STUDIJA

koju je naručio Odbor PEGA

Europski parlament

Utjecaj Pegasusa na temeljna prava i demokratske procese

Resorni odjel za prava građana i ustavna pitanja
Glavna uprava za unutarnju politiku
PE 740.514 – siječanj 2023.

HR

Utjecaj Pegasusa na temeljna prava i demokratske procese

Kratki pregled

U ovoj studiji, koju je naručio Resorni odjel Europskog parlamenta za prava građana i ustavna pitanja na zahtjev Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (PEGA), analizira se utjecaj uporabe Pegasusa i sličnog špijunskog softvera za nadzor na vrijednosti utvrđene u članku 2. Ugovora o Europskoj uniji, privatnost i zaštitu podataka i demokratske procese u državama članicama.

Dokument je naručio Istražni odbor Europskog parlamenta za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (PEGA).

AUTORI
Prof. dr. Giovanni SARTOR, Sveučilište u Bologni i Europski sveučilišni institut
Prof. dr. Andrea LOREGGIA, Sveučilište u Bresciji

ODGOVORNI SLUŽBENIK:
Mariusz MACIEJEWSKI

POMOĆNIK UREDNIKA
Ivona KLECAN

JEZIČNE VERZIJE
Izvornik: EN

O UREDNIKU
Resorni odjeli osiguravaju interna i vanjska stručna znanja kako bi pružili potporu odborima EP-a i ostalim parlamentarnim tijelima u oblikovanju zakonodavstva i provedbi demokratskog nadzora nad unutarnjim politikama EU-a.

Ako želite stupiti u kontakt s resornim odjelom ili se pretplatiti na njegove novosti, pišite na adresu:
Resorni odjel za prava građana i ustavna pitanja
Europski parlament
B-1047 Bruxelles
E-pošta: mailto:poldep-citizens@europarl.europa.eu

Rukopis dovršen u prosincu 2022

Ovaj dokument dostupan je na mrežnoj stranici:
http://www.europarl.europa.eu/supporting-analyses

IZJAVA O ODRICANJU ODGOVORNOSTI I ZAŠTITA AUTORSKIH PRAVA

SADRŽAJ

POPIS KRATICA

AGRI	Odbor za poljoprivredu i ruralni razvoj
ALDE	Klub zastupnika Saveza liberala i demokrata za Europu
BAS	Sustavi za pomoć pri kočenju
ZPP	Zajednička poljoprivredna politika
ZRP	Zajednička ribarstvena politika
ZOT	Zajednička organizacija tržišta
OR	Odbor regija
CULT	Odbor za kulturu i obrazovanje
ECOSOC	Gospodarsko i socijalno vijeće
ECR	Europski konzervativci i reformisti
ECTS	Europski sustav prijenosa bodova
EFDD	Klub zastupnika Europe slobode i demokracije
ENS	Klub zastupnika Europe naroda i slobode
EPP	Klub zastupnika Europske pučke stranke (kršćanski demokrati)
FAO	Organizacija za prehranu i poljoprivredu Ujedinjenih naroda
FPS	Prednji zaštitni sustavi
BDP	Bruto domaći proizvod
GM	Genetski modificirano
Zeleni/ESS	Klub zastupnika Zelenih/Europskog slobodnog saveza
GUE/NGL	Konfederalni klub zastupnika Ujedinjene europske ljevice i Nordijske zelene ljevice
IFI	Međunarodni fond za Irsku
S&D	Klub zastupnika Progresivnog saveza socijalista i demokrata u Europskom parlamentu

POPIS SLIKA

SAŽETAK

Kontekst

Ciljani nadzor temeljen na tehnološkim alatima izaziva opravdanu zabrinutost zbog svoje dubine, budući da može obuhvatiti sve aspekte života pojedinaca na koje je usmjeren. Sustavi špijunskog softvera koji se upotrebljavaju za hakiranje mobilnih uređaja, poput Pegasusa koji je razvila izraelska Grupa NSO, omogućuju sveobuhvatan tajni nadzor. Pegasus ima potpun i neograničen pristup hakiranom uređaju: može izvući s njega sve podatke (početno izvlačenje podataka), pratiti sve aktivnosti koje se provode na njemu (pasivno praćenje) i aktivirati funkcionalnosti uređaja u svrhu prikupljanja dodatnih podataka (aktivno praćenje), a možda može i zadirati u sadržaj uređaja i poruke koje se šalju s njega (manipulacija). Osobe na koje je usmjeren ne moraju izvršiti nikakvu radnju kako bi se softver instalirao na njihov uređaj i softver ne ostavlja nikakav trag o svojem radu (ili ostavlja vrlo malo tragova).

Cilj

Cilj ovog izvješća je (a) utvrditi ključna pitanja u vezi s načinima na koje Pegasus i drugi špijunski softver mogu ometati prava pojedinaca te demokratske procese i institucije, (b) procijeniti relevantni pravni okvir, (c) utvrditi u kojoj se mjeri i pod kojim uvjetima špijunski softver može zakonito upotrebljavati te (d) preporučiti načine za provedbu tih uvjeta.

Utjecaj na prava i demokraciju

Sveobuhvatni nadzor utječe na privatnost osoba, zaštitu podataka i druga prava pojedinaca, poput prava na slobodu govora, udruživanja i okupljanja, kao i na demokratske institucije u društvu. Špijunski softver utječe na političko sudjelovanje utoliko što se građani podvrgnuti špijuniranju mogu osjećati primoranima da se suzdrže od sudjelovanja u interakcijama političkog sadržaja, od iskrenog izražavanja njihovih stajališta i od udruživanja s drugima u političke svrhe. Zbog toga je narušena kvaliteta demokratske javne sfere, koja u konačnici ovisi o doprinosima i reakcijama građana. Konkretnije, špijunski softver utječe na pojedince (poput novinara, političara i aktivista) koji imaju posebnu ulogu u javnoj sferi. Podvrgavanjem takvih pojedinaca nadzoru otvara se prostor za represiju, manipulaciju, ucjenjivanje, krivotvorenje i klevetu. To može utjecati i na sam izborni proces na način da se prikupljeni podaci, kojima se možda manipuliralo, iskoriste za provođenje kampanja sramoćenja usmjerenih na određene kandidate ili za druga djelovanja koja će utjecati na njihove izglede za uspjeh na izborima. Sam strah da bi ih netko mogao špijunirati može navesti ljude da se ne kandidiraju za neku funkciju ili ih može spriječiti u vođenju djelotvorne kampanje.

Špijunski softver i nacionalna sigurnost

Uporaba špijunskog softvera obično se opravdava pozivanjem na nacionalnu sigurnost ili svrhe kaznenog progona. Međutim, čini se da se špijunski softver u mnogim slučajevima upotrebljava za neke druge svrhe koje se često odnose na stranačke političke ciljeve ili suzbijanje socijalnog ili političkog protivljenja. Prepoznato je da je nacionalna sigurnost poslužila mnogim državama kao ciničan pravni izgovor za ograničavanje slobode izražavanja, davanje legitimiteta mučenju i drugim oblicima zlostavljanja te zastrašivanje manjina, aktivista i političke opozicije. Postoje opsežni dokazi o uporabi Pegasusa protiv pojedinaca koji nisu bili ni na koji način povezani s teškim kaznenim djelima ni prijetnjama nacionalnoj sigurnosti, kao što su politički protivnici, aktivisti za ljudska prava, odvjetnici i novinari. Kako bi se spriječila široka uporaba pojma *nacionalne* sigurnosti, taj bi pojam trebalo tumačiti

ograničeno i razlikovati ga od koncepta *unutarnje* sigurnosti, pri čemu je potonja širi pojam i uključuje sprečavanje rizika kojima su izloženi pojedinačni građani, posebno provedbu kaznenog prava.

Međunarodno pravo u području ljudskih prava

U okviru UN-a aktivnosti nadzora procjenjuju se na temelju sporazuma o ljudskim pravima kao što je Međunarodni pakt o građanskim i političkim pravima. Zlouporabom nadzora utječe se na pravo na privatnost, ali i na slobodu izražavanja i druga prava utvrđena u tom paktu. Privatnost i slobodu izražavanja moguće je ograničiti isključivo putem zakona i u mjeri u kojoj je to potrebno za zakonite svrhe. Ograničenje se može opravdati nacionalnom sigurnošću, no zahtjevi zakonitosti i nužnosti vjerojatno nisu ispunjeni u slučaju Pegasusa.

Prema Europskoj konvenciji o ljudskim pravima, u kontekstu demokratskog društva na sve slučajeve ciljanog nadzora primjenjuju se zahtjevi legitimnosti, zakonitosti, nužnosti i proporcionalnosti. Širokom sudskom praksom Europskog suda za ljudska prava (ESLJP) utvrđeni su uvjeti za sukladnost tajnog nadzora s ljudskim pravima, posebno s obzirom na zakonitost (pristupačnost zakona kojima se odobrava nadzor i predvidljivost njihovih posljedica) te obavješćivanje. Sud je osim toga priznao aktivnu procesnu legitimaciju pojedincima koji su samo potencijalno bili mete tajnog nadzora.

Pravo EU-a

U kontekstu prava EU-a, ciljani nadzor relevantan je za prava sadržana u Povelji Europske unije o temeljnim pravima, načela sadržana u Ugovorima (poput demokracije i vladavine prava) i razne instrumente sekundarnog prava EU-a, na primjer, one koji se odnose na zaštitu podataka.

Prema Ugovoru o Europskoj uniji (UEU), nacionalna sigurnost isključiva je odgovornost svake države članice, no time se u načelu ne isključuje da aktivnosti nacionalne sigurnosti podliježu pravu EU-a, što je slučaj kad one utječu na aktivnosti regulirane pravom EU-a.

Primjena prava EU-a na uporabu špijunskog softvera u svrhe nacionalne sigurnosti, međutim, otežana je zbog toga što je nacionalna sigurnost isključena iz područja primjene dvaju temeljnih instrumenata: Opće uredbe o zaštiti podataka i Direktive o e-privatnosti. To se ne može opravdati s obzirom na prava zajamčena Poveljom i načela sadržana u Ugovorima. Budući da se to izuzeće može preširoko upotrebljavati, moramo istaknuti da se ono odnosi isključivo na slučajeve kad se špijunski softver zaista upotrebljava za zaštitu nacionalne sigurnosti, pri čemu se taj pojam ispravno tumači. Pravo EU-a u potpunosti se primjenjuje na tajne istrage koje se provode u svrhe kaznenog progona. Međutim, dokazi o zlouporabama postoje čak i u tom području.

Preporuke

Uporaba špijunskog softvera prijetnja je temeljnim pravima i osnovnim načelima prava EU-a poput (predstavničko-deliberativne) demokracije i vladavine prava. Zbog toga postoji rizik od potkopavanja samih načela na kojima se temelji pravni sustav EU-a.

U međunarodnom i europskom pravnom sustavu, ograničenja temeljnih prava mogu se opravdati aktivnostima u području nacionalne sigurnosti, ali ta ograničenja moraju zadovoljavati uvjete *legitimnosti, zakonitosti, nužnosti, uravnoteženja* i *usklađenosti s demokracijom* kako bi bila zakonita.

Pegasus dosad nije zadovoljio te zahtjeve u mnogim dosadašnjim slučajevima njegove primjene, s obzirom na to da se upotrebljavao za nelegitimne svrhe, bez odgovarajućeg pravnog okvira i bez istinske nužnosti, uzrokujući nerazmjernu štetu pravima pojedinaca te narušavanje demokracije.

Predlažemo različite strategije koje bi mogle pomoći u sprečavanju zlouporaba:

- Ograničavanje materijalnog područja primjene aktivnosti povezanih s nacionalnom sigurnošću kako bi državama bilo teže pozivati se na nacionalnu sigurnost kao lažno pravno obrazloženje za aktivnosti usmjerene u druge svrhe.
- Ograničavanje osobnog područja primjene aktivnosti povezanih s nacionalnom sigurnošću na način da se iz njega isključe određene aktivnosti koje provode privatni subjekti.
- Uključivanje aktivnosti povezanih s nacionalnom sigurnošću u područje primjene prava o zaštiti podataka kako bi ograničenja prava ispitanika u svrhe nacionalne sigurnosti bila podložna zahtjevima zakonitosti i proporcionalnosti.
- Pružanje potpore donošenju odgovarajućih pravnih okvira na nacionalnoj razini, budući da je nacionalna sigurnost i dalje rezervirana nadležnost država članica i one moraju na djelotvoran način uskladiti svoje aktivnosti s temeljnim pravima i načelima prava EU-a. Ti bi okviri trebali biti usklađeni s načelima kao što su: zakonitost, legitimna svrha, nužnost, proporcionalnost, nadležno tijelo, pravičan sudski postupak, obavještavanje korisnika, transparentnost, javni nadzor, sigurnost i certificiranje te tehnička prilagodljivost.

Politički izvediv moratorij na uporabu alata za hakiranje uređaja mogao bi se sastojati od snažne pretpostavke protiv zakonitosti njihove uporabe, temeljene na opsežnim dokazima o njihovoj zlouporabi. Ta bi se pretpostavka mogla nadići isključivo kad neka država uvjerljivo pokaže spremnost i kapacitet za sprečavanje svih zlouporaba.

Nadalje, trebalo bi potaknuti sve države članice da zabrane uporabu konkretnih alata špijunskog softvera za koje, kao što je to slučaj s Pegasusom, postoje čvrsti dokazi o njihovoj širokoj uporabi u nezakonitim aktivnostima, posebno na području EU-a. Sve dok ne postoje jasni dokazi da se takve neprihvatljive prakse više ne provode, nastavak uporabe Pegasusa, čak i u okviru zakonitih aktivnosti, ekvivalentan je pružanju potpore njegovim proizvođačima i razvojnim inženjerima te kao takav implicira političko (iako ne i pravno) sudioništvo u takvim praksama.

1. OPĆE INFORMACIJE

U ovoj studiji ispitat ćemo u kojoj se mjeri pravo o ljudskim pravima i pravo EU-a mogu primijeniti na uporabu špijunskog softvera u navodne svrhe nacionalne sigurnosti. Nakon predstavljanja raznih vrsta zlonamjernih napada na digitalne uređaje (2. poglavlje) bit će govora o sustavima koji funkcioniraju tako da hakiraju mobilne uređaje, poput Pegasusa (3. poglavlje). Razmotrit ćemo utjecaje Pegasusa na demokraciju (4. poglavlje) i pozivanje na nacionalnu sigurnost kao opravdanje za tajni nadzor (5. poglavlje). Razmotrit ćemo primjenjivi pravni okvir: instrumente kojima se štite ljudska prava poput Međunarodnog pakta o građanskim i političkim pravima i Europske konvencije o ljudskim pravima (6. poglavlje) i pravo EU-a, uključujući Ugovore EU-a, Povelju EU-a o temeljnim pravima i instrumente za zaštitu podataka (7. poglavlje). Konačno, iznijet ćemo određena razmatranja u vezi s pitanjem može li se špijunski softver zakonito primjenjivati i pod kojim uvjetima (8. poglavlje).

2. ZLONAMJERNI SOFTVER, NEDOSTACI I PRIJETNJE

KLJUČNI ZAKLJUČCI

Tehnološki uređaji sučelja su kojima se povezujemo s digitalnim svijetom. Radi se o rastućoj mreži uređaja povezanih s internetom koji imaju mogućnost međusobnog komuniciranja i komuniciranja s ljudima. Tim se uređajima koristimo za pohranjivanje podataka i komunikaciju; u njih su ugrađeni senzori ili druge tehnologije koje im omogućuju prikupljanje podataka iz fizičkog okruženja. Špijunski softver omogućuje neovlaštenim osobama da pristupe digitalnim uređajima i koriste se njima bez znanja ili privole legitimnih korisnika. Podaci koji se pritom prikupljaju, uključujući osjetljive podatke, mogu se upotrebljavati na načine koji ne odgovaraju očekivanjima ili preferencijama korisnika. Postoje razne vrste alata temeljenih na zlonamjernom softveru koji iskorištavaju nedostatke za provođenje neovlaštenih aktivnosti.

Mnogo je potencijalnih razloga zbog kojih bi treće strane mogle biti zainteresirane za stjecanje neovlaštenog pristupa nekom uređaju ili skupini uređaja. Neki od mogućih ciljeva su:

- Prikupljanje podataka o meti (korisniku uređaja). To može uključivati osobne podatke poput imena, adrese i telefonskog broja te informacije o aktivnostima i navikama mete na internetu.
- Prikupljanje podataka o poznanicima mete. To može uključivati podatke o osobama s kojima meta komunicira i informacije o njihovim aktivnostima i navikama na internetu.
- Stjecanje pristupa uređaju kako bi se zatražila otkupnina. U tom slučaju treća strana može pokušati preuzeti kontrolu nad uređajem i onemogućiti pristup njegovu sadržaju (šifrirajući ga) te zatim od vlasnika zahtijevati isplatu kako bi mu vratila kontrolu nad uređajem i omogućila mu pristup podacima.
- Krađa identiteta. Ako neka treća strana stekne pristup uređaju, može se predstavljati kao njegov vlasnik i slati poruke ili vršiti druge aktivnosti koje prividno potječu od legitimnog vlasnika. To može biti posebno opasno ako treća strana putem uređaja uspije steći pristup osjetljivim osobnim ili financijskim podacima.
- Onemogućivanje mete da se koristi uređajem. To se može izvršiti brisanjem važnih datoteka ili onemogućivanjem ključnih funkcija uređaja.

Za izvođenje kibernapada mogu se upotrebljavati različite tehnologije[1]. Pojedinci i organizacije koje razumiju tehnologije kojima bi se napadači mogli služiti mogu poduzeti mjere kako bi se zaštitile i kako bi zaštitile svoje sustave. Sljedeći su pristupi najznačajniji:

- Zlonamjerni softver[2]. Pojam potječe od engleske riječi *malware* (*malicious software*). Zlonamjerni softver namijenjen je izvođenju napada na samostalno računalo ili povezano osobno računalo u svrhe kao što je krađa informacija ili identiteta, špijunaža i prekid usluga.
- Lažno predstavljanje (*phishing*)[3]. Radi se o prijevari koja se vrši putem interneta, a cilj joj je na prijevaru navesti korisnike da otkriju osjetljive informacije poput lozinki, brojeva računa ili

[1] Saeed, I.A., Selamat, A. i Abuagoub, A.M. „A survey on malware and malware detection systems" (Pregled zlonamjernog softvera i sustava za njegovo otkrivanje).

[2] Saeed, I.A., Selamat, A. i Abuagoub, A.M. „A survey on malware and malware detection systems" (Pregled zlonamjernog softvera i sustava za njegovo otkrivanje). *International Journal of Computer Applications* (2013.), 67.(16.).

[3] Kathrine, G.J.W., Praise, P.M., Rose, A.A. i Kalaivani, E.C. „Variants of phishing attacks and their detection techniques" (Varijante *phishing* napada i tehnika za njihovo otkrivanje). U *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019., str. 255-259.

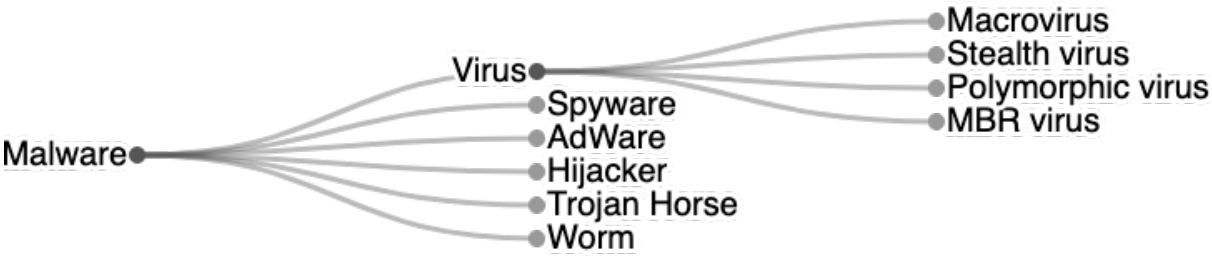
osobnih podataka. Te se informacije zatim mogu upotrijebiti u zlonamjerne svrhe kao što je krađa novca s korisnikova bankovnog računa ili se mogu upotrijebiti za nezakonito pristupanje korisnikovim računima ili uređajima. Pri takvim napadima često se upotrebljavaju lažne mrežne stranice ili poruke e-pošte koje su osmišljene da korisnike na prijevaru navedu na otkrivanje osjetljivih informacija.

- Otimanje klikova (*clickjacking*)[4]. Takvim napadom na prijevaru se navodi korisnike interneta da kliknu lažnu hipervezu ili gumb koji su dizajnirani kako bi ih zavarali. Kad korisnici kliknu poveznicu, mogu biti preusmjereni na neku drugu mrežnu stranicu, na njihov se uređaj može preuzeti prijevarna aplikacija ili mogu biti izloženi povjerljivi podaci. Ti se napadi mogu upotrebljavati za krađu osobnih podataka, instalaciju zlonamjernog softvera na korisnikov uređaj ili vršenje drugih štetnih radnji.
- Društveni inženjering[5]. Pri toj vrsti napada manipulira se žrtvama kako bi se ostvario pristup osjetljivim informacijama ili sustavima. Počinitelji društvenog inženjeringa služe se raznim taktikama kao što su poruke e-pošte koje sadrže *phishing*, telefonski pozivi ili osobne interakcije. Napadač se može predstavljati kao netko kome žrtva vjeruje, na primjer kolega, predstavnik službe za korisnike ili član neke financijske institucije, kako bi stekao žrtvino povjerenje i naveo žrtvu da otkrije osjetljive informacije ili poduzme neke druge radnje kojima će ugroziti svoju sigurnost.

2.1. Zlonamjerni softver

Kao što već spomenuli, ova vrsta napada uključuje uporabu zlonamjernog softvera.

Slika 1.: Taksonomija zlonamjernog softvera



Postoje različite vrste zlonamjernog softvera (**Slika 1**.).

- Virusi se mogu replicirati i proširiti na druga računala. Često se prenose zaraženim datotekama ili porukama e-pošte i mogu uzrokovati razne probleme, među ostalim usporiti rad računala, izbrisati važne datoteke ili omogućiti krađu osobnih podataka. Virusi se mogu pojavljivati u različitim oblicima i razvijati u različitim programskim jezicima. Neki od primjera su:
    - Makronaredbeni virusi. Izrađeni su s pomoću makro programskih jezika kao što je Visual Basic for Applications (VBA). Makronaredbe služe za automatizaciju i pojednostavnjenje zadaća u softveru poput Microsoft Officea i mogu se pohraniti u dokumentu ili proračunskoj tablici. Makronaredbeni virusi šire se kad se zaraženi

[4] Sahani, R. i Randhawa, S. „Clickjacking: Beware of Clicking" (*Clickjacking*: klikajte oprezno). *Wireless Personal Communications* (2021.), 121.(4.), str. 2845-2855.

[5] Salahdine, F. i Kaabouch, N., „Social engineering attacks: A survey" (Napadi društvenim inženjeringom: pregled). *Future Internet* (2019.), 11.(4.), str. 89.

dokumenti ili datoteke pošalju drugima. Kad korisnik otvori zaraženu datoteku i omogući makronaredbe, virus se izvršava i uzrokuje štetu uređaju korisnika ili njegovim podacima ili krađu osjetljivih informacija.
    - Nevidljivi (*stealth*) virusi. Imaju mogućnost sakriti se od operativnog sustava ili antivirusnog softvera na način da izvršavaju promjene u veličinama datoteka ili strukturi direktorija. Nevidljivi su virusi antiheuristički, što znači da su dizajnirani tako da ih je teško otkriti.
    - Polimorfni virusi. Dizajnirani su tako da promijene svoj izgled i kod svaki put kad zaraze neki drugi sustav. To im može pomoći da izbjegnu da ih otkrije antivirusni softver.
    - Virusi koji napadaju početni sektor. Ovi virusi zaraze prvi sektor tvrdog diska na napadnutom računalu u kojem je pohranjen glavni zapis za učitavanje (*Master Boot Record*; MBR). Glavni zapis za učitavanje sadržava primarnu particijsku tablicu diska i upute za samopokretanje koje se izvršavaju čim se računalo pokrene[6]. Kad se uključi računalo zaraženo virusom koji napada početni sektor, virus se odmah pokreće i učitava u memoriju, što mu omogućuje kontrolu nad sustavom.

