Europaparlamentet
2019-2024

Plenarhandling

A9-0189/2023

22.5.2023

BETÄNKANDE

om utredning av påstådda överträdelser och missförhållanden vid tillämpningen av unionsrätten i fråga om användningen av Pegasus och liknande spionprogram
(2022/2077(INI))

Undersökningskommittén för utredning av användningen av Pegasus och liknande spionprogram

Föredragande: Sophie in ‘t Veld

INNEHÅLL

Sida

UTKAST TILL RESULTAT

från utredningen av påstådda överträdelser och missförhållanden vid tillämpningen av unionsrätten i fråga om användningen av Pegasus och liknande spionprogram (2022/2077(INI))

Europaparlamentet utfärdar detta betänkande

– med beaktande av artikel 226 i fördraget om Europeiska unionens funktionssätt (EUFfördraget),

– med beaktande av sitt beslut av den 10 mars 2022 om tillsättning av en undersökningskommitté för att utreda användningen av Pegasus och liknande spionprogram och fastställande av föremålet för undersökningen samt kommitténs ansvarsområden, sammansättning och mandatperiod,

– med beaktande av artiklarna 54 och 208 i arbetsordningen,

– med beaktande av rapporten från undersökningskommittén för att utreda användningen av Pegasus och liknande spionprogram (A9-0189/2023).

Allmän inledning

1. I juli 2021 offentliggjorde en grupp bestående av undersökande journalister, icke-statliga organisationer och forskare – Pegasusprojektet – en rapport på grundval av en förteckning som de förfogar över med omkring 50 000 telefonnummer som kan ha varit måltavlor för spionprogrammet Pegasus. Sådana spionprogram har använts i stor utsträckning av både auktoritära och demokratiska regeringar världen över, både med och utan rättslig tillsyn, för att förfölja journalister, advokater, domare, aktivister, politiker och statstjänstemän. Människor har också utsatts för spionprogram i Europeiska unionen: vissa av aktörer utanför EU och andra av aktörer inom EU, inbegripet statliga myndigheter. De flesta, om inte alla, medlemsstaters regeringar har köpt spionprogram, i princip för brottsbekämpnings- och säkerhetsändamål. Det finns dock gott om bevis för att spionprogram i flera medlemsstater har missbrukats för rent politiska ändamål, där måltavlorna har varit kritiker och motståndare till de makthavande partierna, eller i samband med korruption. Undersökningsresultat kopplar Pegasus och andra spionprogram till olika kränkningar av de mänskliga rättigheterna från regeringarnas sida, däribland övervakning, utpressning, smutskastningskampanjer, hotelser och trakasserier. Detta ger upphov till betänkligheter avseende olika nivåer i EU:s rättsordning vad gäller dataskydd och integritet, yttrandefrihet, pressfrihet, föreningsfrihet, prövningsmekanismer, rättsmedel och rättvisa rättegångar samt demokratiska processer och institutioner. Även om användning av spionprogram kan klara nödvändighets- och proportionalitetsprövningen i händelse av allvarliga hot mot den nationella säkerheten, är missbruk av spionprogram för politiska ändamål ytterst oroväckande och väcker stor oro över övervakningsmetodernas formella och materiella lagenlighet samt över den skyddsnivå som garanteras i europeisk och nationell lagstiftning. Sådant missbruk av spionprogram undergräver direkt de grundläggande rättigheterna och demokratin, de grundläggande värden som EU bygger på. Efterföljande rapporter från undersökande medier och andra källor har visat att

spionprogram exporteras från EU-länder till tredjeländer med odemokratiska regimer och en hög risk för kränkningar av de mänskliga rättigheterna, vilket uppenbart bryter mot EU:s exportregler. Spionprogramsbranschen är fast etablerad i EU och gynnas av mycket gynnsamma villkor för företagen.

2. Som svar på denna växande skandal beslutade Europaparlamentet den 10 mars 2022 att inrätta en undersökningskommitté i enlighet med artikel 226 i EUF-fördraget för att undersöka påstådda överträdelser, eller administrativa missförhållanden vid genomförandet, av unionsrätten vad gäller användningen av Pegasus och motsvarande spionprogram. En överträdelse innebär olagligt beteende, oavsett om det rör sig om handlingar eller försummelser som strider mot lagen, från EU-institutionernas eller EU-organens eller medlemsstaternas myndigheters sida när de genomför och verkställer EU-lagstiftningen, och administrativa missförhållanden innebär dåliga administrativa åtgärder eller avsaknad av sådana, till exempel om principerna om god förvaltning inte respekteras. Exempel på administrativa missförhållanden är oriktigheter och underlåtenheter, maktmissbruk, oskälighet, felaktigt eller inkompetent handlande och diskriminering, men även onödig fördröjning, vägran att delge information, försummelse och andra brister som innebär en bristfällig tillämpning av unionsrätten.

3. I denna undersökning har PEGA använt en bred definition av vad som utgör spionprogram, nämligen spionprogram som installeras på mobila enheter genom att utnyttja it-sårbarheter. Under undersökningen användes även definitionen av ”cyberövervakningsprodukter” i förordningen om dubbla användningsområden: här beskrivs de som ”produkter med dubbla användningsområden som är särskilt konstruerade för att möjliggöra dold övervakning av fysiska personer genom monitorering extraktion, inhämtning eller analys av data från informations- och telekommunikationssystem”. I september 2022 föreslog kommissionen en definition av spionprogram i sitt förslag till mediefrihetsakt, nämligen ”varje produkt med digitala element som är specifikt utformad för att utnyttja sårbarheter i andra produkter med digitala delar och som möjliggör hemlig övervakning av fysiska eller juridiska personer genom avlyssning, extrahering, insamling eller analys av data från sådana produkter eller från de fysiska eller juridiska personer som använder sådana produkter, i synnerhet genom hemlig inspelning av samtal eller annan användning av mikrofoner i slutanvändarenheter, genom filmning av fysiska personer, maskiner eller deras omgivning, kopiering av meddelanden, fotografering, spårning av surfning, spårning av geolokalisering, insamling av andra sensordata eller spårning av aktiviteter via flera slutanvändarenheter, utan att den berörda fysiska eller juridiska personen specifikt har upplysts om och gett sitt uttryckliga samtycke till detta”.

4. Den 19 april 2022 inledde PEGA sitt arbete med att samla in information genom offentliga utfrågningar, uppdrag, samråd med experter, förfrågningar om uppgifter, bevis och forskning.

5. Under flera offentliga utfrågningar utreddes genom undersökningen hur spionprogram fungerar. Spionprogram är en typ av sabotageprogram som spionerar på en användares aktiviteter utan dennes vetskap eller samtycke. Denna spionverksamhet kan omfatta tangentloggning, aktivitetsövervakning och datainsamling samt andra former av datastöld. Spionprogram sprids vanligtvis som en trojan eller genom att utnyttja

sårbarheter i programvara[1]. Spionprogram kan installeras på distans på mobiltelefoner tillhörande föridentifierade personer, även över gränserna. I vissa fall används telekommunikationsnät för överföring av spionprogram till målenheten. När spionprogrammet har infiltrerat systemet inaktiveras skyddsmekanismer och säkerhetsuppdateringar. Den infekterade enheten överför sedan insamlade data från enheten och gör det möjligt för operatörerna att utföra realtidsövervakning genom att läsa inkommande textmeddelanden, spåra samtal och platser och komma åt och spela in ljud och video via enhetens mikrofon och kamera.

6. I motsats till konventionell telefonavlyssning, som endast möjliggör övervakning av kommunikation i realtid, kan spionprogram ge fullständig, retroaktiv åtkomst till filer och meddelanden som skapats tidigare, lösenord och metadata om tidigare kommunikation. Till följd av detta utgör ett rättsligt beslut om startdatum och varaktighet för en övervakningsinsats ineffektiva skyddsåtgärder när spionprogram ger full retroaktiv tillgång till uppgifter. Det är även tekniskt möjligt att utge sig för att vara någon annan genom att få tillgång till personens digitala behörighetsuppgifter och identitet. Det är extremt svårt för offret att upptäcka om ett intrång med spionprogram har skett. Spionprogram lämnar få eller inga spår på målenheten, och även om det upptäcks är det mycket svårt att bevisa vem som var ansvarig för attacken.

7. PEGA har fått minimala eller inga svar från nationella myndigheter om förvärv och användning av spionprogram i medlemsstaterna, och inte heller om budgetaspekterna. Leverantörer och länder som utfärdar exportlicenser (mestadels Israel) delar ingen information om kunderna. Många medlemsstaters myndigheter har inte tillhandahållit PEGA någon meningsfull information om de rättsliga ramar som styr användningen av spionprogram eller om användningen av spionprogram i medlemsstaterna, utöver vad som redan var allmänt känt, främst på grund av nationella rättsliga krav på sekretess och konfidentialitet.

8. Vissa medlemsstater har använt spionprogram och vägrat att kommentera det genom att åberopa den nationella säkerheten, som enligt artikel 4.2 i fördraget om Europeiska unionen (EU-fördraget) ”också i fortsättningen [ska] vara varje medlemsstats eget ansvar”. Enligt rättspraxis från Europeiska unionens domstol (EU-domstolen) och Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen) måste dock nationella säkerhetshänsyn vara förenliga med de grundläggande rättigheter och demokratiska normer som är starkt inbyggda i EU-rätten. Även om det är medlemsstaternas sak att definiera sina grundläggande nationella säkerhetsintressen och att vidta lämpliga åtgärder för att säkerställa deras inre och yttre säkerhet har EU-domstolen slagit fast att ”den omständigheten att en åtgärd har vidtagits för att skydda nationell säkerhet [kan] nämligen inte [...] leda till att unionsrätten inte är tillämplig och befria medlemsstaterna från skyldigheten att iaktta unionsrätten”[2], och har förtydligat de kriterier som medlemsstaterna måste följa när de definierar frågor som omfattas av den nationella säkerheten. Flera medlemsstater har hävdat att användningen av spionprogram omfattas av nationell säkerhet och att detta innebär att EU-lagstiftningen inte är tillämplig. När medlemsstaterna endast hänvisar till den nationella säkerheten som sådan kan begränsningen av de grundläggande rättigheterna dock inte motiveras som en del av den nationella säkerheten. EU-lagstiftningen måste tillämpas, med alla de

[1] https://www.enisa.europa.eu/topics/incident-response/glossary/malware.
[2] Dom av den 6 oktober 2020, *Privacy International* mot *Secretary of State for Foreign and Commonwealth Affairs and Others*, C-623/17, EU:C:2020:790.

skyddsåtgärder som den föreskriver. Det finns gott om bevis för missbruk av spionprogram av skäl som helt saknar koppling till den nationella säkerheten. Medlemsstaterna bör inte kunna undgå ansvarsskyldighet för sådant allvarligt missbruk av spionprogram, med hänvisning till den nationella säkerheten. På grund av denna tvetydighet var det svårt att få tillräcklig information under utfrågningar och uppdrag och efter informationsförfrågningar. Bristande tydlighet när det gäller hur den nationella säkerheten definieras och de nationella myndigheternas alltför breda tolkning av dess tillämpningsområde utgör en utmaning när det gäller att förstå berättigandet av användningen av spionprogram.

9. Genom att sammanställa information från olika källor kunde PEGA dock återskapa en partiell men tydlig bild och identifiera problem som gav upphov till oro och förtjänade ytterligare undersökningar.

10. Det kan med säkerhet antas att myndigheter i alla medlemsstater använder spionprogram på ett eller annat sätt, vissa lagligt, andra olagligt. Spionprogram kan förvärvas direkt eller via ett ombud, ett mäklarföretag eller en mellanhand. Det kan också finnas arrangemang för särskilda tjänster i stället för faktiska inköp av programvaran. Ytterligare tjänster kan erbjudas, såsom utbildning av personal eller tillhandahållande av servrar. Spionprogram ska inte ses som ett isolerat fenomen, utan som en del av ett brett utbud av produkter och tjänster som erbjuds på en växande och lönsam global marknad. Det är viktigt att inse att inköp och användning av spionprogram är mycket kostsamt och uppgår till miljontals euro. Men i många medlemsstater ingår dessa utgifter inte i den ordinarie budgeten, och kan därmed undgå granskning.

11. Utifrån information från NSO Group är det känt att Pegasus såldes i minst 14 EU-länder tills avtalen med två länder avslutades. Det är inte känt vilka länder det rör sig om, men det finns ett allmänt antagande om att är Polen och Ungern. Men så länge som NSO Group eller den israeliska regeringen inte gör något officiellt uttalande om uppsägning av ett avtal kan det inte kontrolleras.

12. Ytterligare information är deltagarlistan i 2013 års upplaga av mässan ISS World (Intelligence Support Systems), även kallad ”telefonavlyssningsbalen”. Med undantag för Portugal och Luxemburg företräddes alla nuvarande EU-medlemsstater av ett stort antal organisationer, inbegripet lokala polisstyrkor[3]. Under de senaste åren har NSO Group blivit huvudsponsor för evenemanget, men i sponsorlistan nämns även Intellexa, Candiru, RCS och många andra[4].

13. Medlemsstaterna är inte bara kunder hos kommersiella spionprogramsleverantörer, de har också olika andra roller i spionprogramshandeln. En del är värdar för spionprogramsleverantörer, en del föredras för finans- och banktjänster, andra erbjuder medborgarskap och bosättning till branschföreträdare.

14. I de allra flesta medlemsstater regleras underrättelsetjänsterna av en rättslig ram – ofta med bestämmelser om hur dessa tjänster ska organiseras och fungera samt vilka uppdrag och befogenheter de ska ha, däribland deras verktyg och villkoren för att använda dem, samt tillsynsmekanismer som omfattar verkställande kontroll,

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

parlamentarisk tillsyn, expertorgan och rättslig prövning. Ändå har farhågor framförts angående vissa länders tillåtande underrättelseramar, ineffektiva kontroller, släpphänta tillsynsrutiner och politiska inblandning.

15. Spionprogram används uppenbarligen också av brottsbekämpande myndigheter, inte bara av underrättelsetjänster. Det finns allvarliga betänkligheter kring tillåtligheten i domstol av sådant material som bevis inom ramen för EU:s polisiära och rättsliga samarbete, även inom Europol och Eurojust, om sådan information skulle härröra från utredningsmetoder som tillämpas utan ordentlig rättslig kontroll. Beroende på nationell lagstiftning är det legitimt att använda spionprogram i utredningar under rättslig tillsyn.

16. Missbruk av spionprogram är ett hot mot demokratin och de grundläggande rättigheterna. Sedan Pegasusprojektets avslöjanden har Förenta staterna vidtagit flera åtgärder för att undersöka och reglera detta. Hittills har mycket få åtgärder vidtagits inom EU. Tydliga regler måste fastställas för användningen av och handeln med spionprogram, helst tillsammans med andra länder, såsom Förenta staterna.

I. Användningen av spionprogram i EU

I.A Polen

17. Ministeriernas företrädare vägrade att sammanträda med kommitténs delegation. Som svar på det frågeformulär som skickades ut av PEGA den 15 juli 2022 besvarade de polska myndigheterna inte alla frågorna och insisterade på att de befintliga bestämmelserna var tillräckliga och att de verkade strikt inom lagens gränser[5]. Inrikesministern Mariusz Kaminski vägrade också att godta en inbjudan från PEGA att utbyta åsikter[6].

18. PEGA:s undersökningsuppdrag i Polen i september 2022 var av yttersta vikt för kommittén, och gjorde det möjligt för den att samla in information och fakta om användningen av spionprogrammet Pegasus. Mötena i Warszawa kastade nytt ljus över den olagliga användningen av inkräktande övervakningsprogramvara mot demokratiska aktörer i Polen. Ledamöterna lärde sig hur systemet med rättsliga och institutionella kontroller och motvikter har avvecklats för att göra det möjligt att rikta in sig på personer som anses vara politiska motståndare med militära cybervapen. Till följd av detta har viktiga demokratiska normer och medborgerliga rättigheter som är inskrivna i EU:s och Polens lagar kränkts grovt. Detta är ännu en dimension av rättsstatskrisen i Polen.

INKÖP AV PEGASUS

19. I november 2016 var den tidigare premiärministern och nuvarande parlamentsledamoten Beata Szydło, och den tidigare utrikesministern Witold Waszczykowski, på middag hemma hos den israeliske premiärministern Benjamin Netanyahu[7]. I juli månad följande år träffade Beata Szydło och Benjamin Netanyahu regeringscheferna i länderna i Visegradgruppen. De påstås ha diskuterat ”stärkt samarbete kring innovation och

[5] Svar från Polens ständiga representant vid EU, Andrzej Sadós, till PEGA-kommittén, 7 september 2022.
[6] Svar från inrikesministern, Mariusz Kaminski, genom en skrivelse till PEGA-kommittén, 12 juli 2022.
[7] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29 januari 2022.

högteknologi” och ”frågor som rör medborgarnas säkerhet i den allmänna betydelsen”[8]. En kort tid efter att detta möte ägde rum år 2017 införskaffade den polska regeringen Pegasus efter ett möte mellan premiärminister Mateusz Morawiecki, Ungerns premiärminister Viktor Orbán samt Benjamin Netanyahu[9].

20. Inledningsvis förnekade den polska regeringen och PiS-ledaren Jarosław Kaczyński inköpet av Pegasus[10]. I början av januari 2022 bekräftade de dock den polska regeringens köp av spionprogram[11] [12] [13]. Under samma månad avslöjades det att centrala bevis för inköpet av Pegasus hade samlats in av högsta revisionsmyndigheten under 2018 vid en revision av rättsfonden som drivs av justitieministeriet och inrättats för att stödja brottsoffer. Den 18 januari 2022 vittnade den tidigare chefen för Polens högsta revisionsmyndighet (NIK) och därefter den oberoende senatorn Krzysztof Kwiatkowski om köpet av Pegasus inför senatens särskilda utskott för fall av övervakning med användning av Pegasussystemet[14]. Efter att ha befriats från tystnadsplikten med anledning av sin befattning överlämnade han två fakturor till utskottet som bekräftade köpet av spionprogrammet till den centrala byrån för korruptionsbekämpning (CBA) med 25 miljoner zloty från rättsfonden som förvaltas av justitieministeriet[15]. Krzysztof Kwiatkowski vittnade om att NIK hade upptäckt konton från Polens centralbank som styrkte överföringen[16].

21. Fakturorna utfärdades av Matic Sp. z o.o., som fungerade som en mellanhand genom vilken CBA genomförde detta inköp[17]. Matic Sp. z o.o. är ett it- och säkerhetsföretag med säte i Warszawa, som ägs och drivs av personer som var verksamma inom underrättelse- och säkerhetstjänsten under kommunistperioden[18].

22. Matic blev ett aktiebolag omedelbart efter köpet av Pegasus i november 2017 och bedriver verksamhet med ett tillstånd från inrikesministeriet för handel med teknik med säkerhetstjänsterna och polisen samt vapenhandel enligt Wyborcza[19]. Företaget har också ett särskilt licensieringscertifikat från byrån för inre säkerhet, varav det senaste utfärdades 2019, som gör det möjligt för företaget att hemlighålla viss konfidentiell

[8] Gazeta, https://wiadomosci.gazeta.pl/wiadomosci/7,114884,28052298,jak-polska-kupila-pegasusa-nyt-kolacja-beaty-szydlo-z-premierem.html, 29 januari 2022.
[9] Financieele Dagblad, ”De wereld deze week: het beste uit de internationale pers”, 7 januari 2022.
[10] https://www.politico.eu/article/poland-government-scrambles-minimize-hacking-backlash/.
[11] Financieele Dagblad, ”Liberalen Europarlement eisen onderzoek naar spionagesoftware”, 12 januari 2022.
[12] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/.
[13] Januari 2022, Financial Times, https://www.ft.com/content/d8231ec7-5c44-42fc-b32e-30b851f1c25e, 8 februari 2022.
[14] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 januari 2022.
[15] ONET, https://wiadomosci.onet.pl/kraj/wiceminister-michal-wos-nie-wiem-co-to-jest-pegasus/e9fbrvh, 3 januari 2022, Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 januari 2022.
[16] The Wire, https://thewire.in/world/poland-audit-office-invoice-pegasus-purchase-reopen-investigation, 4 januari 2022, Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 januari 2022.
[17] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 januari 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 januari 2022.

information fram till slutet av årtiondet[20]. Företrädare för Matic vägrade att träffa och dela information med undersökningskommittén.

23. Enligt polsk lag kan verksamheten vid CBA endast finansieras genom statsbudgeten. Inköpet av Pegasus finansierades dock genom rättsfonden, som inte ingår i statsbudgeten utan är en offentlig fond som öronmärkts för brottsoffer[21]. Köpet bröt därför mot polsk lag. Enligt de ursprungliga bestämmelserna för denna fond får den dessutom inte användas för att finansiera de särskilda tjänsternas verksamhet[22]. I september 2017 lades dock ett förslag om att ändra rättsfondens finansieringsplan fram för sejmens (det polska parlamentets underhus) utskott för offentliga finanser av Michał Woś, biträdande justitieminister[23], och en nära medarbetare till justitieministern Zbigniew Ziobro[24]. Parlamentsledamöterna godkände denna ändring. När det senare avslöjades att rättsfonden användes för att finansiera Pegasus för CBA sade parlamentsledamöterna att detta inte hade nämnts med ett enda ord under utskottssammanträdet[25]. Det verkar därför som om de vilseleddes av regeringen. Även om NIK har lämnat in en officiell anmälan till åklagarmyndigheten om en överträdelse av lagen avseende användning av resurser från rättsfonden för att köpa Pegasus 2017, finns det inga förväntningar på att åklagarmyndigheten kommer att vidta åtgärder i ett sådant fall, med tanke på den nuvarande institutionella och politiska miljön.

24. Michał Woś ansökte även hos finansministeriet om medgivande till att omfördela de 25 miljoner zloty som spenderades på Pegasus från rättsfonden till ”annan verksamhet” som syftade till att ”bekämpa effekterna av brottslighet”. Den biträdande ministern godkände därefter överföringarna från rättsfonden till CBA. Efter att ha blivit tillfrågad om saken i januari 2022 nekade emellertid Michał Woś först till att ha någon kännedom om själva Pegasus-verktyget, än mindre om statens köp av detsamma, men han har sedan dess bekräftat köpet. Det är oklart hur driftskostnaderna för användningen av Pegasus har finansierats.

25. Det har rapporterats att NSO Group hittills har sålt Pegasus till 14 länder i Europa. NSO Group har dock även medgett att företaget har återkallat licenserna för två av dessa länder[26]. Under sitt vittnesmål i PEGA-kommittén uppgav NSO Group att den endast undersöker frågor om användningen av Pegasus när den får information från

[20] Gazeta Wyborcza, https://wyborcza.pl/7,75398,28007064,kupili-pegasusa-dla-pis-i-wzieli-miliony-rodzinna-firma-ludzi.html, 17 januari 2022.
[21] The Guardian, ”More Polish opposition figures found to have been targeted by Pegasus spyware”, 17 februari 2022, The Guardian, ”Polish senators draft law to regulate spyware after anti-Pegasus testimony”, 24 januari 2022, 2022 års rapport från kommissionen om rättsstatsprincipen, lanskapitlet om rättsstatssituationen i Polen, 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 januari 2022.
[22] Business Insider, https://businessinsider.com.pl/wiadomosci/kwiatkowski-ujawnil-faktury-za-zakup-pegasusa/qyx3zs1, 18 januari 2022.
[23] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 januari 2022, Gazeta Wyborcza, https://wyborcza.pl/7,75398,27966080,jak-ziobro-kupowal-pegasusa-dla-cba.html, 3 januari 2022.
[24] Gazeta Wyborcza, https://wyborcza.pl/7,75398,27970483,z-dystansem-patrze-na-te-panike-wos-w-polskim-radiu-o-pegasusie.html, 4 januari 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 januari 2022.
[26] Diskussion med NSO Group, undersökningskommitténs uppdrag att utreda användningen av Pegasus och liknande spionprogram i Israel, juli 2022.

visselblåsare eller via medierna. När NSO Group får in klagomål undersöker och granskar den dem och kan därefter stänga ner Pegasus för aktörer som har missbrukat programmet[27]. På grundval av det stora antalet medierapporter om användningen av Pegasus i Polen är det högst troligt att Polen är ett av dessa två länder mot bakgrund av deras överträdelse av NSO Groups användarvillkor, även om detta inte har bekräftats.

26. Sedan de första tecknen på att de polska myndigheterna använder Pegasus har den polska ombudsmannen försökt fråga myndigheterna om så varit fallet och har argumenterat för att förbättra skyddsåtgärderna för de demokratiska och mänskliga rättigheterna för att förhindra missbruk av övervakning, bland annat genom årliga rapporter till det polska parlamentet. I januari 2023 skickade den polska ombudsmannen ett brev till inrikesministern där det uppgavs att det saknas rättslig grund för användning av Pegasus eller liknande spionprogram i Polen, med åberopande av rättspraxis från den polska författningsdomstolen och rättspraxis från Europadomstolen[28].

RÄTTSLIG RAM

27. Författningsdomstolen genomförde 2014 en översyn av polislagen från 1990 och andra befintliga lagar om övervakning av medborgare som ansågs vara oförenliga med Polens konstitution[29]. Domstolen avslutade med att avkunna en dom med särskilda rekommendationer och en tidsfrist på 18 månader inom vilken lagstiftningsändringar skulle genomföras[30]. Efter valet 2015 införde den nya regeringen lagändringar. Lagen av den 15 januari 2016 om ändring av 1990 års polislag och vissa andra lagar (2016 års polislag) åtgärdade dock inte någon av bristerna i lagen, vilket författningsdomstolen krävde[31]. I stället har 2016 års polislag försvagat de befintliga bestämmelser som i sig varken skyddade medborgarnas rättigheter i tillräcklig utsträckning eller skapade ordentlig tillsyn.

28. I sitt yttrande om polislagen 2016 uppger Venedigkommissionen att ”... skyddsåtgärderna och de väsentliga villkor som föreskrivs i polislagen för genomförande av hemlig övervakning fortfarande inte är tillräckliga för att förhindra att det används i alltför hög grad och utgör ett omotiverat intrång i enskilda personers integritet”[32]. Bristen på specificitet när det gäller tillsyn, garantier mot övergrepp och de kategorier av personer och brott som de skulle kunna inrikta sig på utgör också överträdelser av domarna från Europadomstolen[33]. I domen *Roman Zakharov* mot *Ryssland* från 2015 undersökte domstolen särskilt behovet av tydlighet när det gäller användning av spionprogram. Den slog fast att när det gäller hemlig övervakning av

[27] Vittnesmål av Chaim Gelfand, chefsjurist och huvudansvarig för regelefterlevnad, NSO Group, vid PEGA, 21 juni 2022.
[28] PEGA-kommitténs sammanträde, 19 januari 2023.
[29] Yttrande nr 839/2016 om lagen av den 15 januari 2016 om ändring av polislagen och vissa andra lagar, som antogs av Venedigkommissionen vid dess 107:e plenarsammanträde den 10–11 juni 2016.
[30] https://trybunal.gov.pl/en/hearings/judgments/art/8821-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani.
[31] Lag av den 15 januari 2016 om ändring av polislagen och vissa andra lagar, artikel 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[32] Yttrande nr 839/2016 om lagen av den 15 januari 2016 om ändring av polislagen och vissa andra lagar, som antogs av Venedigkommissionen vid dess 107:e plenarsammanträde den 10–11 juni 2016.
[33] Se, bland annat, *Roman Zakharov* mot *Ryssland* [GC], nr 47143/06, Europadomstolen, dom av den 4 december 2015, *Klass m.fl.* mot *Tyskland*, nr 5029/71, Europadomstolen, dom av den 6 september 1978, punkt 40, *Prado Bugallo* mot *Spanien*, nr 58496/00, Europadomstolen, dom av den 18 februari 2003, punkt 30, *Liberty m.fl.* mot *Förenade kungariket*, nr 58243/00, dom av den 1 juli 2008, punkt 62.

medborgare behövs stränga kriterier, korrekt rättslig tillsyn, omedelbar förstörelse av irrelevanta uppgifter, domstolsgranskning av brådskande förfaranden och ett krav på underrättelse av brottsoffer[34]. Domstolen uppgav dessutom uttryckligen att det skulle ”strida mot rättsstatsprincipen” om beslut när det gäller hemlig övervakning helt koncentrerades till rättsväsendets verkställande organ[35]. Polislagen från 2016, som fortfarande gäller i Polen, avspeglar inte på något sätt detta avgörande av domstolen. Dess bestämmelser står i själva verket i direkt strid med stora delar av domen.

29. Europadomstolen för de mänskliga rättigheterna har också varit otvetydig i sin inställning till nödvändighetstestet, vilket innebär att övervakningen måste vara tillräckligt viktig för att göra ett sådant integritetsintrång nödvändigt. I sin dom i målet *Klass m.fl.* mot *Tyskland* år 1978 beskrevs denna punkt tydligt, och domstolen slog fast att oavsett övervakningssystem måste domstolen känna sig trygg med att det finns ”tillräckliga och ändamålsenliga garantier mot övergrepp”[36]. Den noggrant iscensatta förstörelsen av kontroll- och maktdelningsmekanismerna i Polen visar det styrande partiets uppenbara trots mot domstolarna. Trots allt detta insisterar PiS på att de befintliga bestämmelserna är tillräckliga och att de verkar strikt inom lagens ramar[37]. Samtidigt har regeringen avslagit alla förfrågningar om dialog och förtydliganden om hur övervakning används i Polen.

2016 ÅRS LAG MOT TERRORISM

30. Utöver 2016 års polislag antog sejmen 2016 även en lag som reglerar övervakningen av utländska medborgare, som den kallar ”lagen mot terrorism”. Lagen föreskriver att icke-polska medborgare kan övervakas utan domstolens samtycke under en period på tre månader om deras identitet är ”tveksam”, bl.a. genom avlyssning av telefoner, insamling av fingeravtryck, biometriska foton och DNA samt genom en skyldighet att registrera förbetalda telefonkort[38]. Enligt artikel 9.8 i lagen har riksåklagaren befogenhet att besluta om förstöring av icke-relevant material. Med tanke på att den nuvarande riksåklagaren Zbigniew Ziobro också är justitieminister finns det allvarliga farhågor om huruvida han kan fatta oberoende och opartiska beslut utan att påverkas av de politiska intressena hos den regering han företräder[39] [40].

STRAFFPROCESSORDNINGEN

31. I juli 2015 infördes lagen om ändring av straffprocessordningen i Polen för att säkerställa att bevisning som har erhållits på olagligt sätt inte kan användas i straffrättsliga förfaranden. Efter att PiS kom till makten omarbetades dock lagen i mars 2016 för att inkludera artikel 168a[41]. Detta tillägg säkerställer att bevis som samlats in i

[34] *Roman Zakharov* mot *Ryssland* [GC], nr 47143/06, Europadomstolen, dom av den 4 december 2015.
[35] *Roman Zakharov* mot *Ryssland* [GC], nr 47143/06, Europadomstolen, dom av den 4 december 2015, punkterna 229 och 230. Se även Venedigkommissionens yttrande nr 839/2016, juni 2016, https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2016)012-e, s. 11.
[36] *Klass m.fl.* mot *Tyskland*, 6 september 1978, punkt 50, serie A nr 28. 40.
[37] Skrivelse från Mariusz Kaminski, Polens inrikes- och förvaltningsminister, till PEGA-kommittén, 8 september 2022.
[38] Lag av den 10 juni 2016 om åtgärder mot terrorism, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000904/T/D20160904L.pdf.
[39] Lag av den 10 juni 2016 om åtgärder mot terrorism, 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 juni 2016.
[41] Lag av den 11 mars 2016 om ändring av straffprocesslagen och vissa andra lagar,

strid med lagen, eller ”frukt från det giftiga trädet”, t.ex. information som inhämtats med hjälp av Pegasus, får användas i rättsliga förfaranden[42]. Det måste dock tilläggas att högsta domstolen i Polen i sin dom slog fast att denna artikel inte kan tillämpas i strid med bestämmelserna i Europakonventionen om de mänskliga rättigheterna och Polens konstitution, som i vissa fall begränsar dess tillämpning i praktiken[43]. Det har också meddelats domar där man har funnit att artikel 168a är delvis okonstitutionell[44]. Att denna bestämmelse finns i rättssystemet ger dock upphov till osäkerhet när det gäller respekt för de grundläggande rättigheterna.

LAGEN OM TELEKOMMUNIKATION

32. Efter 2016 års ändring av 2004 års telekommunikationslag innehåller lagen om telekommunikation i Polen bestämmelser om att polisen ska få obegränsad tillgång till metadata och i vissa fall utan medverkan av telekomföretagen[45]. Denna tillgång kan erhållas under en mycket bred motivering som rör ”förebyggande eller upptäckt av brott”. Åklagaren beslutar sedan hur man ska gå vidare med mottagandet av dessa uppgifter. Det kan dock inte betraktas som en skyddsåtgärd, med tanke på att åklagarmyndigheten efter sammanslagningen av justitieministerns och riksåklagarens roll inte kan anses vara oberoende av den verkställande makten[46].

33. Ovan nämnda ändring av straffprocessordningen för att möjliggöra ”frukt från det giftiga trädet” har haft betydande påverkan på betydelsen av telekomoperatörerna och de data som dessa företag lagrar. I Polen måste de största telekomleverantörerna i själva verket ha ett särskilt team som svarar på flera begäranden om avlyssning från myndigheterna. De har dock vanligen inte mycket insikt i innehållet i avlyssning eller operativa detaljer i enskilda fall[47].

LAGEN OM GENOMFÖRANDE AV DATASKYDDSDIREKTIVET FÖR POLIS- OCH ÅKLAGARMYNDIGHETERNA

34. Polen har inte genomfört dataskyddsdirektivet (EU) 2016/680[48] för polis- och åklagarmyndigheterna, som kräver specifika standarder för insamling och behandling av personuppgifter av polisen och andra myndigheter. Dataskyddsdirektivet för polis- och åklagarmyndigheterna införlivades genom 2018 års lag om skydd av personuppgifter

---

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] T.ex. dom från högsta domstolen i Polen av den 26 juni 2019, IV KK 328/18.

[44] T.ex. dom från högsta domstolen i Polen av den 26 juni 2019, IV KK 328/18.

[45] Lag om telekommunikation av den 16 juli 2004 https://www.dataguidance.com/legal-research/telecommunications-act-16-july-2004.

[46] Lag av den 15 januari 2016 om ändring av polislagen och vissa andra lagar, artikel 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_SV.pdf, The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, 17 februari 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] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

som behandlas i samband med förebyggande och bekämpande av brott. Lagen har väsentligt utvidgat omfattningen av de skäl som föreskrivs i direktivet för att vägra att underrätta personer om behandlingen av deras personuppgifter och ignorerat den mekanism som föreskrivs i artikel 17 i direktivet, som ger personerna en möjlighet att utöva sina befogenheter genom en relevant tillsynsmyndighet – i Polen ordföranden för myndigheten för skydd av personuppgifter. I lagen föreskrivs vidare betydande försiktighet för den nationella säkerheten, inbegripet genomförande av lagstadgade uppgifter genom olika organ inom säkerhetsstyrkorna[49].

35. Polen har heller fortfarande inte genomfört EU:s visselblåsardirektiv. Landet höll inte tidsfristen i december 2021 efter det att det första utkastet till lagstiftning förkastades. Ett andra utkast offentliggjordes i april 2022, men inga ytterligare framsteg har gjorts och den föreslagna lagstiftningen innehåller betydligt svagare bestämmelser. I januari 2022 inledde kommissionen ett överträdelseförfarande mot Polen för underlåtenhet att fullt ut genomföra direktivet, och i februari 2023 beslutade kommissionen att hänskjuta Polen till EU-domstolen[50].

36. Sejmen, särskilt ledamöter i PiS-partiet, utarbetar för närvarande en lag om elektroniska kommunikationer. Denna lag skulle göra det enklare för myndigheterna att komma åt polska medborgares e-postmeddelanden och meddelanden i sociala medier. Leverantörer skulle behöva spara e-postmeddelanden och meddelanden på sina servrar så att relevanta domstolar skulle kunna besluta om åtkomst till data, ip-adresser och innehållet i meddelandena[51].

FÖRHANDSGRANSKNING

37. Även om övervakning i Polen kräver rättsligt tillstånd fungerar det befintliga tillståndsförfarandet inte som ett skydd mot övergrepp, utan ger snarare övervakning som används för politiska syften en aura av lagenlighet. Det har inte gjorts uttryckligen klart huruvida något av de hittillsvarande offren för Pegasus har spionerats på med rättsligt tillstånd. Ansökan om rättsligt tillstånd för en övervakningsinsats lämnas in av specialtjänsten[52]. För bedömningen av ansökan har domarna endast den information som sökanden har lämnat (dvs. specialtjänsten) till sitt förfogande, och det är åklagaren som avgör vilket material som det är relevant att lämna in[53]. Informationen består ofta bara av en sammanfattning, och exkluderar ibland även de mest grundläggande uppgifterna om personer som är måltavlor (namn, yrke, det brott som de misstänks för) och en beskrivning av de övervakningsmetoder som ska användas.

38. Men om en domare avslår en ansökan måste de ge en välgrundad motivering för ett

[49] Adam Bodnar m.fl, ”How to saddle Pegasus: Observance of civil rights in the activities of security services: objectives of the reform”, september 2019 https://bip.brpo.gov.pl/sites/default/files/HOW%20TO%20SADDLE%20PEGASUS%20(OSIOD%C5%81A%C4%86%20PEGAZA).pdf.
[50] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_703.
[51] Euractiv, ”Polish government working on controversial surveillance bill”, https://www.euractiv.com/section/politics/news/polish-government-working-on-controversial-surveillance-bill/.
[52] Lag av den 15 januari 2016 om ändring av polislagen och vissa andra lagar, artikel 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.
[53] Lag av den 15 januari 2016 om ändring av polislagen och vissa andra lagar, artikel 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.

sådant beslut och det kan överklagas[54]. Det är i brådskande fall avgörande att åklagaren initialt kan godkänna användningen av avlyssningsmetoder utan godkännande från en domare, förutsatt att domstolen därefter beviljar tillstånd inom fem dagar[55]. Detta är ett betydande och medvetet kryphål i den polska rättsliga ramen.

39. Ansökningar om tillstånd för övervakning av de viktigaste myndigheterna, dvs. CBA, polisen (Policja KGP) och underrättelsetjänsterna (Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Krajowa Administracja Skarbowa, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, Służba Ochrony Państwa, Biuro Nadzoru Wewnętrznego MSWiA och det nyligen tillkomna Inspektorat Służby Więziennej) överlämnas nästan uteslutande till distriktsdomstolen i Warszawa (Sad Okręgowy), där de flesta av dessa byråer finns.

40. Flera dussin övervakningsansökningar lämnas in varje dag, vilket försvårar domstolens kapacitet att genomföra en djupgående granskning av varje begäran[56]. Systemet som slumpmässigt fördelar mål till domstolarnas domare är tekniskt sett fortfarande i drift i Polen, men det fungerar endast under kontorstid. Men med tanke på att domstolen som godkänner övervakning gör det dygnet runt, finns det stora möjligheter för systemet att kringgås. Genom att lämna in en ansökan på helgen eller utanför ordinarie öppettider kommer ärendet automatiskt att tilldelas den jourhavande domaren[57]. Informationen om vem som har jour vid en viss tidpunkt är känd för underrättelsetjänsten, som då helt enkelt kan välja en ”vänlig domare” som de kan skicka sina övervakningsansökningar till[58]. Dessutom kan slumpmässig tilldelning också förbigås av it-personal som har tillgång till systemet och kan tilldela övervakningstillstånd till ”vänliga domare”[59]. Allt detta undergräver på ett allvarligt sätt domstolens förmåga att utöva effektiv rättslig tillsyn.

EFTERHANDSGRANSKNING

41. I Polen finns i princip ingen parlamentarisk tillsyn. Före 2016 leddes den parlamentariska tillsynskommittén för specialtjänsten (KSS) av ett roterande ordförandeskap mellan de styrande partierna och oppositionspartierna. PiS har dock ändrat denna parlamentariska regel och installerat PiS-medlemmarna Waldemar Andzel som permanent ordförande och Jarosław Krajewski som vice ordförande för kommittén[60]. Regeringspartierna har absolut majoritet i kommittén[61]. Detta gör kommitténs tillsynsfunktion meningslös. Dessutom avvisade regeringsmajoriteten i sejmen kravet på en parlamentarisk utredning av påståendena om olaglig användning av

[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.
[56] Vittnesmål av Ewa Wrzosek, landsspecifik utfrågning om Polen, möte i undersökningskommittén för utredning av användningen av Pegasus och liknande spionprograms möte den 15 september 2022.
[57] Vittnesmål av Ewa Wrzosek, landsspecifik utfrågning om Polen, möte i undersökningskommittén för utredning av användningen av Pegasus och liknande spionprograms möte den 15 september 2022.
[58] Vittnesmål av Ewa Wrzosek, landsspecifik utfrågning om Polen, möte i undersökningskommittén för utredning av användningen av Pegasus och liknande spionprograms möte den 15 september 2022.
[59] Vittnesmål av Ewa Wrzosek, landsspecifik utfrågning om Polen, möte i undersökningskommittén för utredning av användningen av Pegasus och liknande spionprograms möte den 15 september 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.

spionprogram[62] [63] [64] [65] [66]. Å andra sidan tillsatte senaten, där regeringspartierna inte har någon majoritet, en undersökningskommitté i början av 2022. Senatens kommitté saknar dock de undersökningsbefogenheter som sejmen[67] har, vars undersökningskommitté kan kalla vittnen och höra vittnesmål. Kommittén har vid varje tillfälle stött på motstånd från det styrande partiet i sejmen[68], regeringstjänstemän och säkerhetsmyndigheter, som alla har vägrat att samarbeta eller genomföra en egen utredning[69].

42. Granskning och korrigerande åtgärder som erbjuds av andra oberoende organ har också kraftigt försvagats. Högsta revisionsmyndigheten har effektiva tillsynsbefogenheter, men dess medlemmar och personal utsätts för ständiga hinder, trakasserier och hot, vilket allvarligt påverkar dess operativa kapacitet[70]. Sejmen har också hittills misslyckats att utse tio av nitton medlemmar i NIK[71]. Den erforderliga granskningen av rådsmedlemmar som utförs av specialtjänsten, under ledning av minister Kaminski, går mycket långsamt[72].

43. När ett brott mot lagen upptäcks av NIK har de befogenhet att lämna in en anmälan till åklagarmyndigheten[73]. Det är dock upp till åklagarmyndigheten att inleda ett ärende på grundval av den anmälan. I situationer där åklagaren inte vidtar åtgärder är det lite som kan göras av NIK. När en anmäld överträdelse gäller verksamheten vid själva åklagarmyndigheten skapas en ond cirkel av ansvarsfrihet. Dessutom ska alla ärenden som NIK anmäler till åklagarmyndigheten anmälas till riksåklagaren, som också är justitieminister, som leder just det departement som köpte spionprogrammet från början.

---

[62] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17 januari 2022.
[63] 2022 års rapport från Europeiska kommissionen om rättsstatsprincipen, landskapitlet om rättstatssituationen i Polen, 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 december 2021.
[65] The Guardian, 'Polish senators draft law to regulate spyware after anti-Pegasus testimony', 24 januari 2022.
[66] Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 januari 2022.
[67] 2022 års rapport från Europeiska kommissionen om rättsstatsprincipen, landskapitlet om rättstatssituationen i Polen, https://ec.europa.eu/info/sites/default/files/48_1_194008_coun_chap_poland_en.pdf, s. 27, fotnot 220.
[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 januari 2022.
[69] AP, https://apnews.com/article/technology-canada-europe-toronto-hacking-b5f7e36e8b22611aa6bfc27c17024422, 17 januari 2022, 2022 års rapport från Europeiska kommissionen om rättsstatsprincipen, lanskapitlet om rättsstatssituationen i Polen, 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 december 2021, The Guardian, "Polish senators draft law to regulate spyware after anti-Pegasus testimony", 24 januari 2022, Politico, https://www.politico.eu/article/polish-leader-jaroslaw-kaczynski-under-fire-over-pegasus-hack-scandal/, 18 januari 2022.
[70] Reuters, https://www.reuters.com/article/poland-pegasus-idUSL8N2UF596, 4 februari 2022, diskussion med den högsta revisionsmyndigheten, undersökningskommitténs uppdrag att undersöka användningen av Pegasus och liknande spionprogram mot Polen, september 2022.
[71] https://www.nik.gov.pl/en/about-us/the-council-of-nik/; diskussion med den högsta revisionsmyndigheten, undersökningskommitténs uppdrag att undersöka användningen av Pegasus och liknande spionprogram mot Polen, september 2022.
[72] Diskussion med den högsta revisionsmyndigheten, undersökningskommitténs uppdrag att undersöka användningen av Pegasus och liknande spionprogram mot Polen, september 2022.
[73] Lag av den 23 december 1994 om den högsta revisionsmyndigheten, https://www.nik.gov.pl/en/about-us/legal-regulations/act-on-the-supreme-audit-office.html, artikel 63.

Riksåklagaren har befogenhet att avbryta utredningar eller återuppta utredningar som åklagarmyndigheten avslutat. Han kan också inleda disciplinära förfaranden mot åklagare som han misstänker har fattat felaktiga beslut.

44. Den nuvarande ombudsmannen Marcin Wiącek utsågs 2021 när sejmen och senaten enades om en partipolitisk kompromisskandidat efter en lång dragkamp[74]. När det gäller fallet med senator Brejza, hävdade Wiącek att ombudsmannen inte bör engagera sig i de tidiga stadierna av ett ärende. Trots detta har både de tidigare och nuvarande ombudsmännen övervakat situationen och utövat ett visst mått av press på behovet av att skapa ett oberoende tillsynsorgan för att ge demokratisk kontroll över underrättelsetjänstens verksamhet[75].

RAPPORTERING

45. Enligt 2016 års polislag är polisen endast skyldig att lämna in rapporter två gånger per år till de behöriga domstolarna om antalet insamlingar av telekommunikations-, post- eller internetuppgifter tillsammans med deras juridiska resonemang (som rör förebyggande åtgärder eller upptäckande av brott, skydd av människors liv eller hälsa eller stöd till sök- och räddningsinsatser)[76]. Dessa rapporter kan endast göras i efterhand och offentliggörs inte. Om det uppstår ett problem med inlagan kommer domstolen att lägga fram sina slutsatser som svar inom 30 dagar, men kan inte besluta att några uppgifter ska förstöras, även om den finner att de är oförenliga med lagen. Ytterst viktigt att poängtera är att dessa tillsynsåtgärder endast är frivilliga, inte obligatoriska.

RÄTTSMEDEL

46. Trots de omfattande bevisen för att grova brott har begåtts har den polska åklagaren hittills agerat mycket förhalande. Det verkar som om endast målet med åklagaren Ewa Wrzosek och Krzysztof Brejza har tagits upp av domstolarna. Ewa Wrzosek ingav ursprungligen sitt ärende till åklagarmyndigheten. Efter att den officiellt vägrade att ta upp ärendet kunde hon dock överklaga till domstolarna. I slutet av september 2022 beordrade distriktsdomstolen i Warszawa (Mokotów) åklagaren att inleda en utredning. Hittills har dock åklagaren inte genomfört några meningsfulla förfaranden som är nödvändiga för att ärendena ska kunna fortskrida, såsom att inhämta vittnesmål från måltavlan.

47. Det är viktigt att notera att Wrzosek endast kunde inleda detta överklagande i domstolarna efter att ha fått ett officiellt avslag från åklagarens kontor. I många andra fall drar åklagaren ut på utredningen för att undvika att någonsin behöva utfärda ett officiellt svar, eftersom han är medveten om att om han gör det kommer han att bli utsatt för överklagandeförfarandet i domstolarna.

48. Medborgare som har blivit spionerade på kan givetvis föra ett civilmål inför domstol,

---

[74] Euractiv, https://www.euractiv.com/section/politics/short_news/poland-elects-new-ombudsman-in-rule-of-law-standoff/, 22 juli 2021.

[75] Europaparlamentet. Generaldirektoratet för parlamentarisk utredning och analys, ”Europe’s PegasusGate: Countering spyware abuse”, studie, 6 juli 2022, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, s. 22.

[76] Lag av den 15 januari 2016 om ändring av polislagen och vissa andra lagar, artikel 20c, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20160000147/T/D20160147L.pdf.

men bevisbördan för att de varit föremål för övervakning ligger på dem och det är praktiskt taget omöjligt att bevisa den illegala användningen av spionprogram utan myndigheternas samarbete. Bristen på genomförande av skyldigheten att lämna ut uppgifter i Polen, som beskrivs i *Klass*-domen, innebär att många personer kanske aldrig vet att de har blivit utsatta.

49. För närvarande står målen *Pietrzak* mot *Polen* och *Bychawska-Siniarska m.fl.* mot *Polen* inför Europadomstolen, som ifrågasätter bristen på insyn, tillsyn, underrättelse och korrigerande åtgärder när det gäller övervakning i Polen. Domstolen beslutade att genomföra en sällsynt förhandling för dessa fall, som ägde rum den 27 september 2022. Fallen gällde fem medborgare[77] som lämnade in klagomål till Europadomstolen i september 2017 respektive februari 2018. Elva enheter lämnade in *amicus curiae*-briefingar i det här fallet, bland annat European Criminal Bar Association[78], den polska ombudsmannen och FN:s särskilda rapportör för främjande och skydd av mänskliga rättigheter och grundläggande friheter samtidigt som terrorism bekämpas[79].

50. Även om denna väg för klagomål till Europadomstolen är öppen för medborgare är det tveksamt om detta kvalificerar sig som ett effektivt rättsmedel, med tanke på hur lång tid förfarandet tar. Fem år efter det första klagomålet finns det fortfarande inget domstolsbeslut i detta fall.

51. Med stöd av artikel 227 i förvaltningsprocesslagen hade klagomål lämnats in tidigare under 2017 till statsministern och respektive chef för de olika polis- och underrättelsetjänsterna. Dessa underrättelsetjänster omfattade CBA, den interna säkerhetstjänsten, den nationella skatteförvaltningen, den militära kontraspionagetjänsten, den nationella polisen, gränspolisen och det nationella gendarmeriet. Deras klagomål gällde att lagstiftningen tillät medlemmar av dessa polis- och underrättelsetjänster att övervaka deras telekommunikation och digitala kommunikation utan deras vetskap. Eftersom medlemmarna i de aktuella tjänsterna inte var skyldiga att informera dem om eventuell övervakning kunde sökandena följaktligen inte få lagenligheten av denna verksamhet prövad av en domstol, vilket enligt deras uppfattning stred mot den polska konstitutionen.

52. Mellan juni och september 2017 skickade cheferna för de ovan nämnda polis- och underrättelsetjänsterna sina svar på sökandenas klagomål. Med åberopande av artikel 8 (rätten till respekt för privatliv och familjeliv) i Europeiska konventionen om mänskliga rättigheter klagade sökandena över att de hemliga systemen för övervakning av telekommunikation, post- och digitalkommunikation och insamling av metadata, som infördes i tillämpningen av lagen, och antiterroristlagen, inkräktar på deras rätt till respekt för sitt privatliv. Med åberopande av artikel 8 tillsammans med artikel 13 (rätt till ett effektivt rättsmedel) hävdar sökandena att de inte hade något effektivt rättsmedel som skulle ha gjort det möjligt för dem att fastställa om de själva hade blivit föremål för

---

[77] Mikołaj Pietrzak, advokat, dekanus för Warszawas advokatsamfund, Dominika Bychawska-Siniarska, medlem och anställd i Helsingforsstiftelsen för mänskliga rättigheter, Barbara Grabowska-Moroz, universitetslektor och forskare och extern expert vid Helsingforsstiftelsen för mänskliga rättigheter, Wojciech Klicki och Katarzyna Szymielewicz, medlemmar av Panoptykon Foundation baserad i Warszawa.

[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.

hemlig övervakning och, om nödvändigt, få lagligheten av denna övervakning prövad av en domstol.

OFFENTLIG GRANSKNING

53. De oberoende medierna, som utövar offentlig granskning, är en annan del av de demokratiska kontrollerna och motvikterna. När det gäller användningen av spionprogram blev det polska public service-företaget, som i stor utsträckning kontrolleras av regeringspartierna, i praktiken delaktigt i den olagliga övervakningsskandalen genom att offentliggöra material som hämtats ur smartphones för flera av måltavlorna, däribland senator Krzysztof Brejza från oppositionen. Att offentliggöra information som erhållits vid specialtjänstens övervakningsinsats är en brottslig handling i sig, men ändå har inga åtgärder vidtagits av polisen eller den allmänna åklagaren.

POLITISK KONTROLL

54. Många nyckelpositioner i hela kedjan innehas av regeringspartiernas medlemmar eller av partitrogna. Inrikesministern och samordnaren för specialtjänsten, Mariusz Kaminski, fälldes 2015 för maktmissbruk och dömdes till tre års fängelse[80]. Men omedelbart efter parlamentsvalet 2015 benådade president Andrzej Duda honom på ett högst oegentligt sätt, vilket bl.a. fördömdes av högsta domstolen i Polen, EU-domstolen, Venedigkommissionen och det amerikanska utrikesministeriet. Det väcker frågor om hans oberoende och neutralitet. Kaminski har vägrat att träffa eller i avsevärd utsträckning samarbeta med PEGA-kommittén[81].

55. CBA kontrolleras helt och hållet av den styrande majoriteten och saknar oberoende, trots dess titel och mandat, som inrättades enligt lagen av den 9 juni 2006 om den centrala byrån för korruptionsbekämpning[82], i vilken det i artikel 1.1 anges att den centrala byrån för korruptionsbekämpning har inrättats som en särskild inrättning för att bekämpa korruption i det offentliga och ekonomiska livet, särskilt vid offentliga och lokala myndigheter samt för att bekämpa verksamhet som skadar statens ekonomiska intressen[83]. I 2022 års rapport om rättsstatsprincipen konstaterar kommissionen att oberoendet för de viktigaste institutionerna för bekämpning av korruption fortfarande är ett problem, särskilt med tanke på att den centrala byrån för korruptionsbekämpning är underordnad den verkställande makten och det faktum att justitieministern också är riksåklagare[84].

56. Regeringens ansträngningar för att få kontroll över rättsväsendet har dokumenterats och bekräftats i många olika instanser, däribland kommissionen, EU-domstolen och Europadomstolen.

---

[80] *Reuters*, https://www.reuters.com/article/uk-poland-president-pardon-idUKKCN0T62H620151117, 17 november 2015.
[81] EU Observer, https://euobserver.com/rule-of-law/156063, 15 september 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, Article 1.1.
[84] 2022 års rapport från kommissionen om rättsstatsprincipen, landskapitlet om rättsstatsprincipen i Polen, https://commission.europa.eu/system/files/2022-07/48_1_194008_coun_chap_poland_en.pdf, s. 1.

57. Det rättsliga och institutionella sammanhanget har inte bara skapats för att möjliggöra nästintill obegränsad övervakning med spionprogram, utan så gott som alla delar av processen kontrolleras också i hög grad av regeringspartierna. Till följd av detta har skyddsåtgärder som kan finnas på papper noll eller liten betydelse i praktiken.

MÅLTAVLORNA

58. De första dokumenterade fallen av användning av Pegasus i Polen går tillbaka till 2018. En av dessa gällde den tidigare biträdande finansministern, Pawel Tamborski, vars telefon hade hackats med Pegasus i februari 2018, vilket avslöjades av Amnesty International och Wyborcza i juli 2022. Samma dag grep CBA honom samt fem före detta tjänstemän vid ministeriet och marknadsanalytiker, som anklagades för att ha undervärderat marknadsvärdet på kemikalieföretaget CIECH i utbyte mot mutor. Domstolen samtyckte inte till gripandet och beordrade att de skulle friges. Den verkställande direktören och ägaren till PR-byrån Cross Media, Andrzej Długosz, var också en måltavla och hackades minst 61 gånger mellan mars 2018 och november 2019. Därefter begärde ombudsmannen mer information från myndigheterna, men ansträngningen var förgäves. Vid den tidpunkten fortsatte regeringen att förneka köpet av spionprogrammet.

59. Efter undersökningarna av Associated Press och Citizen Lab-forskarna vid universitetet i Toronto avslöjades att tre personer till hade varit måltavlor för Pegasus i Polen 2019[85], nämligen senator Krzysztof Brejza från oppositionen, advokat Roman Giertych och åklagare Ewa Wrzosek. Vissa medlemmar av den styrande majoriteten har bekräftat köpet av programvaran från NSO Group, men regeringen har inte officiellt erkänt att några specifika personer utsetts till måltavlor. Ingen av de tre måltavlor som nämns nedan har formellt anklagats för något brott, de har inte kallats till förhör, och det har heller inte framlagts någon begäran om att häva immuniteten för de måltavlor som innehar offentliga ämbeten med koppling till detta ärende.

60. Citizen Lab hade upptäckt ett antal infektioner i Polen i slutet av 2017, men de kunde inte identifiera offren vid den tidpunkten[86].

61. Användningen av spionprogram och insatser för att kontrollera medborgarna har en nära koppling till valsystemet. Flera av Pegasus måltavlor var på något sätt kopplade till val: senator Krzysztof Brejza (chef för valkampanjen för det största oppositionspartiet), Roman Giertych (advokat för oppositionsledaren och före detta ordföranden för Europeiska rådet, Donald Tusk), Ewa Wrzosek (åklagaren som undersöker poströstning för presidentvalet), högsta revisionsbyrån (NIK) (som offentliggjorde rapporter om poströstningen för presidentvalet) och Michael Kolodziejczak (grundaren av ett jordbrukspolitiskt parti som konkurrerar om samma väljare som regeringspartierna).

62. Samtidigt har den nationella valkommissionens oberoende ifrågasatts på grund av att den består av domare som valts av parlamentet och domstolar som det styrande partiet har skaffat sig kontroll över. Dessutom har distriktsdomstolen i Warszawa, som har

[85] The Guardian, https://www.theguardian.com/world/2022/feb/17/more-polish-opposition-figures-found-to-have-been-targeted-by-pegasus-spyware, *17 februari 2022*.
[86] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.

ansvar för registreringen av nya politiska partier[87], fyllts med regeringstrogna ”neodomare”, vars oberoende skulle kunna ifrågasättas.

KRZYSZTOF BREJZA

63. Senator Krzysztof Brejza tjänstgjorde som ledare för oppositionspartiet Medborgarplattformens valkampanj under Europavalet och de nationella valen när han blev måltavla för hackning med spionprogram[88]. Krzysztof Brejzas telefon attackerades 33 gånger under tiden han ledde Medborgarplattformens parlamentsvalskampanj 2019, med början den 26 april 2019 och fram till den 23 oktober 2019, bara några dagar efter valperiodens slut[89].

