposlechu telefonické a telematické komunikace v případě vyšetřování závažných trestných činů, jako je terorismus nebo trestné činy spáchané prostřednictvím počítačových nástrojů nebo jiných informačních či komunikačních technologií nebo komunikačních služeb. Kromě toho musí být

[531] https://variston.net/.
[532] Ústava Španělska z roku 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, článek 18.
[533] Ústava Španělska 1978,**https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx,** článek 18.
[534] Ústava Španělska z roku 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, článek 55.
[535] Trestní řád z roku 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal Procedure Act 2016.pdf.
[536] Královský dekret ze dne 14. září 1882, kterým se schvaluje trestní řád, https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20220907.

omezení povolena soudním orgánem. Povolení podléhají čtyřem konkrétním zásadám: Za prvé, zásadě speciálnosti (že se sledování týká konkrétního trestného činu). Za druhé, zásadě přiměřenosti (vymezení doby trvání, objektivní a subjektivní rozsah). Za třetí, zásadě proporcionality (síla dostupných důkazů, závažnost případu a požadovaný výsledek) a konečně zásadě výjimečnosti a nezbytnosti (neexistují žádná jiná opatření a bez nich by bylo vyšetřování narušeno)537. Článek 588 *písm.* a), b) a c) výslovně stanoví podmínky pro dálkové prohledávání počítačů. Příslušný soudce může povolit podle článku 588e instalaci softwaru, který umožňuje dálkové a telematické zkoumání bez vědomí vlastníka nebo uživatele, pokud sleduje vyšetřování určitých trestných činů. Za tímto účelem se opatření přísně omezuje na dobu jednoho měsíce s možností prodloužení na o jeden měsíc, nejvýše však na tři měsíce.

313. Článek 197 trestního zákoníku stanoví tresty odnětí svobody v rozmezí od 12 měsíců do čtyř let a pokutu od 12 do 24 měsíců pro osoby, které bez řádného povolení zadrží nebo zachytí mimo jiné elektronickou poštu a telekomunikace[538]. Kromě toho článek 264 trestního zákoníku dále upravuje trestný čin vymazání nebo odstranění údajů a umožňuje přístup k údajům v situacích, kdy bylo příslušným orgánem uděleno požadované povolení[539].

314. Požadavky na soudní dohled jsou následující: a) soudní policie musí vyšetřujícího soudce informovat o provádění a o výsledcích opatření; b) soudce v povolujícím soudním rozhodnutí stanoví četnost a formu informování ze strany soudní policie o provádění opatření; c) soudní policie musí soudci ve stanovených lhůtách zpřístupnit dva různé digitální nosiče, jeden s přepisem pasáží, které jsou považovány za zajímavé, a druhý s kompletními pořízenými záznamy; d) na záznamech musí být uveden původ a cíl každé komunikace; e) soudní policie musí používat pokročilý systém elektronických pečetí nebo podpisů nebo dostatečně spolehlivý varovný systém pro zaručení pravosti a neporušenost informací přenášených z centrálního počítače na digitální nosiče, na nichž byla komunikace zaznamenána; f) soudní policie musí po ukončení provádění opatření podat zprávu o jeho výsledcích.

315. Španělské zpravodajské služby jsou tvořeny třemi hlavními agenturami. Za prvé, Národní zpravodajská služba (CNI) která plní své úkoly shromažďováním informací ve Španělsku i v zámoří a působí pod dohledem a kontrolou výkonné, zákonodárné a soudní moci a je přičleněna k ministerstvu obrany[540]. Ředitel CNI, kterého jmenuje ministr obrany, je hlavním poradcem předsedy vlády v otázkách špionáže a kontrašpionáže[541]. Druhým úřadem je Zpravodajské středisko pro boj s terorismem a organizovaným zločinem (CITCO), které analyzuje domácí situaci, a třetím subjektem je Španělské zpravodajské středisko ozbrojených sil (CIFAS). CIFAS také spadá pod

---

537 . Trestní řád z roku 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal Procedure Act 2016.pdf .

538 Trestní zákoník 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, článek 197.

539 Trestní zákoník z roku 2016 https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal Procedure Act 2016.pdf v článku 264.

540 Národní zpravodajská služba (CNI), https://www.cni.es/.

541 https://www.cni.es/en/intelligence.

přímý dohled ministerstva obrany[542] [543]. Služba CNI byla zřízena zákonem 11/2002 se zmocněním vést „bezpečnostní vyšetřování“[544]. Policejní a donucovací složky v zemi, známé jako „Guardia Civil“, mají „vojenskou povahu“ a jsou rovněž odpovědné ministerstvu obrany[545].

316. Zákon o úředním tajemství z roku 1968 se vztahuje na utajované dokumenty ve Španělsku a nestanoví lhůtu pro odtajnění, po jejímž uplynutí úřední tajemství zaniká[546]. Pokud vláda výslovně nenařídí zveřejnění dokumentů, tj. výslovné odtajnění dokumentu ministerstvem nebo jiným úředním orgánem, zůstávají tyto dokumenty tajné. Tento zákon je v současné době přezkoumáván španělskou vládou, a přestože nebyl stanoven termín jeho přijetí, předběžný návrh zákona o utajovaných informacích byl schválen 1. srpna 2022. Stanoví, že utajované informace budou muset být zveřejněny ve lhůtě 4 až 50 let, která však může být prodloužena.

PŘEDBĚŽNÁ KONTROLA

317. Zpravodajská služba CNI má za úkol poskytovat španělské vládě zpravodajské a jiné informace nezbytné k předcházení a zamezení jakéhokoli rizika nebo hrozby, které mají vliv na nezávislost a integritu státu, národní zájmy a stabilitu právního státu a jeho institucí. Velkou část sledování prováděných ve Španělsku prováděla služba CNI. CNI byla zřízena zákonem 11/2002 ze dne 6. května, který ji zmocňuje vést „bezpečnostní vyšetřování“ osob nebo subjektů[547]. Prostředky používané k těmto činnostem nebo jejich omezení jsou však málo jasné[548], neboť činnosti CNI, její organizace a vnitřní struktura, prostředky a postupy, zaměstnanci, zařízení, databáze a datová centra, zdroje informací a informace nebo údaje, které mohou vést k poznání výše uvedených skutečností, jsou utajovanými skutečnostmi s příslušným stupněm utajení[549]. Zákon 11/2022 dále stanoví parlamentní, výkonný a legislativní dohled výkonné moci nad CNI[550]. Parlamentní kontrolu vykonává Výbor pro využívání a kontrolu úvěrů přidělených tajným fondům (tzv. výbor pro zpravodajské služby) španělského parlamentu ustavený v roce 1995[551]. Z důvodu opožděného ustavení výboru během 14. funkčního období španělského parlamentu (zvoleného v prosinci 2019) nepředložil Výbor pro úřední tajemství výroční zprávu o činnosti CNI, jak vyžaduje zákon. Do dubna 2023 nebyla v tomto volebním období předložena žádná výroční zpráva. Vládní výbor pověřený zpravodajskými záležitostmi koordinuje zpravodajskou činnost všech

[542] https://emad.defensa.gob.es/en/?__locale=en.
[543]Zpráva Ženevského centra pro správu bezpečnostního sektoru 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf na s. 40.
[544] Zákon 11/2002 6. května,https://www.global-regulation.com/translation/spain/1451143/law-11-2002%2c-6-may%2c-regulating-the-national-intelligence-centre.html Článek 5.5.
[545] https://www.guardiacivil.es/es/institucional/Conocenos/index.html.
[546] El País, https://english.elpais.com/spanish_news/2021-04-05/spanish-government-begins-reform-of-franco-era-official-secrets-law.html, 5. dubna 2021; Zákon o úředním tajemství z roku 1968.
[547] Zákon 11/2002 ze dne 6. května, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%2c-6-may%2c-regulating-the-national-intelligence-centre.html v článku 5.5.
[548] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. května 2022.
[549] Zákon č. 11/2002 ze dne 6. května 2002, kterým se upravuje Národní zpravodajské středisko, článek 5.1.
[550] Zákon 11/2002 ze dne 6. května, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html v článku 5.5.
[551] Zákon 11/1995 ze dne 11. května, https://www.boe.es/eli/es/l/1995/05/11/11/con.

španělských zpravodajských a informačních služeb[552]. Legislativním dohledem nad CNI je pak pověřen parlamentní Výbor pro obranu[553]. Priority CNI jsou každoročně určeny v pokynech pro zpravodajské služby.

318. Soudní kontrola činnosti CNI je stanovena v organickém zákoně č. 2/2002 ze dne 6. května 2002[554][555], který doplňuje zákon 11/2022 o CNI ze dne 7. května. Toto nařízení zejména vyžaduje, aby v případě, že CNI hodlá provádět sledování, byl státní tajemník, ředitel CNI povinen požádat příslušného soudce Nejvyššího soudu v souladu s organickým zákonem o soudnictví o povolení přijmout opatření, která se dotýkají nedotknutelnosti obydlí a komunikačního tajemství[556], pokud jsou tato opatření nezbytná pro výkon funkcí CNI. Kromě toho tento zákon stanoví, že sledování nesmí trvat déle než tři měsíce a že každé prodloužení této lhůty musí být řádně odůvodněno. Tato ustanovení však byla uvedena v platnost v době, kdy technologie sledování byla mnohem méně vyspělá a neexistoval špionážní software, jako je Pegasus a Candiru. Hrozí tedy, že právní záruky jsou zastaralé a neposkytují občanům dostatečnou ochranu. Výkonná moc proto oznámila, že provede reformu právního rámce CNI, ale žádné návrhy dosud nepředložila.

NÁSLEDNÁ KONTROLA

319. Zákon, kterým byla zřízena CNI, rovněž ustavil parlamentní Výbor pro obranu, který rozhoduje o financování CNI (jehož výše podléhá utajení) a vypracovává o CNI výroční zprávy. Částky přidělené tajným fondům jsou stanoveny ve španělském obecném zákoně o rozpočtu na každý rozpočtový rok[557]. Všechny orgány pověřené dohledem nad CNI, jako je Výbor pro obranu, Výbor pro úřední tajemství nebo veřejný ochránce práv, mají přístup k informacím potřebným k posouzení, zda byly operace prováděny zákonně a správně. Vláda každoročně stanovuje a schvaluje cíle CNI prostřednictvím pokynů pro zpravodajské služby, které jsou tajné[558] [559]. Ředitel CNI má výlučnou pravomoc určovat účel a určení přidělených finančních prostředků a pravidelně podává zprávu o jejich využití předsedovi vlády. Výbor pro úřední tajemství je informován o cílech zpravodajských služeb a má právo předkládat výroční zprávu o činnosti zpravodajských služeb[560]. Má rovněž přístup k výroční zprávě ředitele CNI o hodnocení činnosti CNI, její situace a míry, v jaké splnila své cíle. Španělské zákony však nestanoví, že by byl veřejnosti umožněn přístup k dokumentům nebo informacím týkajícím se práce zpravodajských služeb. Tento požadavek chybí také v právním rámci

[552] Zákon 11/2002 ze dne 6. května, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%2c-6-may%2c-regulating-the-national-intelligence-centre.html v článku 6.
[553] Zákon 11/2002 ze dne 6. května, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html v článku 5.5.
[554] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4. května 2022.
[555] Organický zákon 2/2002 ze dne 6. května, https://www.global-regulation.com/translation/spain/1451142/law-2-2002%2c-6-may%2c-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. května 2022.
[557] Zákon 11/1995 ze dne 11. května, který upravuje použití a kontrolu úvěrů přidělených tajným fondům, článek 2, https://www.boe.es/eli/es/l/1995/05/11/11/con.
[558] Zákon 11/2002 ze dne 6. května 2002, kterým se upravuje Národní zpravodajské středisko (CNI), článek 3.
[559]Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 2.
[560] Zákon 11/1995 ze dne 11. května, který upravuje použití a kontrolu úvěrů přidělených tajným fondům, článek 7.4.

zákona o transparentnosti[561]. Vzhledem k tomuto utajení nelze s jistotou určit, zda španělská vláda uzavřela smlouvy s NSO Group nebo zda získala a využívala software Pegasus. Osoby, proti nimž je opatření namířeno, neznají důvody, rozsah a důsledky odposlechu své komunikace[562].

320. V důsledku odhalení, že CNI využívalo programy Pegasus a Candiru, oznámil španělský veřejný ochránce práv vyšetřování z moci úřední[563]. Španělský veřejný ochránce práv ve svém oficiálním prohlášení ze dne 18. května 2022 uznal, že Rada ministrů mu poskytla plný přístup k utajovaným dokumentům, aniž by využila své výsady stanovené v článku 22 organického zákona č. 3/1981 o veřejném ochránci práv. Toto vyšetřování se však týkalo pouze 18 osob, u nichž španělské orgány potvrdily, že se na ně zaměřily se soudním povolením[564] [565]. Šetření dospělo k závěru, že odposlechy byly provedeny v souladu se zákonem, protože zjistilo, že byly schváleny soudem a k povolení bylo připojeno požadované odůvodnění[566]. Veřejný ochránce práv však nemá pravomoc posuzovat přiměřenost, tu může určit pouze soudce[567]. Rovněž nekontaktoval ani nevyslechl žádnou z cílových osob nebo jejich právníky. Veřejný ochránce práv doporučil přezkoumat stávající právní předpisy a v případě potřeby provést reformy, které by odrážely modernizaci systémů dohledu[568]. V návaznosti na to španělská vláda v květnu 2022 oznámila, že bude proveden přezkum zákona o úředním tajemství z roku 1968 a organického zákona č. 2/2002[569] [570], ale nestanovila žádný časový rámec pro tento přezkum.

321. Parlamentní výbor pro zpravodajské služby má každoročně předkládat zprávu o jejich činnosti. Byl svolán dne 5. května 2022 s ohledem na sledovací činnosti CNI, ale jednalo se o první schůzi tohoto orgánu po více než třech letech v důsledku narušení parlamentní činnosti způsobeného pandemií COVID-19. Ředitelka CNI Paz Estebanová předstoupila před výbor a přiznala sledování 18 vůdců separatistického hnutí. Výboru rovněž předložila soudní příkazy k těmto 18 případům[571] [572]. V souladu s čl. 5 odst. 5 zákona č. 11/2002 však bylo slyšení neveřejné a přítomným nebylo dovoleno vstupovat

[561] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna, s. 2.
[562] Amnesty International - 10 medidas que garanticen la no repeticion de violaciones des Derechose Humanos.
[563] . https://www.reuters.com/article/us-spain-politics-catalonia-spying-idCAKCN2MG0A6, 24. dubna 2022.
[564] The Guardian, https://www.theguardian.com/world/2022/may/05/catalans-demand-answers-after-spanish-spy-chief-confirms-phone-hacking, 5. května 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. května 2022.

[567] Informace z mise ve Španělsku.
[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. května 2022.
[570] https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. května 2022.
[571] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. května 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. května 2022.

s jakýmikoli elektronickými zařízeními[573]. Kromě počtu případů nebyly k dispozici žádné oficiální informace. Podle mluvčích přítomných na jednání se jeho předmětem stali téměř výhradně katalánské oběti, nikoli Pedro Sánchez nebo Margarita Roblesová a údajné 3 GB dat, které byly z jejich zařízení odcizeny námezdním špionážním softwarem[574]. Roblesová opakovaně zdůrazňovala, že zacílení na 18 Katalánců bylo oprávněné.

322. Sánchez se k této otázce vyjádřil také ve španělském parlamentu, kde znovu zopakoval, že vše bylo provedeno v rámci zákona a že národní bezpečnost podléhá kontrole parlamentu a dalších vládních orgánů[575]. Bývalý generální ředitel NSO Group Shalev Hulio také tvrdil, že použití softwaru Pegasus bylo zcela legální, když pro New Yorker uvedl, že použití softwaru Pegasus Španělskem bylo legitimní vzhledem k tomu, že Španělsko důrazně respektuje právní stát a vyžaduje povolení Nejvyššího soudu[576].

323. Dne 3. května 2022 španělský Kongres hlasoval proti návrhu na zřízení vyšetřovacího výboru pro používání programu Pegasus. Dne 21. září 2022 zřídil katalánský parlament vyšetřovací výbor pro špionáž politických představitelů, aktivistů, novinářů a jejich rodin ze strany Španělského království pomocí programů Pegasus a Candiru.

VEŘEJNÁ KONTROLA

324. Od odhalení v dubnu 2022 se na veřejnost dostalo značné množství informací o používání špionážního softwaru proti členům španělské vlády a zastáncům nezávislosti Katalánska. Španělské sdělovací prostředky a světová média se s pomocí organizací občanské společnosti intenzivně snažily rozkrýt španělský systém pro sledování osob a důrazně vystupovaly na obranu základních práv obětí. Několik španělských politiků se naopak snažilo zdiskreditovat organizaci Citizens Lab a naznačovalo, že její metody jsou nespolehlivé a její práce je politicky motivovaná.

ZJEDNÁNÍ NÁPRAVY

325. Generální advokát[577] podal u španělského Národního soudu (Audiencia Nacional) v Madridu žalobu ve věci sledování předsedy vlády Pedra Sáncheze a ministryně obrany Margarity Roblesové pomocí špionážního softwaru. Příslušnost Národního soudu je stanovena v čl. 65 odst. 1a organického zákona č. 6/1985 o soudnictví, podle něhož údajné skutečnosti spadají do působnosti Národního soudu, neboť se týkají osob ve vysokých státních orgánech, jako je předseda vlády a ministr obrany. Soudcem v tomto stále probíhajícím řízení byl jmenován předseda Ústředního vyšetřovacího soudu č. 4 José Luis Calama[578]. Soudce Calama předložil 13. října 2022 ministryni Roblesové i

[573] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. května 2022.
[574] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. května 2022.
[575] . La Moncloa, https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, 26. května 2022.
[576] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 2022.
[577] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. května 2022.
[578] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. května 2022.

ministru vnitra Grande-Marlaskovi dotazník, který mimo jiné obsahoval otázku, jak zjistili napadení telefonu špionážním softwarem Pegasus, což měli oficiálně doložit. Dotazníky ministrům zaslal také Úřad veřejného žalobce a Nejvyšší státní zastupitelství[579].

326. Žaloby týkající se sledování špionážním softwarem byly podány u Vyšetřovacího soudu v Barceloně osobami s přímými či nepřímými vazbami na katalánské hnutí za nezávislost a probíhá vyšetřování, i když pomalým tempem. První žalobu podali v roce 2020 Roger Torrent, bývalý předseda katalánského parlamentu a současný ministr obchodu a práce Katalánska, a Ernest Maragall, bývalý ministr zahraničních věcí, institucionálních vztahů a transparentnosti Katalánska a současný předseda barcelonské městské rady ze strany ERC[580] [581]. Případ byl přidělen vyšetřovacímu soudu číslo 32 v Barceloně, který jej předběžně uzavřel. Jedním z právníků zastupujících pány Torrenta a Maragalla v tomto případě je Andreu Van Den Eynde, který byl sám spywarem Pegasus sledován. Andreu Van Den Eynde soudům soustavně vytýká, že zdržují, a tak de facto paralyzují řízení[582]. Òmnium Cultural, katalánské národní shromáždění (ANC), a Kandidátka lidové jednoty (CUP) rovněž podaly několik trestních oznámení u stejného soudu v Barceloně, ale žádné vyšetřování zatím nebylo zahájeno. Vyšetřovací soud číslo 32 v Barceloně žádost o společné řízení zamítl, takže se jimi nyní zabývají různé soudy a soudci. Žaloby Òmnium Cultural a CUP byly přiděleny vyšetřovacímu soudu číslo 21 v dubnu 2022 a žaloby ANC soudu číslo 23 dne 26. července 2022. Žalobám dosud nebylo plně vyhověno, ani nebylo dohodnuto zahájení vyšetřování, takže žádný z těchto případů se nevyšetřuje. Většinu případů soudci odložili, dokud nebudou shromážděny další důkazy, protože klíčové důkazy – údajně infikované mobilní telefony – nebyly v držení žalobců [583]. Soudci se mohou rozhodnout, že zprávy organizace Citizen Lab přijmou jako znalecký důkaz v dané věci. Pokud to však soudci neumožní, ztěžuje to cílovým osobám prokázání jejich případu[584].

327. Vzhledem k tomu, že Národní soud má pravomoc rozhodovat o nejzávažnějších trestných činech v celém Španělsku, mohl by státní zástupce požádat o spojení všech případů softwaru Pegasus[585]. Jinými slovy, soudní jednání v případech všech sledovaných členů španělské vlády a osob sledovaných v souvislosti se skandálem „CatalanGate“ proběhnou u Národního soudu v Madridu. Advokáti zastupující sledované osoby z Katalánska tvrdí, že mezi případy neexistuje žádná souvislost, pokud se neprokáže, že pachatel je ve všech případech stejný[586].

---

[579] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. května 2022.
[580] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. května 2022.
El Diario, https://www.eldiario.es/catalunya/juez-archiva-investigacion-espionaje-pegasus-torrent-maragall_1_9030414.html, 30. května 2020
[582] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30. května 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. května 2022.
[584] Mise do Španělska.
[585] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. května 2022.
[586] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. května 2022.

328. V případech 65 sledovaných Katalánců stále probíhá řada soudních řízení. Jednu z žalob podal právník zastupující nejméně 19 obětí hackerského útoku, Gonzalo Boye, který byl sám softwarem Pegasus sledován. Žalobu podal proti společnosti NSO, jejím třem zakladatelům, jimiž jsou Niv Karmi, Shalev Hulio a Omri Lavie, proti společnosti Q Cyber Technologies a dceřiné společnosti OSY se sídlem v Lucembursku[587] [588]. Bývalý premiér Katalánska Quim Torra a bývalý místopředseda katalánského parlamentu Josep Costa podali stížnost k Nejvyššímu soudu, ale i o rok později ještě soudní orgány nerozhodly, zda má být věc projednána před Nejvyšším soudem nebo španělským Národním soudem; Do té doby neprobíhá žádné vyšetřování. Ve Francii, Belgii, Švýcarsku, Německu a Lucembursku probíhají soudní řízení týkající se sledování katalánských separatistů v exilu [589].

CÍLE SLEDOVÁNÍ

329. Sledování členů katalánského hnutí za nezávislost a jejich rodinných příslušníků a zaměstnanců s nimi spojených špionážním softwarem údajně začalo již v roce 2015, kdy byl krátce po velké demonstraci v Barceloně napaden tehdejší předseda Katalánského národního shromáždění (ANC) Jordi Sánchez. Podle zprávy organizace Citizen Lab z dubna 2022 bylo v letech 2017 až 2020 terčem špionážního softwaru nejméně 65 osob: 63 osob bylo terčem softwaru Pegasus, čtyři softwaru Candiru a nejméně u dvou osob šlo o útoky obou softwarů[590]. Napadena byla zařízení 51 osob[591]. Mezi těmi, kteří byli údajně přímo či nepřímo cílem, byli političtí představitelé katalánské nezávislosti, jako ministr pro podnikání a práci a bývalý předseda katalánského parlamentu Roger Torrent; současný předseda Republikánské levice Katalánska (ERC) v barcelonské městské radě a bývalý ministr pro vnější věci, institucionální vztahy a transparentnost Katalánska Ernest Maragall a čtyři poslanci Evropského parlamentu. Jelikož od začátku hackerských útoků do okamžiku zveřejnění těchto informací uplynula značná doba, nebylo možné odhalit nebo dále prošetřit řadu případů, a to z různých důvodů, například proto, že některé sledované osoby se inkriminovaných telefonů zbavily[592].

330. Španělský premiér Pedro Sánchez, ministryně obrany Margarita Roblesová a ministr vnitra Fernando Grande-Marlaska se stali terčem útoků špionážního softwaru Pegasus v období od května do června 2021[593]. O podrobnostech tohoto hackerského útoku je dosud k dispozici jen málo informací, neboť o nich informovala pouze vláda, a nevyplynuly tedy z vyšetřování organizace Citizen Lab ani práce žádné jiné výzkumné služby nebo investigativních novinářů a jsou stále součástí probíhajícího vyšetřování.

---

[587] El Nacional, https://www.elnacional.cat/en/politics/boye-catalangate-legal-offensive-pegasus_751530_102.html, 3 května 2022.
[588] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19. dubna 2022.
[589] Catalan News, https://www.catalannews.com/politics/item/catalangate-solid-evidence-points-to-perpetrators-within-spanish-government-says-citizen-lab, 19. dubna 2022.
[590] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna, s. 5.
[591] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna, s. 5.
[592] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 5.
[593] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2. května 2022.

Premiér Sánchez a ministryně Roblesová stojí včele dvou rezortů, které dohlíží na činnost CNI, tedy orgánu, který ve Španělsku provádí sledování. Napadeny byly jejich služební telefony, které jsou příležitostně kontrolovány, zda neobsahují špionážní software[594]. V případě ministra Grande-Marlasky šlo o napadení soukromého telefonu[595]. Terčem útoku se stal také ministr zemědělství Luis Planas, který dříve působil jako diplomat v Maroku, ale nedošlo k úspěšnému napadení. Podle některých zpráv mohla být za útoky na jeho zařízení odpovědná marocká vláda. Takové informace se však nepotvrdily[596].

331. Z 65 případů bylo potvrzeno 18 případů, na které se španělské orgány zaměřily, ale ke zbývajícím 47 osobám se vláda nevyjádřila[597]. Zůstává nejasné, zda se na ostatní osoby zaměřila CNI na základě soudního příkazu, nebo zda soudní příkaz k jejich zaměření obdržel jiný orgán. Přestože soud vydal příkaz k použití špionážního softwaru u 18 osob, nebyly tyto osoby následně obviněny z trestného činu souvisejícího s příkazem k použití špionážního softwaru. Mezi cíli, jejichž sledování bylo povoleno, jsou současný premiér Katalánska Pere Aragonès, bývalý premiér a současný poslanec Evropského parlamentu Carles Puigdemont a další politici a spolupracovníci podporující nezávislost Katalánska[598]. S výhradou požadavků na utajení a důvěrnost obsažených v zákoně se ministryně obrany Roblesová odvolává na zákon o úředním tajemství, protože nerozšiřuje důvody sledování těchto konkrétních cílů[599]. Většina z 65 Katalánců, kteří byli terčem útoků, byla v určitém okamžiku v kontaktu se členy katalánského hnutí za nezávislost žijícími mimo Španělsko. Některé z osob, které se staly terčem napadení spywarem, se v době nákazy nacházely mimo Španělsko, mimo jiné v Belgii, Švýcarsku, Německu a Francii. Takové digitální sledování by bylo v Německu nezákonné, pokud by nebylo výslovně povoleno spolkovými orgány.

332. Jednou z klíčových skupin osob, u nichž bylo prokázáno, že se staly terčem sledování, jsou katalánští poslanci Evropského parlamentu podporující nezávislost Katalánska. Všichni se stali obětí hackerských útoků buď přímo, nebo nepřímo poté, co byli špionážním softwarem napadeny jejich blízké osoby, což je strategie, kterou Citizen Lab označuje ve své zprávě jako „cílení na příbuzné a známé“. Jednalo se o tyto poslance EP[600]: Diana Riba i Ginerová, Jordi Solé, Carles Puigdemont a Clara Ponsatíová. Úspěšně byl spywarem Pegasus napaden také mobilní telefon bývalého akreditovaného parlamentního asistenta paní Ponsatíové. V případě Antoniho Comína, který během slyšení před výborem PEGA obvinil španělský stát, že ho špehoval, organizace Citizen Lab uznala, že napadení bylo chybně přiřazeno kvůli chybě v označení iniciál.

---

[594] The Economist, https://www.economist.com/europe/spyware-in-spain-targeted-the-prime-minister-and-his-enemies/21809099, 7. května 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. května 2022.
[597] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. května 2022.
[598] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5. května 2022.
[599] El Nacional, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html 5. května 2022.
[600] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 6.

333. Telefon Diany Riba i Ginerové, poslankyně EP za stranu Esquerra Republicana de Catalunya (ERC), byl dne 28. října 2019 přímo napaden špionážním softwarem Pegasus, a to pouze tři měsíce poté, co se ujala funkce v Parlamentu. Během rozhovoru, který vedla se svou asistentkou po telefonu, byla jejich komunikace přerušena a její zaměstnankyně slyšela záznam rozhovoru, který právě vedla s paní Riba i Ginerovou. Načasování tohoto útoku se přímo časově shodovalo s klíčovým rozhodnutím soudu o katalánských separatistech, z nichž jedním je Raül Romeva, manžel paní Riba i Giner, který nakonec dostal trest odnětí svobody v délce 12 let[601]. Paní Riba i Ginerová na jednání výboru PEGA v Evropském parlamentu uvedla, že v té době se většina jejích telefonních hovorů týkala daného soudního případu a řady setkání a návštěv soudů. Vedlejší úlovek v projednávané věci byl jako takový mimořádně významný, včetně pana Romevy a dalších osob spojených s tímto zásadním případem[602].