- Špijunski softver namijenjen je prikupljanju informacija o korisnicima bez njihova znanja ili pristanka. Može se upotrebljavati za praćenje aktivnosti korisnika na internetu, krađu osobnih podataka ili prikazivanje neželjenih oglasa. Špijunski softver može se širiti putem zaraženih datoteka ili poruka e-pošte ili se može instalirati bez znanja korisnika zajedno s drugim softverom. Može i preuzimati druge zlonamjerne programe s interneta i instalirati ih na uređaj.
- Programi s neželjenim oglasima (*adware*) prikazuju neželjene oglase. Mogu se automatski instalirati na uređaj bez znanja njegova korisnika kad korisnik aktivira neki program ili pristupi mrežnoj stranici na kojoj se nalazi program s neželjenim oglasima. Taj program obično prikazuje oglase u skočnim prozorima ili na trakama na zaslonu te može prikupljati i slati informacije o korisniku.
- Trojanski konj prerušen je u legitimne programe ili datoteke. Za razliku od virusa, ne može se replicirati i proširiti na druga računala. Trojanski konji često otvaraju „stražnja vrata" putem kojih napadači ili zlonamjerni programi mogu pristupiti uređaju i njegovu sustavu. Na taj se način mogu upotrijebiti za krađu povjerljivih i osobnih podataka ili za izvođenje drugih neovlaštenih radnji.
- Crvi (*worm*) su dizajnirani tako da se repliciraju i prošire u računalnoj mreži, često bez korisnikova znanja. Za razliku od virusa, ne vezuju se za postojeće programe i obično ne uzrokuju štetu na podacima ili programima. Međutim, troše resurse i šire se na druge uređaje. Usporavaju mrežne performanse ili troše kapacitet prijenosa podataka.

2.2. Nedostaci

Nedostaci su slabosti ili manjkavosti u sustavu ili uređaju koje napadači mogu iskoristiti za neovlašteni pristup ili izvršenje drugih zlonamjernih radnji. Ti nedostaci mogu biti prisutni u operativnom sustavu, softverskim aplikacijama ili samom hardveru i mogu napadačima omogućiti ometanje normalnog rada nekog uređaja ili informatičke infrastrukture.

Nedostatke mogu otkriti istraživači u području sigurnosti ili napadači. Mogu se iskorištavati primjenom raznih metoda poput zlonamjernog softvera, *phishing* napada ili posebnih „iskorištavatelja slabih

[6] Odmah nakon izvršenja BIOS-a (*Basic Input/Output System*), ugrađene programske opreme koja pokreće hardver računala.

točaka" (*exploits*) (softverski programi, blokovi podataka ili sljedovi naredbi čija je svrha iskoristiti nedostatak). Napadači mogu iskoristiti nedostatke kako bi pristupili osjetljivim podacima, omeli normalan rad uređaja ili sustava ili izvršili druge štetne radnje.

Dosad nepoznati nedostatak (*zero day vulnerability*)[7] je sigurnosni nedostatak za koji još ne postoji zakrpa jer nije bio poznat razvojnim inženjerima koji su razvili softver ili istraživačima u području sigurnosti koji bi obično radili na njegovu otklanjanju. Korisnici nemaju načina da se zaštite jer nisu svjesni nedostatka.

Dosad nepoznati iskorištavatelji slabih točaka (*zero-day exploits*) su digitalni napadi usmjereni na dosad nepoznate nedostatke. Kiberkriminalci se žure iskoristiti te nedostatke kako bi zaradili na svojim programima.

Međunarodne inicijative održavaju javno dostupne skupove podataka o poznatim nedostacima; kibersigurnosna zajednica prihvatila je Popis čestih nedostataka i izloženosti (*Common Vulnerabilities and Exposures List* – CVE)[8] koji održava katalog javno poznatih kibersigurnosnih nedostataka. Zapisi iz tog kataloga služe za jedinstveno identificiranje nedostataka i njihovo objavljivanje na popisima za praćenje kao što je *Top 10 Web Application Security Issues* (Najvažnijih deset sigurnosnih problema mrežnih aplikacija) koji održava organizacija Open Web Application Security Project (OWASP)[9].

Na temelju ove analize nedostataka i iskorištavatelja slabih točaka možemo razlikovati dvije vrste napada:

- Napadi bez klika (*zero-click attacks*)[10] ne zahtijevaju nikakvu intervenciju korisnika. Često se temelje na dosad nepoznatom nedostatku i osobito su opasni jer korisnici obično nisu svjesni takvih napada i stoga se ne mogu boriti protiv njih niti ublažiti njihove učinke.
- Napadi jednim klikom zahtijevaju radnju korisnika na koje je napad usmjeren, koja se obično sastoji od klikanja poveznice ili gumba koji se prikazuje u mrežnoj aplikaciji. Iako žrtva mora izvršiti radnju, možda neće znati što se događa jer će je obmanuti zavaravajući izgled poruke ili sučelja kojim se napadač koristi.

Posljednjih godina svjedočimo povećanom broju napada koji su se proširili izvan okvira tradicionalnih kanala (poput poruka e-pošte) na pristupe koje je teže izbjeći (poput automatskih zlonamjernih (*drive-by*) preuzimanja koja se pokreću na zaraženim mrežnim stranicama), koji zlonamjernim akterima omogućuju da pristupe kompromitiranim uređajima, preuzmu kontrolu nad njima i probiju se u njih te da s njih prikupljaju velike količine podataka.

---

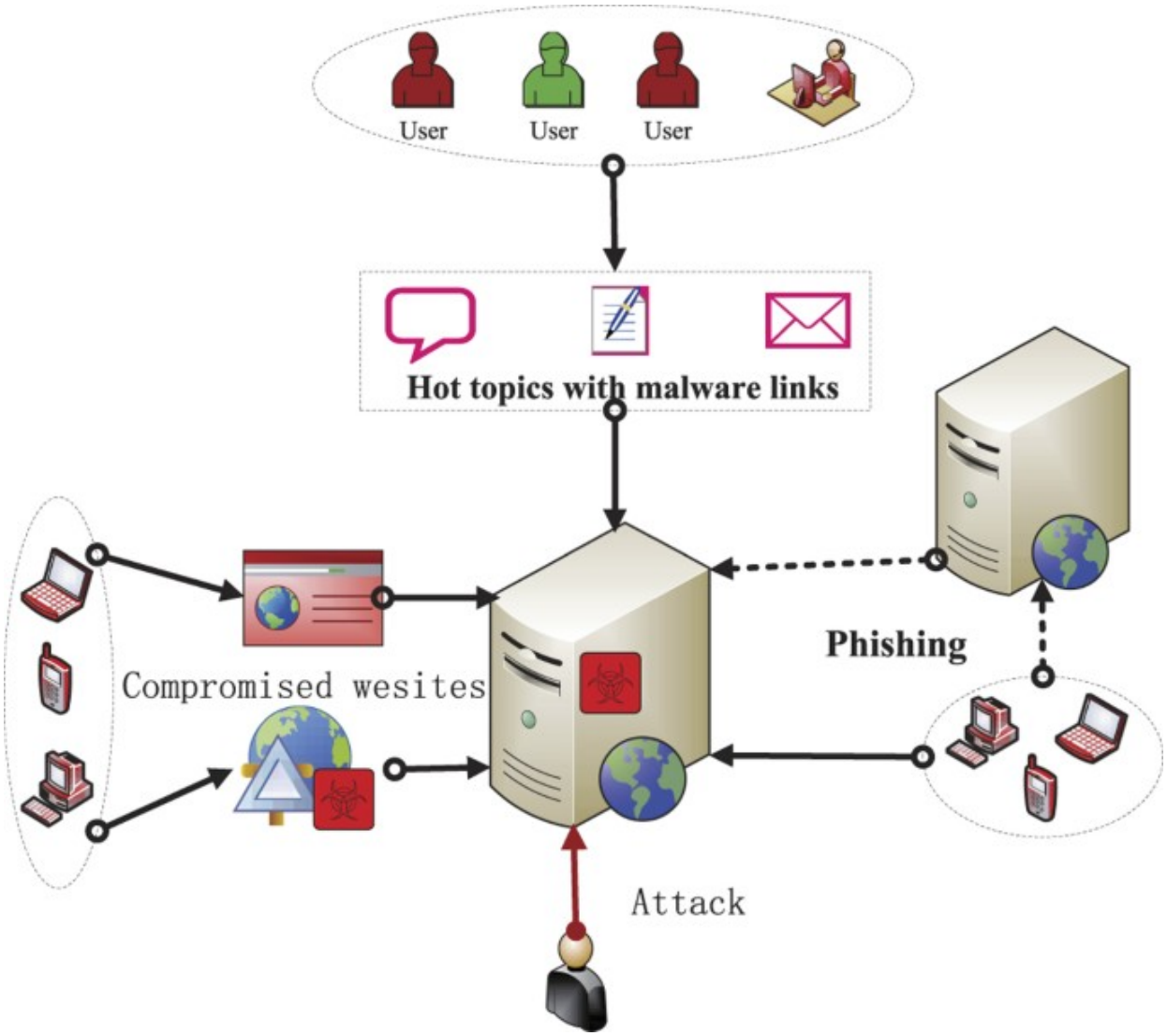
[7] Singh, U.K., Joshi, C. i Kanellopoulos, D. „A framework for zero-day vulnerabilities detection and prioritization" (Okvir za otkrivanje i određivanje prioriteta dosad nepoznatih nedostataka). *Journal of Information Security and Applications* (2019.), 46., str. 164-172.

[8] Popis čestih nedostataka i izloženosti, https://cve.mitre.org/cve/.

[9] Open Web Application Security Project, https://owasp.org/www-project-top-ten/.

[10] Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. i Ng, A. „Cybersecurity data science: an overview from machine learning perspective" (Kibersigurnosna podatkovna znanost: pregled iz perspektive strojnog učenja). *Journal of Big data* (2020.), 7.(1.), str. 1-29.

Slika 2.: Dijagram mehanizma širenja mrežnog zlonamjernog softvera[11]



2.3. Nove prijetnje

U izvješćima o kiberprijetnjama obično se naglasak stavlja na poslovnu domenu i zanemaruju se kiberprijetnje usmjerene na civilno društvo[12] iako se alati špijunskog softvera često upotrebljavaju protiv disidenata, boraca za ljudska prava, novinara i zagovaratelja civilnog društva (vidjeti Poglavlje 3.2. Izazov koji proizlazi iz špijunskog softvera). Nadzor nad civilnim društvom i napadi na njega tek su

[11] Liu, W. i Zhong, S. „Web malware spread modelling and optimal control strategies" (Modeliranje širenja mrežnog zlonamjernog softvera i optimalne strategije za kontrolu). *Scientific reports* (2017.), 7.(1.), str. 1-19.

[12] ENISA. „Threat Landscape 2022" (Okružje prijetnji 2022.). https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

nedavno privukli pažnju medija i potaknuli zakonodavni/regulatorni nadzor zbog incidenata koji su uključivali špijunski softver poput Pegasusa (vidjeti Poglavlje 3.), Predatora[13] i drugih.

Agencija Europske unije za kibersigurnost (ENISA) u studenome 2022. uključila je digitalni nadzor u deset najvažnijih novih kibersigurnosnih prijetnji do 2030. (vidjeti 3..)[14]. Slične su zabrinutosti izrazili i mnogi drugi izvori.

Slika 3.: Kibersigurnosne prijetnje

Skupine koje se nazivaju naprednim ustrajnim prijetnjama (*Advanced Persistent Threat* – APT), tj. dionici koji stječu neovlašteni pristup računalima i mrežama i uspijevaju dugo vremena ostati neotkriveni, ulažu u razvoj ili kupnju naprednih kapaciteta za napad i usto sve više usvajaju javno dostupne zlonamjerne alate, uključujući zlonamjerni softver otvorenog koda[15]. Široka dostupnost jeftinih osnovnih alata dovodi do proširenja pristupa kapacitetima za hakiranje i nadzor, budući da se prepreke

[13] Stevis-Gridneff, M. i Pronczuk, M. „Senior European Parliament Member Targeted as Spyware Abuse Spreads" (Viši zastupnik u Europskom parlamentu na meti dok se zlouporaba špijunskog softvera širi). *The New York Times* (27. srpnja 2022.). https://www.nytimes.com/2022/07/27/world/europe/eu-spyware-predator-pegasus.html.

[14] Priopćenje za medije agencije ENISA. *„Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride!" (Predviđanja o kibersigurnosnim prijetnjama za 2030.: pričvrstite sigurnosni pojas prije vožnje!)* 11. studenoga 2022. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030.

[15] Nimmo, B. „Meta's Adversarial Threat Report, Second Quarter 2022" (Metino izvješće o neprijateljskim prijetnjama za drugo tromjesečje 2022.) Meta Newsroom. 4. kolovoza 2022. https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/.

ulasku snižavaju. Istraživači u području sigurnosti zbog šireg pristupa toj tehnologiji ne mogu pravovremeno identificirati te skupine, koje zahvaljujući tome ostaju neotkrivene[16].

Vrijedi podsjetiti da je proizvođač Pegasusa, Grupa NSO, tek jedno poduzeće u mnogo široj globalnoj kiberplaćeničkoj industriji. Meta je 2021. podijelila informacije o sedam aktera koje je to poduzeće uklonilo sa svoje platforme zbog sumnji da provode nadzor[17]. Microsoft je 2021. utvrdio da Candiru iskorištava dosad nepoznati nedostatak. Složeni napadi konstruirani su za ubacivanje špijunskog softvera na žrtvin uređaj. Primjerice, tvrdi se da je mrežna stranica iranskog veleposlanstva u Abu Dabiju 2020. izmijenjena umetanjem malog softverskog programa čija je funkcija bila ubaciti špijunski softver pod nazivom Karkadann, sličan Candiruu[18].

IMalwarebytes je 2021. zabilježio detekciju 54 677 aplikacija s pomoću kojih su se nadzirali Android sustavi i 1 106 aplikacija koje su se upotrebljavale za špijuniranje tih sustava (što je 4,2 % odnosno 7,2 % više detekcija nego u 2020.). Čini se da je 2021. bila najgora dosad zabilježena godina u pogledu špijunskog softvera. Neki zlonamjerni softveri unaprijed se instaliraju u operativni sustav na mobilnim uređajima koje proizvode jeftiniji proizvođači i stoga ih je vrlo teško ukloniti[19].

Mnogim napadima zajedničke su tri faze: izviđanje, napad i iskorištavanje. Dok se neki subjekti specijaliziraju za neku određenu fazu nadzora, drugi podržavaju cijeli lanac napada.

1. Izviđanje. Hakeri profiliraju pojedince na koje usmjeravaju napade u ime svojih klijenata kako bi utvrdili načine na koje mogu uspješno napasti uređaje tih pojedinaca. Hakeri u toj fazi obično pokreću softver za automatizaciju prikupljanja i analize podataka. Izvlače podatke iz svih dostupnih mrežnih zapisa kao što su blogovi, društvene mreže, platforme za upravljanje znanjima itd.

2. Napad. S pojedincima na koje je usmjeren napad može se stupiti u kontakt kako bi se pridobilo njihovo povjerenje, kako bi se prikupili podaci i možda kako bi ih se prijevarom navelo da kliknu zlonamjerne poveznice ili datoteke. Napadači se u tu svrhu mogu poslužiti taktikama društvenog inženjeringa. Mogu preuzeti lažne osobnosti i kontaktirati s ljudima putem e-pošte, telefonskih poziva, tekstualnih poruka ili izravnih poruka na društvenim mrežama.

3. Iskorištavanje. Napadači plasiraju svoje zlonamjerne „korisne podatke" služeći se vlastitim posebno izrađenim iskorištavateljima slabih točaka ili zlonamjernim alatima kupljenim od drugih. Ovisno o iskorištavatelju slabih točaka, napadači mogu pristupiti bilo kojim podacima na telefonu ili računalu svoje mete, uključujući lozinke, kolačiće, tokene za pristup, fotografije, videozapise, poruke i kontakte, te mogu neprimjetno aktivirati mikrofon, kameru i praćenje geolokacije.

---

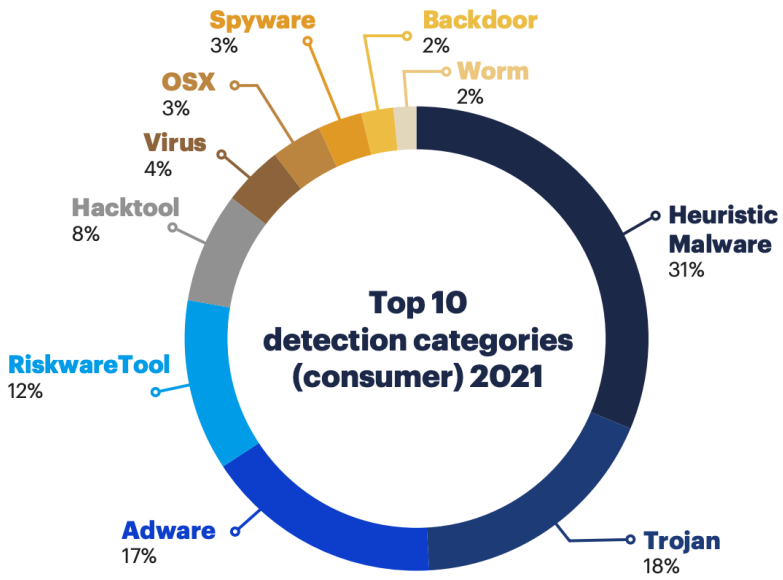
[16] Nimmo, B., Agranovich, D., Franklin, M., Dvilyanski, M. i Gleicher, N. „Quarterly Adversarial Threat Report" (Tromjesečno izvješće o neprijateljskim prijetnjama). *Meta*. Kolovoz 2022. https://about.fb.com/wp-content/uploads/2022/08/Quarterly-Adversarial-Threat-Report-Q2-2022.pdf.

[17] Agranovich, D. i Dvilyanski, M. „Taking Action Against the Surveillance-for-Hire Industry" (Djelovanje protiv industrije nadzora za najam). *Meta Newsroom*. 16. prosinca 2021. https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/.

[18] Faou, M. „Strategic Web Compromises in the Middle East with a Pinch of Candiru: ESET Researchers Have Discovered Strategic Web Compromise (aka Watering Hole) Attacks against High-Profile Websites in the Middle East" (Strateška kompromitiranja putem mreže na Bliskom istoku s pomoću Candirua: ESET-ovi istraživači otkrili su napade strateškog kompromitiranja putem mreže (*watering hole* napadi) protiv poznatih mrežnih stranica na Bliskom Istoku). *welivesecurity*. 16. studenoga 2021. https://www.welivesecurity.com/2021/11/16/strategic-web-compromises-middle-east-pinch-candiru/.

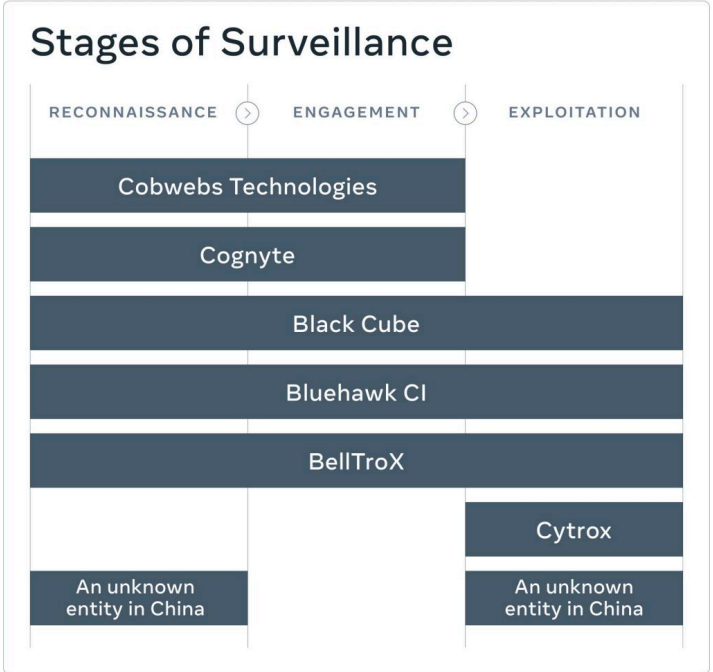
[19] Malwarebytes Cyberprotection. *„Threat Review: Cyberprotection Starts with Understanding the Latest Attacks, Cybercrimes, and Privacy Breaches"* (Pregled prijetnji: Kiberzaštita počinje razumijevanjem najnovijih napada, kibernetičkih kaznenih djela i povreda privatnosti). 2022. https://www.malwarebytes.com/resources/malwarebytes-threat-review-2022/index.html (dohvaćeno 26. prosinca 2022).

Slika 4.: Deset najvažnijih kategorija detekcije u 2021[20]



Utvrđeno je da sedam subjekata koji se nalaze u Kini, Izraelu, Indiji i Sjevernoj Makedoniji prati pojedince u više od 100 država iskorištavajući te tri faze u lancu nadzora (Slika 5.).

Slika 5.: Faze nadzora i sedam subjekata koje je identificirala Meta[21]



[20] Malwarebytes Cyberprotection. *„Threat Review: Cyberprotection Starts with Understanding the Latest Attacks, Cybercrimes, and Privacy Breaches"* (Pregled prijetnji: Kiberzaštita počinje razumijevanjem najnovijih napada, kibernetičkih kaznenih djela i povreda privatnosti).

[21] Nimmo, B. „Meta's Adversarial Threat Report" (Metino izvješće o neprijateljskim prijetnjama).

3. PEGASUS KAO SREDSTVO NADZORA

KLJUČNI ZAKLJUČCI

Ciljani nadzor primjenom tehnoloških alata izaziva opravdanu zabrinutost zbog svoje dubine, budući da može obuhvatiti sve aspekte života osoba na koje je usmjeren. Sustavi špijunskog softvera za hakiranje mobilnih uređaja, poput Pegasusa koji je razvila izraelska Grupa NSO, omogućuju sveobuhvatan tajni nadzor. Pegasus ima potpun i neograničen pristup uređaju na koji je usmjeren: može izvući s njega sve podatke (početno izvlačenje podataka), pratiti sve aktivnosti koje se provode na njemu (pasivno praćenje) i aktivirati funkcionalnosti uređaja u svrhu prikupljanja dodatnih podataka (aktivno praćenje), a možda može i zadirati u sadržaj uređaja i poruke koje se šalju s njega. Za njegovu instalaciju nije potrebno da pogođene osobe izvrše ikakvu radnju i ne ostavlja nikakva traga svojeg rada (ili ostavlja vrlo malo tragova). Postoje opsežni dokazi o uporabi Pegasusa u mnogim državama, uključujući države članice EU-a.

U ovom poglavlju najprije ćemo uvesti pojam nadzora. S jedne strane razlikujemo tradicionalni nadzor i novi nadzor temeljen na tehnologiji, a s druge ciljani i masovni nadzor. Zatim ćemo naglasak staviti na Pegasus kao ekstremni slučaj ciljanog nadzora temeljenog na tehnologiji.

3.1. Tradicionalni i novi nadzor

Vlade se oduvijek služe metodama tajne istrage kao načinom za suzbijanje rizika za nacionalnu sigurnost, ali i za provođenje aktivnosti čiji je cilj ostvarivanje političkih ili gospodarskih prednosti. Takve se metode često primjenjuju u svrhu „nadzora"[22] odnosno namjernog, sustavnog i kontinuiranog nadziranja pojedinaca i skupina uz „pridavanje pažnje osobnim pojedinostima u svrhe utjecaja, upravljanja, zaštite ili usmjeravanja"[23].