64. Som ett direkt resultat av hackningen av Krzysztof Brejzas telefon ska textmeddelanden ha stulits, manipulerats och därefter offentliggjorts i det statligt kontrollerade TV-nätet[90] under valet 2019, i en påstådd iscensatt smutskastningskampanj[91]. Detta har fått senator Krzysztof Brejza att ifrågasätta legitimiteten i valet 2019, som det styrande PiS-partiet vann med knapp marginal[92].

65. Även om PiS-regeringen medger att den har köpt in Pegasus, förnekar den kraftfullt anklagelserna att programvaran användes för politiska ändamål[93]. Jarosław Kaczyński har varken bekräftat eller förnekat att Krzysztof Brejza var en måltavla, men har hävdat att senatorn var kopplad till ”misstänkt brottslighet”, något som Brejza förnekar med kraft[94]. Inget åtal väcktes mot Brejza och han kallades aldrig för att vittna. Detta tyder på att användningen av spionprogram inte tjänade något utredningssyfte. Genom att antyda att Krzysztof Brejza hade kopplingar till brottslig verksamhet försökte regeringen att formellt legitimera användningen av spionprogram genom att skapa omständigheter under vilka den polska regeringen kunde använda spionprogrammet Pegasus av ett av de skäl som NSO Group anser vara ”legitimt”, när den överväger att sälja sin programvara till en regering, nämligen utredning av grov brottslighet[95].

66. I veckor var senator Krzysztof Brejza måltavla för en smutskastningskampanj som innehöll material som erhållits genom användning av spionprogrammet Pegasus. Det är anmärkningsvärt att sådant material offentliggjordes i public service-tv. Det finns inte någon förklaring till hur ett offentligt programföretag får tillgång till sådant material.

---

[87] Lag av den 27 juni 1997 om politiska partier, https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970980604/U/D19970604Lj.pdf, artikel 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 april 2022.
[89] The Guardian, ”More Polish opposition figures found to have been targeted by Pegasus spyware”, 17 februari 2022.
[90] 2022 års rapport från kommissionen om rättsstatsprincipen, landskapitlet om rättsstatssituationen i Polen, 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 december 2021.
[91] AP, https://apnews.com/article/technology-business-middle-east-elections-europe-c16b2b811e482db8fbc0bbc37c00c5ab, 23 december 2021.
[92] Financieele Dagblad, https://fd.nl/politiek/1426857/liberalen-europarlement-eisen-onderzoek-naar-spionagesoftware, 12 januari 2022.
[93] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 januari 2022.
[94] Politico, https://www.politico.eu/article/kaczynski-poland-has-pegasus-but-didnt-use-it-in-the-election-campaign/, 7 januari 2022.
[95] BBC, https://www.bbc.com/news/technology-57881364, 19 juli 2021.

Om Pegasus-hackningen av senator Krzysztof Brejza verkligen hade handlat om nationell säkerhet, vilket regeringen tycks antyda, skulle det vara ett mycket allvarligt brott att läcka det material som erhållits vid en hemlig säkerhetsoperation. Det faktum att det offentliga programföretaget också gisslantagits av regeringspartiet pekar snarare i riktning mot en smutskastningskampanj som arrangerats av regeringspartierna.

67. Vid den tidpunkten inleddes dock en brottsutredning av senator Krzysztof Brejzas far, Ryszard Brejza. Under sin tid som borgmästare i Inowrocław, en stad i centrala Polen, kallades Brejza Sr till förhör om påstådd misskötsel av offentliga medel och underlåtenhet att utföra sina plikter[96]. Detta förhör ägde rum direkt efter det att Brejza Jr inledde ett rättsligt förfarande mot Jarosław Kaczyński för förtal. Både Krzysztof och Ryszard Brejza har hävdat att anklagelserna mot Brejza Sr var en hämnd för stämningen.

68. Ryszard Brejza tog själv emot tio textmeddelanden mellan juli och augusti 2019 som Amnesty Internationals säkerhetslabb betraktade som misstänkta och som stämde överens med Pegasus kännetecken[97]. Medan hon drev senator Brejzas Europaparlamentskampanj fick dessutom senator Brejzas före detta assistent Magdalena Losko fyra misstänkta textmeddelanden i april 2019, som enligt Amnesty Internationals kriminaltekniska granskare var tekniskt förenliga med NSO Groups spionprogram Pegasus[98].

ROMAN GIERTYCH

69. Roman Giertych var måltavla för spionprogrammet Pegasus under de sista veckorna av parlamentsvalet 2019. Mellan september och december 2019 hackades Roman Giertych hela 18 gånger, och merparten av dessa skedde strax före valdagen den 13 oktober 2019. Vid den tidpunkten tjänstgjorde han som advokat för ledaren för oppositionspartiet Medborgarplattformen och f.d. premiärminister Donald Tusk. Under denna period företrädde Roman Giertych även Radosław Sikorski, tidigare utrikesminister och nuvarande parlamentsledamot i Europeiska folkpartiets grupp (kristdemokrater) (PPE). Radosław Sikorski tog sig an ett ärende för att undersöka Jarosław Kaczyńskis och dennes allierades inblandning i olaglig avlyssning som ledde till att Sikorskis samtal spelades in och offentliggjordes[99].

70. Liksom i fallet med Krzysztof Brejza har regeringen varken bekräftat eller förnekat om den var ansvarig för dessa attacker. Det rapporterades av Associated Press att en begäran om att arrestera Roman Giertych ingavs av en åklagare, angående en påstådd utredning av ekonomisk brottslighet, bara några timmar innan talespersonen för statens säkerhet Stanisław Żaryn besvarade frågor från AP om hackningen av Roman Giertychs telefon. Roman Giertych förnekar med kraft dessa påståenden. Stanisław Żaryn vägrade att kommentera det eventuella sambandet mellan dessa händelser. I en liknande incident

[96] AP, https://apnews.com/article/technology-business-software-hacking-spyware-8cc528ba7d46a61b378adf1ede9dd00f, 10 januari 2022.
[97] The Guardian, ”More Polish opposition figures found to have been targeted by Pegasus spyware”, 17 februari 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 juli 2022.
[98] The Guardian, ”More Polish opposition figures found to have been targeted by Pegasus spyware”, 17 februari 2022.
[99] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.

blev Roman Giertych föremål för en husrannsakan och hans hem genomsöktes av tjänstemän från CBA under 2020[100].

71. Under denna tid 2019 företrädde Roman Giertych dessutom Gerald Birgfellner, en österrikisk utvecklare. Birgfellner hade varit delaktig i ett byggprojekt för PiS-ledaren Jarosław Kaczynski, som han hade familjeband till, när affären blåstes av. Efter att inspelade samtal mellan de två offentliggjorts uppstod en politisk skandal för Kaczynski som sedan ställde in projektet. Gerald Birgfellner påstår att han aldrig fick betalt för sina tjänster och anlitade därför Roman Giertych[101]. Ministern för rättsliga frågor och riksåklagare Zbigniew Ziobro framhöll också under 2021 att han försökte väcka åtal mot Roman Giertych angående misstänkt brottslighet[102].

EWA WRZOSEK

72. Åklagare Ewa Wrzosek utsattes för hackning med spionprogrammet Pegasus så mycket som sex gånger mellan den 24 juni och den 19 augusti 2020[103]. Wrzosek är medlem i Lex Super Omnia, en sammanslutning av åklagare som arbetar för åklagarmyndighetens oberoende. Hon undersökte beslutet att hålla 2020 års presidentval i Polen mitt i den globala covid-19-pandemin när hon fråntogs fallet, som sedan lades ned. Det hör till riksåklagaren Zbigniew Ziobros, och hans högra hand den nationella åklagaren Bogdan Święczkowskis, befogenhet att besluta att inte väcka åtal i vissa fall eller att stryka underordnade åklagare från särskilda ärenden[104]. Därefter skickades Ewa Wrzosek med 48 timmars varsel till en annan åklagarmyndighet i en stad flera timmar från sitt hem. Det var när Ewa Wrzosek återvände till Warszawa som hon blev måltavla för spionprogrammet Pegasus. De polska myndigheterna har följt mönstret att inte bekräfta eller förneka sitt ansvar[105] [106].

73. Wrzosek har också inlett ett rättsligt klagomål om Pegasus-infektionen i sin mobiltelefon. Domstolen beordrade ett expertutlåtande från Citizen Lab om Pegasus-infektionen och Wrzosek har själv begärt att hennes telefon ska granskas av experterna på Citizen Lab. Åklagaren avslog dock denna begäran och valde ut en annan expert som inte kunde koppla någon infektion till Pegasus. Åklagaren bad dessutom teleoperatören att lämna över alla metadata som rör Wrzosek, under en period som inte är relevant för domstolsutredningarna. Wrzosek anser att hon fortfarande övervakas och att åklagarens förfarande syftar till att tillhandahålla ytterligare bevis som skulle kunna användas mot

---

[100] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.
[101] AP, https://apnews.com/article/elections-international-news-jaroslaw-kaczynski-european-parliament-poland-bed5ffc814e649f4bb4d10f82628b4c2, 16 februari 2019, TVP World, https://tvpworld.com/41262080/ruling-party-leader-im-no-dictator, 11 februari 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 december 2021.
[103] AP, https://apnews.com/article/technology-business-poland-hacking-warsaw-8b52e16d1af60f9c324cf9f5099b687e, 21 december 2021.
[104] 2022 års rapport från Europeiska kommissionen om rättsstatsprincipen, landskapitlet om rättstatssituationen i Polen, 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 december 2021.
[106] The Guardian, https://www.theguardian.com/world/2022/jan/24/polish-senators-draft-law-to-regulate-spyware-after-anti-pegasus-testimony, 24 januari 2022.

henne i andra fall[107].

74. Som Wrzosek lyfte fram under PEGA-kommitténs sammanträde den 19 januari 2023 åtalas hon för närvarande av åklagarmyndigheten för att hon avslöjat information om ett fall som inte har något samband med Pegasus och för att hon har deltagit i politisk verksamhet. Wrzosek kan inte bygga upp sitt rättsliga försvar, eftersom åklagarmyndigheten förnekar tillgång till handlingar[108]. Detta förefaller vara en uppenbar kränkning av rätten till en rättvis rättegång, och det ger intrycket av att det enda syftet med målet är att misskreditera Wrzosek.

ANDRA MÖJLIGA MÅLTAVLOR

HÖGSTA REVISIONSMYNDIGHETEN

75. Även om den inte var måltavla för Pegasus har de polska myndigheterna angripit och trakasserat NIK – den högsta revisionsmyndigheten – som har till uppgift att skydda de offentliga utgifterna och förvaltningen av offentliga tjänster och som offentliggjorde fakturorna för ”inköp av särskild teknik för att upptäcka och förebygga brottslighet” till ett totalt belopp av 25 miljoner zloty. Tidpunkten för attackerna är särskilt relevant med tanke på arten av den undersökning som NIK genomförde. Talespersonen för NIK bekräftade att man undersökte ogiltigförklaringen av presidentvalet år 2020. Resultatet av denna undersökning var att premiärministern, medlemmar av hans regering och en av justitieministeriets fonder delgavs anmälan om brott. Detta verkar förstärka misstankarna om att Pegasus främst har använts för politiska ändamål i Polen[109].

BUNDSFÖRVANTER TILL PIS

76. Det verkar som om Pegasus användes för ”förebyggande avlyssning” av ledare för och organisatörer av gatuprotester mot de reformer av författningsdomstolen som genomfördes av PiS. Det är dock inte bara motståndare till det styrande partiet som kan ha fallit offer för Pegasus. Enligt de källor som Wyborcza citerade blev den före detta talespersonen för PiS-partiet, Adam Hofman, spionerad på 2018, vilket gjorde honom till en av de första personerna som var måltavla efter köpet av spionprogrammet. Hofman grundade R4S, ett PR-företag, efter att ha blivit utesluten ur PiS-partiet[110] [111]. Enligt uppgift retade detta upp det styrande partiet som gjorde Hofman till en måltavla för övervakning. Han uppger att den information som inhämtades om honom senare användes i en smutskastningskampanj.

77. Enligt Wiadomości påstås dessutom den tidigare parlamentsledamoten för PiS Mariusz Antoni Kaminski och den före detta PiS-ministern för statskassan Dawid Jackiewicz ha fallit offer för regeringens användning av Pegasus[112]. Mariusz A. Kaminski uteslöts ur

[107] PEGA-kommitténs sammanträde, 19 januari 2023.
[108] PEGA-kommitténs sammanträde, 19 januari 2023.
[109] Notes from Poland, https://notesfrompoland.com/2022/02/07/polish-state-auditor-claims-7300-cyberattacks-made-against-it-including-suspected-use-of-pegasus/, 7 februari 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 oktober 2014.
[112] https://wiadomosci.onet.pl/kraj/pegasus-oto-kolejne-osoby-ktore-mialy-byc-inwigilowane-przez-sluzby-pis/yvt6tym.

PiS till följd av att han blev indragen i en skandal samtidigt som Hofman, men Jackiewicz förblir en medlem av det styrande partiet trots sitt plötsliga steg tillbaka från sin ministerroll[113].

78. En liknande smutskastningskampanj genomfördes också mot den tidigare ordföranden för Republiken Polens arbetsgivare, Andrzej Malinowski, av det styrande partiet i februari 2018. Han vittnade inför ett särskilt sammanträde i senatskommittén i april 2022 om hackandet av hans telefon med Pegasus för att samla in information för detta offentliga avlägsnande[114]. Han beskrev att meddelanden togs från hans WhatsApp och sms genom Pegasus och användes strategiskt för att sprida näthat mot honom. Attacken var vedergällning för att han inte höll med det styrande partiet och krävde alternativ ekonomisk politik.

AVSLUTANDE KOMMENTARER

79. Missbruket av Pegasus i Polen måste ses mot bakgrund av rättstatskrisen i landet, som inleddes 2015 när regeringen – under ledning av PiS – började avveckla rättsväsendet och sedan dess systematiskt har tagit över de flesta viktiga institutioner i landet och installerat partitrogna vid alla strategiska organ. Det styrande partiet sammanställde avsiktligt och metodiskt de rättsliga, institutionella och politiska byggstenarna i detta system för att skapa en sammanhängande och mycket effektiv ram, där användningen av Pegasus är en integrerad och viktig del av ett system för övervakning av oppositionen och regeringens kritiker för politisk vinning. Den utformades för att hålla kvar den styrande majoriteten och regeringen vid makten.

80. Övervakningen i Polen utvidgades enormt, vilket försvagade eller avlägsnade skyddsåtgärder och tillsynsbestämmelser. Under de systematiska och målinriktade lagändringar som den styrande majoriteten har infört har offrens rättigheter minimerats och rättsmedel har gjorts meningslösa i praktiken. Effektiv förhands- och efterhandsgranskning samt oberoende tillsyn har i själva verket avskaffats. Medlemmar i den polska regeringen och partitrogna kontrollerar direkt eller indirekt huvudpositionerna i systemet. Den information som inhämtas med hjälp av spionprogram används i smutskastningskampanjer mot regeringskritiker och oppositionen via de statligt kontrollerade medierna. Det faktum att den polska regeringen har breddat stadgar på det här systematiska och riktade sättet genom nationell lagstiftning håller den rättsliga grunden för övervakning kvar i strid med EU-rätten, avgörandet från 2014 av den polska författningsdomstolen och de polska medborgarnas grundläggande rättigheter. På så sätt legaliserades i grund och botten olaglig övervakning som tydligt strider mot EU:s lagstiftning och nationell lagstiftning.

I.B. Ungern

81. Ungern var ett av de första länderna som blev indraget i den europeiska spionprogramskandalen. År 2021 avslöjades det av Pegasusprojektet och bekräftades av

[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.

Amnesty International[115] att över 300 ungrare kan ha fallit offer för missbruk genom Pegasus, inbegripet politiska aktivister, undersökande journalister, advokater, entreprenörer, en oppositionspolitiker och en före detta regeringsminister.

82. I februari 2023 besökte en delegation från PEGA-kommittén Ungern. Kommittén drog slutsatsen att allt tyder på att spionprogram har missbrukats grovt i Ungern och att myndigheternas förklaring som hänvisar till den nationella säkerheten ansågs vara mycket osannolik. Starka bevis visar att människor har spionerats på i syfte att få ännu större politisk och finansiell kontroll över den offentliga sfären och mediemarknaden.

83. Kommittén var övertygad om att rättsstatsprincipen och de grundläggande demokratiska normerna allvarligt har överträtts i Ungern och att situationen är bland de värsta i EU. Till följd av åratal av demokratisk tillbakagång tycks statliga institutioner inte vara inriktade på att tjäna medborgarna och skydda deras rättigheter och friheter, utan snarare sträva efter att uppnå regeringens politiska mål. Kommittén uppmanade myndigheterna att tillåta en meningsfull undersökning av missbruk.

INKÖP AV PEGASUS

84. År 2017 röstade det ungerska parlamentets nationella säkerhetsutskott om att tillåta landets underrättelsetjänster att förvärva viss utrustning genom att följa det ordinarie offentliga upphandlingsförfarandet. På begäran av specialtjänsten för den nationella säkerheten (Nemzetbiztonsági Szakszolgálat, NBSZ) stödde det ungerska parlamentet förvärvet av sofistikerade spionprogram[116]. Förfarandet var dock hemligt och i begäran om godkännande angavs inte det specifika märket och typen av teknik[117].

85. Det ungerska inrikesministeriet köpte indirekt Pegasus för 6 miljoner euro via Communication Technologies Ltd. av NSO Groups företag i Luxemburg år 2017, kort efter att premiärminister Viktor Orbán träffat Polens premiärminister Mateusz Morawiecki och den tidigare israeliske premiärministern Benjamin Netanyahu[118] [119]. Det ungerska inrikesministeriet bekräftade inte detta förrän i november 2021, när ordföranden för parlamentsutskottet för försvar och brottsbekämpning, Lajos Kósa, erkände Fidesz-regeringens köp av Pegasus[120]. Lajos Kósa insisterade dock fortfarande på att spionprogrammet aldrig använts mot ungerska medborgare[121].

86. Den ungerska nationella myndigheten för dataskydd och informationsfrihet (NAIH)

---

[115] Euractiv, 'Hungary employed Pegasus spyware in hundreds of cases, says government agency', *1 februari 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*, Europaparlamentet, generaldirektoratet för unionens interna politik, utredningsavdelning C – Medborgerliga rättigheter och konstitutionella frågor, 5 december 2022, finns på https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf. Direkt36, "The inside story of how Pegasus was brought to Hungary", https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/.
[117] PEGA-uppdraget i Ungern, möte med ledamöterna i det ungerska parlamentets nationella säkerhetsutskott, 20–21 februari 2023.
[118] Financieele Dagblad, De wereld deze week: het beste uit de internationale pers. 7 januari 2022.
[119] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[120] DW, Hungary admits to using NSO Group's Pegasus spyware, 4 november 2021.
[121] DW, Hungary admits to using NSO Group's Pegasus spyware, 4 november 2021.

frågade om upphandlingsförfarandet för inköp av spionprogram och fick tillgång till det hemliga avtalet med NSO. Under PEGA-uppdraget i Budapest i februari 2023 uppgav NAIH:s ordförande, Attila Péterfalvi, inledningsvis att det inte var sant att Pegasus inte längre tillhandahölls de ungerska myndigheterna, vilket skulle innebära att Ungern inte var en av de två EU-medlemsstater som hade strukits från förteckningen över de 14 länder som NSO tillhandahåller Pegasus till. Péterfalvi drog senare tillbaka sitt uttalande och vidhöll att han inte hade någon information om huruvida NSO hade avslutat användningen av Pegasus i Ungern eller inte.

RÄTTSLIG RAM

87. I Ungern fastställs ramen för laglig avlyssning av kommunikation inom ramen för en brottsutredning i polislagen. Enligt polislagen kan övervakning av privatpersoner i en brottsutredning endast ske med rättsligt godkännande. I frågor som rör terrorism avser polislagen dock den utredningsövervakning som nämns i lagen om nationell säkerhet[122]. Enligt denna bestämmelse behöver man inte söka rättsligt godkännande för att godkänna användningen av denna teknik, utan justitieministern är i stället ansvarig för att utfärda tillståndet[123]. I begäran om tillstånd för övervakning anges inte vilken typ av teknik som kommer att användas[124].

88. Enligt lag CXXV från 1995 definieras nationella säkerhetsintressen som att säkerställa Ungerns suveränitet och skydda den lagliga ordningen, och inom denna ram, vilket är en ganska bred definition.

89. I ett historiskt mål (*Szabó och Vissy* mot *Ungern*[125]) konstaterade Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen) att lagen om nationell säkerhet inte innehöll tillräckligt exakta, effektiva och heltäckande garantier för att övervakningsåtgärderna skulle kunna vidtas, verkställas och åtgärdas. Lagen om nationell säkerhet utelämnar inte bara ett krav på att de som övervakas ska upplysas om detta, utan den föreskriver särskilt att måltavlorna inte får informeras av den tillståndsgivande parten om att de spioneras på[126]. Kravet på att anmäla offer fastställdes otvetydigt av Europadomstolen i målet *Klass m.fl.* mot *Tyskland*[127]. Dessutom finns det inga effektiva rättsmedel vid missbruk och ingen ordentlig tillsyn. Den ungerska regeringen har hittills inte genomfört någon av domarna.

FÖRHANDSGRANSKNING

90. Enligt lagen om nationell säkerhet är övervakning som utförs av specialtjänsten för nationell säkerhet med hjälp av spionprogram i de flesta fall beroende av tillstånd från justitieministern och av den domare som utses av ordföranden för huvudstaden

---

[122] Europeiska unionens byrå för grundläggande rättigheter (FRA), *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary*, 26 september 2014.
[123] FRA, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies: Hungary*, rättslig uppdatering, 23 oktober 2017.
[124] PEGA-uppdraget i Ungern, 20–21 februari 2023.
[125] Szabó och Vissy mot Ungern, ansökan nr 37138/14, dom av den 12 januari 2016, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-160020%22]}.
[126] Lag CXXV från 1995 om nationella säkerhetstjänster, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf.
[127] Klass m.fl. mot Tyskland, 6 september 1978, punkt 50, serie A nr 28.

Budapests lokala domstol i vissa specifika fall [128] [129]. Dessa beslut kan inte överklagas och det saknas i praktiken tillsyn över processen[130] [131].

91. När den nuvarande justitieministern Judit Varga inte är tillgänglig delegerar hon ansvaret för att godkänna användning av spionprogram mot medborgare, trots allvaret i ett sådant beslut, till statssekreteraren för justitieministeriet, en befattning som för närvarande innehas av Robert Repassy[132]. Detta har bekräftats av Repassy själv i ett svar han författat på skriftliga frågor om situationen[133]. Det har rapporterats omfattande om att Varga regelbundet överlät ansvaret till Repassys föregångare Pál Völner, som tvingades avgå från posten i december 2021 på grund av en stor korruptionsskandal[134]. Det rapporterades utförligt om att han tog emot miljoner ungerska forint i mutor från flera högt uppsatta aktörer i utbyte mot fördelaktiga beslut och utnämningar till viktiga befattningar av Völner i egenskap av statssekreterare[135].

92. Inrikesministern Sándor Pintér betonar att tillståndsförfarandet genom ministern eller domstolen alltid tillämpas utan undantag[136], men de svaga rättsliga bestämmelserna i lagen om nationell säkerhet gör det även möjligt för generaldirektörerna för specialtjänsten för nationell säkerhet att bevilja tillfälliga tillstånd för övervakning utan medgivande fram till dess att ett officiellt tillstånd kan beviljas. Detta innebär att specialtjänsten för nationell säkerhet kan agera utan något vederbörligt rättsligt tillstånd så länge de hävdar att en fördröjning av beviljandet av tillstånd skulle skada deras verksamhet. I sådana fall kan den obehöriga övervakningen fortsätta[137].

93. Den lagstadgade gränsen på högst 90 dagar för övervakning som föreskrivs i lagen kan förlängas med ytterligare 90 dagar på en enkel begäran från en generaldirektör till den tillståndsgivande tjänstemannen[138], vilket endast är avsett att verka som en rättslig säkerhet.

---

[128] Lag CXXV från 1995 om nationella säkerhetstjänster, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, avsnitt 56–58.
[129] *Europe's PegasusGate: Countering Spyware Abuse* – rapport från Europaparlamentets utredningstjänst, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, juli 2022, s. 20.
[130] Lag CXXV från 1995 om nationella säkerhetstjänster, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, avsnitt 57 och 58.
[131] 2022 års rapport från Europeiska kommissionen om rättsstatsprincipen, https://ec.europa.eu/info/sites/default/files/40_1_193993_coun_chap_hungary_en.pdf, s. 26.
[132] https://telex.hu/belfold/2021/12/10/repassy-robert-igazsagugyi-allamtitkar-varga-judit-igazsagugyi-miniszterium; *Europe's PegasusGate: Countering Spyware Abuse*, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729397/EPRS_STU(2022)729397_EN.pdf, juli 2022, s. 20.
[133] https://telex.hu/belfold/2022/01/27/varga-judithoz-kerulhetett-vissza-a-titkos-megfigyelesek-engedelyezese.
[134] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye; https://hungarytoday.hu/444-key-figure-in-volner-corruption-case-gyorgy-schadl-judge-fired-judiciary-obh/.
[135] https://telex.hu/belfold/2021/12/13/itt-vannak-a-reszletek-mirol-is-szol-a-fideszes-volner-pal-korrupcios-ugye.
[136] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 november 2021.
[137] Lag CXXV från 1995 om nationella säkerhetstjänster, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, avsnitt 59.
[138] Lag CXXV från 1995 om nationella säkerhetstjänster, http://jogszabalykereso.mhk.hu/translated/doc/J1995T0125P_20200701_FIN.pdf, avsnitt 58.

94. Dataskyddsmyndighetens roll är dessutom att se över all övervakning som utförs av säkerhetstjänsten. NAIH:s ordförande, Attila Péterfalvi, har kontinuerligt hävdat att all användning av Pegasus var för nationella säkerhetsändamål, vilket faller under de nationella regeringarnas exklusiva behörighet[139]. NAIH kontrollerade dock endast tillståndsförfarandet av tekniska skäl för att fastställa om behandlingen av uppgifter var laglig, men undersökte inte innehållet i användningen av Pegasus. NAIH ansåg inte att det var nödvändigt att kalla måltavlorna att vittna, eftersom NAIH hade tillgång till alla relevanta handlingar. Endast de fall som justitieministern hade godkänt undersöktes, eftersom NAIH inte kan utreda tillstånd som beviljats av en domare[140].Enligt Péterfalvi ledde NAIH:s utredning inte till att man upptäckte någon olaglig verksamhet eller något som strider mot NSO Groups försäljningsvillkor[141].

95. Chefen för NAIH utses av premiärministern, och därför kan dess oberoende ifrågasättas[142]. Europadomstolen fällde en dom i frågan i september 2022 i målet *Hüttl* mot *Ungern*[143] som ingavs av Tivadar Hüttl, advokat vid Hungarian Civil Liberties Union (HCLU), när det nationella säkerhetsutskottet, efter det att han påstås ha avlyssnats, beslutade att inte inleda någon ytterligare utredning och inga fler rättsmedel fanns tillgängliga[144]. Europadomstolen slog tydligt fast i sin dom att NAIH, trots sina befogenheter att undersöka säkerhetstjänstens verksamhet, var oförmögen att bedriva oberoende tillsyn av användningen av övervakning. Domstolen ansåg att dataskyddsmyndigheten saknade den kompetens som krävs för att göra det, med tanke på att säkerhetstjänsten har rätt att neka åtkomst till vissa handlingar av sekretesskäl[145]. I en sådan situation är det den minister som har ansvar för säkerhetstjänsten som får i uppgift att utföra en granskning, vilket inte på något sätt kan betraktas som oberoende tillsyn[146].

EFTERHANDSGRANSKNING

96. På oppositionens begäran höll det nationella säkerhetsutskottet och utskottet för säkerhet och försvar i nationalförsamlingen i november 2021 utfrågningar om användningen av spionprogram i Ungern och i synnerhet om att regeringen påstås ha utsett medborgare till måltavlor av politiska skäl. Regeringspartiet innehade fyra av sex platser i det nationella säkerhetsutskottet och förhindrade all meningsfull och demokratisk granskning av användningen av Pegasus. Regeringspartiets företrädare insisterade på att all övervakning hade godkänts via lämpliga kanaler, men vägrade att kommentera huruvida journalister eller politiker hade varit måltavlor eller inte. De vägrade även att kommentera det faktum att tillstånden hade delegerats av justitieministern till statssekreteraren Pál Völner, som är föremål för utredning till följd

[139] HVG, https://hvg.hu/itthon/20111117_Peterfalvi_palyaja_adatvedelem, 21 november 2011.
[140] PEGA-uppdraget i Ungern, 20 februari 2023.
[141] Euractiv, ”Hungary employed Pegasus spyware in hundreds of cases, says government agency”, 1 februari 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]}.
[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.

av anklagelser om korruption och maktmissbruk. De avvisade också begäranden från oppositionsmedlemmarna om att genomföra en djupgående utredning och att besöka säkerhetstjänsten för att genomföra intervjuer med enskilda agenter. Viktiga måltavlor, såsom Zoltán Varga och Szabolcs Panyi, hördes inte av utskottet. I augusti 2021 genomfördes endast en allmän proformautredning, eftersom detta var det enda som fick stöd från majoriteten[147]. Det går dock inte att veta exakt vad som sades, eftersom det styrande partiet har hemligstämplat protokollet från mötet fram till 2050[148].

97. NAIH inledde en utredning efter anklagelser från minst tio advokater, ordföranden för det ungerska advokatsamfundet och minst fem journalister som hade blivit måltavlor[149]. I rapporten om undersökningen, som publicerades den 31 januari 2022, fastslogs att Pegasus använts uteslutande av skäl som rör den nationella säkerheten.

98. Den ungerska åklagarmyndigheten avslutade även sin utredning om måltavlorna den 15 juni 2022 och slog fast att ingen obehörig övervakning hade skett.

99. Med tanke på att det är justitieministeriet som har befogenhet att bevilja tillstånd och att den Fidesz-stödda riksåklagaren Péter Polt omvaldes 2019 för ytterligare nio år (efter att redan ha innehaft posten i sammanlagt 15 år under två skilda mandatperioder fram till dess) kan en verklig tillsyn av regeringen ifrågasättas.

100. I Ungerns ram för korruptionsbekämpning finns inget stöd för detta med tanke på att inrikesministeriet, som från början köpte Pegasus av NSO Group, ansvarar för samordningen av all politik för korruptionsbekämpning och översyn av densamma[150].

RÄTTSMEDEL

101. När Pegasusskandalen inträffade i Ungern var journalister en av de grupper som regeringen mest inriktade sig på. Till följd av detta inledde i början av 2022 en grupp med sex journalister och aktivister rättsliga förfaranden inför de ungerska myndigheterna, kommissionen och Europadomstolen. Hungarian Civil Liberties Union (HCLU) företräder journalisterna Brigitta Csikász, Dávid Dercsényi, Dániel Németh och Szabolcs Panyi jämte Adrien Beauduin, en belgisk-kanadensisk doktorand och aktivist. Den sjätte parten har valt att förbli anonym. HCLU arbetar också med Eitay Mack i Israel för att inge ett ärende till justitieministern i syfte att inleda en utredning av NSO Group[151].

102. Det är många teknikaliteter som står i vägen för att pröva detta ärende i de ungerska domstolarna. Eftersom det inte finns någon omfattande rättspraxis på detta område är förfarandet oklart. Exempelvis har frågor om jurisdiktion uppstått. Dessa åtgärder och obevekliga fördröjningar betraktas främst som försök att få ärendet att läggas ned på

[147] PEGA-uppdraget i Ungern, möte med ledamöterna i det ungerska parlamentets nationella säkerhetsutskott, 20 februari 2023.
[148] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 november 2021.
[149] 2022 års rapport från kommissionen om rättsstatsprincipen, https://commission.europa.eu/system/files/2022-07/40_1_193993_coun_chap_hungary_en.pdf, s. 26.
[150] 2022 års rapport från kommissionen om rättsstatsprincipen, 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 januari 2022.*

grund av en teknikalitet eller ordningsfråga.

103. Det finns också en allvarlig fråga om tillgång till information. För att kunna begära åtkomst till filerna som innehåller alla data som samlats in om en enskild medborgare måste man ange det exakta namnet på den fil man vill begära ut, vilket är en nästan omöjlig uppgift att få tillgång till. Eftersom begärandena från de sex parter som företräds av HCLU oundvikligen avslogs av högsta domstolen sökte HCLU ett avgörande från författningsdomstolen där denna praxis, och den ungerska högsta domstolens dom, förklaras strida mot författningen. Författningsdomstolen avvisade dock HCLU:s begäran 2021.

104. Förutom att inleda rättsliga förfaranden inför domstolarna har HCLU även undersökt andra möjligheter att få åtkomst till uppgifter om sina sex klienter. Ett administrativt förfarande inleddes och godkändes enligt lagen om sekretessbelagda uppgifter och dataskyddslagen. Myndigheten för grundlagsskydd kommer dock att utföra en ettårig granskning i varje enskilt fall innan några resultat kommer att tillkännages[152]. Spionprogramsattackerna har även rapporterats till kommissionären för grundläggande rättigheter (ombudsmannen). Författningsdomstolen har fastställt att ombudsmannen har ansvaret för att utreda säkerhetstjänstens missbruk[153].

105. I ett ytterligare försök att uppnå öppenhet har HCLU begärt åtkomst till de data som samlats in och behandlats till följd av hackningen av de sex måltavlorna i ett förfarande som genomförs utanför domstolssystemet. Rätten till denna information finns dock endast så länge tillhandahållandet av uppgifterna till föremålen inte inverkar på den nationella säkerheten[154]. Detta ger de ungerska myndigheterna ytterligare en förevändning att återigen hävda skäl som har med den nationella säkerheten att göra[155]. Hittills har myndigheten för grundlagsskydd avvisat 270 förfrågningar från HCLU avseende informationsfrihet som lämnats in mellan 2018 och maj 2022[156].

POLITISK KONTROLL

106. Politisk kontroll över användningen av övervakning i Ungern är fullständig. Den Orbán-ledda Fidesz-regimen har skapat ett system där de kan göra advokater, journalister, politiska motståndare och organisationer i det civila samhället till måltavlor.

107. Inrikesministern ansvarade för inköpet av spionprogrammet Pegasus från början, och justitieministern har ännu ansvaret för att godkänna användandet av det. Ungerns rättsliga ram för övervakning av sina medborgare har upprepade gånger visat sig vara bristfällig. Det styrande partiet gör dock inga ansatser för att ändra den eftersom den passar deras behov.

108. Det är premiärministern som utser chefen för dataskyddsmyndigheten, det organ som ansvarar för oberoende tillsyn av säkerhetstjänstens användning av Pegasus. Med tanke på att han är politiskt utsedd saknas oberoende tillsyn. Ungern och Fidesz-regeringen är inte främmande för den här typen av politiska tillsättningar. Regeringen har

[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.
[155] https://hclu.hu/en/pegasus-whats-new.
[156] https://hclu.hu/en/pegasus-whats-new.

systematiskt tillsatt partitrogna i ledande roller i organ såsom författningsdomstolen, högsta domstolen, revisionsrätten, åklagartjänsten, Ungerns centralbank och den nationella valkommittén[157]. Detta medför att de institutioner som inrättas i syfte att bedriva tillsyn av de verkställande organen inte kan utföra sin uppgift på ett oberoende sätt[158].

109. När det gäller de praktiska aspekterna av att utföra övervakning med hjälp av spionprogram har telekomföretag en betydande roll att spela. Det finns flera exempel på måltavlor vars enheter blivit infekterade genom länkar som skickats via sms, och de stora mängder data som telekomföretagen har åtkomst till är mycket attraktiva för dem som vill utföra övervakning. Situationen i Ungern har blivit farligare eftersom den ungerska regeringen nyligen köpte telekomleverantören Vodafone Hungary[159]. Med stöd från den ungerska regeringen köpte företaget 4iG 51 % av Vodafone genom ett dotterbolag. Dessutom köpte den ungerska regeringen 49 % av aktierna i Vodafone genom ett annat företag. Det finns tydliga kopplingar mellan 4iG och regeringen. Företagets nuvarande ordförande är nära lierad med den ungerska oligarken Lőrinc Mészáros, som är en barndomsvän till Viktor Orbán. Den totala kostnaden för förvärvet är 1,7 miljarder euro och ger regeringen enkel och direkt åtkomst till mer än 3 miljoner kunders data[160]. Till följd av detta förvärv får staten dessutom en åtkomstpunkt till det flera decennier gamla globala meddelandesystemet SS7[161]. Med detta system kan mobiloperatörer förbinda användare över hela världen. Den ungerska staten kommer även att kunna hyra ut denna åtkomstpunkt till andra parter, som i fallet Rayzone[162].

MÅLTAVLORNA

110. Det rapporterades att telefonnummer till över 300 personer fanns med i slutsatserna från Pegasusprojektet[163]. Bland dem fanns minst fem journalister, tio advokater, Gödöllős borgmästare, som är medlem av ett oppositionsparti, en anställd av oppositionspartiet samt aktivister och framstående företagsägare[164]. Ingen av dem var dock föremål för någon brottsutredning eller anklagad för något. Även om förekomsten av telefonnummer på denna lista inte nödvändigtvis innebär att dessa telefoner faktiskt blev hackade är det en avslöjande insikt i regeringen Orbáns metodiska och systematiska agerande och inställning till grundläggande rättigheter och mediefrihet.

---

[157] Martin, J och Ligeti, M., ”Hungary. Lobbying, State Capture and Crony Capitalism”, Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. och Harris, P. (red.), Springer, 2017, s. 177–193, s. 178.

[158] Martin, J. och Ligeti, M., ”Hungary. Lobbying, State Capture and Crony Capitalism”, Lobbying in Europe: Public Affairs and the Lobbying Industry in 28 EU Countries, Bitonti, A. och Harris, P. (red.), 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 augusti 2022.

[160] *Reuters*, https://www.reuters.com/markets/deals/vodafone-agrees-sell-hungarian-unit-18-bln-2022-08-22/, 22 augusti 2022, Volkskrant, ”Orbán verstevigt met overname Vodafone Hongarije grip op telecommunicatie, critici uiten zorgen”.

[161] The Guardian, https://www.theguardian.com/world/2020/dec/16/israeli-spy-firm-suspected-accessing-global-telecoms-channel-islands, 16 december 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 juli 2021.

[164] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021 och Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.

Sedan den tiden 2021 har det bekräftats att ett antal måltavlor har hackats med hjälp av spionprogram. Från den tidpunkt då spionprogramsskandalen bröt ut i Ungern har det varit mycket tydligt att regeringens agerande var politiskt motiverat.

SZABOLCS PANYI

111. Hackningen av journalisten och redaktören Szabolcs Panyis telefon skedde när han arbetade på Direkt36. Som en av de få oberoende nyhetskällor som fortfarande finns i Ungern är den en viktig måltavla för det styrande partiet. Szabolcs Panyi är en välkänd och högt ansedd journalist, och det innebär att förutom inhämtande av viktig information direkt från Panyi själv skulle många av kontakterna och källorna i hans telefon vara värdefulla bifångster för regeringen.

112. Amnesty International bekräftade att Panyis telefon regelbundet hade hackats under en period på sju månader 2019[165]. Dessa attacker var riktade och skedde ofta vid tidpunkter då Panyi hade bett regeringen att uttala sig i någon fråga. Ett specifikt och oroande exempel på detta ägde rum den 3 april 2019. Panyi kontaktade då regeringen och bad dem att uttala sig om den artikel han hade skrivit om en rysk banks flytt till den ungerska huvudstaden, vilken uppmärksammades brett eftersom det fanns frågor om huruvida banken egentligen agerade täckmantel för den ryska underrättelsetjänsten[166]. Amnesty International bekräftade att Panyis telefon hackades dagen därpå och även att det fanns ytterligare elva liknande tillfällen då telefonen hackats omedelbart efter en begäran om ett uttalande från Orbáns regering[167]. Detta innebär att över hälften av Panyis förfrågningar ledde till att han blev måltavla under den sjumånadersperioden[168].

113. Myndigheterna har spelat ovetande om de riktade attackerna mot Panyi och vägrar att vare sig bekräfta eller förneka att de bär ansvar för dem. Regeringen har dock tidigare attackerat Panyi öppet, då Orbáns talesperson hävdade att han var en fanatisk politisk aktivist och anklagade honom för Orbánofobi och Ungernfobi[169]. Detta är ett uppenbart försök att rubba förtroendet för Panyi och måla ut både hans källor och honom själv som ”fienden” med hjälp av regeringens egna statligt kontrollerade medier.

114. Efter att Panyi undersökt det ungerska mäklarföretaget Communication Technologies Ltd, genom vilket Pegasus köptes, stämde företaget honom[170].

ZOLTÁN VARGA

115. Som vd och ordförande för Central Media Group är Zoltán Varga ägare till Ungerns största återstående oberoende nyhetssida, 24.hu. Efter att regeringen Orbán år 2020 inledde ett övertagande av dess största konkurrent, Index.hu, blev Varga siste man kvar

[165] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[166] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[167] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[168] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[169] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[170] PEGA-uppdraget i Budapest, 20–21 februari 2023.

som trotsade det styrande partiet[171].

116. Fidesz har under en tid bedrivit en smutskastningskampanj mot Varga via de statligt kontrollerade medierna för att rubba förtroendet för såväl hans egen offentliga persona som för publikationen, trots dess popularitet med över 7,5 miljoner läsare varje månad[172]. Varga hävdar att man vid olika tillfällen har försökt övertala honom att sälja genom både löften och hot, bland annat med erbjudanden om generösa statliga bidrag för annonsering i utbyte mot att anställa redaktörer som valts ut av regeringen[173]. Varga började misstänka att hans telefon var hackad av Pegasus när han mitt i ett samtal började höra en inspelning av samtalet. Senare under 2021 upptäckte Amnesty International att Varga mycket riktigt sannolikt hade blivit hackad av Pegasus, men det kunde inte bekräftas eftersom telefonen då hade ersatts[174].

117. Kort efter valet 2018 försökte den omvalde Orbán även att komma åt Varga indirekt. Efter en middag som Varga anordnade på våren 2018 för att diskutera regeringens övertagande av medierna, där en av gästerna var Attila Chikán, en före detta Fidesz-minister som numera är Orbán-kritiker, bekräftades att alla som närvarade hade antecknats som kandidater för övervakning[175]. Senare bekräftades det att en av gästerna var hackad vid tidpunkten för middagen, medan andras telefoner visade tecken på potentiella Pegasus-hackningar, men inga bevis på faktisk hackning[176]. Hackningen bekräftades mer eller mindre av en bekant till Vargas med anknytning till regeringen, som uttryckligen hänvisade till middagen i ett samtal och varnade för att umgås med personer som kunde vara ”farliga”[177].

118. Varga har även varit föremål för traditionell övervakning. Tjuvlyssning i arbetslivet, bilar utanför hans hem, helikoptrar ovanför huset och flera intrång i hans trädgård har fått honom att anlita säkerhetspersonal dygnet runt.

119. I oktober 2022 väcktes åtal mot Varga. Han kallades in för förhör av polisen och bara minuter senare rapporterade regeringsvänliga medier om det[178].

ADRIEN BEAUDUIN

120. Adrien Beauduin dök upp på Orbán-regimens radar 2018 när han tog sin doktorsexamen i genusvetenskap vid det centraleuropeiska universitetet. Institutionen grundades av George Soros och regeringen försökte då få den att lämna Ungern tillsammans med hela

[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 juli 2020.
[173] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[174] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[175] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[176] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[177] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[178] PEGA-uppdraget i Budapest, 20–21 februari 2023.

ämnet genusvetenskap[179]. Efter att ha deltagit i en protest i Budapest arresterades Adrien Beauduin i vad som betraktas som ett högst politiskt motiverat drag och åtalades för att ha angripit en polis, vilket han kraftfullt förnekar[180]. Det rapporterades att det i princip inte fanns några bevis mot Adrien Beauduin, och de bevis som presenterades hade tagits ordagrant från polisens vittnesmål i ett annat fall[181]. 2020 avslutades det straffrättsliga förfarandet mot Adrien Beauduin, som företräddes av HCLU i målet.

121. Företrädare för regeringen fördömde öppet det så kallade invandringsvänliga Soros-nätverket för att ha organiserat ”våldsamma demonstrationer i Budapest”[182]. Senare hittade man spår av Pegasus i Beauduins telefon, men det gick inte att bekräfta huruvida hackningen hade lyckats.

122. Med tanke på att Beauduin var en belgisk medborgare bosatt i Ungern vid tidpunkten för dessa incidenter går det inte att nog betona vikten av den gränsöverskridande aspekten i fallet. Den är av central betydelse, eftersom den påverkar EU-medborgarnas suveräna rättigheter, såsom rörelsefriheten och rätten att arbeta. Kommissionen har ett klagomålsförfarande som vem som helst kan använda sig av vid kränkning av de grundläggande rättigheterna. Adrien Beauduin ingav ett sådant klagomål den 24 januari 2022. Men sju månader senare, i ett svar till hans advokat daterat den 17 augusti 2022, framgick det att kommissionen inte kunde göra något, eftersom den saknar befogenhet[183].

ILONA PATÓCS

123. Advokaten Ilona Patócs misstänktes ha utsatts för övervakning med hjälp av Pegasus sommaren 2019, medan hon företrädde en klient i ett mycket uppmärksammat, utdraget mordfall[184]. Pga. den typ av mobilenhet hon använde var det dock inte möjligt att bekräfta huruvida hackningen lyckades helt och hållet eller när exakt den inträffade. Hennes klient, István Hatvani, hade redan avtjänat sju år för ett mord, vilket Ilona Patócs hävdar var en ”politiskt motiverad” dom[185]. Trots att en annan part senare tog på sig ansvaret för mordet skickade den ungerska appellationsdomstolen Hatvani tillbaka till fängelset för att sitta av den kvarvarande tiden av det ursprungliga straffet. Många andra advokaters telefonnummer har tagits upp på listan över potentiella måltavlor för Pegasus, däribland János Bánáti, ordförande för det ungerska advokatsamfundet[186]. I synnerhet detta utseende av måltavlor visar på ett tydligt åsidosättande från regeringens sida av advokatsekretessen.

---

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

GYÖRGY GÉMESI

124. György Gémesi, borgmästaren i Gödöllő, blev också måltavla för spionprogrammet Pegasus i slutet av 2018, samtidigt som han var under hård press från regeringen och okända personer bröt sig in i hans hem och hans barns hem. Samtidigt som den oppositionsledande borgmästaren, i slutet av 2018, blev även en bekant till Gémesi i regeringen utsatt för spionprogrammet. Dessutom fanns även två telefonnummer som kopplades till Gémesis partikolleger och hans före detta vice borgmästare med på listan.

BRIGITTA CSIKÁSZ

125. Under övervakningen av Brigitta Csikász, en av Ungerns mest erfarna brottsjournalister, höll hon bland annat på att undersöka missbruk av EU-medel. Csikász undersökningar avslöjade att de ungerska myndigheterna, trots varningar från Europeiska byrån för bedrägeribekämpning (Olaf), saknade antingen viljan eller förmågan att lagföra misstänkt användning av EU-medel, vilket återigen bevisar att chefsåklagaren, trots att åklagarmyndigheten är rättsligt oberoende och i högsta grad hierarkisk, faktiskt har nära anknytning till regeringspartiet och premiärministern.

126. Även János Bánáti, ordförande för det ungerska advokatsamfundet och försvarsadvokat, och flera andra advokater har utsatts för Pegasus.

ANDRA MÅLTAVLOR

127. Personer inom det styrande partiets kretsar har också blivit måltavlor för spionprogram. Den oberoende ungerska nyhetskanalen Direkt36 rapporterade i december 2021 att chefen för János Áders, president för republiken och en nära allierad till Orbán, skyddstjänst och hans personliga livvakt hade hackats med hjälp av spionprogrammet Pegasus. Szabolcs Panyi, journalist vid Direkt36 och offer för spionprogram, har rapporterat att denna typ av spioneri främst beror på den ungerske premiärministerns växande paranoia. Cecília Szilas, Ungerns före detta ambassadör i Kina, blev utsatt för Pegasus strax innan hon blev förste rådgivare till Viktor Orbán. Attila Aszódi, statssekreterare i Orbáns regering med ansvar för anläggningen och utvecklingen av kärnkraftverket Paks II, som ska anläggas av Roszatom, har också blivit utsatt för spionprogrammet Pegasus. Han blev måltavla 2018 när han ingick i regeringen men hade konflikter med sin överordnade, minister János Süli.

128. Dessutom har både sonen och advokaten till en av Orbáns äldsta vänner, Lajos Simicska, hackats med Pegasus[187]. Simicska gick från att vara en nära vän till Orbán till att bli en motståndare. Han höll på att sälja sitt mediekonsortium som varit en stor drivkraft bakom konflikten efter Orbáns valseger 2018 när attackerna mot sonen och advokaten inträffade[188]. Simicska var inte själv måltavla av den enkla anledningen att han inte använder smartphone, vilket gör det omöjligt att hacka honom med

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

spionprogram som Pegasus[189]. Ajtony Csaba Nagy, Simicskas advokat, misstänkte att han blivit hackad när han hörde en inspelning av sitt samtal med Simicska under ett telefonsamtal. Dessa misstankar verkade senare bekräftas när information som endast diskuterats vid dessa samtal dök upp i ungerska medier[190]. Med tanke på att majoriteten av alla nyhetskanaler i Ungern ägs av staten är det troligt att regeringen själv lämnade informationen direkt till medierna.

SPIONPROGRAMSFÖRETAG

129. Den ungerska regeringen har inte bara köpt och använt spionprogrammet Pegasus mot sin befolkning, utan har också agerat värd för andra företag på underrättelsemarknaden, såsom Black Cube och Cytrox. Black Cube är en israelisk privat underrättelsetjänst som består av före detta anställda vid Mossad, den israeliska militären samt den israeliska underrättelsetjänsten[191]. På företagets egen webbplats beskrivs det som en ”kreativ underrättelsetjänst” som tar fram ”skräddarsydda lösningar på komplexa företagsrelaterade utmaningar och rättsliga tvister”[192]. Black Cube har varit inblandat i ett antal offentliga hackningskontroverser, bland annat i USA och i Rumänien[193]. Kritiska kopplingar har också upptäckts till NSO Group och spionprogrammet Pegasus. Efter stora påtryckningar från allmänheten om det faktum att NSO anlitar Black Cube för att göra sina motståndare till måltavlor erkände NSO:s tidigare vd, Shalev Hulio, att de anlitat Black Cube i åtminstone en situation på Cypern.

130. Black Cube började verka i Ungern under valet 2018, när de spionerade på flera olika icke-statliga organisationer och personer som hade något slags koppling till George Soros och rapporterade till Viktor Orbán, så att han skulle kunna använda uppgifter om deras aktiviteter i en smutskastningskampanj[194]. Bland måltavlorna fanns bland annat Marta Pardavi, advokat och medlem i Ungerns Helsingforskommitté, en framstående icke-statlig organisation för mänskliga rättigheter[195]. Den information som samlades in genom övervakningen av dessa personer och organisationer dök inte bara upp i de ungerska statligt kontrollerade medierna, utan även i Jerusalem Post[196].

131. Ytterligare en koppling till Ungern är Cytrox Holdings Zrt., som är registrerat på en adress i Budapest. Cytrox, skaparen av spionprogrammet Predator, grundades ursprungligen i Nordmakedonien innan det köptes av WiSpear, som nu är en del av Intellexa Alliance som drivs av Tal Dilian.

---

[189] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[190] The Washington Post, https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/, 19 juli 2021.
[191] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7 oktober 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 april 2022.
[194] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.
[195] *Reuters*, https://www.reuters.com/article/meta-facebook-cyber-idCNL1N2T12MC, 16 december 2021.
[196] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.

132. Användningen av Pegasus i Ungern tycks vara en del av regeringens beräknande och strategiska kampanj för att förstöra mediefriheten och yttrandefriheten[197]. Regeringen har använt detta spionprogram för att inleda en regim av trakasserier, utpressning, hot och påtryckningar mot oberoende journalister, medier, politiska motståndare och organisationer i det civila samhället, med lätthet och utan rädsla för repressalier. Regeringens kontroll över nästan alla ungerska mediekanaler, såväl tryckta som i radio och tv, gör det möjligt för den att fortsätta att sprida sin egen version av sanningen och förhindra att en stor del av den offentliga granskning som de oberoende medierna genomför når de ungerska medborgarna.

133. Den lag som tillåter avlyssning är snarare ett verktyg för regeringen för att kontrollera och utöva makt, än en sköld för medborgarnas rättigheter och privatliv, och den är en av de svagaste i Europa[198] [199]. Systemet bryter uppenbart mot europeiska krav och standarder för övervakning av medborgare som fastställs i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna och i domar från Europadomstolen[200], trots att regeringen insisterar på att de har agerat lagligt i alla skeenden och helt efterlever lagen[201] [202]. Även om regeringen konsekvent faller tillbaka på grunden ”nationell säkerhet”[203] är påståenden att offren utgör ett hot mot den nationella säkerheten befängda.

I.C. Grekland

134. Kommittén besökte Grekland i november 2022 som en del av ett gemensamt uppdrag mellan Grekland och Cypern. Medlemmarna träffade biträdande minister Giorgos Gerapetritis och diskuterade uppmärksammade övervakningsfall och den bredare frågan om mediepluralism och rättsstatsprincipen i Grekland. De träffade också undersökande journalister, ledamöter av det grekiska parlamentet, ordföranden för den grekiska dataskyddsmyndigheten (HDPA), företrädare för ADAE och icke-statliga organisationer samt människorättsförsvarare.

135. Besöket visade att ökade insatser krävs för att garantera öppenhet. Anklagelserna om missbruk av övervakning och användning av spionprogram måste undersökas grundligt och vara föremål för sanktioner vid behov. Alla nödvändiga skyddsåtgärder bör införas och reformer bör förbättra insynen och säkerställa lämplig rättslig tillsyn av användningen av övervakning. Besöket bekräftade också att det behövdes tydliga regler för att begränsa användningen av nationell säkerhet som grund för övervakning,

[197] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[198] The Guardian, https://www.theguardian.com/news/2021/jul/18/viktor-orban-using-nso-spyware-in-assault-on-media-data-suggests, 18 juli 2021.
[199] DW, ”Pegasus scandal: In Hungary, journalists sue state over spyware”, 29 januari 2022.
[200] Se, bland annat, Roman Zakharov mot Ryssland [GC], nr 47143/06, ECHR 2015 39. Klass m.fl. mot Tyskland, 6 september 1978, § 50, serie A nr 28. 40, Prado Bugallo mot Spanien, nr 58496/00, § 30, 18 februari 2003, Liberty m.fl. mot Förenade kungariket, nr 58243/00, § 62, 1 juli 2008.
[201] AP, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0, 4 november 2021.
[202] Euractiv, ”Hungary employed Pegasus spyware in hundreds of cases, says government agency”, 1 februari 2022.
[203] Euractiv, ”Hungary employed Pegasus spyware in hundreds of cases, says government agency”, 1 februari 2022.

säkerställa en ordentlig rättslig tillsyn och garantera en sund, pluralistisk mediemiljö.

136. Under 2022 skakades Grekland genom en rad rapporter om användningen av spionprogram, vilket är olagligt enligt grekisk lagstiftning. Den 26 juli 2022 ingav Nikos Androulakis, ledamot av Europaparlamentet och ledare för det grekiska oppositionspartiet PASOK, ett klagomål till högsta domstolens åklagarmyndighet om försök att smitta hans mobiltelefon med spionprogrammet Predator[204]. Försöket att smitta Nikos Androulakis telefon med spionprogram upptäcktes när Europaparlamentets it-avdelning kontrollerade telefonen[205]. Enligt it-avdelningens kriminaltekniska analyser skedde hackningsförsöken medan Nikos Androulakis kandiderade till ledare för oppositionspartiet. Detta avslöjande satte ljuset på de klagomål som ekonomireportern Thanasis Koukakis ingivit tidigare, i april och maj 2022, om att hans telefon smittats med Predator. Infektionen bekräftades av CitizenLab. I september hävdade också Christos Spirtzis[206], tidigare minister för infrastruktur och lagstiftare för partiet Syriza, att han varit måltavla för spionprogrammet Predator. Även om hans mobiltelefon inte kontrollerades officiellt delade Spirtzis de länkar han mottagit med två tekniker som muntligen bekräftade att han hade blivit utsedd till måltavla[207]. Dessutom avslöjades det senare samma månad att den grekiska nationella underrättelsetjänsten enligt uppgift hade planterat spionprogram hos två av sina egna anställda[208]. Den 5 och 6 november avslöjade de grekiska medierna en lista med 33 måltavlor för Predator, varav alla var kända personligheter[209]. Listan – som varken bekräftats eller förnekats av regeringen eller av dem som övervakats – innehåller namn på personer som arbetar inom politik, affärsliv och medier i Grekland. Effekterna av den påstådda övervakningen av personer som finns med i förteckningen kan bli mer omfattande, eftersom alla deras respektive kontakter och förbindelser också indirekt kan bli föremål för spionverksamheten, inbegripet deras kontakter i EU:s organ. Den stora förekomsten av spionprogram var enligt uppgift synlig redan i bilagan till Meta-rapporten 2021, där 310 falska webbplatser med anknytning till spionprogramföretaget Cytrox nämns, varav 42 skapades för att vilseleda måltavlor enbart i Grekland[210] [211]. I slutet av november 2022 publicerade *Documento* en lista över 498 webbadresser som använts för att spionera med spionprogrammet Predator. En del av webbadresserna var identiska med dem som publicerades i Meta-rapporten 2021[212]. Den 28 februari 2023 bekräftade HDPA:s ordförande att 300 textmeddelanden avseende spionprogrammet Predator hade skickats till cirka 100 enheter. ADAE:s ordförande uppgav dessutom att ADAE hade agerat med anledning av flera klagomål och identifierat två fall av användning av Predator och ett bankkontonummer till en person bakom de falska textmeddelandena. ADAE:s undersökning av nya klagomål pågår[213].