334. Podle výzkumu organizace Citizen Lab byl poslanec EP Jordi Solé, rovněž ze strany ERC, původně napaden hackery 11. i 27. června 2020[603]. Později však bylo odhaleno pět dalších útoků během stejného období[604]. Solé zjistil, že se stal obětí softwaru Pegasus, pouze náhodou, když obdržel potenciálně podezřelé zprávy, předložil svůj telefon ke kontrole jako součást dokumentu[605]. Podobně jako v případě jeho kolegyně stojí za pozornost načasování tohoto útoku. Došlo k němu během kritických politických diskusí o neobsazeném křesle Oriola Junquerase, kterému nebylo uděleno povolení k nástupu do funkce poslance EP, jelikož byl ve Španělsku uvězněn za rozvratnou činnost[606], a pouze měsíc předtím, než byl Solé jmenován, aby toto křeslo převzal v červenci 2020. Navíc v té době probíhaly diskuse o strategii strany a mezinárodních soudních sporech týkajících se jejích vězněných a exilovaných kolegů v době těchto hackerských útoků[607].

335. Carles Puigdemont, poslanec EP za stranu JUNTS a bývalý prezident Katalánska, se stal cílem útoků prostřednictvím své manželky Marcely Toporové, zaměstnanců a řady spolupracovníků[608]. Organizace Citizen Lab celkem uvádí, že oběťmi útoků bylo až 11 osob v úzkém kontaktu s Puigdemontem, včetně nejméně dvou potvrzených úspěšných útoků na zařízení paní Toporové dne 7. října 2019 a 4. července 2020[609].

336. Na Claru Ponsatíovou, poslankyni EP za stranu JUNTS a bývalou ministryni školství Katalánska, se útoky zaměřily rovněž skrze blízké osoby. Bylo potvrzeno, že dne 7.

---

[601] Vyšetřovací výbor pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru – svědectví ze slyšení poslankyně EP paní Diany Riba i Ginerové, Štrasburk, 6. října 2022.
[602] Vyšetřovací výbor pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru – svědectví ze slyšení poslankyně EP paní Diany Riba i Ginerové, Štrasburk, 6. října 2022.
[603] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna, s. 7.
[604] Vyšetřovací výbor pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru – svědectví ze slyšení poslance EP pana Jordiho Solého, Štrasburk, 6. října 2022.
[605] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 2022.
[606] Vyšetřovací výbor pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru – svědectví ze slyšení poslance EP pana Jordiho Solého, Štrasburk, 6. října 2022.
[607] Politico, https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/, 9. ledna 2020.
[608] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 7.
[609] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 7.

července 2020 byl proveden úspěšný útok na Pola Cruze, zaměstnance Evropského parlamentu[610].

337. Terčem útoků špionážního softwaru byli všichni předsedové katalánské vlády od roku 2010, a to buď během svého funkčního období, nebo i po něm[611]. Mezi 65 sledovanými bylo i 12 členů Republikánské levice Katalánska, včetně generální tajemnice strany Marty Rovirové, jejíž telefon byl podle zprávy Citizen Lab v červnu 2020 napaden nejméně dvakrát. Nanejvýš významná je přitom skutečnost, že Gabrielová i Rovirová žily v době, kdy byly sledovány, ve Švýcarsku, kam se uchýlily v důsledku krize, která nastala po referendu v roce 2017.

CIVILNÍ CÍLE, VČETNĚ NOVINÁŘŮ, PRÁVNÍKŮ A ZÁSTUPCŮ OBČANSKÉ SPOLEČNOSTI

338. Jordi Domingo byl jedním z prvních katalánských aktivistů, o jejichž sledování informovaly v roce 2020 sdělovací prostředky. Ačkoli byl zastáncem katalánské nezávislosti a členem katalánského Národního shromáždění (ANC), deník *The Guardian* uvedl, že sám Domingo pokládal sledování své osoby za omyl. Jelikož při událostech v roce 2017 nehrál žádnou významnou úlohu, byl přesvědčen, že zamýšleným terčem byl jeho jmenovec, právník, který se podílel na vypracování případné ústavy pro nezávislé Katalánsko[612].

339. Katalánské národní shromáždění (ANC), katalánská organizace občanské společnosti podporující katalánskou nezávislost, bylo jednou z prvních organizací, která byla před katalánským referendem napadena, a od té doby je obětí rozsáhlého sledování[613]. Mezi šesti oběťmi z ANC jsou dva bývalí předsedové, Jordi Sánchez (2015–2017) a Elisenda Paluzieová (2018–2022), jejichž sledování špionážním softwarem bylo povoleno soudním příkazem, stejně jako sledování odborníka na digitální hlasování a decentralizaci Jordiho Baylina, dvou členů jeho Národní rady (Arià Bayè a Sònia Urpíová) a jednoho člena místní pobočky (Jordi Domingo).

340. Zařízení osob blízkých Jordimu Cuixartovi, předsedovi organizace Òmnium Cultural (do února 2022), byla napadena, protože byl v té době ve vězení. Patřil mezi ně i Marcel Mauri, který zastával funkci místopředsedy této nevládní organizace a jehož sledování pomocí špionážního softwaru bylo povoleno na základě soudního příkazu.

341. Organizace Citizen Lab odhalila v únoru 2021 aktivní software Candiru na notebooku Joana Matamaly, podnikatele a aktivisty s úzkými vazbami na katalánské politiky podporující nezávislost[614]. Sledování Matamaly špionážním softwarem bylo povoleno na základě soudního příkazu. Candiru je výrazně těžší vysledovat než Pegasus a tento objev aktivní infekce umožnil výzkumným pracovníkům v Citizen Lab lépe porozumět

---

[610] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 7.
[611] Artur Mas (po odchodu z funkce), Carles Puigdemont (cílení na příbuzné), Joaquim Torra (během výkonu funkce), Pere Aragonès (napaden během výkonu funkce vicepremiéra pro pana Torru). 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. července 2020.
[613] Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.
[614] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 2022.

jejím vzorcům. Následně bylo na zařízení pana Matamaly nalezeno dalších 16 napadení[615]. Microsoft následně zranitelná místa opravil prostřednictvím aktualizací, ale není možné zjistit počet napadení softwarem Candiru, které zůstaly bez povšimnutí[616].

342. Prostřednictvím softwaru Pegasus bylo zaútočeno na nejméně tři renomované vývojáře a podnikatele s otevřeným zdrojovým kódem. Cílem útoku se stali Xavier Vives a Pau Escrich, spoluzakladatelé společnosti Vocdoni, což je protokol s otevřeným zdrojovým kódem založený na blockchainu Ethereum pro bezpečné digitální hlasování odolné vůči cenzuře. Vives byl konkrétně napaden škodlivým softwarem Candiru, zatímco Escrich byl napaden softwary Pegasus i Candiru[617]. Sledování pánů Vivese a Escricha pomocí špionážního softwaru bylo povoleno soudním příkazem.

343. Gonzalo Boye je právník bývalých předsedů katalánské vlády pánů Puigdemonta a Torrase[618]. Během pěti měsíců od ledna do května 2020 byl Boye až 18krát terčem útoků prostřednictvím textových zpráv, které se objevily jako tweety organizací občanské společnosti nebo významných zpravodajských serverů[619]. Organizace Citizen Lab potvrdila, že jeho telefon byl minimálně jednou napaden úspěšně a to dne 30. října 2020. Došlo k tomu jen 48 hodin po zatčení jednoho z jeho klientů[620]. S útoky na pana Boyeho vyvstal problém nezákonného porušení pravidla zachování profesního tajemství mezi advokátem a klientem.

344. Elena Jimenezová, mezinárodní zástupkyně Òmnium Cutural, a Jordi Bosch, právník Òmnium Cultural odpovědný za institucionální vztahy, byli oba sledování pomocí softwaru Pegasus v době, kdy působili v právním týmu Jordiho Cuixarta. Paní Jimenezová byla trvale ve styku s celým právním týmem pana Cuixarta, včetně mezinárodního týmu, který připravoval stížnost k ESLP. Organizace Citizen Lab zatím analyzovala pouze mobilní telefon, který paní Jimenezová používala naposledy, nicméně v únoru 2020 potvrdila úspěšné napadení metodou „zero-click“. Bosch, méně veřejná tvář právního týmu, byl v červenci 2020 sledován ani ne týden poté, co byly zmírněny Cuixartovy vazební podmínky, a téhož dne, kdy poprvé vystupoval v katalánské televizi za Òmnium Cultural.

345. Andreu van den Eynde i Adroer byl softwarem Pegasus napaden dne 14. května 2020[621]. K hackerskému útoku došlo v době, kdy jako advokát obhajoval Raüla Romevu a Oriola Junquerase v soudním řízení u Nejvyššího soudu.

346. Napadeno bylo i zařízení právníka Jaume Alonso-Cuevillase, když zastupoval klíčové katalánské představitele, jako např. Carlese Puigdemonta. Datum, kdy k napadení jeho telefonu došlo, však Citizen Lab nebyla schopna přesně určit.

---

615 The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 2022.
616 The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 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/.
621 Zpráva organizace Citizen Lab o „CatalanGate“, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18. dubna 2022, s. 10.

347. Poté, co se dne 22. dubna 2022 veřejnost dozvěděla o kauze „Catalangate“, zahájily španělské orgány proces kontroly na politické úrovni, jehož cílem je zajistit správné uplatňování pokynů pro sledování. Tato opatření zahrnovala předvolání Paza Estebana, ředitele CNI, před Výbor pro úřední tajemství dne 5. května, které oznámil ministr předsednictví Felix Bolaños, zasedání parlamentní kontroly vlády a ministra obrany ve dnech 26. a 27. dubna a nezávislé hodnocení provedené veřejným ochráncem práv, které bylo zahájeno 26. dubna 26 a ukončeno 18. května. Ministryně obrany Margarita Roblesová, vázaná mlčenlivostí v souladu se zákonem o úředním tajemství, naznačila, že opatření byla přijata v reakci na jednání těch, kteří „porušili ústavu, uchvátili veřejnou infrastrukturu, narušovali veřejný pořádek a [těch, kteří] mají vazby na politické představitele země, která provádí invazi na Ukrajinu“[622]. Vládní strana PSOE a tři hlavní opoziční strany (PP, Vox a Ciudadanos) uvedly, že ředitel poskytl uspokojivé vysvětlení, pokud jde o nezbytnost a zákonnost přijatých opatření[623] [624].

348. Španělský veřejný ochránce práv potvrdil, že velká část dohledu prováděného ve Španělsku ze strany CNI byla plně v souladu se zákonem. V návaznosti na jeho doporučení ohledně přiměřenosti parlamentních a soudních kontrol a za účelem aktualizace právních předpisů, posílení záruk soudní kontroly a zajištění maximálního dodržování základních práv jednotlivců se španělská výkonná moc zavázala:

1. provést vnitřní šetření v CNI;

2. zahájit ve výboru šetření týkající se využívání a kontroly prostředků přidělených tajným fondům španělského Kongresu a uskutečnit slyšení, na něž se dostaví ředitel CNI; a

3. poskytnutí informací výboru ohledně využívání a kontroly prostředků přidělených tajným fondům španělského Kongresu a Nejvyššího soudu, ohledně 18 příkazů k povolení vniknutí do systému a ohledně odtajnění dokumentů CNI týkajících se členů hnutí za nezávislost Katalánska, proti nimž byly vedeny útoky, na žádost soudce;

4. novelizovat španělský zákon o úředním tajemství z r. 1968[625];

5. provést reformu právního rámce CNI[626];

6. přijmout novou směrnici o zpravodajských informacích, která stanoví zpravodajské cíle CNI; a

7. aktualizovat národní bezpečnostní strategii z roku 2021 a plán kybernetické

[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. dubna 2022.
[623] La Vanguardia, https://www.lavanguardia.com/politica/20220505/8245084/cni-aporta-autorizaciones-judiciales-parte-espionaje-catalangate.html, 5. května 2022.
[624] El Periodico de Espana, https://www.epe.es/es/politica/20220505/frente-comun-pp-vox-cs-13614030, 5. května 2022.
[625] EL País, *El Gobierno Inicia la reforma de la ley franquista de secretos oficiales*, 5. dubna 2021
[626] La Moncloa, *Pedro Sánchez anuncia una reforma de la regulación del control judicial del CNI para reforzar sus garantías*, 26. května 2022

bezpečnosti.

349. Španělský vrchní soud[627] zahájil vlastní vyšetřování poté, co vláda uvedla, že software Pegasus byl použit ke špionáži ministrů, včetně předsedy vlády Sáncheze. V rámci tzv. vyšetřovací komise pro vyšetřování špionáže vyzval soud generálního ředitele izraelské společnosti NSO Group, která prodává špionážní software Pegasus, a ministra Felixa Bolañose, aby vypovídal jako svědci. Vyšetřující soudce rovněž vyslechl bývalou ředitelku Národního zpravodajského centra Paz Estebanovou[628] [629], jakož i ministry obrany a vnitra, jejichž zařízení byla mezi napadenými. Soud[630] zaslal izraelské vládě formální žádost o mezinárodní soudní pomoc s žádostí o informace o „různých aspektech tohoto softwaru“. Soud rovněž odtajnil dokumenty týkající se případu a zrušil zákaz vyšetřování odposlechů mobilních telefonů předsedy vlády Sáncheze a ministryně obrany Roblesové.

ZÁVĚREČNÉ POZNÁMKY

350. Španělsko má nezávislý soudní systém s dostatečnými zárukami. Po objevení těchto dvou kategorií cílů ve Španělsku však zůstávají některé otázky, které by mohly být zodpovězeny rychlými a hlubokými reformami a jejich účinným prováděním. Španělská vláda pracuje na úpravách, které mají nedostatky odstranit. Pokud jde o reformu CNI, španělská vláda 26. května 2022 oznámila svůj záměr reformovat právní rámec CNI, ale žádný návrh dosud nepředložila. Dne 1. srpna 2022[631], vláda předložila legislativní změny zákona o úředním tajemství. Vláda v současné době čeká na stanovisko Státní rady.

351. 47 osob, na které se zaměřila zpráva Citizen Lab a u nichž není jasné, zda byly cílem CNI na základě soudního příkazu, nebo zda soudní příkaz k jejich zaměření obdržel jiný orgán, nezná důvody, rozsah ani aktéry, kteří stáli za zaměřením pomocí programu Pegasus. Tyto osoby by měly mít přístup ke spravedlnosti a mělo by být zahájeno vyšetřování, aby se tyto případy objasnily.

352. Pokud jde o 18 případů, u nichž byl vydán soudní příkaz, jejich zákonnost byla ověřena a potvrzena veřejným ochráncem práv, ale jejich zvláštní povahu, přiměřenost, výjimečnost, přiměřenost a nezbytnost[632] může ověřit pouze soud.

353. Obecněji řečeno, soudní řízení vedená cílovými osobami neprobíhají tak rychle, jak se očekávalo, s cílem zajistit transparentnost a přístup ke smysluplné právní ochraně. Klíčová je zde spolupráce úřadů. K zajištění větší jasnosti a přispění technickými znalostmi by mohl být přizván Europol, který by mohl poskytnout podporu při

---

[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.
[632] Článek 588 a. i. kapitoly IV Trestního řádu.

zajišťování řádného forenzního postupu.

I.F. Další členské státy

NIZOZEMSKO

354. V koaliční dohodě nizozemské vlády z roku 2017 se uvádí, že nizozemská policie nesmí nakupovat špionážní software od poskytovatelů, kteří své produkty dodávají „pochybným režimům“, které byly později označeny jako „země, jež se dopustily závažného porušování lidských práv nebo mezinárodního humanitárního práva“. Před pořízením špionážního softwaru se nizozemská policie musí poskytovatele dotázat, zda jsou mezi jeho klienty země, na něž EU nebo OSN uvalily sankce, a ověřit, zda země, v níž má poskytovatel sídlo, provádí kontroly vývozu, při nichž je v rámci postupu udělování vývozních licencí posuzováno dodržování lidských práv. Toto hodnocení se pravidelně opakuje. Je třeba poznamenat, že uvedené omezení se zřejmě vztahuje pouze na nákup špionážního softwaru policií. Zpravodajské služby výslovně zmíněny nejsou. Podle vlády používá policie špionážní software od roku 2019, ačkoli orgány neuvádějí, o jaký typ softwaru se konkrétně jedná[633]. Zdá se, že NSO Group a její špionážní software Pegasus výše uvedené normy nesplňují – každopádně je nesplňovaly před zpřísněním režimu vývozu z Izraele v prosinci 2021[634]. O výdajích policejních a zpravodajských služeb na nákup a používání špionážního softwaru nejsou k dispozici žádné informace.

355. V Nizozemsku začal v roce 2018 fungovat nový orgán (Toetsingscommissie Inzet Bevoegdheden, TIB), který předem posuzuje zákonnost povolení k používání sledovacích technik, které vláda uděluje zpravodajským službám. Sledování nesmí proběhnout, pokud TIB označí povolení za protiprávní. TIB doplňuje hlavní orgán dohledu, revizní výbor pro zpravodajskou a bezpečnostní službu (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD). CTIVD dohlíží na probíhající sledovací činnosti zpravodajských služeb po udělení povolení a vyřizuje stížnosti.

356. Je třeba poznamenat, že v období od listopadu 2014 do prosince 2016 mohla společnost NSO Group působit díky dvěma společnostem, Shapes 1 BV a Shapes 2 BV se sídlem v Nizozemsku, v odvětvích „finanční holdingy“ a „inženýrské a další technické návrhy a poradenství.“ Jejich činnost byla po dvou letech ukončena[635].

357. Dne 4. října 2022 bylo zjištěno, že v listopadu 2019 se nizozemské ministerstvo obrany chystalo podepsat dohodu se společností WiSpear, kterou vlastní Tal Dilian a kterou předtím zakoupila společnost Cytrox, výrobce špionážního softwaru Predator[636]. Společnost WiSpear vyhrála nabídkové řízení nizozemského ministerstva. Z e-mailové korespondence není zřejmé, zda se jedná o software Predator, nebo jiný produkt. Ze zveřejněných e-mailů vyměněných mezi kyperským ministerstvem energetiky, obchodu a průmyslu a společností WiSpear je zřejmé, že zástupce nizozemského ministerstva

[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.
[635] Amnesty International, *Operating from the Shadows: Inside NSO Group's corporate structure*.“ (Aktivita ze zákulisí: uvnitř podnikové struktury společnosti NSO Group) https://www.amnesty.org/en/documents/doc10/4182/2021/en/.
[636] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/.

obrany se ve dnech 13.–15. listopadu 2019 obrátil na kyperské ministerstvo obchodu, aby získal ujištění o WiSpear, a to pouze několik dní před tím, než vypukl skandál se „špionážní dodávkou“ Tala Diliana. Pan Dilian informoval zástupce kyperského ministerstva obchodu, že by ocenil jeho okamžitou pomoc v této věci, neboť se blíží uplynutí lhůty pro podepsání smlouvy[637]. Zda byla smlouva podepsána a zda byl jakýkoli špionážní software nizozemskému ministerstvu obrany dodán, není jasné.

358. Nizozemsko je rovněž domovem dceřiné společnosti Cognyte, zapsané pod názvem Cognyte Netherlands B.V. Jak je patrné z výňatku z nizozemské obchodní komory, jediným akcionářem nizozemské dceřiné společnosti je společnost UTX Technologies se sídlem na Kypru. Jak je popsáno v kapitole o Kypru a softwarovém průmyslu, UTX Technologies má za sebou historii vývozu zpravodajských a sledovacích systémů do Bangladéše a dodávek systémů sledování do členských států EU. Kromě toho byla izraelská společnost Verint – která rovněž vlastnila Cognyte před odštěpením v roce 2021 – hlavním dodavatelem monitorovacího systému nizozemské policii[638]. Vazby mezi policií a tímto izraelským dodavatelem jsou ještě jasnější, jakmile vezmeme v úvahu, že bývalý policista Robert van Bosbeek nastoupil roku 2014 do funkce ředitele společnosti Cognyte Netherlands B.V.[639]. Další ředitel této nizozemské dceřiné společnosti, David Abadi, je rovněž finančním ředitelem izraelské společnosti Cognyte Software Ltd, která byla spojena s prodejem špionážního softwaru Myanmaru[640].

359. Dne 2. června 2022 média informovala, že nizozemská zpravodajská služba Algemene Inlichtingen– en Veiligheidsdienst (AIVD) použila program Pegasus, když pomáhala policii při pátrání po podezřelém ze závažné trestné činnosti Ridouanu T., který se stal hlavním podezřelým z několika vražd souvisejících s organizovaným zločinem, obchodem s drogami a vedením zločinecké organizace a byl zatčen 16. prosince 2022 v Dubaji[641]. Nizozemská vláda se k tomu odmítla vyjádřit. Jedná se o pozoruhodný případ, který si zasluhuje větší pozornost. K únikům došlo v době, kdy byly Pegasus a NSO Group pod velkou kritikou veřejnosti a zařazení na černou listinu Ministerstvem obchodu USA společnost NSO Group finančně poškodilo. Nizozemský úspěch, kdy se podařilo chytit jednoho z nejhledanějších pachatelů trestné činnosti posledních let, bylo vítanou pozitivní zprávou. Mediální zpráva vychází z prohlášení čtyř zdrojů v rámci AIVD. Jejich motivy k únikům informací nejsou ve zprávě zmíněny. Rovněž se nezdá, že by došlo k vyšetřování těchto úniků, což vyvolává otázku, zda únik nebyl schválen vedením AIVD. Je však velmi nepravděpodobné, že by AIVD únik celého příběhu umožnila bez vědomí a souhlasu izraelských orgánů.

BELGIE

360. V rozhovoru pro časopis *The New Yorker* prozradil bývalý pracovník izraelských zpravodajských služeb, že belgická policie používá při svých operacích software Pegasus[642]. V reakci na to belgická policie uvedla, že „nebude o technických prostředcích používaných pro vyšetřování a mise poskytovat žádné informace“. V září

[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*“ (Izraelská společnost Cognyte vyhrála výběrové řízení na prodej špionážního softwaru pro odposlech Myanmaru před převratem, ukazují dokumenty'.
[641] https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/.
[642] https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.

2021 ministr spravedlnosti Vincent Van Quickenborne uvedl, že zpravodajské služby mohou software Pegasus používat legální cestou, ale nechtěl potvrdit, zda je belgická zpravodajská služba klientem společnosti NSO nebo zda proti pachatelům trestné činnosti používá některý špionážní software[643].

361. EL Mahjoub Maliha, obránce lidských práv ze Západní Sahary žijící v Belgii, a Carine Kanimbová, dcera rwandského politického aktivisty Paula Rusesabaginy, byli během svého pobytu v Belgii rovněž špehováni prostřednictvím softwaru Pegasus, a dokonce i během setkání s belgickými vládními úředníky. Špionážní útoky byly s největší pravděpodobností provedeny marockými a rwandskými orgány, v příslušných případech, nebo jejich jménem. Rwanda je rovněž obviněna z použití špionážního softwaru Pegasus v případě, kdy se měla zaměřit na kritiky žijící v belgickém exilu, včetně předních představitelů opozice Placida Kayumby a Davida Batengy[644]. Belgická vojenská zpravodajská služba ADIV dále zjistila, že Pegasus Rwanda velmi pravděpodobně nainstalovala na chytrý telefon belgického novináře Petera Verlindena, kriticky vystupujícímu vůči prezidentu Kagamemu, a jeho manželky Marie Bamuteseové[645]. Mezi další belgické cíle špionážního softwaru patří bývalý předseda vlády Charles Michel a jeho otec Louis Michel (tehdejší poslanec EP, bývalý komisař a ministr zahraničních věcí). Podle belgických sdělovacích prostředků stála za útoky marocká vláda[646].

NĚMECKO

362. Německými subjekty, které provádějí a používají hackerské útoky, jsou Bundesnachrichtendienst, spolková zpravodajská služba neboli BND, armáda, celní správa a policie. BND je agentura, která využívá hackerské útoky v největší míře. Už v roce 2009 monitorovala 2 500 zařízení[647].

363. V Německu je zaveden právní rámec upravující používání špionážního softwaru. Od roku 2008 uděluje německé spolkové právo policii pravomoc ke státem posvěceným hackerským útokům v případech mezinárodního terorismu a za účelem předcházení teroristickým útokům[648]. V roce 2017 vstoupil v platnost nový zákon, který v případě 42 trestných činů umožňuje všem donucovacím orgánům použití státního hackingu. Mezi tyto trestné činy patří mimo jiné podávání podvodných žádostí o azyl, daňové úniky a drogové trestné činy[649]. V roce 2021 přijal Spolkový sněm návrh zákona spolkové vlády „o úpravě zákona o ochraně ústavy“. Tato změna legalizuje státní hackerské útoky pro všech 19 německých zpravodajských služeb[650] a stanoví povinnost poskytovatelů

[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/.
[647] Evropský parlament. Slyšení o Německu; 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.

komunikačních služeb se státem na hackingových činnostech spolupracovat[651].

364. Zákony o hackingu jsou v Německu často odůvodněny případy trestných činů proti sexuálnímu sebeurčení, dětské pornografie, vytváření zločineckých organizací a vražd. Většina vyšetřování, při nichž policie používá hackingové nástroje, však s výše uvedenými trestnými činy nesouvisela[652]. Nejnovější údaje z roku 2020 ukazují, že německá policie získala povolení k 48 hackerským útokům. Realizováno bylo pouze 22 z nich, z nichž ale žádný se netýkal boje proti terorismu či vraždy[653].

365) V září 2021 bylo oznámeno, že německý Spolkový kriminální úřad (Bundeskriminalamt – BKA) koncem roku 2020 zakoupil software Pegasus. Zde je třeba poznamenat, že německé právo rozlišuje dvě formy použití špionážního softwaru[654]: přístup ke všem informacím (Online-Durchsuchung[655]) a přístup pouze k přímé komunikaci (Quellen-TKÜ[656]). Vzhledem k tomu, že původní software Pegasus umožňoval přístup ke všem údajům v zařízení, a nikoli pouze k přímé komunikaci, jeho použití ze strany úřadu BKA by bylo v rozporu se zákonem. Od přelomového rozhodnutí německého Spolkového ústavního soudu z roku 2008 musí veškerý špionážní software používaný policejními orgány splňovat normy pro telekomunikační a online sledování stanovené pro úřad BKA [657] [658]. Úřad proto společnost NSO požádal o změnu zdrojového kódu tak, aby Pegasus zprostředkovával přístup ke komunikaci pouze v mezích zákona. Společnost NSO to zpočátku odmítala[659]. Souhlasila až po dalším jednání, na jehož základě byla dodána nová modifikovaná verze softwaru[660]. Ačkoli to nebylo veřejně přiznáno, Martina Linková, tehdejší náměstkyně ředitele BKA, potvrdila nákup upravené verze během neveřejného zasedání Innenausschuss v Bundestagu[661]. Ta se začala údajně používat v březnu 2021. Verze, kterou úřad BKA zakoupil, měla zablokované některé funkce, aby se zabránilo jejímu zneužití, avšak není jasné, jak toto funguje v praxi. BKA vypracoval o této modifikované verzi zprávu, která stále zůstává v režimu utajení[662]. Úřad dále odpíral organizacím občanské společnosti přístup ke smlouvám se společnostmi poskytujícími spyware, dokud k tomu nebyl donucen soudem. I v takovém případě však smlouvy zveřejnil pouze v silně redigovaných

---

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

[652] Evropský parlament, Slyšení o Německu**.**

[653]Quellen-TKÜ (§ 100a StPO) byl schválen 25krát a proveden 14krát a Online-Durchsuchung (§ 100b StPO) byl schválen 23krát a proveden 8krát. Údaje byly získány z: 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.