Tehnologija, posebno digitalne tehnologije, nadopunjuju upućivanje ljudskih agenata za prikupljanje informacije infiltracijom, osobnim kontaktom i pristupom povjerljivim dokumentima. Tradicionalni nadzor, temeljen na ljudskim osjetilima bez pomoći tehnologije, tako je ustupio mjesto veoma drugačijem modelu društvene kontrole pod nazivom „novi nadzor", koji je definiran kao „nadzor pojedinaca, skupina i okruženja digitalnim sredstvima u svrhu izvlačenja ili stvaranja informacija", čime su prevladana prostorna, vremenska, kvantitativna i druga ograničenja tradicionalnog nadzora[24].

Današnje informacijske tehnologije u nezapamćenoj mjeri omogućuju provedbu „nadzora nad komunikacijama", koji je visoki povjerenik Ujedinjenih naroda za ljudska prava ovako opisao:

---

[22] Engleska riječ koja označava nadzor, *surveillance*, potječe od francuskog *surveiller*, složenice koja se sastoji od *sur*, što znači „nad", i *veiller*, od latinskog *vigilare*, što znači „promatrati", a u engleskom se jeziku udomaćila za vrijeme Francuske revolucije (1789. – 1799.), kada su u svakoj francuskoj općini oformljeni odbori za nadzor čija je zadaća bila pratiti postupke i kretanje stranaca, disidenata i sumnjivih osoba. Vidjeti: Watt, E. *„State Sponsored Cyber Surveillance"* (Kibernadzor pod pokroviteljstvom države). Elgar, 2021. „On cybersurveillance and national security" (O kibernadzoru i nacionalnoj sigurnosti), vidjeti i Monti, A. i Wacks, R. *„National Security in the New World Order"* (Nacionalna sigurnost u novom svjetskom poretku). Routledge, 2022.

[23] Lyon, D. *„Surveillance Studies" (Studije o nadzoru)*. Polity Press, 2007.

[24] Marx, G. T. *„Windows into the Soul. Surveillance and Society in an Age of High Technology"* (Prozori duše. Nadzor i društvo u dobu visoke tehnologije). Chicago University Press, 2016.

> *praćenje, presretanje, prikupljanje, pribavljanje, analiza, uporaba, čuvanje, zadržavanje, manipulacija, pristup ili slične radnje koje se poduzimaju s obzirom na podatke koji uključuju ili odražavaju prošlu, sadašnju ili buduću komunikaciju neke osobe ili iz nje proizlaze ili se na nju odnose*[25].

Istina je da je masovni nadzor bio moguć i prije pojave sadašnjih tehnologija, što pokazuje slučaj Ministarstva državne sigurnosti Demokratske Republike Njemačke, poznatog pod nazivom Stasi, za čije se arhive procjenjuje da su sadržavali datoteke o šest milijuna osoba.

> *Procjenjuje se da je to ministarstvo zapošljavalo 274 000 osoba, od čega najmanje 174 000 doušnika, što bi činilo oko 2,5 % radno sposobnog stanovništva. Doušnici su špijunirali u svakom uredu i kulturnom i sportskom društvu te u svakoj stambenoj zgradi. Snimali su ljude u njihovim vlastitim domovima i domovima njihovih prijatelja*[26].

Modernim nadzorom koji se temelji na digitalnoj tehnologiji može se postići i nadmašiti ta razina sveobuhvatnosti uz mnogo manje potrebe za ljudstvom. S pomoću senzora i softvera za hakiranje mogu se prikupiti bilo kakvi podaci izravno od pojedinca kojeg se špijunira, uz ograničenu ljudsku intervenciju ili bez nje, a velike količine podataka o elektroničkim komunikacijama mogu se prikupiti izravno iz kabela putem kojih se te komunikacije prenose i poslužitelja na kojima se one pohranjuju.

U analizi nadzora ključno je razlikovati ciljani i masovni nadzor.

Ciljani nadzor usmjeren je na konkretne osobe od interesa. Može se sastojati od presretanja komunikacija koje su potekle od neke određene osobe ili s neke lokacije, ali može uključivati i daljinsko ometanje opreme (poznato i pod nazivom „hakiranje") koje se upotrebljava za izvlačenje podataka s uređaja povezanih s internetom kao što su stolna računala, prijenosna računala, tablet računala ili pametni telefoni. Budući da su digitalne komunikacije u sve većoj mjeri šifrirane, sigurnosne agencije i tijela kaznenog progona oslanjanju se na ometanje opreme kako bi pristupila sadržaju komunikacija prije nego što on postane nedostupan zbog šifriranja. Napredni špijunski softver poput Pegasusa predstavlja trenutačnu evoluciju tehnologija koje su u uporabi već desetljećima.

Za razliku od ciljanog nadzora, masovni nadzor neselektivno je usmjeren na velike skupine osoba (može uključivati čak i čitav narod). Počinje se provoditi bez ikakve sumnje u neku konkretnu osobu ili osobe i ima proaktivnu funkciju, pri čemu mu je cilj identificirati buduće prijetnje i označiti pojedince kao sumnjive. Masovni nadzor omogućen je digitalnim tehnologijama koje mogu u kratkom vremenu i uz ograničen trošak obraditi goleme količine podataka prikupljenih iz telekomunikacijskih linija ili postojećih repozitorija podataka (koje često vode vodeća digitalna poduzeća). Masovni nadzor predmet je velikih kontroverzi na svjetskoj razini, posebno nakon što su otkrića Edwarda Snowdena ukazala na raširenost te pojave i mjeru u kojoj se ona zloupotrebljava. Europski parlament izrazio je zabrinutost u vezi s utjecajem nadzora na temeljna prava i načela prava EU-a[27]. Europski sud za ljudska

---

[25] Ujedinjeni narodi. *Izvješće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, Frank La Rue.* A/HRC/23/40, 2013.

[26] Amnesty International. *„Lessons from the Stasi—a cautionary tale on mass surveillance"* (Što smo naučili od Stasija – poučna priča o masovnom nadzoru). 2015.,
url: https://www.amnesty.org/en/latest/news/2015/03/lessons-from-the-stasi/

[27] Vidjeti Europski parlament (2014.). *Rezolucija od 12 ožujka 2014. o programu nadzora Agencije za nacionalnu sigurnost SAD-a (NSA), nadzornim tijelima u različitim državama članicama i njihovu utjecaju na temeljna prava građana EU-a te o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima (2013/2188(INI)); Agencija EU-a za temeljna prava. „Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU" (Nadzor koji provode obavještajne službe: mjere zaštite temeljnih prava i pravni lijekovi u EU-u). Svezak II.: „Field perspectives and legal update"* (Perspektive s terena i pravne novosti). Ured za publikacije Europske unije, 2017.

prava (ESLJP) i Sud Europske unije u nekoliko su predmeta dali mišljenja protiv prešiokog nadzora koji provode države[28].

Za razliku od njega, ciljani nadzor, koji je glavni predmet ovog izvješća, donedavno nije bio u središtu pozornosti. Međutim, nedavni razvoj tehnologije – što pokazuje softver poput Pegasusa – nalaže da razmotrimo i utjecaje ciljanog nadzora na pojedince i društvo. Zapravo, ako masovni nadzor izaziva opravdanu zabrinutost zbog svoje *širine*, budući da njime mogu biti obuhvaćeni svi članovi neke zajednice, ciljni nadzor i raspoloživi tehnološki alati u tom području izazivaju jednako opravdanu zabrinutost zbog svoje *dubine*, budući da njime mogu biti obuhvaćeni svi aspekti života pojedinaca na koje je usmjeren.

3.2. Izazov koji proizlazi iz špijunskog softvera

Sustavi špijunskog softvera poput Pegasusa, koji se upotrebljavaju za hakiranje mobilnih uređaja, omogućuju sveobuhvatan nadzor. Njihov utjecaj na pojedince protiv kojih se upotrebljava i na društvo u cjelini potencijalno je ogroman i mogao bi ugroziti temeljna prava EU-a i temeljne vrijednosti prava EU-a.

Dubinu njihova utjecaja možemo razumjeti samo ako uzmemo u obzir da ljudi danas žive u svijetu koji je hiperpovezan i u kojem se mnoge pojedinačne i društvene aktivnosti, ako ne i većina njih, odvijaju posredstvom digitalne infrastrukture kojom se koristimo za pohranjivanje i razmjenu goleme količine podataka te za usmenu i pismenu komunikaciju i interakciju. U tome posebnu ulogu imaju naši osobni uređaji, obično pametni telefoni, budući da služe kao sučelja putem kojih pristupamo toj dimenziji koju nastanjujemo, koju omogućuju i sačinjavaju digitalne tehnologije.

Može se činiti da se tehnologije za hakiranje uređaja mogu uklopiti u tradicionalno prisluškivanje, tehniku za tajni pristup komunikacijama koju tijela kaznenog progona i službe nacionalne sigurnosti u velikoj mjeri upotrebljavaju od početka razvoja telekomunikacijskih mreža. U širem smislu, pod prisluškivanjem podrazumijevamo tajno pristupanje sadržaju neke poruke koja se šalje putem komunikacijskih linija i slanje kopije te poruke agenciji koja vrši presretanje. Prisluškivanje se izvorno sastojalo od postavljanja električnog uređaja (prisluškivača) na telefonsku liniju, ali danas se to može izvršiti na daljinu zahvaljujući tehnologijama digitalnog uključivanja koje aktiviraju komunikacijski operateri. Ta se praksa uređuje nacionalnim zakonima i razmatra u nadnacionalnim instrumentima poput Rezolucije Vijeća o zakonitom presretanju[29].

Međutim, postoje važne razlike između prisluškivanja i hakiranja uređaja, budući da je potonjim moguće prikupiti veću količinu informacija: uz pristupanje porukama na napadnutom uređaju, hakiranjem se može pristupiti *svim* podacima koji su na njemu pohranjeni, a možda i manipulirati njima. Hakiranje uređaja provodi se s ciljem prikupljanja većeg skupa podataka, ali i s ciljem prevladavanja tehnologija za šifriranje, kao što se navodi u Poglavlju 3.1. U slučaju sveobuhvatnog šifriranja izvorna se komunikacija prije slanja pretvara u šifrirani tekst koji nije razumljiv trećim stranama: kako bi se izvorna komunikacija oporavila, šifrirani tekst mora se dešifrirati s pomoću tajnog ključa koji je dostupan isključivo primatelju. Hakiranje uređaja omogućuje da se šifriranje zaobiđe na način da se

[28] Među najnovijim predmetima ESLJP-a vidjeti *Big Brother Watch i ostali protiv Ujedinjene Kraljevine* [GC] (br. 58170/13, 62322/14 i 24960/15, 25. svibnja 2021.); među predmetima Suda Europske unije vidjeti *Povjerenik irske policije (Garda Síochána) i ostali* (C-140/20, 5. travnja 2022.).

[29] Rezolucije Vijeća od 17. siječnja 1995. o zakonitom presretanju telekomunikacija (96/C 329/01).

izvorne poruke zabilježe *prije* šifriranja. Kad se napredne tehnologije šifriranja primjenjuju u kriminalnim aktivnostima, može biti opravdano pribjeći hakiranju uređaja kako bi se suzbila najteža kaznena djela i prijetnje nacionalnoj sigurnosti. Međutim, u nastavku ćemo pokazati da se u nedostatku strogih ograničenja i djelotvornih kontrola praksa hakiranja uređaja teško može uskladiti s pravnim okvirom EU-a i općenitije s očuvanjem demokracije i ljudskih prava.

3.3. Ključne značajke Pegasusa

Prema navodima Europskog nadzornika za zaštitu podataka, možemo razlikovati tri istaknute značajke Pegasusa zbog kojih on „može uzrokovati nezapamćene rizike i nanijeti nezapamćene štete ne samo u odnosu na temeljne slobode pojedinaca, već i u odnosu na demokraciju i vladavinu prava"[30]. Riječ je o mogućnostima Pegasusa da (a) stekne *potpuni* pristup uređaju na koji je usmjeren, (b) provede napade bez klika i (c) iza sebe ostavi vrlo malo tragova ili uopće ne ostavi tragove. Analizirajmo svaku od tih značajki pojedinačno.

3.3.1. Potpuni pristup

Prva je značajka Pegasusov „potpun i neograničen pristup uređaju na koji je usmjeren"[31], što se pokazalo u istragama koje je proveo Security Lab[32] organizacije Amnesty International. U opisu proizvoda koji je objavio Security Lab[33] navodi se da Pegasus može prikupljati podatke na tri načina:

- *Prvobitno izvlačenje podataka*, kojim se prikupljaju svi podaci koji su već dostupni na uređaju u vrijeme instalacije Pegasusa, uključujući zapise o SMS porukama, pojedinosti o kontaktima, povijest poziva (zapisnik poziva), zapise kalendara, poruke e-pošte, razmjenu izravnih poruka i povijest pregledavanja.
- *Pasivno praćenje*, kojim se u stvarnom vremenu prikupljaju svi novi zapisi koji postanu dostupni dok je špijunski softver u funkciji (uključujući već navedene informacije i praćenje lokacije na temelju „ID-a ćelije", tj. broja kojim se identificira obližnja primopredajna postaja na koju se telefon spaja kako bi pristupio komunikacijskoj mreži).
- *Aktivno praćenje*, koje se sastoji od uporabe funkcionalnosti napadnutog uređaja za izvršavanje daljnjih aktivnosti s ciljem prikupljanja podataka, poput praćenja lokacije s pomoću GPS-a, snimanja glasovnih poziva, dohvaćanja datoteka, snimanja zvukova iz okoliša te snimanja fotografija i snimki zaslona.

---

[30] Europski nadzornik za zaštitu podataka. „Preliminary remarks on modern spyware" (Preliminarne opaske o modernom špijunskom softveru), 2022. https://edps.europa.eu/system/files/2022-02/22-02-15edpspreliminaryremarksonmodernspywareen0.pdf

[31] Europski nadzornik za zaštitu podataka. „Preliminary Remarks", str. 3.

[32] Amnesty International. *„Forensic Methodology Report. How to Catch NSO Group's Pegasus*" (Izvješće o forenzičkoj metodologiji. Kako uhvatiti Pegasus Grupe NSO). Amnesty International, 2021. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[33] „Pegasus – *Product Description*" (Pegasus – Opis proizvoda).

Slika 6.: Prikupljanje podataka s pomoću Pegasusa[34]

Pegasus omogućuje razinu nadzora i manipulacije koja je dosad bila nezamisliva (Slika 6..). Slavni citat Hannah Arendt kaže „svemu što živi potrebna je sigurnost koju pruža tama da bi uopće moglo rasti”.[35] U slučaju uporabe Pegasusa ništa se ne ostavlja u tami.

3.3.2. Napadi bez klika

Pegasus omogućuje takozvane napade bez klika, što znači da pojedinac protiv kojeg je usmjeren ne mora izvršiti nikakvu radnju da bi se softver instalirao: nije potrebno da klikne neko upozorenje ili odgovori na poruku (vidjeti Slika 7..). U opisu Pegasusa o toj se značajci navodi sljedeće:

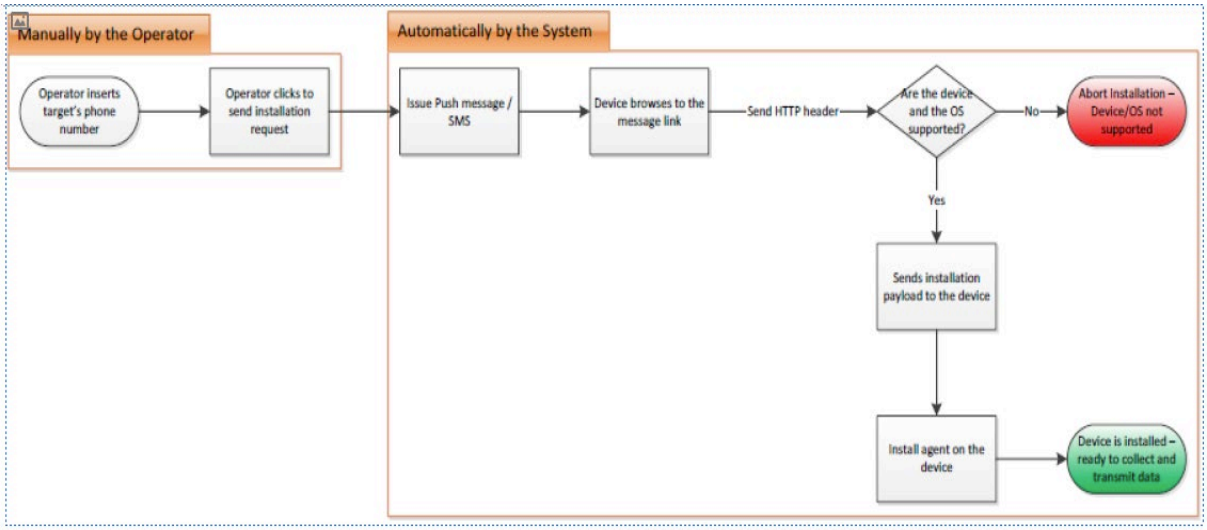
> *Na mobilni se uređaj daljinski i tajno šalje automatska poruka. Ta poruka pokreće preuzimanje i instalaciju agenta na uređaj. Tijekom cijelog procesa instalacije ne traži se suradnja ni sudjelovanje mete (npr. da klikne poveznicu ili otvori poruku) i na uređaju se ne prikazuje nikakav znak o tome. Instalacija je potpuno tiha i nevidljiva i meta je ne može spriječiti*[36].

[34] „Pegasus – *Product Description” (Pegasus – Opis proizvoda)*, str. 16.

[35] Arendt, H. „The Crisis in Education” (Kriza u obrazovanju). U *„Between Past and Future: Six Exercises in Political Thought”. (Između prošlosti i budućnosti: šest primjena političke misli). Viking*, 1961. [1954.].

[36] Pegasus – *Product Description (Pegasus – Opis proizvoda)*, str. 12.

Slika 7.: Instalacija agenta Pegasus[37]



Stoga ni pažljiv korisnik koji je vješt s digitalnim tehnologijama možda neće biti svjestan da špijunski softver kontrolira njegov uređaj. Zahvaljujući radu organizacija Amnesty International i Citizen Lab iz Toronta[38], među ostalima, identificirani su različiti iskorištavatelji slabih točaka koji ne zahtijevaju klikanje, tj. dijelovi softvera i podataka koji stječu kontrolu nad uređajima korisnika i iskorištavaju njihove nedostatke, pri čemu korisnik ne mora izvršiti nikakvu konkretnu radnju. Ti iskorištavatelji slabih točaka preuzimaju agent Pegasus (dio softvera Pegasus koji se instalira na žrtvin uređaj), koji zatim prikuplja podatke i vrši interakciju s udaljenim Pegasusovim poslužiteljima (Slika 7.. i Slika 8..). Čak ni najveća i tehnološki najnaprednija poduzeća u području informacijsko-komunikacijskih tehnologija poput Googlea i Applea nisu dosad uspjela osigurati djelotvornu preventivnu zaštitu jer vodeća poduzeća koja proizvode špijunski softver na raspolaganju imaju vrhunske vještine koje se mogu mjeriti s onima kojima raspolažu obavještajne agencije neke države[39].

3.3.3. Bez tragova (ili s vrlo malo tragova)

Vrlo je teško otkriti instalaciju Pegasusa, pribaviti dokaze o njegovim aktivnostima i identificirati tko je počinio upad, osim ako napadnuti sustav ima funkciju sigurnog bilježenja (koja bilježi sve aktivnosti uređaja), što je, čini se, slučaj s Appleovim telefonima. Zapravo, Pegasus tijekom deinstalacije nastoji ukloniti sve tragove svoje prisutnosti. Prema navodima Europskog nadzornika za zaštitu podataka, nove verzije Pegasusa može biti još teže otkriti jer se instaliraju samo privremeno ili se nalaze u oblaku. Konačno, nije moguće identificirati udaljene operatere Pegasusa jer se koriste mrežom kojom se anonimizira veza između Pegasusova agenta i Pegasusova poslužitelja (Slika 8.).

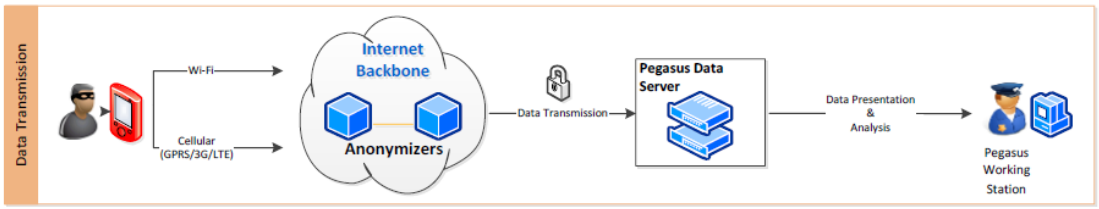
---

37 Pegasus – *Product Description (Pegasus – Opis proizvoda)*, str. 13.

38 Citizen Lab je interdisciplinarni laboratorij koji djeluje pri Munk School of Global Affairs & Public Policy na Sveučilištu u Torontu.

39 Newman, L. H. „Google Warns That NSO Hacking Is On Par With Elite Nation-State Spies" (Google upozorava da je hakiranje koje provodi NSO usporedivo s elitnim špijunima nacionalnih država). U *Wired* (15. prosinca 2021.).

Slika 8.: Pegasusov proces prikupljanja podataka[40]



3.3.4. Višeslojno otvoreno okruženje

Infrastruktura kojom se koristi Pegasus (i ostale slične tehnologije za hakiranje uređaja) znatno je drugačija od tehnoloških okvira za tradicionalno prisluškivanje. Nadležni službenici se pri presretanju komunikacija koje se prenose telefonskim linijama obično mogu osloniti na certificiranu i kontroliranu opremu i na transparentnu suradnju telekomunikacijskih operatera. To često nije tako u slučajevima kad se tijela kaznenog progona ili službe nacionalne sigurnosti koriste „posebnim istražnim tehnikama", a posebno kad hakiraju računalne uređaje u svrhu prikupljanja podataka i praćenja komunikacija. Sustav poput Pegasusa funkcionira na temelju mnoštva mreža i hardvera u privatnom vlasništvu (uključujući hardver koji pripada žrtvi), bez dogovorenog okvira u kojem sudjeluju telekomunikacijska poduzeća. Stoga se može tvrditi da Pegasus ne jamči sigurnost komunikacija i samim time ne jamči da se prikupljeni podaci neće nezakonito izmijeniti ili upotrebljavati u dodatne svrhe.

3.3.5. Manipulacija sadržaja

Kao što smo već spomenuli, Pegasus preuzima kontrolu nad uređajem na koji je usmjeren i koristi se njegovim funkcionalnostima. To mu omogućuje vršenje aktivnog nadzora, na primjer, može narediti mikrofonu i kameri uređaja da snimaju podatke iz okruženja.

Nadalje, kontrola koja se uspostavlja nad uređajem primjenom Pegasusa u načelu bi se mogla iskoristiti u razne nezakonite svrhe: za izmjenu sadržaja uređaja kreiranjem i pohranjivanjem lažnih poruka ili drugih dokumenata; za slanje lažnih poruka, uz pretvaranje da ih šalje vlasnih uređaja; za ostvarivanje pristupa digitalnoj ili fizičkoj imovini vlasnika uređaja, a možda i za izvršavanje transakcija u ime vlasnika; ili za podmetanje lažnih dokaza o kaznenim ili drugim nezakonitim djelima na uređaj[41].