137. I augusti 2022 medgav den grekiska regeringen att EYP hade övervakat Androulakis och Koukakis, men förnekade att den någonsin hade använt eller förvärvat

---

[204] Euractiv, EU Commission alarmed by new spyware case against Greek socialist leader.
[205] Tagesspiegel, Griechenlands Watergate: Ein Abhörskandal bringt Athens Regierung in Not.
[206] *Reuters*, One more Greek lawmaker files complaint over attempted phone hacking.
[207] https://insidestory.gr/article/predator-perissoteroi-apo-20-oi-stohoi-toy-stin-ellada-symfona-me-tin-arhi-prostasias.
[208] Efsyn, Targeting the disliked.
[209] Documento, Apocalypse: They Watched – This Sunday in Document.
[210] Meta, Threat Report on the Surveillance-for-Hire Industry.
[211] Inside Story, ”Who was tracking the mobile phone of journalist Thanasis Koukakis?”
[212] Documento, 27 november 2022.
[213] Diskussion i PEGA-kommittén med Konstantinos Menoudakos och Christos Rammos, den 28 februari 2023.

spionprogrammet Predator. Även andra fall av övervakning av EYP avslöjades under denna period, däribland övervakningen av journalisten Stavros Malichoudis[214]. Hittills har inga officiella skäl till övervakningen uppgetts.

138. Den 8 augusti 2022 publicerade premiärminister Mitsotakis ett videomeddelande där han tvetydigt hävdade att övervakningen av Androulakis var ”laglig” men ”politiskt oacceptabel”. Han sa ingenting om övervakningen av Koukakis eller några av de andra påstådda fallen. Han hävdade även att han inte hade haft kännedom om övervakningen, men att om så varit fallet skulle han inte ha tillåtit den[215]. Enligt det officiella uttalandet från regeringens talesman Yiannis Oikonomou försökte statsminister Giorgos Gerapetritis ge Androulakis fullständig information om skälen till att han övervakats, så snart premiärministern fick kännedom om den ”lagliga avlyssningen” av Androulakis[216]. Androulakis avvisade erbjudandet om att bli informerad och förklarade att en sådan privat genomgång skulle vara olaglig och att den enda lagliga vägen var genom det grekiska parlamentet. Senare förklarade minister Gerapetritis inför parlamentet att han aldrig hade känt till skälen och begärde att relevant information skulle hållas strikt hemlig. EYP står under direkt kontroll av premiärminister Kyriakos Mitsotakis till följd av en lagändring som antogs strax efter att hans parti Néa Dimokratía kom till makten 2019[217].

139. Efter avslöjandena avgick Grigoris Dimitriadis, regeringens generalsekreterare med ansvar för samarbetet mellan den grekiska regeringen och EYP samt EYP-direktören Panagiotis Kontoleon[218].

INKÖP

140. I slutet av 2019 stod generalsekreteraren Dimitriadis i kontakt med NSO Group för inköp av spionprogrammet Pegasus. I januari 2020 lämnade NSO Group in ett officiellt förslag om ett avtal mellan regeringar om 50 miljoner euro. Efter att avtalet undertecknats skulle den enskilda undertecknaren dra sig ur och EYP ta över. EYP skulle samarbeta med Mossad för att installera systemet. Förslaget avslogs så småningom[219].

141. Både EYP och regeringen förnekar bestämt att Predator någonsin har köpts eller använts av de grekiska myndigheterna[220].142. I frånvaro av bevis för identiteten på köparen och användaren av Predator i de grekiska fallen kan det inte med säkerhet fastställas om eller hur regeringen eller en annan aktör hade förvärvat Predator. Om det inte var den grekiska regeringen måste det slås fast att en icke-statlig aktör bar ansvaret för (försöken till) hackning av Koukakis och Androulakis telefoner. Detta skulle vara ett brott enligt grekisk lagstiftning, som då måste utredas. Hypotesen om privata aktörer

---

[214] Solomon, ”Solomon’s reporter Stavros Malichudis under surveillance for ‘national security reasons’”, Ekathimerini, ”Wiretapping case: The phone data that triggered developments”, Europaparlamentets utredningstjänst. *Greece’s Predatorgate. The latest chapter in Europe’s spyware scandal?*
[215] *Reuters*, ”Greek PM says he was unaware of phone tapping of opposition party leader”.
[216] 1b LIFO, ”Androulakis denied information in private upon his surveillance”, https://www.lifo.gr/now/politics/o-androylakis-arnithike-idiotiki-enimerosi-apo-ton-gerapetriti-kai-zita-na-toy.
[217] Euractiv, ”Another Greek opposition lawmaker victim of Predator”.
[218] POLITICO, ”PM Mitsotakis feels the heat as two top Greek officials quit in spy scandal”.
[219] https://insidestory.gr/article/greek-state-and-spyware-vendor-intellexa-they-are-acquainted-after-all.
[220]Europaparlamentets utredningstjänst. *Greece’s Predatorgate. The latest chapter in Europe’s spyware scandal?*

bakom Predatorattackerna är vidare högst osannolik, eftersom den inte skulle förklara valet av måltavlor. I princip är det dock inte omöjligt att förvärva eller använda spionprogram utan att statliga organ faktiskt direkt köper programmet. Spionprogram kan köpas via ombud, mäklarföretag eller mellanmän, som vi har sett i andra fall, eller så kan arrangemang göras med försäljare av spionprogram för att tillhandahålla vissa tjänster som hör samman med spionprogram. Det råder inget tvivel om att det fanns nära förbindelser och ömsesidiga beroendeförhållanden mellan vissa personer och händelser som rörde regeringen, EYP och leverantörerna av spionprogram, framför allt Krikel, en prioriterad leverantör av kommunikations- och övervakningsutrustning till bland annat polisen och EYP. Krikel är nära knutet till personer i kretsen kring premiärminister Mitsotakis. Det finns allt fler bevis för de omfattande förbindelserna mellan Intellexa, det företag som äger spionprogrammet Predator, och den grekiska staten. Den 16 januari 2023 ålade den grekiska dataskyddsmyndigheten Intellexa böter om 50 000 euro för underlåtelse att samarbeta och vägran att lämna över uppgifter om dess kundkrets, som en del av den undersökning som inleddes i juli 2020 efter Androulakis klagomål. Undersökningen pågår fortfarande[221].

143. En möjlighet är att Predator förvärvades genom Ketyak, centret för tekniskt stöd, utveckling och innovation, som inrättades av Kontoleon, den tidigare generaldirektören för EYP. Det är oberoende av EYP[222] och deltar i projekt som rör forskning, innovation och teknisk utveckling[223].

MÅLTAVLORNA

GRIGORIS DIMITRIADIS

144. Dimitriadis är brorson till premiärminister Mitsotakis, och var fram till augusti 2022 generalsekreterare på hans kontor. I denna roll var han ansvarig för regeringens kontakter med EYP. Han tvingades avgå den 5 augusti 2022 efter avslöjandet om att EYP hade avlyssnat Androulakis telefon. Inledningsvis tillskrevs hans avgång det skadliga politiska klimatet, men senare ålade premiärministern honom det politiska ansvaret för avlyssningen av Androulakis och andra politiker[224].

145. Panagiotis Kontoleon, före detta chef för EYP, erkände sin ”sociala relation” med Dimitriadis för det grekiska parlamentets undersökningskommitté. Kontoleon hade utsetts av Mitsotakis regering, men vissa lagbestämmelser behövde ändras för att legitimera utnämningen[225].

146. Dimitriadis har även en nära förbindelse på flera sätt med Felix Bitzios och Giannis Lavranos. Dessa tre män känner varandra personligen. Dimitriadis och Lavranos var varandras best man (”koumbaroi”)[226] och Dimitriadis är gudfar till Lavranos andra barn[227]. Dimitriadis har även haft en direkt förbindelse med Bitzios via

---

[221] https://www.dpa.gr/el/enimerwtiko/deltia/epiboli-prostimoy-stin-intellexa-ae-gia-mi-synergasia-me-tin-arhi.
[222] https://www.tovima.gr/print/politics/to-trigono-lfpou-egkatestise-lfto-predator-crstin-ypiresia-crpliroforion-crkai-i-lista-crton-xeiriston-tou/.
[223] https://www.nis.gr/en/ketyak.
[224] https://www.iefimerida.gr/politiki/paraitisi-dimitriadi-klima-toxikotitas-ohi-predator?amp, https://primeminister.gr/2022/08/08/29961.
[225] *Ieidiseis*, ”SYRIZA – PASOK findings on wiretapping: Both scandal and cover-up”.
[226] TVXS, Giannis Lavranos: ”The koumbarias with Tsouvala and Dimitriadis”.
[227] Ieidiseis, ”SYRIZA – PASOK findings on wiretapping: Both scandal and cover-up”.

affärstransaktioner med Bitzios bror[228].

147. Det innebär att han är i centrum för ett nätverk av både professionella och personliga förbindelser med personer vid Intellexa, Krikel och EYP.

148. Dimitriadis är enligt uppgift även bekant med Andreas Loverdos, kandidat till ledare för PASOK-KINAL 2021.

FELIX BITZIOS

149. Affärsmannen Felix Bitzios hade varit inblandad i den enorma skandalen kring Bank of Piraeus brott mot kapitalrörelserestriktioner. Under utredningen hade Bitzios tillgångar frysts[229]. Bitzios gynnades av en lagstiftningsändring som infördes av premiärminister Mitsotakis snart efter att han kom till makten 2019. Den kontroversiella ändringen fastställde en tidsfrist för frysning av tillgångar, som gjorde att frysta tillgångar kunde släppas efter högst 18 månader[230]. Tack vare ändringen av Mitsotakis regering kunde Bitzios tillgångar släppas.

150. Bitzios har kopplingar till Cypern genom sitt företag Santinomo, som är registrerat på Cypern, och sin förbindelse med Tal Dilian. Bitzios verkar ha spelat en avgörande roll för överföringen av Intellexa till Grekland[231].

151. Bitzios ägde 35 % av aktierna i Intellexa, genom sitt företag Santinomo. Den 4 augusti 2022 registrerade han dock överlåtelse av alla sina aktier till Thalestris, Intellexas moderbolag[232]. Datumet för registreringen av överföringen är ett par dagar efter avslöjandet av hackningen av Androulakis. Överföringen i sig skulle dock ha ägt rum den 28 december 2020, över 19 månader tidigare. Bitzios distanserade sig därmed retroaktivt från sitt 1/3-ägande i Intellexa. Bitzios hade dock varit knuten till Intellexa från mars 2020 till juni 2021 som biträdande administratör[233].

GIANNIS LAVRANOS

152. Giannis Lavranos hade åtalats för skatteundandragande och journalisten Koukakis hade rapporterat om Lavranos fall.

INTELLEXA

153. Spionprogrammet Predator säljs via Intellexa, ett konsortium av säljare av spionprogram med närvaro i bland annat Cypern, Grekland, Irland och Frankrike. Tal Dilian, som tidigare hade en karriär i det israeliska försvaret, upprättade konsortiet i Cypern. Hans andra exfru, den polska medborgaren Sara Hamou, är en central figur i det intrikata nätverket av företag. Tal Dilian har också förvärvat maltesiskt medborgarskap. Greklands regering förklarade att två exportlicenser hade tilldelats Intellexa, varav en godkände export till Madagaskar. Dessutom utfärdade den grekiska regeringen en exportlicens för Predator till Sudan. Det har inte bekräftats till vem

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

licensen utfärdades, om det var till Intellexa eller någon annan enhet. Intellexa har enligt uppgift också exporterat sina produkter till Bangladesh.

154. Den 30 november 2022 avslöjade en utredningsrapport från Lighthouse Reports, i samarbete med den israeliska tidningen *Haaretz* och den grekiska kanalen Inside Story, att Tal Dilians Predator-verksamhet i Grekland påstås vara kopplad till ett Cessna-plan som flög från Grekland och Cypern till Sudan mellan april och augusti 2022. Det rapporterades att detta jetplan i hemlighet olagligen överlämnade avancerad övervakningsteknik till milisen Rapid Support Forces (RSF)[234]. Genom flygjournaler kunde man koppla samman det privata jetplanet, som flög in och ut via Cypern, med Tal Dilian, tidigare verksam i det israeliska försvaret, som inrättade Intellexa Alliance 2019, som har säten i Cypern och Grekland. Den 18 februari 2023 bekräftade kommissionen att den hade kontaktat de nationella myndigheterna i Grekland och Cypern för att klargöra denna fråga. Kommissionen har dock inte fått något svar[235]. Den 19 april 2023 bekräftade den grekiska utrikesministern Miltiadis Varvitsiotis att den grekiska regeringen hade godkänt exportlicensen för spionprogrammet Predator till Sudan. Ministern förnekar dock Predators roll i de senaste sammanstötningarna mellan de sudanesiska väpnade styrkorna och RSF-milisen i Sudan[236].

155. I december 2022 avslöjade den grekiska regeringen att den hade tillhandahållit Intellexa två exportlicenser den 15 november 2021. Enligt Alexandros Papaioannou, talesperson för Greklands utrikesministerium, gav en av dessa licenser tillstånd att sälja Predator till Madagaskar[237]. Licensen beviljades trots landets bristande respekt för mänskliga rättigheter[238] och eventuellt i strid med EU:s lagstiftning om varor med dubbla användningsområden[239]. Generalsekreteraren för internationella ekonomiska förbindelser, Ioannis Smyrlis – som godkände försäljningen av Predator till Madagaskar – avgick efter dessa avslöjanden[240] och tillträdde som vice generaldirektör för det styrande partiet Néa Dimokratía, som är ansvarigt för det kommande valet.

156. Utöver exporten av spionprogram visar ett fall enligt uppgift att Grekland stod värd för utbildningsresor för användning av spionprogram. I juni 2021 köpte Bangladesh ett fordon med spionprogram från det cypriotiska företaget Passitora. Enligt handlingar från Bangladesh inrikesministerium utbildades personal från det nationella centrumet för övervakning av telekommunikation (NTMS) i användning av spionfordonet i

---

[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, sammanträde i PEGA kommittén, 28 mars 2023.

[236] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/; https://www.aa.com.tr/en/africa/greek-government-admits-opposition-s-claim-of-spyware-export-to-sudan/2876824.

[237] *The New York Times*, 8 december 2022, ”How the Global Spyware Industry Spiraled Out of Control”, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[238] *The New York Times*, 8 december 2022, ”How the Global Spyware Industry Spiraled Out of Control”, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[239]Europaparlamentets och rådets förordning (EU) 2021/821 av den 20 maj 2021 om upprättande av en unionsordning för kontroll av export, förmedling, transitering och överföring av samt tekniskt bistånd för produkter med dubbla användningsområden (EUT L 206, 11.6.2021, s. 1).

[240] *The National Herald*, ”Top Greek Official Who Authorized Predator Spyware Sale Resigns”.

Grekland mellan 2021 och 2022. Fordonet anlände till Bangladesh i juni 2022[241].

KRIKEL

157. Krikel är en prioriterad leverantör av utrustning till grekiska brottsbekämpande myndigheter och säkerhetsmyndigheter. Det är också den grekiska representanten i RCS Lab, ett italienskt företag som säljer övervakningsprogram. Dessutom sägs det att Giannis Lavranos är 50 %-ägare av Krikel, genom ett annat företag med namnet Mexal[242]. Det verkar dock inte möjligt att med säkerhet fastställa vem som är den verkliga ägaren av Krikel, trots dess många kontakter med statliga myndigheter.

158. År 2014 såldes Giannis Lavranos företag Ioniki Technologiki till Tetra Communications i London. Samma år var Ioniki Technologiki ett av de tre företag som donerade Tetra Communications Systems till det grekiska ministeriet för skydd av medborgare[243]. 2014 hade den grekiska regeringen även visat intresse för det italienska spionprogrammet RCS Galileo från företaget Hacking Team, vilket avslöjades av Wikileaks, men denna programvara förvärvades aldrig[244]. Donationen av Tetra underlättades av ett företag baserat i Florida, vilket gjorde det möjligt att kringgå de vanliga anbudsförfarandena. Donationen till den grekiska regeringen accepterades 2017. År 2018 undertecknade Krikel ett avtal om underhåll och teknisk support på 10,8 miljoner euro. Krikels administratör Stanislaw Pelczar undertecknade på Krikels vägnar, men det verkar som att Lavranos var informellt involverad i alla förhandlingarna[245]. Krikel blev en viktig leverantör till det grekiska ministeriet för skydd av medborgare. Sedan 2018 har det undertecknat sju kontrakt med den grekiska regeringen, varav sex är hemliga[246].

159. Företaget Krikel blev också den lokala representanten för det italienska företaget RCS Lab. I juni 2021 påstås EYP ha köpt ett avlyssningssystem från RCS Lab[247] genom Krikel[248]. Vid denna tidpunkt var Dimitriadis ansvarig för kontakterna mellan regeringen och EYP. Några källor har dokumenterat att det var under installationen av detta nya system som material som innehöll information om övervakningen av Androulakis och Koukakis försvann, vilket påstods bero på ett tekniskt problem[249]. Andra källor hävdade dock att Kontoleon hade beordrat att arkiven skulle förstöras den

---

[241] *Haaretz*, ”Israeli Spy Tech Sold to Bangladesh, World’s Third-largest Muslim Country, Despite Dismal Human Rights Record”.
[242] Det finns flera intressanta kopplingar här. Lavranos sålde sin familjs hus i Aten till ett pris under marknadsvärdet till Albitrum Properties i april 2021. Företrädaren för Albitrum Properties under försäljningen var Felix Bitzios halvbror Theodoros Zervos. Albitrum är ett cypriotiskt företag och aktieägare är Mexal Services Ltd. Mexal Services äger 100 % av Eneross Holdings Ltd. Eneross Holdings äger dessutom Krikel. Giannis Lavranos har sitt kontor registrerat på samma adress som Eneross Holdings och Mexal Services i Cypern. Se Inside Story, ”Predatorgate’s invisible privates”, och TVXS, ”G. Lavranos behind KRIKEL – How the deception of the Parliament was attempted [Revealing documents]”.
[243] Inside Story, ”Predatorgate’s invisible privates”.
[244] Inside Story, ”The timeless interest of the Greek authorities in spyware”.
[245] Inside Story, ”Predatorgate’s invisible privates”.
[246] Inside Story, ”Predatorgate’s invisible privates”.
[247] *Hellas Posts English*, ”The EYP supplier contaminates smartphones in Greece as well”.
[248] TVXS, ”G. Lavranos behind KRIKEL – How the deception of Parliament was attempted [Revealing documents]”.
[249] TVXS, ”G. Lavranos behind KRIKEL – How the deception of Parliament was attempted [Revealing documents]”.

29 juli 2022[250].

160. Intressant nog har anställda på Krikel setts arbeta på Ketyak, vilket påstås ha varit ”pro bono”. Ketyak har enligt uppgift tilldelats 40 miljoner euro från EU:s facilitet för återhämtning och resiliens, genom ett konfidentiellt upphandlingsförfarande som bygger på ett hemligt beslut av premiärministern[251]. Olaglig användning av EU-medel för att finansiera olagliga spionprogram skulle vara ett allvarligt brott mot EU-rätten och faller inom ett flertal europeiska organs behörighetsområde, bland annat Europeiska åklagarmyndigheten.

161. Anställda på Krikel påstås även ha besökt EYP:s kontor i Agia Paraskevi i december 2021 och januari 2022 i egenskap av ”utbildare”. Dessa kontor styrs av den grekiska regeringen och påstås vara de platser där spionprogrammet Predator har installerats[252].

BITZIOS OCH LAVRANOS INBLANDNING

162. Bitzios och Lavranos var båda aktivt involverade i att inrätta Krikel 2017. Tillsammans arrangerade de utnämnandet av den polska advokaten Stanislaw Pelczar som administratör i Krikel i oktober 2017[253]. Bitzios företag Viniato Holdings Limited anlitades senare som konsult av Krikel mellan januari och augusti 2018 mot ett arvode på cirka 550 000 euro (trots att Krikel endast hade en omsättning på 840 000 euro det året)[254].

163. Bitzios och Pelczar har även andra gemensamma affärsförbindelser. Det framgår i Paradisläckan att de gemensamt äger ett företag som är registrerat på Malta under namnet Baywest Business[255]. Tal Dilian, grundaren av Intellexa, innehar dessutom ett maltesiskt (gyllene) pass[256] och har även ett brevlådeföretag vid namn MNT Investments LTD på östaten[257].

164. Bitzios och Lavranos är två nyckelfigurer i leveransen av kommunikations- och övervakningsmaterial till statliga myndigheter såsom polisen och EYP. Bitzios var ytterst viktig i det företag som säljer Predator. De stod nära Dimitriadis och gynnades båda av lukrativa statliga kontrakt. De gynnades av den nya regeringens lagändring om att släppa deras frysta tillgångar. De hade ett motiv att använda spionprogram mot Koukakis. Det finns en mycket uppenbar och hög risk för intressekonflikt och korruption när företagsintressen, personliga förbindelser och politiska anknytningar vävs samman. De skulle dessutom vara i en sådan position att de kan lämna avgörande

[250] Euractiv, ”Greek MEP spyware scandal takes new turn”.
[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”.
[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”.
[255] Internationella konsortiet för undersökande journalistik, Offshore Leaks Database, Paradise Papers – Malta Corporate Registry.
[256] Maltas regering, naturaliserade personer registrerade som medborgare i 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/.

information om förvärvet och användningen av Predator i Grekland.

165. Trots den uppenbara betydelsen av att Bitzios och Lavranos vittnade inför det grekiska parlamentets undersökningskommitté avvisade Néa Dimokratías majoritet i kommittén oppositionens begäranden om att kalla dessa personer till en utfrågning.

FÖRHANDSGRANSKNING

166. I Grekland är det ett brott att infektera en enhet med spionprogram, vilket föreskrivs i flera artiklar i den grekiska strafflagen, däribland artikel 292 om brott mot säkerheten i telefonkommunikationer, artikel 292B om hindrande av driften av informationssystem och artikel 370 om brott mot brevsekretess. Dessutom är framställning, försäljning, leverans, användning, import, innehav och distribution av skadlig programvara (vilket inbegriper spionprogram) ett brott på det sätt som beskrivs i artikel 292C i den grekiska strafflagen[258]. Denna artikel ändrades av den grekiska regeringen den 9 december 2022.

167. Antalet godkända avlyssningar har ökat avsevärt under åren. Från 4 871 år 2015 till 11 680 år 2019 till 15 475 år 2021[259]. För närvarande behandlas omkring 60 ansökningar varje dag, fram till nyligen av en enda åklagare. I EYP:s bestämmelser om att häva sekretessen för kommunikation mellan medborgare av skäl som rör den nationella säkerheten nämns heller inte namnet på den berörda personen eller skälet till hävandet av sekretessen. Det enda som anges är telefonnumret och åberopandet av den nationella säkerheten[260].

168. Rättsliga tillstånd att övervaka privat kommunikation samt förlängning och hävning av sådana tillstånd måste godkännas av den behöriga åklagaren. Enligt lag 3649/2008 ska den åklagare som är behörig att häva sekretess och konfidentialitet vara EYP:s interna åklagare. Genom en lagändring under Tsipras II-regeringen 2018 minskades antalet åklagare som krävs för att godkänna avlyssning från två till en. Den åklagare som ansvarar för de aktuella fallen är Vasiliki Vlachou[261]. Vlachou träffade inte PEGA under deras uppdrag i Grekland.

RÄTTSAKT OM LAGSTIFTNINGSINNEHÅLL

169. Efter avslöjandena om övervakning har premiärminister Mitsotakis föreslagit ändringar av EYP:s verksamhetsram. En av dessa ändringar är införandet av rättsakten om lagstiftningsinnehåll av regeringen den 9 augusti 2022. Punkt 2 i artikel 9 i lag 3649/2008 har uppdaterats och kräver nu ett yttrande från det permanenta utskottet om institutioner och transparens om utnämnandet av EYP-guvernören[262]. Eftersom det styrande partiet för närvarande har absolut majoritet i parlamentets särskilda permanenta utskott om institutioner och transparens godkände det dock utnämnandet av Themistoklis Demiris som ny EYP-guvernör, medan alla andra oppositionspartier var

[258] International Comparative Legal Guide, *Cybersecurity Laws and Regulation Greece 2022*.
[259] Ekathimerini, ”Wiretapping and ’national security’”.
[260] Reporters United, ”Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis”.
[261] Reporters United, ”Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis”.
[262] EfSyn, ”What (does not) change with the Act of Legislative Content for EYP?”.

emot[263]. För övrigt är EYP:s andra biträdande befälhavare Dionysis Melitsiotis[264], en f.d. medlem i premiärministerns privata kontor, och en annan biträdande direktör är Anastasios Mitsialis, en f.d. företrädare för Ny Demokrati[265].

170. Genom lagen återinfördes även bestämmelsen att två åklagare ska godkänna begäranden om övervakning[266]. Artikel 5 i lag 3649/2008 om bestämmelsen om hävande av sekretessen för kommunikation av EYP kompletterades med en ansökan om godkännande till den behöriga åklagaren och därefter godkännande av riksåklagaren vid appellationsdomstolen[267].

EFTERHANDSGRANSKNING

171. Sedan 2019 har EYP:s åtgärder stått under premiärminister Kyriakos Mitsotakis direkta kontroll efter en lagändring till följd av Ny Demokratis seger 2019[268].

172. Den parlamentariska kontrollen utövas av det permanenta utskottet om institutioner och transparens. Detta utskott övervakar EYP:s verksamhet och har behörighet att samla in dokument, utreda personer och kalla generaldirektören till förhör[269]. Det styrande partiet har absolut majoritet i utskottets nuvarande sammansättning.

173. Den grekiska myndigheten för kommunikationssäkerhet och sekretess (ADAE) säkerställer sekretesskydd för brev och all annan typ av kommunikation[270]. Enligt dess stadga är ADAE administrativt oberoende[271]. ADAE kan utföra undersökningar av EYP:s anläggningar, databaser och arkiv samt tekniska utrustning och handlingar[272].

174. Sekretessen för kommunikationer i enlighet med lag 2225/1994 föreskriver att denna sekretess endast kan avstås i fall som rör den nationella säkerheten och för utredning av allvarliga brott. Efter att sekretessen har hävts föreskrivs i artikel 5 i denna lag att ADAE kan informera måltavlorna för utredningarna, förutsatt att syftet med utredningen inte äventyras[273]. En enskild persons rätt att få tillgång till information om huruvida han eller hon har varit föremål för övervakning beskrivs i lag 2472/1997[274]. När ADEA i mars 2021 upplyste EYP om Thanasis Koukakis rätt att informeras ingav regeringen dock omedelbart lagändringsförslag 826/145 den 31 mars 2021, genom vilket man upphävde ADAE:s möjlighet att underrätta medborgare om att sekretessen

---

[263] Ekathemirini, ”Themistoklis Demiris: His appointment to the management of EYP was approved by a majority”.
[264] Ekathimerini, ”National security takes center stage”.
[265] Greek City Times, ”Greek PM appoints new security and intelligence chiefs”.
[266] Kort sammanfattning, *Greece’s Predatorgate: The latest chapter in Europe’s spyware scandal?*, Europaparlamentet, Generaldirektoratet för parlamentarisk utredning och analys, den 8 september 2022.
[267] EfSyn, ”What (does not) change with the Act of Legislative Content for EYP?”.
[268] Euractiv, ”Another Greek opposition lawmaker victim of Predator”.
[269] Centre for European Constitutional Law, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies*.
[270] ADAE, *Presentation*.
[271] ADAE*, Regulatory framework.*
[272] Centre for European Constitutional Law, *National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies*.
[273] Constitutionalism, ”Oförenlighet mellan artikel 87 i lag 4790/2021 med Europeiska domstolen för de mänskliga rättigheternas garantier för att skydda konfidentialitet vid kommunikation”.
[274] Den grekiska dataskyddsmyndigheten, *Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data*

för kommunikationer hade hävts[275]. Detta berövar i praktiken den enskilda personen hans eller hennes rätt till information. Lagändringen infördes på ett mycket irreguljärt sätt. Den lades till en orelaterad lag (som rörde covidåtgärder) och de tidsfrister som krävdes enligt konstitutionen respekterades inte[276] [277] [278]. Ingen korrekt samrådsprocess genomfördes därmed.

175. Mitsotakis syfte med akten om lagstiftningsinnehåll var att stärka transparensen och ansvarsskyldigheten. Akten upphäver dock inte ändring 826/145.

176. Den 9 december 2022 antog den grekiska regeringen lag 5002/2022 i syfte att uppdatera och skapa en effektiv rättslig ram för skydd av personuppgifter, kommunikationssekretess och stärkande av cybersäkerheten. Genom lagen införs dock flera bestämmelser som försvagar skyddsåtgärder, granskning och ansvarsskyldighet. I enlighet med artikel 4.7[279] ska alla förfrågningar om information från individer om huruvida de har övervakats av skäl som rör den nationella säkerheten utredas av en kommitté med tre ledamöter som består av EYP:s chef, den EYP-anslutna åklagaren samt chefen för ADAE. Detta innebär att majoriteten är personer som gav order om (EYP:s chef) och godkände (åklagaren) övervakningen från början. Detta gör det dessutom praktiskt taget omöjligt för individer som övervakas av skäl som rör den nationella säkerheten att på ett lämpligt sätt informeras i efterhand, eftersom de enligt lagen inte får begära denna information förrän tre år efter att övervakningen har avslutats. Detta är oförenligt med relevant rättspraxis vid Europadomstolen och den europeiska stadgan om de mänskliga rättigheterna[280] och medför inga bestämmelser om institutionella kontroller och motvikter för att säkerställa att de statliga myndigheterna fungerar korrekt. ADAE har uttryckt sin oenighet när det gäller organet med tre ledamöter. Hittills finns ingen operativ ram för trepartskommittén, vilket innebär att den i praktiken inte fungerar[281]. Dessutom kriminaliserar den nya lagen enskildas eller privata företags användning av spionprogram, och gör det för första gången lagligt för offentliga myndigheter att köpa spionprogram och ger regeringen rätt att inrätta förfarandet genom ett presidentdekret. Det finns inga bestämmelser om rättslig tillsyn över användningen av spionprogram eller om utläggning av avlyssning till privata enheter.

177. Privata aktörers tillhandahållande av spionprogram är enbart olagligt om sådan

---

[275] https://www.reportersunited.gr/8646/eyp-koukakis/.
[276] Det grekiska parlamentet, Konstitutionen.
[277] Det grekiska parlamentet, Representanthusets arbetsordning.
[278] Govwatch, *Violation of the legislative process for amendments in law 4790/2021*.
[279] https://www.kodiko.gr/nomothesia/document/844300/nomos-5002-2022.
[280] https://www.dsa.gr/%CE%B4%CE%B5%CE%BB%CF%84%CE%AF%CE%B1-%CF%84%CF%8D%CF%80%CE%BF%CF%85/%CE%B1%CF%80%CE%BF%CF%86%CE%AC%CF%83%CE%B5%CE%B9%CF%82-%CE%B4%CF%83/%CE%B1%CF%80%CF%8C%CF%86%CE%B1%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B4%CE%B9%CE%BF%CE%B9%CE%BA%CE%B7%CF%84%CE%B9%CE%BA%CE%BF%CF%8D-%CF%83%CF%85%CE%BC%CE%B2%CE%BF%CF%85%CE%BB%CE%AF%CE%BF%CF%85-%CF%84%CE%BF%CF%85-%CE%B4%CF%83%CE%B1-%CE%B3%CE%B9%CE%B1-%CF%84%CE%B7-%CE%B3%CE%BD%CF%89%CE%BC%CE%BF%CE%B4%CF%8C%CF%84%CE%B7%CF%83%CE%B7-%CF%84%CE%BF%CF%85-%CE%B5%CE%B9%CF%83%CE%B1%CE%B3%CE%B3%CE%B5%CE%BB.
[281] Diskussion i PEGA-kommittén med Konstantinos Menoudakos och Christos Rammos, den 28 februari 2023.

programvara ingår på en uttömmande lista över ”förbjudna spionprogram” som uppdateras av chefen för EYP var sjätte månad. Det bemyndigar EYP att lagligen förvärva spionprogram, eftersom viktiga relevanta frågor uteslutande hanteras via sekundärlagstiftning (t.ex. presidentdekret). Därför anses en uppdaterad version av ett befintligt spionprogram vara laglig fram till dess att den upptas på ovan nämna lista. Definitionen av ”nationell säkerhet” i lagen är extremt bred och vag och står därmed i strid med artikel 19.1 i konstitutionen, som kräver en snäv tolkning. ADAE hämmas vidare i sina ansträngningar att utöva konstitutionsenliga roll när det gäller att kontrollera hävande av sekretessen. Den oberoende myndighetens roll, som var avgörande för avslöjandet av övervakningsskandalen, tonas ned i den nya lagen, trots relevanta konstitutionella garantier.

178. Möjligheterna till efterhandsgranskning försvagades vidare av att det tog lång tid för Grekland att fullt ut genomföra EU:s visselblåsardirektiv[282]. Den 27 januari 2022 inledde kommissionen ett överträdelseförfarande genom att skicka en formell underrättelse till Grekland. Den 15 juli 2022[283] skickade kommissionen ett motiverat yttrande med en svarsfrist om två månader. Det grekiska parlamentet röstade slutligen om lag 4990/2022 den 11 november 2022 om införlivande av EU:s visselblåsardirektiv i grekisk lagstiftning.

OFFENTLIG GRANSKNING

179. Grekland ligger sist av alla EU-länder i det internationella pressfrihetsindexet 2022 – på plats 108 av 180[284]. År 2021 mördades journalisten Giorgos Karaivaz. Mordet har fortfarande inte klarats upp. Journalister utsätts för trakasserier och strategiska rättegångar mot allmänhetens deltagande. Grigoris Dimitriadis[285] inledde strategiska rättegångar mot allmänhetens deltagande mot nyhetsbolagen Reporters United och *Efimerida ton Syntakton* (EfSyn)[286] efter att han tvingades avgå. Minister Oikonomou försökte misskreditera en reporter från Politico, Nektaria Stamouli, genom att antyda att hennes artiklar om spionprogramskandalen hade politiska motiv[287]. Två av måltavlorna för övervakning, Thanasis Koukakis och Stavros Malichoudis, hade faktiskt rapporterat på ett kritiskt sätt om fall av korruption och bedrägeri, samt den dåliga behandlingen av migranter. Athanasios Telloglou och Eliza Triantafillou rapporterade om spionprogramskandalen, och de påstås ha satts under övervakning[288]. Isidoros Dogiakos, åklagare vid Greklands högsta domstol, misskrediterade dessutom mediekanaler som kritiserade Greklands rättsliga myndigheter för att inte ha hanterat den grekiska avlyssningsskandalen på ett tillräckligt sätt. Han försökte rentav skrämma de medier som undersökte skandalen genom att begära selektiv skatterevision av deras ägare[289].

---

[282] https://ec.europa.eu/commission/presscorner/detail/SV/inf_22_3768.
[283] https://ec.europa.eu/commission/presscorner/detail/SV/inf_22_3768.
[284] https://rsf.org/en/index.
[285] Tagesspiegel.
[286] EUobserver, ”Greece accused of undermining rule of law in wiretap scandal”.
[287] https://www.ekathimerini.com/news/1191760/foreign-press-association-rejects-targeting-of-journalist-by-govt-spox/.
[288] Heinrich-Böll-Stiftung, ”In conditions of absolute loneliness”.
[289] Journalistförbundet ESIEA fördömer hot från åklagaren vid högsta domstolen, https://www.esiea.gr/oi-dimosiografikes-enoseis-gia-tis-di/.

RÄTTSMEDEL

DEN NATIONELLA TRANSPARENSMYNDIGHETEN

180. Enligt artikel 82 i lag 4622/2019 bär den nationella transparensmyndigheten (EAD) ansvar för att stärka ansvarsskyldigheten, transparensen och integriteten för åtgärder som vidtas av regeringsorgan, statliga organ, administrativa myndigheter och offentliga organisationer. EAD ska dessutom förebygga, upptäcka och åtgärda bedrägeri och korruption hos offentliga och privata enheter. Enligt denna nya lag har EAD tagit över alla ansvarsområden, rättigheter och skyldigheter från följande offentliga organ: Generalsekretariatet för korruptionsbekämpning, myndigheten för inspektörer och revisorer för offentlig förvaltning, tillsynsmyndigheten för offentlig förvaltning, inspektionsorganet för hälso- och sjukvårdstjänster, inspektionsorganet för offentliga bygg- och anläggningsarbeten samt myndigheten för inspektörer och revisorer för transport[290]. Även om ADAE:s oberoende föreskrivs i konstitutionen är EAD inte en oberoende myndighet.

181. Den 22 juli 2022 inledde EAD en utredning av det påstådda köpet av spionprogrammet Predator av ministeriet för skydd av medborgare och EYP. Granskningen omfattade den grekiska polisen, EYP och företagen Intellexa och Krikel. EAD slutförde sin rapport den 10 juli 2022, men lämnade rapporten till EYP för föregående godkännande. Den officiella rapport som skickades till Thanasis Koukakis den 22 juli innehöll bara en bråkdel av den fullständiga granskning som utfördes av EAD. Under sken av skydd av personuppgifter doldes flera namn i granskningen, däribland namnen på EAD:s revisorer, den EYP-åklagare som kontrollerade EAD:s ursprungliga rapport och advokater och revisorer för de inblandade juridiska personerna[291].

182. I EAD-rapporten slogs det slutligen fast att varken EYP eller ministeriet för skydd av medborgare hade ingått avtal med Intellexa eller andra relaterade nationella företag. De hade inte heller köpt eller använt spionprogrammet Predator[292]. EAD utredde dock inte bankkontona som tillhörde Intellexa och Krikel, eller de bankkonton som tillhör de anslutna offshorebolagen. Dessutom besökte EAD Intellexas och Krikels kontor först efter att två månader gått sedan den första publikationen om användningen av Predator i Grekland, och då arbetade medarbetarna hemifrån på grund av covid-19. EAD träffade inte heller juridiska företrädare för de aktuella företagen[293].

183. Det finns frågetecken kring EAD-ledningens oberoende. Den nuvarande direktören, en tidigare anställd hos Mitsotakis, har haft denna befattning tillfälligt sedan sommaren 2022. Det är oklart varför rekryteringsförfarandet inte har inletts. Direktören för EAD träffade inte PEGA under uppdraget i november 2022. Direktören träffade delegationen från utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor den 7 mars 2023, och vid detta tillfälle togs frågor upp om spionprogram i Grekland.

DEN GREKISKA MYNDIGHETEN FÖR KOMMUNIKATIONSSÄKERHET OCH SEKRETESS (ADAE)

184. I juli 2022 bekräftade Nikos Androulakis att han hade lämnat in ett klagomål till Högsta

[290] https://www.kodiko.gr/nomothesia/document/545222/nomos-4622-2019.
[291] Inside Story, ”From Koukakis to Androulakis: A new twist in the Predator Spyware case”.
[292] Inside Story, ”From Koukakis to Androulakis: A new twist in the Predator Spyware case”.
[293]Inside Story, ”From Koukakis to Androulakis: A new twist in the Predator Spyware case”.

domstolens åklagarmyndighet om att han påstods vara måltavla för spionprogrammet Predator den 21 september 2021. Efter Nikos Androulakis klagomål inledde ADAE en utredning i augusti 2022, som började med att information inhämtades från Androulakis telekomoperatör.

185. Spionprogrammet Predator lämnar knappt några spår av smitta hos telekomoperatörerna. ADAE upptäckte dock att Nikos Androulakis mobiltelefon övervakades av EYP[294] och att EYP:s interna åklagare Vasiliki Vlachou hade godkänt övervakningen och hävandet av sekretessen i september 2021, under samma tidsperiod som den påstådda Predator-attacken ägde rum.

186. Efter resultaten av ADAE:s undersökning avgick Grigoris Dimitriadis och Panagiotis Kontoleon från sina regeringsposter[295]. Panagiotis Kontoleon uppgav att övervakningen av Nikos Androulakis inleddes på begäran av utländska myndigheter – närmare bestämt Armeniens och Ukrainas underrättelsetjänster – med anledning av Nikos Androulakis deltagande i Europaparlamentets utskott för internationell handel, som arbetar med handelsförbindelser mellan EU och Kina[296]. Både Ukraina och Armenien har avfärdat dessa påståenden[297].

187. Den 15 december 2022 följde myndigheten upp förfrågningarna från journalisten Tasos Telloglou och Europaparlamentsledamoten Giorgos Kyrtsos om huruvida de varit måltavla för EYP. I en granskning som ADAE gjorde av telekomföretaget Cosmote visade det sig att både Tasos Telloglou och Giorgos Kyrtsos mycket riktigt stod under övervakning[298]. Cosmote informerade högsta domstolen om detta och ifrågasatte lagligheten i ADAE:s undersökning[299]. ADAE inrättade en särskild arbetsgrupp för att granska telekomoperatörerna och letade särskilt efter ytterligare begäranden från EYP om att häva sekretessen[300].

188. Regeringen har försökt ersätta ADAE:s styrelseledamöter. Greklands chefsåklagare Isidoros Dogiakos utfärdade dessutom ett officiellt yttrande den 10 januari 2023 enligt vilket ADAE inte får genomföra undersökningar av telekomoperatörers register för att söka efter begäranden om att häva sekretessen för kommunikation. Enligt yttrandet kan straffrättsliga påföljder vara tillämpliga om ADAE skulle inleda sådana granskningar[301]. Yttrandet, som går emot justitiekanslerns tidigare yttranden, strider uppenbart mot ADAE:s oberoende[302] och försöker hindra den från att utföra undersökningar. Under ett sammanträde i PEGA-kommittén den 28 februari 2023 uppgav Christos Rammos att Isidoros Dogiakos yttrande inte är bindande och att ADAE kan fortsätta som vanligt med sina arbetsuppgifter[303].

---

[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”.
[296] https://www.kathimerini.gr/politics/561988786/ypothesi-parakoloythiseon-ta-dedomena-poy-pyrodotisan-tis-exelixeis/.
[297] Kort sammanfattning, *Greece’s Predatorgate: The latest chapter in Europe’s spyware scandal?*, Europaparlamentet, Generaldirektoratet för parlamentarisk utredning och analys, den 8 september 2022.
[298] Euractiv, ”Exclusive: Another MEP and journalist the latest victims of ’Greek Watergate’”.
[299] Internationella pressinstitutet, ”Greece: MFRR alarmed by latest revelations of spying on journalists”.
[300] Euractiv, ”Exclusive: Another MEP and journalist the latest victims of ’Greek Watergate’”.
[301] Euractiv, ”Chief prosecutor puts Greece’s rule of law to the test”.
[302]http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/bdilosi-toy-proedroy-tis-adae-christoy-rammoy-gia-tin-g/.
[303] Diskussion i PEGA-kommittén med Konstantinos Menoudakos och Christos Rammos, den 28 februari 2023.

189. ADAE har bekräftat att EYP även har spionerat på den grekiska försvarsmaktens chef Konstantinos Floros, en sittande minister, flera officerare med ansvar för militär utrustning samt en före detta rådgivare om den nationella säkerheten. På grund av ADAE:s nuvarande oförmåga att informera personerna som är måltavlor planerade ADAE att presentera resultaten för det grekiska parlamentets transparensutskott och det grekiska parlamentets institutioner[304]. Christos Rammos skickade ett brev till det grekiska parlamentet och bad om denna presentation. Till en början undvek talmannen att ta upp frågan till diskussion genom att säga att han inte hade haft tid att läsa Christos Rammos brev på sin namnsdag. I slutändan avslog Ny Demokratis majoritet i utskottet om institutioner och transparens hans begäran. Den 24 januari 2023 angrep regeringens talesman ADAE och dess ordförande för dess utredningar[305] och hävdade att Christos Rammos bedrev ”aktivism” och ”översteg” sitt mandat, vilket inte bidrog till ADAE:s utredningar. Den 25 januari 2023 offentliggjorde Syrizas ledare, Alexis Tsipras, namnen på de som upptagits i rapporten vid det grekiska parlamentet, och det bekräftades att försvarsmaktens chef, den dåvarande överbefälhavaren för den grekiska armén, arbetsmarknadsministern, den före detta premiärministerns rådgivare om den nationella säkerheten samt två rådgivare från direktoratet för försvarets utrustning övervakades av EYP. Med tanke på allvaret i resultaten innebär avslaget på ADAE:s begäran om att rapportera till det grekiska parlamentet och misskrediteringen av myndigheten ett hindrande av ansvarsskyldighet och transparens[306].

190. Christos Rammos uppgav dessutom att ändringarna av ADAE:s rättsliga ram har skapat osäkerhet, vilket har lett till en skriftväxling med ministerierna för att klargöra myndighetens operativa ram för klagomål och utredningar. Christos Rammos nämnde att ADAE tar emot ungefär tio klagomål per dag[307].

UTSKOTTET FÖR INSTITUTIONER OCH TRANSPARENS

191. I juli 2022 kallade utskottet för institutioner och transparens Panagiotis Kontoleon och ordföranden för ADAE Christos Rammos till en parlamentsutfrågning. Under den här utfrågningen medgav Panagiotis Kontoleon tydligen att EYP hade spionerat på Thanasis Koukakis av skäl som rörde den nationella säkerheten, men uppgav att han inte kände till försöket till hackning av Nikos Androulakis anordning med Predator. Giannis Oikonomou – talesperson för regeringen – rapporterade att de grekiska myndigheterna varken har förvärvat eller använt spionprogrammet Predator[308].

192. Trots att mötena hölls inom stängda dörrar[309] vägrade tydligen både Panagiotis Kontoleon och Grigoris Dimitriadis att lägga fram några omfattande bevis, och hävdade skäl som rör nationell sekretess[310]. EYP:s nya chef, Themistocles Demiris, nekade

---

[304]https://www.protothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/.

[305] https://www.protothema.gr/politics/article/1332198/kuvernisi-paramagazo-tou-suriza-ekane-tin-adae-o-rammos-ola-sti-dikaiosuni-o-prothupourgos-den-gnorize-to-paramikro/AMP/, http://www.adae.gr/nomothetiko-plaisio/leptomereies/article/b-deltio-typoy-tis-adae-25012023-b/.

[306]Newsbomb, ”SYRIZA: Maximos circles’ through ADAE – What he sees behind the ’blockade’ of ND in Rammos”.

[307] Diskussion i PEGA-kommittén med Konstantinos Menoudakos och Christos Rammos, den 28 februari 2023.

[308] Reuters. ”Greek intelligence service admits spying on journalist - sources”.

[309] Ekathimerini, ”Transparency committee to hold closed-door meeting on phone hacking allegation”.

[310] Tovima, ”In combat positions for eavesdropping”.

utskottet åtkomst till en rapport med information om den påstådda förstörelsen av övervakningsuppgifter[311]. Detta innebär i praktiken att EYP vägrar ta på sig ansvaret och att det grekiska parlamentet inte kan utöva sitt mandat för parlamentarisk tillsyn.

193. Den 30 augusti 2022 kallade utskottet nio personer till förhör bakom stängda dörrar, däribland riksåklagaren Vasiliki Vlachou, före detta generalsekreteraren Grigoris Dimitriadis och före detta EYP-chefen Panagiotis Kontoleon. Samtliga åberopade sekretess och undvek att svara på några frågor under utskottets förhör[312].

PARLAMENTETS UNDERSÖKNINGSKOMMITTÉ

194. Ett förslag från partiet PASOK-KINAL om att inrätta en undersökningskommitté för den påstådda användningen av spionprogram[313] godkändes av 142 parlamentsledamöter från oppositionen, medan de 157 ledamöterna från Ny Demokrati lade ned sina röster[314]. ND hade dock en absolut majoritet i undersökningskommittén. Kraven på en byrå med stöd av båda partierna avvisades. ND fastställde arbetsprogrammet och listan över de vittnen som skulle bjudas in och avvisade flera av de vittnen som föreslogs av oppositionspartierna. Kommittén inrättades den 29 augusti 2022. Den inledde sitt arbete den 7 september 2022 och avslutade sitt arbete den 10 oktober 2022.

195. Regeringsmajoriteten i vägrade att bjuda in Felix Bitzios och Giannis Lavranos, men den bjöd in Stamatis Tribalis – nuvarande chef för Krikel – och Sara Hamou. Den 22 september vittnade Tribalis inför denna parlamentariska kommitté. Tribalis presenterade uppenbart falsk information om Felix Bitzios och Giannis Lavranos inblandning i Krikel, och påstod bland annat att han själv var ägare av Krikel[315].

196. Ett vittne, Sara Hamou från Intellexa, påstod sig inte kunna infinna sig personligen (trots att hon bor på Cypern), och hon tilläts att lämna in svar skriftligt. Inga gemensamma slutsatser kunde nås på grund av den allvarliga polariseringen av det politiska landskapet. En regeringsledd majoritet beslutade att hemligstämpla omkring 5 500 sidor dokument, inbegripet protokollet och Sara Hamous vittnesmål samt parternas huvudsakliga fynd, har hemligstämplats, även om det ligger helt inom parlamentets befogenheter att avlägsna denna hemligstämpel och ge tillgång till denna information. Därför utarbetades ingen offentlig sammanfattning. Endast slutdebatten i det grekiska parlamentets plenarförsamling var offentlig och fynden från både PASOK och Syriza offentliggjordes av partierna själva.

197. Oppositionen föreslog andra vittnen, bland andra Koukakis, Mitsotakis, Dimitriadis, Vlachou, Lavranos och Bitzios, men utskottet nekade till slut till att kalla dem. Den 10 oktober 2022 avslutade utskottet sina undersökningar och de olika politiska partierna lämnade in sina slutrapporter[316].

---

311 Tovima, ”In combat positions for eavesdropping”.
312 Ieidiseis, ”Syrizas och PASOK:s fynd gällande avlyssning: Både skandal och mörkläggning”, https://www.ieidiseis.gr/politiki/167144/ta-porismata-syriza-pasok-gia-tis-ypoklopes-kai-skandalo-kai-sygkalypsi.
313 Tovina. Ingripanden: Undersökningskommitté ska övervaka Androulakis – Pasoks förslag i detalj.
314 Tovina. *Parlamentet: 2016 års undersökning av övervakning antogs – med 142 röster för.*
315 TVXS. *G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament*.
316 Ieidiseis. *SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up*.

DEN GREKISKA DATASKYDDSMYNDIGHETEN

198. Den grekiska dataskyddsmyndigheten är en oberoende myndighet och har i uppgift att övervaka tillämpningen av den allmänna dataskyddsförordningen[317], andra förordningar och nationella lagar som gäller skydd av personuppgifter i Grekland[318]. Genom lag 4624/2019 exkluderas den nationella säkerheten från den grekiska dataskyddsmyndighetens ansvarsområde, trots att den ingått sedan lagen från 1997[319]. Efter Nikos Androulakis klagomål i juli 2022 inledde myndigheten i juli 2022 en undersökning om installationen av spionprogram på mobiltelefoner och den insamling och behandling av personuppgifter som följde därpå. Myndigheten utförde en granskning på Intellexas kontor i Chalandri samt på en av Intellexas anläggningar i Elliniko. Intellexa underlät dock att lämna viktiga uppgifter och besvarade frågeformulären efter betydande försening och hindrade därmed myndighetens granskning[320].

199. Den 16 januari 2023 ålade den grekiska dataskyddsmyndigheten Intellexa S.A. Böer om 50 000[321] böter för deras obstruerande och ovilja att samarbeta under granskningen på grundval av artikel 31 i den allmänna dataskyddsförordningen.

200. Efter den grekiska dataskyddsmyndighetens åtgärder har Intellexa överlämnat dokument, men myndigheten undersöker dem fortfarande. Enligt den grekiska dataskyddsmyndighetens ordförande, Konstantinos Menoudakos, upptäckte myndigheten domännamn som möjligen tillhör företag som samarbetar med Intellexa inom och utanför EU. Den grekiska dataskyddsmyndighetens undersökning pågår fortfarande[322].

201. Under ett sammanträde i PEGA-kommittén den 28 februari 2023 nämnde den grekiska dataskyddsmyndighetens ordförande att en myndighetsundersökning granskade internetapplikationer för att skicka textmeddelanden. Enligt Konstantinos Menoudakos har företag använt dessa internetapplikationer för att skicka textmeddelanden om spionprogrammet Predator. Myndigheten försöker för närvarande identifiera målen men har hittills bekräftat att 300 textmeddelanden har skickats till ungefär 100 mottagare med denna metod. Myndigheten har instruerat företagen att spara dessa uppgifter och har betonat att om dessa företag inte har någon rättslig företrädare i EU bryter de mot dataskyddsförordningen[323].

MÅLTAVLORNA

THANASIS KOUKAKIS

---

[317] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (EUT L 119, 4.5.2016, s. 1).
[318] Den grekiska dataskyddsmyndigheten. *Personal data*.
[319] Government Gazette of the Hellenic Republic.
[320] Den grekiska dataskyddsmyndigheten. Åläggande av böter för Intellexa S.A. för bristande samarbete med myndigheten.
[321] Den grekiska dataskyddsmyndigheten. Åläggande av böter för Intellexa S.A. för bristande samarbete med myndigheten.
[322] Diskussion i PEGA-kommittén med Konstantinos Menoudakos och Christos Rammos. 28.02.2023.
[323] Diskussion i PEGA-kommittén med Konstantinos Menoudakos och Christos Rammos. 28.02.2023.

202. Sommaren 2020 avlyssnades journalisten Thanasis Koukakis av EYP. På den tiden rapporterade han om ekonomiska ämnen, inbegripet skandalen med Piraeus/Libra, som involverade Felix Bitzios, och påstått skatteundandragande av den grekiska affärsmannen Giannis Lavranos, samt om kontroversiella banklagar som infördes av den grekiska regeringen i väntan på åtal i fall av penningtvätt och andra ekonomiska brott (den retroaktiva effekten ledde faktiskt till att tolv pågående fall avskrevs)[324]. Thanasis Koukakis utredde också upphandlingen för nya id-kort, där Giannis Lavranos och Felix Bitzios hade ett affärsintresse. Runt tiden för Thanasis Koukakis första inställelse vid PEGA drogs offerten plötsligt tillbaka och den ansvariga generalsekreteraren avgick.

203. Den 29 juli 2022 förklarade EYP:s chef Panagiotis Kontoleon att EYP hade övervakat Thanasis Koukakis telefon av skäl som rör ”den nationella säkerheten”.

204. Den 1 juni 2020 lämnade EYP in en första begäran om att häva sekretessen för Thanasis Koukakis telefonnummer i två månader, fram till den 1 augusti 2020. EYP lämnade in en begäran om förlängning med ytterligare två månader[325], dvs. fram till den 1 oktober 2020. Vasiliki Vlachou, åklagare vid appellationsdomstolen, godkände alla dessa begäranden av skäl som rör den nationella säkerheten[326].

205. Tolv dagar senare, den 12 augusti 2020, begärde dock EYP plötsligt att upphävandet av sekretessen för Thanasis Koukakis telefonnummer skulle avbrytas, dvs. en och en halv månad tidigare än vad som angavs i den ursprungliga begäran. Detta hände samma dag som Thanasis Koukakis vände sig till ADAE för att begära information om huruvida hans två mobiltelefoner och hans fasta telefon avlyssnades.

206. Den 10 mars 2021 rapporterade ADAE till EYP:s åklagare om möjligheten att meddela Thanasis Koukakis om övervakningen av hans mobiltelefon. Den 31 mars antog dock den grekiska regeringen ändring 826/145, som retroaktivt fråntog ADAE befogenheten att informera medborgare om hävandet av sekretessen för kommunikation[327]. ADAE:s ordförande Christos Rammos och två andra medlemmar av ADAE invände mot denna ändring och påpekade i en debattartikel att ändringen strider mot den rätt till respekt för privatliv och familjeliv som är inskriven i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna samt mot skyddet av sekretess för kommunikation enligt konstitutionen[328].

207. Mellan den 12 juli 2021 och den 14 september 2021 smittades Thanasis Koukakis telefon med spionprogrammet Predator[329]. Enligt Thanasis Koukakis fick han ett sms med en länk till en webbplats för ekonominyheter[330]. Den 28 mars 2022 avslöjade

---

[324] Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis*?.
[325] Reporters United. *Statens fiende: Vi bevisar att regeringen Mitsotakis övervakade journalisten Thanasis Koukakis*.
[326] Reporters United. *Statens fiende: Vi bevisar att regeringen Mitsotakis övervakade journalisten Thanasis Koukakis*; Inside Story. *Who was tracking journalist Thanasis Koukakis' cell phone?*.
[327] Reporters United. Enemy of the State: We prove that the Mitsotakis government was watching the journalist Thanasis Koukakis: https://www.reportersunited.gr/8646/eyp-koukakis/ Inside Story. Inside Story. *Who was tracking the mobile phone of journalist Thanasis Koukakis?*.
[328] Constitutionalism. Oförenlighet mellan artikel 87 i lag 4790/2021 med Europeiska domstolen för de mänskliga rättigheternas garantier för att skydda konfidentialitet vid kommunikation. 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?*.
[330] Europaparlamentet. Utfrågning den 8 september 2022.

Citizen Lab officiellt smittan[331].

208. Thanasis Koukakis gjorde flera försök att få upprättelse för övervakningsförsöken. Han lämnade in två klagomål till ADAE: Det första klagomålet inkom den 6 april 2022, och där begärde han en grundlig undersökning av att hans telefon smittats med Predator. Det andra inkom den 13 maj 2022, mot bakgrund av de nya avslöjanden som publicerades av InsideStory och Reporters United. Dessutom lämnade Thanasis Koukakis in ett klagomål till EAD den 4 maj 2022, där han begärde en utredning av bakgrunden till avlyssningarna av EYP och Predator-attacken[332].

209. Den undersökning som gjordes av den nationella transparensmyndigheten (EAD) den 21 juli 2022 av Intellexas (leverantören av spionprogrammet Predator) kontor i Aten var begränsad och ytlig, trots att viktig information om Predator-attackerna – ett brott – kunde ha hittats. Inga servrar, it-maskinvaror eller administrativa handlingar beslagtogs och säkrades. Verifieringen av den ekonomiska förvaltningen begränsades till år 2020[333]. Intellexas dotterbolag på Cypern och Irland undersöktes inte alls[334]. Utredningarna innehöll inga uppgifter om Intellexas och dotterbolagens bankkonton[335]. Thanasis Koukakis överklagade till Europeiska domstolen för de mänskliga rättigheterna den 27 juli 2022[336].

210. Den 5 oktober 2022 ingav Thanasis Koukakis ett klagomål till åklagare i Aten mot Intellexa Alliance, och särskilt Tal Dilian och Sara Hamou[337], för att ha brutit mot sekretessen för hans kommunikation[338].

NIKOS ANDROULAKIS

211. Den 21 september 2021 blev Nikos Androulakis, ledare för mitten-vänsterpartiet PASOK-KINAL och ledamot i Europaparlamentet, måltavla för spionprogrammet Predator när en skadlig länk skickades till hans telefon[339]. Nikos Androulakis fick ett sms med texten ”Let’s get a little serious, man, we’ve got a lot to gain”. Meddelandet innehöll även en länk för att installera spionprogrammet Predator på hans telefon, men till skillnad från Thanasis Koukakis klickade Nikos Androulakis inte på den länk som skickades till honom[340]. Under ett sammanträde i PEGA-kommittén den 28 februari 2023 uppgav Nikos Androulakis att den grekiska dataskyddsmyndigheten identifierade det kreditkortskonto som betalade för de textmeddelanden som skickades till honom. Denna information delades med den berörda åklagaren[341].