[657] „Používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru: Stávající právní rámec v členských státech EU za získání a používání softwaru Pegasus a jiného ekvivalentního špionážního software“; 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/.

verzích[663]. Navzdory dvěma pozváním do výboru PEGA se úřad BKA nemohl z časových důvodů žádného slyšení zúčastnit.

366. V říjnu 2021 bylo rovněž zjištěno, že německá zahraniční zpravodajská služba Spolková zpravodajská služba (BND) rovněž zakoupila pozměněnou verzi softwaru Pegasus, ačkoli akvizice byla tajná[664]. V odpovědi na parlamentní otázku spolková vláda uvedla, že používání softwaru Pegasus je povoleno pouze v jednotlivých případech a musí splňovat přísné zákonné podmínky stanovené německým trestním řádem (StPO), zákonem o omezeních listovního tajemství, tajemství pošt a telekomunikací (zákon G-10) a zákonem o Spolkovém kriminálním úřadě (zákon o BKA), ale nechtěla se vyjadřovat konkrétněji[665].

POUŽÍVÁNÍ ŠPIONÁŽNÍHO SOFTWARU

367. V letech 2012 a 2013 spolkový úřad BKA i berlínský úřad LKA nezávisle na sobě zakoupily špionážní software FinSpy od společnosti FinFisher. I zde, stejně jako v případě softwaru Pegasus, BKA příslušnou společnost požádal, aby špionážní software FinFisher upravila v zájmu souladu s německým právem tak, aby neumožňoval přístup ke všem údajům v zařízení, ale pouze k přímé komunikaci. Úřad BKA nadále testoval nové verze špionážního softwaru poskytnutého společností FinFisher, aby mohl být používán pouze „legálně bezpečným a technicky čistým“ způsobem, a teprve po pěti letech v roce 2018 jej spolkové ministerstvo vnitra schválilo. Bylo to ve stejném roce, kdy bylo zjištěno používání softwaru FinFisher proti opozičním stranám v Turecku, zatímco Německo od roku 2015 nevydalo žádnou vývozní licenci na vývoz sledovacího softwaru do třetích zemí[666]. Smlouva mezi společností FinFisher a berlínskou policií však již v té době vypršela, takže policie v hlavním městě jej nikdy nepoužila. Úřad BKA se k žádnému použití softwaru od společnosti FinFisher při svých operacích dále nevyjádřil a ani se nevyjádřil k tomu, zda je smlouva stále platná[667].

368. V roce 2017 zahájil spolkový ministr vnitra činnost Ústředního úřadu pro IT v bezpečnostním sektoru (ZITiS) za účelem usnadnění výzkumu a vývoje hackingových nástrojů ze strany vlády, jakož i nákupu hackingových nástrojů od komerčních prodejců[668]. Dne 6. dubna 2022 se objevila zpráva, že agentura ZITiS hledá dostupné technologie jinde v reakci na to, že zdiskreditovaná spywarová společnost Finfisher podala oznámení o úpadku[669]. Zprávy hovořily mimo jiné o tom, že se od roku 2019 pětkrát[670] sešel s italskou společností zabývající se sledováním RCS Lab, ale nejsou

---

[663] Svědectví Andre Meistera, slyšení pro jednotlivé země týkající se Německa, schůze vyšetřovacího výboru pro prošetření používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru v Polsku, 14. listopadu 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.
[666] „Používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru: Stávající právní rámec v členských státech EU za získání a používání softwaru Pegasus a jiného ekvivalentního špionážního software“; 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] Odpověď na parlamentní otázku poslankyně Strany levice Martiny Rennerové https://dserver.bundestag.de/btd/20/038/2003840.pdf.

důkazy o tom, že by od RCS Lab nějaký nástroj zakoupil[671]. Kromě toho se úřad ZITiS seznámil se špionážními produkty rakouské společnosti DSIRF[672], izraelské Quadream[673] a Candiru[674] a posuzoval je.

369. V lednu 2023 pořad *Tagesschau* uvedl, že úřad ZITiS byl rovněž v kontaktu se společností Intellexa nebo její dceřinou společností Cytrox, ačkoli není jasné, zda byl spyware Predator nakonec zakoupen. Bývalý koordinátor tajných služeb Bernd Schmidbauer údajně vystupoval jako zástupce produktů společnosti Intellexa. Podle e-mailů z listopadu 2021 byl pan Schmidbauer v kontaktu s bývalým předsedou Spolkového úřadu pro bezpečnost informací Arne Schönbohmem a snažil se sjednat si schůzku se společností Intellexa. V únoru 2022 se pan Schmidbauer rovněž obrátil na ředitele ZITiS za účelem prezentace společnosti Intellexa. Kromě toho byl Schmidbauer v kontaktu s místopředsedou Spolkového úřadu pro ochranu ústavy (BfV), což údajně vedlo k tomu, že na začátku července 2022 byla společnost Intellexa představena zaměstnancům BfV . Vláda se k těmto schůzkám kvůli kontroverzní lobbistické činnosti pana Schmidbauera nevyjádřila[675]. V roce 2021 se pan Schmidbauer setkal také s Janem Marsalkem, který má vazbu na DSIRF[676].

MALTA

370. Na Maltě zaregistrovalo svou společnost několik klíčových aktérů obchodování se špionážním softwarem a několik jich získalo maltský pas. Zdá se však, že tam ve skutečnosti nežijí a tyto jejich společnosti nevykazují podle všeho žádnou činnost. Dosud bylo identifikováno několik takových významných osob.

371. Tal Dilian je izraelský občan, bývalý příslušník izraelské armády. Je zakladatelem společnosti Intellexa a žije na Kypru. V roce 2017 rovněž získal maltský pas[677]. Na Maltě také spoluvlastní společnost s názvem MNT Investments LTD[678].

372. Anatolij Hurgin je rusko-izraelský občan a bývalý izraelský vojenský inženýr. V roce 2015 rovněž získal maltský pas[679] Je zakladatelem společnosti Ability Ltd, která spolupracovala se společností NSO Group na softwaru Pegasus a zajišťovala síťovou stránku činnosti NSO[680]. V době, kdy žádal o maltský pas, byl již vyšetřován

---

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.
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 Osoby naturalizované/registrované jako občané Malty 2017, zveřejněno dne 21. prosince 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/.

americkými i izraelskými orgány pro různé trestné činy[681]. Investigativní novinářka Daphne Caruana Galiziová, která byla později v říjnu 2017 zavražděna, o něm v srpnu 2016 napsala[682]. V roce 2017 byla společnost Ability Ltd vyšetřována Komisí USA pro cenné papíry a burzu, protože údajně lhala o stavu svých financí, a burza NASDAQ ji rovněž téměř vyřadila z kótace[683]. Pan Hurgin údajně rovněž vlastní společnost v Litvě s názvem UAB „Communication technologies“ působící v oblasti „připojení a telekomunikačních služeb“[684]

373. Felix Bitzios je ředitel společnosti Baywest Business Europe Ltd se sídlem na Maltě[685], dříve byl majitelem a zaměstnancem společnosti Intellexa a podílel se na případu podvodu Piraeus/Libra[686];

374. Stanislaw Szymon Pelczar je právním zástupcem společnosti Baywest Business Europe Ltd, registrované na Maltě, a byl bývalým správcem společnosti Krikel. Jeho jméno je zmiňováno v souvislosti s Paradise Papers[687].

375. Peterh Thiel státní příslušník USA narozený v Německu, v roce 2011 získal občanství Nového Zélandu, přestože tam nežije. V roce 2022 požádal o maltský zlatý pas (krátce po oznámení založení nového společného podniku Kuze a Hulia)[688]. Je zakladatelem společnosti PayPal a kontroverzní společnosti Palantir (figuruje ve skandálu Cambridge Analytica). Je sponzorem Donalda Trumpa a prvním externím investorem Facebooku. Najal Sebastiana Kurze jako stratéga (který nedávno založil podnik s Shalevem Huliem, bývalým pracovníkem NSO)[689].

FRANCIE

SLEDOVANÉ OSOBY VE FRANCII

376. V roce 2021 projekt Pegasus odhalil, že ve Francii došlo k pokusům o napadení několika osob špionážním softwarem Pegasus[690]. Uniklý soubor údajů zahrnoval telefonní číslo prezidenta Emmanuela Macrona a telefonní čísla 14 členů jeho kabinetu[691] [692]. Výsledky forenzních analýz provedených francouzskou státní zpravodajskou službou potvrdily, že telefony ministra školství Jeana-Michela

[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.
[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.* (V telefonech novinářů byl nalezen špionážní software Pegasus, potvrdila francouzská rozvědka).
[691] The Guardian, *Spyware found on phones of five French cabinet members.* (V telefonech pěti členů francouzské vlády byl nalezen špionážní software).
[692] Euractiv, *France's Macron targeted in project Pegasus spyware case.* (Francouzský prezident Macron terčem útoku v kauze špionážního softwaru Pegasus)

Blanquera, ministryně pro územní soudržnost Jacqueline Gouraultaové, ministra zemědělství Juliena Denormandieho, ministryně bydlení Emmanuelle Wargonové a ministra zahraničních věcí Sebastiena Lecornua, byly nakaženy spywarem Pegasus[693]. Napaden byl také telefon poslance Adriena Quatennense[694].

377. Rejstřík podle projektu Pegasus údajně obsahoval také telefonní čísla dalších francouzských občanů, mezi nimiž byli novináři, bývalí politici a jejich příbuzní. Francouzská národní agentura pro bezpečnost informačních systémů (Agence nationale de la sécurité des systèmes d'information) potvrdila napadení softwarem Pegasus v mobilních zařízení patřících řediteli pařížské rozhlasové stanice TSF Brunu Delportovi, bývalému ministru Arnaudu Montebourgovi a investigativním novinářům Edwymu Plenelovi, Lénaïg Bredouxové a nejmenovanému novináři z Francie[695]. Kromě toho se terčem softwaru Pegasus stala i Claude Manginová – manželka Naâma Asfariho, saharského politického vězně v Maroku[696]. Dále se software Pegasus zaměřil také na pařížského obhájce několika aktivistů Fronty Polisario za Saharu Josepha Brehama[697].

378. Zdá se, že Maroko stojí za mnoha útoky na novináře i politiky ve Francii[698], včetně marockých novinářů žijících ve francouzském exilu, konkrétně investigativního novináře Hichama Mansouriho, který v roce 2016 uprchl před neustálým obtěžováním ze strany marockých orgánů, a nezávislého novináře Aboubakra Jamajho, který Maroko opustil v roce 2007[699].

379. Francie se údajně sama chystala koupit špionážní software Pegasus v roce 2021. V době závěrečných jednání se společností NSO Group vedla odhalení údajného používání špionážního softwaru proti francouzským vládním úředníkům k náhlému pozastavení prodeje[700]. Francouzské ministerstvo zahraničí popřelo, že by se společností NSO Group vedlo rozhovory[701].

380. Na schůzi výboru PEGA dne 9. ledna 2023 Serge Lasvignes, předseda Národního výboru pro kontrolu zpravodajských technik, uvedl, že rozhodnutí nepovolit používání Pegasus ve Francii bylo přijato před odhaleními projektu Pegasus. Podle pana Lasvignese francouzské zpravodajské služby využívají pouze produkty pro sledování vytvořené ve Francii, aby zabránily zahraničním výrobcům špionážního softwaru získat

---

693 The Guardian, Spyware found on phones of five French cabinet members. (V telefonech pěti členů francouzské vlády byl nalezen špionážní software).
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.
695 Haaretz, *The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.* (Spis NSO: Úplný (aktualizující) seznam osob sledovaných pomocí spyware Pegasus).
696 Haaretz, *The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.* (Spis NSO: Úplný (aktualizující) seznam osob sledovaných pomocí spyware 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*. (Vláda a celá francouzská politika v hledáčku Maroka).
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 se chystala prodat hackerské nástroje do Francie. Nyní se nachází v krizi).
701 MIT Technology Review, *NSO was about to sell hacking tools to France. Now it's in crisis.* (NSO se chystala prodat hackerské nástroje do Francie. Nyní se nachází v krizi).

přístup k informacím. Pan Lasvignes však upřesnil, že technické ředitelství, které vyrábí francouzský špionážní software, ve skutečnosti dováží některé díly od jiných než francouzských společností[702].

381. Žádosti o povolení sledování určité osoby musí ve Francii schválit nejprve generální ředitel útvaru a poté ministr vnitra. V konečném důsledku musí být všechny žádosti schváleny předsedou vlády. V současné době je ve Francii sledováno 23 000 osob, přičemž každý případ byl schválen předsedou vlády. Pokud si oběť přeje zjistit, zda je nebo byla sledována, je jí přístup ke spisům odepřen s ohledem na národní bezpečnost. Osoba může požádat o ověření soudcem. Soudce však může pouze rozhodnout, zda sledování bylo či nebylo legální, ale nemůže oběť informovat z důvodu otázky důvěrnosti národní obrany[703]. To znamená, že v praxi nemá právo na právní ochranu smysl, neboť důkazní břemeno nese jednotlivec a je prakticky nemožné od orgánů získat jakýkoli důkaz.

382. Podle brožury ISS z roku 2013 zástupci francouzského ministerstva vnitra, ministerstva obrany, Interpolu a velvyslanectví Toga ve Francii navštívili veletrh ISS World 2012, známý také jako „ples odposlouchávačů“. Podle seznamu ISS obsahujícího dodavatele a technologické integrátory byly na této akci přítomny následující francouzské společnosti zabývající se špionážním softwarem: 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 a WAHOUE AND PARTNERS[704].

SPOLEČNOSTI OBCHODUJÍCÍ SE ŠPIONÁŽNÍM SOFTWAREM VE FRANCII

383. Francie je domovem různých společností vyrábějících špionážní software, z nichž nejvýznamnější jsou Nexa Technologies a Amesys. Nexa Technologies, součást společnosti Intellexa Alliance Tala Diliana, je francouzská společnost založená v roce 2000, která se zabývá kybernetickou ochranou a zpravodajskou činností[705]. Ředitelem Nexa Technologies je jeden z bývalých manažerů společnosti Amesys. Společnost Amesys byla založena v roce 1979[706] a je známá prodejem programu Cerebro, který umožňuje zaznamenávat elektronickou komunikaci svých cílů, např. e-mailové adresy a telefonní čísla[707].

384. V roce 2007 společnost Amesys údajně tuto technologii pro sledování telekomunikací prodala Libyi a Kaddáfího režim ji využil k zatýkání a mučení kritiků režimu. Podle společnosti *Telerama* byla společnost Nexa založena s cílem změnit značku sledovacího softwaru a pokračovat v prodeji společnosti Amesys egyptskému režimu[708]. V roce 2014 společnost Nexa Technologies údajně prodala egyptskému režimu odposlouchávací systém pod názvem Eagle. Tento systém byl využíván v souvislosti se zadržením a mučením politických oponentů režimu al-Sísího[709]. Společnost Amesys

[702] Slyšení výboru PEGA ze dne 9. ledna 2022.
[703] Slyšení výboru PEGA ze dne 9. ledna 2022.
[704] ISS World, programový plán na rok 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, Vedoucí pracovníci společností Amesys a Nexa Technologies byli obviněni.
[709] Trial International, Amesys (Nexa Technologies).

Eagle instalovala a udržovala od roku 2007 do roku 2011[710].

385. Na společnosti Amesys i Nexa Technologies bylo podáno několik žalob. V říjnu 2011 podaly Mezinárodní federace pro lidská práva (FIDH) a Liga lidských práv (LDH) u pařížského vrchního soudu žalobu na společnost Amesys v souvislosti s údajným prodejem Libyi[711]. V létě 2013 bylo vyslechnuto pět libyjských cílů a v prosinci 2015 jeden libyjský cíl. Vzhledem k novým důkazům svědčícím o tom, že Kaddáfího režim používal technologii sledování společnosti Amesys, byla tato společnost v letech 2007 až 2011 oficiálně označena za svědka a spolupachatele mučení[712].

386. V roce 2010 byla společnost Amesys převzata francouzskou počítačovou firmou Bull. V roce 2014 společnost Atos, v té době vedená Thierrym Bretonem, převzala společnost Bull, a získala tak rovněž společnost Amesys[713]. Již v době převzetí byly známy pochybné aktivity společnosti Amesys v oblasti obchodu s autoritářskými režimy. Žaloba již byla podána.

387. V roce 2017 odhalila zpráva investigativních sdělovacích prostředků prodej systémů sledování Nexa Technologies Egyptu v roce 2014, což vyvolalo žalobu FIDH, LDH a Káhirského institutu pro studium lidských práv (CIHRS) proti této společnosti[714] [715].

388. V červnu 2021 pařížský soud na základě několika stížností organizací na ochranu lidských práv obžaloval čtyři vedoucí pracovníky společností Amesys a Nexa Technologies kvůli prodeji sledovacích technologií vládám Libye a Egypta[716]. Je znepokojující, že mezi první stížností a zahájením soudního řízení uplynulo celých deset let. Mezitím mohla společnost Amesys pokračovat ve své činnosti bez překážek, včetně výše uvedeného prodeje sledovacích technologií do Egypta.

389. Navzdory těmto kontroverzím podepsala francouzská d'Agence Nationale des Titres Sécurisés (ANTS) v říjnu 2016 se společností Amesys smlouvu v hodnotě více než 5 milionů EUR na technickou správu databáze TES (obsahující osobní údaje a biometrické údaje všech francouzských občanů). Toto rozhodnutí francouzských orgánů zapojit společnost Amesys, která je již známá svými praktikami, do takového projektu bylo předmětem kritiky. Ačkoli by společnost Amesys neměla plnou kontrolu nad systémy používanými pro kontroverzní databázi TES, byla by nápomocna projektovým manažerům agentur, kteří se zabývají souborem TES, takže nelze vyloučit, že společnost Amesys bude mít přístup k osobním údajům. Ředitel úřadu ANTS se však domníval, že proti uzavření obchodu se společností Amesys neexistují žádné právní námitky[717].

390. Ve Francii je poskytování vývozních licencí kontrolováno službou pro zboží dvojího užití (SBDU) ministerstva hospodářství, průmyslu a digitálních záležitostí. Kromě toho

[710] ZDNet, Vedoucí pracovníci společností Amesys a Nexa Technologies byli obviněni.
[711] Trial International, Amesys (Nexa Technologies).
[712] Trial International, Amesys (Nexa Technologies).
[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, Vedoucí pracovníci společností Amesys a Nexa Technologies byli obviněni.
[716] *Amnesty, Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture* (Vedoucí pracovníci sledovacích společností Amesys a Nexa Technologies obviněni ze spoluúčasti na mučení).
[717] L'Obs, *Amesys file un coup de main à l'agence en charge du fichier monstre*.

meziministerská komise pro zboží dvojího užití, jíž předsedá ministerstvo pro Evropu a zahraniční věci, kontroluje citlivější zboží dvojího užití. V době vypracování tohoto dokumentu nebyly k dispozici žádné informace o udělení vývozních licencí ze strany francouzské vlády pro společnost Nexa Technologies.

IRSKO

391. Irsko je členským státem, v němž se zaregistrovaly některé z nevýznamnějších společností odvětví špionážních technologií zapletené do skandálů. Důvodem byly irské daňové zákony. Dne 20. září 2022 odhalil irský vydavatelský dům zaměřený na investigativní žurnalistiku *The Currency*, že jak společnost Thalestris Limited, mateřská společnost společnosti Intellexa, tak samotná Intellexa mají v Irsku své sídlo a jsou registrovány u advokátní kanceláře ve městě Balbriggan. Je pozoruhodné, že žádost o zřízení společnosti Thalestris Limited v Irsku podal v listopadu 2019 specialista na zakládání společností, a to pouze 12 dnů poté, co bylo kyperskými orgány veřejně oznámeno, že probíhá trestní vyšetřování Tala Diliana a jeho společnosti WiSpear. Sám Tal Dilian, generální ředitel společnosti Intellexa, v listinách irské společnosti nefiguruje, ale jeho údajná druhá manželka Sara Hamouová je uvedena jako ředitelka společnosti Thalestris i Intellexa[718].

392. Z účetních závěrek zveřejněných společností Thalestris za období končící dnem 31. prosince 2020 vyplývá, že v Řecku, na Kypru, ve Švýcarsku a na Britských Panenských ostrovech existuje dalších 10 dceřiných společností a že společnost Thalestris není povinna platit žádnou daň z příjmu právnických osob. Použila řadu daňových předpisů rovněž používaných nadnárodními společnostmi působícími v Irsku, a byla proto technicky ztrátová[719].

393. Irská vláda odmítla odpovědět na otázku, zda se na ni nebo donucovací orgány obrátily společnosti Thalestris nebo Intellexa, nebo zda někdy využily jejich služeb s tím, že: „Z řádných provozních důvodů a z důvodů národní bezpečnosti by nebylo vhodné vyjadřovat se k podrobnostem vnitrostátních bezpečnostních opatření, ani by nebylo vhodné zveřejnit opatření ministerstva v oblasti kybernetické bezpečnosti nebo opatření státních úřadů, agentur a subjektů spadajících do působnosti ministerstva.“ Irská vláda rovněž odmítla komentovat případné irské vazby na špionážní software vyráběný společnostmi Thalestris a Intellexa[720]. Nejsou veřejně známy žádné důkazy o zneužívání špionážního softwaru v Irsku.

394. Deník *Haaretz* odhalil, že společnost GoNet Systems, která se podílela na poskytování služeb infrastruktury Wi-Fi na letišti Larnaka a která byla napojena na společnost WiSpear pana Diliana a v roce 2022 byla uzavřena, měla v Irsku rovněž korporátní

[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/.

majetek[721].

395. V lednu 2023 bylo oznámeno, že Výbor Oireachtasu pro spravedlnost má na základě dopisu poslance Evropského parlamentu Barryho Andrewse prověřit existenci společností, které se v Irsku podílejí na výrobě spywaru. Výbor uvedl, že se touto otázkou zabýval na neveřejném zasedání dne 18. ledna a souhlasil se zařazením tohoto tématu do svého pracovního programu na rok 2023[722].

396. Je třeba poznamenat, že irské právo obchodních společností je průběžně přezkoumáváno a pravidelně aktualizováno, aby se zvýšila transparentnost obchodních struktur. Příkladem může být zákon o společnostech (orgánu pro prosazování korporátního práva) z roku 2021, který aktualizoval režim prosazování práva a jehož nadcházející aktualizace se očekává v roce 2023, a návrh zákona o různých ustanoveních (transparentnost a registrace komanditních společností a obchodních názvů) z roku 2023. Irská vláda dále oznámila další investice do Národního centra kybernetické bezpečnosti (NCSC) s cílem zvýšit jeho schopnost aktivně odhalovat a potírat kybernetické hrozby zaměřené na kritickou infrastrukturu a kritické sítě prostřednictvím různých prostředků. Schopnost NCSC monitorovat incidenty a reagovat na ně bude rozvíjena prostřednictvím pokračujícího vývoje Společného bezpečnostního operačního střediska (JSOC) a rozšířených analytických a ohlašovacích schopností. Pokračuje rovněž práce na vývoji technologické strategie NCSC s externími konzultanty[723].

LUCEMBURSKO

397. Lucembursko hostí devět subjektů přímo souvisejících se společností NSO Group, jak odhalila organizace Amnesty International v červnu 2021 a později potvrdil lucemburský ministr zahraničních věcí Jean Asselborn[724]. Skutečnost, že názvy devíti společností (jako Triangle Holdings SA, Square 2 SARL a Q Cyber Technologies SARL), které zastřešuje management a soukromá kapitálová společnost Novalpina Capital, neprozrazují hned spojení se společností NSO Group, ukazuje, jak neprůhledné obchodní struktury v Lucembursku umožňují společnostem působit zcela mimo dohled veřejnosti.

398. Po odhalení Amnesty o devíti subjektech NSO v Lucembursku v červnu 2021 zaslal ministr zahraničí Jean Asselborn každému z nich dopis, v němž je vyzval, aby se zdrželi jakéhokoli rozhodování, které by mohlo vést k nezákonnému využívání zboží a technologií, jež poskytují svým zákazníkům. Podle deníku LuxTimes společnost NSO Group odpověděla, že vyváží svůj špionážní software z Izraele pouze se souhlasem izraelské vlády, ale v říjnu 2021 pan Asselborn uvedl, že tuto skutečnost nemůže ověřit[725]. V každém případě podle ministra žádný z devíti subjektů nebyl oprávněn vyvážet zboží kybernetického dohledu z Lucemburska, jelikož Lucembursko neudělilo

[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/.
[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.

žádnou vývozní licenci[726]. „Lucembursko nebude za žádných okolností tolerovat, že vývozní operace ze země přispívají k porušování lidských práv ve třetích zemích, a případně zajistí přijetí nezbytných opatření k nápravě jakéhokoli porušování lidských práv a k zabránění jejich porušování v budoucnu," uvedl Asselborn[727]. Společnost NSO Group je však stále schopna fungovat díky subjektům se sídlem v Lucembursku, jako je společnost Q Cyber Technologies, která odpovídá za vyřizování faktur, smluv a plateb od zákazníků svého softwaru[728]. Dne 24. srpna 2022 bylo zjištěno, že NSO Group zaúčtovala více než polovinu svých prodejů v předchozích dvou letech v Lucembursku, což jasně ukázalo, že Lucembursko funguje jako důležité obchodní centrum pro NSO Group[729].

399. V říjnu 2021 premiér Xavier Bettel potvrdil, že Lucembursko koupilo a používalo Pegasus „z důvodů státní bezpečnosti"[730].

ITÁLIE

400. Zatím nejsou k dispozici žádné zprávy o tom, že by špionážní software zakoupily italské orgány. Nebyly hlášeny žádné případy špionáže na vysoké úrovni, ačkoli telefonní číslo bývalého předsedy vlády a předsedy Komise Romana Prodiho bylo uvedeno na seznamu zveřejněném v rámci projektu Pegasus[731]. Jako bývalý zvláštní vyslanec OSN pro oblast Sahelu mohl být Prodi pro Maroko zajímavým cílem vzhledem ke svým možným kontaktům s vysoce postavenými činiteli v Západní Sahaře nebo Alžírsku.

401. Společnosti prodávající špionážní software, Tykelab a RCS Lab, si však vybraly Itálii jako základnu pro podnikání.

402. Další společností nabízející ofenzivní intrusivní software z Itálie přinejmenším od roku 2012 byla Hacking Team, nyní nazývaná Memento Labs. Společnost se stala nechvalně známou po hackerském útoku, který odhalil prodej několika autoritářským zemím, které použily špionážní software RCS k útokům na politické disidenty, novináře a obránce lidských práv. Vyšetřování vývozu špionážního softwaru RCS do Súdánu, které zahájily nevládní organizace a vyšetřovatelé OSN, nakonec vedlo italské orgány k tomu, že z důvodu obav o lidská práva zavedly v rámci italského vývozního práva univerzální ustanovení, a společnost tak musela žádat o individuální povolení pro každý vývoz. Společnost Hacking Team nejen odmítla spolupracovat během šetření, ale využila také svých úzkých vztahů s vyššími představiteli vlády, zpravodajských služeb a donucovacích orgánů v Itálii, aby se stal aktivem národní bezpečnosti a nakonec vyvíjel nátlak na ministerstvo pro hospodářský rozvoj, aby jim znovu udělilo celkovou licenci

[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.
[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/.

pro vývoz[732].

RAKOUSKO

403. V odpovědi na písemné otázky rakouského parlamentu rakouská spolková vláda uvedla, že Rakousko není klientem společnosti NSO[733]. Bývalý kancléř Sebastian Kurz má však na zakladatele této skupiny úzké vazby a v Rakousku navíc sídlí významný dodavatel špionážního softwaru, společnost DSIRF.

404. Po své rezignaci byl pan Kurz následně najat jako globální strategický pracovník pro Thiel Capital, jehož vlastníkem je miliardář Peter Thiel[734]. V říjnu 2022 založili Sebastian Kurz a Shalev Hulio (zakladatel NSO Group) firmu pro kybernetickou bezpečnost nazvanou Dream Security[735]. Ačkoli pan Hulio odstoupil z funkce výkonného ředitele NSO Group v srpnu 2022, Dream Security a NSO Group mají úzké vazby prostřednictvím různých osobností a obchodních vazeb. Jeden z jejích investorů, Adi Shalev, byl rovněž počátečním investorem do NSO. Gil Dolev je dalším zakládajícím členem společnosti Dream Security. Sestra Doleva Shiri Dolevová je ředitelkou NSO Group. Shalev Hulio dříve nabyl jednu ze společností Gil Doleva[736].