3.3.6. Uporaba Pegasusa

Kao što je već spomenuto, Pegasus je razvilo izraelsko poduzeće pod nazivom Grupa NSO[42] koje taj softver prodaje vladama diljem svijeta, pri čemu te prodaje odobrava izraelsko Ministarstvo obrane. NSO tvrdi da se prema njegovim ugovornim klauzulama Pegasus može upotrebljavati isključivo za borbu protiv terorizma i zločina (unatoč tomu što, kao što ćemo vidjeti, postoje opsežni dokazi o

[40] Pegasus – *Product Description* (Pegasus – Opis proizvoda), str. 13.

[41] Europski nadzornik za zaštitu podataka. „Preliminary remarks on modern spyware" (Preliminarne opaske o modernom špijunskom softveru), str. 3.

[42] Naziv NSO čine prva slova imena osnivača poduzeća: Niv, Shalev i Omri.

uporabi Pegasusa u druge svrhe). Poduzeće je navelo da je prodalo Pegasus 60 vladinih agencija u 40 država.

Javnost je prvi put saznala za raširenost uporabe (i zlouporabe) Pegasusa iz istrage koju je 2018. proveo Citizen Lab Sveučilišta u Torontu, utvrdivši naznake o prisutnosti Pegasusa u 45 država, među kojima neke imaju autoritarne režime.

Prema izvješću koje je 2021. objavio Pegasus Project, zajednička inicijativa više od 80 novinara iz 17 medijskih organizacija u deset država koju je koordinirao Forbidden Stories uz tehničku potporu organizacije Amnesty International, uporaba špijunskog softvera Pegasus protiv aktivista za ljudska prava, pripadnika opozicije, odvjetnika, sudaca i stranih vođa široko je rasprostranjena među vladama diljem svijeta[43]. Pegasus Project također je objavio popis 50 000 brojeva telefona za koje se čini da pripadaju pojedincima koje su klijenti izraelske Grupe NSO odabrali kao moguće mete nadzora.

Europski parlament osnovao je istražni odbor PEGA sa zadaćom da istraži uporabu Pegasusa i ekvivalentnog špijunskog softvera za nadzor[44]. Istraga koju je taj odbor proveo pokazala je da postoje čvrsti dokazi o uporabi Pegasusa u EU-u. Čini se da je Grupa NSO svoje proizvode prodala 22 krajnja korisnika u najmanje 14 država članica, uključujući Poljsku, Mađarsku, Španjolsku, Nizozemsku i Belgiju. Dvije države članice, Cipar i Bugarska, služile su kao središta izvoza špijunskog softvera[45].

U SAD-u su se već počela provoditi određene mjere protiv zlouporaba počinjenih s pomoću Pegasusa. Ta je država 2021. stavila Grupu NSO na crnu listu zbog bavljenja aktivnostima protivnim interesima Sjedinjenih Državama povezanim s nacionalnom sigurnošću ili vanjskom politikom (poduzeće je stoga isključeno iz ugovora s državnim agencijama SAD-a i poslovanja s poduzećima iz SAD-a). Radi se o značajnoj promjeni politike SAD-a, budući da se čini da je sam SAD otpočeo pregovore s ciljem kupnje Pegasusa i čak ga kupio za vladu Džibutija. Međutim, čini se da se agencije iz SAD-a i dalje služe špijunskim softverom koji ima slične funkcije, kao što je Graphite, koji je razvilo izraelsko poduzeće Paragon[46]. Apple i Meta također su 2021. podnijeli sudske tužbe protiv Grupe NSO zbog nadzora i ciljanja njihovih korisnika. Jedan okružni sud u SAD-u odbacio je u lipnju 2022. zahtjev za imunitetom Grupe NSO u tužbi koju je podnio Apple.

U studenome 2021. doznalo se da je Izrael uklonio 65 država sa svojeg popisa država u koje se smiju izvoziti kiberproizvodi, čime je njihov broj smanjen sa 102 na 37. Ipak, u medijima je objavljeno da je Izrael ponovno dao odobrenje za uporabu Pegasusa Saudijskoj Arabiji.

---

[43] Amnesty International. „Forensic Methodology Report. *How to Catch NSO Group's Pegasus*" (Izvješće o forenzičkoj metodologiji. Kako uhvatiti Pegasus Grupe NSO). 2021.

[44] PEGA (Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor). https://www.europarl.europa.eu/committees/hr/pega/home/highlights.

[45] Europski parlament. Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor, izvjestiteljica: Sophie in 't Veld (2022.). *Nacrt izvješća*.

[46] Mazetti, M., Bergman, R., i Sevis-Grindneff, M. „US strains to control spyware, but uses it" (SAD se trsi kontrolirati špijunski softver, ali se koristi njime). *The New York Times* (1. prosinca 2022.). s.

4. PEGASUS I (DELIBERATIVNA) DEMOKRACIJA

KLJUČNI ZAKLJUČCI

Sveobuhvatni nadzor utječe na privatnost osoba i njihova prava povezana sa zaštitom podataka, ali i na druga prava pojedinaca, poput prava na slobodu govora, udruživanja i okupljanja, kao i na demokratski ustroj društva (koji podrazumijeva ostvarivanje navedenih prava).

Špijunski softver utječe na političko sudjelovanje utoliko što se građane podvrgnute špijuniranju može zastrašiti da se suzdrže od sudjelovanja u interakcijama političkog sadržaja, od iskrenog izražavanja njihovih stajališta i od udruživanja s drugima u političke svrhe. To utječe na kvalitetu demokratske javne sfere koja u konačnici ovisi o doprinosima i reakcijama građana.

Konkretnije, špijunski softver često se upotrebljava za napade na pojedince (poput novinara, političara i aktivista) koji imaju posebnu ulogu u javnoj sferi. Podvrgavanjem takvih pojedinaca nadzoru otvara se prostor za represiju, manipulaciju, ucjenjivanje, krivotvorenje i klevetu.

To može utjecati i na sam izborni proces, pri čemu se prikupljeni podaci, kojima se možda manipuliralo, mogu iskoristiti za provođenje kampanja sramoćenja usmjerenih na neželjene kandidate ili za druga djelovanja koja negativno utječu na njihove izglede za uspjeh. Sam strah da bi ih netko mogao špijunirati može navesti ljude da se ne kandidiraju za neku funkciju ili ih može spriječiti u vođenju djelotvorne kampanje.

Sveobuhvatni nadzor utječe na privatnost osoba i prava povezana sa zaštitom podataka, ali i na druga prava pojedinaca, poput prava na slobodu govora, udruživanja i okupljanja, kao i na demokratsko tkivo društva (koje podrazumijeva ostvarivanje navedenih prava).

Veza između zaštite podataka i demokracije oduvijek je bila ključni aspekt rasprave o zaštiti podataka[47] i posljednjih je godina sve više dobivala na važnosti zbog sve veće digitalizacije društva i sve moćnijih tehnologija za nadzor.

> *Ni sloboda govora ni sloboda udruživanja ni sloboda okupljanja ne mogu se u cijelosti ostvarivati dokle god i dalje nije sigurno prikupljaju li se i obrađuju osobni podaci, u kojim okolnostima i u koje svrhe. Razmatranja o zaštiti privatnosti sežu dalje od bilo kojeg pojedinačnog prava: ona određuju izbor između demokratskog i autoritarnog društva*[48].

U razdoblju nakon Snowdenovih otkrića, Parlamentarna skupština Vijeća Europe navela je u svojoj rezoluciji br. 2045 da se praksama nadzora koje primjenjuju države ugrožavaju ljudska prava, koja čine „okosnice demokracije' i čijom se „povredom bez odgovarajućeg sudskog nadzora također ugrožava vladavina prava"[49].

---

[47] Vidjeti: Simitis, S. „Reviewing Privacy in the Information Age" (Preispitivanje privatnosti u informacijskom dobu). U *University of Pennsylvania Law Review* (1987.), str. 707-46.; Rodotà, S. „Data Protection as a Fundamental Right" (Zaštita podataka kao temeljno pravo). U *„Reinventing Data Protection*?" (Preobrazba zaštite podataka?) Ur. Serge Gutwirth i dr. Springer, 2009., str. 77–82.

[48] Simitis. „Reviewing Privacy in the Information Age" (Preispitivanje privatnosti u informacijskom dobu), str. 734.

[49] Vidjeti: Vijeće Europe. *„Mass surveillance: Who is watching the watchers?" (Masovni nadzor: tko promatra promatrače?)* Council of Europe Publishing, 2016.

U sljedećim poglavljima razmotrit ćemo načine na koje nadzor, posebno nadzor koji se vrši uporabom Pegasusa, može ozbiljno utjecati na ekologiju demokracije i ometati njezine različite aspekte.

4.1. Ideja predstavničko-deliberativne demokracije

Kako bismo razumjeli kako nadzor može utjecati na demokratske procese, moglo bi biti korisno razmotriti vrstu društvenog uređenja koja je potrebna za djelotvornu demokraciju. Iako postoje brojne definicije demokracije i brojni pristupi demokraciji[50], ovdje ćemo se fokusirati na ideju deliberativne demokracije u sklopu koje se pruža širok normativni okvir za pristup političkom sudjelovanju i za razumijevanje njegovih nedostataka. Koncepte vijećanja i deliberativne demokracije možemo definirati na sljedeći način:

> *Vijećanje definiramo minimalno kao međusobnu komunikaciju koja uključuje odvagivanje i razmatranje preferencija, vrijednosti i interesa u vezi s pitanjima od zajedničkog interesa. Deliberativna demokracija uključuje zahtjeve da se to vijećanje odvija u okruženjima jednakog priznavanja, poštovanja, reciprociteta i dovoljno jednakih ovlasti da bi komunikativni utjecaj mogao funkcionirati*[51].

To znači da bi, s obzirom na ideal deliberativne demokracije, javne odluke trebale biti podržane odgovarajućim javnim opravdanjima tako da u konačnici može prevladati „sila bez sile koju čini bolji argument"[52] ili kako bi barem postojala sklonost da se saslušaju argumenti i da se ostvari pomak prema razumnim ishodima. Političke odluke uistinu bi trebale biti ishod otvorenih i uključivih procesa u kojima se iznose različita mišljenja i o njima se raspravlja na temelju razloga koje građani mogu razumjeti kako bi se „represija, ugnjetavanje i bezobzirno zanemarivanje mogli zamijeniti uvjeravanjem pri kojem se ističu relevantna razmatranja"[53]. Promicanje predstavničke i deliberativne demokracije jedan je od ciljeva Komisijina akcijskog plana za europsku demokraciju[54] iz 2020.

Iz perspektive liberalnog i deliberativnog pristupa, institucionalnim oblikovanjem suvremenih demokracija trebalo bi zajamčiti tri temeljna aspekta:

> *kao prvo, privatnu autonomiju građana, koji svi vode vlastiti život; kao drugo, demokratsko građanstvo, to jest uključivanje slobodnih i jednakih građana u političku zajednicu; i kao treće, neovisnost javne sfere koja funkcionira kao posrednički sustav između države i društva*[55].

---

50 Među nedavnim osvrtima vidjeti npr.: Beckman, L. „Democracy" (Demokracija). U *Oxford Research Encyclopedias, Politics*. Oxford University Press, 2021.; Christiano, T. i Sameer B. „Democracy" (Demokracija). U *The Stanford Encyclopedia of Philosophy*, Stanford University, 2022.

51 Bächtiger, A. i dr. „Deliberative Democracy: An Introduction" (Deliberativna demokracija: Uvod). U *The Oxford Handbook of Deliberative Democracy*. Oxford University Press, rujan 2018., str. 1.

52 Habermas, J. *„Legitimation Crisis" (Kriza legitimacije)*. Cambridge, Beacon Press, 1975., str. 108.

53 Mansbridge, J. i dr. „A systemic approach to deliberative democracy" (Sustavni pristup deliberativnoj demokraciji). U: *„Deliberative Systems: Deliberative Democracy at the Large Scale*" (Deliberativni sustavi: deliberativna demokracija u velikim razmjerima). Ur. J. Parkinson i J. Mansbridge. Cambridge University Press, 2012.

54 Komisija Europskih zajednica. *Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija o akcijskom planu za europsku demokraciju.* COM(2020) 790 final, 2020.

55 Habermas, J. *„Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research" (Politička komunikacija u medijskom društvu: uživa li demokracija i dalje epistemičku dimenziju? Utjecaj normativne teorije na empirijsko istraživanje). U: Communication Theory* (2006.), str. 412.

4.2. Utjecaj sveobuhvatnog nadzora na demokraciju

Nije teško uvidjeti da sveobuhvatni nadzor primjenom špijunskog softvera poput Pegasusa može ozbiljno utjecati na predstavničko-deliberativnu demokraciju.

Razmotrimo najprije položaj svih pojedinaca koji mogu opravdano sumnjati da su pod nadzorom, to jest da su njihovi uređaji hakirani ili bi mogli biti hakirani u skoroj budućnosti na takav način da bi se cijeli njihov život mogao promatrati sa zlom namjerom. To će u njima pobuditi strah da bi mogli biti podvrgnuti štetnim mjerama u slučaju da se otkrije neko neželjeno ponašanje ili okolnosti uslijed kojih će se pojaviti nove mogućnosti da im se uzrokuje šteta (na primjer, napadom na njihov ugled ili predviđanjem njihovih postupaka). Te štetne mjere mogu uključivati pravne ili društvene sankcije, nametnute gubitke (otkaz, onemogućivanje prilika), klevetu te nezakonite i moguće nasilne napade. Ljudi se pod takvim uvjetima mogu suzdržati od bilo kakvih aktivnosti koje bi se mogle otkriti i dovesti do štetnih reakcija. U tom pogledu katkad se govori o učinku Panopticona (naziv zatvora koji je krajem 18. stoljeća osmislio filozof Jeremy Bentham, u kojem su čuvari vidjeli zatvorenike, ali zatvorenici nisu mogli vidjeti promatra li ih netko u bilo kojem datom trenutku): sama mogućnost da ih se promatra i da će biti „kažnjeni" pojedince izlaže pritisku da se ponašaju u skladu s onime što smatraju da se od njih očekuje.

Nadalje, svi koji vjeruju da bi i sami mogli biti podvrgnuti sličnim mjerama mogu izvući pouke iz štetnog utjecaja nadzora na određene pojedince. Sve potencijalne žrtve nadzora uče da se ne bi trebale ponašati na način zbog kojeg bi mogle biti podvrgnute nadzoru. Osim toga, uče da se ne bi trebale ponašati na način koji bi mogao dovesti do štetnih društvenih, političkih ili pravnih učinaka ako se uoči u okviru nadzora. Ljudi podložni takvim rizicima mogli bi izbjegavati djelovanja usmjerena na društvena i politička pitanja, mogli bi se samocenzurirati i izbjegavati izražavanje vlastitog mišljenja čak i u privatnim okruženjima te bi mogli odlučiti živjeti skrivajući se i ostati izvan javne sfere.

S obzirom da tako utječe na pojedince, špijunski softver utječe i na demokratsko-deliberativni stroj društva na način koji ovisi o konkretnoj ulozi koju različiti pojedinci imaju u tom ustroju. U nedavnim radovima u području demokratske teorije usvaja se sustavni pristup deliberativnoj demokraciji: zdrava deliberativna demokracija zahtijeva da joj više segmenata društva doprinosi na različite načine kako bi se društvene odluke temeljile na promišljenim javno dostupnim razlozima do kojih se došlo u okviru uključivog procesa. Sveobuhvatni nadzor, a posebno uporaba špijunskog softvera poput Pegasusa, može snažno utjecati na funkcioniranje različitih aspekata demokratskog uređenja.

U prvom redu, špijunski softver može utjecati na prvi od tri utvrđena aspekta, to jest na *privatnu autonomiju* pojedinaca, odnosno njihove privatne odluke i interakcije. Špijunski softver utječe na demokraciju zadirući u privatnu autonomiju pojedinaca utoliko što se demokracija zasniva na premisi da ljudi imaju mogućnost samostalno donositi svoje životne odluke (koje se odnose na obitelj, rad, slobodno vrijeme itd.) i sudjelovati u neformalnim interakcijama s drugima te u skladu s time razvijati vlastite interese i ideje. Pojedinci mogu dati autentične doprinose javnoj sferi samo ako mogu razvijati vlastitu osobnost bez neopravdanog pritiska izvana.

Međutim, izloženost sveobuhvatnom nadzoru utječe i na drugi od spomenuta tri aspekta, a to je *demokratsko građanstvo*. U tom pogledu moramo uzeti u obzir da demokratsko građanstvo uključuje „političko sudjelovanje što većeg broja zainteresiranih građana putem jednakih prava komunikacije i sudjelovanja; periodične izbore (i referendume) koji se održavaju na temelju uključivog prava glasa;

natjecanje različitih stranaka, platformi i programa; i načelo većine za političke odluke u predstavničkim tijelima"[56].

Špijunski softver utječe na političko sudjelovanje utoliko što se građani podvrgnuti špijuniranju mogu suzdržati od sudjelovanja u interakcijama političkog sadržaja, od iskrenog izražavanja svojih stajališta i od udruživanja s drugima u političke svrhe. Time bi se građane spriječilo u ostvarivanju slobode izražavanja i udruživanja. Osim toga, to će utjecati na kvalitetu demokratske javne sfere koja u konačnici ovisi o doprinosu i reakcijama građana.

Špijunski softver ugrožava i treći od navedena tri aspekta, *neovisnost javne sfere*, jer ometa komunikaciju građana, medijskih kuća i političara te ih podvrgava neopravdanom utjecaju u političke svrhe.

Kako bismo razumjeli kako se sve navedeno može dogoditi, moramo uzeti u obzir da je deliberativno-demokratsko uređenje, kao što je spomenuto, ekologija koja se temelji na kombinaciji različitih sastavnica: zdravo demokratsko okruženje moguće je samo ako svaka od njih na odgovarajući način izvršava svoju funkciju.

> *Središte političkog sustava sastoji se od poznatih institucija: parlamenata, sudova, upravnih tijela i vlada. Svaka grana može se opisati kao specijalizirana deliberativna arena* [...]. *Na rubu političkog sustava, javna sfera temelji se na mrežama za neograničen protok poruka – vijesti, izvješća, komentara, razgovora, prizora i slika te programa i filmova informativnog, polemičkog, edukativnog ili zabavnog sadržaja. Ta mišljenja koja se objavljuju potječu od raznih vrsta aktera – političara i političkih stranaka, lobista i interesnih skupina ili sudionika civilnog društva. Odabiru ih i oblikuju djelatnici masovnih medija, a primaju ih široke publike koje se međusobno preklapaju, tabori, supkulture itd.*

U tom kontekstu

> *na pozitivne ili negativne stavove o kontroverznim javnim pitanjima koji se prešutno oblikuju utječu svakodnevni razgovori u neformalnim okruženjima ili epizodne javnosti civilnog društva barem u jednakoj mjeri u kojoj na njih utječe obraćanje pozornosti na tiskane ili elektroničke medije.*

Iako svaki građanin može imati neku ulogu u javnoj sferi, političari i medijski djelatnici obično se nalaze u središtu političkog sustava u dvojnoj ulozi suautora i primatelja javnog mnijenja. To je tako u velikoj mjeri i danas kada zahvaljujući internetu svatko ima mogućnost objavljivati informacije i komentare na forumima, blogovima, mrežnim repozitorijima, društvenim mrežama itd.

Konačno, izbori imaju nužnu funkciju u svakom demokratsko-deliberativnom uređenju: oni osiguravaju kontinuiranu relevantnost javnog mnijenja za donošenje javnih odluka na način da biračima omogućuju da odaberu predstavnike čija su stajališta usklađena s njihovim vlastitima.

Slučaj Pegasusa i drugih sličnih špijunskih softvera pokazuje kako se sve te različite procese demokratske ekologije može ometati i kako ih se ustvari i ometalo.

Kao prvo, mogućnost izloženosti špijuniranju u širokom smislu utječe na političku aktivnost svih pojedinačnih građana. Zbog nadzora će se možda suzdržati od pristupanja političkim informacijama i distribucije tih informacija (s obzirom na to da se može nadzirati pregledavanje interneta i digitalnih komunikacija) te se kloniti političkih interakcija, od svakodnevnih razgovora u neformalnim okruženjima do sudjelovanja u političkim pokretima i zajedničkom djelovanju.

---

[56] Habermas J. „*Political Communication in Media Society*" (Politička komunikacija u medijskom društvu), str. 412.

Konkretnije, špijunski softver utječe na pojedince koji, kao što smo naveli, imaju posebnu ulogu u javnoj sferi. Zapravo, često se upotrebljava protiv novinara i političara te općenitije osoba uključenih u politički aktivizam. Podvrgavanjem takvih pojedinaca nadzoru otvara se prostor za represiju, manipulaciju, ucjenjivanje, krivotvorenje i klevetu. To negativno utječe ne samo na pojedince koji su podvrgnuti nadzoru, već i na proces oblikovanja mišljenja u javnoj sferi. Novinari koje se špijunira možda neće moći izvještavati, primjerice, zbog straha da se njihovi povjerljivi kontakti prate ili zbog zapreka s kojima se susreću u svojem istraživačkom radu ili će se suzdržati od objavljivanja priča zbog straha od štetnih reakcija temeljenih na povjerljivim podacima prikupljenim s njihovih uređaja. Slična razmatranja odnose se i na političare ako ih promatramo s obzirom na njihov doprinos javnoj komunikacijskoj sferi. Kad vladajuće političke snage upotrijebe špijunski softver protiv svojih protivnika, ugrožen je i jedan temeljni aspekt demokratskog ustroja, koji je, doduše, uvijek ugrožen, a to je odvojenost medija i političke moći.

Zbog špijunskog softvera može biti izravno narušeno funkcioniranje temeljnih institucija u demokratskom uređenju, a to su zakonodavna i sudska vlast. Napadi mogu biti usmjereni protiv osoba koje već služe kao izabrani predstavnici ili suci: neki od njih mogu iskusiti štetne mjere temeljene na prikupljenim podacima; drugi se jednostavno mogu bojati špijuniranja. I u jednom i u drugom slučaju ti se pojedinci mogu suzdržavati od djelovanja u skladu sa standardima svoje uloge zakonodavaca ili sudaca. Ti standardi u prvom slučaju od njih zahtijevaju reguliranje društva za opće dobro njegovih građana, uz poštovanje ustavnih ograničenja, a u drugom slučaju zahtijevaju od njih nepristrano presuđivanje u sporovima u skladu sa zakonom.

Konačno, to može utjecati i na sam izborni proces, pri čemu se prikupljeni podaci, kojima se možda manipuliralo, iskorištavaju za provođenje kampanja sramoćenja usmjerenih na neželjene kandidate ili za druga djelovanja kojima će se smanjiti njihovi izgledi za uspjeh na izborima (u korist njihovih protivnika)[57]. Nadalje, sam strah od izloženosti špijuniranju može ljude navesti da se ne kandidiraju za neku funkciju ili ih može spriječiti u vođenju djelotvorne kampanje. Time može biti narušena pravednost i jednakost izbornog procesa, budući da će pojedinci i stranke kojima je na raspolaganju špijunski softver – izravno ili zahvaljujući vezama s pojedincima na vlasti – imati prednost u odnosu na pojedince i stranke protiv kojih se natječu i koji su podvrgnuti špijuniranju. Špijunski softver može omogućiti različite načine „kibernetičkog upletanja u izbore"[58]. Izvlačenjem privatnih podataka s uređaja žrtava špijunski softver omogućuje poduzimanje prvog koraka u *doxingu* (objavljivanju nečijih podataka bez dopuštenja)[59], to jest

> *praksi neovlaštenog pristupanja nekom računalnom sustavu ili digitalnom servisu poput računa na društvenim medijima ili računa e-pošte, izvlačenja nejavnih podataka i puštanja tih podataka u javnost.*

Zapravo, u istragama o Pegasusu pokazalo se da su materijali pribavljeni primjenom tog špijunskog softvera omogućili dvije vrste zlonamjernog *doxinga* (koji treba razlikovati od zviždanja u javnom interesu): „strateška hakiranja", koja se sastoje od selektivnog objavljivanja materijala koji su od interesa

---

[57] Slučaj Watergate (1972.) jedan je od veoma slavnih primjera upletanja u izborni proces nezakonitim prisluškivanjem. Upad u sjedište Demokratskog nacionalnog odbora i postavljanje uređaja za prisluškivanje doveli su do ostavke predsjednika SAD-a Richarda Nixona.