212. I juli 2021 tillkännagav Nikos Androulakis att han skulle kandidera till partiledarposten[342]. Enligt ADAE:s undersökning övervakades Nikos Androulakis

---

[331] Inside Story. *Who was tracking journalist Thanasis Koukakis’ cell phone?*.
[332] Avgi. *Thanasis Koukakis / Filed a lawsuit for the Predator – Who and why was watching him*.
[333] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[334] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[335] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[336] BBC. *”Greece wiretap and spyware claims circle around PM Mitsotakis”*.
[337] News 24 7. ”Wiretapping scandal: Lawsuit against Intellexa by Thanasis Koukakis”.
[338] Heinrich Boll Stiftung. *A State of Absolute Solitude*.
[339] InsideStory. *From Koukakis to Androulakis: A new twist in the Predator spyware case*.
[340] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader*.
[341] Diskussion i PEGA-kommittén med Konstantinos Menoudakos och Christos Rammos. 28.02.2023.
[342] Tovima. Androulakis lashes out at PM, ND spokesman says Pasok leader should say why his phone was tapped.

mobiltelefon vid den tidpunkten av EYP genom telekommunikationsleverantörerna[343]. EYP:s åklagare Vasiliki Vlachou godkände att sekretessen för Nikos Androulakis telefon hävdes på grund av ”nationell säkerhet”. Godkännandet sammanföll med både Predator-incidenten och Nikos Androulakis kandidatur.

213. När Nikos Androulakis valdes till partiledare i december 2021 avslutades den ”officiella” EYP-övervakningen plötsligt[344], trots det faktum att det två månader långa förnyade godkännandet av övervakningen av honom ännu inte hade löpt ut.

214. Den 28 juni 2022 kontrollerade Europaparlamentets GD ITEC Nikos Androulakis telefon och fann bevis för försöket till Predator-hackning i september 2021, och informerade Nikos Androulakis om detta[345]. Nikos Androulakis lämnade in till brottsanmälan till högsta domstolens åklagarmyndighet den 26 juli 2022[346].

215. Några dagar senare, den 29 juli, presenterade Nikos Androulakis informationen om Predator-attacken för ADAE. Samma dag hörde det permanenta utskottet om institutioner och transparens EYP:s chef Panagiotis Kontoleon och ADAE:s ordförande Christos Rammos, i närvaro av ministern för e-förvaltning och den biträdande ministern. Mötet ägde rum bakom stängda dörrar[347].

216. Den 8 september 2022 bad Nikos Androulakis ADAE att lämna över hans avlyssningsfiler[348]. Samma dag rapporterade dock Ta Nea om en officiell briefing som hölls av ADAE om att både Nikos Androulakis och Thanasis Koukakis filer hade förstörts av EYP[349]. Förstörelsen är ett otvetydigt faktum, men historien bakom den är fortfarande oklar. Å ena sidan skyller vissa källor förstörelsen av filerna på förändringen av EYP:s elektroniska system under 2021[350]. Denna ändring av det nya rättsliga insamlingssystemet påstods ha orsakat ett tekniskt problem som ledde till förstörelsen. Å andra sidan hävdar andra källor att Panagiotis Kontoleon utfärdade ett beslut om att filerna skulle förstöras den 29 juli 2022, dvs. samma dag som Nikos Androulakis informerade ADAE om övervakningsförsöken[351]. Under en utfrågning i PEGA-kommittén varken bekräftade eller förnekade ADAE:s ordförande, Christos Rammos, någon förstörelse av handlingar[352].

217. Den 5 augusti avgick Panagiotis Kontoleon och Grigoris Dimitriadis från sina positioner. Den 8 augusti gjorde Mitsotakis ett tv-uttalande där han erkände avlyssningen av Nikos Androulakis, men upprepade att han inte kände till övervakningen[353].

218. EYP har hittills vägrat att redogöra för skälen till övervakningen. Byrån har erbjudit sig att privat informera Nikos Androulakis om skälen. Det skulle vara olagligt. Nikos

---

[343] Kathimerini. *Övervakningsfallet: uppgifterna som utlöste skeendena*.
[344] Euractiv. *EU Commission alarmed by new spyware case against Greek socialist leader.*
[345] Euractiv. EU Commission alarmed by new spyware case against Greek socialist leader.
[346] News 247. Nikos Androulakis: Near-Victim of Predator Software - Filed a Lawsuit.
[347] Avgi. *Predator-skandalen/EYP tvingat infinna sig vid parlamentet på grund av övervakning*.
[348] Ekathimerini. Androulakis asks ADAE for his wiretapping file.
[349] TaNea*. The archive of the surveillance of Nikos Androulakis destroyed.*
[350] TVXS. *G. Lavranos behind KRIKEL - How attempts were made to deceive the Parliament.*
[351] Ieidiseis. *SYRIZA-PASOK findings on wiretapping: Both scandal and cover-up.*
[352] Europaparlamentet. Utfrågning den 8 september 2022.
[353] Reuters*. Greek PM says he was unaware of phone tapping of opposition party leader.*

Androulakis bad om att hans övervakningsfil skulle lämnas in till utskottet för institutioner och transparens, men det avslogs.

219. Den 7 december 2022 lämnade Nikos Androulakis in ett klagomål till Europeiska domstolen för de mänskliga rättigheterna om EYP:s avlyssning av honom och bristen på officiell information om hans fall[354].

220. Övervakning av en politiker är mycket ovanlig, och den grekiska konstitutionen föreskriver särskilt skydd för politiker. EYP förnekar all inblandning i övervakningen med Predator. Regeringen lade inledningsvis fram förslag om utländsk makt som påstods ha begärt avlysning av Nikos Androulakis, eller så föreslog de att skälet skulle kunna vara att han var ledamot i ett parlamentsutskott med ansvar för förbindelserna med Kina. Ingen av dessa hypoteser var särskilt trovärdig. Övervakningen ägde rum i en politisk kontext med kommande val. PASOK skulle vara den koalitionspartner som föredrogs. Hösten 2021 fanns det fyra kandidater i kampen om ledarskapet för PASOK, var och en med olika åsikter om en sådan koalition. Nikos Androulakis påstods vara öppen för tanken, men inte med Mitsotakis som premiärminister. En annan kandidat, Andreas Loverdos, hade tidigare arbetat som minister i koalitionen Ny Demokrati-PASOK, och man trodde att han skulle erbjuda ett större stöd. Han var bekant med Grigoris Dimitriadis. Offentliggörandet av förteckningen över andra påstådda måltavlor av Documento förstärker misstanken om politiska orsaker till övervakningen. Det finns inga bevis för några av dessa hypoteser, men det är nödvändigt att dessa avenyer utreds och elimineras när så är möjligt.

GIORGOS KYRTSOS

221. Den 15 december 2022 bekräftade en ADAE-granskning av telekommunikationsföretaget Cosmote att ledamoten av Europaparlamentet, Giorgos Kyrtsos, övervakades av EYP[355]. Både hans mobiltelefoner och hans fasta telefon var avlyssnade. Övervakningen förlängdes enligt uppgift nio gånger[356] för en period om 18 månader.

222. Giorgios Kyrtsos är en före detta medlem i Ny Demokrati och Europeiska folkpartiet. I februari 2022 uteslöt ND Giorgios Kyrtsos från det grekiska styrande partiet på grund av att han ogillade regeringens åtgärder i samband med covid-19-pandemin, inskränkningar av mediefriheten och strategin när det gäller Novartis-skandalen[357]. Efter uteslutningen anslöt sig Giorgios Kyrtsos till Renew Europe.

STAVROS MALICHOUDIS

223. Den 13 november 2021 avslöjade tidningen EFSYN att flera journalister som rapporterade om flyktingärenden påstods vara avlyssnade av EYP. Ett internt dokument från EYP visade att EYP beordrade övervakning och insamling av uppgifter om den grekiska journalisten Stavros Malichoudis[358][359]. Stavros Malichoudis skrev om en syrisk

[354] Ekathimerini. *Socialist leader appeals to European Court over tapping.*
[355] Euractiv. *Another MEP and journalist the latest victims of 'Greek Watergate'.*
[356] Politico. *Greek prosecutor slams unflattering comparisons to Belgium's Qatargate probe.*
[357] Euractiv. *Renew Europe welcomes first Greek MEP who left EPP.*
[358] Efsyn. *Πολίτες σε καθεστώς παρακολούθησης από την ΕΥΠ.*
[359] Solomon. *Solomon's reporter Stavros Malichudis under surveillance for 'national security reasons'.*

tolvåring som tvingades leva i flera månader i ett fängläger på den grekiska ön Kos[360].

224. Den 15 november 2021 bekräftade regeringens talesman Giannis Oikonomou indirekt påståendena. Han uppgav att EYP kunde avlyssna enskilda personer om det finns en risk för den nationella säkerheten till följd av ”interna eller externa hot”[361]. Den 24 november och den 17 december 2021 förnekade dock den biträdande ministern George Gerapetritis all övervakning av journalister i Grekland, inbegripet den av Stavros Malouchidis, men enligt nyhetsmediet Solomon varken bekräftade eller förnekade han att EYP:s interna dokument var äkta[362].

225. Under PEGA:s utfrågning om Grekland den 8 september 2022 uppgav Stavros Malichoudis att EYP genom att avlyssna hans telefon också kunde samla in information från kolleger och journalister som han hade kontakt med under den tiden[363]. EYP kunde enligt uppgift ha lyssnat på de samtal som Stavros Malichoudis hade haft med Internationella organisationen för migration (IOM)[364], vilket belyser riskerna för andra med de så kallade ”bifångsterna” från avlyssning av en enskild person. Under utfrågningen uppvisade Stavros Malichoudis dessutom bevis för att EYP var intresserat av hans arbete och källor, men att skälet till övervakningen omfattas av ”nationell säkerhet”[365].

CHRISTOS SPIRTZIS

226. Den 9 september 2022 påstod den f.d. ministern för infrastruktur och lagstiftaren för partiet Syriza, Christos Spirtzis, att han varit måltavla för spionprogrammet Predator på sin mobiltelefon[366]. Spirtzis lämnade den 15 november 2021 in kritiska parlamentsfrågor till regeringen om EYP:s övervakningsuppgifter. Samma dag fick han ett liknande meddelande[367] som det som Nikos Androulakis fick. Den 19 november sändes ett andra meddelande till Christos Spirtzis, med en länk till en artikel i Efimerida ton Syntakton[368]. Även om CitizenLab inte kontrollerade dessa meddelanden delade Christos Spirtzis de länkar han mottagit med två tekniker som verbalt bekräftade att han hade blivit utsedd till måltavla[369]. Den 9 september 2022 lämnade Christos Spirtzis in ett klagomål till åklagaren vid högsta domstolen[370]. Christos Spirtzis är nära vän med partiledaren Alexis Tsipras, och deltar vid högnivåmöten i partiledningen.

TASOS TELLOGLOU, ELIZA TRIANTAFYLLOU OCH THODORIS CHONDROGIANNOS

227. Journalisterna Tasos Telloglou och Eliza Triantafylou påstos ha utsatts för spionage under deras undersökande arbete för nyhetsmediet Inside Story. I en artikel för Heinrich-Böll-Stiftung den 24 oktober 2022 delade Tasos Telloglou med sig av sina

[360] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*
[361] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*
[362] Solomon, *Solomon's* reporter *Malichudos* under surveillance for national security reasons.
[363] Europaparlamentet. Utfrågning den 8 september 2022.
[364] BalkanInsight. *Greek Intelligence Service Accused of 'Alarming' Surveillance Activity.*
[365] Europaparlamentet. Utfrågning den 8 september 2022.
[366] Ekathimerini. Former SYRIZA minister says he was targeted by Predator.
[367] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware.*
[368] Govwatch, *Attempted hack of opposition MP Christos Spirtzis with illegal Predator spyware.*
[369] Inside story, *Predator: Fler än 20 måltavlor i Grekland enligt dataskyddsmyndigheten.*
[370] Reuters. *One more Greek lawmaker files complaint over attempted phone hacking. Euractiv. Another Greek opposition lawmaker victim of Predator.*

upplevelser av att bli övervakad och skrämd medan han undersökte övervakningsskandalerna i Grekland. Enligt dessa upplevelser tror han att han övervakades mellan maj och augusti 2022[371].

228. Dessutom hade en källa från säkerhetstjänsten informerat Tasos Telloglou i juni 2022 om att både han och hans kolleger Eliza Triantafyllou (InsideStory) och Thodoris Chondrogiannos (Reporters United) övervakades av myndigheterna för att bedöma vilka källor de träffade[372]. I skrivande stund har den grekiska regeringen ännu inte svarat på anklagelserna.

229. Den 15 december 2022 bekräftade en ADAE-granskning av telekommunikationsföretaget Cosmote att Tasos Telloglou övervakades av EYP. På grund av ”den nationella säkerheten” avslöjades inte skälen till övervakningen[373].

ANDRA MÅLTAVLOR

230. Den 29 oktober 2022 rapporterades att andra politiker hade utsatts för spionprogrammet Predator, däribland en regeringsminister som inte kom överens med premiärministern. Dessutom rapporterades det att en annan medlem i Ny Demokrati fick en länk för att installera Predator[374]. En talesperson för regeringen, Giannis Oikonomou, har uppgett att artikeln saknar konkreta bevis[375].

231. Den 5 och 6 november 2022 rapporterade Documento om en förteckning med 33 namn på personer som hade varit måltavlor för spionprogrammet Predator[376]. Förteckningen innehöll många högprofilerade politiker, däribland aktuella regeringsledamöter, f.d. premiärminister Samaras, f.d. EU-kommissionär Avramopoulos, chefredaktören på en nationell regeringsvänlig tidning och personer i kretsen kring Vangelis Marinakis, fartygsägare, mediemogul och ägare av fotbollsklubbarna Olympiakos och Nottingham Forest. ADAE bekräftade att vissa namn på förteckningen övervakades av EYP genom traditionell avlyssning. Bland dessa namn finns parlamentsledamoten Giorgos Kyrtsos[377], stabschefen general Konstantinos Floros[378], den grekiska överbefälhavaren Haralambos Lalousis[379], ministern för arbetsmarknadsfrågor och sociala frågor Kostis Hatzidakis[380], de före detta generaldirektörerna för försvarsmateriel och investeringar Theodoros Lagios och Aristides Alexopoulos[381], den före detta säkerhetsrådgivaren Alexandros Diakopoulos[382] och den grekiska undersökande journalisten Tasos

---

371 Heinrich-Böll-Stiftung. *A State of Absolute Solitude*.
372 MapMF, *Three Greek journalists allegedly surveilled and monitored in connection with spyware scandal investigations.*
373 Euractiv, Another MEP and journalist the latest victims of ‘Greek Watergate’.
374 Ta Nea, *Fyra olagliga manipulationer av misstänkt center.*
375 Politico, *Brussels Playbook: Lula wins in Brazil - Trick or trade - Grain deal woes.*
376 Documento, den 6 november 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/.*

Telloglou[383].

232. Dessutom fanns Metas tidigare policychef för cybersäkerhet, Artemis Seaford, med på förteckningen över 33 namn och bekräftades samtidigt vara avlyssnad av EYP och spionerad på med hjälp av Predator. Seaford avlyssnades av EYP från juli 2021 till sommaren 2022, vilket innebär att tillståndet för avlyssning av Seafords enhet förnyades sex gånger, vilket i princip kräver godkännande från EYP:s interna åklagare, Vasiliki Vlachou. CitizenLab bekräftade att hennes mobiltelefon också var smittad med Predator i minst två månader per september 2021. Predator-smittan inträffade således ungefär en till två månader efter det att den traditionella avlyssningen påbörjades. Artemis Seaford uppgav att information om hennes inbokade tid för vaccinering mot covid-19 erhölls från hennes textmeddelanden via traditionell avlyssning. Denna information användes därefter för att skapa ett sofistikerat automatiserat sms, med samma utseende som den officiella tidsbokningen, och med en begäran om att hon skulle bekräfta tidsbokningen via en länk. Genom att klicka på den här länken smittades hennes telefon med spionprogrammet Predator. Sms-meddelandena innehöll korrekt och detaljerad information om hennes vaccinationsärende, och det sändes bara minuter efter de verkliga, officiella meddelandena, vilket visade att den som sände meddelandena hade tillgång till innehållet i och tidpunkten för sms-meddelandena, vilket EYP skulle ha fått genom den traditionella avlyssningen.

233. Avlyssning och/eller övervakning av en privatperson är ovanligt, särskilt när den nationella säkerheten inte kan åberopas på ett legitimt sätt i ett sådant fall. Detta väcker frågan om vilka andra motiv som kunde ha spelat en roll vid utseende av måltavla. Övervakningen ägde rum medan Artemis Seaford arbetade på Meta, ett företag som har publicerat en hotbildsrapport om industrin för uthyrning av övervakning och har bannat flera spionprogramföretag, inklusive Cytrox, från sin plattform. Det är dock högst osannolikt att hennes roll vid Meta var anledningen till övervakningen. Metas hotbildsrapporten offentliggjordes först i december 2021, några månader senare än den tidpunkt då Artemis Seafords telefon utsågs till måltavla, och ingen av de andra personer som var inblandade i rapportskrivningen blev utsedda till måltavlor. Artemis Seaford uppgav[384] dessutom att hon endast delvis deltog i denna verksamhet och att Meta är mycket diskreta när det gäller att offentliggöra namnen på sina anställda.

234. I mars 2021 publicerade tidskriften Marie-Claire en artikel som innehöll ett utdrag ur en bokserie som hade skrivits av Artemis Seaford. I artikeln nämns Artemis Seafords erfarenheter av daglig sexism och dagliga trakasserier i Grekland, och i den beskrivs särskilt ett fall av sexuella trakasserier av ”en politiker”[385]. Övervakningen började några månader senare. En förklaring kan vara att den berörda politikern läste artikeln och fruktade att hans namn skulle offentliggöras. En annan förklaring kan vara att någon annan kände igen politikern från beskrivningen i artikeln och ville samla in mer information om den personen av politiska skäl. I vilket fall som helst skulle endast ett fåtal personer ha befogenhet att både lämna in en officiell begäran om avlyssning till EYP och göra arrangemang för användning av spionprogrammet Predator. Kombinationen av övervakning av EYP och genom spionprogrammet Predator har

[383] *https://www.euractiv.com/section/politics/news/exclusive-another-mep-and-journalist-the-latest-victims-of-greek-watergate/*.
[384] Sammanträde i PEGA kommittén, den 20 april 2023.
[385] https://www.marieclaire.gr/art-lifestyle/artemis-seaford-i-chiroteri-morfi-katapiesis-ine-afti-pou-den-katalavenis-oti-ifistase/.

också bekräftats i andra fall.

235. Det är viktigt att dessa möjligheter undersöks ytterligare, särskilt frågan om vem som begärde övervakning av EYP. Artemis Seaford har lämnat in en förfrågan till ADAE och har lämnat in ett klagomål till domstolen i Grekland. Undersökningen pågår dock fortfarande. Hon är den första amerikanska medborgare som man vet har blivit måltavla i EU[386][387].

236. Andra namn på förteckningen som inte officiellt bekräftats är den före detta ministern för utbildning och religiösa frågor Andreas Loverdos, den före detta premiärministern Antonis Samaras, statsminister George Gerapetritis, den före detta kommissionsledamoten Dimitris Avramopoulos, minister Nikos Dendias, utbildningsminister Niki Kerameus, minister Akis Skertsos, investeringsminister Nikos Papathanasis, den före detta ministern för medborgarskydd Mihalis Chrysochoidis, Greklands vice försvarsminister Nikos Hardalias, Aristotelia Peloni, parlamentsledamot Christos Spirtzis, den före detta ministern för medborgarskydd Olga Gerovasili, den grekiska polischefen Michalis Karamalakis, ekonomiska åklagarmyndighetens chef Christos Barkadis, EYP:s interna åklagare Eleni Vlachou, regeringens talesperson Oikonomou, EYP:s ställföreträdande chef Vassilis Grizis. Avslöjandena på förteckningen är mycket stötande inte bara på grund av de högprofilerade namnen på den, utan också för att missbruket av spionprogram är systematiskt och storskaligt.

237. 2023 rapporterade ADAE att EYP även har avlyssnat en sittande minister, flera officerare med ansvar för militär utrustning och en före detta nationell säkerhetsrådgivare[388].

AVSLUTANDE KOMMENTARER

238. Det finns mönster som tyder på att regeringen möjliggör användning av spionprogram mot journalister, politiker och företagare. Den tillåter även export av spionprogram till länder som inte värnar de mänskliga rättigheterna samt tillhandahåller ett utbildningscentrum till aktörer från tredjeländer som vill lära sig om spionprogram. Trots att det är olagligt i Grekland att använda spionprogram tog utredningen av ursprunget till spionprogramattackerna fart först under sommaren 2022. En politisk majoritet används enligt uppgift för att främja särintressen snarare än allmänintresset, särskilt genom att man utser bundsförvanter och lojalister till nyckelbefattningar som t.ex. EYP, EAD (den nationella transparensmyndigheten) och Krikel (ett företag som specialiserar sig på elektroniska säkerhetssystem). Landets högsta politiska ledare använder spionprogram som ett verktyg för politisk makt och politisk kontroll, i vissa fall parallellt med eller efter laglig avlyssning. Grekland har i princip en tämligen robust rättslig ram. Lagändringar har dock försvagat viktiga skyddsåtgärder och politiska utnämningar till nyckelpositioner utgör ett hinder mot granskning och ansvarsskyldighet. Mekanismer för förhands- och efterhandsgranskning har avsiktligt försvagats och insyn och ansvarsskyldighet undviks. Kritiska journalister eller tjänstemän som bekämpar korruption och bedrägerier utsätts för hot och hinder.

---

[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] Sammanträde i PEGA kommittén, den 20 april 2023.

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

Systemet med skyddsåtgärder mot och tillsyn över övervakning är på det hela taget otillräckligt för att skydda medborgarna mot statliga organs och privata aktörers missbruk. Det behöver göras mer för att ta itu med detta problem. Dessutom åberopas förevändningen om ”nationell säkerhet” som motivering för att avlyssna människor.

239. Politiskt motiverat spionerі är inget nytt för Grekland, men den nya spionprogramstekniken gör den olagliga övervakningen mycket enklare, särskilt när skyddsåtgärderna kraftigt försvagats. Till skillnad från andra fall, t.ex. Polen, verkar missbruk av spionprogram inte vara en del av en integrerad auktoritär strategi, utan snarare ett verktyg som används i särskilda fall för politisk och finansiell vinning. Det urholkar dock demokratin och rättsstatsprincipen lika mycket och ger stort utrymme för korruption, när dessa oroliga tider kräver ett pålitligt och ansvarstagande ledarskap.

I.D. Cypern

240. Kommittén besökte Cypern i november 2022 som del av ett gemensamt uppdrag i Grekland och Cypern. Ledamöterna träffade energi-, handels- och industriministern, andra regeringstjänstemän och representanthusledamöter som sitter i relevanta utskott för att diskutera den nuvarande rättsliga ramen för spionprogram. De hörde också juridiska experter, företrädare för icke-statliga organisationer och journalister som framställde dokumentation om övervakning och korruption till kommittén. Kommittén betonade att mer bör göras när det gäller register över verkligt huvudmannaskap, där insyn saknas trots att de utformades för att belysa sådana frågor.

241. Till skillnad från andra medlemsstater finns det inte mycket information om Cyperns användning av spionprogram. Det finns inga officiellt bekräftade fall av personer som olagligen utsätts eller har utsatts för spionprogram. Journalisten Makarios Drousiotis övervakades dock enligt utsaga med hjälp av både avlyssningsteknik och spionprogram av den cypriotiska regeringen i februari 2018[389]. På papperet finns det en robust rättslig ram, inbegripet EU-regler, men i praktiken är Cypern en attraktiv plats för företag som säljer övervakningsteknik. Regeringen förnekar dock detta och pekar på en minskning av registrerade spionprogramföretag i landet. Skandaler på senare år har dock skadat landets rykte och en uppsättning nya lagstiftningsinitiativ som skärper den rättsliga ramen för export och förbättrar efterlevnaden förväntas slutföras 2023.

242. Det finns nära förbindelser mellan Cypern och Grekland när det gäller spionprogram. Tal Dilians Intellexa är etablerat i Grekland och hans spionprogram Predator har använts i de grekiska hackningsskandalerna. Båda länderna var också inblandade i olaglig export av spionprogrammet Predator till sudanesiska Rapid Support Forces (RSF)[390]. Grekland utfärdade en exportlicens, medan materialet skickades till Sudan från Larnacas flygplats[391].

243. Utöver export av spionprogram utanför EU underlättar Cypern också handeln med undersystem och spionprogramsteknik till medlemsstaterna. Namnet UTX Technologies – registrerat på Cypern och förvärvat av den israeliska teknikjätten Verint – har upptäckts på fakturor från tyska, franska och polska företag för transport av Gi2-teknik

[389] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/.
[390] LightHouse Reports. Flight of the Predator.
[391] https://www.euractiv.com/section/politics/news/greek-government-admits-exporting-predator-to-sudan/.

och övervakningssystem[392].

244. På papperet finns det en rättslig ram som föreskriver skydd av privat kommunikation, behandling av personuppgifter och den enskildas rätt till information. I praktiken finns det emellertid, när det gäller den nationella säkerheten, inga tydliga regler som reglerar användning av uppfångningsanordningar och skydd av medborgarnas konstitutionella rättigheter.

RÄTTSLIG RAM

FÖRORDNINGEN OM PRODUKTER MED DUBBLA ANVÄNDNINGSOMRÅDEN

245. Cypern verkar ha ett mycket nära samarbete med Israel på området för övervakningsteknik. Cypern konsulterade Israel och USA om reformen av sin rättsliga ram och systemet för kontroll av export av produkter med dubbla användningsområden. Cypern är en populär destination för många israeliska spionprogramföretag.

246. Avdelningen för exportlicenser för strategiska produkter vid ministeriet för energi, handel och industri reglerar export av produkter med dubbla användningsområden[393]. Som svar på PEGA-frågeformuläret som skickades till alla medlemsstater uppgav Cypern att man övervakar och bedömer alla ansökningar om exportlicenser för varor med dubbla användningsområden från fall till fall, i full överensstämmelse med relevanta sanktionssystem. Dessa system består av Europeiska unionens globala system för sanktioner avseende mänskliga rättigheter samt EU:s förordning om produkter med dubbla användningsområden, styrt av kriterierna i rådets relevanta gemensamma ståndpunkt (2008/944/Gusp)[394]. PEGA-kommittén konstaterar att Cypern inte deltar i Wassenaar-arrangemanget om exportkontroller av konventionella vapen samt varor och teknik med dubbla användningsområden. Under PEGA-kommitténs uppdrag uppgavs det att Turkiet blockerade Cyperns deltagande i detta arrangemang. Regeringen förklarar dock att den följer samma normer.

247. Ministeriet för energi, handel och industri kan samråda med den så kallade rådgivande kommittén om beviljande av exportlicenser. Denna kommitté består av företrädare för försvarsministeriet, ministeriet för rättsväsendet och den allmänna ordningen, utrikesministeriet, bland annat tull- och punktskattedepartementet[395]. Enligt den cypriotiska regeringen hörs denna kommitté regelbundet när exportansökningar granskas. Vid flera tillfällen har export av varor med dubbla användningsområden till tredjeländer nekats till följd av ett negativt yttrande från denna kommitté[396]. Handelskammaren tillhandahåller vanligtvis ingen information om antalet godkända och avvisade licenser för saluföring av programvara[397].

248. Under PEGA-kommitténs uppdrag i Cypern den 1–2 november 2022 hade deltagarna i uppdraget ett möte med ministeriet för energi, handel och industri och biträdande ministern för forskning, innovation och digital politik. Ministrarna Natasa Pilides och Kyriacos Kokkinos uppgav att antalet företag som är verksamma inom spionprogram på

[392] Philenews. Cyprus is a pioneer in software exports (documents).
[393] http://www.meci.gov.cy/meci/trade/ts.nsf/ts08_en/ts08_en?OpenDocument.
[394] Svar från Cypern på Europaparlamentets frågeformulär.
[395] Lelaw, 'Export Controls for dual-use products'.
[396] Svar från Cypern på Europaparlamentets frågeformulär.
[397] Inside Story, 'Who signs the exports of spyware from Greece and Cyprus?'.

Cypern har minskat kraftigt. 32 företag är registrerade, men enligt ministern är för närvarande endast 8–10 verksamma, varav 3–4 tillverkar spionprogram[398]. De tillstod dock också tekniska utmaningar med att övervaka och kontrollera företag med säte i Cypern som oberoende säljer enskilda delar av spionprogram.

249. I praktiken rapporteras Cypern vara ganska frikostigt med att bevilja spionprogramföretag exportlicenser[399]. Företag använder olika tekniker för att kringgå reglerna. Produktens fysiska hårdvara kan skickas till ett mottagarland utan att programvaran är installerad på den[400]. Därefter skickas aktiveringsprogrammet (även kallat ”licensnyckeln”) separat på ett usb-minne till destinationslandet[401]. Ett annat sätt är att uppge att produkten endast exporteras i demonstrationssyfte, även om en detaljerad beskrivning av produkten ingår[402]. Dessutom anges oklara beskrivningar av spionprogrammen i exportformuläret för exportlicenser, vilket har hindrat lämpliga tullkontroller.

250. Flera cypriotiska företag har enligt uppgift erhållit exportlicenser för försäljning av produkter med dubbla användningsområden till länder utanför EU. Dessa företag är UTX Technologies, Coralco Tech, Prelysis och Passitora[403].

251. UTX Technologies har deltagit i försäljningen av spionprogram till EU:s medlemsstater och till länder utanför EU. Mellan 2013 och 2014 har UTX nämnts på fakturor till tyska (Syborg Informationsysteme), franska (COFREXPORT) och polska (Verint) företag för handel med övervakningssystem och Gi2-teknik[404].

252. Det cypriotiska handelsorganet har tillhandahållit tillfälliga exportlicenser till Cognytes dotterbolag UTX Technologies för försäljning av övervakningsprogramvara till Mexiko, Förenade Arabemiraten, Nigeria, Israel, Peru, Colombia, Brasilien och Sydkorea[405]. UTX Technologies uppges också ha ingått ett avtal med Thailand om försäljning av övervakningsdelsystem för 3 miljoner dollar. Beskrivningen av dessa undersystem hänvisade till en typ av ”produkter med dubbla användningsområden” med ”talanalysalgoritm” och ”metadata och röst”. Avtalet innehöll också en särskild hänvisning till ett litauiskt företag. Eftersom de cypriotiska myndigheterna inte skulle utfärda exportlicensen kunde ministeriet för energi, handel och industri kringgås genom det Litauen-registrerade UAB Communication Technologies[406]. Den rysk-israeliska medborgaren Anatoly Hurgin äger detta företag och innehar dessutom ett maltesiskt pass[407]. Dessutom säkerställde UTX också ett avtal med Bangladesh om ett webbaserat underrättelsesystem för 2 miljoner dollar 2019 och ett mobilt spårningssystem för 500 000 dollar 2021[408].

---

[398] Möte med Natasa Pilides, minister för energi, handel och industri samt Kyriacos Kokkinos, biträdande minister för forskning, innovation och digital politik under PEGA:s uppdrag den 2 februari 2022.
[399] InsideStory, ‘Who signs the exports of spyware from Greece and Cyprus?’.
[400] InsideStory, ‘Who signs the exports of spyware from Greece and Cyprus?’.
[401] Philenews, ‘This is how interception patents are exported from Cyprus’.
[402] Philenews, ‘Export of monitoring software confirmed’.
[403] Philenews, ‘Cyprus is a pioneer in software exports (documents)’; Haaretz, ‘Israeli Spy Tech Sold to Bangladesh, despite Dismal Human Rights Record’.
[404] Philenews, ‘Cyprus is a pioneer in software exports (documents)’.
[405] Philenews, ‘Cyprus is a pioneer in software exports (documents)’.
[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’.

253. Cyperns exporthistoria visar också att Coralco Tech – ursprungligen från Singapore men även registrerat i Israel och Nicosia – skickade övervakningsutrustning för 1,6 miljoner dollar till den bangladeshiska militären efter ett anbudsförfarande 2018. Ägaren till Coralco Tech är den israeliska Eyal Almog[409].

254. År 2019 köpte Bangladeshs interna underrättelsetjänst (NSI) en wifi-avlyssningsprogramvara från Prelysis (registrerat i Cypern) för totalt 3 miljoner dollar. Kobi Naveh – Prelysis grundare och direktör – arbetade för det israeliska företaget Verint fram till 2014. Verint är också det företag som förvärvade det Cypern-registrerade företaget UTX Technologies[410].

255. Under sommaren 2021 köpte Bangladesh dessutom ett spionfordon från Tal Dilians företag Passitora (tidigare WiSpear). Det schweiziska företaget Toru Group Limited, som är registrerat på Brittiska Jungfruöarna, fungerade som mellanhand för de avtal som ingåtts med Dilians Passitora[411].

256. Den 4 oktober 2022 avslöjades det att det nederländska försvarsministeriet i november 2019 var på att underteckna ett avtal med WiSpear, det företag som ägs av Tal Dilian, som tidigare hade förvärvat Cytrox, tillverkaren av spionprogram från Predator[412]. Enligt mediarapporter och uttalanden från ordföranden för Demokratisk samling (Dimokratikós Sinagermós) skickade WiSpearett e-postmeddelande till regeringspartiet Demokratisk samling och ministern för energi, handel och industri för att begära bistånd med att genomföra avtalet med det nederländska försvarsministeriet[413]. Det är oklart om kontraktet undertecknades och spionprogram levererades till det nederländska försvarsministeriet.

257. Dessa exempel visar att det finns en hel del verksamhet inom övervakningsbranschen i Cypern, som involverar samma aktörer som de som framträder i den spionprogramskandal som undersöks av PEGA.

258. Många israeliska företag kommer till Cypern för att påbörja sin europeiska verksamhet[414]. Olika källor rapporterade vidare att landet är hem till cirka 29 israeliska företag[415]. Vissa källor pekar på ett nära samband mellan handeln med programvara och diplomatiska förbindelser. I utbyte mot underlättandet av licenser för israeliska företag påstås Cypern ha fått några av de produkter som dessa företag utvecklar och exporterar, exempelvis spionprogrammet Pegasus från NSO[416] samt spionprogrammaterial från WiSpear[417]. Cypern som fotfäste i handeln med israeliska spionprogram på EU:s inre marknad och i exporten av spionprogram till länder utanför EU.

FÖRHANDSGRANSKNING

259. I lagen om skydd av sekretess för privat kommunikation 92(I)/1996 föreskrivs att

[409] Haaretz, ‘Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record’.
[410] Haaretz, ‘Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record’.
[411] Haaretz, ‘Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Record’.
[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.
[415] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022.
[416] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022.
[417] Inside Story, ‘Predator: the ‘spy’ who came from Cyprus’.

justitiekanslern får lämna in en ansökan till domstolen om utfärdande av ett domstolsbeslut som tillåter eller förlänger avlyssning av privat kommunikation genom en behörig person. Denna ansökan från justitiekanslern till domstolen kräver en skriftlig begäran av polischefen, chefen för Cyperns underrättelsetjänst eller en undersökningsdomare. Bestämmelser om tillstånd eller godkännande kan dock upphävas i fall där avlyssning av privat kommunikation ligger i Cyperns säkerhetsintresse eller för att förhindra, utreda eller lagföra brott[418].

260. Efter ansökan ger polischefen – i samförstånd med den biträdande polischefen och chefen för Cyperns underrättelsetjänst – ett skriftligt tillstånd till anställda i deras tjänst, eller anställda som utför uppdrag för deras tjänst, att avlyssna privat kommunikation och/eller få tillgång till övervakningsutrustning i syfte att utföra tekniskt arbete[419].

261. Dessutom anges i artikel 4.2 i lag 92 (I)/1996, i dess ändrade lydelse från 2020[420], att ingen får importera, tillverka, marknadsföra, sälja eller på annat sätt distribuera sådana produkter eller maskiner som i första hand har konstruerats, producerats, anpassats eller tillverkats för att möjliggöra eller underlätta avlyssning eller övervakning av privat kommunikation. Överträdelse av denna artikel kan leda till böter på 50 000 euro och/eller upp till fem års fängelse[421]. Dessa bestämmelser gäller inte om leverantören har informerat den centrala underrättelsetjänsten (KYP), polisen och kommissionsledamoten och fått deras godkännande. Dessa bestämmelser gäller inte för de övervakningssystem som används av polischefen och befälhavaren för KYP[422].

EFTERHANDSGRANSKNING

262. I Cypern anges i lagen om skydd av enskilda vid behandling av personuppgifter och fri rörlighet för sådana uppgifter från 2018 att om personuppgifter används eller om en person har varit föremål för behandling har personen i fråga rätt att bli informerad[423]. Denna rätt kan kringgås när kommissionsledamoten med ansvar för skydd av personuppgifter beslutar annorlunda mot bakgrund av bland annat nationella säkerhetsskäl[424].

263. Dessutom anges i lagen om skydd av sekretess för privat kommunikation som antogs 1996 att justitiekanslern är skyldig att informera personen i fråga om avlyssning av privat kommunikation från brottsbekämpande myndigheters sida. Den enskilde måste underrättas inom högst 90 dagar från ikraftträdandedatumet för domstolsbeslutet[425], eller inom högst 30 dagar från verkställigheten av detta domstolsbeslut. Justitiekanslern

---

[418] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).

[419] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).

[420] CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020.

[421] Svar från Cypern på Europaparlamentets frågeformulär.

[422] Svar från Cypern på Europaparlamentets frågeformulär.

[423] Lag 125(I) från 2018. https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf.

[424] Europeiska unionens byrå för grundläggande rättigheter, serveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volym II: field perspectives and legal update.

[425] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).

måste förse den berörda personen med en rapport med en detaljerad redogörelse för utfärdandet av domstolsbeslutet, datum för utfärdandet av domstolsbeslutet och det faktum att avlyssning eller åtkomst till privat kommunikation har ägt rum under denna period. Denna skyldighet kan tillfälligt upphävas om justitiekanslern beslutar att undanhållande av denna information är av intresse för Cyperns säkerhet, bland annat[426]. Domstolen kan också besluta att uppgifterna inte ska lämnas ut mot bakgrund av Cyperns säkerhetsintressen[427].

264. Åsidosättande av skydd för privat kommunikation ett brott enligt lag. I praktiken döljs denna olaglighet ofta genom att den nationella säkerheten åberopas[428]. Det finns ingen lagstiftning som tar upp hur polisen eller annan underrättelsetjänst använder de uppfångande anordningarna, vem som reglerar förfarandena för uppfångande och hur medborgarnas konstitutionella skydd garanteras. De relevanta reglerna och protokollen är för närvarande vilande i representanthuset för debatt och antagande. För närvarande är denna verksamhet fortsatt okontrollerad[429].

RÄTTSMEDEL

265. Lagenligheten i den cypriotiska underrättelsetjänstens åtgärder utvärderas av en kommitté med tre ledamöter enligt bestämmelserna i Cyperns lag om underrättelsetjänsten 74 (I)/2016. Trepartskommittén utses av ministerrådet på grundval av en rekommendation av republikens president[430].

266. Lag 92(I)/1996 ändrades 2020 och stärkte Republikens tillsynsram, särskilt bestämmelserna om trepartskommittén. Som del av sitt mandat kan kommittén inleda utredningar på eget initiativ och påbörja undersökningar av anläggningar, teknisk utrustning och arkiverat material från KYP. Såsom det fastställs i artikel 17A.1 i lag 92(I)/1996, ändrad genom lag 13(I)/2020, kan kommittén också inleda undersökningar av polisens anläggningar, tekniska utrustning och arkiverade material. Mot bakgrund av sådana utredningar kan kommittén hänskjuta frågan till justitiekanslern, kommissionsledamoten med ansvar för skydd av personuppgifter eller kommissionsledamoten med ansvar för elektronisk kommunikation och postförordningen om ytterligare åtgärder. Kommittén lägger också fram en årsrapport för republikens president där den beskriver verksamheten, formulerar iakttagelser och rekommendationer och identifierar försummelser[431].

267. Cyperns president har stor talan i sammansättningen av kommittén med befogenhet att inleda kritiska undersökningar av KYP:s handlingar. Dessutom skickas årsrapporterna med kommitténs rön först till presidenten[432]. I skrivande stund finns det ingen information om kommitténs exakta sammansättning, dess arbete eller den granskning

[426]Europeiska unionens byrå för grundläggande rättigheter, serveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Volym II: field perspectives and legal update.
[427] CyLaw, The Protection of Privacy of Private Communications (Interception and Access to Recorded Private Communications Content) Law of 1996 (92(I)/1996).
[428] Makarios Drousiotis, 'Κράτος Μαφία', kapitel 6, 2022.
[429] Philenews. 'Legal but uncontrolled interceptions'.
[430] Svar från Cypern på Europaparlamentets frågeformulär.
[431] Svar från Cypern på Europaparlamentets frågeformulär. CyLaw. E.U. Par. J(J) OF LAW 13(J)/2020.
[432] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.

som den utför[433].

VIKTIGA AKTÖRER I SPIONPROGRAMSINDUSTRIN

268. Tal Dilian har spelat en viktig roll i många av utvecklingarna i Cypern och Grekland. Han fick maltesiskt medborgarskap 2017[434]. Tal Dilian verkade i olika ledande positioner i det israeliska försvaret i 25 år innan han gick i pension från militären 2002[435]. Dilian inledde sin karriär som ”underrättelseexpert, samhällsbyggare och serieentreprenör” i Cypern, och startade sedan Aveledo Ltd., som senare döptes om till Ws WiSpear Systems ltd. och därefter Passitora Ltd[436].

269. I Cypern knöt Dilian nära band med Abraham Sahak Avni. Avni har tidigare varit involverad i den israeliska polisens specialstyrkor som specialdetektiv[437]. I november 2015 fick han cypriotiskt medborgarskap och ett gyllene pass på grund av en fastighetsinvestering på 2,9 miljoner euro[438]. Avni grundade det cypriotiska NCIS Intelligence Services ltd[439], ett företag som rapporterades vara involverat i de mäktigaste teknikföretagen i världen[440]. NCIS Intelligence and Security Services tillhandahöll säkerhetsprogram till polisens huvudkontor mellan 2014 och 2015 och tillhandahöll utbildning till anställda på byrån för brottsanalys och -statistik mellan 2015 och 2016[441]. Regeringspartiet Demokratisk samling ingår också i företagets klientel. Avni rapporteras ha installerat säkerhetsutrustning i partiets kontor[442]. Utöver Avnis säkerhetsutrustning såldes även Dilians material till Cyperns myndighet för narkotikabekämpning och den cypriotiska polisen[443].

270. Vid ett tillfälle upptäckte polisens brottsutredningsavdelning att sekretessen hade kränkts för privat kommunikation där Avnis företag deltog. Polisen beslöt att avsluta fallet[444].

271. Kopplingarna mellan Dilian och Avni är många. Dilians företag WiSpear delade en byggnad i Lacarna och en del av sin personal med Avni[445]. År 2018 lanserade de två männen företaget Poltrex, som senare har döpts om till Alchemycorp Ltd. Poltrex har kontor i Novel Tower, som delas med Avni[446], och ingår också i Intellexa Alliance. Avnis förbindelser med DISY-partiet skapade också ett försöksområde för Dilians

---

[433] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.
[434] Maltas regering. 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.
[437] ShahakAvni. About Shahak Avni.
[438] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.
[439] Philenews, ‘FILE: The state insulted Avni and Dilian’.
[440] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.
[441] Philenews, ‘FILE: The state insulted Avni and Dilian’.
[442] Tovima, The unknown ‘bridge’ between Greece and Cyprus for the eavesdropping system’.
[443] Inside Story, ‘Predator: The ‘spy’ who came from Cyprus’.
[444] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.
[445] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.
[446] CyprusMail, ‘Akel says found ‘smoking gun’ linking Cyprus to Greek spying scandal’.

produkter[447].

DILIANS SPIONPROGRAMSBIL

272. Efter försäljningen av Circles-teknik och grundandet av WiSpear lanserade Tal Dilian dessutom Intellexa Alliance år 2019, vilket enligt webbplatsen är ett ”EU-baserat och EU-reglerat företag med syftet att utveckla och integrera teknik för att stärka underrättelsebyråer”[448]. Det finns olika övervakningssäljare som faller inom ramen för Intellexa Alliances marknadsföringsmärke, däribland Cytrox, WiSpear (som senare fick namnet Passitora Ltd.) Nexa technologies och Poltrex Ltd. Dessa olika säljare inom Dilians företagsgrupp möjliggör ett bredare sortiment av övervakningsprogram och -tjänster som Intellexa kan erbjuda och kombinera för sina klienter[449]. Mer detaljerad information om denna företagsstruktur finns i kapitlet om spionprogramsindustrin.

273. Den 5 augusti 2019 intervjuades Dilian av Forbes om sin svarta WiSpear-skåpbil och visade på de olika spionprogramsmöjligheter som hans företag erbjuder. Denna skåpbil till ett värde av 9 miljoner euro kunde hacka enheter inom ett avstånd på 500 meter[450]. Den allmänna uppmärksamhet som genererades av Forbes- intervjun[451] ledde till en utredning av de cypriotiska myndigheterna. Advokat Elias Stefanou utsågs till oberoende brottsutredare för denna utredning. Under denna utredning upptäckte myndigheterna ett annat av Dilians åtaganden som drevs på Larnacas internationella flygplats[452].

274. Den 16 juni 2019 uppges Tal Dilian ha ingått ett avtal med Hermes Airports om att använda hans WiSpear-utrustning i det påstådda syftet att förbättra wifi-signalen för passagerare vid Larnacas internationella flygplats, varefter tre wifi-antenner installerades[453]. Även om det israeliska företaget Go Networks inte var registrerat på Cypern deltog det också i de förhandlingar som ledde fram till arrangemanget[454]. Det verkliga skälet till avtalet var dock att testa WiSpears avlyssningsteknik. De mottagna uppgifterna om passagerare sparades i flygplatsens serverrum, i närheten av WiSpears kontor i Larnaca, som delades med Avni[455]. Under den tid då antennerna var i drift inhämtades uppgifter från 9 507 429 mobila enheter[456].

275. Efter klagomålen mot Dilian uppgavs det israeliska Go Networks vara knutet till Intellexa genom ett gemensamt bolagsägande i Irland. ledande företrädare för israeliska Go Networks påstods ha fått toppbefattningar på Intellexa[457]. Dessutom kom polisutredningarna fram till att exportlicenser hade beviljats WiSpear för ”uppfångande

[447] Inside Story, ‘Predator: The ‘spy’ who came from Cyprus’.
[448] https://intellexa.com/.
[449] Haaretz, ‘As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire’.
[450] Haaretz, ‘As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire’.
[451] Forbes, ‘A Multimillionaire Surveillance Dealer Steps Out Of The Shadows ... And His $9 Million Whatsapp Hacking Van’.
[452] Haaretz, ‘As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire’.
[453] Haaretz, ‘As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire’.
[454] Makarios Drousiotis, ‘Κράτος Μαφία’, kapitel 6, 2022.
[455] Makarios Drousiotis, ‘Κράτος Μαφία’, kapitel 6, 2022.
[456] Makarios Drousiotis, ‘Κράτος Μαφία’, kapitel 6, 2022.
[457] Haaretz. As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.

utrustning utformad för att utvinna röst eller data som överförs via luften”[458] [459]. Dilians företag har enligt handelskammaren inte fått några exportlicenser under de senaste två åren. I skrivande stund är det fortfarande oklart vem som godkände dessa exportlicenser[460].

276. De elektroniska uppgifter som hämtats från den konfiskerade utrustningen för utredningen lämnades in för en kriminalteknisk undersökning på tre nivåer av polisen, en akademisk expert och Europol[461]. Skåpbilen finns kvar i förvar hos polisen, men det är inte klart vad som har hänt med övervakningsutrustningen. Det påstås att den har återlämnats till Dilian, men det verkar inte finnas någon bekräftelse.

277. Den 15 november 2021 togs målet upp vid brottmålsdomstolarna, med WS WiSpear Systems Ltd, Tal Dilian och två andra WiSpear-anställda som svarande. Därefter upprätthöll justitiekanslern George Savvides målet mot företaget WiSpear, men det straffrättsliga förfarandet mot Dilian och de anställda lades ned[462]. Skälen till beslutet är sekretessbelagda. Justitiekanslern kan dock när som helst besluta att återuppta målet mot de tre personerna.

278. WiSpear erkände sig skyldig till 42 åtalspunkter och bötfälldes med 76 000 euro i domstolen för grövre brott den 22 februari 2022[463]. WiSpear erkände åtalspunkterna om olaglig övervakning av privat kommunikation och överträdelser av uppgiftsskydd[464]. Domstolen offentliggjorde sitt slutliga domslut och uppgav följande: ”Domstolen för grövre brott noterade och godkände att den överträdelse som tillskrivs företaget aldrig omfattade någon avsikt, hackning eller avlyssning, och det gjordes aldrig något försök och fanns inget syfte att personifiera några uppgifter. Domstolen betonade att ingen skada åsamkats någon enskild person”[465]. Utöver de böter som utdömts av domstolen för grövre brott bötfällde kommissionsledamoten med ansvar för skydd av personuppgifter, Irini Loizidou Nicolaidou, WiSpear med 925 000 euro mot bakgrund av brott mot den allmänna dataskyddsförordningen[466]. Även om det hävdades den svarta skåpbilen berör frågor av nationellt intresse och kritisk infrastruktur, var sanktionerna för förövarna mycket lätta. Denna händelse kan ha politisk betydelse utöver kränkningen av passagerarnas privatliv. Med tanke på att Cypern på många sätt är beläget i ett vägskäl finns det länder utanför EU som skulle kunna vara intresserade av att få insikt i vilka resenärer som rör sig genom Larnacas flygplats: till exempel Turkiet, Israel, Ryssland och USA.

279. Oppositionspartiet AKEL uttryckte sin upprördhet över målen mot Dilian och dennes personal, och avvisade det rättsliga beslutet som en mörkläggning av justitiekanslern[467].

---

[458] Makarios Drousiotis. Κράτος Μαφία. Chapter 6. Published 2022.

[459] Philenews. Export of tracking software from Cyprus.

[460] Inside Story, ‘Who signs the exports of spyware from Greece and Cyprus?’.

[461] Pressmeddelande av den 10 augusti 2022 från biträdande justitiekanslern om PEGA-uppdraget i Cypern av den 2 november 2022.

[462] Financial Mirror, ‘Anger after ‘spy van’ charges dropped’.

[463] Makarios Drousiotis, ‘Κράτος Μαφία’, kapitel 6, 2022; Pressmeddelande av den 10 augusti 2022 från biträdande justitiekanslern om PEGA-kommitténs uppdrag i Cypern av den 2 november 2022.

[464] Financial Mirror, ‘Spy van company fined €76,000’.

[465] Haaretz, ‘As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire’.

[466] CyprusMail. Israeli company that deployed ‘spy van’ fined €925,000 for data violations; Financial Mirror, ‘Anger after ‘spy van’ charges dropped’.

[467] Financial Mirror. Anger after ‘spy van’ charges dropped.

Den cypriotiska regeringen påstods trots allt ha köpt utrustning från Dilians företag och en av de anklagade medarbetarna påstods ha arbetat för NSO, och försett KYP med utbildning om användningen av spionprogrammet Pegasus[468]. Att ärendet avskrevs garanterade att informationen om kopplingarna mellan Dilians företag och den cypriotiska regeringen skulle fortsätta att vara skyddade[469]. Justitiekanslern vägrade att överlämna slutsatserna från utredningen, trots att de begärdes av PEGA-kommitténs officiella uppdrag i Cypern. Detta exempel visar att det inte finns fullständiga rättsliga garantier för enskildas rättigheter till skydd av personuppgifter mot massövervakningsutrustning. Trots att rättsmedel existerar på papperet kan påverkas utgångarna i domstol ofta av regeringen, där det enskilda offret är försvarslöst. Undersökningen visade vidare att Cypern har blivit en grogrund för de Cypernbaserade företagen själva att experimentera med övervakningsutrustning.

FÖRFLYTTNING TILL GREKLAND

280. Efter händelsen med skåpbilen och stämningsansökan flyttade Dilian Intellexas verksamhet till Grekland, men han lämnade aldrig Cypern. Enligt uppgift planerar han att återvända till Tel Aviv[470]. Indirekta förbindelser mellan flera fysiska och juridiska personer som är registrerade i Cypern och Grekland avslöjar flytten av Dilians verksamhet till Aten[471]. Vad som följer är några av de namn som ingår i förbindelserna mellan Cypern och Grekland, även om den viktigaste roll som Intellexa SA spelar i Grekland förklaras närmare i kapitlet om Grekland.

281. De rättsliga utredningarna ledde till att Avnis och Dilians verksamhet i Poltrex överfördes till Yaron Levgoren. Levgoren är permanent bosatt i Kanada. Han blev aktieägare, styrelseledamot och sekreterare i Poltrex. Levgoren är också kopplad till Intellexa i Grekland[472]. Enligt hans Linkedin-profil företräder han för närvarande det Greklandsbaserade Intellexa-företaget Apollo Technologies.

SPIONPROGRAMFÖRETAG OCH CYPERN

282. Utöver Intellexa Alliance påstods Cypern också vara säte för NSO Group. År 2010 lanserade Tal Dilian tillsammans med Boaz Goldman och Eric Banoun företaget Circles Technologies, som är specialiserat på försäljning av system som utnyttjar SS7-sårbarheter[473]. Sex år senare såldes Circles Technologies till Francisco Partners för knappt 130 miljoner dollar, varav 21,5 miljoner dollar gick till Dilian. Detta Kalifornien-baserade privatkapitalbolag erhöll på liknande sätt 90 % av NSO Group, vilket ledde till sammanslagningen av Circles Technologies och NSO Group under namnet L.E.G.D Company Ltd., sedan den 29 mars 2016 känt som Q Cyber Technologies Ltd[474].

283. Enligt den cypriotiska regeringens svar till PEGA-kommittén omfattar departementet för företagsregister och immateriell äganderätt inte NSO Group som en registrerad

[468] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[469] Makarios Drousiotis. Κράτος Μαφία.. Chapter 6. Published 2022.
[470] Intelligence Online, Israeli cyber tsar Tal Dilian plans Tel Aviv return.
[471] *Haaretz*, As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire.
[472] Philenews, How the spyware scandal in Greece is related to Cyprus.
[473] Amnesty International, ”Operating from the Shadows.
[474] Amnesty International, ”Operating from the Shadows.

juridisk person. NSO Group innehar inga aktier i någon juridisk person som är registrerad i Cypern. Enskilda styrelseledamöter i NSO Group har dock antingen startat eller köpt sex företag. Dessutom verkar spionprogrammet Pegasus inte ha utvecklats i eller officiellt exporterats från Cypern[475].

284. Utvidgningen inom ramen för Francisco Partners mellan 2014 och 2019 omfattade sex cypriotiska företag. Francisco Partners kompletterades med ITOA Holdings Ltd., registrerat på Cypern och moderbolag till CS-Circles Solutions Ltd., Global Hubcom Ltd. och MS Magnet Solutions. Ms Magnet Solutions äger Mi Compass Ltd. CS-Circles Solutions Ltd. äger dessutom CI-Compass Ltd. Förutom de cypriotiska enheterna äger CS-Circles Solutions Ltd. även bulgariska enheter. NSO Group har uppgett att ”de bulgariska företagen på kontraktsbasis tillhandahåller forsknings- och utvecklingstjänster till sina respektive cypriotiska dotterbolag och exporterar nätverksprodukterna för statlig användning”[476].

285. Den cypriotiska regeringen förnekar exporten och utvecklingen av Pegasus. Den 21 juni 2022 uppgav dock NSO-tjänstemannen Chaim Gelfad att NSO-företag i Cypern och Bulgarien var engagerade i programvara som tillhandahåller underrättelsetjänster[477]. Enligt ett dokument som delats av oppositionspartiet Arbetande folkets progressiva parti med Europaparlamentet har NSO Group enligt uppgift exporterat spionprogrammet Pegasus genom ett av sina dotterbolag i Cypern till ett företag i Förenade Arabemiraten. Ett av dotterbolagen ska enligt uppgift ha utfärdat en faktura på 7 miljoner dollar för tjänster till det berörda företaget[478]. Denna information kan dock inte bekräftas.

286. Enligt uppgift hade NSO Group också ett aktivt företag i Cypern som påstods vara värd för ett kundtjänstcenter. 2017 hölls ett möte med NSO:s tjänstemän och de saudiska kunderna på Four Seasons Hotel i Limassol för att presentera den senaste kapaciteten hos Pegasus 3#versionen av spionprogrammet. Den här versionen hade den nya ”nollklick”-kapaciteten som kunde infektera en enhet utan behov av att klicka på en länk, till exempel genom ett missat WhatsApp-samtal. De saudiarabiska kunderna köpte omedelbart tekniken till ett belopp av 55 miljoner euro[479] [480]. Det bör noteras att ett år senare, den 2 oktober 2018, dödade den saudiska regimen Jamal Khashoggi på det saudiska konsulatet i Turkiet, efter att ha övervakat hans närmaste med hjälp av Pegasus. Detta bestrids av NSO.

287. Enligt Citizen Lab var 25 statliga aktörer kunder till Circles Technologies 2020. Bland dessa statliga aktörer fanns Belgien, Danmark, Estland och Serbien[481]. NSO Group stängde sitt Circles-kontor i Cypern under 2020. I skrivande stund är det fortfarande oklart vilka Circles-företag som fortfarande är i drift[482].

288. Israeliska QuaDream är ett annat företag som enligt uppgift är kopplat till exporten av dess spionprogramprodukt ”Reign” från Cypern. I april 2023 rapporterade media att

---

[475] Svar från Cypern på Europaparlamentets frågeformulär.
[476] Amnesty International, ”Operating from the Shadows.
[477] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.
[478] Akel report, PEGA-kommitténs uppdrag i Cyprus.
[479] Makarios Drousiotis, Κράτος Μαφία, kapitel 6, publicerad 2022.
[480] Haaretz, Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale With Saudis, Haaretz Reveals.
[481] Citizen Lab. Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles.
[482] Amnesty International, ”Operating from the Shadows.

QuaDream stängde sina israeliska kontor[483]. QuaDream sålde sina produkter indirekt till kunder genom via InReach, ett företag som är registrerat i Cypern sedan 2017, och kringgick därmed israeliska exportkontroller. De två företagen befinner sig i en pågående rättstvist[484].