405. V červenci 2022 provozovatelé používali špionážní software z rakouské společnosti DSIRF k hackerským útokům na právnické firmy, banky a poradenské firmy v Rakousku, Panamě a Spojeném království. Podle výzkumných pracovníků společnosti Microsoft používá nástroj „Subzero“ společnosti DSIRF pro přístup k důvěrným informacím, jako jsou hesla a další přihlašovací údaje[737]. V říjnu 2022 spolkové ministerstvo práce a hospodářství uvedlo, že si není vědomo žádných žádostí o vývozní licence ze strany DSIRF a že za posledních 10 let nebyla podána žádná žádost o vývoz „intrusivního softwaru“[738]. Vzhledem k tomu, že společnost DSIRF neměla vývozní licenci na vývoz softwaru, zahájilo vídeňské státní zastupitelství předběžné vyšetřování pro podezření z nezákonného přístupu k počítačovému systému podle rakouských právních předpisů.

ESTONSKO

406. Také Estonsko mělo údajně zájem o nákup špionážního softwaru Pegasus společnosti NSO Group. Počáteční jednání mezi Estonskem a společností NSO Group proběhla v

---

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 Odpovědi bývalého ministra vnitra Karla Nehammera poslanci Národní rady Nikolausi Scherakovi, 22. září 2021, čj. 2021-0.580.421.

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 Studie s názvem *„Pegasus and the EU's external relations“*, (Pegasus a vnější vztahy EU) Evropský parlament, generální ředitelství pro vnitřní politiky, tematická sekce C – Občanská práva a ústavní záležitosti, 25. ledna 2023, s. 52 Microsoft (2022), *Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits* (Rozplétání aféry KNOTWEED: Evropský útočný aktér ze soukromého sektoru využívající tzv. útoky nultého dne).

738 https://www.parlament.gv.at/dokument/XXVII/AB/11698/imfname_1473647.pdf.

roce 2018 a na jejich základě Estonsko zaplatilo zálohu na nákup sledovacího softwaru v hodnotě 30 milionů USD[739].

407. O rok později však představitel ruské obrany Izrael informoval o estonském záměru používat špionážní software Pegasus na ruských telefonních číslech. Tyto informace vedly izraelské ministerstvo obrany k tomu, aby Estonsku zablokovalo špionáž jakýchkoli ruských zařízení po celém světě, přičemž uvedlo, že dohoda by poškodila izraelsko-ruské vztahy[740]. Případ Estonska zdůrazňuje, že špionážní software Pegasus není pouze sledovací zbraní, ale slouží také jako politická měna v diplomatických vztazích.

LITVA

408. Litevskou společnost UAB Communication Technologies, která působí v oblasti spojovacích a telekomunikačních služeb, vlastní Anatolij Hurgin, rusko-izraelský občan, bývalý izraelský vojenský inženýr a spolu s NSO spolutvůrce systému Pegasus[741]. V roce 2015 rovněž získal maltský zlatý pas[742].

BULHARSKO

409. V Bulharsku jsou kontroly vývozu a vývozní licence u produktů, které jsou nařízením EU o dvojím užití klasifikovány jako zboží dvojího užití, pod dohledem ministerstva hospodářství, konkrétně meziministerské komise pro kontrolu vývozu a nešíření zbraní hromadného ničení[743]. Současným ministrem hospodářství a průmyslu je Nikola Stojanov[744]. Bulharské orgány popírají, že by společnosti NSO Group nebo jejím dceřiným společnostem udělily vývozní licence[745]. Bývalý soukromý vlastník této společnosti, investiční firma Novalpina Capital, však zdůraznil, že k vývozu produktů NSO z EU dochází jak z Kypru, tak z Bulharska[746] [747] [748]. Tato dvě tvrzení jsou tedy ve vzájemném rozporu. Kromě toho média tvrdí, že některé servery síťové infrastruktury, přes kterou jsou vedeny útoky Pegasus, se nacházejí v bulharském datovém centru vlastněném bulharskou společností. Tato společnost je vlastněna společnostmi NSO Group, Circles Bulgaria a Magnet Bulgaria, které od úřadů obdržely vývozní licence. Tato dceřiná společnost NSO Group poskytuje z Bulharska kyperským dceřiným společnostem služby v oblasti výzkumu a vývoje a vyváží síťové produkty vládám[749].

---

[739] The New York Times, „*Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia* (Izrael ze strachu z ruské reakce zablokoval špionážní software pro Ukrajinu a Estonsko)“, 23. března 2022.
[740] The New York Times, „*Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia* (Izrael ze strachu z ruské reakce zablokoval špionážní software pro Ukrajinu a Estonsko)“, 23. března 2022.
[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] Bulharská republika, Ministerstvo hospodářství a průmyslu, Meziministerská komise pro kontrolu vývozu a nešíření zbraní hromadného ničení.
[744] Rada ministrů Bulharské republiky.
[745] Politico, „*Pegasus makers face EU grilling. Here's what to ask them*,“ (Tvůrci softwaru Pegasus čelí tvrdému výslechu v EU. Na co se jich zeptat?) 21. června 2022.
[746] Amnesty International, „Odpověď společnosti Novalpina Capital na otevřený dopis koalice nevládních organizací“, 18. února 2019.
[747] Access Now, „*Is NSO Group's infamous Pegasus spyware being traded through the EU?*“ (Je nechvalně známý spyware Pegasus společnosti NSO Group obchodován prostřednictvím EU?), 12. září 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*.“ (Aktivita ze zákulisí: uvnitř podnikové struktury NSO Group)

Společnost Magnet je v současné době v útlumu, ale Circles je stále aktivní a obdržela vývozní licenci, která je platná do 25. dubna 2023[750].

410. V únoru 2022 zahájila Sofijská městská prokuratura vyšetřování, jehož cílem bylo zjistit, zda státní služby nelegálně používaly špionážní software Pegasus ke sledování bulharských občanů. Vyšetřování stále probíhá[751]. V lednu ve věci *Ekimdzhiev a další* v. *Bulharsko* ESLP shledal, že stávající právní předpisy v Bulharsku týkající se tajného sledování a uchovávání sdělení a přístupu ke komunikaci nesplňují požadavky úmluvy na kvalitu, a požádal vládu, aby provedla nezbytné změny vnitrostátního práva za účelem ukončení porušování[752]

I.G. Orgány EU

POKUSY O SLEDOVÁNÍ ÚŘEDNÍKŮ EVROPSKÉ KOMISE

411. Dne 11. dubna 2022 agentura Reuters oznámila, že komisař pro spravedlnost Didier Reynders a nejméně čtyři zaměstnanci Komise byli v listopadu 2021 napadeni softwarem Pegasus[753]. 23. listopadu 2021 společnost Apple odeslala na zařízení komisaře Reynderse a „dalších zaměstnanců Komise“ oficiální oznámení, v němž je informovala, že se stali „cílem státem sponzorovaných útočníků“ a jejich zařízení mohla být kompromitována[754].

412. V návaznosti na tato odhalení byl komisař Reynders vyzván, aby 30. května 2022 vystoupil před výborem PEGA, a rovněž písemně odpověděl na jeho otázky. Již 19. července 2021, po odhaleních Forbidden Stories a Amnesty International, Komise zřídila „specializovaný tým interních odborníků, který byl pověřen interním vyšetřováním“, aby „ověřil, zda byla terčem softwaru Pegasus i zaměstnanců Komise a komisařů“[755]. Komise také v září 2021 nasadila na všech služebních telefonech řešení pro detekci a reakci na mobilní koncové body (EDR), které pomáhá službám Komise identifikovat potenciálně infikovaná služební mobilní zařízení.

413. V průběhu šetření Komise sdělila, že „ani ... před tímto datem ani po něm [23. listopadu 2021]“ tyto kontroly nepotvrdily, že by osobní nebo služební zařízení komisaře Reynderse byla ohrožena. Příslušné útvary Komise rovněž zkontrolovaly zařízení ostatních zaměstnanců, kteří ve stejný den obdrželi od společnosti Apple podobná oznámení, ale „ani jedno z kontrolovaných zařízení nepotvrdilo podezření společnosti Apple“[756].

---

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 a další v. Bulharsko, žádost č. 70078/12, rozsudek ze dne 11. ledna 2022, dostupné na: https://hudoc.echr.coe.int/fre?i=001-214673.

753 https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/.

754 Dopis komisařů Hahna a Reynderse s odpovědí adresovaný zpravodaji – 25. července 2022; Dopis komisařů Hahna a Reynderse s odpovědí adresovaný výboru PEGA – 9. září 2022

755 Dopis komisařů Hahna a Reynderse s odpovědí adresovaný zpravodaji – 25. července 2022.

756 Dopis komisařů Hahna a Reynderse s odpovědí adresovaný výboru PEGA – 9. září 2022

414. Komise však ve svém dopise ze dne 9. září 2022 uznala, že v průběhu probíhajícího vyšetřování zaměřeného na Komisi pomocí programu Pegasus „několik kontrol zařízení vedlo k odhalení ukazatelů napadení“. Komise dosud výsledky svého vyšetřování dále nerozváděla, a to ani veřejně, ani ve výboru PEGA, protože „by protivníkům prozradily vyšetřovací metody a možnosti Komise, čímž by vážně ohrozily bezpečnost orgánu“[757]. Neoficiální zprávy o více než 50 zjištěných napadeních nebyly Komisí potvrzeny.

415. Na otázku výboru PEGA, který aktér nebo aktéři by mohli stát za těmito útoky, Komise odpověděla, že „není možné s plnou jistotou přiřadit tyto ukazatele konkrétnímu pachateli“. Dva z úředníků Komise, o nichž je známo, že se stali terčem sledování, komisař Reynders a člen kabinetu komisařky Věry Jourové[758], se však zabývají týmž ústředním tématem, a sice záležitostmi právního státu. V odpovědi na otázku výboru PEGA ohledně možné souvislosti Komise odmítla sdělit další informace o počtu oddělení, která mohla být napadena, o profesích postižených zaměstnanců nebo jakékoli další informace, které by byly pro práci výboru PEGA zajímavé a mohly by určit původ útoku, a uvedla, že „nemá k dispozici dostatek informací, které by nám umožnily vyvodit definitivní závěry o souvislosti mezi geolokací a možným pokusem o napadení zařízení prostřednictvím systému Pegasus“[759].

416. S ohledem na výše uvedené lze identifikovat několik problémů. Zaprvé, Komise neprokázala dostatečné povědomí a pochopení obrovských politických rizik, která jsou spojena s tím, že se stala terčem spywaru. Jakýkoli pokus o hackerský útok, ať úspěšný, či nikoliv, na Komisi nebo jednoho či více z jejích členů, je velmi závažnou politickou skutečností, která ovlivňuje integritu demokratického rozhodovacího procesu. Při jednáních s výborem PEGA Komise opakovaně uvedla, že pokus o napadení telefonu komisaře Reynderse softwarem Pegasus nebyl úspěšný. Jak však sama Komise uvedla, „několik kontrol zařízení [zaměstnanců] vedlo k odhalení indicií o napadení“, o čemž nebylo dále informováno. Zdá se, že Komise bagatelizuje závažnost útoku na orgán EU.

417. Za druhé se zdá, že neexistují dostatečné kapacity a schopnosti v oblasti IT, které by chránily komisaře a zaměstnance před útoky nebo monitorovaly a ověřovaly jejich kybernetickou bezpečnost. Přestože Komise zavedla nová opatření, jako je řešení EDR, na všech telefonech Komise a průběžně spolupracuje s CERT-EU[760], vzhledem k nedostatku informací, které výbor PEGA od Komise obdržel, není jasné, do jaké míry byla opatření Komise k analýze předchozích útoků spywaru úspěšná a do jaké míry budou zavedená opatření v budoucnu dostatečná.

418. Zatřetí, Komise oficiálně nenahlásila oznámení ani indicie belgické policii za účelem dalšího vyšetřování, ale v rámci „pravidelné spolupráce“ byla s belgickou policií v kontaktu pouze ohledně „technických detailů“. Komise prohlásila, že „oznámení tohoto druhu dostávají příslušná oddělení IT Komise několikrát denně“, a proto nemá smysl oficiálně je hlásit policii. Podle Komise, jelikož oznámení společnosti Apple nesignalizovalo „definitivní napadení, ale možnost pokusu malwaru zaměřit se na příslušné zařízení“, Komise nepodnikla následné kroky s orgány činnými v trestním řízení[761].

[757] https://pro.politico.eu/news/148627.
[758] https://pro.politico.eu/news/148627.
[759] Dopis komisařů Hahna a Reynderse s odpovědí adresovaný výboru PEGA – 9. září 2022
[760] Dopis komisařů Hahna a Reynderse s odpovědí adresovaný výboru PEGA – 9. září 2022
[761] Dopis komisařů Hahna a Reynderse s odpovědí adresovaný výboru PEGA – 9. září 2022

V jiných případech, například ve Španělsku a Francii, bylo zahájeno trestní vyšetřování použití špionážního softwaru vůči vládním ministrům a hlavám států. Spyware používají především státní subjekty s odvoláním na národní bezpečnost. Komise tvrdí, že „některé aspekty související s národní bezpečností nespadají do pravomoci Komise“[762], ale už nevysvětluje, jak by komisaři a zaměstnanci Komise mohli ohrožovat národní bezpečnost.

419. Za čtvrté, skutečnost, že Komise neposkytla výboru PEGA smysluplné informace, a to ani *neveřejně* o zaměření Komise, ani obecněji žádné základní informace týkající se vyšetřování, znamená, že Parlament nemohl řádně vykonávat demokratickou kontrolu. Komise by měla přehodnotit, jaké informace může zveřejnit, aby umožnila smysluplný parlamentní dohled.

ZACÍLENÍ NA ČLENY EVROPSKÉ RADY, RADY A KOMISE

420. Terčem útoku byl nejen jeden současný člen Komise a další zaměstnanci Komise, ale také vládní představitelé, ministři a bývalý komisař, kteří byli údajně napadeni špionážním softwarem zvenčí i zevnitř Unie.

421. Telefonní číslo francouzského prezidenta Macrona se objevilo na seznamu potenciálních cílů sestaveném projektem Pegasus a španělská vláda potvrdila, že telefony španělského premiéra Pedra Sáncheze, ministryně obrany Margarity Roblesové a ministra vnitra Fernanda Grande-Marlasky byly infikovány špionážním softwarem Pegasus, údajně ze zemí mimo Unii.

422. Podle řeckých novin Documento, které zveřejnily rozsáhlý seznam osob, u nichž byly údajně nalezeny stopy Predatoru v jejich zařízeních[763], Dimitris Avramopulos, který byl v letech 2014 až 2019 evropským komisařem, a několik současných ministrů vlády, včetně ministra zahraničních věcí a ministra financí, byli terčem spywaru. Není jasné, zda k údajným pokusům o hackerský útok na pana Avramopulose došlo v době, kdy byl členem Komise, ani kdo za nimi stál. Na dlouhém seznamu osob, proti nimž byl útok namířen, je však řada řeckých politiků z vládní i opoziční strany. 432. Tato potvrzená a údajná napadení a pokusy o hackerské útoky ukazují, že je možné, aby se současní vládní představitelé a ministři a současní nebo bývalí komisaři, včetně jejich komunikace s kolegy, stali terčem útoků zvenčí nebo zevnitř Unie v době, kdy jsou členy Evropské rady, Rady a Komise. Jeden napadený telefon by proto mohl vážně ohrozit informace, které mají orgány k dispozici, včetně informací sdílených během zasedání Komise a Rady v reálném čase.

I.H. Třetí země

423. V následující části bude zdůrazněno, do jaké míry používání softwaru Pegasus nebo obdobného špionážního softwaru, do něhož jsou přímo či nepřímo zapojeny subjekty spojené s EU, pomohlo k nezákonné špionáži novinářů, politiků, zaměstnanců donucovacích orgánů, diplomatů, právníků, podnikatelů, aktérů občanské společnosti, obránců lidských práv nebo jiných aktérů ve třetích zemích. To zahrnuje i to, do jaké

[762] Dopis komisařů Hahna a Reynderse s odpovědí adresovaný zpravodaji – 25. července 2022.
[763] Documento, vydání ze dne 6. listopadu 2022.

míry vedlo nasazení špionážního softwaru k porušování lidských práv, které vzbuzuje vážné obavy, pokud jde o cíle společné zahraniční a bezpečnostní politiky EU, a zda bylo takové použití špionážního softwaru v rozporu s hodnotami zakotvenými v článku 21 SEU a v Listině, a to i s náležitým ohledem na obecné zásady OSN v oblasti podnikání a lidských práv a další práva zakotvená v mezinárodním právu v oblasti lidských práv.

424. Mezi třetími zeměmi, které se zabývají špionážním softwarem, se zvláštní pozornosti ze strany výboru PEGA dostalo Izraeli a Maroku. V červenci 2022 proběhlo slyšení a pracovní cesta do Izraele a v únoru 2023 se uskutečnilo slyšení zasedání věnované Maroku během slyšení o geopolitice špionážního softwaru. Kromě toho byla v srpnu 2022 část jednoho slyšení věnována Rwandě a vystoupila na něm Carine Kanimba, která byla cílem programu Pegasus.

IZRAEL

425. Výbor PEGA navštívil Izrael v červenci 2022. Hlavním cílem cesty bylo setkání s výrobcem špionážního softwaru Pegasus, izraelskou společností NSO Group. Delegace výboru PEGA se dozvěděla, že společnost NSO Group prodala špionážní software 14 vládám EU s využitím vývozních licencí vydaných izraelskou vládou. Diskutovalo se o zneužívání námezdních sledovacích nástrojů a jejich dopadu na demokracii, právní stát a základní práva v EU. Výbor se rovněž setkal se zástupci vlády, Knesetu, odborníků a občanské společnosti. Tato návštěva zdůraznila neúčinnost stávajících ochranných opatření proti zneužívání špionážního softwaru a potřebu mnohem přísnější regulace jeho prodeje, nákupu a používání ze strany Evropské unie. Oblast kybernetického zpravodajství je třeba účinně regulovat, aby se v budoucnu zabránilo zneužívání špionážního softwaru.

426. Geopolitická a bezpečnostní situace Izraele přiměla jeho vládu a soukromý sektor k vývoji nástrojů pro shromažďování zpravodajských informací, které by rozšířily možnosti kybernetické bezpečnosti země, zejména pokud jde o její obranu. Izrael se v průběhu let stal jedním z předních světových výrobců pokročilých sledovacích technologií a špionážního softwaru, protože má značné zkušenosti s vývojem nástrojů pro shromažďování zpravodajských informací. Toto odvětví vyváží své výrobky do celého světa. Studie zadaná Evropským parlamentem a zveřejněná v roce 2023 pod názvem Pegasus a vnější vztahy EU uvádí, že „pro vyvážející země může být odvětví špionážního softwaru lukrativním zdrojem příjmů a pákou diplomatického vlivu“[764]. To potvrzují i zprávy, v nichž odborníci zdůrazňují užitečnost programu Pegasus při navazování diplomatických vztahů, tj. se státy Perského zálivu[765].

427. Kromě strategických domácích důvodů se Izrael úspěšně prosazuje jako inovativní země začínajících podniků, kde působí firmy s nejmodernějšími technologiemi v oboru, jako jsou NSO, Cellebrite, Candiru, QuaDream a Intellexa. Kolektivní tržby tohoto odvětví se odhadují na nejméně 1 miliardu USD ročně[766] a dosahují zhruba 0,6 %

[764] „*Pegasus and the EU's external relations*“, (Pegasus a vnější vztahy EU) Evropský parlament, generální ředitelství pro vnitřní politiky, tematická sekce C – Občanská práva a ústavní záležitosti, 25. ledna 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.

izraelského vývozu[767]. Izraelské obranné složky a zpravodajská služba, zejména její divize pro kybernetickou bezpečnost „oddělení 8200“, hrají klíčovou úlohu pro úspěšný izraelský průmysl špionážního softwaru a mnoho izraelských firem s ní udržuje úzké vztahy. Podle studie z roku 2018 bylo 80 % z 2 300 lidí, kteří založili 700 izraelských společností zabývajících se kybernetickou bezpečností bývalými zaměstnanci zpravodajských jednotek izraelských obranných sil. Jednou z jejích nejvýznamnějších postav v odvětví je majitel a zakladatel společnosti Intellexa Tal Dilian (viz oddíl Intellexa a Tal Dilian)[768].

428. Izraelské špionážní společnosti prodaly sledovací technologie do celého světa, včetně 14 členských států EU a autoritářských zemí Perského zálivu. Podle listu Haaretz byl prodej softwaru Pegasus použit jako diplomatický trumf a usnadnil jednání o navázání oficiálních diplomatických styků s Marokem, Bahrajnem a formálně i se Spojenými arabskými emiráty v rámci Abrahámovských dohod[769]. Prodej špionážního softwaru autoritářským režimům byl kritizován, zejména v rámci projektu Pegasus. V důsledku toho izraelská vláda v prosinci 2021 zpřísnila pravidla pro vývoz vybavení pro kybernetickou válku. V souvislosti s plánovanou revizí izraelského soudnictví údajně Řecko, Kypr a Portugalsko nabízejí mnoha izraelským technologickým společnostem pobídky k přesídlení jejich podniků do těchto zemí. Podle zpráv médií tyto tři země údajně nabízejí izraelským technologickým společnostem daňové úlevy a Řecko údajně nabízí urychlené udělení občanství[770].

429. Podle odborníků vytváří připravenost Izraele testovat nové sledovací systémy na Palestincích na okupovaných územích pobídky pro obchodní model v oblasti sledování, z něhož těží i NSO[771]. V důsledku toho země, které získávají od Izraele špionážní software „vytrénovaný v praxi“, přispívají k porušování lidských práv ve výše uvedených regionech. Členské státy EU, které patří mezi nejprestižnější klienty NSO, se tedy ocitají v přímém rozporu s programem zahraniční a bezpečnostní politiky EU, pokud jde o podporu lidských práv a demokracie[772].

430. Špionážní software Pegasus společnosti NSO byl použit k útoku na palestinskou občanskou společnost, mimo jiné na šest palestinských obránců lidských práv[773]. V případech Ubaje Al-Abudiho, výkonného ředitele Bisanského centra pro výzkum a rozvoj, a Salaha Hammuriho, francouzsko-palestinského státního příslušníka s dvojí

---

[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.

[769] Haaretz (2022) „*Netanyahu Used NSO Pegasus for Diplomacy*“ (Netanjahu využíval software Pegasus společnosti NSO k diplomacii), https://www.haaretz.com/israel-news/2022-02-05/ty-article/.premium/netanyahu-used-nsos-pegasus-for-diplomacy-now-he-blames-it-for-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] Mise výboru PEGA do Izraele, 18. až 20. července 2022.

[772] V souladu s většinou závěrů výroční zprávy Komise za rok 2021 o uplatňování Listiny základních práv EU „Ochrana základních práv v digitálním věku“ je EU povinna usnadnit práci osob zabývajících se ochranou lidských práv online.

[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/.

příslušností, právníka a terénního výzkumníka sdružení Addameer Prisoner Support and Human Rights Associations, vedlo použití sledovacího špionážního softwaru zřejmě k jejich administrativnímu zadržení. Sledování všech šesti osob se časově shoduje s velmi kontroverzním označením šesti palestinských lidskoprávních organizací za „teroristické“, což vyvolalo mezinárodní protesty odsuzující rozhodnutí izraelské vlády. Případ sledování palestinských obránců lidských práv je dalším důkazem nedostatečného prosazování politiky lidských práv společnosti NSO[774], kterou společnost využívá k posílení své legitimity a důvěryhodnosti při prodeji do členských států EU.

431. Je třeba uvést, že Komise jednala s izraelskými orgány ohledně zpráv o zneužívání špionážního softwaru Pegasus společnosti NSO Group k porušování lidských práv. V dopise výboru PEGA ze dne 9. září 2022 Komise odpověděla, že se izraelskými vývozními orgány zabývala obavami z možného zneužití a „požádala o informace o případných souvisejících zmírňujících opatřeních, jejichž přijetí by mohly příslušné izraelské orgány pro kontrolu vývozu v budoucnu zvážit“. V době odeslání dopisu Komise žádné takové informace od příslušných izraelských orgánů pro kontrolu vývozu neobdržela, ale měla v úmyslu „vrátit se k otázce možných zmírňujících opatření na příštím zasedání podvýboru EU-Izrael pro průmysl, obchod a služby v rámci dohody o přidružení“.

MAROKO

432. V mnoha zprávách bylo zdokumentováno rozsáhlé používání špionážního softwaru v Maroku. Maroko, které má licenci na přibližně 10 000 telefonních čísel, lze považovat za jednoho z největších klientů pro špionážní software Pegasus společnosti NSO[775]. Maroko odmítlo obvinění spojené s projektem Pegasus jako „mylné“. V prosinci 2020 zpráva organizace Citizen Lab odhalila, že Maroko je jedním z 25 zákazníků Circles, dceřiné společnosti NSO Group[776].

433. Odhalení také ukázala, že v zemi se k hackování a následnému zastrašování novinářů a aktivistů údajně používá sledování pomocí špionážního softwaru[777]. V nedávném usnesení o sledování a věznění investigativního novináře Omara Radiho Evropský parlament odsoudil trvalé soudní pronásledování novinářů marockou vládou a vyzval marocké úřady, „aby ukončily sledování novinářů, mj. prostřednictvím špionážního softwaru Pegasus společnosti NSO“[778]. Jedna ze sledovaných osob, Ignacio Cembrero, investigativní novinář španělského deníku El Confidential, předstoupil před výbor PEGA 29. listopadu 2022. O hackerském útoku na svůj telefon se dozvěděl poté, co byly v marockých novinách zveřejněny textové zprávy mezi ním a španělskou vládou. Když španělský soud požádal izraelské orgány o spolupráci, odmítly poskytnout další informace, které by případu pomohly.

434. Maroko rovněž pronásledovalo marocké novináře ve francouzském exilu Hichama

[774] https://www.amnesty.org/en/latest/researc h/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/.
[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] Usnesení Evropského parlamentu ze dne 19. ledna 2023 o situaci novinářů v Maroku, zejména o případu Omara Rádího https://www.europarl.europa.eu/doceo/document/TA-9-2023-0014_CS.html.

Mansuriho a Abúbakra Jamaima[779], kteří jsou v exilu ve Francii, jakož i stoupence Západní Sahary, včetně pařížského obhájce Josepha Brehama a západosaharského obhájce lidských práv El Mahžuba Maliha žijícího v Belgii[780].

435. Maroko zahájilo několik soudních řízení v reakci na obvinění z účasti na používání systému Pegasus ve Francii, Španělsku a Německu. Ve Francii podaly marocké úřady žaloby pro pomluvu proti několika médiím a organizacím občanské společnosti, včetně Le Monde, Forbidden Stories, Radio France, Mediapart, L'Humanité a Amnesty International. Dne 25. března 2022 pařížský trestní soud případy zamítl jako nepřípustné a marocké orgány se proti tomuto rozhodnutí odvolaly. Ve Španělsku marocké úřady podaly žalobu na novináře Ignacia Cembrera, kdy ho na základě středověkého ustanovení trestního zákoníku obvinili z „chvástání“. Případ stále probíhá a byl odsouzen jako snaha zastrašit pana Cembrera a další osoby, aby neinformovaly o používání špionážního softwaru v Maroku[781].

436. Podle novinové zprávy bylo Maroko před rozsáhlým používáním softwaru Pegasus také klientem nejméně tří evropských poskytovatelů špionážního softwaru, konkrétně francouzských společností Amesys a Vupen[782] a italského Hacking Teamu. Podle důvěrných dokumentů bylo Maroko třetím největším klientem italské společnosti a během šesti let zaplatilo více než 3 miliony EUR za pořízení softwaru RCS společnosti Hacking Team pro domácí Vysokou radu národní obrany (CSDN) a Ředitelství územního dohledu[783]. Prostřednictvím špionážního softwaru byla sledována řada vysoce postavených oddělení a útvarů OSN.