[58] Za razmatranje i klasifikaciju različitih vrsta „kibernetičkog upletanja u izbore", zajedno s referencama, vidjeti: Sanders, B. „Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections" (Demokracija pod utjecajem: paradigme odgovornosti države za operacije kibernetičkog utjecaja na izbore). U *Chinese Journal of International Law* (2019.); Watt, Eliza. *„State Sponsored Cyber Surveillance"* (Kibernadzor pod pokroviteljstvom države), poglavlje 2.4.3.

[59] Pojam *doxing* ili *doxxing* dolazi od kolokvijalnog izraza *dropping dox*, u kojem *dox* označava dokumente, a odnosi se na neželjenu distribuciju povjerljivih podataka (dokumenata).

za javnost, ali u svrhu promicanja stranačkih političkih interesa, i „manipulirana curenja", pri kojima se lažne ili na drugi način obmanjujuće informacija namjerno uključuju u veći skup autentičnih povjerljivih podataka koji se javno objavljuju. U potonjem slučaju *doxing* se može smatrati i jednim vidom dezinformiranja, što je naziv za praksu širenja

> *dokazivo lažnih ili obmanjujućih informacija koje su smišljene, iznesene i šire se radi stjecanja ekonomske koristi ili namjernog zavaravanja javnosti te koje mogu naškoditi javnom interesu […uključujući] ugrožavanje demokratskih političkih procesa i procesa donošenja politika*[60].

Čini se da dezinformacije imaju sve veću ulogu u izbornim procesima, u kojima se upotrebljavaju za diskreditiranje političara i stranaka u protivničkom taboru te općenitije za širenje lažnih ili obmanjujućih informacija koje pogoduju jednoj strani na štetu njezinih protivnika:

> *Dezinformacije su sada dio većeg broja alata koji se koriste za manipuliranje izbornim postupcima, kao što su hakerski napadi ili deformacija web-mjesta ili dobivanje pristupa osobnim podacima o političarima i njihovo objavljivanje. Operacije koje su kibernetski omogućene mogu se upotrebljavati da bi se kompromitirao integritet javnih informacija i spriječilo identificiranje izvora dezinformacija. To je ključno tijekom izbornih kampanja u kojima zbijeni raspored može spriječiti pravodobno otkrivanje dezinformacija i odgovor na njih.* [61]

4.3. Neki dokazi o primjeni Pegasusa za upletanje u demokratske procese

Istrage koje su proveli *Guardian* i 16 drugih medijskih organizacija upućuju na široko rasprostranjenu i kontinuiranu zlouporabu Pegasusa kako bi se utjecalo na stranačku politiku i medije. Također je objavljen popis s više od 50 000 telefonskih brojeva za koje se čini da pripadaju pojedincima koje su klijenti izraelske Grupe NSO odabrali kao moguće mete nadzora.

Na tom su popisu, uz teroriste i poznate zločince, i stotine poslovnih rukovoditelja, vjerskih vođa, pripadnika akademske zajednice, zaposlenika nevladinih organizacija te sindikalnih i vladinih dužnosnika, uključujući ministre u vladama, predsjednike država i predsjednike vlada. Na popisu je i više od stotinu novinara, uključujući reportere, urednike i rukovoditelje vodećih tiskovina.

U jednom izvješću Europskog parlamenta[62] navodi se da je Grčka optužena za napade na novinare i opozicijske političare izvršene špijunskim softverom za hakiranje uređaja[63]. Među žrtvama napada Pegasusom navodno su političari iz Mađarske, Francuske, Španjolske, Finske, Poljske, Belgije i Europske komisije.

---

60 Europska komisija. *Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija naslovljena „Suzbijanje dezinformacija na internetu: europski pristup"*. COM(2018) 236 final, 2018.

61 Europska komisija. *Komunikacija o suzbijanju dezinformacija na internetu*, poglavlje 3.2.

62 Marzocchi, O. i Mazzini, M. *Pegasus and surveillance spyware (Pegasus i špijunski softver za nadzor)*.

63 U Grčkoj dokazi upućuju na Predator. Radi se o špijunskom softveru sličnom Pegasusu koji su također razvila izraelska softverska poduzeća (koja posluju pod nazivom Intellexa). Vidjeti Benjakob, O. „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire" (Dok Izrael obuzdava svoju industriju kiberoružja, bivši obavještajac gradi novo carstvo), *Haaretz* (rujan 2022.), dostupno na: 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

Konkretno, u izvješću se citiraju istrage koje su pokazale da se u Mađarskoj na meti Pegasusa našlo više od 300 osoba, među kojima su novinari, političari, pripadnici akademske zajednice, odvjetnici i vladini dužnosnici.

Slično tomu, u izvješću se primjećuje da je, prema navodima organizacije Citizen Lab, poljska Vlada upotrijebila Pegasus kako bi pod nadzor stavila brojne poljske građane, uključujući odvjetnike, tužitelje, zastupnike u parlamentu i vođe političkih stranaka.

Pred Posebnim odborom poljskog Senata među ostalim je svjedočio profesor Zoll, koji je tvrdio da je Pegasus nezakonit u Poljskoj zbog nedostatka certifikacije te zbog mogućnosti koje pruža za curenje podataka i manipulaciju podacima. Nadalje, svjedočio je u upletanju u izbore 2019. izvršenom s pomoću Pegasusa, kojim je znatno izmijenjen jednak položaj kandidata u izbornom procesu i pravednost njegova ishoda. Kandidati koji su se našli na meti Pegasusa zapravo su bili u nepovoljnijem položaju u odnosu na svoje protivnike, posebno u slučajevima kad su se potonji zahvaljujući političkim vezama mogli poslužiti prikupljenim podacima za predviđanje i diskreditiranje protivničkih kandidata.

Senator Krzysztof Brejza svjedočio je 27. studenoga 2022. na saslušanju pred odborom PEGA naslovljenom „Utjecaj špijunskog softvera na temeljna prava / demokraciju i izborne procese”. U svojem je svjedočenju naveo da je tijekom izbora održanih 2019. godine bio podvrgnut sveobuhvatnom nadzoru, uključujući prisluškivanje te krađu i krivotvorenje korespondencije. Podaci pribavljeni putem nadzora, a posebno tekstualne poruke pribavljene s pomoću Pegasusa, izneseni su selektivno i na obmanjujući način u kontekstu klevetničke kampanje čiji je cilj bio utjecati na izbore. Njegovo svjedočenje ilustrira dubinu utjecaja nadzora na aktivnost pojedinačnih dionika te posljedično na funkcioniranje demokratskih institucija.

5. NACIONALNA SIGURNOST: OPRAVDANJE ILI IZLIKA?

KLJUČNI ZAKLJUČCI

Uporaba špijunskog softvera obično se opravdava pozivanjem na nacionalnu sigurnost. Međutim, čini se da se špijunski softver u mnogim slučajevima upotrebljava u neke druge svrhe, a posebno za ciljeve koji se odnose na stranačke političke interese ili suzbijanje socijalnog ili političkog protivljenja.

Kako bi se spriječila pretjerano široka uporaba pojma *nacionalne* sigurnosti, taj bi pojam trebalo tumačiti ograničeno i razlikovati ga od koncepta *unutarnje* sigurnosti, pri čemu je potonja širi pojam i uključuje sprečavanje rizika kojima su izloženi pojedinačni građani, a posebno provedbu kaznenog prava.

Prepoznato je da je nacionalna sigurnost poslužila mnogim državama kao pravni izgovor za ograničavanje slobode izražavanja, davanje legitimiteta mučenju i drugim oblicima zlostavljanja te zastrašivanje manjina, aktivista i političke opozicije.

Postoje opširni dokazi o uporabi Pegasusa protiv pojedinaca kao što su politički protivnici, aktivisti za ljudska prava, odvjetnici i novinari, koji nisu ni na koji način povezani s teškim kaznenim djelima i ne predstavljaju nikakvu prijetnju nacionalnoj sigurnosti.

U ovom poglavlju najprije ćemo razmotriti koncept nacionalne sigurnosti, a zatim ćemo preispitati uporabu tog koncepta kao opravdanja za djelovanje države, među ostalim u slučajevima kad se pod izlikom navodnih interesa nacionalne sigurnosti nastoje ostvariti neki drugi ciljevi na štetu temeljnih prava i demokracije.

5.1. Koncept nacionalne sigurnosti

Koncept sigurnosti primjenjuje se u različitim kontekstima, a njegovo područje primjene razlikuje se ovisno o tome o kakvoj se prijetnji radi[64]. U tom smislu možemo razlikovati vanjsku sigurnost, koja se odnosi na prijetnje koje potječu izvan državnog područja neke države; unutarnju sigurnost, koja se odnosi na sve prijetnje sigurnosti osoba na području neke države ili regije, bez obzira na to odakle potječu; i globalnu sigurnost, koja se odnosi na prijetnje koje je moguće suzbijati isključivo transnacionalnim mjerama. Primjerice, Europsko vijeće opisuje unutarnju sigurnost na sljedeći način:

> *Unutarnja sigurnost EU-a znači zaštitu osoba i vrijednosti slobode i demokracije kako bi svi mogli uživati u svojim svakodnevnim životima bez straha*[65].

Vijeće navodi sljedeće glavne prijetnje unutarnjoj sigurnosti:

---

[64] Pojam *sigurnost* (eng. *security*) dolazi od latinskog *securitas*, što označava stanje opisano pridjevom *securus*. *Securus* se sastoji od prefiksa *se*, što znači „bez", te imenice *cura*, koja označava „brigu". Stoga je biti u stanju sigurnosti prvobitno značilo biti bez brige ili tjeskobe te samim time ne biti u nikakvoj opasnosti ili biti na odgovarajući način zaštićen od svih mogućih prijetnji. U smislu aktivnosti, a ne stanja, sigurnost je aktivnost koja se provodi s ciljem sprečavanja ili suzbijanja prijetnji kako bi se postiglo stanje sigurnosti.

[65] Europsko vijeće Strategija unutarnje sigurnosti Europske unije – oblikovanje europskog modela sigurnosti. Ured za publikacije Europske unije, 2010.

> *„terorizam, teški i organizirani kriminal, trgovina drogom, kiberkriminal, trgovanje ljudima, seksualno iskorištavanje maloljetnika i dječja pornografija, gospodarski kriminal i korupcija, trgovina oružjem i prekogranični kriminal", uz „nasilje samo po sebi i prirodne katastrofe i katastrofe uzrokovane ljudskim djelovanjem" te „ostale česte pojave koje izazivaju zabrinutost i predstavljaju prijetnje sigurnosti i zaštiti ljudima diljem Europe, primjerice prometne nesreće".*

Pojam nacionalne sigurnosti ograničenijeg je područja primjene nego unutarnja sigurnost i obuhvaća izazove koji prijete egzistenciji i cjelovitosti neke nacije. Tako bismo mogli reći da je nacionalna sigurnost dovedena u pitanje kad je nanesena šteta temeljnim interesima neke nacije ili kad su oni u opasnosti te da je svrha aktivnosti nacionalne sigurnosti spriječiti takvu štetu i otkloniti takve prijetnje. Taj se pojam izvorno uglavnom upotrebljavao za pitanja koja se odnose na teritorijalnu cjelovitost i političku autonomiju nacionalnih država, uključujući upletanje stranih sila, ali i na terorizam i nasilnu subverziju. Čini se da je sigurnost tako bila povezana s idejom nacionalne obrane iako je uključivala aktivnosti usmjerene na zaštitu od stranih, ali i od unutarnjih (nasilnih) prijetnji političkoj zajednici u cjelini.

Takva se definicija, primjerice, može pronaći u pravu SAD-a[66]:

> *Nacionalna sigurnost odnosi se na aktivnosti koje izravno obuhvaćaju odnose Sjedinjenih Država s inozemstvom ili zaštitu nacije od unutarnje subverzije, strane agresije ili terorizma.*

Predloženi su širi pojmovi nacionalne sigurnosti kojima se taj koncept proširuje izvan okvira njegovog prvobitnog fokusa i uključuje sve prijetnje državnoj vlasti (suverenosti) i njezinoj sposobnosti da nadzire svoj teritorij:

> *Međunarodni terorizam nije jedina prijetnja koju zapadne države utvrđuju u svojim izgledima nacionalne sigurnosti. Raspon konvencionalnih prijetnji i dalje je uključen u njihove procjene rizika. To uključuje transnacionalni kriminal, oružja masovnog uništenja, sukobe unutar propalih država i između njih, izbijanje konvencionalnih ratova između naprednih vojski i pandemije. Osim toga, prepoznaje se niz kvalitativno „novih" prijetnji koje se uključuju u portfelj „sigurnosti", među ostalim klimatske promjene, siromaštvo, sigurnost opskrbe vodom, energijom i hranom te tehnološke kvarove kritične infrastrukture*[67].

Na primjer, u sigurnosnoj strategiji EU-a spominju se sljedeći glavni sigurnosni problemi: širenje oružja masovnog uništenja, terorizam i organizirani kriminal, kibersigurnost, energetska sigurnost i klimatske promjene[68].

Taj prošireni pojam nacionalne sigurnosti trebao bi se upotrebljavati pažljivo i pri njegovoj bi uporabi trebalo voditi računa o kontekstu. S jedne strane moglo bi biti korisno proširiti opseg pojma „nacionalne sigurnosti" kako bi on implicitno obuhvaćao hitnost koja se obično povezuje s nacionalnom obranom i zaštitom od terorizma na druga ključna područja državnog djelovanja kao što je politika o klimatskim promjenama. To bi proširenje s druge strane moglo imati neželjene popratne učinke, budući da koncept nacionalne sigurnosti također pruža temelje za ograničavanje temeljnih prava i drugih pravnih zaštita. Ako je nekim ustavnim poretkom dopušteno ograničavanje temeljnih prava u svrhe nacionalne sigurnosti ili su iz primjene određenih pravnih ograničenja isključene aktivnosti povezane s nacionalnom sigurnošću, u tom slučaju široka i neselektivna primjena proširenog

---

66 5 CFR § 1400.102 – Definicije i primjenjivost.

67 Legrand, T. „National Security and Public Policy: Exceptionalism Versus Accountability" (Nacionalna sigurnost i javna politika: iznimnost nasuprot odgovornosti). U *The Palgrave Handbook of National Security*. Ur. Michael Clarke i dr., 2022., str. 53–72.

68 Glavno tajništvo Vijeća. Europska sigurnosna strategija. Sigurna Europa u boljem svijetu. 2009.

koncepta nacionalne sigurnosti sa sobom povlači rizik od proširenja ovlasti države na ograničavanje temeljnih prava i djelovanje bez pravnih ograničenja. Kako bi se spriječila pretjerano široka primjena pojma *nacionalne* sigurnosti, taj bi pojam trebalo pažljivo razlikovati od koncepta *unutarnje* sigurnosti, pri čemu je potonja širi pojam i uključuje sprečavanje rizika kojima su izloženi građani, a posebno provedbu kaznenog prava.

Pitanje koliko bi širok trebao biti pojam nacionalne sigurnosti povezano je s „iznimnošću" koja se u tom području često pridaje djelovanju države. Tu „iznimnost" ne bi trebalo tumačiti kao mogućnost suspenzije vladavine prava (i samog prava) kako bi se zaštitila nacionalna zajednica[69], što bi bilo moguće prema autoritarnom tumačenju načela da je „sigurnost naroda vrhovni zakon"[70], već bi ga trebalo tumačiti kao mogućnost ograničavanja područja primjene određenih temeljnih prava u minimalnoj mjeri koja je potrebna kako bi se demokratska zajednica zaštitila od ozbiljnih rizika (pri čemu ta zaštita uključuje održavanje njezinih demokratskih institucija i prava njezinih građana) i kako bi se to postiglo unutar pravnog okvira.

Međutim, istina je da aktivnosti povezane s nacionalnom sigurnošću zahtijevaju posebnu pozornost čak i u demokratskom ustavnom poretku, jer ograničenja i kontrole koje se primjenjuju u drugim područjima možda neće biti prikladne za ovo područje s obzirom na moguću potrebu za tajnim i pravovremenim intervencijama za suzbijanje određenih ozbiljnih rizika (kao što su teroristički napadi)[71]. Stoga je potrebno donijeti posebne mjere kako bi se spriječilo neopravdano ograničavanje prava pojedinaca i demokratskih načela i kako tajne službe ne bi postale „država u državi" koja je izuzeta od svih pravnih ograničenja: veći naglasak na preciznom pravnom okviru, *ex ante* odobravanje i *ex post* kontrola koje vrše neovisna tijela, djelotvorni standardi kojima se zahtijeva da sva upletanja budu utemeljena na dokazima ozbiljnih prijetnji, *ex post* obavijesti predmetnim pojedincima i pristup pravnim lijekovima te usklađenost s načelima ljudskih prava.

5.2. Nacionalna sigurnost kao stvarno ili navodno opravdanje

Često se tvrdi da su prijetnje nacionalnoj sigurnosti postale složenije, nepredvidive i alarmantne, zbog čega je opravdano poduzimati ekstremne mjere kako bi se one suzbile. Međutim, tvrdnja da je trenutačna razina opasnosti „nezapamćena" mogla bi biti pretjerana, budući da su događaji koji mogu odnijeti velik broj ljudskih života (na primjer, pandemija kuge, od koje je prema nekim procjenama umrlo pola europskog stanovništva) bili prisutni u svim povijesnim razdobljima. Neke su prijetnje nesumnjivo postale sofisticiranije (npr. teroristički napadi), ali su sofisticiranija postala i sredstva kojima se možemo boriti protiv tih prijetnji i povećati otpornost društava.

Čak i ako zanemarimo pretjerane pozive na uzbunu, i dalje je istina da potreba da se zaštiti nacionalna sigurnost može poslužiti kao opravdanje za mjere koje uključuju ozbiljna ograničenja temeljnih prava građana, pod uvjetom da su te mjere proporcionalne i nužne za zaštitu demokratskog društva. Vidjet ćemo da to prepoznaju i Europski sud za ljudska prava i Sud Europske unije (vidjeti poglavlja 6.2. i 7.2.).

---

[69] Primjer je pristup koji je razvio njemački pravnik Carl Schmitt, čiji je rad doprinio legitimiziranju fašističkih vlada: Schmitt, C. *Political Theology* (Politička teologija). MIT, 1985. [1922.].

[70] Taj moto dolazi od latinskog *salus populi suprema lex* i potječe iz Ciceronova djela *O zakonima* (*De Legibus*), knjiga III., dio III., pododjeljak VIII.

[71] Vidjeti: Auriel, P., Beaud, O., i Wellman, C. *The Rule of Crisis: Terrorism, Emergency Legislation and the Rule of Law*. (Pravilo krize: terorizam, izvanredno zakonodavstvo i vladavina prava). Springer, 2018.

Prema Agenciji Europske unije za temeljna prava, značenje pojma nacionalne sigurnosti široko je i nije jasno razgraničeno[72]:

> *[U] sudskoj praksi Europskog suda za ljudska prava u području nacionalne sigurnosti [...] potonja seže dalje od zaštite teritorijalne cjelovitosti neke države i zaštite njezinih demokratskih institucija te obuhvaća i ozbiljne prijetnje javnoj sigurnosti, uključujući kibernapade na kritičnu infrastrukturu.*

Međutim, ne bi se trebalo smatrati da se pod tim podrazumijeva da države mogu proglasiti bilo koje inicijative pitanjima nacionalne sigurnosti kako bi te inicijative pravno i moralno opravdale. Uistinu, postoje čvrsti dokazi iz različitih zemalja, uključujući neke države članice EU-a, koji upućuju na to da se špijunski softver često zloupotrebljava i služi potpuno drugačijim svrhama pod izlikom da je nužan za nacionalnu sigurnost.

Vijeće UN- a za ljudska prava prepoznalo je da su mnoge države iskoristile ovlasti za suzbijanje terorizma kao ciničan pravni izgovor za ograničavanje slobode izražavanja, davanje legitimiteta mučenju i drugim oblicima zlostavljanja te zastrašivanje manjina, aktivista i političke opozicije. Konkretnije, posebni izvjestitelj UN-a izjavio je sljedeće o pozivanjima na nacionalnu sigurnost kako bi se dao legitimitet kršenju ljudskih prava:

> *Mnoge su države donijele zakone u kojima se uopćeno pozivaju na nacionalnu sigurnost, nacionalni interes ili javni red kao sveobuhvatne kategorije koje često obuhvaćaju bilo koje djelo koje se kriminalizira isključivo iz subjektivne perspektive njegovog mogućeg utjecaja, uključujući djela koja „utječu na nacionalnu sigurnost i političku i društvenu stabilnost" i koja su „opasna za politički, gospodarski ili društveni sustav". Takvim zakonima, čiji je glavni cilj kriminalizirati legitimna izražavanja mišljenja, bit će obuhvaćene mnoge djelatnosti organizacija civilnog društva, boraca za ljudska prava, novinara, blogera ili političkih protivnika.* [73]

Čak se i u izvješću Agencije za nacionalnu sigurnost SAD-a (NSA) koje je izradila Obamina administracija[74] navodi da se nikad ne bi smjelo pozivati na nacionalnu sigurnost kao opravdanje za određena zadiranja u prava pojedinaca i društvene vrijednosti:

> *Neke zaštitne mjere uopće ne podliježu uravnoteženju. U slobodnom društvu javni službenici nikad ne bi trebali provoditi nadzor kako bi kaznili svoje političke neprijatelje; kako bi ograničili slobodu govora ili vjeroispovijesti; kako bi suzbili legitimne kritike i protivljenje; kako bi pomogli poduzećima ili industrijama koje podržavaju; kako bi domaćim poduzećima osigurali nepravednu konkurentsku prednost; kako bi pogodovali članovima neke skupine definirane na temelju vjere, etničke pripadnosti, rase i roda ili kako bi ih opteretili.*

Povjerenik Europske unije za pravosuđe Didier Reynders snažno je osudio zlouporabu pozivanja na nacionalnu sigurnost. U svojem govoru u Europskom parlamentu u rujnu 2021. „snažno je osudio" navodne pokušaje službi nacionalne sigurnosti da nezakonito pribave podatke o političkim

---

[72] Agencija EU-a za temeljna prava. „Surveillance by intelligence services: *Fundamental rights safeguards and remedies in the EU" (Nadzor koji provode obavještajne službe: mjere zaštite temeljnih prava i pravni lijekovi u EU-u). Svezak II.: „Field perspectives and legal update" (Perspektive s terena i pravne novosti).* Ured za publikacije Europske unije, 2017.

[73] Izvješće posebnog izvjestitelja za promicanje i zaštitu ljudskih prava i temeljnih sloboda u borbi protiv terorizma (2019.). *Utjecaj mjera za suzbijanje terorizma i nasilnog ekstremizma na prostor za građansko djelovanje i prava aktera civilnog društva i boraca za ljudska prava.* Predstavljeno na 40. sjednici Vijeća za ljudska prava.