289. Nuvarande direktör och sekreterare för InReach är A.I.L. Nominee Services Ltd. Detta företag var redan registrerat i Cypern 2010 och dess grundande aktieägare var den nuvarande biträdande justitiekanslern Savvas Angelides[485]. Angelides sålde sina aktier i A.I.L. Nominee Services till Christos Ioannides den 16 februari 2018, några veckor innan han blev försvarsminister[486]. A.I.L. Nominee Services är dock fortfarande direktör och sekreterare för InReach[487] och bedriver därmed verksamhet med ett företag som exporterar QuaDream-produkter till tredjeländer.

290. År 2011 grundade Abraham Sahak Avni ett företag tillsammans med Michael Angelides, bror till den f.d. ministern och nuvarande biträdande justitiekanslern Savvas Angelides. Deras företag S9S registrerades i bolagsregistret den 10 november 2011[488] med hjälp av Savvas Angelides f.d. advokatbyrå[489]. Dessutom identifierades A.I.L. Nominee Services Ltd som sekreterare för S9S. Under den tiden var Savvas Angelides fortfarande den största aktieägaren i A.I.L. Nominee Services[490]. Partnerskapet mellan Michael Angelides och Avni upplöstes dock 2012. Savvas Angelides tillträdde som biträdande justitiekansler 2020 och var den person som ansvarade för att utreda Avni och Dillian i fallet med övervakningsbilen[491]. I ett pressmeddelande den 10 augusti 2022 förklarade biträdande justitiekanslern att varken han eller hans familj hade någon koppling till Tal Dilian. När det gäller partnerskapet mellan Michael Angelides och Avni nämnde han att ”det yrkesmässiga samarbetet misslyckades redan från början, tillsammans med det faktum att det företag som registrerades av min tidigare advokatbyrå, på instruktioner från en släkting till mig, aldrig aktiverades” och därför aldrig utgjorde ett ”hinder för mitt deltagande i beslutet om ärendet om *den svarta skåpbilen*”[492]. I pressmeddelandet nämns dock inte Savvas Angelides företag A.I.L Nominee Services Ltd. som aktiverades juli 2010[493], eller företagets roll som sekreterare i partnerskapet mellan hans släkting och Avni i S9S.

---

[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.
[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, ‘Interceptions’ file: Classified Police Report (2016) shows he knew everything about Avni.
[489] Pressmeddelande från biträdande justitiekanslern av den 10 augusti 2022 såsom det förvärvades under PEGA-kommitténs uppdrag i Cypern den 2 november 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] Utredning utförd av Fanis Makridis, PEGA-kommitténs uppdrag i Cypern den 1 november 2022.
[492] Pressmeddelande från biträdande justitiekanslern av den 10 augusti 2022 såsom det förvärvades under PEGA-kommitténs uppdrag i Cypern den 2 november 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.

BLACK CUBE

291. Black Cube är ett företag som anställer tidigare officerare från israeliska underrättelsetjänster, såsom Mossad. Företaget använder sig av agenter med falska identiteter. Enligt *New Yorker* anlitade tidigare vd:n för NSO Group, Shalev Hulio, Black Cube efter det att tre advokater – Mazen Masri, Alaa Mahajna och Christiana Markou – stämt NSO och ett dotterbolag i Israel och Cypern[494]. Under 2018 mottog de tre advokaterna flera meddelanden från så kallade bekanta från vissa företag och individer, där möten i London föreslogs. Hulio uppgav att det för stämningen på Cypern fanns en inblandning av Black Cube eftersom stämningen kom från ingenstans och han vill förstå.[495] Black Cube exponerades också i spionskandaler i Ungern och Rumänien.

CYPERNS INKÖP OCH ANVÄNDNING AV SPIONPROGRAM

292. Förutom att underlätta ett välkomnande exportklimat för spionprogramsföretag har den cypriotiska regeringen själv en historia av inköp av spionprogram. Landet påstås också ha använt övervakningssystem själva. I skrivande stund är det fortfarande oklart i vilka fall Cypern har använt sig av konventionella övervakningsmetoder eller spionprogram.

293. Efter valet 2013 utsågs Andreas Pentaras till chef för Cyperns underrättelsetjänst, medan övervakningsexperten Andreas Mikellis var ansvarig för skyddet av president Anastasiades kommunikation. Samma år besökte Mikellis enligt uppgift ISS-övervakningsutställningen i Prag, där han enligt uppgift förhandlade med Hacking Team för inköp av den så kallade DaVinci-programvaran[496]. Programmet DaVinci kunde infektera applikationer i en mobiltelefon och uppfyllde därför inte de officiella kraven för att häva sekretessen[497].

294. Röjd kontaktinformation mellan Mikellis och Hacking Team som avslöjades av WikiLeaks visade att anbudsförfaranden kringgicks och att det förvärvade övervakningssystemet inte sågs över på rätt sätt. I början av 2014 rapporterades att programvaran hade installerats och att fyra av KYP:s anställda hade utbildats, däribland Mikellis[498].

295. När WikiLeaks avslöjade köpet av Hacking Teams övervakningsprogramvara bekräftade KYP att detta system endast användes för nationella ändamål[499]. Trots Mikellis kontakt med Hacking Team[500] var det chefen för KYP, Andreas Pentaras, som slutligen avgick efter dessa avslöjanden[501]. Kyriakos Kouros ersatte Pentaras.

296. Enligt WikiLeaks var ytterligare en polisavdelning tydligen också intresserad av att köpa ett kommunikationsövervakningssystem från Hacking Team. Avdelningen försökte säkra systemet genom Sahak Avni[5021a]. Det är dock oklart vilken

---

494 The New Yorker, How Democracies Spy on their Citizens.
495 The New Yorker, How Democracies Spy on their Citizens.
496 Makarios Drousiotis, Κράτος Μαφία, kapitel 6, publicerad 2022.
497 Inside Story, Predator: The 'spy' who came from Cyprus.
498 Makarios Drousiotis, Κράτος Μαφία, kapitel 6, publicerad 2022.
499 Inside Story, Predator: The 'spy' who came from Cyprus.
500 Makarios Drousiotis, Κράτος Μαφία, kapitel 6, publicerad 2022.
501 CyprusMail, Intelligence chief resigns after spy tech revelations. https://cyprus-mail.com/2015/07/11/intelligence-chief-resigns-after-spy-tech-revelations/.
502 Inside Story, Predator: The 'spy' who came from Cyprus.

polisavdelning det handlar om här**.**

MÅLTAVLAN MAKARIOS DROUSIOTIS

297. Från och med februari 2018 utredde den cypriotiska regeringen journalisten Makarios Drousiotis med hjälp av både avlyssningsteknik och spionprogram[503]. Detta fall av spionage inleddes då Drousiotis tjänstgjorde som assistent till den cypriotiska EU-kommissionären för humanitärt bistånd och krishantering Christos Stylianides och under hans undersökningar om de ekonomiska förbindelserna mellan president Anastasiades och ryska personer såsom oligarken Dmitrij Rybolovlev. Enligt Drousiotis var det hans senare roll som utlöste det första övervakningsförsöket[504].

298. Under Drousiotis undersökning av de ryska förbindelserna började avslöjanden om NSO Groups verksamhet från Cypern dyka upp i internationella medier, bland annat på Pegasus 3#presentationen på Four Season Hotels. Citizen Lab misstänkte dessutom att Cypern var ett av de länder som använde NSO-tekniken för avlyssning av kommunikation via det brittiska utrikesministeriets datorsystem[505]. I detta skede började Drousiotis att minnas flera tecken på att spionprogrammet Pegasus infiltrerade hans telefon, däribland ett missat WhatsApp-samtal, snabb urladdning av batteriet och att enheten ofta blev överhettad utan att han använde den[506]. Mot bakgrund av dessa händelser anser Drousiotis att den cypriotiska regeringen – särskilt den cypriotiska underrättelsetjänsten – ligger bakom infektionen av hans telefon.

299. I maj 2019 skickade Drousiotis ett brev till president Anastasiades där han uttryckte sin oro över övervakningen av hans telefon och redogjorde för de potentiella motiven bakom denna övervakning samt höll presidenten personligen ansvarig för allt som kan hända honom efter spionaget. Anastasiades vidarebefordrade brevet till den nuvarande chefen för Cyperns underrättelsetjänst, Kyriakos Kouros. Både Anastasiades och Kouros har motsatt sig den påstådda övervakningen med programvaran Pegasus, och upprepat att NSO Group i själva verket inte ens var registrerat i Cypern[507].

300. Under de efterföljande månaderna inträffade flera skrämselförsök, bland annat försvann bevis på hans dator, säkerhetskameran i Drousiotis hem kopplades bort och han förföljdes av främlingar. Efter att ha offentliggjort sin historia och lämnat in ett klagomål till den cypriotiska polismyndigheten kontaktade Drousiotis Lambros Katsonis, chef för avdelningen för tekniskt stöd vid Panda Security, ett cypriotiskt företag specialiserat på antivirusutrustning. Drousiotis var dock inte medveten om att den cypriotiska regeringen också använde detta antivirusprogram för sina egna enheter. Mot denna bakgrund verkar Katsonis ha skickats till Drousiotis hem under falska förevändningar, eventuellt i syfte att ytterligare infiltrera Drousiotis enheter enligt anvisningar från den cypriotiska underrättelsetjänsten[508].

301. Under 2019 blev Drousiotis medveten om de misstänkta intrången i hans Android-telefon och kontaktade Google Ones support för att bekräfta karaktären på dessa

[503] https://www.euractiv.com/section/media/news/whistleblower-spyware-helps-the-mafia-rule-in-cyprus/
184 Makarios Drousiotis, Κράτος Μαφία, kapitel 5, publicerad 2022.
[504] Makarios Drousiotis, Κράτος Μαφία, kapitel 5, publicerad 2022.
[505] BBC, No 10 network targeted with spyware, says group.
[506] Makarios Drousiotis, Κράτος Μαφία, kapitel 5, publicerad 2022.
[507] Makarios Drousiotis, Κράτος Μαφία, kapitel 5, publicerad 2022.
[508] Makarios Drousiotis. Κράτος Μαφία. Kapitel 5. Publicerad 2022.

intrång. Google svarar dock i allmänhet inte på övervakningsrelaterade frågor och hänvisar kunden i fråga till de nationella brottsbekämpande myndigheterna1a. Även om Drousiotis inte hade något förtroende för polisen gick han med på att överlämna sina enheter för kriminalteknisk undersökning[509].

AVSLUTANDE KOMMENTARER

302. Cypern har en stabil rättslig ram för skydd av personuppgifter och integritet, för godkännande av övervakning och för export. I praktiken verkar det dock vara lätt att kringgå reglerna och det finns ett nära samband mellan politiker, säkerhetsmyndigheter och övervakningsindustrin. Det verkar vara en slapp tillämpning av reglerna som gör Cypern till en så attraktiv plats för handel med spionprogram. En bättre tillämpning av befintliga regler behövs. Cypern är också av stort strategiskt intresse för Ryssland, Turkiet och USA. Dessutom verkar nära förbindelser med Israel vara av särskild ömsesidig nytta när det gäller handeln med spionprogram. Exportlicenser för spionprogram har blivit valuta i diplomatiska förbindelser.

Spanien

303. Efter inbjudan från PEGA-kommittén i Europaparlamentet inbjöds de spanska myndigheterna till en utfrågning den 29 november 2022 för att, i den mån det var möjligt inom ramen för deras rättsliga skyldigheter, redogöra för användningen av spionprogram för övervakning i Spanien. På grund av dessa uttalade ”rättsliga begränsningar” var svaren till kommittén begränsade och lämnade de flesta frågor öppna.

304. PEGA-kommittén besökte Madrid i mars 2023. Delegationen träffade statssekreteraren för EU-frågor och personer som enligt Citizen Lab var måltavlor för spionprogram, nämligen Kataloniens regionspresident, den katalanska regionala ministern för utrikesfrågor och en ledamot i Barcelonas stadsfullmäktige. De träffade också ledamöter av det katalanska parlamentets undersökningskommitté för Pegasus, en företrädare för ombudsmannens kontor, icke-statliga organisationer som arbetar med grundläggande rättigheter samt journalister.

305. Avslöjandena i juli 2021 av Pegasus-projektet visade på ett stort antal misstänkta fall i Spanien. Angreppen verkar dock ha riktats mot olika aktörer och av olika skäl. I maj 2022 pekade man i en rapport publicerad av *The Guardian* ut Marocko som möjligt ansvarig för spionaget mot 200 spanska mobiltelefoner. Den spanska regeringen bekräftade att premiärminister Pedro Sánchez, försvarsminister Margarita Robles och inrikesminister Fernando Grande-Marlaska har infekterats av spionprogrammet Pegasus, medan jordbruksministern Luis Planas var måltavla, men inte infekterades[510]. Vid samma datum ska även den dåvarande utrikesministern, Arancha González Layas, mobiltelefon ha utsatts för spionage - men man har inte kunnat bevisa varken varifrån detta cyberangrepp kom eller huruvida Pegasus användes vid angreppet. Härvan med den andra gruppen måltavlor kallas ”CatalanGate”[511]. Den omfattar katalanska

[509] Makarios Drousiotis. Κράτος Μαφία. Kapitel 5. Publicerad 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 maj 2022.
[511] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022.

parlamentsledamöter, ledamöter av Europaparlamentet, advokater, journalister, medlemmar av civilsamhällesorganisationer, akademiker och en del familjemedlemmar och personal med anknytning till dessa måltavlor[512], vilket kan betecknas som ”indirekt målinriktning” eller ”relationsmålinriktning”. Övervakningsskandalen ”CatalanGate” omnämndes för första gången 2020 efter en gemensam utredning av *The Guardian* och *El País*[513], men det var först i april 2022 som Citizen Lab slutförde sin fördjupade undersökning och skandalens omfattning avslöjades. Resultaten av det arbetet visade att minst 65 personer var måltavlor[514]. Det bör noteras att Citizen Lab i december 2022 erkände att fall felaktigt betecknades som en infektion på grund av ett fel vid märkningen med initialer[515], även om det totala antalet katalanska måltavlor förblev oförändrat. De spanska myndigheterna medgav i maj 2020 att man hade avlyssnat 18 personer med tillstånd från domstol[516], men dessa fullmakter har inte offentliggjorts. Tidigare direktören för Spaniens nationella underrättelsetjänst (CNI) Paz Esteban inställde sig inför parlamentets kommitté för statshemligheter inför stängda dörrar för att motivera övervakningen av dessa 18 personer

306. Den spanska regeringen har hittills gett begränsad information om sin roll i dessa fall och åberopat behovet av sekretess när det gäller den nationella säkerheten och rättsliga skäl. På grundval av en rad indikatorer[517], varav flera erkändes av den ovannämnda kommittén för statshemligheter, antas det dock att övervakningen av de katalanska måltavlorna utfördes av de spanska myndigheterna,

307. En noggrann analys av övervakningen visar ett tydligt mönster. De flesta av ”CatalanGate”-avlyssningarna sammanfaller med och har koppling till avgörande politiska händelser, frågor och personer, såsom tillåtligheten av det katalanska parlamentets utträdeslagar, domstolsmål mot katalanska separatister, offentliga möten som organiserats av Tsunami Democràtic och kommunikation med katalanska separatister som bor utanför Spanien[518]. Sådan övervakning omfattar till exempel en fängslad separatists kommunikation med sin advokat dagen före rättegången, kontakter mellan makar eller meddelanden som rör fördelning av platser i Europaparlamentet. När det gäller de återstående 47 fallen med spionprogram har det inte varit möjligt att bedöma hur målen skulle ha haft en omedelbar inverkan på den nationella säkerheten eller statens integritet eller hur de utgjorde ett överhängande hot mot dessa, och ingen information har lämnats om detta[519]. Även om vissa av de personer som hade varit mål för övervakningen tidigare hade åtalats för brott, har inga åtal väckts mot någon av de

[512] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022* på sidan 1.
[513] https://www.theguardian.com/world/2020/jul/16/two-catalan-politicians-to-take-legal-action-targeting-spyware
[514] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, *18 april 2022* på sidan 1.
[515] Citizen Lab*, Correcting a case,* CatalanGate report https://citizenlab.ca/2022/12/catalangate-report-correcting-a-case/ 22 december 2022.
[516] El National, https://www.elnacional.cat/en/politics/spain-cni-admits-spying-catalan-independence-judge_752448_102.html, 5 maj 2022.
[517] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 1+3.
[518] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ , 18 april 2022.
[519] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ , 18 april 2022.

18 personerna till följd av övervakningen med spionprogram[520].

INKÖP AV SPIONPROGRAM

308. De spanska myndigheterna har sedan tidigare erkänt inköp av verktyg för avlyssning av telekommunikation och förvärv av SITEL (System för the Lawful Interception of Telecommunications) under 2001. De erkände också att spionprogramtjänster inköptes av inrikesministeriet, CNI och den spanska nationella polisen från Hacking Team 2010 som en del av genomförandet av det integrerade systemet för telekommunikationsavlyssning, vilket försåg de statliga säkerhetsstyrkornas (FCSE) operativa enheter med medel för avlyssning och registrering av elektronisk kommunikation som godkänts genom ett domstolsbeslut[521]. Sedan SITEL förvärvades har det använts av de spanska myndigheterna för bland annat narkotikabekämpning, för att lokalisera medlemmarna i jihadistcellen bakom attackerna i Madrid den 11 mars 2004 och för att bekämpa fall av politisk korruption. Tidigare rapporterades det också av Citizen Lab att Spanien var en misstänkt kund till FinFisher[522]. År 2020 rapporterade den spanska tidningen *El Pais* att Spanien har gjort affärer med NSO Group och att det nationella underrättelsecentrumet rutinmässigt använder Pegasus[523]. Den spanska regeringen påstås ha köpt in spionprogrammet under första halvan av 2010-talet till ett uppskattat belopp på 6 miljoner euro[524] [525]. Inköpet av SITEL bekräftades av f.d. vicepresident de la Vega 2009[526], medan upphandlingen av Hacking Teams tjänster erkändes av CNI i en kommentar till tidningen *El Confidencial* 2015[527]. Dessutom har en tidigare anställd vid NSO bekräftat att Spanien har ett konto hos företaget[528] trots att de spanska myndigheterna avstår från att kommentera eller bekräfta detta[529].

309. Enligt Googles hotanalysgrupp är spionprogramföretaget Variston IT, med sitt säte i Barcelona, enligt uppgift kopplat till ett ramverk som utnyttjar kända sårbarheter i Microsoft Defender, Chrome och Firefox och installerar spionprogram på målenheter. Sårbarheterna åtgärdades 2021 och i början av 2022[530]. Enligt sin webbplats erbjuder Variston skräddarsydda informationssäkerhetslösningar[531].

---

[520] Uppdrag i Spanien.
[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] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 5.
[523] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 5.
[524] Politico, https://www.politico.eu/article/catalan-president-stronger-eu-rules-against-digital-espionage/, 20 april 2022.
[525] El Pais, https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html, 20 april 2022.
[526] Newtral, https://www.newtral.es/sitel-programa-espia-guardia-civil-policia-espana/20220509/ 9 maj 2022.
[527] El Confidencial, https://www.elconfidencial.com/tecnologia/2015-07-06/cni-hackers-team-espionaje-contratos_916216/ 6 juli 2015.
[528] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens 18 april 2022.
[529] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[530] Threat Analysis Group. *New details on commercial spyware vendor Variston.; Techcrunch. Spyware vendor Variston exploited Chrome, Firefox and Windows zero-days, says Google.*
[531] *https://variston.net/.*

310. Rätten till privatliv skyddas enligt artikel 18 i den spanska konstitutionen från 1978, inbegripet rätten till sekretess vid kommunikation och garanterar särskilt post-, telegrafi- och telefonkommunikation[532]. Användningen av spionprogram som Pegasus och Candiru skulle vara en överträdelse av artikel 18 om domstolstillstånd saknades, en möjlighet som erkänns i den spanska lagstiftningen[533]. I konstitutionen föreskrivs också ytterligare undantag från dessa rättigheter i avsnitt 55 i del I genom att det anges att vissa friheter kan upphävas med deltagande av domstolarna och ordentlig parlamentarisk kontroll om man har kommit överens om att utlysa undantags- eller belägringstillstånd enligt villkoren i konstitutionen eller när det gäller personer som är föremål för utredning för verksamhet som rör väpnade grupper eller terroristorganisationer[534]. På samma sätt beskrivs i artikel 55 demokratiska garantier för att se till att ”oberättigad användning eller missbruk” av dessa befogenheter leder till åtal.

311. För åtgärder som kan påverka hemmets okränkbarhet och kommunikationssekretessen krävs enligt artikel 18 i den spanska författningen ett domstolsbeslut. Enligt artikel 8 i Europakonventionen ska alla åtgärder som en myndighet vidtar som påverkar utövande av denna rättighet vara förenliga med lagen och utgöra åtgärder som i ett demokratiskt samhälle är nödvändiga för den nationella säkerheten, den allmänna säkerheten, landets ekonomiska intressen, skyddet av den allmänna ordningen och förebyggandet av brottslighet, skyddet av hälsa eller moral samt skyddet av andras rättigheter och friheter.

312. Ytterligare information om undantagen från rätten till privatliv enligt artikel 18 finns i straffprocesslagen[535] [536]. I artikel 588 i denna lag begränsas specifikt användningen av utredningsåtgärder till utredning av sakförhållanden som, på grund av deras särskilda allvar, motiverar en begränsning av de grundläggande rättigheterna. De fall som avses i följande punkter omfattas dock inte av denna bestämmelse: a) Grundlag 2/2002 av den 6 maj 2002 om reglering av rättslig förhandskontroll av den nationella underrättelsetjänsten. b) Grundlag 4/1981 av den 1 juni 1981 om varningstillstånd, undantagstillstånd och belägring. och c) Grundlag 2/1989 av den 13 april om militärt förfarande, som innehåller kompletterande bestämmelser som är tillämpliga på straffprocesslagen. Enligt artikel 588 i lagen ska en domare ge tillstånd till avlyssning av telefon- och telematikkommunikation när utredningen gäller allvarliga brott såsom terrorism eller brott som begås genom datoriserade instrument eller någon annan informations- eller kommunikationsteknik eller kommunikationstjänst. Dessutom måste begränsningar godkännas av en rättslig myndighet. Tillstånden beviljas med förbehåll för fyra särskilda principer. För det första, specialisering (att övervakningen är relaterad

[532] Spaniens författning 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, vid avsnitt 18.
[533] Spaniens författning 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx**,** avsnitt 18.
[534] Spaniens författning 1978, https://www.lamoncloa.gob.es/lang/en/espana/leyfundamental/Paginas/titulo_primero.aspx, vid avsnitt 55.
[535] Criminal Procedure Act 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf.

[536] Royal Decree of 14 September 1882 approving the Criminal Procedure Act, https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036&tn=1&p=20220907.

till ett specifikt brott). För det andra, lämplighet (med beskrivning av varaktighet, mål och subjektiv omfattning). För det tredje, proportionalitet (den befintliga bevisningens styrka, ärendets allvar och det eftersträvade resultatet), och slutligen, exceptionell karaktär och nödvändighet (det finns inga andra åtgärder tillgängliga och utan den kommer utredningen att störas)[537]. I artikel 588 f (a, b och c) fastställs särskilt villkoren för sökningar på distans. Den behöriga domaren får enligt artikel 588 f godkänna installation av programvara som möjliggör fjärr- och telematikundersökning utan ägarens eller användarens vetskap, under förutsättning att det eftersträvar att utreda vissa brott. I detta syfte ska åtgärden vara strängt begränsad till en strikt varaktighet på en månad, som kan förlängas med en månad i taget upp till högst tre månader.

313. I artikel 197 i strafflagen föreskrivs påföljder som sträcker sig från tolv månader till fyra års fängelse och böter på tolv till 24 månader för personer som beslagtar eller avlyssnar bland annat e-post och telekommunikationer utan korrekt tillstånd[538]. Dessutom reglerar artikel 264 i strafflagen ytterligare brottsliga handlingar som innebär radering av uppgifter och ger tillgång till uppgifterna i situationer där det nödvändiga tillståndet har beviljats av en behörig myndighet[539]

314. Kraven på rättslig tillsyn är följande: a) Polisen ska informera den undersökande domaren om åtgärdens utveckling och resultat. b) Domaren i det rättsliga avgörandet fastställer hur ofta och i vilken form polisen måste informera honom eller henne om åtgärdens utveckling. c) Polisen ska inom de fastställda tidsfristerna ge domaren tillgång till två olika digitala stöd, ett med transkribering av de avsnitt som anses vara av intresse och det andra med fullständiga inspelningar. d) Inspelningarna ska ange ursprung och destination för varje kommunikation. e) Polisen måste använda ett avancerat elektroniskt system för försegling eller underskrift eller ett tillräckligt tillförlitligt varningssystem ska säkerställa äktheten och integriteten hos den information som överförs från den centrala datorn till de digitala medier där kommunikationen har registrerats. f) Polisen måste rapportera om resultaten av åtgärden när åtgärden avslutas.

315. Den spanska underrättelsetjänsten består av tre huvudbyråer. För det första, det nationella underrättelsecentrumet (CNI) som utför sitt uppdrag genom att insamla information i Spanien och utomlands och agerar under den verkställande, lagstiftande och dömande maktens översyn och kontroll och hör till försvarsministeriet[540]. Chefen för CNI utses av försvarsministern och fungerar som premiärministerns huvudrådgivare i frågor som rör underrättelseverksamhet och kontraspionage[541]. Det andra organet är den inhemska underrättelsetjänsten, underrättelsetjänsten för terrorismbekämpning och organiserad brottslighet (CITCO). Det tredje organet är den spanska försvarsmaktens underrättelsetjänst (CIFAS). CIFAS står också under direkt tillsyn av

---

[537] . Criminal Procedure Act 2016, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal%20Procedure%20Act%202016.pdf .
[538] Criminal Code 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, artikel 197.
[539] Criminal Code 1995, https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf, artikel 264.
[540] National Intelligence Centre (CNI), https://www.cni.es/.
[541] https://www.cni.es/en/intelligence.

försvarsministeriet[542] [543]. CNI inrättades genom lag nr 11/2002 den 6 maj 2002 och bemyndigar CNI att genomföra ”säkerhetsutredningar”[544] Landets polis- och brottsbekämpningsorgan, som kallas ”Guardia Civil”, är av ”militär karaktär” och är också ansvarigt inför försvarsministeriet[545].

316. Lagen om statshemligheter, som stiftades 1968, omfattar sekretessbelagda handlingar i Spanien och innehåller ingen tidsram för när en officiell hemlighet löper ut[546]. Såvida inte regeringen uttryckligen beslutar att handlingar ska lämna ut, det vill säga att ett ministerium eller ett annat officiellt organ uttryckligen lyfter sekretessen från en handling, förblir handlingarna hemliga. Denna lag håller för närvarande på att ses över av den spanska regeringen och antagandet har inget slutdatum, men ett preliminärt lagförslag om sekretessbelagd information antogs den 1 augusti 2022. Enligt lagförslaget måste sekretessbelagda uppgifter offentliggöras inom en period på mellan 4 och 50 år, även om detta kan förlängas.

FÖRHANDSGRANSKNING

317. CNI har i uppdrag att förse den spanska regeringen med den information och de underrättelser som krävs för att förebygga och undvika alla risker eller hot som påverkar statens oberoende och självständighet, de nationella intressena samt rättsstatens och dess institutioners stabilitet. Mycket av den övervakning som genomfördes i Spanien utfördes av CNI. CNI inrättades genom lag nr 11/2002 av den 6 maj 2002, som ger CNI befogenhet att genomföra ”säkerhetsutredningar” av ”individer eller enheter”[547]. Det finns dock få klargöranden om medlen eller begränsningarna för sådan verksamhet[548], då CNI:s verksamhet, liksom dess organisation och interna struktur, medel och förfaranden, personal, lokaler, databaser och datacentraler, informationskällor och information eller data som kan leda till kunskap om ovannämnda frågor, utgör sekretessbelagd information med relevant sekretessgrad[549]. Genom lag 11/2002 inrättades även parlamentarisk, verkställande och lagstiftande tillsyn över CNI[550]. Parlamentarisk tillsyn utförs av spanska parlamentets utskott för användning och kontroll av anslag till hemliga medel (kommittén för statshemligheter), som inrättades 1995[551]. På grund av kommitténs försenade sammansättning under det spanska parlamentets fjortonde mandatperiod (vald i december 2019) har kommittén för statshemligheter inte lämnat in sin årsrapport om CNI:s verksamhet, i enlighet med lagens krav. I april 2023 har ingen årsrapport lämnats in under denna mandatperiod.

---

[542] https://emad.defensa.gob.es/en/?__locale=en.
[543]Geneva Centre for Security Sector Governance report 2020, https://www.dcaf.ch/sites/default/files/publications/documents/ParliamentaryOversightMilitaryIntelligence_jan2021.pdf på sidan 40.
[544] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 5.5.
[545] https://www.guardiacivil.es/es/institucional/Conocenos/index.html.
[546] El Pais, https://english.elpais.com/spanish_news/2021-04-05/spanish-government-begins-reform-of-franco-era-official-secrets-law.html, 5 april 2021; Official Secrets Act of 1968.
[547] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 5.5.
[548] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4 maj 2022.
[549] Law 11/2002, of May 6, Regulating the National Intelligence Centre, artikel 5.1.
[550] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 11.
[551] Law 11/1995 May 11, https://www.boe.es/eli/es/l/1995/05/11/11/con .

Regeringens delegerade utskott för underrättelsefrågor samordnar underrättelseverksamheten inom alla spanska underrättelse- och informationsbyråer[552]. Slutligen utövar deputeradekongressens försvarskommitté tillsyn över CNI[553]. I det årliga underrättelsedirektivet fastställs prioriteringarna för CNI:s underrättelseverksamhet.

318. Den rättsliga kontrollen över CNI:s åtgärder föreskrivs i grundlag nr 2/2002 av den 6 maj 2002[554] [555], som kompletterar lag 11/2002 av den 7 maj 2002 som reglerar CNI. Enligt denna lag krävs särskilt att CNI:s statssekreterare, när CNI avser att genomföra övervakning, begär tillstånd från en behörig domare vid högsta domstolen, i enlighet med domstolsväsendets grundlag, att anta åtgärder som påverkar privatlivets okränkbarhet och sekretess för kommunikation[556], förutsatt att sådana åtgärder är nödvändiga för att CNI ska kunna fullgöra sina uppgifter. Dessutom föreskrivs i lagen att övervakningen inte får pågå längre än tre månader, och en förlängning av denna period måste motiveras vederbörligen. Dessa bestämmelser trädde dock i kraft i en tid då övervakningstekniken var betydligt mindre avancerad, och spionprogram såsom Pegasus och Candiru inte fanns. De rättsliga skyddsåtgärderna riskerar därför att bli föråldrade och ger inte medborgarna tillräckligt skydd. Därför tillkännagav regeringen att den skulle reformera CNI:s rättsliga ram, men inga förslag har ännu lagts fram.

EFTERHANDSGRANSKNING

319. Genom de lagar som inrättade CNI inrättades även deputeradekongressens försvarskommitté, som ansvarar för att anslå konfidentiella medel till CNI och utarbeta en årsrapport om CNI. De belopp som avsätts till hemliga medel fastställs i den spanska allmänna budgetlagen för varje budgetår[557]. Alla organ som har i uppdrag att utöva tillsyn över CNI, såsom försvarskommittén, kommittén för statshemligheter eller ombudsmannen, har fullständig tillgång till den information som krävs för att bedöma om verksamheten genomfördes på ett lagligt och korrekt sätt. Regeringen fastställer och godkänner årligen målen för CNI genom underrättelsedirektivet, som är hemligt[558] [559]. Direktören för CNI har exklusiv behörighet att fastställa syftet med och destinationen för de tilldelade medlen, och måste regelbundet rapportera om deras användning till premiärministern. Kommittén för statshemligheter är informerad om underrättelsemålen, har befogenhet att lämna in en årsrapport om underrättelsetjänsternas verksamhet[560]. Den har också tillgång till den årsrapport som

[552] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 6.
[553] Law 11/2002 May 6, https://www.global-regulation.com/translation/spain/1451143/law-11-2002%252c-6-may%252c-regulating-the-national-intelligence-centre.html artikel 11.
[554] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4 maj 2022.
[555] Organic Law 2/2002 May 6, https://www.global-regulation.com/translation/spain/1451142/law-2-2002%252c-6-may%252c-regulating-the-prior-judicial-control-of-the-national-intelligence-center.html.
[556] OMCT, https://www.omct.org/en/resources/urgent-interventions/state-surveillance-on-journalists-politicians-and-lawyers-in-spain, 4 maj 2022.
[557] Lag 11/1995 av den 11 maj 1995, som reglerar användningen och kontrollen av krediter som tilldelats hemliga medel, artikel 2, https://www.boe.es/eli/es/l/1995/05/11/11/con.
[558] Lag 11/2002 av den 6 maj som reglerar den nationella underrättelsetjänsten (CNI), artikel 3.
[559] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022, sidan 2.
[560] Lag 11/1995 av den 11 maj 1995, som reglerar användningen och kontrollen av krediter som tilldelats hemliga medel, artikel 7.4.

utarbetas årligen av direktören för CNI om bedömningen av verksamhet, status och grad av uppfyllande av målen. I den spanska lagstiftningen föreskrivs dock inte att offentlig tillgång ska beviljas till handlingar eller information som rör underrättelsetjänsternas arbete. Detta krav saknas också i synnerhet i den rättsliga ramen för lagen om öppenhet[561]. Med tanke på denna sekretess kan det inte med säkerhet fastställas om den spanska regeringen ingick avtal med NSO-koncernen eller om den förvärvade och använde Pegasus. De berörda personerna känner inte till orsakerna till, omfattningen av och konsekvenserna av avlyssningen av deras kommunikation[562].

320. Till följd av avslöjandet att CNI har använt Pegasus och Candiru inledde den spanska ombudsmannen en utredning på eget initiativ[563]. Den spanska ombudsmannen erkände i sitt officiella uttalande av den 18 maj 2022 att ministerrådet gav ombudsmannen fullständig tillgång till sekretessbelagda handlingar för granskning och inte utnyttjade sina befogenheter enligt artikel 22 i grundlag 3/1981 om ombudsmannen. Denna utredning gällde dock endast de 18 personer som de spanska myndigheterna har bekräftat utgjorde måltavlor med domstolstillstånd[564] [565]. Vid undersökningen drogs slutsatsen att de avlyssningar som gjorts var lagliga, eftersom det konstaterades att de hade godkänts av en domstol och att tillståndet åtföljdes av den nödvändiga motiveringen[566]. Ombudsmannen har dock inte behörighet att bedöma proportionaliteten. Detta kan endast fastställas av en domare[567]. Han kontaktade eller intervjuade inte heller någon av de berörda personerna eller deras advokater. Ombudsmannen rekommenderade vid behov en översyn av gällande rättsliga bestämmelser och reformer för att återspegla moderniseringen av övervakningssystemen[568]. Därefter meddelade den spanska regeringen i maj 2022 att det skulle genomföras en översyn av lagen om statshemligheter från 1968 och grundlagen om reglering av rättslig förhandskontroll av CNI (lag 2/2002)[569] [570], men ingen tidsram har fastställts för antagandet av denna översyn.

321. Kommittén för statshemligheter är skyldig att lämna in en årlig rapport om underrättelsetjänsternas verksamhet. Den sammankallades den 5 maj 2022 till följd av övervakningen av CNI, men detta var organets första möte på mer än tre år på grund av störningarna av parlamentets verksamhet till följd av covid-19-pandemin. Chef för CNI Paz Esteban framträdde inför kommittén och medgav att 18 ledare för separatiströrelsen

---

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

[567] Information från uppdraget i Spanien.
[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 maj 2022.
[570] https://www.lamoncloa.gob.es/lang/en/presidente/news/Paginas/2022/20220526_appearance.aspx, den 26 maj 2022.

hade övervakats. Hon ingav även domstolsbesluten för dessa 18 fall till kommittén[571] [572]. Utfrågningen skedde dock bakom slutna dörrar i enlighet med artikel 5.5 i lag 11/2002 och de närvarande fick inte komma in med elektronisk utrustning av något slag[573]. Ingen officiell information offentliggjordes utöver antalet fall. Enligt de talespersoner som närvarade vid utfrågningen låg fokus nästan uteslutande på de katalanska offren och inte på Pedro Sánchez eller Margarita Robles och de påstådda 3 GB data som togs från deras utrustning av legosoldatspionprogram[574]. Robles har upprepade gånger insisterat på att övervakningen av de 18 katalanska målen var motiverad.

322. Sánchez har också talat om frågan i det spanska parlamentet, där han än en gång upprepade att allt har skett inom lagens ramar och att den nationella säkerheten står under tillsyn av det spanska parlamentet och andra statliga organ[575]. Tidigare verkställande direktören för NSO Group, Shalev Hulio, hävdade också att användningen av Pegasus var helt laglig när han sade till *New Yorker* att Spaniens användning av Pegasus var laglig mot bakgrund av Spaniens stora respekt för rättsstaten och kravet på tillstånd från högsta domstolen[576].

323. Den 3 maj 2022 röstade den spanska kongressen ned ett förslag om att inrätta en utredningskommitté om användningen av Pegasus. Den 21 september 2022 tillsatte Kataloniens parlament en undersökningskommitté om spionage av politiska företrädare, aktivister, journalister och deras familjer av Spanien med hjälp av programmen Pegasus och Kandiru.

OFFENTLIG GRANSKNING

324. Sedan avslöjandena i april 2022 har det förekommit en betydande offentlig granskning av användningen av spionprogram mot personer i den spanska regeringen och förespråkare för ett självständigt Katalonien. De spanska medierna och mediekanaler runtom i världen har arbetat intensivt tillsammans med det civila samhällets organisationer för att granska övervakningssystemet i Spanien och förespråka de övervakade personernas grundläggande rättigheter. Omvänt har vissa spanska politiker försökt misskreditera Citizens Lab och antytt att deras metoder är osunda eller att de är politiskt motiverade.

RÄTTSMEDEL

325. Ett rättsfall om övervakning av premiärminister Pedro Sánchez och försvarsminister

---

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

Margarita Robles med hjälp av spionprogram ingavs av den spanska riksåklagaren[577] i Madrids spanska nationella domstol (SNC), Audiencia Nacional. SNC:s behörighet fastställs i artikel 65.1 a i grundlagen om domstolsväsendet 6/1985, eftersom de påverkar högt uppsatta nationella organ, såsom premiärministern och statsministern. Domare José Luis Calama, chef för den centrala förundersökningsdomstolen nummer 4, ansvarar för detta pågående mål[578]. Den 13 oktober 2022 överlämnade domare Calama ett frågeformulär till både Robles och Grande-Marlaska, som innehöll en begäran, som skulle bekräftas av rättsliga källor, om hur Pegasus-infektionerna identifierades. Åklagarmyndigheten och riksåklagarens kontor skickade också frågor till ministrarna[579].

326. Rättsfall om övervakning med hjälp av spionprogram har ingetts till undersökningsdomstolen i Barcelona av personer med direkt eller indirekt anknytning till den katalanska självständighetsrörelsen, och utredningar pågår, om än i långsam takt. Det första klagomålet ingavs 2020 av ordföranden för Kataloniens parlament och nuvarande ministern för näringsliv och arbete, Roger Torrent, och f.d. ministern för utrikesfrågor, institutionella förbindelser och öppenhet i Katalonien och nuvarande ordförande för Kataloniens republikanska vänster i kommunfullmäktige i Barcelona, Ernest Maragall, [580] [581]. Ärendet tilldelades undersökningsdomstol nr 32 i Barcelona som preliminärt avslutade målet. Andreu Van den Eynde är en av de advokater som företräder Torrent och Maragall i det här målet och har själv varit måltavla för Pegasus. Van Den Eynde har konsekvent kritiserat domstolarna för att fördröja förfarandet och praktiskt taget ”förlama” målet[582]. Omnium Cultural och den katalanska nationalförsamlingen (ANC), såväl som Candidatura d’Unitat Popular (CUP), har också lämnat in flera brottsanmälningar vid samma domstol i Barcelona, men ingen utredning har ännu inletts. Undersökningsdomstol nr 32 i Barcelona avvisade begäran om att samla rättsprocesserna, så de behandlas nu av olika domstolar och domare. Klagomålen från Omnium Cultural och CUP tilldelades undersökningsdomstol den 21 april 2022 och målen från den katalanska nationalförsamlingen (ANC) tilldelades domstol 23 den 26 juli 2022. Klagomålen har ännu inte tillåtits att gå vidare fullt ut, och man har inte heller enats om att inleda en undersökning, så inget av dessa fall utreds för närvarande. De flesta fallen har skjutits upp av domarna tills fler bevis har samlats in, eftersom de viktigaste bevisen – de påstått infekterade mobiltelefonerna – inte längre var i klagandenas ägo[583]. Domarna kan besluta att godta Citizen Labs utlåtanden som expertbevisning i målet. Men om domarna inte tillåter detta gör det svårt för de berörda personerna att bevisa sin sak[584].

---

[577] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 maj 2022.
[578] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 maj 2022.
[579] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 maj 2022.
[580] El Nacional, https://www.elnacional.cat/en/politics/catalangate-hands-judge-spain-national-audience_750840_102.html, 2 maj 2022.
[581] El Diario, https://www.eldiario.es/catalunya/juez-archiva-investigacion-espionaje-pegasus-torrent-maragall_1_9030414.html, 30 maj 2020.
[582] El Diario, https://www.eldiario.es/catalunya/investigacion-espionaje-independentismo-divide-languidece-juzgados_1_9037282.html, 30 maj 2022.
[583] El Pais, 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 maj 2022.
[584] Uppdrag i Spanien.

327. Eftersom SNC har behörighet i hela Spanien i de allvarligaste brottsärendena, kan åklagaren begära att alla Pegasusärenden ska samlas[585]. Med andra ord skulle alla personer som övervakats av den spanska regeringen och målen i ”CatalanGate” höras i SNC i Madrid. De advokater som företräder de katalanska offren hävdar att det inte finns något samband mellan fallen om inte gärningsmannen bevisas vara densamma i alla fall av övervakning[586].

328. Det finns ett antal andra pågående rättsfall kopplade till de 65 katalanska offren. Ett sådant mål ingavs av advokaten och måltavlan för övervakning med Pegasus Gonzalo Boye för minst 19 personer som utsatts för övervakning mot NSO, dess tre grundare Niv Karmi, Shalev Hulio och Omri Lavie, Q Cyber Technologies och OSY, ett dotterbolag med säte i Luxemburg[587] [588]. Quim Torra, tidigare president i Katalonien, och Josep Costa, tidigare vice ordförande för det katalanska parlamentet, har lämnat in en ansökan till högsta domstolen, men ett år senare har domstolarna fortfarande inte avgjort om målet ska prövas inför högsta domstolen eller den spanska nationella domstolen. Under tiden ingen utredning utförts. Rättsliga åtgärder pågår också i Frankrike, Belgien, Schweiz, Tyskland och Luxemburg avseende övervakning av katalanska separatister i exil [589].

MÅLTAVLORNA

329. Övervakningen av medlemmar i den katalanska självständighetsrörelsen och deras familj och personal med spionprogram började redan 2015, då den dåvarande ordföranden för den katalanska nationalförsamlingen (ANC), Jordi Sánchez, övervakades kort efter en stor demonstration i Barcelona. Enligt Citizen Lab-rapporten från april 2022 övervakades minst 65 personer med spionprogram mellan 2017 och 2020: 63 med Pegasus, fyra med Candiru och minst två med båda[590]. Minst 51 individers enheter infekterades[591]. Bland dem som påstås har blivit utsatta, direkt eller indirekt, fanns politiska personer som var för Kataloniens självständighet, såsom regionministern för näringsliv och arbete och f.d. talman i det katalanska parlamentet, Roger Torrent, den nuvarande ordföranden för Kataloniens republikanska vänster i kommunfullmäktige i Barcelona och tidigare minister för utrikesfrågor, institutionella förbindelser och öppenhet i Katalonien, Ernest Maragall, och fyra av Europaparlamentets ledamöter. Med tanke på den betydande tid som passerat sedan hackningen inleddes och dessa avslöjanden gjordes kunde ett antal måltavlor inte identifieras eller undersökas ytterligare på grund av olika faktorer, däribland ett antal

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

måltavlor som gjort sig av med telefonen i fråga[592].

330. Spaniens premiärminister Pedro Sánchez, försvarsminister Margarita Robles och inrikesminister Fernando Grande-Marlaska blev offer för Pegasus mellan maj och juni 2021[593]. Hittills finns det inte mycket information tillgänglig om detaljerna i denna hackning, eftersom de tillkännagavs av regeringen och inte var resultatet av en utredning av Citizen Lab eller någon annan sådan forskningsavdelning eller utredande journalister och fortfarande är föremål för en pågående utredning. Sánchez och Robles är chefer för de två regeringsgrenar som övervakar CNI, det organ som ansvarar för övervakningen i Spanien. Sánchez och Robles smittade enheter hade utfärdats av regeringen och då och då scannats för spionprogram[594]. Grande-Marlaskas personliga enhet infekterades[595]. Jordbruksminister Luis Planas, som tidigare tjänstgjort som diplomat i Marocko, var också måltavla för spionprogram, men försöken till infektion lyckades inte. Det har rapporterats att den marockanska regeringen potentiellt skulle kunna vara ansvarig för denna övervakning. Emellertid har ingen sådan information bekräftats[596].

331. Av de 65 fallen medgav de spanska myndigheterna att man hade avlyssnat 18 personer, men regeringen har inte kommenterat de återstående 47 fallen[597]. Det är fortfarande oklart om de andra personerna avlyssnades av CNI enligt ett domstolsbeslut eller om någon annan myndighet hade fått domstolsbeslut om att avlyssna dem. Trots domstolsbeslut om användning av spionprogram på 18 personer åtalades dessa därefter inte för ett brott med anknytning till det domstolsbeslut som tillät användning av spionprogram. Bland de mål för vilka övervakning hade godkänts ingick den nuvarande presidenten för Katalonien Pere Aragonès, den tidigare presidenten och den nuvarande europaparlamentsledamoten Carles Puigdemont samt andra politiker och medarbetare i den katalanska självständighetsrörelsen[598]. Om inte annat följer av lagens krav på sekretess och konfidentalitet har försvarsminister Robles hänvisat till lagen om statshemligheter för att inte utveckla skälen till övervakningen av dessa specifika mål[599]. De flesta av dessa 65 katalanska offer har någon gång varit i kontakt med de medlemmar av den katalanska självständighetsrörelsen som bor utanför Spanien. Vissa av de berörda personerna befann sig utanför Spanien när angreppet ägde rum, bland annat i Belgien, Schweiz, Tyskland och Frankrike. En sådan digital övervakning skulle vara olaglig i Tyskland, om inte de federala myndigheterna uttryckligen tillåter det.

332. En av de viktigaste grupper som visat sig vara måltavlor är separatistiska katalanska ledamöter av Europaparlamentet. De har samtliga hackats med hjälp av spionprogram

---

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

antingen direkt eller indirekt genom vad Citizen Lab kallar relationsmålinriktning[600]: Diana Riba i Giner, Jordi Solé, Carles Puigdemont och Clara Ponsati. En mobiltelefon som tillhörde en tidigare ackrediterad assistent till Ponsatí infekterades med Pegasus. I fallet med Antoni Comin, som anklagade den spanska staten för att ha spionerat på honom under en utfrågning i PEGA-kommittén, erkände Citizen Lab att infektionen felaktigt hade kopplats till honom på grund av ett fel vid märkningen med initialer.

333. En telefon som tillhör Diana Riba i Giner, ledamot av Europaparlamentet för Kataloniens republikanska vänster (ERC), infekterades direkt med Pegasus spionprogram den 28 oktober 2019, endast tre månader efter att hon hade tillträtt sin plats i parlamentet. När hon diskuterade med sin assistent i telefon avbröts kommunikationen och hennes assistent hörde en inspelning av det samtal hon precis hade haft med Riba i Giner. Tidpunkten för denna infektion sammanföll direkt med ett avgörande domstolsbeslut om de katalanska separatisterna, varav en är Raül Romeva, make till Riba i Giner, som slutligen dömdes till 12 års fängelse[601]. Riba i Giner beskrev vid en utfrågning av PEGA-kommittén i Europaparlamentet att de flesta hennes telefonsamtal vid den tidpunkten handlade om domstolsmålet och att hon genomförde otaliga möten och besök i domstolarna. Bifångsten i detta fall var därför oerhört betydelsefull, inklusive Romeva och de som var kopplade till det historiska fallet[602].

334. Jordi Solé, även han ledamot av Europaparlamentet för ERC, rapporterades ursprungligen ha hackats både den 11 juni och den 27 juni 2020 enligt Citizen Labs forskning[603]. Fem ytterligare attacker under samma period upptäcktes dock senare[604]. Solé upptäckte först att han hade blivit måltavla för Pegasus av en tillfällighet när han, efter att ha mottagit några potentiellt misstänkta meddelanden, lämnade in sin telefon för granskning i samband med en dokumentär[605]. Som i fallet med hans kollega är tidpunkten då han blev måltavla värd att notera. Den sammanföll med viktiga politiska diskussioner om den lediga platsen för Oriol Junqueras, som inte fick tillstånd att tillträda sin post som ledamot av Europaparlamentet när han satt fängslad i Spanien[606], och endast en månad innan Solé utsågs till att ta över den platsen i juli 2020. Dessutom fördes vid tiden för infektionerna diskussioner om partistrategi och internationella rättstvister om deras fängslade och landsflyktiga kolleger[607].

335. Carles Puigdemont, ledamot av Europaparlamentet för JUNTS och tidigare president i Katalonien blev avlyssnad genom sin maka Marcela Topor, sina anställda och ett antal

---

[600] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 6.
[601]Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Ms. Diana Riba i Giner MEP, Strasbourg 6 October 2022.
[602]Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware hearing testimony of Ms. Diana Riba i Giner MEP, Strasbourg 6 October 2022.
[603] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 7.
[604] Undersökningskommittén för utredning av användningen av Pegasus och liknande spionprogram, vittnesmål från Jordi Sole, ledamot av Europaparlamentet, Strasbourg, 6 oktober 2022.
[605] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[606] Undersökningskommittén för utredning av användningen av Pegasus och liknande spionprogram, vittnesmål från Jordi Sole, ledamot av Europaparlamentet, Strasbourg, 6 oktober 2022.
[607] Politico, https://www.politico.eu/article/oriol-junqueras-barred-from-european-parliament-seat/, 9 januari 2020.

av sina bundsförvanter[608]. Totalt rapporterar Citizen Lab att upp till elva personer i nära kontakt med Puigdemont var måltavlor, inklusive minst två bekräftade infektioner på Marcela Topors enhet den 7 oktober 2019 och 4 juli 2020[609].

336. Clara Ponsatí, ledamot av Europaparlamentet för JUNTS och tidigare utbildningsminister i Katalonien var också offer för relationsmålinriktning. Pol Cruz, en anställd vid europaparlamentet, bekräftades ha infekterats den 7 juli 2020[610].

337. Alla Kataloniens presidenter sedan 2010 har varit utsatta för spionprogram antingen under eller efter sin mandatperiod[611]. Så många som 12 medlemmar ur Kataloniens republikanska vänster var bland de 65 målen, däribland partiets generalsekreterare Marta Rovira som hackades minst två gånger i juni 2020 enligt Citizen Lab. Det är av stor betydelse att både Gabriel och Rovira bodde i Schweiz vid tidpunkten för övervakningen efter resultatet av folkomröstningen 2017.

CIVILA MÅL, INKLUSIVE JOURNALISTER, ADVOKATER OCH FÖRETRÄDARE FÖR DET CIVILA SAMHÄLLET

338. Jordi Domingo var en av de första katalanska aktivisterna som enligt uppgift var måltavla under 2020. Även om han stödde katalansk självständighet och var medlem av den katalanska nationalförsamlingen (ANC), rapporterades det av *the Guardian* att Domingo trodde sig vara en felaktig måltavla. Eftersom han inte spelade någon större roll i händelserna 2017 anser han att det avsedda målet var en advokat med samma namn som bidrog till utarbetandet av en konstitution för ett självständigt Katalonien[612].

339. Den katalanska nationalförsamlingen (ANC), en katalansk civilsamhällesorganisation som stöder katalansk självständighet, var en av de första organisationer som utsetts till måltavla före folkomröstningen i Katalonien, och har sedan dess varit mål för omfattande övervakning[613]. De sex målen från ANC är två av ANC:s tidigare ordförande, Jordi Sanchez (2015–2017) och Elisenda Paluzie (2018–2022), vars övervakning med spionprogram beviljades genom domstolsbeslut, en expert på digital röstning och decentralisering (Jordi Baylina), två ledamöter av dess nationella styrelse (Arià Bayè och Sònia Urpí) och en medlem av en lokal avdelning (Jordi Domingo).

340. Enheter tillhörande personer nära Jordi Cuixart, ordförande för Òmnium Cultural (fram till februari 2022) infekterades, eftersom han satt fängslad vid tillfället. Bland dessa var Marcel Mauri som tjänstgjorde som vice ordförande för den icke-statliga organisationen. Övervakningen med spionprogram beviljades genom domstolsbeslut.

341. Citizen Lab upptäckte en aktiv Candiru-infektion på den bärbara dator som tillhörde

---

[608] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 7.
[609] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 8.
[610] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ 18 april 2022 på sidan 7.
[611] Artur Mas (efter det att han lämnat sitt ämbete), Carles Puigdemont (relationsmålinriktning), Joaquim Torra (medan han innehade sitt ämbete), Pere Aragones (smittad medan han var Torras vicepresident). 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 juli 2020.
[613] Citizen Lab's CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/.

Joan Matamala, en affärsman och aktivist med nära band till separatistiska katalanska politiker, i februari 2021[614]. Övervakningen av Matamala med spionprogram beviljades genom domstolsbeslut. Candiru är betydligt svårare att spåra än Pegasus, och upptäckten av en aktiv infektion gjorde det möjligt för forskarna i Citizen Lab att bättre förstå dess mönster. Därefter upptäcktes 16 andra infektioner på Matamalas enhet[615]. Microsoft åtgärdade sedan säkerhetsproblemen genom uppdateringar, men det är omöjligt att veta hur många Candiru-infektioner som inte har upptäckts[616].

342. Minst tre kända utvecklare och entreprenörer inom öppen källkod var måltavlor för Pegasus. Xavier Vives och Pau Escrich, medgrundare av Vocdoni, ett protokoll med öppen källkod baserat på Ethereums blockkedja för säker, censurresistent elektronisk röstning, var båda måltavlor. Vives var särskilt måltavla för den skadliga programvaran Candiru, medan Escrich var måltavla för både Pegasus och Candiru[617]. Övervakningen av Vives och Escrich beviljades genom domstolsbeslut.

343. Gonzalo Boye är advokat för före detta presidenterna Puigdemont och Torras[618]. Under fem månader mellan januari och maj 2020 avlyssnades Boye så många som 18 gånger via textmeddelanden som framstod som tweets från det civila samhällets organisationer eller framstående nyhetskanaler[619]. Citizen Lab bekräftade minst en lyckad infektion den 30 oktober 2020. Infektionen kom bara 48 timmar efter gripandet av en av hans klienter[620]. Att Boye blev ett av offren gör att lagligheten i att angripa sekretessen mellan advokat och klient ifrågasätts.

344. Elena Jimenez, den internationella representanten för Òmnium Cultural, och Jordi Bosch, den advokat som ansvarar för Òmnium Culturals institutionella relationer, var båda måltavlor för Pegasus medan de tjänstgjorde i Jordi Cuixarts juridiska team. Jimenez hade ständig kontakt med Cuixarts fullständiga juridiska team, inklusive det internationella team som förberedde ett klagomål för Europadomstolen. Hittills har Citizen Lab endast undersökt Jimenez senaste inskaffade mobiltelefon, men de har bekräftat en framgångsrik nollklickinfektion i februari 2020. Bosch, som är en av de mindre offentliga personerna i det juridiska teamet, blev måltavla i juli 2020, mindre än en vecka innan Cuixart beviljades en mildare form av frihetsberövande och samma dag som han uppträdde i katalansk tv för Òmniums räkning för första gången.

345. Andreu van den Eynde i Adroer infekterades framgångsrikt med Pegasus den 14 maj 2020[621]. Hackningen inträffade när han agerade som advokat för både Raúl Romeva och Oriol Junqueras i deras mål inför högsta domstolen.

346. På samma sätt infekterades också advokaten Jaume Alonso-Cuevillas enhet när han

[614] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[615] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[616] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 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] Citizen Lab CatalanGate Report, https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/, 18 april 2022 på sidan 10.

företrädde katalanska nyckelpersoner som Carles Puigdemont. Citizen Lab kunde dock inte fastställa exakt datum för den lyckade infektionen.

UTREDNINGAR OCH LAGSTIFTNINGSREFORMER

347. Efter att anklagelserna i fallet ”Catalangate” avslöjades den 22 april 2022 inledde de spanska institutionerna ett förfarande för tillsyn som syftade till att säkerställa att riktlinjerna för övervakning hade tillämpats korrekt. Dessa åtgärder inbegrep att Paz Esteban, direktören för CNI, kallades till kommittén för statshemligheter den 5 maj, vilket tillkännagavs av Félix Bolaños, minister för presidentskapet, sammanträdet för parlamentarisk kontroll av regeringen och försvarsministern den 26 och 27 april samt ombudsmannens oberoende utvärdering, som inleddes den 26 april och avslutades den 18 maj. Försvarsminister Margarita Robles, som enligt lagen om officiella hemligheter förbjuds att lämna ut konfidentiell information, antydde att de åtgärder som hade vidtagits var ett svar på handlingar från dem som bryter mot konstitutionen, tar över den offentliga infrastrukturen, stör den allmänna ordningen och har kopplingar till de politiska ledarna i ett land som invaderar Ukraina[622]. Regeringens parti (PSOE) och de tre största oppositionspartierna (PP, Vox och Cs) rapporterade att direktören hade lämnat tillfredsställande förklaringar om nödvändigheten och lagligheten av de åtgärder som vidtogs[623] [624].