437. Maroko získalo v EU nejen špionážní software, ale také technologickou a finanční podporu Evropské komise. Podle deníku Der Spiegel Maroko obdrželo z EU dva špionážní systémy pro špehování osob pro účely hraniční kontroly (francouzsko-libanonský špionážní software MSAB „XRY“ a špionážní software společnosti Oxygen Forensics se sídlem v USA s názvem „Detective“[784]. Kromě toho byla do Maroka vyslána Agentura Evropské unie pro vzdělávání a výcvik v oblasti prosazování práva (CEPOL), aby provedla osobní školení o používání špionážního softwaru a také naučila policii získávat informace z profilů na sociálních sítích prostřednictvím sociálního hackingu[785]. Na rozdíl od softwaru Pegasus mohou výše uvedené spywarové programy do zařízení vstupovat pouze fyzicky a nezanechávají žádné stopy po svém použití. Zpráva popisuje několik případů, kdy byly chytré telefony odebrány cílovým osobám, mezi nimiž byli i novináři a aktivisté, a vráceny zpět s náznaky jejich možné nákazy. Ačkoli není možné ověřit, zda byl spyware třetími stranami řádně používán,

---

[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.
[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.

neexistovaly žádné náznaky, že by Komise ověřovala náležité používání dodaných technologií. Komise neprovedla žádné posouzení dopadů, které by zmapovalo možné zneužití dodaných technologií, což je obdobná situace, jaká byla popsána ve stížnosti veřejnému ochránci práv EU v souvislosti s financováním sledovacích technologií v rámci programu EUTFA (viz příslušný oddíl níže). Komise uvedla, že je na uživateli, Maroku, aby spyware nasadil zodpovědně a v souladu se smluvním ujednáním (tj. pouze pro účely uvedené ve smlouvě)[786].

DALŠÍ TŘETÍ ZEMĚ

438. Na celém světě zakoupilo a/nebo používá špionážní software nejméně 75 zemí, včetně represivních režimů[787]. Organizace na ochranu lidských práv zdokumentovaly řadu případů, kdy byl spyware zneužit k útokům na politiky, novináře, právníky, obránce lidských práv a další aktivisty občanské společnosti prosazující lidská práva, práva žen a ochranu životního prostředí[788].

SPOLUÚČAST ČLENSKÝCH STÁTŮ EU JAKOŽTO KLIENTŮ SPOLEČNOSTI NSO GROUP NA ZNEUŽÍVÁNÍ SYSTÉMU PEGASUS VE TŘETÍCH ZEMÍCH

439. Za více mnoho případů, kdy byly identifikovány oběti a kdy bylo technicky prokázáno použití špionážního softwaru, nese s největší pravděpodobností odpovědnost 14 orgánů zemí mimo EU. Jedná se o tyto země: Salvador, Mexiko, Thajsko, Maroko, Indie, Rwanda, Saúdská Arábie, Bahrajn, Jordánsko, Kazachstán, Togo, SAE, Izrael a Ázerbájdžán[789].

440. Projekt Pegasus, na kterém spolupracovalo více než 80 novinářů ze 17 sdělovacích prostředků, zdokumentoval, jak je systém Pegasus využíván represivními vládami, které se snaží umlčet novináře, útočit na aktivisty a potlačovat disent. Vyšetřování v rámci projektu Pegasus ukázala, že rodinní příslušníci saúdskoarabského novináře Džamála Chášukdžího byli terčem softwaru Pegasus před jeho vraždou a po ní, kterou v Istanbulu dne 2. října 2018 spáchali saúdskoarabští agenti, ačkoliv to společnost NSO Group opakovaně popírá. Security Lab, bezpečnostní laboratoř organizace Amnesty International, zjistila, že pouze čtyři dny po vraždě Chášukdžího byl na telefon jeho snoubenky Hatice Cengizové úspěšně nainstalován špionážní software Pegasus. Rovněž jeho manželka Hanan Elatr byla v období od září 2017 do dubna 2018 opakovaně terčem špionážního softwaru, stejně jako jeho syn Abdullah, který byl vybrán jako cíl sledování tímto spywarem spolu s dalšími rodinnými příslušníky v Saúdské Arábii a Spojených arabských emirátech[790].

441. Z vyšetřování v rámci projektu Pegasus kromě toho vyplynulo, že terčem špionážního

[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*“ (Globální přehled komerčního špionážního softwaru a digitální forenzní analýzy), 11. ledna 2023, https://carnegieendowment.org/programs/democracy/commercialspyware.
[788] Forensic Architecture, Amnesty International and The Citizen Lab, „*Digital Violence*“ (Digitální násilí), 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*“ (Rozsáhlý únik informací odhalil špionážní software izraelské společnosti NSO Group, který se používá k cílení na aktivisty, novináře a vedoucí politické představitele na celém světě), 19. července 2021, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

softwaru Pegasus jsou často novináři: V Mexiku byl zvolen jako cíl sledování skrze jeho telefon novinář Cecilio Pineda, a to pouhých několik týdnů před tím, než byl v roce 2017 zavražděn. Pegasus se používá také v Ázerbájdžánu, v zemi, kde je dnes už nezávislých sdělovacích prostředků jen pár. Podle vyšetřování bylo jako potenciální cíle vybráno více než 40 ázerbájdžánských novinářů. Security Lab, bezpečnostní laboratoř Amnesty International, došla k závěru, že telefon novinářky na volné noze Sevinc Vagifgiziové pracující pro nezávislý mediální subjekt Meydan TV byl spywarem infikován po dobu dvou let – až do května 2021. Mezi lety 2017 a 2021 byl software namířen také na nejméně 40 novinářů z téměř každé významné mediální společnosti v Indii. Forenzní testy prokázaly, že špionážním softwarem Pegasus byly v nedávné době, tj. v červnu 2021[791] napadeny telefony Siddharthy Varadarajana a MK Venu, spoluzakladatelů nezávislého on-line zpravodajství The Wire.

442. Obhájci lidských práv jsou i nadále často terčem útoků, mimo jiné ze strany orgánů těchto zemí: Mexiko, Salvador, Maroko, Rwanda, Izrael, Jordánsko, Saúdská Arábie, Bahrajn, Spojené arabské emiráty, Indie, Kazachstán, Indonésie a Bělorusko[792]. V roce 2021 zveřejnili obhájci lidských práv FrontLine Defenders zprávu dokumentující cílené sledování obhájců lidských práv v různých zemích včetně Indie. V červnu 2018 bylo šestnáct obhájců lidských práv uvězněno podle indického protiteroristického zákona, a to v tzv. případu Bhima Koregaon, který se týká násilí, k němuž došlo v Bhima Koregaon. Jeden z obránců lidských práv, 84letý jezuitský kněz, Stan Swamy, zemřel v červenci 20211 ve vazbě[793]. Při digitálním forenzním vyšetřování bylo zjištěno, že „důkazy“, o něž se opírá trestní stíhání proti této skupině, byly podstrčeny prostřednictvím špionážního softwaru Pegasus na zařízení obránců lidských práv Rona Wilsona a Surendra Gadlinga a že neexistují žádné důkazy o tom, že by tito obránci lidských práv spolupracovali[794].

II. Odvětví špionážního softwaru

443. Evropská unie je atraktivním místem pro obchod se sledovacími technologiemi a službami, včetně špionážních nástrojů. Na jedné straně máme vlády členských států coby potenciální zákazníky. Na druhé straně slouží myšlenka „regulace na úrovni EU“ jako značka kvality, která je užitečná pro celosvětový trh. Vnitřní trh EU nabízí svobodu pohybu a výhodné vnitrostátní daňové režimy. Pokud se vlády odvolají na národní bezpečnost, mohou se vyhnout pravidlům pro zadávání veřejných zakázek, a mohou také využívat zmocněnce nebo prostředníky, takže nákup špionážního softwaru veřejnými orgány je velmi obtížné odhalit a prokázat. EU má přísná vývozní pravidla,

---

[791] Amnesty International, „*Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally*“ (Rozsáhlý únik informací odhalil špionážní software izraelské společnosti NSO Group, který se používá k cílení na aktivisty, novináře a vedoucí politické představitele na celém světě), 19. července 2021, https://www.amnesty.org/en/latest/press-release/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/.

[793] Frontline Defenders (2. prosince 2021): Action needed to address targeted surveillance of human rights defenders (Opatření potřebná k řešení cíleného sledování obránců lidských práv) 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“ (Mobilní telefon Rona Wilsona byl podle nového znaleckého posudku napaden špionážním softwarem Pegasus), 17. prosince 2021, https://thewire.in/rights/rona-wilsonpegasus-iphone-arsenal.

ale v poslední době se objevuje trend, kdy je členské státy obcházejí a snaží se získat konkurenční výhodu jejich nesprávným uplatňováním na vnitrostátní úrovni. Evropská komise navíc často nedostatečně prosazuje dodržování právních předpisů. Například pokaždé, když byl v Izraeli zpřísněn režim vývozních licencí, přemístilo několik společností svá vývozní oddělení do Evropy, zejména na Kypr[795] [796]. Mimo to získalo několik osobností z odvětví špionážního softwaru občanství EU, aby mohly volně působit v rámci EU i z ní.

444. Kromě toho, jak vypověděl předseda společnosti Amnesty Tech Claudio Guarniery před výborem PEGA, byly to evropské společnosti, jako je německý FinFisher a italský Hacking Team, které byly průkopníky odvětví námezdního špionážního softwaru. První zprávy o úloze těchto společností při monitorování novinářů a potlačování disentu se objevily před více než deseti lety, kdy se s nástupem protestních hnutí známých jako Arabské jaro začaly objevovat smlouvy těchto společností v kancelářích tajné policie[797].

445. Průmysl špionážního softwaru má nepřehlednou strukturu postavenou na složité síti osob, míst, vazeb, vlastnických struktur, firemních schránek, neustále se měnících názvů společností, toků peněz, vládních zmocněnců a prostředníků, magnátů a vlád.

446. V mnoha případech se zdá být přesná přezdívka „námezdní špionážní software“. Jak ukazuje počet nezákonně napadených osob, mnoho společností zaostává v dodržování etických norem, často prodávají diktaturám a bohatým nestátním subjektům a pokračují v tom i po odhaleních projektu Pegasus. Společnost Cellebrite v roce 2021 oznámila, že přestane prodávat své produkty ruské vládě, když vyšlo najevo, že její špionážní software byl používán ke sledování aktivistů bojujících proti Putinovi. V říjnu 2022 se však objevily signály, že ruské orgány produkty Cellebrite stále používají[798]. Jedná se o lukrativní a rozporuplný trh. Přesto se však řadě společností zabývajících se špionážním softwarem daří prodávat produkty demokratickým vládám v USA a EU, což jim dodává zdání slušnosti. Navzdory tvrzením, že používání špionážního softwaru je zcela legitimní a nezbytné, nejsou ale vlády ochotné připustit, že špionážní software vlastní. Při jeho nákupu se někdy se uchylují k používání zmocněnců, prostředníků nebo zprostředkovatelů, aby nezanechávaly žádné stopy. Velkou výroční akcí tohoto odvětví je veletrh „ISS World“, jemuž se také přezdívá „ples odposlouchávačů“. Jeho evropská odnož se koná každý rok v Praze. Vystavovatelé na ISS World jsou do značné míry stejní jako vystavovatelé na veletrzích zbrojního průmyslu.

447. Vedle „oficiálních kanálů“ existuje i černý trh s těmito výrobky. Ačkoli mnozí prodejci tvrdí, že prodávají pouze vládám, zdá se, že se tajně snaží obchodovat rovněž s nestátními subjekty. Je velmi obtížné nalézt neprůstřelné důkazy, neboť tento obchod zanechává jen velmi málo stop. Řecké noviny Documento tvrdí, že mají důkazy o tom, že software je prodáván na černém trhu – až za 50 milionů USD – nejen vládám a

[795] Makarios Drousiotis, „State Mafia“ (Státní mafie) 2022, kapitola 6.
[796] Haaretz. „*Cyprus, Cyberspies and the Dark Side of Israeli Intel*“ (Kypr, kybernetičtí špióni a Dark Side of Israel Intel).
[797] Slyšení výboru PEGA ze dne 30.8.2022 o dopadu špionážního softwaru na občany EU https://netzpolitik.org/2022/pega-untersuchungsausschuss-wie-staatstrojaner-gegen-eu-buerger-eingesetzt-werden/
[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.

protiteroristickým agenturám, ale také soukromým osobám[799]. Další řecké noviny, To Vima, uvedly, že software Predator byl prodán 34 zákazníkům z Řecka[800]. Uniklé dokumenty poukazují na to, že pirátská verze produktu, která byla oficiálně prodávána pouze vládám, byla k dispozici za cenu 8 milionů USD, což je částka, která zahrnovala školení agentů, kteří budou program používat, 24hodinovou technickou podporu a sledování účtů oběti na sociálních médiích[801].

448. Toto odvětví nabízí širokou škálu produktů a služeb v oblasti sledování a zpravodajství, nejen špionážní software jako jediný produkt. Špionážní software je pouze jedním nástrojem v souboru nástrojů společností, které provádějí hackerské útoky na objednávku.

Slabá místa

449. Pokud by v softwaru nebyla slabá místa, nebylo by možné spyware instalovat a zavádět. Chceme-li tedy používání špionážního softwaru regulovat, musíme regulovat i odhalování, sdílení a využívání těchto slabých míst[802]. Navzdory posílení obrany digitálních systémů, které je vyžadováno a podporováno směrnicí NIS2 a návrhem aktu o kybernetické odolnosti, je téměř nemožné vyvinout systémy, které by slabá místa neměly.

450. Zranitelná místa je proto třeba odhalit a opravit co nejdříve. Stávající právní předpisy EU ovšem nepodporují jejich odhalení, ale opak. Výzkumní pracovníci v oblasti bezpečnosti informací mohou podle směrnice o počítačové kriminalitě a směrnice o autorském právu čelit občanskoprávní a trestní odpovědnosti při výzkumu zranitelných míst a sdílení svých výsledků. Kromě toho není povinné, aby výzkumní pracovníci sdíleli jakákoli zjištění týkající se zranitelných míst. Mohlo by se tedy stát, že se výzkumní pracovníci rozhodnou prodat své vědomosti o zranitelných místech soukromému zprostředkovateli a získat tak značnou odměnu.

451. Tato praxe vedla k čilému a lukrativnímu obchodu se zranitelnými místy. Zranitelná místa ovšem nehledají pouze ti, kdo se zranitelnostmi nultého dne obchodují: slabá místa vytvářejí také bezpečnostní a donucovací orgány, přičemž někdy je zjistí jejich vlastní odborníci a někdy je získají od zprostředkovatelů. Pokud zranitelná místa nejsou hlášena, nedochází k jejich nápravě, takže naše informační systémy jsou pak oslabeny a uživatelé nejsou chráněni. To umožňuje opětovné používání špionážního softwaru.

Telekomunikační sítě

452. V oblasti legální i nelegální špionáže hrají významnou úlohu poskytovatelé telekomunikačních služeb. Žijeme v moderní éře umělé inteligence, dat velkého objemu a kvantové výpočetní techniky, ale současně se neobejdeme bez mezinárodního telekomunikačního protokolu zvaného Signalizační systém č. 7 (Signalling Systém No

[799] Documento, „Odhalení špionážního softwaru Predator společností Documento týkající se sítě Euractiv – výzvy Europolu pro nizozemského poslance EP“
[800] To Vima, „Odposlechy: Špionážní software má 34 zákazníků“.
[801] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/.
[802] Ot van Daalen, vystoupení ve výboru PEGA dne 27. října 2022;
Studie EDRi: „*Breaking encryption will doom our freedoms and rights*“ (Prolomení šifrování zničí naše svobody a práva) 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.

7, SS7). Tento protokol byl vypracován v roce 1975 a používá se dosud. Uvedený systém kontroluje směrování a účtování telefonních hovorů a umožňuje pokročilé funkce volání a službu krátkých zpráv (SMS)[803]. Prostřednictvím sítě SS7 je možné odposlouchávat telefonní hovory a zachycovat SMS, zjišťovat geolokaci a rovněž infikovat oběť špionážním softwarem, jako je Pegasus, Predator atd.[804].

453. Riziko zneužití přístupu k těmto sítím ze strany poskytovatelů telekomunikačních služeb je vysoké. Máme několik doložených případů zneužití, kdy byla přístupová místa (globální tituly) pronajata společnostem, které monitorovaly a odposlouchávaly komunikaci cílů na základě útoků typu man-in-the-middle. Rovněž shromažďovali geolokační údaje a meta data pro své vlastní ekonomické účely. „Global title“ je adresa používaná pro směrování zpráv v rámci SS7. Lze jej porovnat s IP adresou v tom smyslu, že „global title“ odkazuje na adresu v telekomunikační síti[805]. Podle oznamovatele měla proto společnost NSO takový zájem o přístup k síti SS7 v USA, že se snažila koupit přístup od jejich společnosti[806]. Poskytovatelé telekomunikačních služeb záměrně udržují tyto nízké průmyslové standardy s cílem zajistit snadnější přístup státním donucovacím orgánům na místní úrovni.

Společnost NSO Group

454. Špionážní software Pegasus vyrábí společnost NSO Group, kterou v roce 2010 založili Shalev Hulio, Omri Lavie a Niv Karmi. Vyvinuli technologii, která měla pomoci licencovaným vládním subjektům a donucovacím orgánům odhalovat terorismus a trestnou činnost a předcházet jim[807]. Špionážní software Pegasus je nejznámějším produktem této společnosti. Na světový trh byl uveden v roce 2011[808] [809].

455. Společnost NSO Group je od svého založení v roce 2010 přítomná v Izraeli, Spojeném království, Lucembursku, na Kajmanských ostrovech, na Kypru, v USA, Nizozemsku, Bulharsku a na Britských Panenských ostrovech. Stále chybí mnoho informací o úlohách různých korporátních subjektů a některé z těchto společností již byly zrušeny. Společnost NSO Group však ve své zprávě o transparentnosti a odpovědnosti z roku 2021 uvedla, že jak Bulharsko, tak Kypr jsou vývozními uzly[810]. Podle organizace Amnesty International působily nizozemské subjekty, které byly zrušeny dne 22. prosince 2016, v odvětví finančních holdingů, zatímco společnost Q Cyber Technologies se sídlem v Lucembursku působila jako komerční distributor odpovědný za vystavování faktur, podepisování smluv a přijímání plateb od zákazníků. Kromě toho je možné, že společnost Westbridge Technologies registrovaná v USA napomáhala

[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.
[807] NSO Group. ‘About us’.
[808] The New York Times „The *Battle for the World’s Most Powerful Cyberweapon*“ (Bitva o nejmocnější kybernetickou zbraň na světě).
[809] Shalev Hulio, „*NSO Never Engaged in Illegal Mass Surveillance*“ (NSO se nikdy nepodílela na protiprávním masovém sledování), The Wall Street Journal, 24. února 2022.
[810] NSO Group, „*Transparency and Responsibility Report 2021*“ (Zpráva o transparentnosti a odpovědnosti za rok 2021)“.

prodeji v USA[811].

456. Společnost NSO měla v roce 2020 údajně příjmy ve výši 243 milionů USD[812]. Po odhaleních zveřejněných v rámci projektu Pegasus však společnost čelila několika obtížím. Žaloby podané proti ní společnostmi Apple[813] a Meta[814], její zařazení na černou listinu americkým ministerstvem pro obchod, zpřísnění izraelského režimu vývozu, kritická šetření v několika zemích a vnitřní napětí v rámci fondu soukromého kapitálu, který stojí v pozadí NSO Group, vedly k výraznému poklesu zisku. V jednu chvíli prý dluh NSO Group dosáhl dokonce 6,5násobku jejích běžných ročních příjmů[815].

457. Výbor PEGA se se společností NSO Group sešel dvakrát, z toho jednou v Bruselu a jednou v Izraeli. Špionážní software Pegasus byl původně prodán dvaceti dvěma koncovým uživatelům ve čtrnácti členských státech EU za použití marketingových a vývozních licencí vydaných Izraelem. Smlouvy s koncovými uživateli ve dvou členských státech byly následně ukončeny[816]. Nebylo potvrzeno, které členské státy byly na tomto seznamu čtrnácti zemí, ani které dvě země byly odstraněny. Dalo by se však předpokládat, že se jedná o Polsko a Maďarsko.

KORPORÁTNÍ STRUKTURA, TRANSPARENTNOST A NÁLEŽITÁ PÉČE

458. Dne 25. ledna 2010 založila NSO Group svou první společnost v Izraeli. Ta byla zaregistrována pod názvem NSO Group Technologies Limited. NSO Group je jak název první zaregistrované společnosti, tak zastřešující označení pro různé společnosti usazené v jiných jurisdikcích. Tato první založená společnost je vlastníkem ochranné známky NSO Group[817].

459. V březnu 2014 získal fond soukromého kapitálu Francisco Partners 70% podíl v NSO Group. Pod vedením Francisco Partners společnost rozšířila své subjekty do různých jurisdikcí, včetně Kypru, Bulharska, US, Nizozemska a Lucemburska. Během let 2014 až 2019 pod vedením Francisco Partners fond systematicky přezkoumával prodej produktů NSO Group prostřednictvím výboru pro etiku podnikání. Podle Francisco Partners tento výbor zamítl prodej v hodnotě desítek milionů dolarů, který by jinak byl podle zákonných požadavků schválen[818].

460. Společnost Francisco Partners prodala dne 14. února 2019 veškerý svůj vlastnický podíl, včetně dceřiných společností, společnosti Novalpina Capital. Tímto manažerským odkupem se změnily standardy správy a řízení a výbor pro etiku podnikání byl nahrazen

[811] Amnesty International, „*Operating from the Shadows – inside NSO Group's corporate structure*“ (Aktivita ze zákulisí: uvnitř podnikové struktury NSO Group).
[812] Haaretz, „*NSO Is Having a Bad Year - and It's Showing*“ (NSO má špatný rok a je to znát).
[813] Apple „*Apple sues NSO Group to curb the abuse of state-sponsored spyware*“ (Apple žaluje společnost NSO Group, aby omezila zneužívání státem sponzorovaného spywaru).
[814] Bloomberg Law, „*NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware*“ (NSO prohrála poslední námitku proti žalobě Meta kvůli špionážnímu softwaru WhatsApp).
[815] Bloomberg, „*Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop*“ (Izraelské firmě NSO, která vyrábí špionážní software, hrozí kvůli poklesu tržeb platební neschopnost).
[816] Odpovědi poskytnuté společností NSO Group sekretariátu výboru PEGA po slyšení, 20. července 2022.
[817] Amnesty International, „*Operating from the Shadows – inside NSO Group's corporate structure*“ (Aktivita ze zákulisí: uvnitř podnikové struktury NSO Group).
[818] Amnesty International, „*Operating from the Shadows – inside NSO Group's corporate structure*“ (Aktivita ze zákulisí: uvnitř podnikové struktury NSO Group).

výborem pro správu, rizika a dodržování předpisů pro přezkum situace potenciálních zákazníků v oblasti lidských práv[819].

461. V souladu s osvědčením o konečném použití/uživateli po zpřísnění izraelského režimu vývozu zavedla NSO Group politiku v oblasti lidských práv a postup náležité péče v oblasti lidských práv. Jak je popsáno ve zprávě NSO Group o transparentnosti a odpovědnosti z roku 2021, vyžaduje NSO Group, aby všechny zákaznické dohody obsahovaly doložky o dodržování lidských práv a doložky popisující pozastavení nebo ukončení používání produktů NSO Group v případě zneužití v souvislosti s lidskými právy. NSO Group v písemném podání výboru PEGA potvrdila, že ukončila smlouvy s členskými státy EU[820], které údajně porušily doložky o lidských právech. NSO Group nevysvětlila, zda provedla přezkum auditorských protokolů a zda dotčení zákazníci s takovým šetřením souhlasili. Není tedy známo, zda stále existují důkazy o tomto zneužití, zda má NSO nějaký způsob, jak tyto důkazy zachovat, nebo zda izraelské orgány mají nějaké důkazy.

462. Podle Amnesty International chybí ve zprávě o transparentnosti společnosti NSO Group řádná politika nápravy pro osoby, které se staly terčem nezákonného sledování, a chybí informace o probíhajících soudních sporech proti této společnosti[821]. V rozporu s politikou NSO Group v oblasti lidských práv a postupem náležité péče v oblasti lidských práv je na zařízeních novinářů a kritiků autoritářských režimů nadále odhalován špionážní software NSO[822].

KONTROLY VÝVOZU

463. Vzhledem k tomu, že špionážní software Pegasus je klasifikován jako technologie dvojího užití, musí obdržet vývozní licenci. Společnosti NSO Group získávají vývozní licence v Izraeli, Bulharsku a na Kypru[823]. Sama NSO Group to potvrdila, ale popírá, že by se spyware Pegasus vyvážel z Kypru a Bulharska[824]. Vlády Kypru a Bulharska navíc popřely, že by společnostem NSO Group obecně udělily jakákoliv vývozní povolení. Jiné zdroje toto zpochybňují a uvádějí, že dceřiné společnosti NSO se často skrývají za jiným názvem ve vnitrostátních obchodních rejstřících. Jedna z dceřiných společností NSO působící na Kypru pod názvem „Circles“ však v roce 2020 uzavřela své kanceláře[825]. Licence udělují také izraelské orgány[826]. Izrael není součástí Wassenaarského ujednání, ale uvádí, že některé jeho prvky začlenil do izraelského

[819] Slyšení výboru PEGA s NSO, 21. června 2022.
[820] Slyšení výboru PEGA s NSO, 21. června 2022.
[821] Amnesty International, „*NSO Group's new transparency report is „another missed opportunity*““ (Nová zpráva o transparentnosti společnosti NSO Group je „další promarněnou příležitostí“), tisková zpráva, 1. července 2021.
[822] The New York Times, „*U.S. Blacklists Israeli Firm NSO Group Over Spyware*“ (USA zařadily izraelskou firmu NSO Group na černou listinu kvůli spywaru).
[823] Amnesty International, „*Operating from the Shadows – inside NSO Group's corporate structure*“ (Aktivita ze zákulisí: uvnitř podnikové struktury NSO Group), s. 62.
[824] Amnesty International, „*Operating from the Shadows – inside NSO Group's corporate structure*“ (Aktivita ze zákulisí: uvnitř podnikové struktury NSO Group).
[825] VICE, „*NSO Group Closes Cyprus Office of Spy Firm*“ (NSO Group zavírá kyperskou pobočku špionážní firmy).
[826] Amnesty International, „*Operating from the Shadows – inside NSO Group's corporate structure*“ (Aktivita ze zákulisí: uvnitř podnikové struktury NSO Group).

vnitrostátního zákona o kontrole vývozu obranných prostředků č. 5766-2007[827]. Za vydávání licencí pro uvádění na trh a vývozních licencí je zodpovědná Agentura pro kontrolu vývozu Ministerstva obrany[828]. V návaznosti na odhalení zveřejněná projektem Pegasus a zařazení společnosti NSO na černou listinu byl počet způsobilých zemí snížen ze 102 na 37, přičemž všechny musí podepsat prohlášení o konečném použití/uživateli[829]. V rámci postupu náležité péče považuje Izrael automaticky všechny členské státy EU za státy dodržující normy EU, takže neprovádí dodatečná posouzení pro jednotlivé země. Rozhodnutí ukončit smlouvy se dvěma členskými státy EU však naznačuje, že EU již není pro účely náležité péče považována za jediný subjekt.

NEETICKÉ CHOVÁNÍ, JEHOŽ NÁSLEDKEM JSOU ŽALOBY, ZAŘAZENÍ NA ČERNOU LISTINU A SPORY MEZI INVESTORY

464. V červenci 2021 začal obchodní aktivity NSO Group ovlivňovat konflikt mezi třemi spoluzakladateli společnosti Novalpina Capital, takže se investoři nakonec rozhodli odebrat této společnosti soukromého kapitálu kontrolu[830]. Dne 27. srpna 2021 převzala americká poradenská společnost Berkeley Research Group (BRG) soukromý kapitálový fond a zahájila kritické vyšetřování zákonnosti činnosti NSO Group a jejího souladu s černou listinou USA. Vedení NSO Group však šetření společnosti BRG prováděná v květnu 2022 blokovalo[831]. Jeden z vedoucích pracovníků BRG uvedl, že spolupráce s NSO Group „v podstatě neexistuje“, a to kvůli tlaku NSO Group na pokračování v prodeji do zemí s kontroverzní pověstí v oblasti lidských práv[832]. Dne 25. dubna 2022 podali dva bývalí společníci firmy Novalpina u lucemburského soudu žalobu na BRG, v níž požadovali, aby byl společnosti Novalpina Capital vrácen status společníka a aby byla pozastavena všechna rozhodnutí BRG[833]. Lucemburský soud tyto požadavky zamítl a společnost BRG nadále řídí fond, který kontroluje NSO Group[834].