[74] Clarke, R. A. i dr. *„The NSA Report, Liberty and Security in a Changing World" (NSA-ovo izvješće, Sloboda i sigurnost u svijetu koji se mijenja).* Princeton University Press, 2014.

protivnicima iz njihovih telefona. Naveo je da „svaku naznaku da je zaista došlo do takvog narušavanja privatnosti treba temeljito istražiti i sve odgovorne za moguću povredu privesti pravdi".[75]

Već spomenuti Pegasus Project, međunarodna inicijativa istraživačkog novinarstva[76], predstavio je opširne dokaze o uporabi Pegasusa protiv pojedinaca kao što su politički protivnici, aktivisti za ljudska prava, odvjetnici i novinari, koji nisu ni na koji način povezani s teškim kaznenim djelima i ne predstavljaju nikakve prijetnje nacionalnoj sigurnosti. Kao što je već spomenuto, dokazi o napadima Pegasusom pronađeni su na telefonima više od 300 osoba, među kojima je 100 političkih aktivista, odvjetnika i novinara (vidjeti Slika 9..)[77]. Mnoge takve operacije u kojima je upotrijebljen špijunski softver vjerojatno su pretežno ili isključivo motivirane nezakonitim ciljevima kao što je ometanje zakonitog djelovanja žrtava i podvrgavanje žrtava ucjenama, napadima i sankcijama[78]. Takve operacije (i mjere kojima su one odobrene) nezakonite su prema pravu o temeljnim/ljudskim pravima, budući da se ne može dokazati njihova povezanost s interesom kojim bi se moglo opravdati ograničavanje predmetnih prava. Istina je da pravo na privatni život i pravo na slobodu izražavanja mogu podlijegati zakonitim ograničenjima u interesu nacionalne sigurnosti, ali to bi trebao biti slučaj samo kad su te mjere ograničavanja uistinu usmjerene na nacionalnu sigurnost. Kad zaštita nacionalne sigurnosti služi samo kao izgovor, jasno je da su ograničenja koja su navodno njome motivirana i dalje nezakonita[79].

Slika 9.: Tko su mete Pegasusa[80]

[75] Boffey, D. „EU Commissioner calls for urgent action against Pegasus spyware" (Povjerenik EU-a poziva na hitno djelovanje protiv špijunskog softvera Pegasus). U*The Guardian* (15. rujna 2021.).

[76] Forbidden stories, https://forbiddenstories.org/.

[77] Forbidden stories. https://forbiddenstories.org/pegasus-project-impacts-map/ (pristupljeno 11. prosinca 2022.).

[78] Forbidden stories. https://forbiddenstories.org/pegasus-journalists-under-surveillance/.

[79] O slobodi izražavanja vidjeti: Odbor za ljudska prava. Opća napomena br. 34. o čl. 19.: sloboda mišljenja i izražavanja. Ujedinjeni narodi. CCPR/C/GC/34, 2011., odlomci 29-32.

[80] BBC News, 22. srpnja 2021., https://www.bbc.com/news/world-57891506.

6. PEGASUS I MEĐUNARODNO PRAVO U PODRUČJU LJUDSKIH PRAVA

KLJUČNI ZAKLJUČCI

U okviru UN-a aktivnosti nadzora procjenjuju se na temelju sporazuma o ljudskim pravima kao što je Međunarodni pakt o građanskim i političkim pravima. Zlouporabom nadzora utječe se na prava na privatnost, ali i na slobodu izražavanja i druga prava utvrđena u tom paktu. Privatnost i slobodu izražavanja moguće je ograničiti isključivo u okviru zakona i u mjeri u kojoj je to potrebno za navedene svrhe. Ograničenje se može opravdati nacionalnom sigurnošću, no zahtjevi zakonitosti i nužnosti vjerojatno nisu ispunjeni u slučaju Pegasusa.

Na ciljani nadzor primjenjuje se i okvir Europske konvencije o ljudskim pravima, konkretno u okviru njezinih zahtjeva za legitimnošću, zakonitošću, nužnošću i proporcionalnošću u kontekstu demokratskog društva. Širokom sudskom praksom Europskog suda za ljudska prava utvrđeni su uvjeti za sukladnost tajnog nadzora s ljudskim pravima, posebno s obzirom na zakonitost (pristupačnost zakona kojima se odobrava nadzor i predvidljivost njihovih posljedica) te obavješćivanje. Sud je osim toga priznao aktivnu procesnu legitimaciju pojedincima koji su samo potencijalno pogođeni tajnim nadzorom.

U ovom poglavlju ispitujemo u kojoj mjeri špijunski softver poput Pegasusa može biti usklađen s međunarodnim pravom u području ljudskih prava. Najprije ćemo razmotriti okvir UN-a, a zatim prijeći na Europsku konvenciju o ljudskim pravima.

6.1. Okvir UN-a

U okviru UN-a aktivnosti nadzora procjenjuju se s obzirom na Opću deklaraciju o ljudskim pravima i relevantne sporazume o ljudskim pravima kao što je Međunarodni pakt o građanskim i političkim pravima, koji su ratificirale sve države članice.

Najširа zaštita od zlouporabe nadzora zajamčena je pravom na zaštitu od zadiranja u „privatnost, obitelj, dom ili dopisivanje" i napada na „čast i ugled" (članak 17. Pakta). Prikupljanjem podataka s pojedinačnog uređaja, slanjem tih podataka na druge uređaje i njihovom daljnjom obradom bez pristanka dotičnog pojedinca na te operacije ili čak bez njegova znanja zadire se u to pravo. To se pravo također krši uporabom prikupljenih podataka i mogućom manipulacijom tim podacima s ciljem narušavanja ugleda pojedinaca na koje je nadzor usmjeren.

Ističu se i druga prava i načela kao što je sloboda mišljenja i izražavanja, uključujući slobodu „mišljenja" i „traženja, primanja i širenja informacija i ideja" (članak 19.). Sloboda izražavanja krši se kad pojedinci sumnjaju da bi mogli biti podvrgnuti nadzoru ili su svjesni da bi mu mogli biti podvrgnuti te posljedično smatraju da se moraju suzdržati od izražavanja svojih mišljenja (na primjer, uporabe svojih uređaja za komunikaciju) ili traženja informacija (na primjer, pristupanja sadržaju na internetu).

U pitanje se dovodi i pravo na pravičan sudski postupak (članak 14.). Ono se dovodi u pitanje svaki put kad dotični pojedinci nisu propisno obaviješteni da su predmet mjera nadzora ili nemaju mogućnost pristupa nadležnom sudu ili sredstvima za djelotvorno rješavanje njihovih pritužbi. Slično tomu, nadzor može utjecati na pretpostavku nedužnosti ako su pojedinci na koje je nadzor usmjeren nepravedno

optuženi na temelju pristranih, obmanjujućih ili manipuliranih informacija prikupljenih o njima ili čak na temelju lažnih dokaza podmetnutih na njihove uređaje. U slučaju napada na političke aktiviste i kandidate, što je često bio slučaj s uporabom Pegasusa, prijetnja utječe i na pravo „sudjelovanja u vođenju javnih poslova, izravno ili posredstvom slobodno izabranih predstavnika" i pravo pojedinca „da bira i bude biran na izborima" (članak 25.).

Špijunski softver može utjecati i na druga prava utvrđena Konvencijom, poput jamstava mirnog okupljanja (članak 21.) i udruživanja (članak 22.) te obveza nediskriminacije (članak 2. stavak 1., članak 4. stavak 1. i članak 26.). Štetnim aktivnostima potaknutim informacijama koje su prikupljene primjenom špijunskog softvera mogu se kršiti i druge zaštite poput prava na život (članak 6.), zabrane mučenja (članak 7.), slobode od samovoljnog uhićenja (članak 9.) te prava na slobodu kretanja (članak 12.) i prava na pravičan sudski postupak (članak 14.).

Zakonitost ograničavanja prava sadržanih u Općoj deklaraciji razmatra se u članku 29., u kojem stoji:

> *svatko može biti podvrgnut samo onim ograničenjima koja su utvrđena zakonom, isključivo radi osiguranja potrebnog priznanja i poštovanja prava i sloboda drugih te radi ispunjenja pravednih zahtjeva morala, javnog reda i općeg blagostanja u demokratskom društvu.*

Konkretniji uvjeti pod kojima građanska i politička prava mogu biti ograničena navedeni su u Paktu. Posebno se sloboda izražavanja može povrgnuti isključivo ograničenjima koja su *predviđena zakonom i koja su prijeko potrebna* radi „poštovanja prava i ugleda drugih" ili „zaštite državne sigurnosti, javnog reda (*ordre public*), zdravlja ili morala" (članak 19.). Ista ideja izražava se u odnosu na prava okupljanja i udruživanja (članci 21. i 22.), u kojima se navodi da ograničenja moraju biti prijeko potrebna u *demokratskom društvu*.

I Odbor za ljudska prava i Opća skupština potvrdili su da je potrebno zajamčiti zaštitu ljudskih prava u kontekstu nadzora koji provodi država. Odbor za ljudska prava[81] napomenuo je da pravo na privatnost zahtijeva uspostavu snažnih i neovisnih sustava nadzora u vezi s nadzorom, presretanjem i hakiranjem[82]. Opća skupština[83] primijetila je da nadzor digitalnih komunikacija mora biti usklađen s međunarodnim pravom te je navela da bi „pri svakom zadiranju u pravo na privatnost u obzir trebalo uzeti njegovu zakonitost, nužnost i proporcionalnost".

Posebni izvjestitelji Ujedinjenih naroda opetovano su naglašavali potrebu za temeljitom ocjenom zadiranja nadzora u temeljna prava. Izvjestitelj o promicanju i zaštiti prava na slobodu mišljenja i izražavanja naglasio je da bi nadzor, uključujući nadzor koji se provodi u svrhu nacionalne sigurnosti, trebao biti ograničen i omeđen pravnim jamstvima:

> *Nadzor komunikacija trebao bi se smatrati vrlo narušavajućim činom koji potencijalno zadire u prava na slobodu izražavanja i privatnost te ugrožava temelje demokratskog društva. Zakonodavstvom se mora utvrditi da se nadzor koji država provodi nad komunikacijama smije obavljati samo u najiznimnijim okolnostima te isključivo pod nadzorom neovisnog pravosudnog tijela. Zakonom se moraju propisati zaštitne mjere povezane s prirodom, područjem primjene i trajanjem mogućih mjera, razlozima potrebnim za izdavanje naloga za te mjere, tijelima*

[81] Odbor za ljudska prava. Opća napomena br. 34. o članku 19.

[82] Ujedinjeni narodi. Izvješće posebnog izvjestitelja o pravu na privatnost, Joseph A. Cannataci. A/HRC/34/60, 2017.

[83] Ujedinjeni narodi, Opća skupština. „The right to privacy in the digital age: resolution" (Pravo na privatnost u digitalnom dobu: rezolucija). Ujedinjeni narodi. A/RES/73/179, 2019.

nadležnim za odobravanje, provođenje i nadziranje tih mjera te vrstom pravnog lijeka predviđenog nacionalnim pravom[84].

Nadalje, „pojedinci bi trebali imati pravo da budu obaviješteni o tome da su podvrgnuti nadzoru komunikacija" i trebali bi „imati mogućnost traženja pravne zaštite u pogledu uporabe mjera nadzora komunikacija nakon njihova provođenja".

Izvjestitelj o promicanju i zaštiti prava na slobodu mišljenja i izražavanja[85] primijetio je da se pri aktivnostima nadzora, posebno ometanju računala i hakiranju mobilnih uređaja, moraju poštovati načela zakonitosti (koje zahtijeva da aktivnost bude odobrena na temelju dovoljno preciznih i nedvosmislenih pravnih pravila), nužnosti (trebala bi se upotrijebiti najmanje ograničavajuća sredstva za ostvarenje željene svrhe), proporcionalnosti (nedostaci za prava pojedinaca ili šteta nanesena tim pravima ne bi trebali nadilaziti prednosti za nacionalnu sigurnost) te legitimnosti (namjera ograničenja mora biti da se postignu ciljevi za koje je to ograničenje dopušteno, a to je u našem slučaju nacionalna sigurnost). Ovaj posljednji kriterij znači da se nacionalna sigurnost, ako se njome žele opravdati ograničavanja privatnosti i slobode, mora pravilno tumačiti, to jest mora se tumačiti tako da se odnosi isključivo na „situacije u kojima je ugrožen interes cijele nacije", na primjer kad je u pitanju politička neovisnost i teritorijalna cjelovitost države. Stoga se zahtjevom legitimnosti isključuje mogućnost pozivanja na nacionalnu sigurnost kako bi se opravdala ograničenja „u isključivom interesu neke vlade, nekog režima ili interesne skupine".

Izvjestiteljeve zaključne preporuke uključuju sljedeće[86]:

- Države bi odmah trebale uvesti moratorij na izvoz, prodaju, prijenos, uporabu ili servisiranje alata za nadzor koje su razvila privatna poduzeća dok se ne uspostavi sustav kojim će se zajamčiti njihova sukladnost s mjerama za zaštitu ljudskih prava.
- Države koje nabavljaju tehnologije za nadzor ili se njima služe trebale bi zajamčiti da se nacionalnim zakonima njihova uporaba dopušta isključivo u skladu sa standardima ljudskih prava te bi trebale uvesti mehanizme pravne zaštite.

Prijedlog o moratoriju na špijunski softver dosad je prihvatila jedino Kostarika.

G. Kaye, posebni izvjestitelj UN-a o slobodi mišljenja i izražavanja u razdoblju 2014. – 2022., ponovio je te zaključke u svjedočenju pred Europskim parlamentom. U svom je svjedočenju naveo da uporaba Pegasusa ne zadovoljava uvjete koji su potrebni za zakonito ograničavanje ljudskih prava (posebno u skladu s člancima 17. i 19. Konvencije), budući da Pegasus omogućuje neselektivan pristup podacima na uređaju i njegovim funkcijama snimanja, zbog čega je nemoguće zajamčiti da se prikupljaju samo podaci koji su potrebni za legitimni interes[87].

G. Kaye također je primijetio da se ne bi trebalo pozivati na imunitet država kako bi se zaštitilo države i njihove službenike od odgovornosti za uporabu špijunskog softvera izvan njihovih nacionalnih područja:

---

[84] Ujedinjeni narodi. Izvješće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, Frank La Rue. A/HRC/23/40, 2013.

[85] Ujedinjeni narodi. Izvješće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, David Kaye. A/HRC/41/35, 2019.

[86] Ujedinjeni narodi. Izvješće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, David Kaye, odlomak 66.

[87] Kaye, David. *„The impact of spyware on fundamental rights" (Utjecaj špijunskog softvera na temeljna prava)*. Svjedočenje pred odborom PEGA u Europskom parlamentu, 27. listopada 2022.

> *Strani suvereni i službeni imunitet ne bi se trebali primjenjivati za zaštitu državnih ili nedržavnih aktera koji su odgovorni za prekogranične uporabu špijunskog softvera protiv pojedinaca. To je djelomično zato što države imaju obvezu poduzeti pozitivne korake kako bi zaštitile ostvarivanje prava pojedinaca i pravnih lijekova.*[31]

6.2. Okvir Europske konvencije o ljudskim pravima

Europski sud za ljudska prava utvrdio je da se tajnim nadzorom zadire u „privatni život", ali ponekad i u „dom" i „dopisivanje", zbog čega se postavlja pitanje temeljem članka 8. Konvencije[88].

Takvo zadiranje može biti opravdano samo ako su zadovoljeni uvjeti navedeni u članku 8. stavku 2., tj. ako je zadiranje

> *usklađeno s pravom i potrebno u demokratskom društvu u interesu nacionalne sigurnosti, javne sigurnosti ili gospodarske dobrobiti države, za sprečavanje nereda ili zločina, za zaštitu zdravlja ili morala ili za zaštitu prava i sloboda drugih […].*

U skladu s time, tajna uporaba špijunskog softvera u kontekstu operacija nacionalne sigurnosti prihvatljiva je samo ako je djelotvorno usmjerena na ostvarivanje ciljeva u području nacionalne sigurnosti, čime se ispunjava standard *legitimnosti*, te ako ispunjava standarde *zakonitosti* i *nužnosti u demokratskom društvu*.

Što se tiče pitanja je li neka mjera zaista usmjerena na ostvarivanje ciljeva u području nacionalne sigurnosti, Sud je priznao da države članice imaju prostor za tumačenje pri određivanju kojim se ciljevima doprinosi nacionalnoj sigurnosti i koji su načini najprikladniji za ostvarivanje tih ciljeva. Međutim, korištenje tim prostorom za tumačenje podliježe nadzoru[89]. S obzirom na to da možda nema potrebna sredstva za osporavanje presude nacionalnih sudova u takvim predmetima, Sud zahtjeva da se u slučaju ograničavanja nekog ljudskog prava na temelju bilo kakve navodne prijetnje nacionalnoj sigurnosti ovlasti neovisna nacionalna tijela da u okviru nekog oblika spora provjere je li ta prijetnja u razumnoj mjeri činjenično utemeljena[90].

U pogledu standarda zakonitosti, Sud je naveo da mjera nadzora „mora imati neku osnovu u nacionalnom pravu i u pogledu kvalitete prava o kojem je riječ mora biti dostupna dotičnoj osobi i imati predvidive posljedice"[91]. U njoj mora biti „naveden opseg svake takve diskrecijske ovlasti koja se dodjeljuje nadležnim tijelima i način njezina izvršenja i to dovoljno jasno da se pojedincu pruži odgovarajuća zaštita od proizvoljnog upletanja".[92] Sud je nadalje razvio skup minimalnih zahtjeva kojima zakon mora udovoljavati kako bi se izbjegle zlouporabe ovlasti: „priroda kaznenih djela koja mogu dovesti do naloga za presretanje; definicija kategorija osoba podložnih prisluškivanju telefona; ograničenje trajanja prisluškivanja telefona; postupak koji je potrebno poštovati pri pregledavanju, uporabi i pohranjivanju pribavljenih podataka; mjere opreza koje treba poduzeti pri priopćavanju podataka drugim stranama; i okolnosti u kojima se snimke mogu ili moraju izbrisati ili uništiti"[93].

---

88 Europski sud za ljudska prava. *Vodič kroz sudsku praksu Europskog suda za ljudska prava. Zaštita podataka*. Council of Europe Publishing, 2022.

89 Handyside protiv Ujedinjene Kraljevine, gore citirano, odlomak 49.

90 Janowiec i ostali protiv Rusije [GC] (br. 55508/07 i 29520/09, 21. listopada 2013.).

91 Kennedy protiv Ujedinjene Kraljevine (br. 26839/05, 18. svibnja 2010.).

92 Kennedy protiv Ujedinjene Kraljevine, odlomak 230.

93 Kennedy protiv Ujedinjene Kraljevine, odlomak 231.

Zahtjev nužnosti u demokratskom društvu možda neće biti ispunjen u slučaju neke mjere ako (a) su se mogle donijeti manje ograničavajuće mjere, možda na način da se poduzmu dodatne mjere opreza i uvedu kontrole ili (b) je zadiranje u prava dotičnog pojedinca toliko ozbiljno da nadilazi bilo koju korist koja se tom mjerom mogla ostvariti u području nacionalne sigurnosti.

Sud navodi da „pojam nužnosti podrazumijeva da zadiranje odgovara nekoj hitnoj društvenoj potrebi i posebno da je proporcionalno legitimnom cilju koji se nastoji ostvariti". Stoga, iako nacionalna tijela imaju određeni prostor za tumačenje u pitanjima nacionalne sigurnosti, „mora se postići ravnoteža između interesa tužene države u području zaštite nacionalne sigurnosti i ozbiljnosti zadiranja u pravo tužitelja na poštovanje njegovog privatnog života". [94] U slučajevima nakon toga Sud je smatrao da bi se tajni nadzor trebao tolerirati isključivo kada je „izričito neophodan". [95]

Važan pomak u sudskoj praksi Europskog suda za ljudska prava odnosi se na uvjete pod kojima neka osoba ima aktivnu procesnu legitimaciju pred Sudom kako bi se njezin predmet mogao ispitati. Iako dotični pojedinci obično moraju dostaviti dokaze o izravnom utjecaju na njihova prava, Europski sud za ljudska prava smatrao je da se status žrtve može priznati i da se posljedično može dodijeliti aktivna procesna legitimacija čak i ako ti pojedinci ne mogu dokazati da su mjere tajnog nadzora primijenjene izravno na njih. Dovoljno je dostaviti dokaze o tome da se trenutačno provode mjere tajnog nadzora ili da postoji zakonodavstvo kojim se takve mjere dopuštaju te da djelotvorni nacionalni pravni lijekovi nisu dostupni.

> *Sud prihvaća da tužitelj može tvrditi da je žrtva povrede uzrokovane samim postojanjem mjera tajnog zakonodavstva ili zakonodavstvom kojim se dopuštaju mjere tajnog nadzora ako su zadovoljeni sljedeći uvjeti. Kao prvo, Sud će uzeti u obzir područje primjene zakonodavstva kojim se dopuštaju mjere tajnog nadzora na način da će ispitati je li moguće da su one utjecale na tužitelja zato što on pripada skupini osoba na koje je sporno zakonodavstvo usmjereno ili zato što to zakonodavstvo izravno utječe na sve korisnike komunikacijskih usluga uspostavljajući sustav u kojem je moguće presretanje komunikacija bilo koje osobe. Kao drugo, Sud će uzeti u obzir dostupnost pravnih lijekova na nacionalnoj razini i prilagoditi stupanj nadzora ovisno o djelotvornosti tih pravnih lijekova*[96].

Kako bi se osigurao pristup djelotvornim pravnim lijekovima, Europski sud za ljudska prava uveo je strogi zahtjev obavješćivanja: pojedinci na koje je usmjerena neka mjera tajnog nadzora moraju biti obaviješteni o toj mjeri „čim se to obavješćivanje može izvršiti bez ugrožavanja svrhe ograničenja nakon prekida mjere nadzora"[97]. Pravovremeno obavješćivanje „neodvojivo je povezano s djelotvornošću pravnih lijekova pred sudovima i stoga s postojanjem djelotvornih mjera zaštite od zlouporabe ovlasti za praćenje"[98].

Konačno, Europski sud za ljudska prava razmatrao je povezanost nadzora i slobode izražavanja s obzirom na novinarstvo. Sud je u različitim predmetima sankcionirao pristup povjerljivom novinarskom materijalu u sustavima za masovno presretanje[99]. U tim predmetima naglašava se da je od ključne važnost zaštititi novinarstvo u okviru Konvencije rješavanjem pitanja masovnog nadzora, a ne ciljanog nadzora koji se vrši primjenom špijunskog softvera. Međutim, Sud je u nekim drugim predmetima stavio naglasak na pojedinačni nadzor koji se provodi na način sličan onome koji omogućuje Pegasus,

---

94 Leander protiv Švedske (br. 9248/81, serija A, 26. ožujka 1987.), odlomak 59.

95 Malone protiv Ujedinjene Kraljevine (br. 8691/79, serija A, 2. kolovoza 1984.).

96 Roman Zakharov protiv Rusije (br. 47143/06, § 171), ESLJP 2015.

97 Roman Zakharov protiv Rusije, odlomak 287.

98 Roman Zakharov protiv Rusije, odlomak 234.

99 Big Brother Watch i ostali protiv Ujedinjene Kraljevine (br. 58170/13 i još dva), §§ 447.–50., 25. svibnja 2021.

iako u jednostavnijem tehnološkom okruženju. Na primjer, Sud je jednoglasno smatrao da je Azerbajdžan prekršio pravo na privatnost i slobodu izražavanja u predmetu u kojem je jedna novinarka bila podvrgnuta tajnom nadzoru: u njezinoj su kući postavljene žice i skrivene kamere, u njezinoj spavaćoj sobi snimani su intimni videozapisi u kojima se ona pojavljivala koji su zatim raspačavani na internetu, poslano joj je prijeteće pismo i osjetljivi osobni podaci o njoj otkriveni su u jednom izvješću o istrazi; sve su te mjere navodno provođene u okviru kampanje zastrašivanja[100]. Treba napomenuti kako za utvrđivanje odgovornosti Azerbajdžana nije bilo potrebno dokazati da su službenici države izravno sudjelovali u nadzoru ili ga organizirali, budući da je Sud smatrao da je Azerbajdžan prekršio svoju pozitivnu obvezu u skladu s člankom 10. da zaštiti slobodu izražavanja dotične novinarke.