348. Den spanska ombudsmannen medgav att en stor del av den övervakning som genomfördes av CNI i Spanien skedde med full respekt för de rättsliga förfarandena. I enlighet med hans rekommendationer om tillräckliga parlamentariska och rättsliga kontroller och för att uppdatera lagstiftningen, stärka garantierna för rättslig kontroll och säkerställa största möjliga respekt för enskilda personers grundläggande rättigheter, åtog sig den spanska verkställande makten att

1. utlysa en intern utredning inom CNI,

2. inleda en utredning inom kommittén om användningen och kontrollen av anslag som avsatts för den spanska kongressens hemliga fonder och en utfrågning där direktören för CNI ska framträda, och

3. offentliggöra för kommittén, om användningen och kontrollen av anslag som avsatts till hemliga fonder i den spanska kongressen vid Högsta domstolen, 18 beslut om att tillåta intrången, liksom att häva sekretessen för CNI-handlingar som rör de medlemmar av den katalanska självständighetsrörelsen som utsetts till måltavlor, på begäran av en domare,

4. reformera den spanska lagen om officiella hemligheter från 1968[625],

[622] El Pais, 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 april 2022.
[623] La Vanguardia, https://www.lavanguardia.com/politica/20220505/8245084/cni-aporta-autorizaciones-judiciales-parte-espionaje-catalangate.html, 5 maj 2022.
[624] El Periodico de Espana, https://www.epe.es/es/politica/20220505/frente-comun-pp-vox-cs-13614030, 5 maj 2022.
[625] El País, ‘El Gobierno inicia la reforma de la ley franquista de secretos oficiales’, 5 april 2021.

5. reformera den rättsliga ramen för CNI[626],

6. godkänna ett nytt underrättelsedirektiv där CNI:s underrättelsemål fastställs, och

7. uppdatera 2021 års nationella säkerhetsstrategi och cybersäkerhetsplanen.

349. Spaniens högsta domstol[627] inledde sin egen utredning efter att regeringen sagt att Pegasus-programvaran hade använts för att spionera på ministrar, däribland premiärminister Sanchez. Som en del av en så kallad utredningskommission för att utreda spioneriet kallade domstolen den verkställande direktören för det israeliska företag som står bakom spionprogrammet Pegasus, NSO Group, och ministern Felix Bolaños för att vittna. Utredningsdomaren intervjuade också Paz Esteban, den tidigare chefen för den nationella underrättelsetjänsten[628] [629], samt försvars- och inrikesministrarna, vars enheter var bland dem som hackades. Domstolen[630] skickade en formell begäran om internationell rättslig hjälp till den israeliska regeringen och bad om information om olika aspekter av programvaruverktyget. Högsta domstolen har också hävt sekretessen för de dokument som rör fallet och upphävt förbudet mot att utreda avlyssning av de mobiltelefoner som tillhör premiärminister Pedro Sánchez och försvarsminister Margarita Robles.

AVSLUTANDE KOMMENTARER

350. Spanien har ett oberoende rättssystem med tillräckliga rättssäkerhetsgarantier. Efter upptäckten av de två kategorierna av mål i Spanien kvarstår dock vissa frågor som skulle kunna besvaras genom snabba och djupgående reformer och ett effektivt genomförande av dessa. Den spanska regeringen arbetar med ändringar för att ta itu med brister. När det gäller reformen av CNI tillkännagav den spanska regeringen sin avsikt den 26 maj 2022 att reformera CNI:s rättsliga ram, men inget förslag har ännu ingivits. Den 1 augusti 2022[631] lade regeringen fram ett ändringsförslag till lagen om statshemligheter. Regeringen väntar för närvarande på yttrandet från Högsta förvaltningsdomstolen.

351. De 47 personer som avlyssnats enligt uppgift i rapporten from Citizen Lab, där det fortfarande är oklart om CNI hade beviljats domstolsbeslut eller om någon annan myndighet hade mottagit ett domstolsbeslut om att lagligen avlyssna dem, känner inte till skälen till, omfattningen av eller aktörerna bakom avlyssningen med Pegasus. Dessa personer bör ha tillgång till rättslig prövning och en utredning bör inledas för att belysa dessa fall.

---

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

352. När det gäller de 18 fall för vilka ett domstolsbeslut hade utfärdats har deras laglighet verifierats och bekräftats av ombudsmannen, men deras särskilda karaktär, tillräcklighet, exceptionella karaktär, proportionalitet och nödvändighet[632] kan endast prövas av en domstol.

353. Mer allmänt går de rättsliga förfarandena för de berörda personerna inte så snabbt som man hade hoppats i syfte att skapa insyn och tillgång till meningsfulla rättsmedel. Här är det viktigt att myndigheterna samarbetar. För att skapa större klarhet och bidra med teknisk expertis skulle Europol kunna bjudas in och tillhandahålla stöd för att säkerställa att ett lämpligt utredningsförfarande följs.

Övriga medlemsstater

NEDERLÄNDERNA

354. I koalitionsavtalet från 2017 från den nederländska regeringen anges att den nederländska polisen inte får förvärva spionprogram från leverantörer som tillhandahåller sina produkter till ”tvivelaktiga regimer”, som senare specificeras som ”länder som gjort sig skyldiga till allvarliga kränkningar av de mänskliga rättigheterna eller internationell humanitär rätt”. Före varje förvärv av spionprogram måste den nederländska polisen fråga leverantören om den har tillhandahållit spionprogram till länder som sanktionerats av antingen EU eller FN och utföra en kontroll om det land där leverantören är baserad har ett exportkontrollsystem där de mänskliga rättigheterna bedöms i exportlicensförfarandet. Denna bedömning upprepas regelbundet. Det bör noteras att denna begränsning endast verkar gälla polisens förvärv av spionprogram. Underrättelsetjänsten nämns inte uttryckligen. Enligt regeringen har polisen använt hackningsprogramvara sedan 2019, även om myndigheterna inte nämner vilken typ[633]. Det verkar som om NSO Group och dess spionprogramsprodukt Pegasus inte uppfyller ovannämnda standarder, i alla händelser inte innan Israels exportsystem skärptes i december 2021[634]. Varken polisen eller underrättelsetjänsten har gett några upplysningar om utgifterna för inköp och användning av spionprogram.

355. I Nederländerna inrättades ett nytt organ (Toetsingscommissie Inzet Bevoegdheden, TIB) 2018 för att i förväg bedöma lagenligheten av regeringens tillstånd till underrättelsetjänsterna att använda övervakningstekniker. Övervakningen kan inte inledas om TIB bedömer att tillståndet är olagligt. TIB kompletterar det huvudsakliga tillsynsorganet, övervakningskommittén för underrättelse- och säkerhetstjänster (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD). CTIVD övervakar underrättelsetjänsternas pågående övervakningsverksamhet efter det att tillståndet har beviljats och hanterar klagomål.

356. Det bör noteras att NSO Group under perioden november 2014 till december 2016 kunde bedriva sin verksamhet tack vare två företag, Shapes 1 BV och Shapes 2 BV, som är etablerade i Nederländerna, inom sektorerna ”finansiella holdingbolag” respektive ”ingenjörer och annan teknisk design och rådgivning”. Båda likviderades

[632] Artikel 588 a. i., fjärde kapitlet, straffprocesslagen.
[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.

efter två verksamhetsår[635].

357. Den 4 oktober 2022 avslöjades det att det nederländska försvarsministeriet i november 2019 höll på att underteckna ett avtal med WiSpear, det företag som ägs av Tal Dilian, som tidigare hade förvärvat Cytrox, tillverkaren av spionprogram från Predator[636]. WiSpear hade vunnit ett anbud från det nederländska ministeriet. Det framgår inte klart av e-postväxlingen om det gäller Predator eller en annan produkt. Av de e-postmeddelanden som offentliggjorts av det cypriotiska ministeriet för energi, handel och industri och WiSpear framgår det tydligt att en företrädare för det nederländska försvarsministeriet hade kontaktat det cypriotiska handelsministeriet för att få försäkringar om WiSpear den 13–15 november 2019, bara dagar innan historien om Dilians ”spionbil” kom ut. Dilian informerade företrädaren för det cypriotiska handelsministeriet om att han skulle uppskatta hennes omedelbara hjälp i ärendet eftersom tidsfristen för undertecknande av kontrakt snart löpte ut[637]. Det är oklart om kontraktet undertecknades och spionprogram levererades till det nederländska försvarsministeriet.

358. I Nederländerna finns också ett dotterbolag till Cognyte som är registrerat som Cognyte Netherlands B.V. Som framgår av ett utdrag från den nederländska handelskammaren är Cypernbaserade UTX Technologies den enda aktieägaren i det nederländska dotterbolaget. Såsom beskrivs i kapitlet om Cypern och spionprogramsindustrin har UTX Technologies tidigare exporterat underrättelse- och spårningssystem till Bangladesh och levererat övervakningssystem till EU:s medlemsstater. Dessutom var det israeliska företaget Verint – som också ägde Cognyte före avknoppningen 2021 – den huvudsakliga leverantören av övervakningssystemet till den nederländska polisen[638]. Förbindelserna mellan polisen och denna israeliska leverantör blir ännu tydligare när vi ser att den tidigare polisen Robert van Bosbeek har tagit på sig rollen som direktör för Cognyte Netherlands B.V. sedan 2014[639]. En annan direktör på detta nederländska dotterbolag, David Abadi, är också ekonomichef för israeliska Cognyte Software Ltd som har kopplingar till försäljningen av spionprogram för avlyssning till Myanmar[640].

359. Den 2 juni 2022 rapporterade medierna att den nederländska underrättelsetjänsten Algemene Inlichtingen- en Veiligheidsdienst (AIVD) använde Pegasus när den hjälpte polisen att spåra en misstänkt i ett allvarligt brott, Ridouan T, som blev huvudmisstänkt i flera mord med anknytning till organiserad brottslighet, narkotikahandel och ledare för en kriminell organisation, och greps den 16 december 2022 i Dubai[641]. Den nederländska regeringen vägrade att lämna kommentarer. Detta är ett anmärkningsvärt fall som förtjänar att uppmärksammas närmare. Läckorna inträffade vid en tidpunkt då Pegasus och NSO Group fick mycket offentlig kritik och USA:s handelsdepartements svartlistning skadade NSO Group ekonomiskt. Den nederländska framgångssagan om att fånga en person som varit en av de mest efterlysta brottslingarna på åratal var ett

[635] Amnesty International, ”Operating from the Shadows: Inside NSO Group’s Corporate Structure”, https://www.amnesty.org/en/documents/doc10/4182/2021/en/.
[636] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/.
[637] https://oparatiritis.com.cy/2022/10/04/e-mail-wispear-disy-netherlands/.
[638] Volkskrant: ”Achterdeur in het nationale aftapsysteem van de politie, Israëli’s konden meeluisteren”.
[639] Kamer van Koophandel: Bedrijfsprofiel - Cognyte Netherlands B.V. (34139430).
[640] Reuters: ”Israel’s Cognyte won tender to sell intercept spyware to Myanmar before coup, documents show”.
[641] https://www.volkskrant.nl/nieuws-achtergrond/aivd-gebruikt-omstreden-israelische-hacksoftware~b05a6d91/.

välkommet positivt budskap för företaget. Mediarapporten bygger på uttalanden från fyra källor inom AIVD. Deras motiv för läckan nämns inte i rapporten. Det verkar inte heller ha gjorts någon utredning av dessa läckor, vilket väcker frågan om läckan hade godkänts av AIVD:s ledning. Det är dock högst osannolikt att AIVD skulle tillåta att en sådan historia kommer ut utan de israeliska myndigheternas kännedom och godkännande.

BELGIEN

360. I en intervju med The New Yorker avslöjade en före detta israelisk underrättelsetjänsteman att den belgiska polisen använder Pegasus i sin verksamhet[642]. Som svar uppgav den belgiska polisen att den ”inte kommunicerar om någon teknik eller tekniska hjälpmedel som används för utredningar och uppdrag”. I september 2021 nämnde justitieminister Vincent Van Quickenborne att Pegasus ”kan användas på ett lagligt sätt” av underrättelsetjänsten, men ville inte bekräfta om den belgiska underrättelsetjänsten är kund till NSO eller använder någon spionprogramvara mot brottslingar[643].

361. El Mahjoub Maliha, människorättsförsvarare från Västsahara med säte i Belgien, och Carine Kanimba, dotter till den rwandiska politiska aktivisten Paul Rusesabagina, har också spionerats på med hjälp av Pegasus-programvara i Belgien, till och med under möten med belgiska regeringstjänstemän. Spionprogramsattackerna utfördes med största sannolikhet av de marockanska respektive de rwandiska myndigheterna eller på deras vägnar. Rwanda anklagas också för att använda Pegasus spionprogram för att göra kritiker som lever i belgisk exil till måltavlor, däribland de framstående oppositionsfigurerna Placide Kayumba och David Batenga[644]. Den belgiska militära underrättelsetjänsten ADIV upptäckte vidare att Pegasus med största sannolikhet hade installerats av Rwanda på den smarttelefon som tillhörde den Kagame-kritiska belgiska journalisten Peter Verlinden och hans fru Marie Bamutese[645]. Andra belgiska måltavlor för användningen av spionprogram omfattar tidigare premiärminister Charles Michel och hans far Louis Michel (då ledamot av Europaparlamentet, tidigare ledamot av kommissionen och utrikesminister). Enligt de belgiska medierna låg den marockanska regeringen bakom attackerna[646].

TYSKLAND

362. Tyska enheter som använder sig av hackning är Bundesnachrichtendienst, den federala underrättelsetjänsten eller BND, militären, tullen och polisen. BND är den byrå som använder sig mest av hackning. År 2009 hade de redan övervakat 2500 enheter[647].

363. Det finns en rättslig ram som reglerar användningen av spionprogram i Tyskland. Sedan

---

642 https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens.
643 https://www.tijd.be/politiek-economie/belgie/algemeen/van-quickenborne-duldt-gebruik-controversiele-spionagetool-pegasus/10329450.html.
644 https://www.ft.com/join/licence/88bec95c-78fd-4030-9526-a95fbdeb9da8/details?ft-content-uuid=d9127eae-f99d-11e9-98fd-4d6c20050229.
645 https://www.vrt.be/vrtnws/nl/2021/09/17/pegasus-spionageware-op-de-telefoon-van-journalist-peter-verlind/.
646 https://www.knack.be/nieuws/wereld/belgisch-slachtoffer-van-pegasus-spyware-mijn-leven-is-in-gevaar/; https://www.knack.be/nieuws/pegasus-project-macron-en-michel-in-het-vizier-van-marokko/.
647 Europaparlamentet. Germany Hearing; https://www.spiegel.de/netzwelt/web/online-durchsuchung-bnd-infiltrierte-tausende-computer-im-ausland-a-611954.html.

2008 ger den tyska förbundslagen polisen befogenheter att använda statlig hackning vid fall av internationell terrorism och för förebyggande av terroristattacker[648]. År 2017 trädde en ny lag i kraft, som gjorde det möjligt för alla brottsbekämpande myndigheter att använda sig av statlig hackning vid 42 brott. Dessa brott omfattar inlämning av bedrägliga asylansökningar, skatteundandragande och narkotikabrott bland andra[649]. Förbundsdagen antog 2021 förbundsregeringens lagförslag om anpassning av lagen om konstitutionsskydd. Denna ändring legaliserar statlig hackning för alla 19 tyska underrättelsetjänster[650] och föreskriver att kommunikationsleverantörer är skyldiga att samarbeta med staten i hackningsverksamhet[651].

364. Lagarna om hackning i Tyskland försvaras ofta mot bakgrund av fall av brott mot sexuellt självbestämmande, barnpornografi, bildandet av kriminella organisationer och mord. De flesta utredningar där polisen har använt hackningsverktyg var dock inte kopplade till ovannämnda brott[652]. De senaste siffrorna från 2020 visar att den tyska polisen fick tillstånd att utföra 48 hackningar. De utförde endast 22 hackningar, och ingen av dessa var kopplade till bekämpningen av terrorism och mord[653].

365. I september 2021 rapporterades att den tyska federala kriminalpolisen (BKA) hade förvärvat Pegasus i slutet av 2020. Här är det viktigt att notera att den tyska lagstiftningen skiljer mellan två typer av spionprogramsanvändning[654]: tillgång till all information (Online-Durchsuchung[655]) och endast tillgång till direktkommunikation (Quellen-TKÜ[656]). Eftersom den ursprungliga Pegasus-programvaran kunde få tillgång till all information på en enhet, och inte bara direktkommunikation, skulle dess användning av BKA bryta mot lagen. Sedan ett historiskt avgörande av den tyska federala författningsdomstolen 2008 måste alla spionprogram som används av polismyndigheter uppfylla de normer för telekommunikation och online-övervakning som fastställts för BKA [657] [658]. BKA bad därför NSO att skriva en källkod, så att Pegasus skulle kunna få tillgång till vad som var tillåtet enligt lag. Inledningsvis vägrade NSO att göra det[659]. Först efter nya förhandlingar gick NSO med på det, så att BKA fick en ändrad version[660]. Även om detta inte har erkänts offentligt bekräftade

[648] https://web.archive.org/web/20171008044948/https://www.gesetze-im-internet.de/bkag_1997/__20k.html.
[649] https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html#p0528.
[650] https://www.bundestag.de/dokumente/textarchiv/2021/kw23-de-verfassungsschutzrecht-843408.
[651] https://netzpolitik.org/2020/staatstrojaner-provider-sollen-internetverkehr-umleiten-damit-geheimdienste-hacken-koennen/.
[652] Europaparlamentet, Germany Hearing**.**
[653] Quellen-TKÜ (§ 100a StPO) godkändes 25 gånger och utfördes 14 gånger, och Online-Durchsuchung (§ 100b StPO) godkändes 23 gånger och utfördes 8 gånger. Uppgifter från: 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] ”The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware”, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.
[658] Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.pdf?__blob=publicationFile.
[659] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197.
[660] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197.

Martina Link, dåvarande vice ordförande för BKA, köpet av en modifierad version under ett möte bakom stängda dörrar med Innenausschuss i förbundsdagen[661]. Det påstås ha använts sedan mars 2021. Den version som köptes av BKA hade blockerat vissa funktioner för att förhindra missbruk, även om det är oklart hur detta fungerar i praktiken. BKA har skrivit en rapport om denna ändrade version, som fortfarande är sekretessbelagd[662]. BKA nekade civilsamhällesorganisationer tillgång till avtal med spionprogramföretag tills de tvingats att göra det av domstol. Men till och med då offentliggjorde de endast avtalen i kraftigt redigerade versioner[663]. Trots två inbjudningar till PEGA-utskottet har BKA inte kunnat närvara vid några utfrågningar på grund av planeringsproblem.

366. I oktober 2021 avslöjades också att den tyska underrättelsetjänsten för utlandet, den federala underrättelsetjänsten (Bundesnachrichtendienst, BND), hade köpt en modifierad version av Pegasus, även om förvärvet var sekretessbelagt[664]. Som svar på en parlamentsfråga angav förbundsregeringen att användningen av Pegasus endast är tillåten i enskilda fall och måste uppfylla de strikta rättsliga villkor som fastställs i den tyska straffprocesslagen (StPO), lagen om begränsningar av sekretessen för e-post, post och telekommunikation (G-10-lagen) och lagen om den federala kriminalpolisen (BKAG), men ville inte lämna några ytterligare kommentarer om dess användning av säkerhetsskäl (Geheimhaltungsbedürftigkeit)[665].

ANVÄNDNING AV SPIONPROGRAM

367. Under 2012 och 2013 köpte både den tyska federala polisen (BKA) och Berlinpolisen (LKA) självständigt in FinSpy från FinFisher. Även här, precis som i fallet Pegasus, bad BKA företaget att utveckla FinFisher på ett sådant sätt att det inte kunde få tillgång till alla data på en enhet, utan bara direktkommunikation, för att det skulle vara förenligt med tysk lag. BKA testade hela tiden nya versioner av det spionprogram som FinFisher tillhandahöll för att det endast skulle användas på ett ”rättsligt säkert och tekniskt rent” sätt, och först efter fem år, 2018, godkände det federala inrikesministeriet att det skulle användas. Under samma år upptäcktes även användningen av programvara från FinFisher mot oppositionspartierna i Turkiet, medan Tyskland inte hade utfärdat någon exportlicens för export av övervakningsprogram till tredjeländer sedan 2015[666]. Avtalet mellan FinFisher och Berlinpolisen hade dock redan löpt ut då, så polisen i huvudstaden använde det aldrig. BKA kommenterade inte ytterligare om FinFisher används i dess verksamhet eller om huruvida avtalet fortfarande är giltigt[667].

368. År 2017 lanserade förbundsstatens inrikesminister det centrala kontoret för informationsteknik inom säkerhetssektorn (ZITiS) för att underlätta regeringens

---

[661] https://www.dw.com/en/german-police-secretly-bought-nso-pegasus-spyware/a-59113197.
[662] https://fragdenstaat.de/anfrage/mit-bka-abgestimmter-prufbericht-zur-pegasus-software/.
[663] Testimony of Andre Meister, Country Specific Hearing on Germany, Meeting of the Committee of Inquiry to investigate the use of Pegasus and Equivalent Surveillance Spyware to Poland, 14 November 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] ”The use of Pegasus and equivalent surveillance spyware: The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware”, https://www.europarl.europa.eu/RegData/etudes/STUD/2022/740151/IPOL_STU(2022)740151_EN.pdf.
[667] https://netzpolitik.org/2019/berlin-hat-den-staatstrojaner-finfisher-gekauft-wir-veroeffentlichen-den-vertrag/.

forskning och utveckling av hackningsverktyg och inköp av hackningsverktyg från kommersiella leverantörer[668]. Den 6 april 2022 rapporterades att ZITiS letade efter tillgänglig teknik på annat håll efter det vanhedrade spionprogramföretaget Finfishers konkursansökan[669]. Det rapporterades bland annat att den sedan 2019 hade träffat det italienska övervakningsföretaget RCS Lab fem gånger[670], men det fanns inga bevis för att den hade förvärvat ett verktyg från RCS Lab[671]. Dessutom träffade och utvärderade ZITiS spionprogram från det österrikiska företaget DSIRF[672] och de israeliska företagen Quadream[673] och Candiru[674].

369. I januari 2023 rapporterade Tagesschau att ZITiS också var i kontakt med Intellexa eller dess dotterbolag Cytrox, även om det är oklart om spionprogrammet Predator till slut köptes. Den tidigare samordnaren för underrättelsetjänsten Bernd Schmidbauer uppges ha agerat som representant för Intellexas produkter. Enligt e-postmeddelanden från november 2021 hade Schmidbauer kontakt med den tidigare ordföranden för förbundsmyndigheten för informationssäkerhet Arne Schönbohm i syfte att ordna ett möte med Intellexa. I februari 2022 kontaktade Schmidbauer även ZITiS ordförande för en presentation av Intellexa. Dessutom hade Smidbauer kontakt med vice ordföranden för förbundsmyndigheten för konstitutionsskydd (BfV), vilket enligt uppgift ledde till en presentation av Intellexa för personalen vid BfV i början av juli 2022. Regeringen kommenterade inte dessa möten till följd av Schmidbauers kontroversiella lobbyverksamhet[675]. År 2021 hade Schmidbauer också träffat Jan Marsalek, som har kopplingar till DSIRF[676].

MALTA

370. Flera nyckelpersoner från handeln med spionprogram har antingen registrerat ett företag på Malta eller har erhållit maltesiska pass, men det verkar som om de faktiskt inte bor där, och deras företag verkar inte heller vara aktiva. Några viktiga personer från spionprogramshandeln har hittills identifierats.

371. Tal Dilian är israelisk medborgare, f.d. israelisk militär. Han är grundare av Intellexa och bor på Cypern. Han förvärvade ett maltesiskt pass 2017[677]. Han är också delägare i ett företag på Malta som heter MNT Investments LTD[678].

372. Anatolij Hurgin är rysk-israelisk medborgare och f.d. israelisk militäringenjör. Han

---

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 Answer to a parliamentary question by The Left Party MP Martina Renner https://dserver.bundestag.de/btd/20/038/2003840.pdf.
671 https://netzpolitik.org/2022/rcs-lab-hackerbehoerde-trifft-sich-mehrmals-mit-staatstrojaner-hersteller/.
672 https://dserver.bundestag.de/btd/20/001/2000175.pdf#page=12.
673 https://dserver.bundestag.de/btd/20/001/2000104.pdf#page=29.
674 https://dserver.bundestag.de/btd/20/003/2000327.pdf.
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 Persons naturalised/registered as citizens of Malta 2017, offentliggjord den 21 december 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/.

förvärvade ett maltesiskt pass 2015[679]. Han är grundare av Ability Ltd, som samarbetade med NSO Group kring Pegasus och skötte nätverkssidan av NSO:s verksamhet[680]. Vid tidpunkten för sin ansökan om maltesiskt pass var han redan under utredning av både de amerikanska och israeliska myndigheterna för olika typer av brott[681]. Den undersökande journalisten Daphne Caruana Galizia, som senare mördades i oktober 2017, skrev om honom i augusti 2016[682]. År 2017 undersöktes Ability Ltd av USA:s värdepappersinspektion (Securities and Exchange Commission), eftersom företaget påstods ha ljugit om sina finanser och var dessutom nära att avnoteras från Nasdaq[683]. Hurgin uppges också äga ett företag i Litauen som heter UAB ”kommunikationsteknik” och som tillhandahåller ”anslutnings- och telekommunikationstjänster”[684].

373. Felix Bitzios är ledare för det maltesiska företaget Baywest Business Europe Ltd.[685], var tidigare ägare av och anställd på Intellexa och var inblandad i bedrägerifallet med Piraeus/Libra[686].

374. Stanislaw Szymon Pelczar är rättslig företrädare för Baywest Business Europe Ltd.,, registrerat i Malta, och var tidigare administratör vid Krikel. Han nämns i Paradisläckan[687].

375. Peter Thiel är en tyskfödd amerikansk medborgare som förvärvade nyzeeländskt medborgarskap 2011 trots att han inte var bosatt där. Han har ansökt om ett maltesiskt gyllene pass 2022 (kort efter tillkännagivandet av Kurz och Hulios nystartade företag)[688]. Han är grundare av PayPal och det kontroversiella företaget Palantir (knutet till Cambridge Analytica-skandalen). Han är sponsor av Donald Trump och Facebooks första externa investerare. Han anlitade Sebastian Kurz (som nyligen grundade ett företag med Shalev Hulio, tidigare NSO) som strateg[689].

FRANKRIKE

MÅLTAVLOR I FRANKRIKE

376. Under 2021 avslöjade Pegasusprojektet flera fall av hackningsförsök med hjälp av

---

679 https://timesofmalta.com/articles/view/bought-maltese-passport-given-right-to-vote-through-false-declaration.744429.
680 https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=543a981a3997; https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/.
681 https://www.euractiv.com/section/all/short_news/mep-calls-out-malta-for-selling-passport-to-man-linked-to-pegasus-spyware/.
682 https://daphnecaruanagalizia.com/2016/08/owner-israeli-phone-surveillance-hacking-software-intelligence-operation-buys-maltese-passporteu-citizenship/.
683 https://theshiftnews.com/2021/07/19/international-spy-company-linked-to-maltese-citizen-threatens-to-sue-journalists-for-exposing-surveillance-scandal/.
684 https://rekvizitai.vz.lt/en/company/communication_technologies/anatoly_hurgin_direktorius/.
685 https://offshoreleaks.icij.org/nodes/55071906.
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/.

Pegasus spionprogram i Frankrike[690]. Den läckta datauppsättningen omfattade telefonnumret till president Emmanuel Macron och telefonnumret till 14 medlemmar i hans kabinett[691] [692]. Resultaten av den franska statliga underrättelsetjänstens kriminaltekniska analyser har bekräftat att telefoner som tillhörde utbildningsminister Jean-Michel Blanquer, ministern för territoriell sammanhållning Jacqueline Gourault, jordbruksminister Julien Denormandie, ministern för bostadsfrågor Emmanuelle Wargon och ministern för Frankrikes utomeuropeiska områden Sebastien Lecornu var infekterade med Pegasus spionprogram[693]. Telefonen som tillhörde parlamentsledamoten Adrien Quatennens var också infekterad[694].

377. Registret som Pegasusprojektet fick kännedom om innehöll enligt uppgift även telefonnummer tillhörande andra franska medborgare, däribland journalister, före detta politiker och deras släktingar. Pegasus-infektioner av mobila enheter tillhörande Bruno Delport, direktör för den parisiska radiostationen TSF Jazz, tidigare minister Arnaud Montebourg och de undersökande journalisterna Edwy Plenel, Lénaïg Bredoux samt en anonym journalist från France 24 har bekräftats av Frankrikes datasäkerhetsbyrå (Agence nationale de la sécurité des systèmes d'information)[695]. Dessutom var Claude Mangin – hustru till Naâma Asfari, en saharisk politisk fånge i Marocko – också en måltavla för Pegasus[696]. Joseph Breham, en Parisbaserad försvarsadvokat för flera Polisario Front-aktivister för Sahara, blev också offer för Pegasus[697].

378. Marocko verkar ligga bakom många av attackerna mot både journalister och politiker i Frankrike[698], inbegripet marockanska journalister som lever i fransk exil, särskilt den undersökande journalisten Hicham Mansouri som flydde från de marockanska myndigheternas ständiga trakasserier 2016 och den oberoende journalisten Aboubakr Jamai som lämnade Marocko 2007[699].

379. Enligt uppgift var Frankrike själv på väg att köpa Pegasus spionprogram 2021. Vid tidpunkten för de slutliga förhandlingarna med NSO Group ledde avslöjandena om det spionprogram som påstods ha använts mot franska regeringstjänstemän till ett abrupt avslutande av affären[700]. Det franska utrikesministeriet har förnekat att föra samtal med NSO Group[701].

380. Vid ett möte i PEGA-utskottet den 9 januari 2023 uppgav Serge Lasvignes – ordförande för den nationella kommittén för kontroll av underrättelseteknik – att beslutet att inte tillåta att Pegasus används i Frankrike fattades före avslöjandena av Pegasusprojektet.

---

[690] The Guardian, Pegasus spyware found on journalists' phones, French intelligence confirms.
[691] The Guardian, Spyware 'found on phones of five French cabinet members'.
[692] Euractiv, France's Macron targeted in project Pegasus spyware case.
[693] The Guardian, Spyware 'found on phones of five French cabinet members'.
[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.
[696] Haaretz, The NSO File: A Complete (Updating) List of Individuals Targeted with Pegasus Spyware.
[697] https://www.middleeasteye.net/fr/entretiens/pegasus-espionnage-maroc-france-macron-sahara-occidental-breham-avocat-mangin-algerie.
[698] Radio France, Projet Pegasus: le gouvernement et toute la classe politique française dans le viseur du Maroc.
[699] https://forbiddenstories.org/journaliste/hicham-mansouri/; https://forbiddenstories.org/journaliste/aboubakr-jamai/.
[700] MIT Technology Review, NSO was about to sell hacking tools to France. Now it's in crisis.
[701] MIT Technology Review, NSO was about to sell hacking tools to France. Now it's in crisis.

Enligt Lasvignes använder de franska underrättelsetjänsterna endast de övervakningsprodukter som skapas i Frankrike för att undvika att utländska tillverkare av spionprogram får tillgång till information. Lasvignes angav dock att det tekniska direktorat som konstruerar de franska spionprogrammen faktiskt importerar vissa delar från icke-franska företag[702].

381. I Frankrike måste ansökningar om tillstånd till övervakning av en person först godkännas av generaldirektören för tjänsten, sedan av inrikesministern. I slutändan måste alla ansökningar godkännas av premiärministern. För närvarande övervakas 23 000 personer i Frankrike, och varje operation har fått tillstånd av premiärministern. Om ett mål vill undersöka om denne är eller har varit under övervakning nekas tillgång till dennes handlingar med hänvisning till den nationella säkerheten. Personen får begära prövning av en domare. Domaren kan dock endast avgöra om övervakningen var laglig eller inte, men kan inte informera målet eftersom detta är sekretessbelagt för den nationella säkerheten[703]. Detta innebär att rätten till rättslig prövning i praktiken är meningslös, eftersom bevisbördan ligger på den enskilde, och det är praktiskt taget omöjligt att erhålla några bevis från myndigheterna.

382. Enligt en broschyr från ISS World 2013 var det franska inrikesministeriet, försvarsministeriet, Interpol och Togos ambassad i Frankrike alla närvarande vid ISS World 2012, även känt som ”The Wiretappers Ball” (avlyssnarnas bal), som deltagare. Dessutom visar en förteckning över ISS leverantörer och teknikintegratörer att följande franska spionprogramföretag var närvarande vid detta evenemang: 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 och WAHOUE AND PARTNERS[704].

SPIONPROGRAMSFÖRETAG I FRANKRIKE

383. Frankrike har olika spionprogramsföretag, varav Nexa Technologies och Amesys är mest framträdande. Nexa technologies, som ingår i Tal Dilians Intellexa Alliance, är ett franskt företag för it-försvar och it-underrättelser som grundades 2000[705]. Nexa Technologies drivs av tidigare chefer för Amesys. Amesys grundades 1979[706] och är känt för att sälja ett program som heter Cerebro, som kan spåra målens elektroniska kommunikation, såsom e-postadresser och telefonnummer[707].

384. År 2007 påstås Amesys ha sålt denna teknik för övervakning av telekommunikation till Libyen, som användes av Gaddafiregimen för att arrestera och tortera regimkritiker. Enligt Telerama grundades Nexa för att omprofilera övervakningsprogrammet och fortsätta försäljningen av Amesys till den egyptiska regimen[708]. Under 2014 påstås Nexa Technologies ha sålt ett övervakningssystem till den egyptiska regimen under namnet Eagle. Detta system användes i samband med fängslande och tortyr av politiska

[702] PEGA-kommitténs utfrågning, 9 januari 2022.
[703] PEGA-kommitténs utfrågning, 9 januari 2022.
[704] ISS World, Programme schedule for year 2013.
[705] Bloomberg, Nexa Technologies Inc.
[706] PitchBook, Amesys.
[707] Le Monde, Vente de matériel de cybersurveillance à l’Egypte : la société Nexa Technologies mise en examen.
[708] ZDNet, Amesys and Nexa Technologies executives indicted.

motståndare till Al-Sissi-regimen[709]. Eagle distribuerades och underhölls av Amesys från 2007 till 2011[710].

385. Flera klagomål har lämnats in mot både Amesys och Nexa Technologies. I oktober 2011 ingav internationella federationen för mänskliga rättigheter (FIDH) och människorättsförbundet (LDH) en stämningsansökan till Paris högsta domstol mot Amesys i ljuset av dess påstådda försäljning till Libyen[711]. Fem libyska mål hördes sommaren 2013 och ett libyskt mål hördes i december 2015. Som ett resultat av nya bevis som styrkte Gaddafiregimens användning av Amesys övervakningsteknik tilldelades Amesys officiellt status som assisterat vittne för medverkan i tortyr mellan 2007 och 2011[712].

386. År 2010 övertogs Amesys av det franska datorföretaget Bull. År 2014 tog Atos, under ledning av Thierry Breton, över Bull och förvärvade därför även Amesys[713]. Vid tidpunkten för övertagandet var Amesys tvivelaktiga verksamhet när det gäller handel med auktoritära regimer redan välkänd. Ett klagomål hade redan lämnats in.

387. År 2017 avslöjade en utredande mediarapport att Nexa Technologies sålde övervakningssystem till Egypten 2014, vilket utlöste ett klagomål från FIDH, LDH och Kairos institut för studier av mänskliga rättigheter (CIHRS) mot företaget[714] [715].

388. I juni 2021, efter flera klagomål från människorättsorganisationer, åtalade Paris domstol fyra chefer för Amesys och Nexa Technologies för försäljningen av övervakningsteknik till regeringarna i Libyen och Egypten[716]. Det är oroande att hela tio år hade gått mellan det första klagomålet och inledandet av rättegången. Samtidigt kunde Amesys fortsätta sin verksamhet obehindrat, inklusive ovannämnda försäljning av övervakningsteknik till Egypten.

389. Trots dessa kontroverser undertecknade Frankrikes nationella myndighet för säkra handlingar (ANTS) i oktober 2016 ett kontrakt med Amesys till ett värde av över 5 miljoner euro för den tekniska förvaltningen av TES-databasen (som innehåller personuppgifter och biometriska uppgifter för alla franska medborgare). Detta beslut av de franska myndigheterna att involvera Amesys, som redan då var känt för sin verksamhet, i ett sådant projekt kritiserades. Amesys skulle inte ha full kontroll över de system som används för den kontroversiella TES-databasfilen, men skulle hjälpa de projektledare på myndigheten som hanterar TES-filen, så det kan inte uteslutas att Amesys skulle ha tillgång till personuppgifter. Chefen för ANTS ansåg dock att det inte fanns några rättsliga invändningar mot att bedriva verksamhet med Amesys[717].

390. I Frankrike kontrolleras beviljandet av exportlicenser av tjänsten för varor med dubbla användningsområden (SBDU) vid ministeriet för ekonomi, industri och digitala frågor.

---

[709] Trial International, Amesys (Nexa Technologies).
[710] ZDNet, Amesys and Nexa Technologies executives indicted.
[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, Amesys and Nexa Technologies executives indicted.
[716] Amnesty, Executives of surveillance companies Amesys and Nexa Technologies indicted for complicity in torture.
[717] L'Obs, Amesys file un coup de main à l'agence en charge du fichier monstre.

Dessutom inspekterar den ministeröverskridande kommissionen för produkter med dubbla användningsområden – under ledning av ministeriet för Europa och utrikes frågor – mer känsliga produkter med dubbla användningsområden. I skrivande stund fanns inga uppgifter tillgängliga om den franska regeringens utfärdande av exportlicenser till Nexa Technologies.

IRLAND

391. Irland har blivit den medlemsstat där några av de största spionprogramsföretagen som är inblandade i skandaler har registrerat sig på grund av landets skattelagstiftning. Den 20 september 2022 avslöjade The Currency, en irländsk undersökande journalistförläggare, att både Thalestris Limited, moderbolaget till Intellexa och Intellexa självt har sitt huvudkontor i Irland och är registrerade vid en advokatbyrå i Balbriggan. Det är anmärkningsvärt att ansökan om att införliva Thalestris Limited i Irland lämnades in i november 2019 av en specialist på företagsbildning, endast tolv dagar efter det att de cypriotiska myndigheternas brottsutredning mot Dilian och hans företag WiSpear offentliggjordes. Tal Dilian själv, VD för Intellexa, finns inte med i irländska företagshandlingar, men hans andra fru Sara Hamou påstås omnämnas som direktör för både Thalestris och Intellexa[718].

392. Offentliggjorda räkenskaper från Thalestris för perioden fram till den 31 december 2020 visar att det finns tio andra dotterbolag i Grekland, Cypern, Schweiz och Brittiska Jungfruöarna och att Thalestris inte var skyldigt att betala bolagsskatt. Företaget använde ett antal skattebestämmelser som även används av multinationella företag som är verksamma i Irland och gick därför tekniskt sett med förlust[719].

393. Den irländska regeringen vägrade att svara på frågan om huruvida den eller några brottsbekämpande myndigheter hade kontaktats av Thalestris eller Intellexa, eller om de någonsin hade använt sina tjänster, och hävdade att ”av välgrundade operativa och nationella säkerhetsskäl skulle det inte vara lämpligt att kommentera detaljerna i de nationella säkerhetsarrangemangen, och det skulle inte heller vara lämpligt att avslöja avdelningens it-säkerhetsarrangemang eller säkerhetsarrangemangen för statliga kontor, inrättningar och organ under avdelningens ansvarsområde”. Den irländska regeringen vägrade också att ge kommentarer om eventuella irländska kopplingar till det spionprogram som producerats av Thalestris och Intellexa[720]. Det finns inga allmänt kända bevis för missbruk av spionprogram i Irland.

394. Haaretz avslöjade att ett företag med namnet GoNet Systems, som var involverat i tillhandahållandet av wifi-infrastrukturtjänster på Larnacas flygplats, och som var kopplat till Dilians WiSpear och lades ner 2022, också ägde företag i Irland[721].

---

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

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

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

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

395. I januari 2023 rapporterades det att Oireachtas utskott för rättsliga frågor skulle undersöka förekomsten av företag i Irland som tillverkar spionprogram efter en skrivelse från parlamentsledamoten Barry Andrews. Utskottet uppgav att det hade behandlat frågan under ett privat sammanträde den 18 januari och enades om att lägga till ämnet i sitt arbetsprogram för 2023[722].

396. Det bör noteras att den irländska bolagsrätten ses över fortlöpande och uppdateras regelbundet för att öka insynen i företagsstrukturerna. Exempel på detta är lagen om företag (myndigheten för tillsyn av företag) från 2021, som uppdaterade systemet för tillsyn, och en kommande uppdatering av den förväntas ske 2023, och lagförslaget om diverse bestämmelser (transparens och registrering av kommanditbolag och företagsnamn) 2023. Dessutom angav den irländska regeringen ytterligare investeringar i det nationella cybersäkerhetscentrumet (NCSC) för att öka NCSC:s förmåga att aktivt upptäcka och bekämpa cyberhot som riktas mot kritisk infrastruktur och kritiska nät med hjälp av olika medel. NCSC:s förmåga att övervaka och reagera på incidenter kommer att utvecklas genom den pågående utvecklingen av det gemensamma säkerhetscentret (JSOC) och utökad analys- och rapporteringskapacitet. Arbetet med att utveckla en teknikstrategi för NCSC med hjälp av externa konsulter fortskrider också[723].

LUXEMBURG

397. Luxemburg är säte för nio enheter med direkt anknytning till NSO Group, vilket Amnesty International avslöjade i juni 2021 och bekräftades av Luxemburgs utrikesminister Jean Asselborn[724]. Det faktum att namnen på de nio företagen (t.ex. Triangle Holdings SA, Square 2 SARL och Q Cyber Technologies SARL), som alla tillhör förvaltnings- och privatkapitalbolaget Novalpina Capital, inte omedelbart avslöjar kopplingen till NSO Group, visar hur otydliga affärsstrukturer i Luxemburg gör det möjligt för företag att bedriva verksamhet utom synhåll för allmänheten i Luxemburg.

398. Efter Amnestys avslöjanden om de nio NSO-enheterna i Luxemburg i juni 2021 skickade utrikesminister Jean Asselborn en skrivelse till var och en av dem och uppmanade dem att avstå från alla beslut som skulle kunna leda till olaglig användning av de varor och tekniker som de gör tillgängliga för sina kunder. Enligt LuxTimes svarade NSO Group att det endast exporterar sitt spionprogram från Israel med den israeliska regeringens samtycke, men Asselborn uppgav i oktober 2021 att han inte kunde verifiera detta[725]. Enligt ministern hade ingen av de nio enheterna tillstånd att exportera cyberövervakningsprodukter från Luxemburg, eftersom Luxemburg inte har beviljat några exportlicenser[726]. ”Luxemburg kommer under inga omständigheter att tolerera export från Luxemburg som bidrar till kränkningar av de mänskliga rättigheterna i tredjeländer och kommer i tillämpliga fall att se till att nödvändiga åtgärder vidtas för att avhjälpa eventuella kränkningar av de mänskliga rättigheterna och

[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.
[726] https://www.luxtimes.lu/en/luxembourg/us-blacklists-luxembourg-linked-spyware-firm-6182a606de135b9236d2210e.

förhindra framtida kränkningar", sade Asselborn[727]. NSO Group kan dock fortfarande driva sin verksamhet tack vare de enheter som är baserade i Luxemburg, såsom Q Cyber Technologies, som ansvarar för att hantera fakturor, avtal och betalningar från kunder som använder dess programvara[728]. Den 24 augusti 2022 avslöjades att NSO Group hade bokat mer än hälften av sin försäljning under de två föregående åren i Luxemburg, vilket visar att Luxemburg fungerar som ett viktigt affärsnav för NSO Group[729].

399. I oktober 2021 bekräftade premiärminister Xavier Bettel att Luxemburg köpte och använde Pegasus, "av hänsyn till statens säkerhet"[730].

ITALIEN

400. Hittills har det inte inkommit några rapporter om de italienska myndigheternas eventuella inköp av spionprogram. Inga högnivåfall av spionage har rapporterats, även om telefonnumret till den tidigare premiärministern och kommissionens ordförande Romano Prodi fanns i den förteckning som publicerades av Pegasusprojektet[731]. Som FN:s särskilda sändebud för Sahel kunde han ha varit ett intressant mål för Marocko, med tanke på hans eventuella nätverk med högt uppsatta personer i Västsahara och Algeriet.

401. Spionprogramföretagen Tykelab och RCS Lab har valt Italien som bas för sin affärsverksamhet.

402. Ett annat företag som erbjöd offensiva intrångsprogram från Italien sedan åtminstone 2012 var Hacking Team, som numera kallas Memento Labs. Företaget blev ökänt efter en hackning som avslöjade försäljning till flera auktoritära länder som fortsatte använda spionprogrammet RCS för att attackera politiska oliktänkare, journalister och människorättsförsvarare. En utredning som inleddes av icke-statliga organisationer och av FN:s utredare rörande exporten av spionprogrammet RCS till Sudan ledde slutligen till att de italienska myndigheterna införde en övergripande bestämmelse enligt italiensk exportlagstiftning på grund av oro för de mänskliga rättelserna, och så att företaget var tvunget att söka individuella tillstånd för varje export. Hacking Team vägrade inte bara att samarbeta under utredningen, utan utnyttjade också sina nära förbindelser med högre tjänstemän inom regeringen, underrättelsetjänsterna och de brottsbekämpande myndigheterna i Italien för att positionera sig som en nationell säkerhetstillgång och pressade till slut ministeriet för ekonomisk utveckling att på nytt ge dem en global exportlicens[732].

ÖSTERRIKE

---

[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/.
[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/.

403. Som svar på skriftliga frågor från det österrikiska parlamentet uppgav den österrikiska förbundsregeringen att Österrike inte har varit kund till NSO[733]. Landets tidigare förbundskansler Sebastian Kurz har dock nära band till grundaren av NSO Group, och DSIRF, en stor leverantör av spionprogram, har sitt säte i Österrike.

404. Efter sin avgång rekryterades Kurz senare som global strateg för Thiel Capital, ägt av miljardären Peter Thiel[734]. I oktober 2022 lanserade Kurz och Shalev Hulio (grundare av NSO Group) ett cybersäkerhetsföretag vid namn Dream Security[735]. Även om Hulio avgick som NSO Groups verkställande direktör i augusti 2022 har Dream Security och NSO nära band genom olika personliga och affärsmässiga förbindelser. En av dess investerare, Adi Shalev, var också en tidig investerare i NSO. Gil Dolev är en annan av grundarna av Dream Security. Dolevs syster Shiri Dolev är direktör för NSO Group. Shalev Hulio har tidigare förvärvat ett av Gil Dolevs företag[736].

405. I juli 2022 använde aktörer spionprogram från det österrikiska företaget DSIRF för att hacka advokatbyråer, banker och konsultföretag i Österrike, Panama och Förenade kungariket. Enligt Microsofts forskare använde DSIRF:s ”Subzero”-verktyg så kallade nolldagarssårbarheter (zero-day exploits) för att komma åt konfidentiell information, till exempel lösenord och andra autentiseringsuppgifter[737]. I oktober 2022 uppgav förbundsministeriet för arbete och ekonomi att det inte kände till några ansökningar om exportlicenser från DSIRF och att inga exportansökningar avseende intrångsprogram hade lämnats in under de senaste tio åren[738]. I avsaknad av en exportlicens för DSIRF att exportera programvara inledde åklagarmyndigheten i Wien en preliminär utredning av misstanke om olaglig tillgång till ett datasystem enligt österrikisk rätt.

ESTLAND

406. Estland har enligt uppgift också visat intresse för att köpa NSO Groups spionprogram Pegasus. Inledande förhandlingar ägde rum mellan Estland och NSO Group 2018, varefter Estland gjorde en förskottsbetalning på 30 miljoner US-dollar för övervakningsprogramvaran[739].

407. Ett år senare underrättade dock en rysk försvarstjänsteman Israel om Estlands avsikt att använda Pegasus spionprogram på ryska telefonnummer. Denna information ledde till att det israeliska försvarsministeriet hindrade Estland från att spionera på ryska enheter över hela världen med hänvisning till att affären skulle skada de israelisk-ryska relationerna[740]. Fallet med Estland understryker att Pegasus spionprogram inte bara är

[733] Responses by former Minister of Interior Karl Nehammer to Member of National Council Nikolaus Scherak, 22 september 2021, reference 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] Studien ”Pegasus and the EU’s external relations”, Europaparlamentet, generaldirektoratet för unionens interna politik, utredningsavdelning C – medborgerliga rättigheter och konstitutionella frågor, 25 januari 2023, s. 52. Microsoft (2022), Untangling KNOTWEED: European private-sector offensive actor using 0-day exploits.
[738] https://www.parlament.gv.at/dokument/XXVII/AB/11698/imfname_1473647.pdf.
[739] The New York Times, ”Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia”, 23 mars 2022.
[740] The New York Times, ”Israel, Fearing Russian Reaction, Blocked Spyware for Ukraine and Estonia”, 23 mars 2022.

ett övervakningsvapen, utan fungerar också som en politisk valuta i diplomatiska förbindelser.

LITAUEN

408. Ett litauiskt företag, UAB Communication Technologies, som är verksamt på området anslutnings- och telekommunikationstjänster, ägs av Anatolij Hurgin, en rysk-israelisk medborgare, före detta israelisk militäringenjör och medutvecklare av Pegasus tillsammans med NSO[741]. Hurgin förvärvade också ett maltesiskt gyllene pass 2015[742].

BULGARIEN

409. I Bulgarien kontrolleras exportkontroller och exportlicenser för produkter kategoriserade som produkter med dubbla användningsområden i EU:s förordning om dubbla användningsområden av ekonomiministeriet, och mer specifikt av ministerkommissionen för exportkontroll och icke-spridning av massförstörelsevapen[743]. Den nuvarande ministern för ekonomi och industri är Nikola Stoyanov[744]. De bulgariska myndigheterna vägrar att bevilja exportlicenser till NSO Group eller dess dotterbolag[745]. Den tidigare ägaren av eget kapital i NSO Group, Novalpina Capital, betonade dock att NSO-produkter exporteras från EU från både Cypern och Bulgarien[746] [747] [748]. Dessa två påståenden är motstridiga. Dessutom hävdar mediepublikationer att vissa av servrarna i den nätinfrastruktur som Pegasus attacker utförs på ligger i ett bulgariskt datacenter som ägs av ett bulgariskt företag. Detta företag ägs av NSO Group, Circles Bulgaria och Magnet Bulgaria, som har fått exportlicenser från myndigheterna. Från Bulgarien tillhandahåller detta dotterbolag till NSO Group de cypriotiska dotterbolagen forsknings- och utvecklingstjänster och exporterar nätverksprodukter till regeringar[749]. Magnet är vilande för tillfället, men Circles är alltjämt aktivt för närvarande och har fått en exportlicens som gäller till den 25 april 2023[750].

410. I februari 2022 inledde åklagarmyndigheten i Sofia stad en undersökning för att fastställa om statliga myndigheter olagligt hade använt Pegasus spionprogram för att rikta in sig på bulgariska medborgare. Undersökningen pågår för närvarande[751]. När det gäller Ekimdzhiev m.fl. mot Bulgarien konstaterade Europadomstolen i januari 2022 att

---

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 Republic of Bulgaria, Ministry of Economy and Industry, Interministerial Commission for Export Control and Non-Proliferation of Weapons of Mass Destruction.
744 Council of Ministers of the Republic of Bulgaria.
745 Politico, ”Pegasus makers face EU grilling. Here’s what to ask them”, 21 juni 2022.
746 Amnesty International, ”Novalpina Capital’s response to NGO coalition’s open letter”, 18 februari 2019.
747 Access Now, ”Is NSO Group’s infamous Pegasus spyware being traded through the EU?”, 12 september 2019.
748 https://www.business-humanrights.org/en/latest-news/novalpina-capital-claims-nso-group-received-export-licences-from-bulgaria-cyprus-but-both-states-deny-claims/.
749 Amnesty International, ”Operating From the Shadows: Inside NSO Group’s Corporate Structure”.
750 https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.mi.government.bg%2Ffiles%2Fuseruploads%2Ffiles%2Fexportcontrol%2Fregistar_iznos_transfer_22112018.xls&wdOrigin=BROWSELINK.
751 https://bnr.bg/en/post/101599684/sofia-city-prosecutor-s-office-investigates-possible-use-of-pegasus-spyware-in-bulgaria.

de befintliga lagarna i Bulgarien om hemlig övervakning, bevarande av och tillgång till kommunikation inte uppfyllde konventionens krav på rättslig kvalitet och uppmanade regeringen att göra nödvändiga ändringar i den nationella lagstiftningen för att få ett slut på överträdelsen[752].

EU-institutioner

EUROPEISKA KOMMISSIONEN SOM MÅLTAVLA

411. Den 11 april 2022 rapporterade Reuters att kommissionsledamot med ansvar för rättsliga frågor Didier Reynders och minst fyra av kommissionens anställda hade gjorts till måltavlor med Pegasus programvara i november 2021[753]. Den 23 november 2021 skickade Apple officiella meddelanden till kommissionsledamot Reynders enheter och ytterligare kommissionspersonal och informerade dem om att de hade blivit måltavlor för statsstödda angripare och att deras enheter kunde ha blivit utsatta för angrepp[754].

412. Efter dessa avslöjanden uppmanades kommissionsledamot Reynders att tala inför PEGA-utskottet den 30 maj 2022 och svarade även skriftligen på dess frågor. Redan den 19 juli 2021, efter avslöjandena från Forbidden History och Amnesty International, hade kommissionen inrättat en ”särskild grupp med interna experter med uppgift att genomföra en intern utredning”, i syfte att kontrollera om Pegasus hade riktat in sig på enheter som tillhörde kommissionens personal och ledamöter av kommissionskollegiet”[755]. Kommissionen införde också en mobil lösning för slutpunktsidentifiering och svar på alla företagstelefoner i september 2021, som hjälper kommissionens avdelningar att identifiera potentiellt infekterade företagsmobilenheter.

413. Under undersökningens gång meddelade kommissionen att ”varken före eller efter detta datum [23 november 2021] hade dessa kontroller bekräftat att kommissionsledamot Reynders privata enhet eller arbetsenhet hade äventyrats. Kommissionens behöriga avdelningar inspekterade också den andra personalens enheter, som hade fått liknande meddelanden från Apple samma dag, men ”ingen av de inspekterade enheterna bekräftade Apples misstankar” där heller[756].

414. I sin skrivelse av den 9 september 2022 medgav kommissionen dock att under den pågående utredningen om inriktningen på kommissionen med Pegasus fanns det ”flera enhetskontroller där det fanns misstankar om intrång”. Kommissionen har hittills inte arbetat vidare med resultaten av utredningen, vare sig offentligt eller i PEGA-kommittén, eftersom ”de skulle avslöja för motståndarna kommissionens utredningsmetoder och utredningskapacitet och därmed allvarligt äventyra institutionens säkerhet”[757]. Inofficiella rapporter om mer än 50 upptäckta infektioner har inte bekräftats av kommissionen.

---

[752] Ekimdzhiev m.fl. mot Bulgarien, ansökan nr 70078/12, dom av den 11 januari 2022, finns på: 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] Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 juli 2022. response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 september 2022.
[755] Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 juli 2022.
[756] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 september 2022.
[757] https://pro.politico.eu/news/148627.

415. Som svar på PEGA-kommitténs fråga om vilken eller vilka aktörer som kan ligga bakom dessa attacker svarade kommissionen att det är ”omöjligt att med full säkerhet hänföra dessa indikatorer till en specifik gärningsman”. Den gemensamma och övergripande frågan som de två av kommissionens tjänstemän som blivit måltavlor, kommissionsledamot Reynders och en medlem ur kommissionsledamot Vera Jourovás kabinett[758], behandlar är dock rättsstatsprincipen. Som svar på PEGA:s fråga om ett möjligt samband har kommissionen vägrat att dela med sig av ytterligare information om det antal avdelningar som kan ha äventyrats, om yrkena hos den berörda personalen eller om eventuell ytterligare information som skulle vara av intresse för PEGA-kommitténs arbete och som skulle kunna avgöra orsaken till attacken, och den har uppgett att den ”inte har tillräckligt med information till sitt förfogande för att kunna dra definitiva slutsatser om en koppling mellan geolokalisering och ett möjligt angreppsförsök via Pegasus”[759].

416. Mot bakgrund av ovanstående kan flera problem identifieras. För det första har kommissionen inte visat tillräcklig medvetenhet om och förståelse för de enorma politiska riskerna med att vara måltavla för spionprogram. Alla försök till hackning – vare sig de är framgångsrika eller ej – av kommissionen, eller en eller flera av dess ledamöter, är emellertid ett mycket allvarligt politiskt faktum som påverkar integriteten i den demokratiska beslutsprocessen. I sin kommunikation med PEGA-utskottet förklarade kommissionen upprepade gånger att hackningen av kommissionsledamot Reynders enhet med hjälp av Pegasus inte lyckades. Som kommissionen själv nämnde fanns det dock ”flera enhetskontroller där det fanns misstankar om intrång”, som det inte har kommit några ytterligare meddelanden om. Detta verkar tyda på att kommissionen tonar ned allvaret i situationen med en EU-institution som är måltavla.

417. För det andra verkar det ha funnits otillräcklig it-kapacitet och kapacitet att skydda kommissionsledamöter och personal mot attacker eller att övervaka och kontrollera deras cybersäkerhet. Även om kommissionen har infört nya åtgärder, såsom lösningen för slutpunktsidentifiering och svar på alla kommissionens telefoner, och samarbetar kontinuerligt med CERT-EU[760] på grund av bristen på information som PEGA fått från kommissionen, är det oklart i vilken utsträckning kommissionens åtgärder för att analysera tidigare spionprogramsattacker har varit framgångsrika och i vilken utsträckning de åtgärder som vidtagits kommer att vara tillräckliga i framtiden.

418. För det tredje har kommissionen inte officiellt rapporterat meddelandena eller indikatorerna på intrång till den belgiska polisen för vidare utredning, utan har endast haft kontakt med den belgiska polisen om ”tekniska detaljer” som en del av dess ”regelbundna samarbete”. Kommissionen har förklarat att ”kommissionens berörda it-avdelningar tar emot meddelanden av det här slaget åtskilliga gånger vilken dag som helst” och att de därför inte behöver rapporteras officiellt till polisen. Enligt kommissionen följde man inte upp med de brottsbekämpande myndigheterna eftersom meddelandet från Apple inte tydde på någon ”definitiv infektion, utan på möjligheten att den skadliga programvaran försökte rikta in sig på den motsvarande enheten”[761].I andra fall, t.ex. i Spanien och Frankrike, har det dock inletts en brottsutredning av hur spionprogram använts mot statliga ministrar och statsöverhuvuden. Spionprogram

[758] https://pro.politico.eu/news/148627.
[759] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 september 2022.
[760] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 september 2022.
[761] Response letter by Commissioners Hahn and Reynders to the PEGA Committee, 9 september 2022.

används främst av statliga aktörer, med hänvisning till skäl som rör den nationella säkerheten. Kommissionen hävdar att ”vissa aspekter kopplade till nationell säkerhet ligger utanför kommissionens befogenheter”[762], men man kan inte förklara hur kommissionsledamöter och kommissionspersonal rimligen skulle kunna utgöra en risk för den nationella säkerheten.