465. Kromě dopadů na vlastnictví zařadilo americké ministerstvo obchodu NSO Group dne 3. listopadu 2021 na černou listinu z důvodu neslučitelnosti činností NSO se zahraniční politikou USA a s obavami o národní bezpečnost. Vláda USA zakazuje vývoz technologií pro NSO Group a její dceřiné společnosti, což *de facto* znamená, že žádná americká společnost s NSO Group nemůže spolupracovat[835].

466. V reakci na zařazení na černou listinu USA společnost Credit Suisse jako jeden z věřitelů NSO Group údajně přinutila tuto společnost, aby pokračovala v prodeji

---

[827] Evropská parlamentní výzkumná služba, „*Europe's PegasusGate – countering spyware abuse*“ (Evropská PegasusGate – boj proti zneužívání spywaru).
[828] Amnesty International, „*Novalpina Capital’s reply to NGO coalition letter (15 April 2019) and Citizen Lab letter (6 March 2019)*“ (Odpověď Novalpina Capital na dopis koalice nevládních organizací (15. dubna 2019) a dopis Citizen Lab (6. března 2019).
[829] Evropská parlamentní výzkumná služba, „*Europe's PegasusGate – countering spyware abuse*“ (Evropská PegasusGate – boj proti zneužívání spywaru).
[830] Financial Times, „*Private equity owner of spyware group NSO stripped of control of €1bn fund*.“ (Soukromý vlastník spywarové skupiny NSO zbaven kontroly nad fondem v hodnotě 1 miliardy EUR).
[831] Financial Times, „*NSO Group keeping owners ‘in the dark”, manager says*“ (NSO Group drží vlastníky v nevědomosti, tvrdí manažer).
[832] The New Yorker, „*How Democracies Spy on their Citizens*“ (Jak demokracie špehují své občany).
[833] Dopis panu Jeroenu Lenaersovi a jeho místopředsedům.
[834] Luxembourg Times, „*Top five stories you may have missed*“ (Pět nejzajímavějších příběhů, které jste možná přehlédli).
[835] The New York Times, „*U.S. Blacklists Israeli Firm NSO Group Over Spyware*“ (USA zařadily izraelskou firmu NSO Group na černou listinu kvůli spywaru).

špionážního softwaru Pegasus novým zákazníkům. V dopise zaslaném společností Willkie Farr & Gallagher společnosti BRG několik věřitelů uvedlo, že se obávají, že BRG brání NSO Group „v tom, aby usilovala o získání nových zákazníků“. Ačkoli to v dopise nebylo výslovně uvedeno, dva odborníci na danou problematiku uvedli, že jedním z věřitelů je Credit Suisse. BRG věřitelům odpověděla, že je hluboce znepokojena tlakem v souvislosti s prodejem produktů NSO Group[836].

467. Několik dní poté, co USA zařadily společnost NSO na černou listinu, potvrdil odvolací soud Spojených států, že žaloba společnosti Meta proti NSO může pokračovat. Ihned poté podala společnost Apple stížnost na společnost NSO u federálního soudu[837]. V červnu 2022 obvodní soud Spojených států amerických zamítl nárok NSO Group na imunitu v soudním sporu se společností Apple[838]. V době vzniku tohoto textu článku stále probíhá soudní řízení společnosti Apple proti NSO Group.

468. Navzdory zařazení na americkou černou listinu údajně americká vláda v říjnu 2022 jmenovala bývalého poradce NSO Jeremyho Bashe do poradního výboru pro zpravodajské informace. Bash byl údajně najat pod záštitou Beacon Global Strategies, aby poskytoval poradenství NSO Group prostřednictvím Francisco Partners. Podle listu Guardian byl jedním z osmi členů výboru pro etiku podnikání NSO, což mu údajně umožňovalo hlasovat o navrhovaných prodejích NSO. Společnost Beacon Global Strategies ukončila spolupráci s NSO po realizaci prodeje do Saúdské Arábie[839].

469. Společnost NSO Group podobně trpěla v důsledku odchodu zaměstnanců. Od vraždy Džamála Čhášukdžího a rostoucího znepokojení nad úlohou Pegasus v této věci odešlo z NSO Group mnoho zaměstnanců. Téhož měsíce spoluzakladatel Shalev Hulio odstoupil z funkce výkonného ředitele NSO Group a nahradil jej Yaron Shohat[840]. NSO Group změnila politiku a nyní se zaměřuje pouze na členy NATO[841]. V březnu 2023 bylo oznámeno, že akcie NSO byly převedeny na investiční společnost Dufresne Holding spoluzakladatele Omriho Lavieho[842].

470. Tlak na společnost NSO Group vytvořil poptávku pro další společnosti zabývající se spywarem. Deník Financial Times 31. března 2023 uvedl, že indická vláda údajně hledá možnost nákupu alternativního komerčního špionážního softwaru s podobnými funkcemi jako nyní kontroverzní špionážní software Pegasus a že zvažuje také nákup

---

[836] Financial Times, „*Credit Suisse pushed for spyware sales at NSO despite US blacklisting*“ (Credit Suisse tlačila na prodej spywaru v NSO navzdory černé listině USA).
[837] The New York Times, „*Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*“ (Apple žaluje izraelského výrobce špionážního softwaru a snaží se mu zablokovat přístup k iPhonům).
[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*“ (Bidenův zpravodajský poradce dříve prověřoval dohody pro izraelskou NSO Group).
[840] The Washington Post, „*CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup*“ (CEO izraelské společnosti NSO Spyware Company Steps Down Amid Shakeup); Calcalist, „*After cutbacks and CEO departure, what's next for the controversial NSO?*“ (Co bude dál s kontroverzní NSO po škrtech a odchodu generálního ředitele?).
[841] The Guardian, „*CEO of Israeli Pegasus spyware firm NSO to step down*“ (Generální ředitel izraelské špionážní firmy NSO Pegasus odstoupí).
[842] The Guardian, „*NSO Group co-founder emerges as new majority owner*“ (Novým většinovým vlastníkem se stal spoluzakladatel společnosti NSO Group).

špionážního softwaru Predator společnosti Intellexa[843].

471. V říjnu 2022 založili Shalev Hulio a bývalý rakouský kancléř Sebastian Kurz novou firmu v oblasti kybernetické bezpečnosti nazvanou „Dream Security“. Pan Kurz odstoupil jako kancléř po korupčním skandálu v říjnu 2021 a o dva měsíce později začal pracovat pro investiční firmu Petera Thiela. Tato společnost bude vytvářet řešení v oblasti kybernetických incidentů se zaměřením na umělou inteligenci a zaměří svůj prodej na evropský trh[844]. Spolupráce mezi pány Kurzem a Huliem představuje nepřímé, ale znepokojivé propojení mezi odvětvím špionážního softwaru a Peterem Thielem a jeho firmou Palantir.

472. Dream Security již získala 20 milionů USD od několika investorů, jako je Adi Shalev, který se rovněž podílel na investicích do NSO. Mezi další investory patří Jevgenij Dibrov[845], který zastupuje „nový ruský hlas" v tom, co nazývá „rusko-izraelským technologickým ekosystémem“[846]. To ukazuje, že navzdory turbulencím a ekonomickým problémům, s nimiž se NSO Group potýká, stejná jména stále zakládají nové společnosti zabývající se špionážním softwarem v EU i mimo ni.

BLACK CUBE

473. Black Cube je izraelská soukromá zpravodajská služba, kterou tvoří bývalí zaměstnanci izraelské armády a izraelských zpravodajských služeb[847]. Na svých vlastních internetových stránkách se označuje za „kreativní zpravodajskou službu“, která nalézá „řešení složitých obchodních a soudních problémů podle potřeb konkrétních zákazníků“[848]. Byla zapojena do řady veřejně známých hackerských skandálů v různých zemích, mimo jiné v USA a Rumunsku[849]. Konkrétně vedoucí představitelé Black Cube připustili, že jejich společnost sledovala bývalou vrchní žalobkyni rumunského Národního protikorupčního ředitelství Lauru Kövesiovou[850]. Kövesiová je v současné době první evropskou nejvyšší žalobkyní, stojí tedy v čele Úřadu evropského veřejného žalobce (EPPO). Služby společnosti Black Cube si v této souvislosti údajně objednal Daniel Dragomir, bývalý rumunský tajný agent[851].

474. K těm největším patří odhalení, že existuje spojitost mezi společnostmi Black Cube a NSO Group a jejím špionážním softwarem Pegasus. Bylo zjištěno, že NSO Group najímala Black Cube na sledování svých odpůrců. Po velkém tlaku veřejnosti se bývalý

---

[843] https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9.
[844] Organised Crime and Corruption Reporting Project, „*Former Austrian Chancellor and ex-NSO Chief Start Cybersecurity Firm*“ (Bývalý rakouský kancléř a bývalý šéf NSA zakládají firmu zabývající se kybernetickou bezpečností); The Times, „*Former NSO CEO and ex-Austrian Chancellor found startup*“ (Bývalý generální ředitel NSO a bývalý rakouský kancléř založili startup).
[845] The Times, „*Former NSO CEO and ex-Austrian Chancellor found startup*“ (Bývalý generální ředitel NSO a bývalý rakouský kancléř založili startup).
[846] Calcalist, „*From Russia, With Coding Skills*“ (Z Ruska, s kódovacími dovednostmi).
[847] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7. října 2019.
[848] https://www.blackcube.com/.
[849] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18. dubna 2022.
[850] Balkan Insight. „*Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case*“ (Šéfové zpravodajských firem se přiznali k vině v případu sledování Rumunska).
[851] Haaretz. ‘*Black Cube CEO Suspected of Running Crime Organisation – Revealed:The Romania Interrogation*“ (Generální ředitel Black Cube podezřelý z vedení zločinecké organizace – odhaleno).

generální ředitel NSO Shalev Hulio přiznal, že najal Black Cube přinejmenším v jednom případě na Kypru.

475. Společnost Black Cube se angažovala v Maďarsku během voleb v roce 2018, během nichž špehovala různé nevládní organizace a osoby, které měly jakékoli spojení s Georgem Sorosem, a podávala o nich zprávy Viktoru Orbánovi, aby tyto informace mohl využít v pomlouvačné kampani[852]. Získané informace ze sledování těchto osob a nevládních organizací se objevily nejen v maďarských státem kontrolovaných sdělovacích prostředcích, ale také v Jerusalem Post[853].

INTELLEXA ALLIANCE

476. Společnost Intellexa založil v roce 2019 Tal Dilian na Kypru. Dilian zastával různé vedoucí funkce v izraelských obranných silách a poté zahájil kariéru „zpravodajského experta, odborníka na rozvoj komunit a zakladatele mnoha podniků“[854]. Intellexa Alliance se na svých internetových stránkách prezentuje jako „společnost se sídlem v EU, která se řídí právem EU“ a jejíž náplní činnosti je „vývoj a zavádění technologií podporujících práci zpravodajských služeb“. Mezi dodavatele systémů sledování, kteří jsou součástí marketingové značky Intellexa Alliance, patří Cytrox, WiSpear (později přejmenovaná na Passitora Ltd), Nexa Technologies (vedená bývalými manažery společnosti Amesys) a Poltrex.

477. Všichni tito prodejci umožňují využívat různé systémy. Zatímco Cytrox je schopný získávat údaje z mobilních telefonů, společnost Nexa Technologies nabízí využívání globálních mobilních komunikačních systémů. WiSpear může také získávat údaje z Wi-Fi sítí. Různí prodejci, které pan Dilian sdružuje, tak poskytují širokou škálu softwaru a služeb, které může společnost Intellexa nabízet samostatně nebo v kombinaci svým klientům v rámci EU i mimo ni[855].

478. Mateřská společnost firmy Intellexa Alliance, Thalestris Limited, má různé dceřiné společnosti, které mají korporátní přítomnost v Irsku, Řecku, Britských Panenských ostrovech, Švýcarsku a na Kypru. Sara Aleksandra Hamouová, údajně druhá bývalá manželka Tala Diliana, byla ředitelkou společnosti Thalestris Limited a výkonnou ředitelkou dceřiné společnosti se sídlem v Řecku[856]. Hamouová, která se narodila v Polsku, má kyperský pas vydaný polským velvyslanectvím na Kypru[857].

WISPEAR A CYTROX

479. V roce 2013 založil Tal Dilian společnost zaregistrovanou na Kypru pod názvem Aveledo Ltd., později známou jako Ws WiSpear Systems ltd. a posléze Passitora Ltd[858].

---

[852] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. července 2018.
[853] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6. července 2018.
[854] Tal Dilian. About.
[855] Haaretz, „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Zatímco Izrael omezuje kybernetický zbrojní průmysl, bývalý důstojník tajné služby buduje nové impérium).
[856] Thalestris Limited, výroční zpráva a konsolidovaná účetní závěrka za období od 28. listopadu 2019 do 31. prosince 2020.
[857] ReportersUnited „*The Great Nephew and Big Brother*“ (Velký synovec a velký bratr).
[858] Open Corporates, „Passitora Ltd“, https://opencorporates.com/companies/cy/HE318328.

Společnost Wispear sídlí v kyperském Limassolu a převážně prodává zařízení a software pro lokalizaci a sledování jednotlivců prostřednictvím mobilního telefonu. Když v rozhovoru pro časopis Forbes Tal Dilian vysvětloval, co vlastně jeho software WiSpear dokáže, předvedl svou černou dodávku v hodnotě 9 milionů USD, z níž je možné napadnout telefon vzdálený 500 metrů. Společnost WiSpear také vlastní zařízení schopná zachycovat data ze sítí Wi-Fi[859]. Veřejné skandály v souvislosti s těmito produkty vedly k přesunu hlavní obchodní činnosti společnosti Intellexa z Kypru do Řecka.

480. V roce 2017 založil Ivo Malinkovski v Severní Makedonii společnost Cytrox Holdings Zrt. Společnost Cytrox však ve skutečnosti vznikla v Tel Avivu a Malinkovski byl jen zástěrkou. Po odhalení projektem Pegasus se Malinkovski snažil zahladit všechny stopy, které ho spojovaly se společností Cytrox.

481. Společnost Cytrox byla vývojářem špionážního softwaru Predator. Na rozdíl od spywaru Pegasus vyžaduje Predator, aby cílová skupina klikla na odkaz a nainstalovala software[860]. Když se společnost Cytrox ocitla na pokraji bankrotu, zachránil ji Tal Dilian, přičemž akvizice ho vyšla na méně než 5 milionů USD[861]. Společnost Cytrox byla následně sloučena se společností WiSpear pana Diliana[862]. Tato akvizice rozšířila arzenál technologií společnosti Intellexa o špionážní software Predator. Jak informoval server Lighthouse Reports ve spolupráci s deníkem Haaretz a serverem Inside Story, společnost Intellexa tajně a nelegálně dodala súdánským milicím Rapid Support Force špionážní software Predator pomocí soukromého letadla Cessna[863].

482. Podle organizace Citizen Lab byly dvě společnosti Cytrox zaregistrovány v Izraeli (Cytrox EMEA Ltd. a Cytrox Software Ltd.) a jedna v Maďarsku jako (Cytrox Holdings Zrt.)[864]. Všechny akcie společností Cytrox Holdings Zrt. a Cytrox EMEA Ltd. – později přejmenované na Balinese Ltd. – byly převedeny na společnost Aliada Group Inc., která je registrována na Britských Panenských ostrovech. Aliada Group je rovněž vlastníkem WiSpear. Hlavními akcionáři skupiny Aliada je sám Tal Dilian a Oz Liv, Meir Shamir a Avi Rubinstein. V prosinci 2020 podal pan Rubinstein na své spoluakcionáře Aliada Group žalobu za protiprávní rozředění jeho akcií. Podle žaloby byly přemístěním akcií na Britské Panenské ostrovy a později do Irska obcházeny izraelské a zahraniční zákony o kontrole vývozu[865].

483. Dne 16. prosince 2021 vydala organizace Citizen Lab zprávu, v níž uvedla, že pravděpodobní zákazníci nakupující software Predator byli zjištěni v Arménii, Egyptě,

---

[859] Haaretz, „*As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire*“ (Bývalý důstojník izraelské tajné služby buduje nové impérium, zatímco Izrael omezuje svůj kybernetický zbrojní průmysl).
[860] Evropská parlamentní výzkumná služba, „Řecká Predatorgate. Poslední kapitola evropského špionážního skandálu?“.
[861] *BalkanInsight, „Wine, Weapons and Whatsapp: A Skopje Spyware Scandal*“ (Víno, zbrně a Whatsapp: Skandál se špionážním softwarem ve Skopje).
[862] Pitchbook, Cytrox overview.
[863] https://www.lighthousereports.nl/investigation/flight-of-the-predator/.
[864] Citizen Lab, „*Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*“ (Pegasus vs. Predator: Dvakrát infikovaný iPhone disidenta odhaluje špionážní software Cytrox Mercenary).
[865] Citizen Lab, „*Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*“ (Pegasus vs. Predator: Dvakrát infikovaný iPhone disidenta odhaluje špionážní software Cytrox Mercenary).

Řecku, Indonésii, na Madagaskaru, v Ománu, Saúdské Arábii a Srbsku[866].

AMESYS A NEXA TECHNOLOGIES

484. Součástí Intellexa Alliance jsou rovněž společnosti Amesys a Nexa Technologies a jak bylo popsáno v kapitole o Francii, ani jim se nevyhýbají skandály.

POLTREX

485. Společnost Poltrex byla založena v říjnu 2018 a jejím jediným akcionářem byla Intellexa Ltd registrovaná na Britských Panenských ostrovech. V září 2019 byl jako ředitel společnosti Poltrex zapsán Izraelec Shahak Avni, zakladatel kyperské společnosti NCIS Intelligence Services Ltd[867] a společník Tala Diliana. V říjnu 2019 se Avni i Dilian stali spoluřediteli a název Poltrex byl změněn na Alchemycorp Ltd. Bez ohledu na změnu názvu sídlila společnost stále v Novel Tower – na stejné adrese jako společnost WiSpear[868].

486. V době, kdy probíhalo šetření týkající se špionážního softwaru Dilianovy společnosti, bylo vlastnictví společnosti Alchemycorp Ltd. převedeno na Yarona Levgorena, zaměstnance Cytrox Holdings[869]. Podle jeho účtu na LinkedIn v současné době zastupuje společnost Intellexa Apollo Technologies se sídlem v Řecku[870].

VERINT/COGNYTE

487. Verint je izraelsko-americká kybernetická společnost, která má mnoho dceřiných společností po celém světě. Jen v Evropě je společnost Verint registrována v Bulharsku, Nizozemsku, na Kypru, v Německu a ve Francii (údaje z roku 2021). Společnost Verint měla rovněž dceřiné společnosti působící pod názvem Cognyte. Tyto dceřiné společnosti působí nezávisle od roku 2021, kdy společnost Verint dokončila převod svých zpravodajských a kybernetických činnosti na společnost Cognyte[871]. Evropské dceřiné společnosti Cognyte jsou registrovány na Kypru (UTX Technologies), v Bulharsku (Cognyte Bulgaria EOOD), v Nizozemsku (Cognyte Netherlands B.V.), v Německu (Syborg GmbH, Syborg Grundbesitz GmbH a Syborg Informationsysteme b.h. OHG) a v Rumunsku (Cognyte Romania S.R.L.)[872].

488. Společnost Verint prodala nástroje dohledu několika represivním vládám, mimo jiné do Ázerbájdžánu, Indonésie a Jižního Súdánu. V případě posledně jmenované země používala odposlouchávací zařízení společnosti Verint jihosúdánská národní bezpečnostní služba (NSS) proti aktivistům v oblasti lidských práv a novinářům v

---

[866] Citizen Lab, „*Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*“, (Pegasus vs. Predator: Dvakrát infikovaný iPhone disidenta odhaluje špionážní software Cytrox Mercenary). 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* (SPIS: Stát urazil Avniho a Diliana).

[868] CyprusMail, „*Akel says found 'smoking gun' linking Cyprus to Greek spying scandal*“ (Akel tvrdí, že našel „kouřící zbraň“ spojující Kypr s řeckým špionážním skandálem).

[869] Philenews, „*How the spyware scandal in Greece is related to Cyprus*“ (Jak souvisí skandál se spywarem v Řecku s Kyprem).

[870] https://ca.linkedin.com/in/yaron-levgoren-116948101.

[871] Calcalistech, „*Verint completes spin-off of its defense activities into new company Cognyte Software*“ (Společnost Verint dokončila převod svých obranných aktivit do nové společnosti Cognyte Software).

[872] https://www.sec.gov/Archives/edgar/data/1824814/000182481421000007/exhibit81.htm.

období od března 2015 do února 2017. Podle průzkumu Amnesty International umožnil místní mobilní operátor Vivacell Network of the World službě NSS odposlouchávat všechny telekomunikace v zemi[873]. Společnost Verint na otázky organizace Amnesty International neodpověděla, ale zveřejnila prohlášení, v němž uvádí, že nezávisle fungující jednotka Cognyte společnosti Verint je ve skutečnosti obrannou jednotkou, zatímco Verint se zabývá výhradně zapojením zákazníků. Společnost Verint tvrdí, že k oddělení od společnosti Cognyte došlo již mnoho let před oficiálním odštěpením v roce 2021, čímž se distancovala se od údajného vývozu sledovacích zařízení do zemí se špatnou situací v oblasti lidských práv[874].

489. Společnost Cognyte se v minulosti rovněž podílela na vývozu do zemí se špatnou situací v oblasti lidských práv. V rámci šetření společnosti Meta z roku 2021 byli identifikováni zákazníci v Izraeli, Srbsku, Kolumbii, Keni, Maroku, Mexiku, Jordánsku, Thajsku a Indonésii[875]. Dceřiná společnost firmy Cognyte, UTX Technologies, registrovaná na Kypru, údajně v období od září 2014 do března 2015 obdržela také licence na vývoz monitorovacího softwaru do Mexika, Spojených arabských emirátů, Nigérie, Izraele, Peru, Kolumbie, Brazílie, Jižní Koreje a Thajska[876]. Čtyři z těchto zemí byly také identifikovány jako zákazníci společnosti Cognyte ve zprávě Meta 2021. Kromě toho společnost UTX Technologies získala také dohodu s Bangladéšem na systém Web Intelligence System za 2 miliony USD v roce 2019 a na buňkový sledovací systém za 500 000 USD v roce 2021[877].

490. Dne 15. ledna 2023 sdělovací prostředky oznámily, že izraelská společnost Cognyte Software Ltd vyhrála nabídkové řízení na prodej svého špionážního softwaru Myanmaru, a to měsíc před vojenským převratem, k němuž došlo v únoru 2021. Nákup špionážního softwaru společnosti Cognyte Myanmarem se oficiálně uskutečnil dne 30. prosince 2020[878].

491. Kromě vývozu do třetích zemí společnost Cognyte rovněž zajišťovala přepravu sledovacího zařízení do členských států. Prostřednictvím společnosti UTX Technologies registrované na Kypru byla technologie Gi2 odeslána do jiné dceřiné společnosti Cognyte v Německu pod názvem Syborg Informationsysteme[879]. Tato technologie Gi2 byla údajně rovněž zaslána dceřiné společnosti Verint v Polsku „pro demonstrační účely“. Technologie Gi2 je schopna získat přístup ke konkrétnímu zařízení, a dokonce si může přisvojit totožnost majitele a prostřednictvím téhož zařízení zasílat falešné

[873] Haaretz, „*Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds*“ (Izraelská kybernetická firma prodala Jižnímu Súdánu špionážní techniku, zjistilo vyšetřování); Amnesty International, „*South Sudan: rampant abusive surveillance by NSS instils climate of fear*“ (Jižní Súdán: bezuzdné zneužívání dohledu ze strany NSS vyvolává atmosféru strachu).
[874] Haaretz, „*Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds*“ (Izraelská kybernetická firma prodala Jižnímu Súdánu špionážní techniku, zjistilo vyšetřování);
[875] Meta, „*Threat Report on the Surveillance-for-Hire Industry*“ (Zpráva o hrozbách v odvětví nájemního sledování).
[876] Philenews, „*Cyprus is a pioneer in software exports*“ (Kypr je průkopníkem ve vývozu softwaru), dokumenty.
[877] Haaretz, „*Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record*“ (Izraelská špionážní technika prodána Bangladéši navzdory špatným výsledkům v oblasti lidských práv).
[878] „*Israel's Cognyte won tender to sell intercept spyware to Myanmar before coup, documents show*“ (Izraelská společnost Cognyte vyhrála výběrové řízení na prodej špionážního softwaru pro odposlech Myanmaru před převratem, ukazují dokumenty).
[879] https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex81.htm.

zprávy[880]. Tyto dodávky se uskutečnily v letech 2013 až 2014. V té době byly společnosti Verint a Cognyte stále součástí téže struktury společnosti.

492. Společnost UTX Technologies rovněž v roce 2013 prodala systémy sledování francouzské vývozní společnosti pod názvem COFREXPORT[881]. Tato společnost ukončila svou činnost a je v době vzniku tohoto textu je uzavřena.

493. Stejně jako v případě mnoha dalších prodejců špionážního softwaru je struktura společnosti Cognyte velmi složitá, a to kvůli změnám názvu, rozdělením a odštěpením, které se v průběhu času uskutečnily. Na příkladu dceřiných společností Cognyte je však patrné, že členské státy EU jsou používány nejen jako základny k vývozu sledovacích zařízení z Evropy, ale také k tomu, aby jako základny pro prodej a distribuci zařízení pro sledování v rámci Evropy. Izraelské společnosti zabývající se špionážním softwarem tak těží z vnitřního trhu EU, což usnadňuje přepravu jejich vybavení jak do jejich vlastních dceřiných společností, tak do nových společností registrovaných v členských státech EU.

QUADREAM

494. QuaDream je izraelská společnost, kterou založili bývalý vysoký úředník izraelské vojenské rozvědky Ilan Dabelstein a bývalí zaměstnanci NSO Guy Geva a Nimrod Rinsky. Společnost je známá především díky svému spywarovému produktu Reign, který údajně využívá zneužití bez kliknutí a obsahuje funkci sebezničení, která vymaže všechny stopy po infekci. Tento typ špionážního softwaru má různé funkce, například nahrávání zvuku, sledování polohy, vyhledávání souborů a pořizování snímků prostřednictvím obou kamer.[882]

495. Podle organizace Citizen Lab a analýzy společnosti Microsoft Threat Intelligence fungují systémy QuaDream v Bulharsku, České republice, Maďarsku, Rumunsku, Ghaně, Izraeli, Mexiku, Singapuru, Spojených arabských emirátech a Uzbekistánu. Kromě toho bylo zjištěno, že nejméně pět cíl z řad občanské společnosti se nachází v Severní Americe, střední Asii, jihovýchodní Asii, Evropě a na Blízkém východě.[883]

496. V roce 2017 byla na Kypru zaregistrována společnost s názvem InReach. Tato společnost byla založena výhradně za účelem propagace výrobků společnosti QuaDream, jako je Reign, mimo Izrael. Společnost QuaDream údajně používala InReach k prodeji svých výrobků zákazníkům, aby obešla izraelské vývozní kontroly. Mnoho klíčových zaměstnanců obou společností pracovalo pro NSO Group, Verint a

---

[880] Philenews, „*Cyprus is a pioneer in software exports*“ (Kypr je průkopníkem ve vývozu softwaru), dokumenty.
[881] Philenews, „*Cyprus is a pioneer in software exports*“ (Kypr je průkopníkem ve vývozu softwaru), dokumenty.
[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.
[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/.

UT-X Technologies.[884]

497. V návaznosti na zprávy organizace Citizen Lab a analýzu Microsoft Threat Intelligence bylo 16. dubna 2023 oznámeno, že společnost QuaDream zastavila svou činnost v Izraeli. Podle listu Haaretz se společnost v předchozích měsících potýkala s poklesem tržeb a odchody zaměstnanců[885].