Europski sud za ljudska prava trenutačno ispituje neke druge predmete koji su povezani s nadzorom. Pred Vijećem je 27. rujna 2022. održano saslušanje u predmetu koji su podnijeli jedan odvjetnik i četvero aktivista za ljudska prava u vezi s tužbenim zahtjevom temeljenim na članku 8. Konvencije (pravo na privatni život)[101]. Tužitelji su naveli da je poljskim pravom dopušteno policiji i obavještajnim službama da prate njihove telekomunikacije i digitalne komunikacije bez njihova znanja. Osim toga, tvrdili su da im u okviru poljskog prava nisu dostupni djelotvorni pravni lijekovi, budući da te službe nisu bile obvezne obavijestiti dotične pojedince o mjerama nadzora kojima su izloženi. Stoga te mjere nije bilo moguće podvrgnuti preispitivanju pred sudom.

[100] Khadija Ismayilova protiv Azerbajdžana (br. 65286/13 i 57270/14, 10. siječnja 2019.)

[101] Pietrzak protiv Poljske i Bychawska-Siniarska i drugi protiv Poljske (br. 72038/17 i 25237/18).

7. PEGASUS I PRAVO EU-A

KLJUČNI ZAKLJUČCI

U kontekstu prava EU-a, ciljani nadzor relevantan je za prava utvrđena u Povelji Europske unije o temeljnim pravima, načela utvrđena u Ugovorima (poput demokracije i vladavine prava) i razne instrumente sekundarnog prava EU-a, poput onih koji se odnose na zakonodavstvo o zaštiti podataka.

Prema Ugovoru o Europskoj uniji, nacionalna sigurnost isključiva je odgovornost svake države članice. Time se u načelu ne isključuje primjena prava EU-a na aktivnosti u području nacionalne sigurnosti kada one zadiru u aktivnosti regulirane pravom EU-a.

Međutim, primjena prava EU-a na uporabu špijunskog softvera u svrhe nacionalne sigurnosti otežana je zbog činjenice da su aktivnosti nacionalne sigurnosti isključene iz područja primjene dvaju temeljnih instrumenata, Opće uredbe o zaštiti podataka i Direktive o e-privatnosti. To ograničenje zaštite ispitanika u odnosu na aktivnost države teško se može opravdati s obzirom na prava sadržana u Povelji i načela sadržana u Ugovorima. Budući da se to izuzeće može preširoko upotrebljavati, potrebno je istaknuti da se ono odnosi isključivo na slučajeve u kojima je špijunski softver zaista konstruiran za zaštitu nacionalne sigurnosti, pri čemu se taj pojam ispravno tumači.

Pravo EU-a primjenjuje se na uporabu tajnih istraga u svrhe kaznenog progona, koje podliježu Direktivi o kaznenom progonu. Međutim, čak i u tom području postoje dokazi o nacionalnim praksama koje čine zlouporabu.

U ovom poglavlju razmotrit ćemo odnos između mjera usmjerenih na nacionalnu sigurnost koje donose države članice i prava EU-a, s naglaskom na zaštiti podataka.

7.1. Špijunski softver i nacionalna sigurnost u Ugovorima EU-a

Uporaba špijunskog softvera za postizanje ciljeva u području nacionalne sigurnosti predmet je koji je obuhvaćen područjem primjene brojnih odredaba prava EU-a sadržanih u Ugovorima i u Povelji. To je zbog toga što, kao što smo maloprije napomenuli, sama mogućnost podvrgavanja sveobuhvatnom promatranju (i posljedične izloženosti štetnim mjerama) isključuje autonomno djelovanje u individualnoj, kulturnoj i političkoj sferi.

Nadzor zadire u čitav niz prava i načela. Već je bilo riječi o Paktu UN-a o građanskim i političkim pravima i o Europskoj konvenciji o ljudskim pravima kao standardima na temelju kojih se to zadiranje može ocjenjivati. Međutim, važnim standardom može se smatrati i Povelja koja, kao što smo upravo nagovijestili, sadržava sljedeća relevantna prava i načela:

- načelo dostojanstva (članak 1.)
- pravo na slobodu i sigurnost (članak 6.)
- prava na privatni život i zaštitu podataka (članci 7. i 8.)
- slobodu mišljenja, savjesti i vjeroispovijesti (članak 10.)

- slobodu izražavanja i informiranja, uključujući slobodu medija (posebno u slučajevima u kojima su na meti novinari) (članak 11.)
- slobodu okupljanja i udruživanja (članak 12.), uključujući slobodu učlanjenja u političke stranke (članak 12. stavak 2.)
- slobodu umjetnosti i znanstvenog istraživanja i akademsku sloboda (članak 13.)
- pravo na vlasništvo (članak 17.), posebno ako nadzor uključuje pristup vlasništvu pojedinca, kao što je to slučaj s Pegasusom
- pravo na nediskriminaciju (članak 21.), u slučajevima kad su nadzor ili posljedične radnje izričito usmjereni protiv pojedinaca koji pripadaju određenim skupinama utvrđenim, na primjer, na temelju njihovih političkih stajališta
- pravo na kolektivno djelovanje (članak 28.), u slučajevima kad su na meti radnici i njihove organizacije
- pravo kandidiranja na europskim i lokalnim izborima (članci 39. i 40.), u slučajevima kad su na meti pojedinci koji obnašaju političke funkcije ili teže tome da ih obnašaju, čime se utječe na sudjelovanje u izborima ili pravednost izbornog procesa
- pravo na djelotvoran pravni lijek i na pošteno suđenje (članak 47.), u slučajevima kad pojedinac koji je na meti nema na raspolaganju djelotvoran pravni lijek protiv nezakonitog nadzora
- pretpostavku nedužnosti (članak 48.), u slučajevima kad se prikupljeni podaci upotrebljavaju za iznošenje lažnih optužbi i kad se kontrola nad uređajima upotrebljava za lažiranje dokaza.

Za našu analizu relevantne su i dvije opće odredbe Povelje. Prema članku 51., primjena Povelje ograničena je na provedbu prava Unije:

> *Odredbe ove Povelje odnose se na* […] *države članice samo kada provode pravo Unije.*

Prema članku 52. stavku 1., svako ograničenje pri ostvarivanju prava i sloboda priznatih Poveljom mora zadovoljavati načela zakonitosti i proporcionalnosti (uključujući potrebu ostvarivanja ciljeva od općeg interesa). Stoga svako takvo ograničenje mora (*i.*) biti predviđeno zakonom, (*ii.*) doprinositi nekom cilju od općeg interesa ili zaštiti prava i sloboda drugih, (*iii.*) biti potrebno za taj cilj i (*iv.*) biti uravnoteženo (pri nastojanjima usmjerenim na ostvarivanje cilja nadzora šteta koja nastaje od nepoželjnog zadiranja u ta prava i slobode ne smije nadilaziti koristi):

> *Svako ograničenje pri ostvarivanju prava i sloboda priznatih ovom Poveljom mora biti predviđeno zakonom i mora poštovati bit tih prava i sloboda. Podložno načelu proporcionalnosti, ograničenja su moguća samo ako su potrebna i ako zaista odgovaraju ciljevima od općeg interesa koje priznaje Unija ili potrebi zaštite prava i sloboda drugih osoba.*

Konačno, prema članku 52. stavku 3. pretpostavlja se da prava sadržana u Povelji u pogledu značenja i područja primjene odgovaraju odgovarajućim pravima iz Europske konvencije o ljudskim pravima, što znači da je prethodna analiza izrađena u odnosu na Konvenciju značajna i za Povelju.

Osim što zadire u prava pojedinaca, sveobuhvatni nadzor zadire i u temeljne vrijednosti demokracije i vladavine prava, budući da se povredom prava pojedinaca izravno utječe na provedbu tih vrijednosti (vidjeti poglavlje 4.), koje su nabrojane u članku 2. pročišćene verzije Ugovora o Europskoj uniji (UEU):

> *Unija se temelji na vrijednostima poštovanja ljudskog dostojanstva, slobode, demokracije, jednakosti, vladavine prava i poštovanja ljudskih prava.*

Nezakonitim nadzorom kojim se zadire u politički angažman pojedinaca – posebno pojedinaca koji obnašaju neku javnu dužnost ili su zainteresirani za njezino obnašanje – narušava se načelo predstavničke demokracije koje je u članku 10. stavku 1. UEU-a utvrđeno kao temelj funkcioniranja Unije:

> *Funkcioniranje Unije temelji se na predstavničkoj demokraciji.*

Pitanje nacionalne sigurnosti konkretno se razmatra u članku 4. UEU-a:

> *Unija poštuje temeljne državne funkcije* [*država članica*]*, uključujući osiguranje teritorijalne cjelovitosti države, očuvanje javnog poretka i zaštitu nacionalne sigurnosti. Nacionalna sigurnost posebice ostaje isključiva odgovornost svake države članice.*

EU je stoga obvezan poštovati nacionalnu sigurnost kao temeljnu državnu funkciju koja ostaje isključiva odgovornost svake države članice. Posljedica te odredbe jest da se pojavljuje moguća napetost između ovlasti neke države da samostalno provodi aktivnosti u području nacionalne sigurnosti (koja je utvrđena u članku 4.) s jedne strane i potrebe zaštite temeljnih prava i vrijednosti EU-a s druge strane u slučaju da na njih štetno utječu aktivnosti država prividno usmjerene na zaštitu nacionalne sigurnosti.

Općenito pitanje koje je potrebno razmotriti jest proizlazi li iz činjenice da neka nadležnost ili ovlast nije prenesena na EU da neka država može slobodno postupati u izvršavanju te nadležnosti čak i ako se njezinim ponašanjem krše norme, prava i načela EU-a. Drugim riječima, moramo postaviti pitanje podrazumijeva li činjenica da se mjera neke države provodi u okviru nadležnosti koja nije prenesena na EU (ovlast koja nije rezervirana za EU) da se pravo EU-a ne primjenjuje na tu mjeru. Možemo razlikovati državne nadležnosti koje još nisu prenesene na EU (zadržane nadležnosti) i nadležnosti koje su Ugovorom izričito rezervirane za države članice (rezervirane nadležnosti), poput nacionalne sigurnosti[102].

Činjenica da neka nadležnost još nije prenesena na neku državu članicu svakako ne podrazumijeva da su djela izvršena tijekom izvršavanja te nadležnosti izuzeta iz područja primjene prava EU-a. To je načelo potvrdio Sud Europske unije u cijelom nizu predmeta, na primjer u predmetu *Schwarz*, koji se odnosio na oporezivanje obrazovnih djelatnosti. Sud je naveo da:

> *iako je izravno oporezivanje u nadležnosti država članica, one ipak moraju izvršavati tu nadležnost u skladu s pravom Zajednice* [...] *posebno odredbom o slobodi pružanja usluga*[103].

Slična analiza primjenjuje se i na aktivnosti koje se odnose na nadležnosti rezervirane za države članice, poput nacionalne sigurnosti. Ocjena dopuštenosti mjera u području nacionalne sigurnosti temeljem prava EU-a nije namijenjena tome da se dotičnim državama članicama nameću određeni načini za postizanje njihovih svrha nacionalne sigurnosti (budući da bi to značilo povredu rezerviranih kompetencija država), već tome da se utvrdi jesu li takve mjere u skladu s načelima, pravima i pravilima prava EU-a unutar područja uređenih pravom EU-a. Kad se takvim mjerama zadire u temeljna prava,

---

[102] Na temelju De Witte, B. „Exclusive Member State Competences: Is There Such a Thing?" (Isključive kompetencije država članica – postoje li uopće) U *„The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*" (Podjela nadležnosti između EU-a i država članica: razmatranja o prošlosti, sadašnjosti i budućnosti). Hart, 2017., str. 59–73.

[103] Presuda od 11. rujna 2007. u predmetu *Schwarz i Gootjes*, C-76/05, ECLI:EU:C:2007:492, odlomak 69.

potrebna je ocjena zakonitosti i proporcionalnosti koju u konačnici provodi Sud Europske unije kako bi se to utvrdilo.

Međutim, tom se ocjenom podrazumijeva da do zadiranja dolazi u okviru područja primjene prava EU-a, budući da se i Povelja primjenjuje „na države članice samo kada provode pravo Unije" (članak 51.).

Međutim, zaključak da određena aktivnost države (ili aktivnost koju provodi neka privatna strana na zahtjev države) može poslužiti kao opravdanje za ograničavanje temeljnih prava EU-a ili čak može biti izuzeta iz određenih pravnih instrumenata EU-a jer se odnosi na nacionalnu sigurnost podrazumijeva da je predmetna aktivnost svrstana u aktivnosti koje se odnose na nacionalnu sigurnost. Smatramo da se to prethodno pitanje koje se odnosi na kvalifikaciju prirode državnih aktivnosti nužno odnosi na pravo EU-a te je stoga u nadležnosti Suda Europske unije. Pojam nacionalne sigurnosti u pravu EU-a, iako se njime prihvaćaju različite nacionalne ocjene koje se odnose na pitanje koje ozbiljne prijetnje najviše ugrožavaju nacionalnu zajednicu, nikako ne može uključivati aktivnosti usmjerene protiv političkih protivnika ili manjina.

7.2. Sud Europske unije o temeljnim pravima, zaštiti podataka i nacionalnoj sigurnosti

Sud Europske unije ispitivao je vezu između temeljnih prava i nacionalne sigurnosti u nekim važnim predmetima.

Među njima ćemo spomenuti samo predmete *Schrems I* i *Schrems II*[104], u kojima je Sud proglasio ništavnim sporazum o sigurnoj luci odnosno kasniji sustav zaštite privatnosti (za prijenos osobnih podataka iz EU-a u SAD). Ključna osnova za te presude bila je činjenica da bi podatke prenesene u SAD obrađivale agencije SAD-a za nacionalnu sigurnost bez ograničenja i pravnih lijekova koji postoje u EU-u (čime bi se kršilo pravo na zaštitu podataka i pravo na djelotvoran pravni lijek). Sud je u predmetu *Schrems II* utvrdio da regulacija nadzora u svrhe nacionalne sigurnosti u SAD-u ne ispunjava

> *minimalne zahtjeve koji su u pravu Unije povezani s načelom proporcionalnosti, tako da nije moguće utvrditi da su nadzorni programi koji se temelje na tim odredbama ograničeni na ono što je strogo nužno*[105].

Sud je o pravu na djelotvoran pravni lijek naveo da

> *propis koji pojedincima ne pruža nikakvu mogućnost korištenja pravnim sredstvima radi pristupa osobnim podacima koji se na njih odnose, ili radi ispravka ili brisanja takvih podataka, ne poštuje bitan sadržaj temeljnog prava na djelotvornu sudsku zaštitu* [...][106].

U predmetu *Quadrature du Net*[107] iz 2020. Sud Europske unije razmatrao je francuski zakon kojim se od pružatelja komunikacijskih usluga zahtijeva zadržavanje podataka o prometu. Naveo je da se zakonodavne odredbe slične spornoj odredbi, to jest odredbe u kojima je „preventivno predviđeno

---

[104] Presuda od 6. listopada 2015., Maximillian Schrems protiv povjerenika za zaštitu podataka, C-362/14, ECLI:EU:C:2015:650 (Schrems I), te presuda od 16. srpnja 2020., povjerenik za zaštitu podataka protiv Facebook Ireland Limited i Maximilliana Schremsa, C-311/18, ECLI:EU:C:2020:559 (Schrems II).

[105] *Schrems II*, odlomak 184.

[106] *Schrems II*, odlomak 187.

[107] Presuda od 6. listopada 2020., *La Quadrature du Net i ostali protiv predsjednika Vlade i ostalih*, spojeni predmeti C-511/18, C-512/18 i C-520/18, ECLI:EU:C:2020:791.

opće i neselektivno zadržavanje podataka o prometu i lokaciji"[108], protive članku 15. Direktive o e-privatnosti, tumačenom u skladu s Poveljom. Međutim, Sud je priznao da se u svrhu suzbijanja ozbiljnih prijetnji nacionalnoj sigurnosti od pružatelja usluga elektroničkih komunikacija može zahtijevati „opće i neselektivno zadržavanje podataka o prometu i lokaciji"[109] pod uvjetom da je njegovo trajanje određeno i da podliježe odgovarajućim zaštitnim mjerama. Također je priznao da se od pružatelja može zahtijevati provođenje automatskih analiza podataka o prometu i lokaciji u svrhu suzbijanja ozbiljnih i stvarnih prijetnji nacionalnoj sigurnosti. Nadalje, čak i prikupljanje tehničkih podataka o lokaciji terminalne opreme u stvarnom vremenu može biti opravdano u odnosu na pojedince koje se sumnjiči za bavljenje terorizmom, ali podliježe prethodnom neovisnom preispitivanju.

U spojenim predmetima *SpaceNet* i *Telekom Deutschland*[110] iz 2022. Sud Europske unije potvrdio je da se opće i neselektivno zadržavanje podataka o prometu i lokaciji na preventivnoj osnovi protivi pravu EU-a. Međutim, takvo opće i neselektivno zadržavanje dopustivo je na ograničeno vrijeme u slučaju ozbiljne prijetnje nacionalnoj sigurnosti pod uvjetom da se poduzmu odgovarajuće zaštitne mjere. Nadalje, ciljano zadržavanje podataka o prometu i lokaciji u odnosu na dotične kategorije osoba ili primjenom geografskog kriterija dopustivo je na ograničeno vrijeme u svrhu borbe protiv teških kaznenih djela i zaštite javne sigurnosti.

Sud je stoga podržao pravni okvir kojim se u skladu s načelima zakonitosti i proporcionalnosti priznaje da su znatna ograničenja temeljnih prava i normi zaštite podataka dopustiva u svrhu nacionalne sigurnosti te u manjoj mjeri u svrhu borbe protiv teških kaznenih djela i zaštite javne sigurnosti.

7.3. Nacionalna sigurnost i zaštita podataka u pravu EU-a

Kao što smo napomenuli u poglavlju 5.1., odredbe Povelje „odnose se na države članice samo kada primjenjuju pravo Unije" (članak 51.). Stoga moramo razmotriti u kojoj mjeri su aktivnosti nacionalne sigurnosti obuhvaćene pravom EU-a kako bismo utvrdili u kojoj se mjeri Povelja na njih primjenjuje. Ako su takve aktivnosti izuzete iz određenih odredbi prava EU-a, ne postoji zaštita koja se može pružiti u vezi s njihovim tumačenjem i njihovom primjenom temeljem takvih odredbi ili temeljem Povelje.

To izuzeće može imati neke paradoksalne posljedice. Na primjer, ako su aktivnosti nacionalne sigurnosti u cijelosti izuzete iz područja primjene prava o zaštiti podataka, odluke Suda Europske unije u predmetima *Schrems I* i *II* činile bi se upitnima: temeljile bi se na standardima poput „minimalnih zaštitnih mjera proizašlih iz načela proporcionalnosti temeljem EU-prava" koje sam Sud Europske unije ne primjenjuje unutar EU-a. Sud je u tim odlukama zapravo proglasio ništavnima sustave za prenošenje podataka iz EU-a u SAD jer pravom SAD-a nije predviđena zaštita usporediva sa zaštitom predviđenom pravom EU-a u pogledu obrade osobnih podataka u svrhu nacionalne sigurnosti. Ako se pravo o zaštiti podataka ne primjenjuje na aktivnosti nacionalne sigurnosti, čini se da razlika između pravnih okvira SAD-a i EU-a u odnosu na regulaciju tih aktivnosti u velikoj mjeri nestaje.

Predstavljajući nacrt izvješća o Pegasusu, zastupnica u Europskom parlamentu Sophie in 't Veld istaknula je kako se može činiti da se EU vodi dvostrukim standardom kad je riječ o digitalnim prijetnjama demokraciji: Komisija je odlučna boriti se protiv napada na demokraciju koji dolaze izvana,

[108] Quadrature du Net, odlomak 168.

[109] Ibid.

[110] Presuda od 20. rujna 2022., *Bundesrepublik Deutschland* protiv *SpaceNet AG* (C-793/19) i *Telekom Deutschland GmbH* (C-794/19), ECLI:EU:C:2022:702.

ali kad prijetnja demokraciji potječe od vlada država članica, odjednom smatra da obrana europske demokracije više nije europsko pitanje, već je u nadležnosti država članica[111].

Kako bismo ocijenili u kojoj je mjeri pravo o zaštiti podataka primjenjivo na aktivnosti u području nacionalne sigurnosti, moramo uzeti u obzir da Opća direktiva o zaštiti podataka i Direktiva o e-privatnosti sadržavaju dvije vrste odredbi koje su relevantne za obradu osobnih podataka u svrhu nacionalne sigurnosti:

- odredbe o izuzećima, prema kojima aktivnosti nacionalne sigurnosti nisu uključene u područje primjene takvih instrumenata; odnosno
- odredbe o ograničavanju, prema kojima su ograničenja istih instrumenata u svrhu nacionalne sigurnosti dopustiva, ali samo pod uvjetom da ispunjavaju zahtjeve zakonitosti i proporcionalnosti.

Odredbe o ograničavanju područja primjene

Prema članku 2. stavku 2. Opće uredbe o zaštiti podataka, ona

> *se ne primjenjuje na obradu osobnih podataka u okviru aktivnosti koja nije u području primjene zakonodavstva Unije.*

U uvodnoj izjavi 16. izričito se navodi da je u aktivnosti „koje nisu u području primjene prava Unije" uključena nacionalna sigurnost:

> *Ova se Uredba ne primjenjuje na pitanja zaštite temeljnih prava i sloboda ili slobodnog protoka osobnih podataka u vezi s djelatnostima koje ne ulaze u područje primjene prava Unije, kao što su djelatnosti u vezi s nacionalnom sigurnošću.*

Slično tomu, u članku 1. stavku 3. Direktive o e-privatnosti navodi se da se ona

> *u svakom slučaju* [ne primjenjuje] *na aktivnosti koje se odnose na* […] *državnu sigurnost (uključujući gospodarsku dobrobit države* […]*).*

Odredbe o ograničavanju

Prema članku 23. Opće uredbe o zaštiti podataka

> *Na temelju prava Unije ili prava države članice kojem podliježu voditelj obrade podataka ili izvršitelj obrade zakonskom mjerom može se ograničiti opseg obveza i prava iz članaka od 12. do 22. i članka 34. te članka 5. ako te odredbe odgovaraju pravima i obvezama predviđenima u člancima od 12. do 22., ako se takvim ograničenjem poštuje bit temeljnih prava i sloboda te ono predstavlja nužnu i razmjernu mjeru u demokratskom društvu za zaštitu* [. . .] *nacionalne sigurnosti* [. . .].

Slično tomu, u članku 15. Direktive o e-privatnosti navodi se da:

> *Države članice mogu donijeti zakonske mjere kojima će ograničiti opseg prava i obveza koji pružaju članak 5., članak 6., članak 8. stavci 1., 2., 3. i 4., te članak 9. ove Direktive kada takvo ograničenje predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva s ciljem zaštite nacionalne sigurnosti (odnosno državne sigurnosti).*

Može se činiti da te odredbe o izuzeću i ograničavanju nije moguće uskladiti: ako aktivnosti nacionalne sigurnosti nisu uključene u područje primjene Opće uredbe o zaštiti podataka i Direktive o e-

[111] Vidjeti Rankin, Jennifer. „Dutch MEP says illegal spyware 'a grave threat to democracy'" (Nizozemska europarlamentarka tvrdi da je nezakonit špijunski softver „ozbiljna prijetnja demokraciji"). U *The Guardian* (8. studenoga 2022.).

privatnosti, nema previše smisla utvrđivati pod kojim se uvjetima prava i obveze utvrđene tim instrumentima mogu ograničavati u svrhu nacionalne sigurnosti.