419. För det fjärde innebär det faktum att kommissionen inte gav PEGA någon meningsfull information, varken inom stängda dörrar, om att kommissionen har blivit en måltavla, eller mer allmänt, med någon grundläggande information i samband med utredningen, att parlamentet inte kunde utöva demokratisk granskning ordentligt. Kommissionen bör ompröva vilken information den kan lämna ut för att möjliggöra meningsfull parlamentarisk tillsyn.

GÖRA MÅLTAVLOR AV EUROPEISKA RÅDETS, RÅDETS OCH KOMMISSIONENS LEDAMÖTER

420. Inte bara en nuvarande ledamot av kommissionen och annan personal från kommissionen blev måltavlor, utan även regeringschefer, ministrar och en före detta kommissionsledamot påstås ha blivit måltavlor för spionprogram utifrån och inom unionen.

421. Telefonnumret tillhörande den franska presidenten Macron stod på Pegasus-projektets lista över potentiella mål, och den spanska regeringen bekräftade att telefonerna tillhörande den spanske premiärministern Pedro Sanchez, försvarsministern Margarita Robles och inrikesministern Fernando Grande-Marlaska var infekterade med Pegasus spionprogram, enligt uppgift från länder utanför unionen.

422. Enligt den grekiska tidningen Documento, som offentliggjorde en omfattande lista över personer som påståtts ha spår av Predator på sina enheter[763], blev Dimitris Avramopoulos, som var europeisk kommissionsledamot från 2014 till 2019, och flera nuvarande regeringsministrar, däribland utrikesministern och finansministern, måltavlor för spionprogram. . Det står inte klart om de påstådda hackningsförsöken mot Avramopoulos ägde rum när han var ledamot av kommissionen, och det står inte heller klart vem som låg bakom dem. Den långa listan över måltavlor omfattar dock många grekiska politiker från både regeringspartiet och oppositionen. Dessa bekräftade och påstådda infektioner och hackningsförsök visar att det kan vara möjligt för nuvarande regeringsledare och ministrar, samt nuvarande eller tidigare kommissionsledamöter, inklusive deras kommunikation med kolleger, att bli måltavlor utifrån eller inom unionen under tiden de är medlemmar av Europeiska rådet, rådet och kommissionen. Därför skulle en enda infekterad telefon också allvarligt kunna äventyra informationen som innehas av institutionerna, inklusive information som delas i realtid under kommissionens och rådets möten.

Tredjeländer

423. Följande avsnitt kommer att visa i hur stor omfattning användningen av Pegasus eller motsvarande spionprogram för övervakning, som direkt eller indirekt involverar enheter

[762] Response letter by Commissioners Hahn and Reynders to the rapporteur, 25 juli 2022.
[763] Documento, utgåva av den 6 november 2022.

med koppling till EU, har bidragit till olagligt spionerande på journalister, politiker, tjänstemän inom brottsbekämpning, diplomater, advokater, affärsmänniskor, aktörer i det civila samhället, människorättsförsvarare eller andra aktörer i tredjeländer. Här ingår också i hur stor omfattning utvecklingen av spionprogram har lett till människorättsbrott som är oroväckande med tanke på målen med EU:s gemensamma utrikes- och säkerhetspolitik, och huruvida användningen av spionprogram har gått emot de värden som finns inskrivna i artikel 21 i EU-fördraget och i stadgan, plus att FN:s vägledande principer för företag och mänskliga rättigheter och andra rättigheter som finns med i internationell människorättslagstiftning tas i beaktande.

424. Av de tredjeländer som engagerar sig i spionprogram har Israel och Marocko uppmärksammats särskilt av PEGA-kommittén, med en utfrågning och ett uppdrag till Israel i juli 2022 och en session ägnad åt Marocko i februari 2023 under en utfrågning om spionprogrammens geopolitik. Dessutom ägnades en utfrågning i augusti 2022 delvis åt Rwanda, med kommentarer från Carine Kanimba, som var en måltavla för Pegasus.

ISRAEL

425. PEGA-utskottet besökte Israel i juli 2022. Huvudsyftet med resan var att träffa tillverkaren av Pegasus spionprogram, det israeliska företaget NSO Group. PEGA-delegationen fick veta att NSO Group har sålt spionprogram till 14 regeringar i EU med hjälp av exportlicenser som utfärdats av den israeliska regeringen. De diskuterade missbruk av verktyg för övervakning av legosoldater och deras inverkan på demokratin, rättsstatsprincipen och de grundläggande rättigheterna i EU. Kommittén träffade också företrädare för regeringen, Knesset, experter och det civila samhället. Detta besök underströk de befintliga skyddsåtgärdernas ineffektivitet mot missbruk av spionprogram och behovet av mycket strängare EU-bestämmelser om försäljning, inköp och användning av spionprogram. Cyberförsvarsområdet måste regleras effektivt för att förhindra missbruk av spionprogram i framtiden.

426. Israels geopolitiska och säkerhetsmässiga situation har föranlett landets regering och privata sektor att utveckla verktyg för underrättelseinsamling som skulle utöka landets cybersäkerhetskapacitet, särskilt när det gäller dess försvar. Under årens lopp har Israel blivit en av världens ledande tillverkare av avancerad övervakningsteknik och spionprogram, eftersom de har stor sakkunskap när det gäller att utveckla verktyg underrättelseinsamling. Industrin exporterar sina produkter globalt. I en studie som beställts av Europaparlamentet, och som offentliggjordes 2023 med titeln *Pegasus and the EU's external relations*, noterades att ”spionprogramsindustrin för exporterande länder kan vara en lukrativ inkomstkälla och en språngbräda till demokratiskt inflytande”[764]. Detta bekräftas också av nyhetsrapporteringen, med experter som belyser att Pegasus är användbart för att bygga upp diplomatiska förbindelser, t.ex. med Gulfstaterna[765].

427. Utöver strategiska inhemska skäl har Israel framgångsrikt främjat sig självt som en nation innovativ för nystartade företag, med företag som har den mest sofistikerade

[764] ”Pegasus and the EU's external relations”, Europaparlamentet, generaldirektoratet för unionens interna politik, utredningsavdelning C – medborgerliga rättigheter och konstitutionella frågor, 25 januari 2023.
[765] https://www.france24.com/en/livenews/20210719-pegasus-scandal-showsrisk-of-israel-s-spy-tech-diplomacyexperts.

tekniken på området, såsom NSO, Cellebrite, Candiru, QuaDream och Intellexa. Industrins kollektiva försäljning beräknas uppgå till minst 1 miljard US-dollar årligen[766], vilket motsvarar omkring 0,6 % av Israels export[767]. Israels försvarsmakt och underrättelsetjänst, särskilt dess avdelning för cybersäkerhet Unit 8200, har spelat en viktig roll i Israels framgångsrika spionprogramsindustri och företagen har nära förbindelser med enheten. Enligt en studie från 2018 är 80 % av de 2 300 personer som grundade Israels 700 it-säkerhetsföretag var f.d. anställda på den israeliska försvarsstyrkans underrättelseenheter. En av dess mest framträdande gestalter inom branschen är Intellexas ägare och grundare Tal Dilian (se avsnittet om Intellexa och Tal Dilian)[768].

428. Israeliska spionprogramföretag har sålt övervakningsteknik över hela världen, däribland till EU-medlemsstater och auktoritära Gulfländer. Enligt tidningen Haaretz användes försäljningen av Pegasus som ett diplomatiskt förhandlingsobjekt och underlättade förhandlingarna om upprättandet av formella diplomatiska band med Marocko, Bahrain och, formellt, Förenade Arabemiraten enligt Abrahamavtalen[769]. Försäljningen av spionprogram till auktoritära regimer har kritiserats, särskilt efter Pegasus-projektet. Till följd av detta skärpte den israeliska regeringen i december 2021 exportreglerna för utrustning avseende cyberkrigföring. Mot bakgrund av Israels planerade översyn av rättsväsendet uppges att många israeliska teknikföretag erbjuds incitament av Grekland, Cypern och Portugal för att omlokalisera sin verksamhet till dessa länder. Enligt medierapporter erbjuder de tre länderna skattelättnader för israeliska teknikföretag, medan Grekland enligt uppgift tillhandahåller påskyndat medborgarskap[770].

429. Enligt experter är Israel berett att prova nya övervakningssystem på palestinier i de ockuperade områdena vilket skapar incitament till en affärsmodell i övervakningsindustrin, som också NSO har gynnats av[771]. Till följd av detta bidrar länder som skaffar sig ”fältträ nade” spionprogram från Israel till människorättsbrott i de nämnda regionerna. EU:s medlemsstater är bland NSO:s mest prestigefyllda kunder och går därmed direkt emot EU:s utrikes- och säkerhetspolitiska agenda i fråga om stöd till mänskliga rättigheter och demokrati[772].

430. NSO:s Pegasus-spionprogram har använts med det palestinska civila samhället som

[766] https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.
[767] https://en.globes.co.il/en/article-israels-exports-rise-sharply-in-2022-1001433699#:~:text=According%20to%20a%20conservative%20estimate,a%20then%20record%20%24144%20billion.
[768] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106.
[769] Haaretz (2022) ‘Netanyahu Used NSO’s Pegasus for Diplomacy’, https://www.haaretz.com/israelnews/2022-02-05/tyarticle/.premium/netanyahu-used-nsospegasus-for-diplomacy-now-he-blames-itfor-his-downfall/0000017f-e941-dc91- a17f-fdcd55c80000.
[770] https://www.timesofisrael.com/greece-offering-senior-israeli-tech-executives-tax-breaks-to-relocate-report/ ; https://en.globes.co.il/en/article-israeli-entrepreneurs-in-talks-over-tech-exodus-1001442106.
[771] PEGA:s uppdrag i Israel, 18–20 juli 2022.
[772] I enlighet med vad som mestadels konstaterades i kommissionens årsrapport 2021 om tillämpningen av EU-stadgan om de grundläggande rättigheterna – Skyddet av grundläggande rättigheter i den digitala tidsåldern, måste EU underlätta människorättsförsvarares arbete på internet.

måltavla, däribland sex palestinska människorättsförsvarare[773]. I fallen med Ubai Al-Aboudi, verkställande direktör för Bisancentret för forskning och utveckling, och Salah Hammouri, fransk medborgare med dubbelt medborgarskap, advokat och fältforskare vid Addameer Prisoner Support and Human Rights Association, verkar användningen av spionprogram för övervakning ha resulterat i att de hamnat i förvar. Övervakningen av samtliga sex personer sammanfaller med att sex palestinska människorättsorganisationer högst kontroversiellt betecknats som ”terrorister”, vilket orsakat kraftiga internationella protester där den israeliska regeringens beslut har fördömts. Detta fall av övervakning av palestinska människorättsförsvarare är ytterligare bevis på att NSO inte tillämpar sin människorättspolicy[774], som företaget har använt för att öka sin legitimitet och trovärdighet när man säljer till EU-medlemsstaterna.

431. Det bör noteras att kommissionen har haft kontakt med de israeliska myndigheterna angående rapporter om att NSO:s Pegasus-spionprogram missbrukats till brott mot de mänskliga rättigheterna. I ett brev till PEGA-kommittén av den 9 september 2022 svarade kommissionen att man tagit upp frågor om potentiellt missbruk med de israeliska exportmyndigheterna och ”efterfrågat indikationer på eventuella anknutna begränsande åtgärder som behöriga israeliska exportkontrollmyndigheter skulle kunna överväga att vidta i framtiden”. När brevet skrevs hade kommissionen inte fått några sådana indikationer från de behöriga israeliska exportkontrollmyndigheterna, men avsåg att ”återkomma till frågan om eventuella begränsande åtgärder vid nästa sammanträde med EU:s och Israels underkommitté om industri, handel och tjänster inom ramen för associeringsavtalet”.

MAROCKO

432. Att Marocko i hög grad påstås använda spionprogram har dokumenterats i åtskilliga nyhetsrapporter. Med en licens för ca 100 000 telefonnummer kan Marocko ses som en av NSO:s största kunder för Pegasus[775]. Marocko har tillbakavisat anklagelserna i samband med Pegasus-projektet som ”felaktiga”. I december 2020 visade en rapport av Citizen Lab att Marocko är en av Circles, ett dotterbolag till NSO-gruppen, 25 kunder[776].

433. Avslöjandena har också visat att övervakning med spionprogrammet påstås ha använts inom landet för att hacka och därefter injaga skräck i journalister och aktivister[777]. I en resolution nyligen om övervakningen och fängslandet av den undersökande journalisten Omar Radi fördömde Europaparlamentet den marockanska regeringens kontinuerliga rättsövergrepp mot journalister och kraftfullt uppmanat de marockanska myndigheterna ”att upphöra med sin övervakning av journalister, bland annat via NSO:s spionprogram Pegasus”[778]. En av de personer som varit måltavlor, Ignacio Cembrero, undersökande

[773] https://www.frontlinedefenders.org/en/statement-report/statement-targetingpalestinian-hrds-pegasus; https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/.
[774] https://www.amnesty.org/en/latest/researc h/2021/11/devices-of-palestinian-humanrights-defenders-hacked-with-nso-groupspegasus-spyware-2/.
[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] Europaparlamentets resolution av den 19 januari 2023 om situationen för journalister i Marocko, särskilt fallet Omar Radi, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0014_SV.html.

journalist på den spanska tidningen El Confidential, framträdde inför PEGA-utskottet den 29 november 2022. Han blev medveten om att hans telefon hade blivit hackad efter att sms-meddelanden mellan honom och den spanska regeringen publicerades i en marockansk tidning. När en spansk domstol begärde att få samarbeta vägrade de israeliska myndigheterna att lämna ytterligare upplysningar till stöd för ärendet.

434. Marocko har också förföljt de marockanska journalisterna Hicham Mansouri och Aboubakr Jamaim[779], som är i exil i Frankrike, och även understödjare av Västsahara, däribland försvarsadvokaten Joseph Breham i Paris samt El Mahjoub Maliha, människorättsförsvarare för västsaharier, bosatt i Belgien[780].

435. Marocko har inlett åtskilliga rättsliga förfaranden som svar på anklagelser om att man varit inblandad i användningen av Pegasus i Frankrike, Spanien och Tyskland. I Frankrike har de marockanska myndigheterna väckt åtal för förtal mot flera mediekanaler och organisationer i det civila samhället, däribland Le Monde, Forbidden Stories, Radio France, Mediapart, L'Humanité och Amnesty International. Den 25 mars 2022 avslog brottmålsdomstolen i Paris fallen som ogrundade, varpå de marockanska myndigheterna överklagade beslutet. I Spanien väckte de marockanska myndigheterna åtal mot journalisten Ignacio Cembrero på grundval av en medeltida paragraf i strafflagen och anklagade honom för ”skrytsam handling”. Målet pågår just nu och har fördömts för att syftet är att försöka hindra Cembrero och andra från att rapportera om hur Marocko använder spionprogram[781].

436. Enligt en nyhetsrapport var Marocko, innan man började använda Pegasus i stor omfattning, också kund hos minst tre europeiska leverantörer av spionprogram, nämligen de franska företagen Amesys och Vupen[782] och det italienska företaget Hacking Team. Enligt konfidentiella dokument var Marocko det italienska företagets tredje största kund och betalade under sex år över tre miljoner euro för att få köpa Hacking Teams programvara RCS åt sitt inhemska högsta råd för nationellt försvar (CSDN) och sin katalog för territoriell övervakning (DST)[783]. Åtskilliga avdelningar och inrättningar på hög nivå i FN har övervakats med hjälp av spionprogrammet.

437. Marocko har inte bara köpt spionprogram i EU, utan har också försetts med tekniskt och ekonomiskt stöd från Europeiska kommissionen. Enligt Der Spiegel mottog Marocko två spionprogramsystem från EU för att spionera på enskilda personer i gränskontrollsyfte (fransk-libanesiska MSAB:s spionprogram XRY och amerikanskbaserade Oxygen Forensics spionprogram Detective)[784]. Dessutom skickades Europeiska unionens byrå för utbildning av tjänstemän inom

---

[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.

brottsbekämpning (Cepol) till Marocko för att hålla i personlig träning i hur spionprogrammet användes och för att lära polisen hur man hämtar information från profiler på sociala medier genom social hackning[785]. Till skillnad från Pegasus kan de ovannämnda spionprogrammen bara komma in i enheter fysiskt och lämnar inga spår av användningen. I rapporten beskrivs åtskilliga fall där smarttelefoner har tagits från måltavlorna, bland dem journalister och aktivister, och återlämnats med antydningar om deras möjliga infektion. Även om det inte är möjligt att kontrollera om spionprogram har använts korrekt av tredje parter fanns det inga tecken på att kommissionen kontrollerade att den levererade tekniken användes korrekt. Med tanke på den liknande situation som beskrivs i ett klagomål till EU-ombudsmannen om finansiering av övervakningsteknik inom ramen för programmet inom Europeiska unionens förvaltningsfond för nödåtgärder i Afrika (se relevant avsnitt nedan) har kommissionen inte utfört någon konsekvensbedömning för att kartlägga möjligt missbruk av den levererade tekniken. Kommissionen har uppgett att det är upp till användaren, Marocko, att använda spionprogram på ett ansvarsfullt sätt och i enlighet med avtalet (dvs. endast för de ändamål som anges i avtalet)[786].

ÖVRIGA TREDJELÄNDER

438. Globalt har minst 75 länder, däribland förtryckarregimer, köpt och/eller använt spionprogram[787]. Människorättsorganisationer har dokumenterat åtskilliga incidenter där spionprogram har missbrukats för att kunna riktas mot politiker, journalister, advokater, människorättsförsvarare och andra aktivister i det civila samhället som främjar mänskliga rättigheter, kvinnors rättigheter och miljöskydd[788].

EU-MEDLEMSSTATERNAS MEDHJÄLP TILL ÖVERGREPP MED PEGASUS I ANDRA LÄNDER I EGENSKAP AV KUNDER HOS NSO GROUP

439. Myndigheterna i 14 länder utanför EU är troligtvis ansvariga för många fall där måltavlorna har identifierats och infektionen har bevisats tekniskt. De berörda länderna är El Salvador, Mexiko, Thailand, Marocko, Indien, Rwanda, Saudiarabien, Bahrain, Jordanien, Kazakstan, Togo, Förenade Arabemiraten, Israel och Azerbajdzjan[789].

440. I Pegasus-projektet, ett samarbete mellan över 80 journalister från 17 mediekanaler, har det dokumenterats hur Pegasus har använts av förtryckarregeringar som försökt tysta journalister, angripa aktivister och krossa oliktänkande. Pegasus-projektets utredningar har, trots upprepade nekanden från NSO Group, visat att den saudiske journalisten Jamal Khashoggis familjemedlemmar blivit måltavlor för Pegasus spionprogram före och efter att han mördades i Istanbul den 2 oktober 2018 av saudiska agenter. Amnesty Internationals Security Lab fastställde att Pegasus-spionprogrammet installerades framgångsrikt på Khashoggis fästmö Hatice Cengiz telefon bara fyra dagar efter att han mördades. Hans hustru Hanan Elatr var också upprepade gånger måltavla för spionprogrammet mellan september 2017 och april 2018, liksom hans son Abdullah,

[785] https://privacyinternational.org/longread/4289/revealed-eu-training-regimeteaching-neighbours-how-spy.
[786] https://disclose.ngo/en/article/how-theeu-supplied-morocco-with-phonehacking-spyware.
[787] Carnegie Endowment for International Peace, 'Global Inventory of Commercial Spyware & Digital Forensics', 11 januari 2023, https://carnegieendowment.org/programs/democracy/commercialspyware.
[788] Forensic Architecture, Amnesty International and The Citizen Lab, 'Digital Violence', https://www.digitalviolence.org/#/.
[789] https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.

som valdes ut som måltavla tillsammans med andra familjemedlemmar i Saudiarabien och Förenade Arabemiraten[790].

441. Dessutom har Pegasus-projektet dokumenterat att journalister har varit frekventa mål för Pegasus spionprogram. I Mexiko blev journalisten Cecilio Pinedas telefon utvald som mål bara några veckor innan han dödades 2017. Pegasus har också använts i Azerbajdzjan, ett land där det bara finns några få oberoende mediekanaler kvar. Enligt utredningen valdes över 40 azerbajdzjanska journalister ut som potentiella mål. Amnesty Internationals Security Lab konstaterade att Sevinc Vaqifqizi, frilansjournalist för den oberoende mediekanalen Meydan TV, hade sin telefon infekterad under en tvåårsperiod som slutade i maj 2021. I Indien utvaldes minst 40 journalister från nästan varenda stor mediekanal i landet som potentiella måltavlor mellan 2017 och 2021. Kriminaltekniska tester visade att Siddharth Varadarajan och MK Venu, medgrundare till den oberoende onlinekanalen The Wire, fick sina telefoner infekterade med Pegasus-spionprogrammet så sent som i juni 2021[791].

442. Människorättsförsvarare är fortsatt ofta måltavlor, däribland för myndigheterna i följande länder: Mexiko, El Salvador, Marocko, Rwanda, Israel, Jordanien, Saudiarabien, Bahrain, Förenade Arabemiraten, Indien, Kazakstan, Indonesien och Belarus[792]. År 2021 offentliggjorde Frontline Defenders en rapport med dokumentation av den målinriktade övervakningen av människorättsförsvarare i länder som Indien. I juni 2018 fängslades sexton människorättsförsvarare i enlighet med indisk antiterrorlagstiftning i vad som benämnas Bhima Koregaon-fallet, vilket syftar på det våld som skedde i Bhima Koregaon. En av människorättsförsvararna, den 84-årige jesuitprästen Stan Swamy, avled frihetsberövad i juli 2021[793]. I en digital kriminalteknisk utredning konstaterades att den ”bevisning” som åtalet mot gruppen byggde på hade planterats in med hjälp av Pegasus-spionprogrammet på enheter tillhörande människorättsförsvararna Rona Wilsons och Surendra Gadlings, och att det inte fanns några bevis för att människorättsförsvararna hade haft med saken att göra[794].

II. Spionprogramsindustrin

443. EU är en attraktiv plats för handel med övervakningsteknik och övervakningstjänster, inklusive spionprogram. Å ena sidan är medlemsstaternas regeringar potentiella kunder. Å andra sidan fungerar idén ”EU-reglerat” som ett riktmärke som är användbart för den globala marknaden. EU:s inre marknad erbjuder fri rörlighet och fördelaktiga nationella skattesystem. Upphandlingsregler kan undvikas med hänvisning till nationell säkerhet, och regeringar kan använda fullmakter eller mellanhänder, så att offentliga

[790] Amnesty International, ‘Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally’, 19 juli 2021, https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/.
[791] Amnesty International, ‘Massive data leak reveals Israeli NSO Group’s spyware used to target activists, journalists, and political leaders globally’, 19 juli 2021, https://www.amnesty.org/en/latest/pressrelease/2021/07/the-pegasus-project/.
[792] https://www.amnesty.org/en/latest/news/2022/07/the-pegasus-project-one-year-on-spyware-crisis-continues-after-failure-to-clamp-down-on-surveillance-industry/; https://www.amnesty.org/en/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/.
[793] Frontline Defenders (2 december 2021): Action needed to address targeted surveillance of human rights defenders https://www.frontlinedefenders.org/en/stat ement-report/action-needed-addresstargeted-surveillance-human-rightsdefenders.
[794] The Wire, Rona Wilson’s iPhone Infected With Pegasus Spyware, Says New Forensic Report, 17 december 2021, https://thewire.in/rights/rona-wilsonpegasus-iphone-arsenal.

myndigheters inköp av spionprogram är mycket svåra att upptäcka och bevisa. EU har stränga exportregler, men på senare tid tenderar medlemsstaterna att kringgå dessa och försöker få en konkurrensfördel genom olämpligt nationellt genomförande. Dessutom har Europeiska kommissionens genomförande ofta varit otillräckligt. Varje gång systemet med exportlicenser har skärpts i Israel har flera företag flyttat sina exportavdelningar till Europa, särskilt Cypern[795] [796]. Dessutom har flera personer från spionprogramsindustrin fått EU-medborgarskap för att kunna verka fritt inom och från EU.

444. Som chef för Amnesty Tech har dessutom Claudio Guarnieri vittnat inför PEGA-kommittén om att det är europeiska företag som tyska FinFisher och italienska Hacking Team som varit banbrytande inom industrin för legosoldatspionprogram. De första rapporterna om dessa företags roll i att övervaka journalister och krossa oliktänkande kom ut för över tio år sedan, i och med att företagens avtal började läcka ut från den hemliga polisens olika kontor i samband med att de proteströrelser som kallas för Arabiska våren inleddes[797].

445. Spionprogramsindustrin har en fördunklande struktur som bygger på ett komplicerat nät av personer, platser, förbindelser, ägarstrukturer, brevlådeföretag, företagsnamn som hela tiden ändras, penningflöden, regeringsanknutna fullmakter och mellanhänder, magnater och statliga förvaltningar.

446. I många fall verkar smeknamnet ”legosoldatspionprogram” stämma. Som antalet personer som olagligen inriktas på visar, ligger många företag efter när det gäller etiska normer, och säljer ofta till diktaturer och rika aktörer som inte företräder staten och fortsätter att göra det även efter avslöjandena om Pegasus-projektet. Under 2021 meddelade Cellebrite att man skulle sluta sälja till den ryska regeringen när det blev känt att dess spionprogram hade använts mot anti-Putin-aktivister. I oktober 2022 fanns det dock tecken på att Cellebrite fortfarande användes av de ryska myndigheterna[798]. Det är en lukrativ och tvetydig marknad. Ändå kan många spionprogramföretag sälja sina produkter till demokratiska regeringar i Förenta staterna och EU, som ger dem ett respektabelt yttre. Trots påståenden att användningen av spionprogram är helt legitim och nödvändig tvekar regeringarna när det gäller att erkänna att de har spionprogram. De använder sig ibland av fullmakter, mellanhänder eller mäklare för att köpa spionprogram, för att inte lämna några spår. Det stora årliga evenemanget för industrin är ISS World-mässan, som också kallas ”telefonavlyssningsbalen”. Den årliga europeiska upplagan hålls i Prag. Det finns en betydande överlappning mellan utställarna på ISS World och utställarna på mässor inom vapenindustrin.

447. Förutom de ”officiella kanalerna” finns det också en svart marknad för dessa produkter. Även om många leverantörer hävdar att de bara säljer till regeringar, verkar det som att de även försöker göra affärer med icke-statliga aktörer. Det är mycket svårt att hitta vattentäta bevis, eftersom handeln lämnar få spår. Den grekiska tidningen Documento

---

[795] Makarios Drousiotis, ‘State Mafia’, 2022, kapitel 6.
[796] Haaretz. ”Cyprus, Cyberspies and the Dark Side of Israeli Intel”.
[797] Utfrågning i PEGA-kommittén den 30 augusti 2022 om hur spionprogram drabbar EU-medborgare, 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.

säger sig ha bevis för att programvara säljs på svarta marknaden – för upp till 50 miljoner US-dollar – och inte bara till regeringar och terrorismbekämpande myndigheter utan också till privatpersoner[799]. En annan grekisk tidning, To Vima, har rapporterat att Predator såldes till 34 kunder från Grekland[800]. Läckta dokument visar att en piratkopierad version av produkten som officiellt såldes endast till regeringar fanns tillgänglig till ett pris på 8 miljoner US-dollar, ett belopp där det ingick utbildning för de agenter som skulle använda programmet, teknisk support dygnet runt samt övervakning av målets konton på sociala medier[801].

448. Industrin erbjuder en stor mängd produkter och tjänster för övervakning och underrättelser, inte bara spionprogram som en enskild produkt. Spionprogram är bara ett av många verktyg som företag med ”hackare att hyra” använder sig av.

Sårbarheter

449. Utan säkerhetsproblem i programvaran är det omöjligt att installera och distribuera spionprogram. För att reglera användningen av spionprogram måste upptäckten, delningen och utnyttjandet av sårbarheter också regleras[802]. Trots att förstärkningen av försvaret av digitala system krävs och uppmuntras av NIS2-direktivet och förslaget till cyberresilienslag är det nästan omöjligt att utveckla system utan sårbarheter.

450. Sårbarheter behöver därför offentliggöras och åtgärdas så snart som möjligt. Nuvarande EU-lagstiftning uppmuntrar emellertid det motsatta. Enligt direktivet om it-brottslighet och upphovsrättsdirektivet kan forskare om informationssäkerhet bli civil- och straffrättsligt ansvariga när de forskar om sårbarheter och delar sina resultat. Det är dessutom inte obligatoriskt för forskare att dela några resultat om sårbarheter. Forskarna kan därför välja att sälja sin kunskap om sårbarhet till en privat mäklare mot hög ersättning.

451. Denna praxis har lett till en livlig och lukrativ handel med sårbarheter. Det är dock inte bara mäklare inom dag noll-sårbarheter som är ute efter sårbarheter; även säkerhets- och brottsbekämpningsmyndigheter samlar på sig sårbarheter, vissa som deras egna experter hittar, andra som de skaffar sig av mäklare. Om sårbarheter går orapporterade åtgärdas de inte, vilket gör it-systemen försvagade och användarna oskyddade. På så sätt kan användningen av spionprogram fortsätta.

Telekommunikationsnätverk

452. Leverantörer av telekommunikationstjänster spelar en viktig roll i processen att spionera både lagligt och olagligt. Vi lever i en modern tid av AI, stordata och kvantdatorer, men samtidigt använder vi och förlitar oss starkt på ett internationellt telekommunikationsprotokoll som heter Signalsystem nummer 7 (SS7). Detta protokoll utarbetades 1975 och används fortfarande i dag. Det här systemet styr hur telefonsamtal

---

[799] Documento, ‘Documento’s “Predator” revelations on Euractiv – Europol’s intervention calls for Dutch MEP’.
[800] To Vima, Interceptions ‘Spy software has 34 customers’.
[801] https://en.secnews.gr/417192/ipoklopes-agora-predator-spyware/.
[802] Ot van Daalen, intervention in PEGA Committee, 27 oktober 2022;

EDRi Paper: ”Breaking encryption will doom our freedoms and rights”, https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-Encryption.pdf;
https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu.

kopplas och faktureras och möjliggör avancerade samtalsfunktioner och sms[803]. Via SS7-nätverket är det möjligt att avlyssna telefonsamtal och sms-meddelanden, identifiera geolokaliseringar och infektera ett mål med spionprogram såsom Pegasus eller Predator[804].

453. Risken är hög att telekommunikationsleverantörerna missbrukar sin åtkomst till dessa nätverk. Det finns flera dokumenterade fall av missbruk, där åtkomstpunkter (Global Titles) leasades till företag som övervakade och snappade upp måltavlornas kommunikation med hjälp av man-i-mitten-attacker. De hämtade också in geolokaliseringsdata och metadata för sina egna ekonomiska syften. En Global Title är en adress som används för att koppla meddelanden inom SS7. Den kan jämföras med en ip-adress, på så sätt att en Global Title är en adress inom telekommunikationssystemet[805]. Enligt en visselblåsare var NSO därför så intresserat av att få tillgång till SS7-nätverket i Förenta staterna att det försökte köpa tillträde från sitt företag[806]. Telekommunikationsleverantörer håller medvetet branschens standarder låga för att ge lokala statliga brottsbekämpande myndigheter enklare åtkomst.

NSO Group

454. Pegasus spionprogram tillverkas av NSO Group. NSO Group grundades 2010 av Shalev Hulio, Omri Lavie och Niv Karmi, som utvecklade teknik för att hjälpa licensierade statliga myndigheter och brottsbekämpande organ att upptäcka och förebygga terrorism och brottslighet[807]. Pegasus spionprogram är den mest kända produkten från NSO Group. Det infördes på den globala marknaden 2011[808] [809].

455. Sedan NSO Group startade upp 2010 har man som företag haft närvaro i Israel, Förenade kungariket, Luxemburg, Caymanöarna, Cypern, Förenta staterna, Nederländerna, Bulgarien och Brittiska Jungfruöarna. Det saknas fortfarande mycket information om de olika bolagsenheternas roller, och en del av dessa företag har redan avvecklats. I 2021 års rapport om öppenhet och ansvar uppgav dock NSO Group att Bulgarien och Cypern är båda exportnav[810]. Enligt Amnesty International hade de nederländska enheterna (som avvecklades den 22 december 2016) funktioner i sektorn för finansiella intressen, medan det Luxemburgbaserade Q Cyber Technologies var aktivt som en kommersiell distributör med ansvar för att utfärda fakturor, ingå avtal och ta emot betalningar från kunder. Dessutom kan Westbridge Technologies som registrerats i Förenta staterna ha underlättat företagets amerikanska försäljning[811].

456. NSO rapporteras ha haft intäkter på 243 miljoner US-dollar 2020[812]. Efter avslöjandena från Pegasus-projektet har emellertid företaget mött flera svårigheter.

---

[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. 'Om oss.
[808] New York Times 'The Battle for the World's Most Powerful Cyberweapon'.
[809] Shalev Hulio, 'NSO Never Engaged in Illegal Mass Surveillance', The Wall Street Journal, 24 February 2022.
[810] NSO Group, 'Transparency and Responsibility Report 2021'.
[811] Amnesty International, 'Operating from the shadows – inside NSO Group's corporate structure'.
[812] Haaretz, 'NSO Is Having a Bad Year - and It's Showing'.

Stämningsansökningar från Apple[813] och Meta[814] mot företaget, det amerikanska handelsdepartementets svartlistning av NSO, skärpningen av det israeliska exportsystemet, kritiska utredningar i många länder och interna spänningar inom privatkapitalfonden bakom NSO Group har lett till kraftigt minskad vinst. Vid ett tillfälle uppgav NSO Group att dess skuld enligt uppgift till och med uppgick till 6,5 gånger dess normala årliga intäkter[815].

457. PEGA-kommittén hade två möten med NSO Group, varav ett ägde rum i Bryssel och ett i Israel. Spionprogrammet Pegasus såldes från början till 22 slutanvändare i 14 EU-medlemsstater, med marknadsförings- och exportlicenser utfärdade av Israel. Avtalen med slutanvändarna i två medlemsstater sades därefter upp[816]. Det har inte bekräftats vilka medlemsstater som ingår ibland de 14 eller vilka två det var som togs bort. Emellertid kan det antas att de två var Polen och Ungern.

FÖRETAGSSTRUKTUR, ÖPPENHET OCH TILLBÖRLIG AKTSAMHET

458. Den 25 januari 2010 startade NSO Group sitt första företag i Israel. Detta företag registrerades under namnet ”NSO Group Technologies Limited”. NSO Group är både namnet på det första registrerade företaget och den övergripande termen för de olika företag som etablerats i andra jurisdiktioner. Detta första etablerade företag äger varumärket NSO Group[817].

459. I mars 2014 skaffade sig privatkapitalfonden Francisco Partners en andel på 70 % i NSO Group. Under Francisco Partners utökade företaget sina enheter till andra jurisdiktioner, däribland Cypern, Bulgarien, Förenta staterna, Nederländerna och Luxemburg. Under åren med Francisco Partners (2014-2019) gick fonden systematiskt igenom försäljningen av NSO Groups produkter genom den affärsetiska kommittén (BEC). Enligt Francisco Partners nekade BEC försäljning till ett värde på tiotals miljoner dollar, som annars skulle godkännas enligt de juridiska kraven[818].

460. Francisco Partners sålde hela sin ägarandel, även i dotterbolagen, till Novalpina Capital den 14 februari 2019. I och med detta utköp av ledningen ändrades styrningsnormerna och BEC ersattes av styrnings-, risk- och efterlevnadskommittén (GRCC) för att granska potentiella kunders människorättssituation[819].

461. I enlighet med slutanvändnings-/slutanvändarcertifikatet har NSO Group, efter att Israels exportsystem skärptes, infört en policy för mänskliga rättigheter och en rutin för tillbörlig aktsamhet med avseende på mänskliga rättigheter. Som beskrivs i NSO Groups transparens- och ansvarsrapport för 2021 kräver NSO Group att alla avtal med kunder innehåller paragrafer om efterlevnad av mänskliga rättigheter och paragrafer om indragning eller avslutad användning av NSO Groups produkter vid människorättsrelaterat missbruk. I ett skriftligt meddelande till PEGA bekräftade NSO Group att man har sagt upp avtal med EU-medlemsstater[820] som kan ska ha brutit mot

[813] Apple ‘Apple sues NSO Group to curb the abuse of state-sponsored spyware’.
[814] Bloomberg Law, ‘NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware’.
[815] Bloomberg, ‘Israeli Spyware Firm NSO Seen at Risk of Default as Sales Drop’.
[816] Svar som gavs av NSO Group till PEGA-sekretariatet efter utfrågning, 20 juli 2022.
[817] Amnesty International, ‘Operating from the shadows - inside NSO Group’s corporate structure’.
[818] Amnesty International, ‘Operating from the shadows - inside NSO Group’s corporate structure’.
[819] PEGA-kommitténs utfrågning av NSO, 21 juni 2022.
[820] PEGA-kommitténs utfrågning av NSO, 21 juni 2022.

människorättsparagraferna. NSO Group har inte klargjort om den granskade revisionsloggarna och huruvida kunderna i fråga gett sitt samtycke till en sådan granskning. Det är därför inte känt om det fortfarande finns några bevis på missbruket, om NSO har något sätt att bevara den bevisningen eller om de israeliska myndigheterna har några bevis.

462. Enligt Amnesty International saknar NSO Groups transparensrapport en ordentlig åtgärdspolicy för personer som är föremål för olaglig övervakning, och det finns ingen information om de pågående rättsprocesserna mot NSO Group[821]. NSO:s spionprogram upptäcks fortfarande på enheter tillhörande journalister och kritiker av auktoritära regimer, i strid med NSO:s policy för mänskliga rättigheter och en rutin för tillbörlig aktsamhet med avseende på mänskliga rättigheter[822].

EXPORTKONTROLLER

463. Eftersom Pegasus spionprogram klassificeras som en teknik med dubbla användningsområden måste det få exportlicens. NSO Groups företag får sina exportlicenser i Israel, Bulgarien och Cypern[823]. NSO Group har själv bekräftat detta, men förnekar att Pegasus spionprogram exporteras från Cypern och Bulgarien[824]. De cypriotiska och bulgariska regeringarna har vägrat att bevilja exporttillstånd till NSO-företag i allmänhet. Andra källor har ifrågasatt detta och uppgett att dotterbolag till NSO ofta gömmer sig bakom ett annat namn i nationella företagsregister Ett av NSO:s dotterbolag i Cypern, med namnet Circles stängde sina kontor under 2020[825]. Licenser beviljas också av de israeliska myndigheterna[826]. Israel ingår inte i Wassenaar-avtalet utan uppger att landet har införlivat vissa av dess delar i Israels nationella lag om exportkontroll på försvarsområdet nr 5766-2007[827]. Försvarsministeriets kontrollorgan för export av försvarsprodukter ansvarar för utfärdandet av marknadsförings- och exportlicenser[828]. Efter avslöjandena om Pegasus-projektet och svartlistningen av NSO har listan över berättigade länder minskats från 102 till 37, som alla behöver underteckna ett slutanvändnings/slutanvändarcertifikat[829]. Inom ramen för förfarandet om tillbörlig aktsamhet anser Israel automatiskt att alla EU-medlemsstater uppfyller EU:s normer, så Israel kommer inte att göra några ytterligare bedömningar för enskilda länder. Beslutet att säga upp avtalen med två EU-medlemsstater verkar dock tyda på att EU inte längre betraktas som en enda enhet när det gäller tillbörlig aktsamhet.

OETISKT BETEENDE SOM UTLÖSER STÄMNINGAR, SVARTLISTNING OCH INVESTERARKONFLIKTER

464. I juli 2021 började en konflikt mellan Novalpina Capitals tre samgrundare påverka NSO Groups verksamhet och vilket slutligen tvingade investerarna till beslutet att frånta

[821] Amnesty International, 'NSO Group's new transparency report is "another missed opportunity"', pressmeddelande, 1 juli 2021.
[822] New York Times, 'U.S. Blacklists Israeli Firm NSO Group Over Spyware'.
[823] Amnesty International, 'Operating from the shadows – inside NSO Group's corporate structure', s. 62.
[824] Amnesty International, 'Operating from the shadows – inside NSO Group's corporate structure'.
[825] VICE, 'NSO Group Closes Cyprus Office of Spy Firm'.
[826] Amnesty International, 'Operating from the shadows – inside NSO Group's corporate structure'.
[827] Europaparlamentets utredningstjänst,'Europe's PegasusGate – countering spyware abuse'.
[828] Amnesty International, 'Novalpina Capital's reply to NGO coalition letter (15 april 2019) and Citizen Lab letter (6 mars 2019)'.
[829] Europaparlamentets utredningstjänst,'Europe's PegasusGate – countering spyware abuse'.

privatkapitalbolaget kontrollen[830]. Den 27 augusti 2021 tog det amerikanska konsultföretaget Berkeley Research Group (BRG) över privatkapitalfonden och inledde kritiska utredningar om lagligheten i NSO Groups verksamhet och dess efterlevnad av USA:s svartlistning. BRG-utredningarna i maj 2022 hindrades av NSO Groups ledningsgrupp[831]. En BRG-chef uppgav att samarbetet med NSO Group praktiskt hade upphört på grund av NSO Groups påtryckningar för fortsatt försäljning till länder med ett kontroversiellt förflutet på människorättsområdet[832]. Den 25 april 2022 väckte två av Novalpinas tidigare generalpartner åtal vid en luxemburgsk domstol mot BRG och krävde att Novalpina Capital skulle återinsättas som en allmän partner och att alla beslut som fattats av BRG skulle skjutas upp[833]. Den luxemburgiska domstolen avfärdade dessa krav och BRG ansvarar fortfarande för den fond som kontrollerar NSO Group[834].

465. Utöver de ägarskapsrelaterade sidoverkningarna placerade Förenta staternas handelsdepartement den 3 november 2021 NSO Group på en svart lista pga. att NGO:s verksamhet var oförenlig med amerikanska angelägenheter gällande utrikespolitik och nationell säkerhet. Den amerikanska administrationen förbjuder export av teknik till NSO Group och dess dotterbolag, vilket de facto innebär att inget amerikanskt företag kan arbeta med NSO Group[835].

466. Credit Suisse, en av NSO Groups fordringsägare, påstås ha reagerat på den amerikanska svartlistningen genom att mana på företaget att fortsätta sin försäljning av Pegasus-spionprogrammet till nya kunder. I ett brev till BRG från Willkie Farr & Gallagher uppgav flera fordringsägare att de var bekymrade över att BRG hindrade NSO Group ”från att skaffa sig nya kunder och behålla dem”. Även om det inte uttryckligen angavs i skrivelsen uppgav två experter i frågan att en av borgenärerna var Credit Suisse. BRG svarade långivarna att man var djupt oroad över att NSO Group pressades till mer försäljning[836].

467. Några dagar efter att Förenta staterna svartlistat NSO bekräftade Förenta staternas appellationsdomstol att man kunde gå vidare med Metas stämningsansökan mot NSO. Omedelbart därefter lämnade Apple in ett klagomål mot NSO vid den federala domstolen[837]. I juni 2022 avslog Förenta staternas distriktsdomstol NSO Groups anspråk på immunitet i stämningen från Apple[838]. I skrivande stund är Apples stämning mot NSO Group fortfarande pågående.

468. Trots att Förenta staterna svartlistade NSO ska Bidenadministrationen ha valt in en f.d. rådgivare, Jeremy Bash, åt NSO i en rådgivande underrättelsenämnd i oktober 2022. På uppdrag av Beacon Global Strategies rapporteras Bash ha anlitats för att ge råd åt NSO Group genom Francisco Partners. Enligt The Guardian var han en av de åtta ledamöterna i NSO:s affärsetiska kommitté, vilket ska ha gett honom rösträtt vid NSO:s föreslagna försäljningar. Beacon Global Strategies avslutade sitt arbete med NSO efter

---

[830] Financial Times, ‘Private equity owner of spyware group NSO stripped of control of €1bn fund’.
[831] Financial Times, ‘NSO Group keeping owners ‘in the dark”, manager says’.
[832] The New Yorker, ‘How democracies spy on their citizens’.
[833] Letter to Mr Jeroen Lenaers and his Vice-Chairs.
[834] Luxembourg Times, ‘Top five stories you may have missed’.
[835] New York Times, ‘U.S. Blacklists Israeli Firm NSO Group Over Spyware’.
[836] Financial Times, ‘Credit Suisse pushed for spyware sales at NSO despite US blacklisting’.
[837] New York Times, ‘Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones’.
[838] https://www.docketalarm.com/cases/California_Northern_District_Court/3--21-cv-09078/Apple_Inc._v._NSO_Group_Technologies_Limited_et_al/35/.

den försäljning som bedrevs till Saudiarabien[839].

469. NSO Group har likaså drabbats av personalavgångar. Efter mordet på Jamal Khashoggi och den växande oron över Pegasus roll i detta har många anställda lämnat NSO Group. Samma månad avgick medgrundaren Shalev Hulio som vd för NSO Group och ersattes av Yaron Shohat[840]. NSO Group ändrade policy och är nu enbart inriktade på Natomedlemmar[841]. I mars 2023 rapporterades att aktier i NSO hade överförts till Omri Lavies värdepappersföretag Dufresne Holding[842].

470. Trycket på NSO Group har skapat efterfrågan på andra spionprogramföretag. Financial Times rapporterade den 31 mars 2023 att den indiska regeringen ska ha letat efter en möjlighet att köpa alternativa kommersiella spionprogram med liknande funktioner som det nu kontroversiella spionprogrammet Pegasus, och att den även beaktade Intellexas spionprogram Predator[843].

471. I oktober 2022 lanserade Shalev Hulio och Österrikes före detta förbundskansler Sebastian Kurz ett nytt cybersäkerhetsföretag under namnet Dream Security. Sebastian Kurz avgick som förbundskansler efter en korruptionsskandal i oktober 2021 och började arbeta för Peter Thiels investmentbolag två månader senare. Företaget kommer att ta fram lösningar på cyberincidenter genom att koncentrera sig på artificiell intelligens och fokusera sin försäljning till den europeiska marknaden[844]. Samarbetet mellan Kurz och Hulio utgör en indirekt men alarmerande koppling mellan spionprogramsindustrin och Peter Thiel och hans företag Palantir.

472. Dream Security samlade in 20 miljoner US-dollar från flera investerare, t.ex. Adi Shalev, som också deltog i investeringar i NSO. Bland de andra investerarna hittar man Yevgeny Dibrov[845], som företräder ”den nya ryska rösten” i vad han kallar ”det rysk-israeliska tekniska ekosystemet”[846]. Detta visar att samma namn fortsätter att lansera nya spionprogramföretag inom och utanför EU, trots den turbulens och de ekonomiska utmaningar som NSO Group ställts inför.

BLACK CUBE

473. Black Cube är en israelisk privat underrättelsetjänst som består av före detta anställda vid den israeliska militären samt den israeliska underrättelsetjänsten[847]. Företagets egen webbplats beskriver det som en ”kreativ underrättelsetjänst” som tar fram ”skräddarsydda lösningar på komplexa företagsrelaterade utmaningar och rättsliga tvister”[848]. Black Cube har varit inblandat i ett antal offentliga hackningskontroverser i

[839] The Guardian, ‘Biden intelligence advisor previously vetted deals for Israeli NSO Group’.
[840] Washington Post, ‘CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup’; Calcalist, ‘After cutbacks and CEO departure, what’s next for the controversial NSO?’.
[841] The Guardian, ”CEO of Israeli Pegasus spyware firm NSO to step down”.
[842] The Guardian ”NSO Group co-founder emerges as new majority owner”.
[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’; The Times, ‘Former NSO CEO and ex-Austrian Chancellor found startup’.
[845] The Times, ‘Former NSO CEO and ex-Austrian Chancellor found startup’.
[846] Calcalist, ‘From Russia, With Coding Skills’.
[847] The New Yorker, https://www.newyorker.com/news/annals-of-espionage/the-black-cube-chronicles-the-private-investigators, 7 oktober 2019.
[848] https://www.blackcube.com/.

länder som USA och Rumänien[849]. Närmare bestämt erkände cheferna för Black Cube att de hade spionerat på den tidigare chefsåklagaren för Rumäniens nationella direktorat för korruptionsbekämpning, Laura Kövesi[850]. Kövesi är för närvarande den första europeiska chefsåklagaren, dvs. chef för Europeiska åklagarmyndigheten (Eppo). Den tidigare rumänska hemliga agenten, Daniel Dragomir, ska ha varit den person som beställde Black Cube för jobbet[851].

474. Framför allt har det också avslöjats att Black Cube har kopplingar till NSO Group och spionprogrammet Pegasus. Efter stora påtryckningar från allmänheten om det faktum att NSO anlitar Black Cube för att göra sina motståndare till måltavlor erkände NSO:s tidigare VD, Shalev Hulio, att de anlitat Black Cube i åtminstone en situation på Cypern.

475. Black Cube verkade i Ungern under valet 2018, när det spionerade på flera olika icke-statliga organisationer och personer som hade något slags koppling till George Soros och rapporterade till Viktor Orbán, så att han skulle kunna använda uppgifter om deras aktiviteter i en smutskastningskampanj[852]. Informationen som samlades in genom övervakningen av dessa personer och organisationer dök inte bara upp i de ungerska statligt kontrollerade medierna, utan även i Jerusalem Post[853].

INTELLEXA ALLIANCE

476. Under 2019 inrättades Intellexa på Cypern av Tal Dilian. Dilian hade olika ledarpositioner i den israeliska försvarsstyrkan innan han inledde en karriär som ”underrättelseexpert, samhällsbyggare och serieföretagare”[854]. På sin webbplats beskrivs Intellexa Alliance som ett EU-baserat och EU-reglerat företag vars syfte är att utveckla och integrera teknik för att stärka underrättelsetjänster. De övervakningssäljare som ingår i Intellexa Alliances marknadsföringsetikett är Cytrox, WiSpear (som senare bytte namn till Passitora Ltd), Nexa-teknik (drivs av tidigare chefer i Amesys) och Poltrex.

477. Alla dessa leverantörer främjar olika system. Medan Cytrox kan extrahera data från mobiltelefoner kan man med hjälp av Nexa-tekniken utnyttja globala mobilkommunikationssystem. WiSpear kan också extrahera data från trådlösa nätverk. De olika leverantörerna inom ramen för Dilians allians tillhandahåller således ett brett urval av programvara och tjänster som Intellexa kan erbjuda sina kunder, var för sig eller i kombination, inom och utanför EU[855].

478. Intellexa Alliances moderbolag, Thalestris Limited, har olika dotterbolag som är etablerade i Irland, i Grekland, på Brittiska Jungfruöarna, i Schweiz och i Cypern. Sara

---

[849] The New Yorker, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens, 18 april 2022.
[850] Balkan Insight. ”Intelligence Firm Bosses Plead Guilty in Romania Surveillance Case”.
[851] Haaretz. ”Black Cube CEO Suspected of Running Crime Organisation – Revealed: The Romania Interrogation”.
[852] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.
[853] Politico, https://www.politico.eu/article/viktor-orban-israeli-intelligence-firm-targeted-ngos-during-hungarys-election-campaign-george-soros/, 6 juli 2018.
[854] Tal Dilian. About.
[855] Haaretz, ‘As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire’.

Aleksandra Hamou, som enligt uppgift är Tal Dilians andra f.d. hustru, har varit direktör för Thalestris Limited och verkställande direktör för ett dotterbolag med säte i Grekland[856]. Hamou, som är född i Polen, har ett cypriotiskt pass som har utfärdats av Polens ambassad i Cypern[857].

WISPEAR OCH CYTROX

479. År 2013 startade Tal Dilian ett cypriotiskregistrerat företag under namnet Aveledo Ltd, senare kallat Ws WiSpear Systems Ltd. och därefter Passitora Ltd.[858], som är baserat i Limassol Cypern. WiSpear säljer främst utrustning och programvara för att lokalisera och spåra personer via deras mobiltelefoner. I en intervju med Forbes Magazine förklarade Dilian kapaciteten hos WiSpears programvara genom att visa sin 9 miljoner dollar svarta skåpbil som kan hacka enheter inom ett intervall på 500 meter. WiSpear äger också utrustning som kan fånga upp data från trådlösa nätverk[859]. Offentliga skandaler om dessa produkter ledde till att Intellexas huvudsakliga affärsverksamhet flyttades från Cypern till Grekland.

480. År 2017 grundades Cytrox Holdings Zrt. i Nordmakedonien av Ivo Malinkovski. Cytrox kom dock från Tel Aviv, och Malinkovski var bara en bulvan. Efter avslöjandena om Pegasusprojektet försökte Malinkovski radera alla spår som kopplade honom till Cytrox.

481. Cytrox utvecklade spionprogrammet Predator. Till skillnad från spionprogrammet Pegasus kräver Predator att målet klickar på en länk för att installera programvaran[860]. När Cytrox höll på att gå i konkurs räddade Tal Dilian företaget genom att förvärva det för mindre än 5 miljoner US-dollar[861]. Cytrox slogs sedan ihop med Dilians WiSpear[862]. Detta förvärv lade till spionprogrammet Predator till Intellexa-teknikens arsenal. Enligt rapporter från Lighthouse Reports, i samarbete med Haaretz och Inside Story, levererade Intellexa i hemlighet och olagligt spionprogrammet Predator till den sudanesiska milisen Rapid Support Force, i ett privat Cessnaplan[863].

482. Enligt CitizenLab har två Cytrox-företag registrerats i Israel Cytrox EMEA Ltd. och Cytrox Software Ltd) och ett i Ungern som (Cytrox Holdings Zrt.)[864]. Alla aktier i Cytrox Holdings Zrt. och Cytrox EMEA Ltd. – som senare döptes om till Balinese Ltd. – överfördes till Aliada Group Inc. som är registrerat på Brittiska Jungfruöarna. Aliada Group äger också WiSpear. De största aktieägarna i Aliada Group är Dilian själv, Oz Liv, Meir Shamir och Avi Rubinstein. I december 2020 lämnade Rubinstein in ett klagomål mot de andra aktieägarna i Aliada Group för den olagliga utspädningen av hans aktier. Enligt stämningsansökan kringgick omlokaliseringen av aktier till Brittiska

---

856 Thalestris Limited, Annual Report and Consolidated Financial Statements for the period from 28 November 2019 to 31 December 2020.
857 ReportersUnited 'The Great Nephew and Big Brother'.
858 Open Corporates, 'Passitora Ltd', https://opencorporates.com/companies/cy/HE318328.
859 Haaretz, 'As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire'.
860 Europaparlamentets utredningstjänst, "Greece's Predatorgate. The latest chapter in Europe's spyware scandal?"
861 BalkanInsight, 'Wine, Weapons and Whatsapp: A Skopje Spyware Scandal'.
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'.

Jungfruöarna och senare till Irland israeliska och utländska exportkontrolllagar[865].

483. Den 16 december 2021 offentliggjorde CitizenLab en rapport om att troliga predatorkunder hade påträffats i Armenien, Egypten, Grekland, Indonesien, Madagaskar, Oman, Saudiarabien och Serbien[866].

AMESYS OCH NEXA TECHNOLOGIES

484. Amesys och Nexa Technologies ingår också i Intellexa Alliance och är inte fria från kontroverser, såsom nämns i kapitlet om Frankrike.

POLTREX

485. Poltrex lanserades i oktober 2018 och företagets enda aktieägare var Intellexa Ltd som är registrerat på Brittiska Jungfruöarna. Israeliske Shahak Avni – grundare av det cypriotiska NCIS Intelligence Services Ltd[867] och en partner till Tal Dilians – registrerades som direktör för Poltrex i september 2019. I oktober 2019 blev både Avni och Dilian direktörer och Poltrex bytte namn till Alchemycorp Ltd. Även om företaget hade bytt namn var dess kontor fortfarande kvar i Novel Tower, samma plats som WiSpears kontor[868].

486. När utredningarna om Dilians spionprogramsbil pågick överfördes ägandet av Alchemycorp Ltd. till Yaron Levgoren, anställd vid Cytrox Holdings[869]. Enligt Levgorens LinkedIn-profil företräder han för närvarande Intellexa-företaget Apollo Technologies, som har sitt säte i Grekland[870].

VERINT/COGNYTE

487. Verint är ett israeliskt-amerikanskt cyberföretag med dotterbolag över hela världen. Bara i Europa är Verint registrerat i Bulgarien, Nederländerna, Cypern, Tyskland och Frankrike (från 2021). Verint hade också dotterbolag som verkade under namnet Cognyte. Dessa dotterbolag har varit fristående sedan 2021, när Verint överlät sin underrättelse- och cyberverksamhet till Cognyte[871]. Cognytes europeiska dotterbolag är registrerade i Cypern (UTX Technologies), Bulgarien (Cognyte Bulgaria EOOD), Nederländerna (Cognyte Netherlands B.V.), Tyskland (Syborg GmbH, Syborg Grundbesitz GmbH och Syborg Informationsysteme b.h. OHG) och Rumänien (Cognyte Romania S.R.L.)[872].

488. Verint har sålt övervakningsverktyg till flera regeringar som utövar förtryck, bland annat i Azerbajdzjan, Indonesien och Sydsudan. I det senare fallet använde den sudanesiska nationella säkerhetstjänsten Verints avlyssningsutrustning mot

---

[865] Citizen Lab, 'Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware'.
[866] Citizen Lab, 'Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware', 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'.
[868] CyprusMail, 'Akel says found 'smoking gun' linking Cyprus to Greek spying scandal'.
[869] Philenews, 'How the spyware scandal in Greece is related to Cyprus'.
[870] https://ca.linkedin.com/in/yaron-levgoren-116948101.
[871] Calcalistech, 'Verint completes spin-off of its defense activities into new company Cognyte Software'.
[872] https://www.sec.gov/Archives/edgar/data/1824814/000182481421000007/exhibit81.htm.

människorättsaktivister och journalister mellan mars 2015 och februari 2017. Enligt en utredning som utförts av Amnesty International gjorde den lokala mobiloperatören Vivacell Network of the World det möjligt för den sudanesiska nationella säkerhetstjänsten att lyssna på all telekommunikation i landet[873]. Verint svarade inte på Amnestys frågor, men gjorde ett uttalande som beskriver hur Verints fristående enhet Cognyte i själva verket är försvarsenheten medan Verint endast hanterar kundfrågor. Verint hävdar att uppdelningen med Cognyte hade varit på plats flera år före den officiella avknoppningen 2021, och därmed distanserade sig det från den påstådda exporten av övervakningsutrustning till länder som uppvisar bristande respekt för de mänskliga rättigheterna[874].