CANDIRU

498. Candiru je další společnost registrovaná v Izraeli, která produkuje špionážní software. Založili ji v roce 2014 Ya'acov Weitzman a Eran Shorer. Oba působili v „jednotce 8200" zpravodajské služby izraelské armády a oba jsou bývalými zaměstnanci NSO Group[886]. Největším akcionářem společnosti Candiru se stal bývalý investor NSO Group Isaac Zack. Společnost prodává špionážní software pro hackerské útoky na počítače a servery[887]. Zveřejněné informace o návrhu projektu zdůrazňují, že Candiru prodává své produkty na základě počtu současných infekcí, tj. počtu zařízení, která mohou být v jednom okamžiku napadena spywarem. Například za 16 milionů USD obdrží zákazník neomezený počet pokusů o napadení špionážním softwarem, ale souběžně může útočit pouze na 10 zařízení. Za dalších 1,5 milionu USD si zákazník může zakoupit kapacitu zaútočit na dalších 15 zařízení[888].

499. Podle dotazu TheMarker nyní Candiru nabízí také spyware pro pronikání do mobilních zařízení[889]. Svůj špionážní software prodává pouze vládám a má zákazníky v Evropě, bývalém Sovětském svazu, Perském zálivu, Asii a Latinské Americe[890]. V části věnované Španělsku je uvedeno, že špionážním softwarem bylo napadeno 65 osob: z nich se na čtyři zaměřil software Candiru a nejméně na dva Candiru i Pegasus[891].

500. Stejně jako u ostatních prodejců špionážního softwaru je jádrem této společnosti i „zastírání podniku", neboť v posledních letech prošla několika změnami názvu. Společnost změnila svůj název na DF Associates Ltd. v roce 2017, Grindavik Solutions Ltd v roce 2018, Taveta Ltd v roce 2019 a poslední změna byla na Saito Tech Ltd v

---

[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*" (Jsme na černé listině USA kvůli vám Špinavý střet mezi izraelskými výrobci kybernetických zbraní).

[887] Haaretz, „*Cellphone Hacking and Millions in Gulf Deals:Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*" (Hackerské útoky na mobilní telefony a miliony z obchodů v Perském zálivu: vnitřní fungování přísně tajné izraelské firmy pro kybernetické útoky odhaleno).

[888] Citizen Lab, „*Hooking Candiru:Another Mercenary Spyware Vendor Comes into Focus*" (Zachycení Candiru: Do centra pozornosti se dostává další námezdní prodejce spywaru).

[889] Haaretz, „*Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed*" (Hackerské útoky na mobilní telefony a miliony z obchodů v Perském zálivu: vnitřní fungování přísně tajné izraelské firmy pro kybernetické útoky odhaleno).

[890] Citizen Lab, „*Hooking Candiru*: *Zachycení Candiru: Another Mercenary Spyware Vendor Comes into Focus*" (Do centra pozornosti se dostává další námezdní prodejce spywaru).

[891] Citizen Lab, „*CatalanGate*. *Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru*" (Rozsáhlé žoldácké operace špionážního softwaru proti Kataláncům s využitím programů Pegasus a Candiru).

roce 2020[892]. V zájmu srozumitelnosti budeme na společnost odkazovat jako na společnost Candiru.

501. Stejně jako NSO Group byla společnost Candiru Ministerstvem obchodu USA v listopadu 2021 zařazena na černou listinu USA. Spekuluje se, že důvodem pro zařazení společnosti Candiru na černou listinu je skutečnost, že generální ředitel skupiny CEO Shalev Hulio byl údajně tajným partnerem ve společnosti Candiru a představil tuto společnost důležitým prostředníkům ve světě zpravodajských služeb. Pan Hulio údajně dokonce tvrdil, že produkt Candiru je vlastně přebalením produktu Pegasus[893]. Dne 1. července 2022 identifikovali bezpečnostní výzkumníci nový případ zneužití nultého dne v prohlížeči Chrome, který Candiru použil k napadení osob v Libanonu, Palestině, Jemenu a Turecku[894]. Zneužití řešila společnost Google a od té doby bylo opraveno také společnostmi Microsoft a Apple[895].

TYKELAB A RCS LAB

502. V srpnu 2022 bylo ve zprávě organizace Lighthouse uvedeno, že Tykelab, společnost se sídlem v Římě a patřící společnosti RCS Lab, využívá desítky telefonních sítí, často na ostrovech v jižním Tichomoří, aby po celém světě rozesílala desítky tisíc tajných „sledovacích balíčků“, které útočí na osoby v zemích, jako je Itálie samotná, Řecko, Makedonie, Portugalsko, Libye, Kostarika, Nikaragua, Pákistán, Malajsie, Irák a Mali. Tykelab využívá slabá místa v globálních telefonních sítích, která třetím stranám umožňují určit polohu telefonních uživatelů a případně odposlouchávat jejich hovory, aniž by to na dotčených zařízeních zanechalo jakékoli kompromitující záznamy[896]. V červnu 2022 prozkoumala tato společnost sítě v téměř každé zemi světa za pouhé dva dny[897]. Na svých internetových stránkách Tykelab uvádí, že „kombinuje dvacet let zkušeností s navrhováním, prováděním a údržbou řešení v oblasti hlavních telekomunikačních sítí s vysoce odbornými znalostmi v oblasti poskytování řízených služeb, integrace systémů zaměřených na zákazníky a vývoje mobilních aplikací“[898].

503. Šetření organizace Lighthouse rovněž zdůraznilo úlohu telekomunikačního odvětví, neboť pronájem přístupových bodů k telefonní síti nebo „globálních titulů“ umožňuje, aby toto zneužívání pokračovalo. Podle sdružení GSM Associaton, odvětvové organizace zastupující operátory mobilních sítí po celém světě, nemohou telefonní operátoři vždy identifikovat zdroj a účel provozu, který protéká jejich sítěmi, což zastavení těchto praktik ztěžuje[899].

504. Tykelab je součástí italské společnosti RCS Lab, která je známá svými aktivitami v oblasti odposlechů v Itálii i v zahraničí. Na to upozornilo oznámení třetí společnosti

---

[892] Citizen Lab, „*Hooking Candiru*: *Zachycení Candiru: Another Mercenary Spyware Vendor Comes into Focus*“ (Do centra pozornosti se dostává další námezdní prodejce spywaru).
[893] Haaretz „*We’re on the U.S. Blacklist Because of You: The Dirty Clash Between Israeli Cyberarms Makers*“ (Jsme na černé listině USA kvůli vám Špinavý střet mezi izraelskými výrobci kybernetických zbraní).
[894] TechCrunch, „*Spyware maker Candiru linked to Chrome zero-day targeting journalists*“ (Tvůrce spywaru Candiru je spojen se zero-day v prohlížeči Chrome, který se zaměřuje na novináře).
[895] The HackerNews, „*Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists*“ (Spyware Candiru zachycen při zneužívání zero-day v prohlížeči Google Chrome k cílení na novináře).
[896] https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[897] https://euobserver.com/digital/155849.
[898] http://www.tykelab.it/wp/about/.
[899] https://www.lighthousereports.nl/investigation/revealing-europes-nso/.

Cy4Gate, která získala RCS Lab. Společnost RCS Lab má pobočky ve Francii, Německu a Španělsku[900] a další skrytou dceřinou společnost Azienda Informatica Italiana, která vytváří software pro odposlech na zařízeních Android a iPhone[901].

ŠPIONÁŽNÍ SOFTWARE HERMIT

505. Společnost RCS Lab vyvinula špionážní software Hermit, který lze použít k dálkové aktivaci mikrofonu cílového telefonu, k zaznamenávání hovorů a k přístupu ke zprávám, záznamům o hovorech, kontaktům a fotografiím[902]. V červnu 2022 skupina pro analýzu hrozeb společnosti Google odhalila, že státem podporované subjekty používající špionážní software společnosti RCS Lab spolupracovaly s poskytovateli internetových služeb na vypnutí mobilního datového připojení sledované osoby. Jakmile bylo připojení vypnuto, útočník zaslal sledované osobě prostřednictvím SMS odkaz a požádal ji, aby si nainstalovala aplikaci, díky které se jí připojení obnoví. Společnost Google se domnívá, že to je důvod, proč se většina aplikací vydávala za aplikace mobilního operátora. Pokud není možné využít poskytovatele internetových služeb, vydávají se tyto aplikace za aplikace pro zasílání zpráv. Oběti napadené špionážním softwarem společnosti RCS Lab se nacházely v Itálii a Kazachstánu[903] a software byl nalezen i v Rumunsku[904].

506. Výzkumný pracovník společnosti Lookout v oblasti kybernetické bezpečnosti Justin Albrecht uvedl, že ačkoli metoda instalace softwaru Hermit je méně sofistikovaná než metoda využívaná softwarem Pegasus, jeho schopnosti jsou podobné. Hermit potřebuje, aby uživatel telefonu kliknul na infikovaný odkaz, a ten pak zařízení napadne[905].

507. Podle společnosti RCS Lab „se jakýkoli prodej nebo zavedení produktu realizuje až po obdržení úředního povolení od příslušných vnitrostátních orgánů. Výrobky dodávané zákazníkům jsou instalovány v jejich zařízeních a pracovníci RCS Lab nemohou za žádných okolností vykonávat operační činnosti na podporu zákazníka nebo mít přístup ke zpracovávaným údajům. Vzhledem k závazným dohodám o důvěrnosti nemůže společnost RCS Lab zveřejnit žádné podrobnosti o svých zákaznících. Skupina Cy4gate, jejímž členem je RCS Lab, se řídí iniciativou OSN Global Compact, a proto odsuzuje všechny formy porušování lidských práv. Produkty společnosti RCS Lab mají jasný, konkrétní a výhradní účel: podporovat donucovací orgány při předcházení ohavným trestným činům a při jejich potlačování.“[906]. Není však možné ověřit, zda skupina Cy4gate, včetně RCS Lab, své vlastní deklarované standardy dodržuje.

508. Podle šetření Lighthouse Reports zveřejněných v srpnu 2022 byl sledovací nástroj společnosti Tykelab Hermit použit ke sledování lidí na celém světě, včetně Libye, Nikaraguy, Malajsie, Kostariky, Iráku, Mali, Řecka a Portugalska, jakož i v samotné

[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.
[906] https://euobserver.com/digital/155849.

Itálii[907].

DECISION SUPPORTING INFORMATION RESEARCH AND FORENSIC (DSIRF)

509. Společnost, která se nedávno stala předmětem trestního řízení rakouského ministerstva spravedlnosti, je DSIRF GmbH (LLC)[908]. Rakouská společnost DSIRF se sídlem ve Vídni a mateřskou společností v Lichtenštejnsku byla založena v roce 2016. Tvrdí, že poskytuje „služby šité na míru v oblasti informačního výzkumu, forenzních služeb a zpravodajství založeného na datech nadnárodním společnostem v technologickém, maloobchodním, energetickém a finančním sektoru“[909]. DSIRF své služby zjevně prodává nestátním subjektům.

510. Společnost DSIRF vyvinula špionážní software nazývaný Subzero/KNOTWEED, který lze nasadit s použitím zranitelností nultého dne ve Windows a Adobe Reader a který – podle své vlastní reklamy – může být na cílovém zařízení tajně instalován. Po instalaci převezme software Subzero „úplnou kontrolu nad napadeným počítačem“ a poskytne „úplný přístup ke všem údajům a heslům“. Zákazníci tohoto softwaru mohou získávat hesla, snímky obrazovky, prohlížet aktuální a předchozí lokace a „mít přístup, k souborům na cílovém počítači, stáhnout je, upravit je a nahrávat je“ prostřednictvím internetového rozhraní. DSIRF propaguje software Subzero jako prostředek pro „kybernetickou válku nové generace“, přičemž uvádí, že nástroj byl „navržen pro kybernetickou éru“[910]. V roce 2020 ohodnotila společnost DSIRF svůj software Subzero na 245 milionů EUR.

511. Napojení na Rusko je zřejmé z vazeb několika vysoce postavených zaměstnanců DSIRF. Vlastníkem společnosti DSIRF je Peter Dietenberger, „manažer s nejlepšími vazbami v Kremlu“ a „člověk, jenž v Putinově říši otevírá dveře západním společnostem“[911]. Dietenberger žil několik let v Rusku, vlastnil ruskou společnost a měl několik ruských obchodních partnerů. Jeden z jeho ruských obchodních partnerů, Boris Vasiljev, byl rovněž členem správní rady DSIRF. Společnost DSIRF uvádí pro svou firmu a produkty několik referencí: Michael Harms (CEO Ost-Ausschuss der Deutschen Wirtschaft – německého sdružení zahraničního obchodu), Stephan Fanderl (předseda správní rady Galeria Karstadt Kaufhof, který chtěl do Ruska přivést Walmart), Christian Kremer (bývalý prezident BMW v Rusku a generální ředitel společnosti Russian Machines, na niž USA od roku 2018 uvalují sankce) a Florian Schneider (partner velké obchodní advokátní kanceláře Dentons v Moskvě)[912]. Russian Machines, společnost vlastněná oligarchou Olegem Deripaskou, údajně využívá služeb DSIRF. Mocný místní podnikatel Siegfried „Sigi“ Wolf, který radil straně bývalého kancléře Sebastiana Kurze v hospodářských otázkách, je považován za Deripaskova

[907] Lighthouse Reports, „*Revealing Europe's NSO*“ (Rozkrytí evropské NSO), https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[908] DSIRF je zkratka pro „*Decision Supporting Information Research and Forensic*“ (Rozhodnutí na podporu výzkumu v oblasti informací a forenzních věd).
[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.
[912] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/.

důvěrníka[913]. Figuruje zde i Jan Marsalek, označovaný za zločince a hledaný na základě zatýkacího rozkazu Interpolu z důvodu obvinění z obchodních podvodů ve výši miliard, mimo jiných finančních a hospodářských trestných činů. V srpnu 2018 obdržel e-mail od Floriana Stermanna (generálního tajemníka Rusko-rakouské společnosti přátelství, který byl při vyšetřování státním zastupitelstvím považován za „důvěrníka“ FPÖ)[914] s prezentací společnosti DSIRF. Již v roce 2013 se Marsalek údajně pokusil prodat špionážní software italské společnosti Hacking Team společnosti Grenada. V současné době se má skrývat v Moskvě, a to pod dohledem ruské tajné služby FSB[915]

512. V červenci 2022 společnost Microsoft zjistila, že byl software Subzero použit k nepovolené a nekalé činnosti k útokům na právnické firmy, banky a strategické poradenské společnosti v Rakousku, Spojeném království a Panamě[916]. Rakousko v současné době nemá žádný právní základ pro nepovolené zavádění špionážního softwaru, jako je Subzero, orgány veřejné moci a je rovněž nezákonné, pokud by jej jedna soukromá společnost použila proti jiné. Po zveřejnění oznámení společnosti Microsoft dne 28. července 2022 podala rakouská nevládní organizace Epicenter.works působící v oblasti digitálních práv trestní oznámení na DSIRF u státního zastupitelství ve Vídni za nezákonný přístup k počítačovému systému, poškození údajů, zasahování do fungování počítačových systémů, podvodné zneužití zpracování údajů, zločinné spolčení a porušení zákona o zahraničním obchodu a platbách, pokud jde o zboží dvojího užití[917]. Dne 7. října 2022 rakouské spolkové ministerstvo práce a hospodářství uvedlo, že společnosti DSIRF neudělilo vývozní licenci[918], a podle rakouského spolkového ministerstva spravedlnosti zahájilo státní zastupitelství ve Vídni proti této společnosti trestní vyšetřování[919]. Používání špionážního softwaru Subzero proti neznámým cílům v Rakousku znamená, že buď soukromý, nebo veřejný orgán v Rakousku tento software použil nelegálně, nebo byl software použit zahraničním subjektem a společnost DSIRF porušila vývozní omezení nebo byl software vyvezen do jiného členského státu a používán z tohoto státu legálně nebo protiprávně proti rakouskému cíli. Vyšetřování stále probíhá.

FinFisher

513. Za zmínku v této zprávě stojí také vyšetřování trestného činu a bankrot společnosti FinFisher, bývalé společnosti zabývající se špionážním softwarem se sídlem v německém Mnichově. FinFisher je síť společností založená v roce 2008 a původně měla silné vazby na britskou síť společností působících pod značkou Gamma. FinFisher

[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] Odpověď rakouského spolkového ministra pro digitální a hospodářské záležitosti Martina Kochera na písemné parlamentní otázky Stephanie Krisperové, 7. října 2022, odkaz 2022–0.575.143 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml
[919]Odpověď spolkové ministryně spravedlnosti Almy Zadićové na písemné parlamentní otázky Stephanie Krisperové, 7. října 2022, odkaz 2022–0.575.216 https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml.

propagovala svůj špionážní software jako „kompletní portfolio pro narušování informačních technologií“, přičemž její software používaly desítky zemí po celém světě[920], včetně 11 členských států EU[921] a 13 „nesvobodných“ zemí[922].

514. V roce 2017 se produkt společnosti Finfisher FinSpy objevil v Turecku na falešné verzi internetových stránek mobilizujících tureckou opozici. Software byl zamaskován jako aplikace ke stažení doporučená účastníkům protivládních demonstrací[923]. Sama společnost FinFisher inzerovala své produkty jako prostředky určené jen k boji proti trestné činnosti. V roce 2019 podaly organizace Gesellschaft für Freiheitsrechte, Reporter ohne Grenzen, blog netzpolitik.org a Evropské středisko pro ústavní a lidská práva trestní oznámení na společnost Finfisher za vývoz špionážního softwaru bez potřebné vývozní licence od německého Spolkového úřadu pro hospodářství a kontrolu vývozu. Tím měla porušit nařízení EU o zboží dvojího užití a odpovídající německé právní předpisy. Na základě tohoto trestního oznámení vyšetřovalo státní zastupitelství v Mnichově společnost FinFisher a v říjnu 2020 prohledalo 15 obchodních prostor skupiny společností FinFisher v Německu a Rumunsku a v soukromých bytech. V roce 2021 schválil okresní soud v Mnichově zablokování bankovních účtů společnosti Finfisher státním zastupitelstvím s cílem zajistit konfiskaci nezákonně nabytých zisků po případném odsouzení této společnosti. Společnost FinFisher však v únoru 2022 vyhlásila platební neschopnost. Její obchodní činnost byla ukončena, kancelář byla uzavřena a všech 22 zaměstnanců bylo propuštěno[924]. Trestní vyšetřování osob odpovědných za činnost společnosti FinFisher stále probíhá.

III. Dokáže Evropská unie reagovat?

515. Některé vlády EU napadají občany EU prostřednictvím výkonného a silně invazivního a intrusivního špionážního softwaru, čímž zneužívají své právo uchýlit se ke sledování v případě ohrožení národní bezpečnosti. To ohrožuje demokracii, zásady právního státu a základní práva jednotlivých občanů. EU má jen málo pravomocí, jak proti těmto hrozbám zasáhnout, a ukazuje se, že je na boj proti potenciální trestné činnosti páchané vnitrostátními orgány špatně vybavená, a to i v případě, že se tato činnost dotýká samotné EU. Podle Smluv zůstává národní bezpečnost ve výlučné pravomoci členských států, ale jejich činnost musí být stále v souladu se základními právy a demokratickými normami zakotvenými v právu EU. Pravomoc EU jednat omezují také politické faktory. Evropská komise jako strážce smluv EU nevyvíjí maximální úsilí při prosazování práva EU pomocí právních nástrojů, které má k dispozici. Komise má tendenci vykládat své pravomoci velmi úzce, neboť se týkají téměř výhradně správného provedení práva EU do vnitrostátního práva. Komise se domnívá, že řešení případů porušení práva EU je výhradní odpovědností vnitrostátních orgánů. V případě zjevného porušování zásad

[920] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; https://wikileaks.org/spyfiles4/customers.html.
[921] Belgie, Česká republika, Estonsko, Itálie, Maďarsko, Německo, Nizozemsko, Rumunsko, Slovensko, Slovinsko a Španělsko.
[922] Angola, Bahrajn, Bangladéš, Egypt, Etiopie, Gabon, Jordánsko, Kazachstán, Myanmar, Omán, Katar, Saúdská Arábie a Turecko.
[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.

právního státu a základních práv se však tento postoj, který nemá žádnou oporu ve Smlouvách EU, stává velmi problematickým. Ačkoli subsidiarita a rozdělení pravomocí jsou pilířem práva EU, neměly by vést k beztrestnosti vlád, které se zaměřují na občany EU pomocí špionážního softwaru pro politické účely. Níže se budeme zabývat pravomocemi, které mají orgány, instituce a subjekty EU k dispozici. Parlament, Komise a Rada mají pravomoc a povinnost přijímat a prosazovat právní předpisy a provádět regulaci a musí tak činit razantně a ambiciózně. Obrana naší demokracie přitom musí mít přednost před krátkodobými politickými hledisky.

Evropská komise

516. V návaznosti na zprávy v tisku o používání špionážního softwaru v členských státech a dotazy výboru PEGA Komise v reakci na skandál se špionážním softwarem nejprve pouze písemně požádala o vysvětlení vlády Polska, Maďarska, Španělska, Řecka, Kypru a Francie. Zdá se však, že po tomto napomenutí nenásledovaly další kroky. Je pravda, že striktně vzato nemá Komise v oblasti národní bezpečnost žádnou pravomoc. Jak však ona sama v těchto dopisech upozorňuje, „národní bezpečnost“ by neměla být vykládána jako neomezená výjimka z evropských právních předpisů a Smluv a stát se oblastí bezpráví. Je však na členských státech, aby „prokázaly, že v konkrétním případě je ohrožena národní bezpečnost“. V odpovědi na otázku týkající se toho, jaká opatření Komise přijme, pokud vnitrostátní orgány důkladně neprozkoumají obvinění z nezákonného sledování, Komise pouze odkázala na Soudní dvůr Evropské unie a článek 47 Listiny, který zaručuje právo na účinné prostředky nápravy před soudem. Zdá se, že chybí politická ochota jednat.

517. Dne 21. prosince 2022 navíc Komise zaslala všem členským státům obecný dopis, v němž požádala o informace o používání špionážního softwaru vnitrostátními orgány a o právním rámci, který toto používání upravuje, za účelem „zmapování situace v členských státech“ a prozkoumání „součinnosti s právem EU“[925]. Komise položila konkrétní otázky týkající se mimo jiné účelu použití špionážního softwaru, orgánů oprávněných k jeho nasazení, vnitrostátní definice národní bezpečnosti, příslušných právních předpisů, které upravují zpracování údajů pro účely národní bezpečnosti, záruk, předchozího povolení soudem nebo nezávislým správním orgánem, dohledu a oznamování, přičemž lhůta pro odpověď byla stanovena do 31. ledna 2023. Dne 28. března 2023 komisař Reynders výboru PEGA sdělil, že velká většina členských států odpověděla, ale že Komise stále shromažďuje odpovědi členských států na toto mapování a že odpovědi „pečlivě posoudí“. Na základě tohoto mapování Komise zváží své možnosti týkající se používání špionážního softwaru v členských státech. Komise však nepředpokládá žádné konkrétní datum ukončení hodnocení, „vzhledem k jeho vývoji a citlivé povaze“. Komise rovněž zmínila, že bude velmi pečlivě sledovat zjištění výboru PEGA.

518. Na rozdíl od USA, které na odhalení reagovaly zařazením společností na černou listinu, provedením vyšetřování, a to i na území EU, a vydáním nařízení zakazujícího federálním orgánům USA pořizovat komerční špionážní software, Komise dosud neprovedla analýzu situace ani posouzení společností, které působí na trhu se špionážním softwarem v EU. Proti provedení takové analýzy zjevně nelze z právního hlediska nic namítat. Je pozoruhodné, že velký počet důkazů stále nepřiměl Komisi k

[925] Dopis GŘ JUST členským státům. Ref.: Ares(2022), 8885417, 21. prosince 2022.

přijetí jakéhokoli smysluplného opatření. Její nečinnost lze v podstatě považovat za napomáhání porušování lidských práv a selhání, pokud jde o její povinnosti.

519. EU má několik právních předpisů, které by v souvislosti se špionážním softwarem mohly sloužit jako regulační nástroje. Kromě právních předpisů na ochranu práv občanů, jako jsou právní předpisy o ochraně údajů a soukromí komunikací (GDPR, směrnice o soukromí a elektronických komunikacích[926]), existují právní předpisy týkající se vývozu (nařízení o zboží dvojího užití) a zadávání veřejných zakázek. Komise jako strážce Smluv však neprovádí jejich prosazování v plném rozsahu. Obvykle se omezuje na ověření toho, zda členský stát správně provedl právní předpisy EU ve svém vnitrostátním právu. To však říká velmi málo o tom, jak vypadá reálná situace na místě. Zpráva Komise o provádění nařízení o zboží dvojího užití[927] tedy zdánlivě dospívá k závěru, že provádění je na dobré cestě, přestože existuje mnoho důkazů o tom, že v praxi je nedostatečné a nejednotné, a v některých zemích dokonce zcela záměrně. Provádění směrnice o soukromí a elektronických komunikacích a judikatury z ní vyplývající je nedostatečné. Komise odkazuje na členské státy jako na odpovědné za provádění a prosazování, ale nepřijímá opatření, pokud členské státy tyto úkoly neplní. Bez řádného a smysluplného prosazování jsou právní předpisy EU neúčinné a vytváří dostatek prostoru pro nelegitimní používání špionážního softwaru.

520. Směrnice o prosazování práva měla poskytnout vysoké standardy ochrany údajů a zajistit volný tok údajů v odvětví prosazování práva a trestního soudnictví. Směrnice měla být provedena ve vnitrostátním právu, přičemž členské státy měly širokou diskreční pravomoc. Dnes je zřejmé, že provádění se liší členský stát od členského státu, zejména v oblasti práv subjektů údajů. Komise by měla urychleně posoudit provádění ve všech členských státech a identifikovat nejzávažnější nedostatky. Měla by vypracovat konkrétní pokyny pro členské státy týkající se provádění směrnice s cílem zajistit, aby byly standardy EU dodržovány v celé Unii. Kromě toho by Komise, je-li to nezbytné, měla zahájit řízení o nesplnění povinnosti v případech, kdy směrnice nebyla řádně provedena a členské státy nejsou ochotny tuto situaci napravit.

Evropský parlament

521. Evropský parlament zřídil vyšetřovací výbor PEGA, který pracuje svědomitě a efektivně v rámci svých pravomocí a mandátu. Nemá však pravomoc předvolávat svědky ani je vyslýchat pod přísahou a nemá přístup k utajovaným informacím. Postrádá plné vyšetřovací pravomoci, které má většina vnitrostátních parlamentů. Kromě toho je při jednáních výboru PEGA často patrný vliv vlád členských států, což v některých případech brání důkladnému, zcela nezávislému a objektivnímu vyšetřování. Je poměrně znepokojivé, že Evropský parlament nemá plné vyšetřovací pravomoci, ačkoli se někteří z jeho vlastních členů stali oběťmi špionážního softwaru.

Evropská rada a Rada ministrů

522. Ačkoli vlády členských států tvrdí, že skandál se špionážním softwarem je čistě vnitrostátní záležitostí, byl ve skutečnosti projednáván v Radě Evropské unie a vlády

[926] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Úř. věst. L 201, 31.7.2002, s. 37).
[927] https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

členských států se rozhodly společně odpovědět na dotazník Evropského parlamentu[928]. Tímto postupem daly plně na vědomí, že se ve skutečnosti jedná o záležitost, kterou by se měla Rada zabývat.

523. Evropská rada dosud na skandál veřejně ani věcně nereagovala. Někteří z jejích členů jsou v této věci zainteresováni, neboť mohou být sami za nelegitimní hackerské útoky spoluodpovědní, nebo si prostě přejí, aby EU v této oblasti zůstala slabá a bezmocná.

524. I pokud by se nezákonné nebo trestné jednání nakonec prokázalo, nebylo by možné členy vlád jednotlivých členských států zprostit úřadu nebo přimět, aby odstoupili ze svých unijních funkcí. To znamená, že osoby, které se těmito činy provinily, budou nejspíše moci i nadále beztrestně zasedat v orgánech, institucích a subjektech EU a přijímat rozhodnutí týkající se všech evropských občanů.

Europol

525. Europol nemá samostatné operativní pravomoci a nemůže jednat bez souhlasu a spolupráce dotčeného členského státu, jak uvádí čl. 88 odst. 3 SFEU, zatímco uplatňování donucovacích opatření je ve výlučné pravomoci příslušných vnitrostátních orgánů. To představuje problém v případech, kdy existují jasné důkazy o trestných činech, jako je kyberkriminalita, korupce nebo vydírání, avšak vnitrostátní orgány nepřistoupí k jejich vyšetřování. Europol nedávno získal nové pravomoci, které mu umožňují navrhnout vyšetřování z vlastní iniciativy, a to i v případě, že se jedná o trestný čin spáchaný pouze v jednom členském státě[929], dosud ale tyto pravomoci nevyužil.