489. Cognyte har också exporterat till länder som uppvisar bristande respekt för de mänskliga rättigheterna. I en undersökning som utfördes av Meta 2021 identifierades kunder i Israel, Serbien, Colombia, Kenya, Marocko, Mexiko, Jordanien, Thailand och Indonesien[875]. Cognytes dotterbolag UTX Technologies, som är registrerat i Cypern, uppges också ha erhållit licenser för export av övervakningsprogramvara till Mexiko, Förenade Arabemiraten, Nigeria, Israel, Peru, Colombia, Brasilien, Sydkorea och Thailand mellan september 2014 och mars 2015[876]. Fyra av dessa länder identifierades också som Cognyte-kunder i Metarapporten 2021. Dessutom säkerställde UTX Technologies också ett avtal med Bangladesh om ett webbaserat underrättelsesystem för 2 miljoner dollar 2019 och ett mobilt spårningssystem för 500 000 dollar 2021[877].

490. Den 15 januari 2023 rapporterade media att det israeliska företaget Cognyte Software Ltd hade vunnit en upphandling om försäljning av sitt spionprogram för avlyssning till Myanmar, en månad före militärkuppen i februari 2021. Myanmar köpte officiellt Cognytes spionprogram den 30 december 2020[878].

491. Förutom att exportera till tredjeländer har Cognyte underlättat transporten av spårningsutrustning till medlemsstaterna. Genom Cypernregistrerade UTX Technologies levererades Gi2-tekniken till ett annat dotterbolag till Cognyte i Tyskland, Syborg Informationsysteme[879]. Denna Gi2-teknik ska också ha skickats till ett av Verints dotterbolag i Polen ”för demonstrationsändamål”. Gi2-tekniken har möjlighet att få tillgång till en viss enhet och kan till och med utgöra sig för att vara ägaren och skicka falska meddelanden via samma enhet[880]. Dessa transporter ägde rum mellan 2013 och 2014. Vid den tidpunkten tillhörde Verint och Cognyte fortfarande samma företagsstruktur.

492. UTX Technologies sålde också övervakningssystem 2013 till ett franskt exportföretag med namnet COFREXPORT[881]. Detta företag har upphört med sin verksamhet och har stängt ner när detta skrivs.

---

[873] Haaretz, ‘Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds’; Amnesty International, ‘South Sudan: rampant abusive surveillance by NSS instils climate of fear’.
[874] Haaretz, ‘Israeli Cyber Firm Sold Spytech to South Sudan, Investigation Finds’.
[875] Meta, Threat Report on the Surveillance-for-Hire Industry.
[876] Philenews, ‘Cyprus is a pioneer in software exports’ (documents).
[877] Haaretz, ‘Israeli Spy Tech Sold to Bangladesh, Despite Dismal Human Rights Records’.
[878] Reuters, ‘Israel’s Cognyte won tender to sell intercept spyware to Myanmar before coup’ (documents).
[879] https://www.sec.gov/Archives/edgar/data/1824814/000119312521008526/d52351dex81.htm.
[880] Philenews, ‘Cyprus is a pioneer in software exports’ (documents).
[881] Philenews, ‘Cyprus is a pioneer in software exports’ (documents).

493. Liksom många andra leverantörer av spionprogram har Cognyte en mycket komplex företagsstruktur på grund av namnändringar, uppdelningar och avknoppningar över tid. Cognyte-dotterbolagen visar emellertid att EU:s medlemsstater inte bara används som baser för export av övervakningsutrustning, utan också som fotfäste för försäljning och transport av övervakningsutrustning inom Europa Israeliska spionprogramföretag drar därmed nytta av EU:s inre marknad, som underlättar transporten av deras utrustning både till deras egna dotterbolag och till nya företag som är registrerade i EU:s medlemsstater.

QUADREAM

494. QuaDream är ett israeliskt företag som grundades av en tidigare högre tjänsteman från Israels militära underrättelsetjänst, Ilan Dabelstein, och tidigare anställda vid NSO Guy Geva och Nimrod Rinsky Företaget är bäst känt för sin spionprogramsprodukt Reign, som påstås använda sig av nollklick och har en självförstörande funktion som raderar alla infektionsspår Denna typ av spionprogram har olika funktioner, till exempel att spela in ljud, spåra platser, söka efter filer och ta bilder genom båda kamerorna.[882]

495. Enligt Citizen Lab och en Microsoft Threat Intelligence-analys fungerar QuaDream-system från Bulgarien, Tjeckien, Ungern, Rumänien, Ghana, Israel, Mexiko, Singapore, Förenade Arabemiraten och Uzbekistan. Det finns dessutom minst fem mål för det civila samhället i Nordamerika, Centralasien, Sydostasien, Europa och Mellanöstern.[883]

496. Under 2017 registrerades ett företag i Cypern under namnet InReach. Detta företag grundades enbart för att främja QuaDreams produkter, såsom Reign, utanför Israel. Enligt uppgift använde QuaDream InReach för att sälja sina produkter till kunder för att kringgå israeliska exportkontroller. Många av de viktigaste anställda vid båda företagen har arbetat för NSO Group, Verint och UT-X Technologies.[884]

497. Efter Citizen Labs rapportering och Microsoft Threat Intelligence-analys tillkännagavs den 16 april 2023 att QuaDream hade upphört med sin verksamhet i Israel. Enligt Haaretz hade företaget kämpat med sjunkande försäljningar och avgångar från anställda under de föregående månaderna[885].

CANDIRU

498. Candiru är ett annat israeliskt registrerat företag som tillverkar spionprogram. Företaget

---

[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/.
[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.

grundades 2014 av Ya'acov Weitzman och Eran Shorer. Båda grundarna har en historia i Israeliska försvarsmaktens militära underrättelseenhet 8200 och båda två var tidigare anställda i NSO Group[886]. F.d. investerare i NSO Group, Isaac Zack, blev Candirus största aktieägare. Företaget säljer spionprogram för hackning av datorer och servrar[887]. Information om ett projektförslag visar att Candiru säljer sin utrustning på grundval av antalet samtidiga infektioner, dvs. antalet enheter som kan utsättas för spionprogrammet samtidigt. För 16 miljoner US-dollar får en kund till exempel ett obegränsat antal spionprogramsförsök, men kan bara rikta in sig på 10 enheter samtidigt. En kund kan köpa kapaciteten för att rikta in sig på ytterligare 15 enheter för ytterligare 1,5 miljoner US-dollar[888].

499. Enligt en undersökning från TheMarker erbjuder Candiru nu också spionprogram för att ta sig in i mobila enheter[889]. Det säljer bara sitt spionprogram till regeringar och har kunder i Europa, före detta Sovjetunionen, Persiska viken, Asien och Latinamerika[890]. I avsnittet om Spanien nämns att 65 personer hade utsatts för spionprogram: Av dessa utsattes fyra med Candiru och minst två utsattes med både Candiru och Pegasus[891].

500. Precis som med de andra spionprogramleverantörerna ligger obfuskering detta företag varmt om hjärtat. Det har genomgått flera namnändringar under de senaste åren. Företaget bytte namn till DF Associates Ltd. 2017, Grindavik Solutions Ltd 2018, Taveta Ltd 2019 och senast till Saito Tech Ltd 2020[892]. För tydlighetens skull hänvisar denna rapport till företaget som Candiru.

501. Precis som NSO Group placerades Candiru på Förenta staternas svarta lista av landets handelsdepartement i november 2021. Det spekuleras att orsaken till svartlistningen av Candiru är att VD:n för NSO Group, Shalev Hulio, ska ha varit en hemlig partner till Candiru, som introducerade företaget för viktiga mellanhänder i underrättelsevärlden. Enligt uppgifter har Hulio rent av hävdat att Candirus produkt i själva verket är en ompaketering av Pegasus[893]. Den 1 juli 2022 identifierade säkerhetsforskare en ny dagnollsårbarhet i Chrome som Candiru använde för att göra individer i Libanon, Palestina, Jemen och Turkiet till måltavlor[894]. Sårbarheten åtgärdades Google och har sedan dess även korrigerats av Microsoft och Apple[895].

TYKELAB OCH RCS LAB

502. I augusti 2022 rapporterade Lighthouse Report att Tykelab, ett företag med säte i Rom och som tillhör RCS Lab, hade använt dussintals telefonnät, ofta på öarna i södra Stilla

---

[886] Haaretz '"We're on the U.S. Blacklist Because of You": The Dirty Clash Between Israeli Cyberarms Makers'.
[887] Haaretz, 'Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed'.
[888] Citizen Lab, 'Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus'.
[889] Haaretz, 'Cellphone Hacking and Millions in Gulf Deals: Inner Workings of Top Secret Israeli Cyberattack Firm Revealed'.
[890] Citizen Lab, 'Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus'.
[891] Citizen Lab, 'CatalanGate. Extensive Mercenary Spyware Operations against Catalans Using Pegasus and Candiru'.
[892] Citizen Lab, 'Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus'.
[893] Haaretz, '"We're on the U.S. Blacklist Because of You": The Dirty Clash Between Israeli Cyberarms Makers'.
[894] TechCrunch, 'Spyware maker Candiru linked to Chrome zero-day targeting journalists'.
[895] The HackerNews, 'Candiru Spyware Caught Exploiting Google Chrome Zero-Day to Target Journalists'.

havet, för att skicka tiotusentals hemliga ”spårningspaket” runt om i världen, med inriktning på människor i länder som Italien, Grekland, Makedonien, Portugal, Libyen, Costa Rica, Nicaragua, Pakistan, Malaysia, Irak och Mali. Tykelab utnyttjar sårbarheter i globala telefonnätverk som gör det möjligt för tredje part att se telefonanvändarnas platser och eventuellt avlyssna deras samtal, utan att uppgifter om något misstänkt finns kvar på enheterna[896]. På bara två dagar i juni 2022 undersökte företaget nätverken i nästan alla länder i världen[897]. På sin webbplats uppger Tykelab att man förenar ”20 års erfarenhet av design, implementering och underhåll av kärnnätverkets telekommunikationslösningar, en stark expertis när det gäller att leverera förvaltade tjänster, kundbaserad systemintegration och utveckling av mobilappar”[898].

503. I Lighthouse Reports utredning betonades också telekombranschens roll, med tanke på att leasing av nätanslutningspunkter för telefoner eller ”globala titlar” gör att detta missbruk kan fortsätta. Enligt GSM Association, den branschorganisation som företräder mobilnätsoperatörer över hela världen, kan telefonoperatörerna inte alltid identifiera källan till och syftet med den trafik som passerar genom deras nät, vilket gör det svårt att stoppa detta[899].

504. Tykelab är en del av RCS Lab, ett italienskt företag som är känt för sin avlyssningsverksamhet i Italien och utomlands. Detta framgick av ett tillkännagivande från ett tredje företag, Cy4Gate, som förvärvade RCS Lab. RCS Lab har förgreningar i Frankrike, Tyskland och Spanien[900] samt ett annat hemligt dotterbolag, Azienda Informatica Italiana, som bygger avlyssningsprogram för Android- och iPhone-enheter[901].

SPIONPROGRAMMET HERMIT

505. RCS Lab har utvecklat Hermit, ett spionprogram som kan användas för fjärraktivering av den målinriktade telefonens mikrofon, inspelning av samtal och åtkomst till meddelanden, samtalsloggar, kontaktlistor och foton[902]. I juni 2022 avslöjade Googles hotanalysgrupp att regeringsstödda aktörer som använder RCS Labs spionprogram arbetade med målets internetleverantör för att inaktivera målets mobila dataanslutning. När den väl inaktiverats skickas en skadlig länk via SMS där målet ombads att installera ett program för att återställa sin dataanslutning. Google menar att detta är anledningen till att de flesta av applikationerna maskerades som mobilapplikationer. Om det inte är möjligt att involvera en internetleverantör döljs applikationer som meddelandeapplikationer. De personer som utsätts för RCS Labs spionprogram påträffades i Italien och Kazakstan[903], och spionprogrammet fanns också i Rumänien[904].

506. Justin Albrecht, som forskar om underrättelser om hot vid säkerhetsföretaget Lookout, sa att även om Hermits installationsmetod var mindre sofistikerad än Pegasus, så hade

---

[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/.
[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/.

den liknande kapacitet. Hermit behöver att telefonanvändaren klickar på en infekterad länk för att kunna ta sig in i en enhet[905].

507. Enligt RCS Lab sker ”all försäljning eller implementering av produkter endast efter att företaget har fått ett officiellt godkännande från de behöriga nationella myndigheterna. De produkter som levereras till kunderna installeras i deras lokaler, och personal vid RCS Lab får inte under några omständigheter utföra operativa aktiviteter för att ge kunden stöd eller ha tillgång till de data som behandlas. På grund av bindande sekretessavtal kan RCS Lab inte lämna ut några uppgifter om sina kunder. Cy4gate Group, som RCS Lab är medlem i, efterlever FN:s Global Compact-initiativ och fördömer därför alla former av kränkningar av de mänskliga rättigheterna. RCS Labs produkter har ett tydligt, specifikt och exklusivt ändamål: ”att stödja brottsbekämpande myndigheter för att förebygga och stoppa avskyvärda brott”[906]. Det går dock inte att kontrollera om Cy4gate Group, inklusive RCS Lab, följer sina egna angivna standarder.

508. Enligt en utredning som utfördes av Lighthouse Reports och som offentliggjordes i augusti 2022 användes Tykelabs övervakningsverktyg Hermit för att göra individer till måltavlor runtom i världen, bland annat i Libyen, Nicaragua, Malaysia, Costa Rica, Irak, Mali, Grekland och Portugal – samt i Italien[907].

DECISION SUPPORTING INFORMATION RESEARCH AND FORENSIC (DSIRF)

509. Ett företag som nyligen har blivit föremål för straffrättsliga förfaranden av det österrikiska justitieministeriet är DSIRF GmbH (LLC)[908]. DSIRF grundades 2016 och är ett österrikiskt företag med säte i Wien och ett moderbolag i Liechtenstein. Det påstås tillhandahålla ”uppdragsskräddarsydda tjänster inom informationsforskning, kriminalteknik samt datadrivna underrättelser till multinationella företag inom teknik-, detalj-, energi- och finanssektorerna”[909]. DSIRF säljer uppenbarligen till icke-statliga aktörer.

510. Det DSIRF utvecklade spionprogrammet Subzero/KNOTWEED, som kan distribueras genom att utnyttja dag noll-sårbarheter i Windows och Adobe Reader och som – enligt företagets egen marknadsföring – kan installeras i hemlighet på målenheten. När Subzero har installerats tar det ”full kontroll över måldatorn” och ger ”fullständig åtkomst till alla data och lösenord”. Subzero-kunder kan extrahera lösenord, ta skärmbilder, visa aktuella och tidigare platser och ”komma åt, hämta, ändra och ladda upp filer på måldatorn” via ett webbgränssnitt. DSIRF marknadsför Subzero som ”nästa generations cyberkrigsföring” och säger att verktyget har ”utformats för cyberåldern”[910]. År 2020 värderade DSIRF sin programvara Subzero till 245 miljoner euro.

511. Kopplingen till Ryssland framgår tydligt av kopplingarna för flera av DSIRF:s anställda

[905] https://euobserver.com/digital/155849.
[906] https://euobserver.com/digital/155849.
[907] Lighthouse Reports, ‘Revealing Europe’s NSO’, https://www.lighthousereports.nl/investigation/revealing-europes-nso/.
[908] DSIRF is an abbreviation for “Decision Supporting Information Research and Forensic”
[909] https://dsirf.eu/about/.
[910] https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich/.

på hög nivå. Ägaren till DSIRF är Peter Dietenberger, en ”man med utmärkta kontakter i Kreml” och som ”öppnar dörrar för västerländska företag i Putins imperium”[911]. Dietenberger bodde i Ryssland i flera år och hade ett ryskt företag och flera ryska affärspartner. En av hans ryska affärspartner, Boris Vasilyev, satt också i DSIRF:s styrelse. DSIRF tillhandahåller flera referenser för sitt företag och sina produkter: Michael Harms (VD för det tyska östliga näringslivsförbundet), Stephan Fanderl (styrelseordförande för Galerias Karstadt Kaufhof, som ville etablera Walmart i Ryssland), Christian Kremer (f.d. VD för BMW i Ryssland och VD för Russian Machines, som har sanktionerats av Förenta staterna sedan 2018) och Florian Schneider (partner på den stora affärsadvokatbyrån Dentons i Moskva)[912]. Russian Mahines, ett företag som ägs av oligarken Oleg Deripaska, sägs använda sig av DSIRF:s tjänster. Den mäktige lokala entreprenören Siegfried ”Sigi” Wolf, som rådde den förre förbundskanslern Sebastian Kurz om ekonomiska frågor, betraktas som en av Deripaskas förtrogna[913]. Jan Marsalek, en misstänkt brottsling som är efterlyst via en arresteringsorder som utfärdats av Interpol för näringslivsbedrägerier som uppgår till miljarder, bland annat finansiella och ekonomiska brott, är också inblandad. I augusti 2018 fick han ett e-postmeddelande från Florian Stermann (generalsekreterare för den rysk-österrikiska vänskapsföreningen och som i den allmänna åklagarmyndighetens utredningar betraktas som en av FPÖ:s ”förtrogna”)[914] som innehåll en företagspresentation från DSRIF. Enligt uppgift försökte Marsalek under 2013 sälja spionprogram som tillverkats av det italienska företaget Hacking Team till Grenada. Han sägs gömma sig i Moskva för närvarande där han skyddas av FSB, den ryska säkerhetstjänsten[915].

512. I juli 2022 upptäckte Microsoft att Subzero användes i samband med otillåten skadlig verksamhet för att attackera tio advokatbyråer, banker och strategiska konsultföretag i Österrike, Förenade kungariket och Panama[916]. Österrike har för närvarande ingen rättslig grund för offentliga myndigheters otillåtna utplacering av spionprogram som Subzero, och det skulle också vara olagligt för ett privat företag att använda det mot ett annat. Efter Microsofts offentliggörande, den 28 juli 2022, anmälde den österrikiska icke-statliga organisationen Epicenter.works DSIRF till åklagarmyndigheten i Wien för olaglig åtkomst till datorsystem, skada på data, intrång i datorsystemens funktion, bedrägligt missbruk av databehandling, kriminell organisation och överträdelse av lagen om utrikeshandel och betalningar med avseende på produkter med dubbla användningsområden[917]. Den 7 oktober 2022 uppgav det österrikiska förbundsministeriet för arbetsmarknadsfrågor och ekonomiska frågor att det inte hade utfärdat någon exportlicens till DSIRF[918], och enligt det österrikiska förbundsministeriet

[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/.
[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] Svar från Martin Kocher, Österrikes förbundsminister för digitala och ekonomiska frågor, på den skriftliga frågan till parlamentet från Stephanie Krisper, 7.10.2022, referens 2022-

för rättsliga frågor har åklagarmyndigheten i Wien inlett en brottsutredning om DSIRF[919]. Användningen av spionprogrammet Subzero mot mål i Österrike innebär att en privat eller en offentlig myndighet i Österrike har använt programvaran olagligt, att programvaran har använts av en utländsk aktör och att DSIRF har brutit mot exportrestriktionerna eller att programvaran har exporterats till en annan medlemsstat och använts lagligt eller olagligt mot ett österrikiskt mål. Undersökningen pågår ännu.

FINFISHER

513. Brottsutredningen om och konkursen för FinFisher, ett tidigare spionprogramföretag med säte i München, Tyskland, bör också nämnas i denna rapport. FinFisher är ett nätverk av företag som grundades 2008 och som ursprungligen hade starka band till det brittiska företagsnätverket under varumärket Gamma. FinFisher marknadsförde sitt spionprogram som ett ”komplett it-intrångsportfölj” och dess programvara användes av dussintals länder över hela världen[920], däribland 11 EU-medlemsstater[921] och 13 ”icke-fria” länder[922].

514. 2017 dök FinFishers produkt upp i Turkiet på en falsk version av en mobiliseringswebbplats för den turkiska oppositionen. Programvaran var maskerad som en nedladdningsbar app som rekommenderades för deltagare i regeringsfientliga demonstrationer[923]. FinFisher själv marknadsförde sina produkter som att de enbart användes i brottsbekämpningssyfte. 2019 polisanmäldes FinFisher av Gesellschaft für Freiheitsrechte, Reporter ohne Grenzen, bloggen netzpolitik.org och European Center for Constitutional and Human Rights för att ha exporterat sitt spionprogram utan den exportlicens som krävs från den tyska förbundsmyndigheten för ekonomiska frågor och exportkontroll. Därigenom bröt FinFisher mot EU-förordningen om produkter med dubbla användningsområden och motsvarande tysk nationell lagstiftning. Efter anmälan utredde åklagarmyndigheten i München FinFisher, och i oktober 2020 sökte den igenom 15 affärslokaler som tillhörde FinFisher-gruppen i Tyskland och Rumänien samt privata bostäder. 2021 godkände distriktsdomstolen i München att åklagarmyndigheten beslagtog FinFishers bankkonton för att säkerställa att olagligt erhållna vinster skulle konfiskeras om FinFisher dömdes. FinFisher förklarade sig dock vara insolvent i februari 2022. Affärsverksamheten har upphört, dess kontor har stängts och de 22 anställda har sagts upp[924]. Brottsutredningarna av de personer som ansvarade för FinFishers verksamhet pågår fortfarande.

0.575.143, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12020/index.shtml.

[919] Svar från Alma Zadić, förbundsminister för rättsliga frågor, på den skriftliga frågan till parlamentet från Stephanie Krisper, 7.10.2022, referens 2022-0.575.216, https://www.parlament.gv.at/PAKT/VHG/XXVII/J/J_12019/index.shtml.

[920] https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; https://wikileaks.org/spyfiles4/customers.html.

[921] Belgien, Tjeckien, Estland, Tyskland, Ungern, Italien, Nederländerna, Rumänien, Slovakien, Slovenien och Spanien.

[922] Angola, Bahrain, Bangladesh, Egypten, Etiopien, Gabon, Jordanien, Kazakstan, Myanmar, Oman, Qatar, Saudiarabien och Turkiet.

[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.

III. Europeiska unionens förmåga att reagera

515. Vissa regeringar har riktat in sig på EU-medborgare med hjälp av kraftfulla och mycket invasiva och påträngande spionprogram genom att missbruka sin rätt att tillgripa övervakning i händelser av hot mot den nationella säkerheten. Detta utgör ett hot mot demokratin, rättsstatsprincipen och enskilda medborgares grundläggande rättigheter. EU har få befogenheter att agera mot dessa hot, och visar sig vara dåligt utrustad mot potentiell brottslig verksamhet från nationella myndigheters sida, även om det påverkar EU självt. Enligt fördragen är den nationella säkerheten fortfarande medlemsstaternas exklusiva behörighet, men deras åtgärder måste fortfarande vara förenliga med de grundläggande rättigheter och demokratiska normer som ingår i EU-lagstiftningen. Politiska faktorer begränsar också EU:s handlingskraft. Europeiska kommissionen har som väktare av EU-fördragen inte maximerat sina ansträngningar för att verkställa EU-lagstiftningen genom att använda de rättsliga instrument som står till dess förfogande. Kommissionen tenderar att tolka sina befogenheter mycket snävt, eftersom det nästan uteslutande handlar om ett korrekt införlivande av EU-lagstiftningen i nationell lagstiftning. Kommissionen anser att det är de nationella myndigheternas eget ansvar att ta itu med överträdelser av EU-lagstiftningen. Inför uppenbara kränkningar av rättsstatsprincipen och de grundläggande rättigheterna blir denna hållning – som inte har någon grund i EU-fördragen – mycket problematisk. Även om subsidiaritet och åtskillnad av befogenheter är en pelare i EU-lagstiftningen bör dessa inte leda till straffrihet för regeringar som riktar sig till EU-medborgare med spionprogram för politiska ändamål. Nedan kommer vi att undersöka de befogenheter som EU-institutionerna har till sitt förfogande. Parlamentet, kommissionen och rådet har makten och skyldigheten att lagstifta, reglera och verkställa, och de måste göra det med kraft och ambition och sätta försvaret av vår demokrati framför kortsiktiga politiska överväganden.

Europeiska kommissionen

516. Efter pressrapporter om användningen av spionprogram i medlemsstaterna och frågor från PEGA har kommissionen i sitt svar på spionprogramskandalen inledningsvis bara författat skrivelser med begäran om förtydliganden från regeringarna i Polen, Ungern, Spanien, Grekland, Cypern och Frankrike. Det verkar dock som om kommissionens varning inte har följts av ytterligare åtgärder. Det är sant att kommissionen strängt taget inte har några befogenheter att agera på området för nationell säkerhet. Men som kommissionen själv påpekar i dessa skrivelser bör ”nationell säkerhet” inte tolkas som ett obegränsat undantag från europeiska lagar och fördrag och bli ett område med laglöshet. Det är dock upp till medlemsstaterna att ”visa att den nationella säkerheten skulle äventyras i det aktuella fallet”. Som svar på frågan om vilka åtgärder kommissionen kommer att vidta om de nationella myndigheterna inte grundligt undersöker eventuella anklagelser om olagligt spioneri hänvisar kommissionen endast till EU-domstolen och till artikel 47 i stadgan, som ger rätt till ett effektivt rättsmedel inför en domstol. Det verkar inte finnas någon politisk vilja att agera.

517. Den 21 december 2022 skickade kommissionen dessutom en allmän skrivelse till alla medlemsstater med en begäran om information om nationella myndigheters användning av spionprogram och den rättsliga ram som reglerar sådan användning, i syfte att kartlägga situationen i medlemsstaterna och undersöka samspelet med EU-

lagstiftningen[925]. Kommissionen ställde särskilda frågor om bland annat syftet med användning av spionprogram, de myndigheter som är bemyndigade att använda det, den nationella definitionen av nationell säkerhet, relevant lagstiftning som reglerar behandling av uppgifter för ändamål som rör den nationella säkerheten, skyddsåtgärder, förhandstillstånd från en domstol eller en oberoende administrativ myndighet, tillsyn och anmälan, med en tidsfrist till den 31 januari 2023 för att svara. Den 28 mars 2023 uppgav kommissionsledamot Reynders för PEGA att en stor majoritet av medlemsstaterna hade svarat, men att kommissionen fortfarande höll på att samla in medlemsstaternas svar på kartläggningen, och att den skulle ”noggrant bedöma” svaren. På grundval av denna kartläggning kommer kommissionen att fundera över sina alternativ när det gäller användningen av spionprogram i medlemsstaterna. Inget specifikt slutdatum planeras dock för kommissionens bedömning, ”med tanke på bedömningens ständigt föränderliga och känsliga karaktär”. Kommissionen nämnde också att den skulle följa PEGA:s slutsatser mycket noga.

518. Till skillnad från Förenta staterna, som har svarat på avslöjandena från svartlistade företag, genomfört utredningar, även på EU:s territorium, och utfärdat ett beslut om förbud mot amerikanska federala instansers förvärv av kommersiella spionprogram, har kommissionen hittills inte genomfört någon analys av situationen och inte heller gjort någon bedömning av de företag som är verksamma på spionprogramsmarknaden i EU. Det finns inga uppenbara rättsliga invändningar mot att genomföra en sådan analys. Det är anmärkningsvärt att den omfattande bevisningen ändå inte har fått kommissionen att vidta några meningsfulla åtgärder. Dess passivitet innebär att den är delaktig i kränkningar av de mänskliga rättigheterna och åsidosättande av dess skyldigheter.

519. EU har flera lagar som kan fungera som regleringsverktyg för spionprogram. Utöver lagar som skyddar medborgarnas rättigheter, såsom lagar om dataskydd och integritet vid kommunikation (GDPR, e-integritet[926]), finns det lagar om export (förordningen om dubbla användningsområden) och upphandling. Kommissionens befogenheter som fördragens väktare används dock inte fullt ut. Den tenderar att begränsa sig till att kontrollera om en medlemsstat har införlivat EU-lagstiftningen korrekt i nationell lagstiftning. Detta säger dock mycket lite om den faktiska situationen på plats. Kommissionens genomföranderapport[927] om förordningen om dubbla användningsområden verkar därför dra slutsatsen att genomförandet är på god väg, trots att det finns omfattande bevis för att genomförandet i praktiken är svagt och ojämnt, till och med avsiktligt i vissa länder. Genomförandet av direktivet om integritet och elektronisk kommunikation och rättspraxis som härrör från det är dåligt. Kommissionen hänvisar till medlemsstaterna som ansvariga för genomförande och kontroll av efterlevnaden, men den vidtar inte åtgärder när medlemsstaterna underlåter att utföra dessa uppgifter Utan ett korrekt och meningsfullt genomförande blir EU-lagstiftningen ineffektiv och skapar gott om utrymme för olaglig användning av spionprogram.

520. Syftet med dataskyddsdirektivet för polis- och åklagarmyndigheter var att tillhandahålla höga standarder för dataskydd och säkerställa det fria flödet av uppgifter inom polis- och åklagarsektorerna. Direktivet behövde införlivas i nationell lagstiftning, och gav

[925] Skrivelse från GD Rättsliga frågor till medlemsstaterna. Ref. Ares(2022)8885417, 21 december 2022.
[926] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (EUT L 201, 31.7.2002, s. 37).
[927] https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=COM%3A2022%3A434%3AFIN&qid=1662029750223.

medlemsstaterna bred handlingsfrihet. I dag är det uppenbart att genomförandet skiljer sig mellan medlemsstaterna, särskilt när det gäller registrerades rättigheter. Kommissionen bör snarast utvärdera genomförandet i alla medlemsstater och identifiera de allvarligaste bristerna. Kommissionen bör ta fram konkreta riktlinjer för medlemsstaterna om direktivets genomförande för att säkerställa att EU:s normer respekteras i hela unionen. Dessutom bör kommissionen vid behov inleda överträdelseförfaranden i fall där direktivet inte har införlivats korrekt och där medlemsstaten saknar vilja att korrigera situationen.

Europaparlamentet

521. Europaparlamentet har inrättat undersökningskommittén PEGA, som arbetar omsorgsfullt och effektivt inom ramen för sina befogenheter och sitt mandat. Den har dock inga befogenheter att kalla in vittnen eller höra dem under ed, och den har inte tillgång till sekretessbelagda uppgifter. Den saknar de fullständiga utredningsbefogenheter som de flesta nationella parlament har. Dessutom påverkar de nationella regeringarnas inflytande ofta PEGA:s överläggningar, vilket ibland utgör ett hinder för grundliga, helt oberoende och objektiva utredningar. Det är ganska oroväckande att Europaparlamentet inte har fullständiga befogenheter att utreda när vissa av dess egna ledamöter har utsatts för spionprogram.

Europeiska rådet och ministerrådet

522. Även om de nationella regeringarna hävdar att spionprogramskandalen är en rent nationell fråga diskuterades den faktiskt i Europeiska unionens råd och de nationella regeringarna beslutade att svara kollektivt på Europaparlamentets frågeformulär[928]. Genom att göra detta har de till fullo erkänt att det faktiskt är en fråga för rådet.

523. Hittills har Europeiska rådet inte svarat offentligt eller väsentligt på skandalen. Vissa av dess ledamöter har ett intresse i frågan, eftersom de själva kan vara delaktiga i de olagliga hackningarna, eller så vill de helt enkelt att EU förblir svagt och maktlöst på detta område.

524. Även om olagligt eller brottsligt beteende i slutändan skulle bevisas kunde inte medlemmar av nationella regeringar hindras eller tvingas att avgå från sina EU-jobb. Detta innebär att personer som är skyldiga till sådana handlingar mycket väl kan fortsätta att ostraffat sitta i EU-organ och fatta beslut som påverkar alla EU-medborgare.

Europol.

525. Europol har inga självständiga operativa befogenheter och kan inte agera utan den berörda medlemsstatens eller de berörda medlemsstaternas samtycke och samarbete, i enlighet med artikel 88.3 i EUF-fördraget, medan tvångsmedel endast får tillämpas av de behöriga nationella myndigheterna. Detta utgör ett problem när det finns tydliga bevis för brottsliga handlingar – såsom it-brottslighet, korruption och utpressning – men nationella myndigheter underlåter att utreda. Europol har nyligen fått nya befogenheter som gör det möjligt för Europol att proaktivt föreslå en utredning, även om det rör sig

[928] Draft letter from General Secretariat of the Council to the Delegations, 26 September 2022.

om ett brott som begåtts endast i en medlemsstat[929], men hittills har Europol inte utnyttjat dessa befogenheter.

526. Den 28 september 2022 författade PEGA en skrivelse till Europol[930] och uppmanade byrån att utnyttja sina nya befogenheter enligt artikel 6 i Europolförordningen[931]. I en svarsskrivelse av den 13 oktober 2022[932] uppgav Europol att man ”kontaktat fem medlemsstater för att fastställa om det finns relevant information tillgänglig på nationell nivå för Europol och om det pågår eller planeras en brottsutredning (alternativt en annan utredning enligt tillämpliga bestämmelser i nationell lagstiftning). Den 11 april 2023 uppgav Europol i en skrivelse till PEGA att dess skrivelser hade skickats till Grekland, Ungern, Bulgarien, Spanien och Polen. Efter de fem medlemsstaternas svar på Europols skrivelser nämnde Europol att ingen av dem hade ”relevant information som är tillgänglig för Europol”. I oktober 2022 hade en av de fem medlemsstaterna bekräftat för Europol att ”brottsutredningar har inletts under tillsyn av de behöriga rättsliga myndigheterna, och detta har också kontrollerats av Eurojust”. I december 2022 informerade en andra medlemsstat Europol om att ”ett straffrättsligt förfarande inleddes i samband med den misstänkta olagliga användningen av programvaran Pegasus, som under tiden avslutades av de ansvariga rättsliga myndigheterna i det landet”. En tredje medlemsstat underrättade Europol om att ”förberedande förfaranden har inletts vid en instans på regional nivå” och frågade ”huruvida Europol har tillgång till information om användningen av programvaran Pegasus i respektive land, av relevans för de förberedande förfarandena”. En fjärde medlemsstat informerade Europol om att det inte pågår någon brottsutredning eller planeras”, men att ”rättsliga utredningar hade inletts”. I april 2023 hade den femte medlemsstaten förklarat för Europol att ”efter samråd med de behöriga myndigheterna i det landet finns det ingen relevant information tillgänglig för Europol om olaglig användning av programvara för övervakning och avlyssning, samtidigt som det hänvisas till förberedande förfaranden vid åklagarmyndigheten”. Det är inte känt om ovannämnda straffrättsliga förfaranden i två medlemsstater, förundersökningar i en medlemsstat, rättsliga utredningar i en medlemsstat och förberedande förfaranden vid åklagarmyndigheten i en annan medlemsstat rör missbruk av spionprogram av regeringar i EU:s medlemsstater eller av tredjeländer.

527. EU visar sig vara helt maktlöst mot de nationella myndigheternas potentiella brottsliga verksamhet, även om den påverkar EU.

528. Paradoxalt nog undersöker USA i motsats till Europol aktivt användningen av spionprogram i EU. Den 5 november 2022 rapporterades det att FBI besökte Aten för att ”undersöka hur långt den olagliga övervakningen har spridit sig och vem som smugglat den”[933]. Dessutom utfärdade Förenta staternas president Biden i mars 2023 ett verkställande beslut som till stor del förbjöd amerikanska federala enheter att använda spionprogram. Några dagar senare signalerade andra länder, däribland Frankrike och

[929] Europaparlamentets och rådets förordning (EU) 2022/991 av den 8 juni 2022 om ändring av förordning (EU) 2016/794 vad gäller Europols samarbete med privata parter, Europols behandling av personuppgifter till stöd för brottsutredningar och Europols roll inom forskning och innovation (EUT L 169, 27.6.2022, s. 1).
[930] https://twitter.com/EP_PegaInquiry/status/1576855144574377984.
[931] ”Om den verkställande direktören anser att en utredning bör inledas av ett särskilt brott som rör endast en medlemsstat, men som berör ett gemensamt intresse som omfattas av unionens politik, får han föreslå att den berörda medlemsstatens behöriga myndigheter, via sin nationella enhet, inleder, genomför eller samordnar en sådan brottsutredning.”
[932] Ärende nr 1260379.
[933] https://insidestory.gr/article/ti-ekane-i-epitropi-pega-gia-tis-ypoklopes-stin-athina?token=4U1KNVW1DQ.

Danmark, sitt engagemang för internationellt samarbete i frågan

Europeiskt rättsväsende

529. EU-domstolen och Europadomstolen spelar en viktig roll för att försvara demokratin, rättsstatsprincipen och de grundläggande rättigheterna. De kan dock endast agera på grundval av ett klagomål eller en förrättslig fråga. Förfarandena är mycket långdragna och erbjuder få konkreta rättsmedel i enskilda fall. Under årens lopp har domstolarna skapat en omfattande uppsättning relevant rättspraxis, till exempel att fastställa normer för övervakning. Dessa domstolar har dock ingen möjlighet att se till att deras utslag verkställs. Hittills har ett klagomål om olaglig användning av spionprogram lämnats in till Europadomstolen[934]. Vägen till domstolarna i Strasbourg eller Luxemburg är dock ofta lång, kostsam och besvärlig, eftersom alla alternativ för nationella rättsliga förfaranden först måste uttömmas. Detta gäller särskilt om de nationella åklagarna eller domarna underlåter eller vägrar att ta sig an ett fall. Ribban för att få sitt fall prövat ligger högt.

Ombudsmannen

530. Den 28 november 2022 konstaterade Europeiska ombudsmannen att kommissionen inte bedömde riskerna för de mänskliga rättigheterna tillräckligt innan den bistod afrikanska länder i att utveckla övervakningskapaciteten, särskilt inom ramen för EU:s förvaltningsfond för nödåtgärder i Afrika. Slutsatserna följer av ett klagomål från flera civilsamhällesorganisationer. I Niger anslog fonden 11,5 miljoner euro för leveranser av övervakningsutrustning, inklusive programvara för övervakning, ett avlyssningscenter och en falsk basstation[935], trots att aktivister förtrycks i landet. För att ta itu med de brister som hon identifierade föreslog ombudsmannen förbättringar för att säkerställa att en konsekvensbedömning av mänskliga rättigheter görs före framtida projekt inom EU:s förvaltningsfond för nödåtgärder i Afrika.

Andra EU-organ

531. Europeiska dataskyddsstyrelsen, Europeiska datatillsynsmannen, Europeiska revisionsrätten och Eurojust har få befogenheter att granska eller ingripa i händelse av olaglig användning av eller handel med spionprogram av medlemsstaternas regeringar. Vissa av deras medlemmar kanske är inblandade i skandalerna i sin ursprungsmedlemsstat. Detta kan påverka dessa EU-organs funktion och integritet. Europeiska åklagarmyndigheten skulle kunna ingripa när EU-pengar på något sätt är inblandade.

[934] Appeal by Koukakis to the European Court of Human Rights, 27 July 2022.

[935] https://ec.europa.eu/trustfundforafrica/sites/default/files/final_t05-eutf-sah-ne-05_eci_avenant_1.pdf.

MOTIVERING

EU:s Watergate

Under sommaren 2021 avslöjade Pegasusprojektet, ett kollektiv av grävande journalister, icke-statliga organisationer och forskare, en förteckning över 50 000 personer som hade varit blivit måltavla för legosoldatspionprogram, Bland dem finns journalister, advokater, åklagare, aktivistpolitiker och till och med statschefer. Det mest dramatiska fallet kan mycket väl vara Jamal Khashoggi, den saudiska journalisten, som mördades brutalt 2018 för sin kritik mot den saudiska regimen. Det fanns emellertid också många europeiska mål på listan. Vissa hade varit måltavlor för aktörer utanför EU, men andra för sina egna nationella regeringar. Avslöjandena möttes av upprördhet runtom i världen.

Skandalen fick snabbt etiketten ”EU:s Watergate”. Till skillnad från den politiska thrillern *Alla presidentens män* (*All the President's Men*) om inbrottet i Watergate-byggnaden 1972, påminner dagens spionprogramsskandal om den skrämmande filmen *De andras liv* (*Das Leben der Anderen*) som skildrar den totalitära kommunistregimens övervakning av medborgarna. Dagens digitala inbrott med spionprogram är mycket mer sofistikerade och invasiva, och lämnar knappast några spår. Användningen av spionprogram går långt utöver en persons konventionella övervakning. Det ger spionaktörerna total tillgång och kontroll. I motsats till klassisk avlyssning medger spionprogram inte bara övervakning i realtid, utan även fullständig, retroaktiv åtkomst till filer och meddelanden som skapats tidigare, och även metadata om tidigare kommunikation. Övervakningen kan till och med ske på distans, i länder överallt i världen. Spionprogram kan i huvudsak användas för att ta över en smarttelefon och extrahera allt innehåll, inbegripet dokument, bilder och meddelanden. Material som erhålls på detta sätt används inte bara för att observera handlingar, utan även för att utpressa, misskreditera, manipulera och skrämma offren. Tillgång till offrets system kan manipuleras och tillverkat innehåll kan planteras. Mikrofonen och kameran kan aktiveras på distans och förvandla enheten till en spion i rummet. Offret är under tiden ovetande. Spionprogram lämnar få spår på offrets enhet, och även om det upptäcks är det nästan omöjligt att bevisa vem som var ansvarig för attacken.

Missbruk av spionprogram kränker inte bara individers rätt till privatliv. Det undergräver demokratin och de demokratiska institutionerna i smyg. Det tystar opposition och kritiker, eliminerar granskning och har en avskräckande effekt på den fria pressen och civilsamhället. Det tjänar dessutom till att manipulera valen. Termen ”legosoldatspionprogram” återspeglar mycket väl produktens och branschens karaktär. Även misslyckade försök att infektera en smarttelefon med spionprogram har politiska konsekvenser och kan skada både individen och demokratin. Det blir omöjligt att delta i det offentliga livet utan att vara säker på att man är fri och oövervakad.

Spionprogramskandalen är inte en serie isolerade nationella fall av missbruk, utan ett europeiskt ärende. Regeringarna i EU:s medlemsstater har använt spionprogram på sina medborgare för politiska ändamål och för att dölja korruption och brottslig verksamhet Vissa gick ännu längre och inbäddade spionprogram i ett system som avsiktligt utformades för ett auktoritärt styre. Andra medlemsstaters regeringar kanske inte har ägnat sig åt missbruk av spionprogram, men de har underlättat den obskyra handeln med spionprogram Europa har blivit en attraktiv plats för legosoldatspionprogram. Europa har varit ett exportnav för

förtryckande regimer, såsom Libyen, Egypten och Bangladesh, där spionprogram har använts mot människorättsaktivister, journalister och regeringskritiker.

Missbruket av spionprogram är ett allvarligt brott mot alla EU:s värden och det testar motståndskraften hos den demokratiska rättsstatsprincipen i Europa. Under de senaste åren har EU mycket snabbt byggt upp sin kapacitet att reagera på externa hot mot vår demokrati, vare sig det gäller krig, desinformationskampanjer eller politisk inblandning. Däremot är förmågan att reagera på interna hot mot demokratin fortfarande bedrövligt underutvecklad. Antidemokratiska tendenser kan fritt sprida sig som kallbrand i hela EU, eftersom det finns straffrihet för nationella regeringars överträdelser. EU är dåligt utrustat för att hantera ett sådant angrepp på demokratin inifrån. Å ena sidan är EU i hög grad en politisk enhet som styrs av överstatliga lagar och överstatliga institutioner med en inre marknad, öppna gränser, passlösa resor, EU-medborgarskap och ett gemensamt område med säkerhet, frihet och rättvisa. Å andra sidan, trots högtidliga löften om europeiska värden betraktas dessa värden i praktiken fortfarande i hög grad som en nationell fråga. Spionprogramskandalen avslöjar skoningslöst EU:s omogna och svaga ställning som en demokratisk enhet. När det gäller demokratiska värden bygger EU på nationella regeringars ”presumtion om efterlevnad”, men i praktiken har EU förvandlats till ”förevändningar om efterlevnad”. Scenariot att nationella regeringar avsiktligt ignorerar och bryter mot EU:s lagstiftning förutses helt enkelt inte i EU:s styrningsstrukturer. EU har inte utrustats med instrument för sådana fall. EU-organen har få befogenheter, och ännu mindre vilja, att konfrontera nationella myndigheter vid överträdelser, och definitivt inte inom det känsliga området ”nationell säkerhet”. Med mellanstatlig logik är EU-institutionerna underordnade de nationella regeringarna. Utan effektiva, meningsfulla övernationella tillsynsmekanismer kommer dock ny lagstiftning att vara meningslös. Att lösa problemet kommer att kräva både lagstiftningsåtgärder och styrningsreformer.

Förenta staterna förskonas inte från angrepp på demokratin inifrån, till exempel Watergate, och belägringen av kongressen den 6 januari 2021, men landet är utrustat för att reagera kraftfullt. De har befogenhet att konfrontera även de högsta politiska ledarna när de inte respekterar lagen och konstitutionen.

Efter 2021 års avslöjanden om spionprogram svarade Förenta staterna snabbt och beslutsamt på avslöjandena om Pegasusprojektet. Den amerikanska handelsavdelningen svartlistade snabbt NSO Group, justitiedepartementet inledde en utredning, och man håller på att införa stränga regler för handel med spionprogram. FBI kom även till Europa för att utreda ett spionprogramsangrepp mot en amerikansk-europeisk medborgare med dubbelt medborgarskap. Tech-jättar som Apple och Microsoft har väckt talan mot spionprogramföretag. Brottsoffer har framställt klagomål, åklagare utreder och parlamentariska utredningar har inletts.

Med undantag för Europaparlamentet har de andra EU-institutionerna i stort sett varit tysta och passiva och hävdat att det är en uteslutande nationell fråga.

Europeiska rådet och de nationella regeringarna tillämpar omertà. Det har inte förekommit något officiellt svar på Europeiska rådets skandal. Medlemsstaternas regeringar har i stor utsträckning avböjt inbjudan att samarbeta med PEGA-kommittén. Vissa regeringar vägrade helt enkelt att samarbeta, andra var vänliga och artiga men delade inte riktigt meningsfull information. Inte ens ett enkelt frågeformulär till alla medlemsstater om detaljerna i deras nationella rättsliga ram för användning av spionprogram har fått några konkreta svar. Inför

offentliggörandet av detta förslag till betänkande fick PEGA-utskottet ett gemensamt svar från medlemsstaterna via rådet, även utan innehåll.

Europeiska kommissionen har uttryckt oro och bett några medlemsstaters regeringar om förtydliganden, men endast de fall där en skandal redan hade inträffat på nationell nivå. Kommissionen har motvilligt och gradvis delat information om spionprogramsangreppen mot kommissionens egna tjänstemän.

Europol har hittills vägrat att utnyttja sina nya befogenheter för att inleda en utredning. Först efter att ha pressats av Europaparlamentet skickade det en skrivelse till fem medlemsstater och frågade om en polisundersökning hade inletts och om de kunde vara till hjälp.

Europas sak

Missbruk av spionprogram ses oftast genom den nationella politikens nyckelhål. Den snäva nationella perspektivet fördunklar hela bilden. Det är enbart när man lägger ihop de enskilda bitarna som det står klart att frågan är djupt europeisk i alla dess aspekter.

Även om det inte bekräftas officiellt kan vi på ett säkert sätt anta att alla EU-medlemsstater har köpt en eller flera kommersiella spionprogramsprodukter Enbart ett företag, NSO Group, har sålt sina produkter till tjugotvå slutanvändare i inte mindre än fjorton medlemsstater, varav Polen, Ungern, Spanien, Nederländerna och Belgien I minst fyra medlemsstater, Polen, Ungern, Grekland och Spanien, har det förekommit olaglig användning av spionprogram och det finns misstankar om dess användning på Cypern. Två medlemsstater, Cypern och Bulgarien, fungerar som exportnav för spionprogram. En medlemsstat, Irland, erbjuder förmånliga skattearrangemang för en stor spionprogramsleverantör, och en medlemsstat, Luxemburg, är ett banknav för många aktörer inom spionprogramsindustrin. Den årliga europeiska mässan för spionprogramsindustrin, ISS World ”Wiretappers Ball” (avlyssnarnas bal), hålls i Prag i Tjeckien. Malta verkar vara en populär destination för vissa branschföreträdare. Några slumpmässiga exempel på industrin som använder sig av Europa utan gränser: Intellexa är närvarande i Grekland, Cypern, Irland, Frankrike och Ungern, och dess verkställande direktör har ett maltesiskt pass och (brevlåde)företag. NSO är närvarande i Cypern och Bulgarien och bedriver sin finansiella verksamhet via Luxemburg. DSIRF säljer sina produkter från Österrike, Tykelab från Italien och FinFisher från Tyskland (före nedläggningen).

Handeln med spionprogram gynnas av EU:s inre marknad och den fria rörligheten. Vissa EU-länder är attraktiva som exportnav, eftersom efterlevnaden av exportreglerna är svag trots EU:s rykte om att vara en tuff tillsynsmyndighet. När exportreglerna från Israel skärptes blev EU mer attraktivt för leverantörer. De marknadsför sin verksamhet som ”EU-reglerad”, och använder sin EU-närvaro som en kvalitetsmärkning. ”EU” ger respekt. EU-medlemskap gynnar också regeringar som vill köpa spionprogram: EU:s medlemsstater är undantagna från den individuella bedömning av mänskliga rättigheter som krävs för en exportlicens från de israeliska myndigheterna, eftersom EU-medlemskap anses vara en tillräcklig garanti för att de högsta normerna uppfylls.

Försäljningssidan av handeln med spionprogram är ogenomskinlig och gäckande, men lukrativ och blomstrande. Företagsstrukturer är lämpligt, om inte avsiktligt, komplexa för att dölja oönskade aktiviteter och kontakter, även med EU:s regeringar. På papperet är sektorn

reglerad, men i praktiken lyckas den kringgå många regler, inte minst eftersom spionprogram är en produkt som kan tjäna som politisk valuta i internationella förbindelser. Spionprogramföretag är etablerade i flera länder, men många har inrättats av f.d. israeliska armé- och underrättelsetjänstemän. De flesta leverantörer hävdar att de endast säljer till statliga aktörer, även om vissa säljer till icke-statliga aktörer bakom kulisserna. Det är praktiskt taget omöjligt att få någon information om dessa kunder eller om avtalsvillkoren och efterlevnaden.

Handel med och användning av spionprogram faller helt inom tillämpningsområdet för EU:s lagstiftning och rättspraxis. Inköp och försäljning av spionprogram regleras bland annat av upphandlingsregler och exportregler såsom förordningen om produkter med dubbla användningsområden. Användningen av spionprogram måste uppfylla normerna i dataskyddsförordningen, personuppgiftsförordningen, dataskyddsdirektivet och direktivet om integritet och elektronisk kommunikation. Rättigheterna för målpersoner föreskrivs i stadgan om de grundläggande rättigheterna och internationella konventioner, särskilt rätten till integritet och rätten till en rättvis rättegång, och i EU:s bestämmelser om rättigheterna för misstänkta och anklagade personer. Missbruk av spionprogram kommer i många fall att utgöra it-brottslighet, och det kan innebära korruption och utpressning, som alla faller inom Europols ansvarsområde. Om det rör sig om EU-medel har den europeiska åklagaren mandat att agera. Missbruk av spionprogram kan också påverka polissamarbete och rättsligt samarbete, särskilt utbyte av information och genomförande av den europeiska arresteringsordern och bevishämtningsordern.

Missbruket av spionprogram påverkar direkt och indirekt EU och dess institutioner. Bland dem som var inriktade på spionprogram fanns ledamöter av Europaparlamentet, Europeiska kommissionen och (Europeiska) rådet. Andra påverkades som indirekta mål för bifångster. Omvänt sitter några av ”förövarna” också i (Europeiska) rådet. Dessutom påverkar manipulering av nationella val med hjälp av spionprogram direkt sammansättningen av EU-institutionerna och den politiska balansen i EU:s styrande organ. De fyra eller fem regeringar som anklagas för att missbruka spionprogram utgör nästan en fjärdedel av EU:s befolkning, så de har stor betydelse i rådet.

Spionprogram som en del av ett system

Spionprogram är inte bara ett tekniskt verktyg som används tillfälligt och isolerat. Det används som en integrerad del av ett system. I princip är dess användning inbyggd i en rättslig ram tillsammans med nödvändiga skyddsåtgärder, tillsyns- och granskningsmekanismer samt möjligheter till prövning. Undersökningen visar att dessa garantier ofta är svaga och otillräckliga. Detta är till största delen oavsiktligt, men i vissa fall har systemet – helt eller delvis – utformats för att fungera som ett verktyg för politisk makt och kontroll. I dessa fall är olaglig användning av spionprogram inte en enstaka händelse, utan en del av en avsiktlig strategi. Rättsstatsprincipen förvandlas till härskarens lag. Den rättsliga grunden för övervakning kan utformas i vaga och oprecisa termer för att legalisera en bred och ohämmad användning av spionprogram. Förhandskontroll i form av rättsligt tillstånd för övervakning kan lätt manipuleras och rensas bort av vilken betydelse som helst, särskilt när det gäller politisering, eller statens uppfångande av rättsväsendet. Tillsynsmekanismerna kan hållas svaga och ineffektiva och kontrolleras av de styrande parterna. Rättsmedel och medborgerliga rättigheter kan existera på papperet, men de blir ogiltiga vid obstruktion av statliga organ. Klagande nekas tillgång till information, även gällande anklagelserna mot dem som påstås

motivera deras övervakning. Åklagare, domare och poliser vägrar att utreda och lägger ofta bevisbördan på offren, och förväntar sig att de ska bevisa att de har utsatts för spionprogram. Detta gör att offren befinner sig i en moment-22-situation, eftersom de nekas tillgång till information. Regeringspartierna kan skärpa sitt grepp om offentliga institutioner och medier för att undertrycka en meningsfull granskning. Offentliga eller kommersiella medier nära regeringen kan fungera som kanal för smutskastningskampanjer med hjälp av det material som erhålls med spionprogram. ”Nationell säkerhet” åberopas ofta som en förevändning för att undanröja öppenhet och ansvarsskyldighet. Alla dessa delar tillsammans skapar ett system som är konstruerat för kontroll och förtryck. Enskilda offer lämnas inte bara fullständigt exponerade och försvarslösa mot en allsmäktig regering, det innebär också att alla nödvändiga kontroller och balanser i ett demokratiskt samhälle har slutat fungera.

Vissa regeringar har redan nått denna punkt, medan andra är halvvägs. Lyckligtvis kommer de flesta europeiska regeringar inte att gå den vägen. När de emellertid gör det är EU i sin nuvarande institutionella och politiska struktur inte utrustad för att förebygga eller motverka det. Spionprogram är som kanariefågeln i kolgruvan: Det avslöjar de farliga konstitutionella svagheterna i EU.

Sekretess

Ett stort hinder för att upptäcka och utreda olaglig användning av spionprogram är sekretess.

För de flesta offer är det inte möjligt att få information om deras fall från myndigheterna. I många fall hänvisar myndigheterna till nationella säkerhetsskäl som skäl för sekretess, i andra fall förnekar de helt enkelt förekomsten av uppgifter, eller så förstörs uppgifterna. Samtidigt vägrar åklagare ofta att utreda dessa fall och hävdar att offren inte har tillräckliga bevis. Detta är en ond cirkel där offren lämnas utan någon hjälp.

Regeringarna vägrar oftast att avslöja om de har köpt spionprogram och vilken typ av program. Spionprogramsförsäljare vägrar likaså att avslöja vilka deras kunder är. Regeringar använder ofta mellanhänder, fullmakter eller personliga kontakter för att köpa kommersiella spionprogram eller spionprogramsrelaterade tjänster, för att dölja sin inblandning. De kringgår upphandlingsregler och budgetförfaranden, så att de inte lämnar några statliga fingeravtryck.

Israel är ett viktigt nav för spionprogramföretag och ansvarar för att utfärda marknadsförings- och exportlicenser. Även om Israel och Europa är nära allierade ger Israel inte ut någon information om utfärdandet (eller upphävandet) av licenser för spionprogram till EU-länderna, trots att det används för att kränka EU-medborgarnas rättigheter och undergräva vår demokrati.

Journalisters begäran om informationsfrihet ger lite eller ingen information. Särskilda gransknings- och tillsynsorgan, såsom dataskyddsmyndigheterna eller revisionsrätten, har också svårt att få information. Oberoende tillsyn över underrättelsetjänster är i allmänhet svag och ofta obefintlig. De parlamentariska undersökningskommittéerna blockeras ofta av regeringspartierna. Rättsliga undersökningar fokuserar på tredjeländers hackningar, inte på EU-regeringarnas olagliga användning. Journalister som rapporterar om frågan står inför strategiska stämningsansökningar mot allmänhetens deltagande, verbala angrepp från politiker eller smutskastningskampanjer. De modiga och flitiga journalister som avslöjar

skandalens fakta förtjänar vår respekt och tacksamhet. De är Europas Woodwards och Bernsteins. Dessutom finns det fortfarande inte tillräckligt med skydd för visselblåsare i alla medlemsstater. I vissa fall vill offren för ett spionprogramsangrepp själva tiga, eftersom de inte vill avslöja parterna bakom angreppen, av rädsla för vedergällningsåtgärder eller för konsekvenserna av komprometterande material som avslöjats.

Vad händer nu?

I en tid då europeiska värden attackeras av externa angripare är det desto viktigare att stärka vår demokratiska rättsstat mot angrepp inifrån. Resultaten av PEGA-undersökningen är oroväckande och bör ses som alarmerande för alla EU-medborgare. Det är uppenbart att handeln med och användningen av spionprogram bör omfattas av strikt reglering. PEGA-utskottet kommer att utfärda en rad rekommendationer om detta. Det bör dock också finnas initiativ för institutionella och politiska reformer som gör det möjligt för EU att faktiskt tillämpa och upprätthålla dessa regler och standarder, även när de kränks av medlemsstaterna själva. EU måste snabbt utveckla sina försvarslinjer mot angrepp på demokratin inifrån.

INFORMATION OM ANTAGANDET I DET ANSVARIGA UTSKOTTET

Antagande	8.5.2023
Slutomröstning: resultat	+: 30 –: 3 0: 4
Slutomröstning: närvarande ledamöter	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
Slutomröstning: närvarande suppleanter	Andrzej Halicki, Gabriel Mato, Thijs Reuten, Jordi Solé, Yana Toom
Slutomröstning: närvarande suppleanter (art. 209.7)	Aurélia Beigneux, Theresa Bielowski, Franc Bogovič, Catherine Griset, Andreas Schieder

SLUTOMRÖSTNING MED NAMNUPPROP I DET ANSVARIGA UTSKOTTET

30	+
PPE	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

Teckenförklaring:
+ : Ja-röster
- : Nej-röster
0 : Nedlagda röster