526. Dne 28. září 2022 napsal výbor PEGA Europolu dopis[930], v němž jej naléhavě vyzval, aby svých nových pravomocí podle článku 6 nařízení o Europolu skutečně využíval[931]. Europol ve své písemné odpovědi ze dne 13. října 2022[932] uvedl, že „kontaktoval pět členských států, aby zjistil, zda jsou na vnitrostátní úrovni k dispozici relevantní informace a zda probíhá nebo se plánuje trestní vyšetřování (či případně jiné šetření podle platných ustanovení vnitrostátního práva). Dne 11. dubna 2023 Europol v dopise adresovaném výboru PEGA uvedl, že jeho dopisy byly zaslány Řecku, Maďarsku, Bulharsku, Španělsku a Polsku. V návaznosti na odpovědi pěti členských států na dopisy Europol uvedl, že žádný z nich nemá „relevantní informace, které jsou Europolu k dispozici“. Do října 2022 jeden z pěti členských států Europolu potvrdil, že „bylo zahájeno trestní vyšetřování pod dohledem příslušných justičních orgánů, což ověřil i Eurojust.“ Do prosince 2022 informoval druhý členský stát Europol, „že v souvislosti s podezřením na protiprávní používání softwaru Pegasus bylo zahájeno jedno trestní řízení, které mezitím příslušné justiční orgány v této zemi ukončily“. Třetí členský stát Europolu oznámil, že „bylo zahájeno přípravné řízení na regionální úrovni“, a dotázal

[928] Návrh dopisu generálního sekretariátu Rady delegacím, 26. září 2022.
[929] Nařízení Evropského parlamentu a Rady (EU) 2022/991 ze dne 8. června 2022, kterým se mění nařízení (EU) 2016/794, pokud jde o spolupráci Europolu se soukromými subjekty, zpracování osobních údajů Europolem pro usnadnění trestního vyšetřování a úlohu Europolu v oblasti výzkumu a inovací (Úř. věst. L 169, 27.6.2022, s. 1).
[930] https://twitter.com/EP_PegaInquiry/status/1576855144574377984.
[931] „Pokud se výkonný ředitel domnívá, že by mělo být zahájeno trestní vyšetřování konkrétního trestného činu, který se týká pouze jednoho členského státu, ale dotýká se společného zájmu, jenž je předmětem některé politiky Unie, může prostřednictvím národní jednotky navrhnout příslušným orgánům dotčeného členského státu, aby zahájily, vedly nebo koordinovaly takové trestní vyšetřování.“
[932] Spis č. 1260379.

se, „zda Europol má informace o používání softwaru Pegasus v příslušné zemi, které jsou relevantní pro přípravné řízení.“ Čtvrtý členský stát Europolu sdělil, že „neprobíhá ani se neplánuje trestní vyšetřování“, ale že „soudní vyšetřování bylo zahájeno“. Do dubna 2023 pátý členský stát vysvětlil Europolu, že „po konzultaci s příslušnými orgány v této zemi nemá Europol k dispozici žádné relevantní informace týkající se protiprávního používání rušivého sledovacího a odposlouchávacího softwaru, přičemž odkázal na předběžné řízení státního zastupitelství“. Není známo, zda se výše uvedená trestní řízení dvou členských států, přípravné řízení jednoho členského státu, soudní vyšetřování jednoho členského státu a předběžné řízení státního zastupitelství jiného členského státu týkají zneužití špionážního softwaru vládami členských států EU nebo třetími zeměmi.

527. Ukazuje se, že EU je v boji proti potenciální trestné činnosti páchané vnitrostátními orgány zcela bezmocná, a to i v případě, že se tato činnost dotýká EU.

528. Je paradoxní, že Spojené státy na rozdíl od Europolu používání špionážního softwaru v EU aktivně vyšetřují. Dne 5. listopadu 2022 bylo oznámeno, že zástupci FBI navštívili Atény s cílem prošetřit, „kam až se nezákonné sledování rozšířilo a kdo s ním obchodoval“[933]. V březnu 2023 navíc americký prezident Biden vydal nařízení, které do značné míry zakazuje používání špionážního softwaru federálními subjekty USA. O několik dní později se k mezinárodní spolupráci v této oblasti přihlásily další země, včetně Francie a Dánska.

Evropské soudy

529. Soudní dvůr Evropské unie (SDEU) a Evropský soud pro lidská práva (ESLP) hrají důležitou úlohu při obraně demokracie, právního státu a základních práv. Mohou však jednat pouze na základě žaloby nebo předběžné otázky. Řízení jsou velmi dlouhá a v jednotlivých případech se většinou nelze domoci konkrétní nápravy. V průběhu let vytvořily tyto soudy v dané oblasti rozsáhlou judikaturu, například stanovily normy týkající se sledování. Nemají však žádné prostředky, jak zajistit výkon svých rozhodnutí. Evropský soud pro lidská práva se dosud zabýval jen jednou žalobou ve věci nezákonného používání špionážního softwaru[934]. Cesta ke štrasburskému nebo lucemburskému soudu je nicméně často dlouhá, nákladná a složitá, neboť nejprve musí být vyčerpány všechny možnosti vnitrostátních soudních řízení. Tak je tomu zejména v případě, kdy se státní zástupci nebo soudy odmítnou zabývat určitým případem. Kritéria pro přijetí jsou přísná.

Veřejný ochránce práv

530. Dne 28. listopadu 2022 dospěla veřejná ochránkyně práv EU k závěru, že Komise dostatečně neposoudila rizika v oblasti lidských práv před tím, než poskytla africkým zemím podporu na rozvoj kapacit v oblasti dohledu, zejména v souvislosti s nouzovým svěřenským fondem EU pro Afriku (EUTFA). Její závěry vyplývají ze stížnosti několika organizací občanské společnosti. V Nigeru bylo z fondu přiděleno 11,5 milionu EUR na dodávky vybavení pro sledování, včetně softwaru pro sledování,

[933] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ.
[934] Odvolání, které podal Thanasis Koukakis k Evropskému soudu pro lidská práva, 27. červenec 2022.

odposlechového střediska a zachytávače[935], a to navzdory represím namířeným proti aktivistům v zemi. Veřejná ochránkyně práv navrhla, aby se zjištěné nedostatky odstranily a aby se před budoucími projekty EUTFA provedlo posouzení dopadů na lidská práva.

Další instituce a subjekty EU

531. Evropský sbor pro ochranu osobních údajů, evropský inspektor ochrany údajů, Evropský účetní dvůr a Eurojust mají jen málo pravomocí, aby mohli provádět kontrolu nebo zasáhnout, pokud vlády členských států protiprávně používají špionážní software nebo s ním obchodují. Někteří jejich členové mohou být navíc do těchto skandálů ve svém členském státě původu zapleteni. To může mít dopad na fungování a integritu těchto institucí a subjektů EU. Pokud by se tyto kauzy týkaly finančních prostředků EU, mohl by však zasáhnout Úřad evropského veřejného žalobce.

[935] https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf.

VYSVĚTLUJÍCÍ PROHLÁŠENÍ

Evropská Watergate

V létě 2021 odhalil projekt Pegasus, kolektiv investigativních novinářů, nevládních organizací a výzkumných pracovníků, seznam 50 000 osob, které se staly terčem námezdního špionážního softwaru. Jsou mezi nimi novináři, právníci, státní zástupci, aktivisté, politici, a dokonce i hlavy států. Nejdramatičtějším případem může být případ saúdského novináře Džamála Chášukdžího, který byl v roce 2018 brutálně zavražděn za svou kritiku saúdského režimu. Na seznamu však bylo i mnoho evropských cílů. Některé z nich se staly terčem útoků aktérů mimo EU, jiné však byly terčem útoků jejich vlastních národních vlád. Odhalení se setkalo s rozhořčením po celém světě.

Skandál byl rychle označen za „evropskou Watergate“. Spíše než politický thriller „Všichni prezidentovi muži“ o vloupání do budovy Watergate v roce 1972 však dnešní skandál se špionážním softwarem připomíná mrazivý film „Život těch druhých“ (Das Leben der Anderen) zobrazující sledování občanů totalitním komunistickým režimem. Dnešní digitální loupeže pomocí špionážního softwaru jsou mnohem sofistikovanější a invazivnější a nezanechávají téměř žádné stopy. Použití špionážního softwaru dalece přesahuje rámec běžného sledování osob. Poskytuje aktérům špehování úplný přístup a kontrolu. Na rozdíl od běžného odposlechu umožňuje špionážní software nejen sledování v reálném čase, ale také plný, zpětný přístup k souborům a zprávám vytvořeným v minulosti a k metadatům o minulé komunikaci. Sledování lze provádět i na dálku, v zemích kdekoli na světě. Pomocí špionážního softwaru lze v podstatě převzít kontrolu nad chytrým telefonem a získat veškerý jeho obsah včetně dokumentů, obrázků a zpráv. Takto získané materiály mohou být použity nejen ke sledování činnosti, ale také k vydírání, diskreditaci, manipulaci a zastrašování obětí. Přístup do systému oběti může být zmanipulován a může být podstrčen vykonstruovaný obsah. Mikrofon a kameru lze aktivovat na dálku a proměnit zařízení ve špiona v místnosti. Po celou dobu si oběť není ničeho vědoma. Špionážní software zanechává v cílovém zařízení jen velmi málo stop, a i když je odhalen, je téměř nemožné prokázat, kdo byl za útok zodpovědný.

Zneužívání špionážního softwaru neporušuje pouze právo na soukromí jednotlivců. Skrytě podkopává demokracii a demokratické instituce. Umlčuje opozici a kritiky, vylučuje kontrolu a má mrazivý účinek na svobodný tisk a občanskou společnost. Dále slouží k manipulaci voleb. Termín „námezdní špionážní software“ velmi dobře vystihuje povahu produktu a odvětví. I neúspěšné pokusy o infikování chytrého telefonu špionážním softwarem mají politické důsledky a mohou poškodit jednotlivce i demokracii. Účast na veřejném životě se stává nemožnou bez jistoty svobody a nepozorovanosti.

Skandál se špionážním softwarem není sérií izolovaných případů zneužití v jednotlivých zemích, ale rozsáhlou evropskou aférou. Vlády členských států EU používají špionážní software vůči svým občanům k politickým účelům a k zakrývání korupce a trestné činnosti. Někteří šli ještě dál a do systému záměrně navrženého pro autoritářskou vládu zabudovali špionážní software. Vlády jiných členských států se možná nepodílely na zneužívání špionážního softwaru, ale usnadňovaly neprůhledný obchod s ním. Evropa se stala atraktivním místem pro námezdní špionážní software. Je centrem vývozu do diktátorských a

utlačovatelských režimů, jako je Libye, Egypt a Bangladéš, kde byl špionážní software používán proti aktivistům za lidská práva, novinářům a kritikům vlády.

Zneužívání špionážního softwaru je závažným porušením všech hodnot Evropské unie a je zkouškou odolnosti demokratického právního státu v Evropě. V uplynulých letech EU velmi rychle vybudovala svou schopnost reagovat na vnější hrozby pro naši demokracii, ať už se jedná o války, dezinformační kampaně nebo politické vměšování. Naproti tomu schopnost reagovat na vnitřní ohrožení demokracie je stále žalostně malá. Antidemokratické tendence se mohou volně šířit po celé EU jako gangréna, protože národní vlády se dopouštějí beztrestných prohřešků. EU je špatně vybavena na to, aby se vypořádala s takovým útokem na demokracii zevnitř. Na jedné straně je EU do značné míry politickým subjektem, který se řídí nadnárodními zákony a nadnárodními institucemi, má jednotný trh, otevřené hranice, cestování bez pasu, občanství EU a jednotný prostor bezpečnosti, svobody a práva. Navzdory slavnostním slibům k evropským hodnotám jsou však tyto hodnoty v praxi stále považovány za záležitost jednotlivých států. Skandál se špionážním softwarem nemilosrdně odhaluje nezralost a slabost EU jako *demokratického* subjektu. Pokud jde o demokratické hodnoty, EU je postavena na „předpokladu jejich dodržování“ ze strany národních vlád, ale v praxi se změnila v „předstírané dodržování“. Se scénářem, kdy národní vlády záměrně ignorují a porušují zákony EU, se v řídících strukturách EU jednoduše nepočítá. EU není vybavena nástroji pro tyto případy. Orgány EU mají jen málo pravomocí a ještě méně chuti konfrontovat vnitrostátní orgány v případě prohřešků, a už vůbec ne v citlivé oblasti „národní bezpečnosti“. Podle mezivládní logiky jsou orgány EU podřízeny národním vládám. Bez účinných a smysluplných nadnárodních mechanismů prosazování však budou nové právní předpisy zbytečné. Řešení tohoto problému bude vyžadovat jak regulační opatření, tak reformy správy a řízení.

Útoků na demokracii zevnitř nejsou ušetřeny ani USA, jak ukazuje např. například Watergate a obléhání Kongresu 6. ledna 2021, ale jsou vybaveny k rázné reakci. Mají moc čelit i nejvyšším politickým představitelům, pokud nerespektují zákony a ústavu.

Po odhalení špionážního softwaru v roce 2021 Spojené státy skutečně rychle a rozhodně reagovaly na zjištění v rámci projektu Pegasus. Americké ministerstvo obchodu rychle zařadilo společnost NSO Group na černou listinu, ministerstvo spravedlnosti zahájilo vyšetřování a připravuje se přísná regulace obchodu se špionážním softwarem. FBI dokonce přijela do Evropy vyšetřovat útok špionážním softwarem na dvojího občana USA a Evropy. Technologičtí giganti jako Apple a Microsoft zahájili soudní řízení proti společnostem zabývajícím se špionážním softwarem. Oběti podaly žaloby, státní zástupci vedou vyšetřování a bylo zahájeno parlamentní vyšetřování.

Naproti tomu ostatní instituce EU, s výjimkou Evropského parlamentu, zůstávají do značné míry pasivní a mlčí a tvrdí, že se jedná o výhradně vnitrostátní záležitost.

Evropská rada a národní vlády praktikují omertu. Evropská rada na tento skandál oficiálně nereagovala. Vlády členských států výzvu ke spolupráci s výborem PEGA většinou odmítly. Některé vlády vyloženě odmítly spolupracovat, jiné byly přátelské a zdvořilé, ale ve skutečnosti se o smysluplné informace nepodělily. Dokonce i na jednoduchý dotazník zaslaný všem členským státům ohledně podrobností jejich vnitrostátního právního rámce pro používání špionážního softwaru se téměř nedostalo podstatných odpovědí. Doslova v

předvečer zveřejnění tohoto návrhu zprávy obdržel výbor PEGA prostřednictvím Rady společnou odpověď členských států, rovněž bez jakéhokoli obsahu.

Evropská komise vyjádřila znepokojení a požádala několik vlád členských států o vysvětlení, ale pouze v případech, kdy již na vnitrostátní úrovni vypukl skandál. Komise sdílela – neochotně a po částech – informace o útocích špionážního softwaru na své vlastní úředníky.

Europol zatím odmítl využít svých nových pravomocí a zahájit vyšetřování. Teprve po naléhání Evropského parlamentu se obrátil na pět členských států s dopisem, v němž se dotazoval, zda bylo zahájeno policejní vyšetřování a zda by mohl být nápomocen.

Evropská záležitost

Na zneužívání špionážního softwaru se většinou nahlíží klíčovou dírkou vnitrostátní politiky. Tento úzký vnitrostátní pohled zastírá celkový obraz. Teprve po propojení všech souvislostí je zřejmé, že se jedná o hluboce evropskou záležitost ve všech jejích aspektech.

Ačkoli to není oficiálně potvrzeno, můžeme s jistotou předpokládat, že všechny členské státy EU zakoupily jeden nebo více komerčních produktů špionážního softwaru. Jen jedna společnost, NSO Group, prodala své výrobky dvaadvaceti koncovým uživatelům v nejméně čtrnácti členských státech, mezi nimiž jsou Polsko, Maďarsko, Španělsko, Nizozemsko a Belgie. Přinejmenším ve čtyřech členských státech, Polsku, Maďarsku, Řecku a Španělsku, byl špionážní software používán neoprávněně a existuje podezření na jeho používání na Kypru. Dva členské státy, Kypr a Bulharsko, slouží jako centrum vývozu špionážního softwaru. Jeden členský stát, Irsko, nabízí výhodné daňové podmínky velkému prodejci špionážního softwaru a jeden členský stát, Lucembursko, je bankovním centrem pro mnoho hráčů v tomto odvětví. Domovem každoročního evropského veletrhu špionážního průmyslu ISS World tzv. „plesu odposlouchávačů“ je Praha v České republice. Malta se zdá být pro některé protagonisty obchodu oblíbenou destinací. Několik namátkových příkladů, jak odvětví využívá Evropu bez hranic: Společnost Intellexa je přítomna v Řecku, na Kypru, v Irsku, Francii a Maďarsku a její generální ředitel má maltský pas a spolčenost (typu poštovní schránka). Společnost NSO je přítomna na Kypru a v Bulharsku a své finanční obchody provozuje prostřednictvím Lucemburska. DSIRF prodává své výrobky z Rakouska, Tykelab z Itálie, FinFisher z Německa (před uzavřením).

Obchod se špionážním softwarem těží z vnitřního trhu EU a volného pohybu. Některé země EU jsou atraktivní jako exportní centrum, protože navzdory pověsti EU jako přísného regulátora je vymáhání vývozních předpisů slabé. Po zpřísnění pravidel pro vývoz z Izraele se EU stala pro prodejce atraktivnější. Své podnikání inzerují jako „regulované EU“ a jako označení kvality používají svou přítomnost v EU. „EU“ zaručuje respekt. Členství v EU je výhodné i pro vlády, které chtějí špionážní software nakupovat: Členské státy EU jsou osvobozeny od individuálního posouzení lidských práv, které je vyžadováno pro získání vývozní licence od izraelských orgánů, neboť členství v EU je považováno za dostatečnou záruku dodržování nejpřísnějších norem.

Prodejní stránka obchodu se špionážním softwarem je neprůhledná a nepostižitelná, ale lukrativní a vzkvétající. Struktury společností jsou příhodně, ne-li záměrně, složité, aby skryly před zraky nežádoucí aktivity a vazby, včetně vazeb na vlády EU. Na papíře je toto odvětví regulováno, ale v praxi se mu daří mnohá pravidla obcházet, mimo jiné proto, že spyware je

produkt, který může sloužit jako politická měna v mezinárodních vztazích. Společnosti zabývající se špionážním softwarem jsou usazeny v několika zemích, ale mnoho z nich založili bývalí důstojníci izraelské armády a zpravodajských služeb. Většina prodejců tvrdí, že prodává pouze státním subjektům, ačkoli v zákulisí někteří prodávají i nestátním subjektům. Je prakticky nemožné získat jakékoli informace o těchto zákaznících nebo o smluvních podmínkách a jejich dodržování.

Obchodování se špionážním softwarem a jeho používání spadá přímo do oblasti působnosti práva a judikatury EU. Nákup a prodej špionážního softwaru se řídí mimo jiné pravidly pro zadávání veřejných zakázek a pravidly pro vývoz, jako je nařízení o dvojím užití. Používání špionážního softwaru musí být v souladu s normami GDPR, EUDPR, LED a směrnice o ochraně soukromí v elektronické podobě. Práva dotčených osob jsou stanovena v Listině základních práv a mezinárodních úmluvách, zejména právo na soukromí a právo na spravedlivý proces, a v předpisech EU o právech podezřelých a obviněných; Zneužití špionážního softwaru bude v mnoha případech představovat počítačovou kriminalitu a může mít za následek trestné činy korupce a vydírání, které spadají do působnosti Europolu. Pokud se jedná o evropské finanční prostředky, má mandát jednat evropský veřejný žalobce. Zneužívání špionážního softwaru může také ovlivnit policejní a justiční spolupráci, zejména sdílení informací a provádění evropského zatýkacího rozkazu a důkazního příkazu.

Zneužívání špionážního se přímo i nepřímo dotýká EU a jejích orgánů. Mezi těmi, na které byl špionážní software zaměřen, byli i členové Evropského parlamentu, Evropské komise a (Evropské) rady. Ostatní byli postiženi jako „vedlejší úlovky“, nepřímé cíle. Naopak, někteří z „pachatelů“ zasedají i v (Evropské) radě. Manipulace s vnitrostátními volbami pomocí špionážního softwaru navíc přímo ovlivňuje složení orgánů EU a politickou rovnováhu v řídících orgánech EU. Čtyři nebo pět vlád obviněných ze zneužívání špionážního softwaru představuje téměř čtvrtinu obyvatel EU, takže mají v Radě značnou váhu.

Špionážní software jako součást systému

Špionážní software není pouhým technickým nástrojem používaným ad hoc a izolovaně. Používá se jako nedílná součást systému. Jeho používání je v zásadě zakotveno v právním rámci a je doprovázeno nezbytnými zárukami, mechanismy dohledu a kontroly a prostředky nápravy. Šetření ukázalo, že tato ochranná opatření jsou často slabá a nedostatečná. To je většinou neúmyslné, ale v některých případech byl systém – částečně nebo zcela – přizpůsoben nebo navržen záměrně tak, aby sloužil jako nástroj politické moci a kontroly. V těchto případech není nelegální použití špionážního softwaru náhodou, ale součástí promyšlené strategie. Vláda práva se mění v právo vládce. Právní základ pro sledování může být formulován vágně a nepřesně, aby se legalizovalo široké a neomezené používání špionážního softwaru. Kontrola *ex ante* v podobě soudního povolení ke sledování může být snadno zmanipulována a zbavena jakéhokoli významu, zejména v případě politizace nebo ovládnutí soudnictví státem. Kontrolní mechanismy mohou zůstat slabé a neúčinné a mohou být pod kontrolou vládnoucích stran. Právní prostředky nápravy a občanská práva mohou existovat na papíře, ale tváří v tvář obstrukcím ze strany vládních orgánů se stávají neplatnými. Stěžovatelům je odepřen přístup k informacím, a to i k obviněním, která údajně odůvodňují jejich sledování. Státní zástupci, soudci a policie odmítají vyšetřování a často přenášejí důkazní břemeno na oběti, od nichž očekávají, že prokáží, že se staly terčem špionážního softwaru. Oběti se tak ocitají v situaci „Hlava 22“, protože je jim odepřen přístup k informacím. Vládní strany mohou zpřísnit kontrolu veřejných institucí a médií, aby zadusily

smysluplnou kontrolu. Veřejnoprávní nebo komerční média blízká vládě mohou sloužit jako kanál pro pomlouvačné kampaně využívající materiály získané pomocí špionážního softwaru. „Národní bezpečnost“ je často uváděna jako záminka pro odstranění transparentnosti a odpovědnosti. Všechny tyto prvky dohromady tvoří systém určený k ovládání a utlačování. To nejenže ponechává jednotlivé oběti zcela bezbranné vůči všemocné vládě, ale také to znamená, že byly znemožněny všechny důležité brzdy a protiváhy demokratické společnosti.

Některé vlády již tohoto bodu dosáhly, jiné jsou na půli cesty. Většina evropských vlád se naštěstí touto cestou nevydá. Pokud se tak stane, není EU ve svém současném institucionálním a politickém uspořádání schopna tomu zabránit nebo čelit. Špionáž je jako kanárek v uhelném dole: odhaluje nebezpečné ústavní slabiny EU.

Utajení

Hlavní překážkou při odhalování a vyšetřování nelegálního používání špionážního softwaru je utajení.

Většina obětí nemá možnost získat od úřadů žádné informace o svém případu. V mnoha případech se úřady odvolávají na důvody národní bezpečnosti jako odůvodnění utajení, v jiných případech prostě popírají existenci spisu nebo spisy zničí. Zároveň státní zástupci často odmítají tyto případy vyšetřovat s odůvodněním, že oběti nemají dostatečné důkazy. Jedná se o začarovaný kruh, který nechává oběti bez možnosti odvolání.

Vlády nejčastěji odmítají zveřejnit, zda a jaký typ špionážního softwaru zakoupily. Prodejci špionážního softwaru stejně tak odmítají zveřejnit, kdo jsou jejich zákazníci. Vlády se často uchylují ke zprostředkovatelům, zástupcům nebo osobním kontaktům, aby zakoupily komerční špionážní software nebo služby související se špionážním softwarem a skryly tak svou účast. Obcházejí pravidla pro zadávání veřejných zakázek a rozpočtové postupy, aby nezanechaly žádné vládní otisky.

Izrael je důležitým centrem společností vyrábějících špionážní software a je zodpovědný za vydávání licencí pro uvádění na trh a vývozních licencí. Ačkoli jsou Izrael a Evropa blízkými spojenci, Izrael neposkytuje žádné informace o vydávání (nebo rušení) licencí na špionážní software zemím EU, přestože je využíván k porušování práv evropských občanů a k podkopávání naší demokracie.

Žádosti novinářů o svobodný přístup k informacím přinášejí jen málo informací nebo vůbec žádné. Se získáváním informací se potýkají i specializované kontrolní a dohledové orgány, jako jsou orgány pro ochranu údajů nebo Účetní dvůr. Nezávislý dohled nad tajnými službami je notoricky známý jako slabý a často vůbec neexistuje. Parlamentní vyšetřovací výbory jsou vládními stranami často blokovány. Soudní vyšetřování se zaměřuje na hackerské útoky třetích zemí, nikoli na nezákonné používání vládami EU. Novináři, kteří o této problematice informují, čelí strategickým žalobám proti účasti veřejnosti (SLAPP), slovním útokům ze strany politiků nebo pomlouvačným kampaním. Odvážní a pilní novináři, kteří odhalují fakta o tomto skandálu, si zaslouží naši úctu a vděčnost. Jsou to evropští Woodwardové a Bernsteinové. Kromě toho ve všech členských státech stále není zavedena odpovídající ochrana oznamovatelů. V některých případech si oběti útoku špionážního softwaru samy přejí mlčet, protože nechtějí odhalit osoby, které za útokem stojí, ze strachu z odvetných opatření nebo z následků, které by kompromitující materiál mohl mít.

Další kroky

V době, kdy na evropské hodnoty útočí vnější agresor, je o to důležitější posílit náš demokratický právní stát proti útokům zevnitř. Závěry vyšetřování výboru PEGA jsou šokující a měly by znepokojit každého evropského občana. Je zřejmé, že obchodování se špionážním softwarem a jeho používání by mělo být přísně regulováno. Výbor PEGA v tomto smyslu vydá řadu doporučení. Stejně tak by však měly být iniciovány institucionální a politické reformy, které by EU umožnily tato pravidla a normy skutečně prosazovat a dodržovat, a to i v případech, kdy je členské státy samy porušují. EU musí rychle rozvinout své obranné linie proti útokům na demokracii zevnitř.

INFORMACE O PŘIJETÍ V PŘÍSLUŠNÉM VÝBORU

Datum přijetí	8.5.2023
Výsledek konečného hlasování	+: 30 –: 3 0: 4
Členové přítomní při konečném hlasování	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
Náhradníci přítomní při konečném hlasování	Andrzej Halicki, Gabriel Mato, Thijs Reuten, Jordi Solé, Yana Toom
Náhradníci (čl. 209 odst. 7) přítomní při konečném hlasování	Aurélia Beigneux, Theresa Bielowski, Franc Bogovič, Catherine Griset, Andreas Schieder

JMENOVITÉ KONEČNÉ HLASOVÁNÍ V PŘÍSLUŠNÉM VÝBORU

30	+
ELS	Bartosz Arłukowicz, Vladimír Bilčík, Franc Bogovič, Karolin Braunsberger-Reinhold, Andrzej Halicki, Jeroen Lenaers, Gabriel Mato, Lucia Vuolo, Jörgen Warborn, Juan Ignacio Zoido Álvarez
Renew	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
The Left	Cornelia Ernst, Giorgos Georgiou
Verts/ALE	Saskia Bricmont, Hannah Neumann, Diana Riba i Giner, Jordi Solé

3	-
ECR	Beata Kempa, Dominik Tarczyński
NI	Ernő Schaller-Baross

4	0
ECR	Assita Kanko
ID	Aurélia Beigneux, Catherine Griset
NI	Carles Puigdemont i Casamajó

Význam zkratek:
+ : pro
- : proti
0 : zdrželi se