Međutim, usklađenje se može postići razlikovanjem svrhe određenih aktivnosti obrade podataka i svrhe nametnutih ograničenja prava i obveza koje se odnose na takve aktivnosti. Svrha predmetnih aktivnosti obrade podataka, a ne svrha ograničenja, određuje hoće li te aktivnosti biti uključene u područje primjene prava o zaštiti podataka. Primjerice, zahtjevi za zadržavanje podataka koji se nameću pružateljima usluga u svrhu nacionalne sigurnosti odnose se na aktivnosti obrade čija je svrha pružanje komunikacijskih usluga, a te aktivnosti ulaze u područje primjene Direktive o e-privatnosti. Stoga se takvi zahtjevi moraju ocjenjivati prema kriterijima utvrđenim u članku 15. navedene direktive.

To je pristup koji je utvrdio Sud Europske unije[112] i u odnosu na kazneni progon[113] i u odnosu na nacionalnu sigurnost[114]. Prema Sudu, Direktiva o e-privatnosti mora se primjenjivati na mjere koje se nameću pružateljima usluga u svrhe kaznenog progona i nacionalne sigurnosti jer je člankom 15. stavkom 1. Direktive izričito regulirana zakonitost mjera kojima se ograničavaju prava ispitanika u takve svrhe:

> *Člankom 15. stavkom 1. Direktive 2002/58 nužno se pretpostavlja da nacionalne zakonodavne mjere na koje se u tom članku upućuje ulaze u područje primjene navedene direktive, budući da se njome izričito ovlašćuje države članice da ih donesu samo ako su ispunjeni uvjeti utvrđeni direktivom[115].*

Zakonodavstvo kojim se pružateljima usluga nameću mjere zadržavanja podataka, iako je usmjereno na svrhe koje se odnose na kazneni progon ili nacionalnu sigurnost, ipak se odnosi na pružanje usluga elektroničkih komunikacija. Potonja aktivnost podliježe Direktivi o e-privatnosti, koja regulira

> *sve operacije obrade osobnih podataka koje provode pružatelji usluga elektroničkih komunikacija [...], uključujući operacije obrade koje proizlaze iz obveza koje tim pružateljima nameću javna tijela[116]*

Upravo izneseni argumenti protiv isključivanja određenih mjera nacionalne sigurnosti iz područja primjene zakona o zaštiti podataka ne primjenjuju se na aktivnosti pri kojima špijunski softver upotrebljavaju državni službenici ili privatni ugovaratelji koje su oni imenovali pod uvjetom da te aktivnosti uistinu služe svrhama povezanim s nacionalnom sigurnošću. Međutim, mogu se primjenjivati na slučajeve kad se pružateljima komunikacijskih usluga nalaže da surađuju s tijelima država članica na instalaciji i uporabi špijunskog softvera, čime se zadire u usluge koje ti pružatelji pružaju svojim klijentima.

Važna odredba o zaštiti pružatelja medijskih usluga i novinara uključena je u prijedlog Akta o medijskim uslugama, a posebno u njegov članak 4. stavak 2. podstavak (c), „Prava pružatelja medijskih usluga". Prema toj odredbi, države članice ne smiju

> *ugrađivati špijunski softver u uređaj ili stroj koji upotrebljavaju pružatelji medijskih usluga ili, ako je primjenjivo, članovi njihovih obitelji ili njihovi zaposlenici ili članovi njihovih obitelji, osim ako*

---

[112] Vidjeti Buchta, A. i Kranenborg, H. „Institutional report topic 2: The new EU data protection regime" (Institucijsko izvješće o temi 2.: novi mehanizam EU-a za zaštitu podataka). U *„The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection" (Novi mehanizam EU-a za zaštitu podataka: utvrđivanje globalnih standarda prava na zaštitu osobnih podataka). XXIX. kongres FIDE-a u Haagu.* Eleven, 2020.,str. 79–105.

[113] Presuda Suda od 21. prosinca 2016., predmeti C-203/15 i C-698/15, Tele2/Watson.

[114] Presuda od 6. listopada 2020., C-511/18, C-512/18 i C-520/18, La Quadrature du Net i drugi.

[115] Ibid., odlomak 95.

[116] Ibid., odlomak 101.

je to opravdano, u tom pojedinačnom slučaju, radi zaštite nacionalne sigurnosti i u skladu je s člankom 52. stavkom 1. Povelje i drugim zakonodavstvom Unije.

Tom se odredbom zahtjeva ocjenjivanje svake uporabe špijunskog softvera u te svrhe na temelju proporcionalnosti u skladu s člankom 52. Povelje. Time se također jamči da se primjenjuje Europska konvencija o ljudskim pravima kako je navedena u Povelji.

7.4. Uporaba špijunskog softvera u svrhu kaznenog progona

Iako su aktivnosti nacionalne sigurnosti izuzete iz područja primjene ključnih instrumenata prava EU-a o zaštiti podataka, to nije slučaj s aktivnostima kaznenog progona[117]. Potonje potpadaju pod Direktivu o kaznenom progonu[118], kojom se u skladu s člankom 1. stavkom 1. uređuje

obrada osobnih podataka koju obavljaju nadležna tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje.

Takva je obrada zakonita samo (članak 8.)

ako je nužna i samo u onoj mjeri u kojoj je nužna kako bi nadležno tijelo obavilo zadaću u svrhe navedene u članku 1. stavku 1. te da se temelji na pravu Unije ili pravu države članice.

Nadalje, pri predmetnoj obradi moraju biti zadovoljena načela zaštite podataka (zakonitost, pravednost, smanjenje količine podataka, točnost, sigurnost itd.) navedena u članku 4.

Tajne istrage nisu isključene iz područja primjene navedene direktive. Međutim, prema uvodnoj izjavi 26. takve se istrage mogu provesti isključivo

pod uvjetom da su utvrđene zakonom i predstavljaju nužnu i razmjernu mjeru u demokratskom društvu uz dužno poštovanje legitimnih interesa dotičnog pojedinca.

Stoga se Povelja i uvjeti za ograničavanje temeljnih prava koji se u njoj utvrđuju u potpunosti primjenjuju na takve istrage i na mjere kojima se one odobravaju, kao što je navedeno u uvodnoj izjavi 46:

Svako ograničavanje prava ispitanika mora biti u skladu s Poveljom i Europskom konvencijom o zaštiti ljudskih prava, kako se tumače u sudskoj praksi Suda odnosno Europskog suda za ljudska prava, te se njime posebno mora poštovati bit tih prava i sloboda.

Pri utvrđivanju je li uporaba Pegasusa usklađena s Direktivom i Poveljom moramo razmotriti jesu li ispunjeni svi zahtjevi iz Direktive i iz Povelje.

---

[117] O hakiranju uređaja u kontekstu kaznenog progona vidjeti: Gutheil, M., Liger, Q., Heetman, A., Eager, J., i Crawford, M. *„Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices" (Pravni okviri za hakiranje koje provode tijela kaznenog progona: utvrđivanje, ocjenjivanje i usporedba praksi).* Studija koju je naručio odbor LIBE. Europski parlament, 2017.

[118] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.).

Dopustivost uporabe Pegasusa i sličnih sustava za hakiranje uređaja u svrhe kaznenog progona mora se razmatrati u svakom pojedinačnom slučaju, uzimajući u obzir više čimbenika: ozbiljnost kaznenog djela ili sigurnosnog rizika koji se istražuje ili sprečava, ograničenja pod kojima se upotrebljavaju funkcionalnosti sustava te primjenjivo nacionalno pravo. Međutim, čini se da Pegasus vjerojatno ne bi ispunio zahtjev nužnosti niti temeljem Direktive niti temeljem Povelje dokle god postoje alternative kojima se svrhe kaznenog progona ostvaruju na manje narušavajuće i sigurnije načine[119].

Provedba načela zakonitosti u nacionalnom pravu također se mora pažljivo ispitati kako bi se utvrdila zakonitost tajnih istraga. Na primjer, Venecijanska komisija je u svojem Mišljenju o izmjenama poljskog Zakona o policiji iz 2016.[120] zaključila da

> *postupovne zaštitne mjere i materijalni uvjeti utvrđeni u Zakonu o policiji za provedbu tajnog nadzora još su uvijek nedovoljni da bi se spriječila njegova prekomjerna uporaba i neopravdano zadiranje u privatnost pojedinaca.*

Nadalje, primijećeno je da su poljskim zakonom iz područja primjene Direktive o kaznenom progonu izričito izuzete aktivnosti poljskog Središnjeg antikorupcijskog ureda, čija se aktivnost barem djelomično odnosi na kazneni progon [121] i koji stoga ulazi u područje primjene Direktive o kaznenom progonu[122]. Posljedično se može tvrditi da to izuzeće predstavlja nepravilno prenošenje odredaba Direktive o kaznenom progonu u poljsko pravo i da je stoga u suprotnosti s pravom EU-a.

Općenitije, na pitanje odnosi li se neka aktivnost na kazneni progon kako bi se utvrdilo je li ona obuhvaćena područjem primjene Direktive mora se odgovoriti na temelju prava EU-a (članak 1. Direktive). Stoga, ako je u nacionalnom pravu neka aktivnost koja se prema članku 1. odnosi na kazneni progon klasificirana kao aktivnost koja se odnosi na nacionalnu sigurnost, prva se klasifikacija ne bi trebala primjenjivati u svrhu primjene Direktive kako bi ta aktivnost i dalje bila podložna pravilima kojima se uređuje kazneni progon prema (prenesenoj) Direktivi.

---

[119] O Pegasusu i kaznenom progonu vidjeti Vogiatzoglou, P., Marquenie, T., i Valke, P. *„Assessment of the Implementation of the Law Enforcement Directive" (Procjena provedbe Direktive o provedbi zakona). Studija koju je naručio odbor LIBE*. Europski parlament, 2022.

[120] Mišljenje o izmjenama Zakona o Ustavnom sudu Poljske od 25. lipnja 2015. koje je Venecijanska komisija donijela na 106. plenarnom zasjedanju (Venecija, 11. – 12. ožujka 2016). Venecijanska komisija, službeno Europska komisija za demokraciju putem prava, savjetodavno je tijelo Vijeća Europe sastavljeno od neovisnih stručnjaka u području ustavnog prava.

[121] Litwiński P. *Opinia prawna w sprawie naruszeń, w związku z ujawnionymi przypadkami użycia oprogramowania szpiegującego Pegasus w świetle prawa ochrony danych osobowych, przepisów Karty Praw Podstawowych UE i Konstytucji RP*, Kancelaria Senatu, Varšava 2022., https://www.senat.gov.pl/gfx/senat/pl/senateksper tyzy/6283/plik/oe-390.pdf

[122] Litwiński P. *Opinia prawna w sprawie naruszeń*.

8. DALJNJI KORACI

KLJUČNI ZAKLJUČCI

Uporaba špijunskog softvera prijetnja je temeljnim pravima i osnovnim načelima prava EU-a poput (predstavničko-deliberativne) demokracije i vladavine prava. Zbog toga postoji rizik od potkopavanja samih načela na kojima se temelji pravni sustav EU-a.

Aktivnosti u području nacionalne sigurnosti u međunarodnom i europskom pravnom sustavu mogu poslužiti kao opravdanje za ograničavanja temeljnih prava, ali ta ograničenja moraju zadovoljavati uvjete *legitimnosti, zakonitosti, nužnosti, uravnoteženja* i *usklađenosti s demokracijom* kako bi bila zakonita.

Pegasus dosad nije zadovoljio te uvjete u mnogim dosadašnjim slučajevima njegove uporabe, s obzirom na to da se upotrebljavao za nelegitimne svrhe, bez odgovarajućeg pravnog okvira i bez prave nužnosti, pri čemu je prouzročena nerazmjerna šteta pravima pojedinaca i demokraciji.

Predlažemo različite ideje koje bi mogle pomoći u sprečavanju zlouporaba:

- Ograničavanje materijalnog područja primjene aktivnosti povezanih s nacionalnom sigurnošću kako bi državama bilo teže pozivati se na nacionalnu sigurnost kao lažno pravno obrazloženje za aktivnosti usmjerene u druge svrhe.
- Ograničavanje osobnog područja primjene aktivnosti povezanih s nacionalnom sigurnošću na način da se iz njega isključe određene aktivnosti koje provode privatni subjekti.
- Uključivanje aktivnosti povezanih s nacionalnom sigurnošću u područje primjene prava o zaštiti podataka kako bi ograničenja prava ispitanika u svrhe nacionalne sigurnosti podlijegala zahtjevima zakonitosti i proporcionalnosti.
- Pružanje potpore donošenju odgovarajućih pravnih okvira na nacionalnoj razini, budući da je nacionalna sigurnost i dalje rezervirana nadležnost država članica i one moraju na djelotvoran način uskladiti svoje aktivnosti s temeljnim pravima i načelima prava EU-a. Ti bi okviri trebali biti usklađeni s načelima poput sljedećih: zakonitost, legitimna svrha, nužnost, proporcionalnost, nadležno tijelo, pravičan sudski postupak, obavještavanje korisnika, transparentnost, javni nadzor, sigurnost i certificiranje te tehnička prilagodljivost.

Politički izvediv moratorij na uporabu alata za hakiranje uređaja mogao bi se sastojati od snažne pretpostavke protiv zakonitosti njihove uporabe, temeljene na opsežnim dokazima o njihovim zlouporabama. Ta bi se pretpostavka mogla nadići isključivo kad neka država uvjerljivo pokaže spremnost i kapacitet za sprečavanje svih zlouporaba.

Nadalje, države članice trebalo bi potaknuti da zabrane uporabu konkretnih alata špijunskog softvera za koje, kao što je to slučaj s Pegasusom, postoje snažni dokazi o njihovoj uporabi u nezakonitim aktivnostima, posebno na području EU-a. Sve dok ne postoje jasni dokazi da se takve neprihvatljive prakse više ne provode, nastavak uporabe Pegasusa, čak i u okviru zakonitih aktivnosti, podrazumijeva pružanje potpore njegovim proizvođačima i razvojnim inženjerima te kao takav implicira političko (iako ne i pravno) sudioništvo u takvim praksama.

Ustvrdili smo da je uporaba špijunskog softvera prijetnja temeljnim pravima i osnovnim načelima prava EU-a poput (predstavničko-deliberativne) demokracije i vladavine prava. Zbog toga postoji rizik od

potkopavanja samih načela na kojima se temelji pravni sustav EU-a. U ovom ćemo poglavlju dati sažetak uvjeta za zakonitu uporabu špijunskog softvera i primijeniti ih na slučaj Pegasusa.

8.1. Zakonita ograničenja temeljnih prava u svrhe nacionalne sigurnosti

Aktivnosti u području nacionalne sigurnosti u međunarodnom i europskom pravnom sustavu mogu poslužiti kao opravdanje za ograničavanja temeljnih prava, ali ta ograničenja moraju zadovoljavati sve sljedeće uvjete kako bi bila zakonita:

- *Legitimnost*. Predmetne aktivnosti moraju biti usmjerene na istinske ciljeve u području nacionalne sigurnosti.
- *Zakonitost*. Moraju imati čvrstu pravnu osnovu, to jest, moraju postojati zakoni na kojima se one temelje i ti zakoni moraju biti dovoljno jasno i precizno sročeni.
- *Nužnost*. Ne smije postojati nikakav bolji način za postizanje istih ciljeva u području nacionalne sigurnost, to jest, sva ostala sredstva moraju biti takva da se njima više krše prava (i dovoditi do više zadiranja u prava) ili manje djelotvorna (što znači da se njima ne bi ostvarili ciljevi nacionalne sigurnosti u jednakoj ili većoj mjeri).
- *Uravnoteženje*. Negativni utjecaji na zahvaćena prava i vrijednosti ne smiju nadilaziti važnost postizanja ciljeva u području nacionalne sigurnosti.
- *Usklađenost s demokracijom*. Rad na ostvarenju ciljeva u području nacionalne sigurnosti trebao bi doprinositi zaštiti demokratskih društvenih uređenja, a ne bi trebao ugrožavati demokratske procese.

Potreba za ispunjavanjem takvih standarda u aktivnostima povezanim s nacionalnom sigurnošću može se iščitati iz UN-ovih izvora, Europske konvencije o ljudskim pravima, europskih Ugovora i Povelje, čije odredbe treba tumačiti u skladu s Konvencijom.

Nije lako uskladiti uporabu Pegasusa s tim zahtjevima.

- U mnogim se slučajevima čini da se on upotrebljavao za ostvarivanje ciljeva koji se ne odnose na nacionalnu sigurnost, pod kojom se podrazumijeva zaštita društva u cjelini.
- Sveobuhvatan nadzor koji se omogućuje tim softverom nije uređen odgovarajućim pravnim okvirom.
- U većini tih slučajeva bilo bi moguće ostvariti željeni cilj manje narušavajućim sredstvima od sveobuhvatnog nadzora koji omogućuje Pegasus.
- U mnogim se slučajevima čini da utjecaj na prava pojedinaca i demokratske procese (poput izbora) nadilazi bilo kakvu korist koja se mogla ostvariti u području sigurnosti.
- U nekim se slučajevima čini da se sustav upotrebljavao na načine koji dovode do slabljenja demokratskih procesa i kod kojih postoji opasnost da bi mogli izmijeniti oblikovanje javnog mijenja i ishod izbora.

8.2. Uporaba špijunskog softvera u okviru prava EU-a

U ovom poglavlju iznijet ćemo neka konkretna razmatranja o tome kako se uporaba špijunskog softvera može uskladiti s načelima prava EU-a. Uzet ćemo u obzir činjenicu da su, kao što smo već naveli (vidjeti poglavlje 7.3.), aktivnosti u području nacionalne sigurnosti izuzete iz ključnih odredbi prava o zaštiti podataka kao što je Opća uredba o zaštiti podataka i Direktiva o e-privatnosti. Ako se neka operacija obrade smatra aktivnošću u području nacionalne sigurnosti, ispitanici su lišeni zaštita koje proizlaze iz tih odredbi (iako se i dalje mogu pozvati na druge norme prava EU-a).

Ograničavanje materijalnog područja primjene aktivnosti nacionalne sigurnosti

Kad se koncept nacionalne sigurnosti upotrebljava za izuzeće primjene prava EU-a, potrebno je ograničiti njegovo područje primjene i svesti njegovu primjenu na prijetnje koje se zaista odnose na političku zajednicu u cjelini. Potreba da se taj koncept ograniči na takav način proizlazi upravo iz njegove primjene kako bi se ograničilo područje primjene prava EU-a, posebno instrumenata za zaštitu podataka. U tom kontekstu on se mora tumačiti u skladu s pravom EU-a i pritom se moraju uzeti u obzir namjere zakonodavaca EU-a i ustavni okvir EU-a.

Vidjeli smo da Europski sud za ljudska prava priznaje širok prostor za tumačenje državama članicama pri utvrđivanju ciljeva u području nacionalne sigurnosti i načina na koje će se ti ciljevi ostvarivati. Agencija Europske unije za temeljna prava u nedavnoj je analizi utvrdila da je taj koncept relativno neutvrđen te da se u različitim pravnim sustavima različito tumači[123].

Međutim, iako je teško precizno utvrditi što nacionalna sigurnost obuhvaća, to nas ne bi trebalo spriječiti da jasno utvrdimo što ona nesumnjivo *ne* obuhvaća. Nacionalna sigurnost ne može uključivati aktivnosti koje imaju sljedeće namjene: (*i.*) štetno utjecati na političke protivnike; (*ii.*) utjecati na demokratske procese poput izbora ili na državne funkcije poput pravosuđa i uprave; (*iii.*) zadirati u medije; (*iv.*) ciljati aktiviste za ljudska prava; (*v.*) suzbijati kritike i protivljenje; (*vi.*) dati posebne prednosti favoriziranim poduzećima ili industrijama; ili (*vii.*) pogodovati ili naštetiti članovima skupina definiranih vjeroispovješću, političkim mišljenjima, etničkom pripadnošću, rasom ili rodom ili drugim skupinama pojedinaca koji potencijalno mogu biti predmetom diskriminacije. Ako neka država donese mjere koje su navodno usmjerene na nacionalnu sigurnost, ali se čini da su te mjere isključivo ili dodatno usmjerene na takve nezakonite, nepravedne ili antidemokratske svrhe, ta bi država morala uvjerljivo dokazati da za te mjere postoje razlozi nacionalne sigurnosti, da te mjere nemaju nikakvu drugu svrhu i da su poduzete odgovarajuće mjere opreza kako bi se ograničili bilo kakvi negativni popratni učinci. Ako ne može pružiti dokaze u tom smislu (država ne ispuni teret dokazivanja), trebali bismo zaključiti da takve mjere nisu obuhvaćene izuzećem koje se odnosi na nacionalnu sigurnost i podliježu sveobuhvatnom sudskom nadzoru u skladu s pravnim standardima primjenjivim na stvarne svrhe tih mjera.

Ograničavanje osobnog područja primjene aktivnosti nacionalne sigurnosti

U spomenutoj presudi u predmetu *Quadrature du Net*, Sud Europske unije primijenio je Direktivu o e-privatnosti na treće strane koje su obrađivale (i posebno pohranjivale) osobne podatke kako bi ispunile obvezu koja im je nametnuta u svrhu nacionalne sigurnosti. Sud je tako zauzeo stajalište da se obrada

[123] Agencija EU-a za temeljna prava. *„Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU" (Nadzor koji provode obavještajne službe: mjere zaštite temeljnih prava i pravni lijekovi u EU-u). Svezak II.: „Field perspectives and legal update" (Perspektive s terena i pravne novosti).* Ured za publikacije Europske unije, 2017.

koju provodi treća strana ne smatra aktivnošću nacionalne sigurnosti bez obzira na to što je naložena na temelju razloga povezanih s nacionalnom sigurnošću.

Kako bi se prevladao i pristup Suda Europske unije i njegova moguća proširenja, Europsko vijeće uvelo je novu odredbu u nacrt Uredbe o e-privatnosti, navevši da se ta uredba

> *ne primjenjuje na zaštitu temeljnih prava i sloboda u vezi s aktivnostima izvan područja primjene prava Unije i u svakom slučaju na mjere, aktivnosti obrade i operacije koje se odnose na nacionalnu sigurnost i obranu, bez obzira na to tko provodi te operacije i radi li se o javnom tijelu ili privatnom operateru koji djeluje na zahtjev nekog javnog tijela.*

Toj se izmjeni treba usprotiviti jer bi ona državama dala odriješene ruke da zaobiđu zahtjeve Direktive o e-privatnosti, a posebno da zaobiđu zabranu zadiranja u uređaje korisnika, poput mobilnih telefona, kako je utvrđeno u članku 5. Direktive o e-privatnosti i ponovno utvrđeno u članku 8. predložene Uredbe o e-privatnosti:

> *Zabranjuju se uporaba kapaciteta terminalne opreme za obradu i pohranu i prikupljanje informacija iz terminalne opreme krajnjih korisnika, uključujući informacije o njezinu softveru i hardveru, koje ne provodi dotični krajnji korisnik.*

Uključivanje aktivnosti nacionalne sigurnosti u područje primjene zakona o zaštiti podataka

Navedeni pristupi očigledno pružaju tek ograničenu mogućnost sudskog preispitivanja. Snažnija i sigurnija zaštita od zlouporabe špijunskog softvera mogla bi se postići kad bi se preispitale odredbe kojima se isključuje primjena Opće uredbe o zaštiti podataka i Direktive (i Uredbe) o e-privatnosti kako bi svrhe nacionalne sigurnosti mogle poslužiti kao razlog za ograničavanje odredaba o zaštiti podataka samo na temelju zakonitosti i proporcionalnosti (umjesto izravnog isključenja iz takvih instrumenata).

Čini nam se da postoje snažni argumenti za odbacivanje takvih isključenja kako bi nadzor koji se provodi u svrhe nacionalne sigurnosti bio usklađen sa zahtjevom koji je utvrdio Europski sud za ljudska prava, to jest zakonitošću, nužnošću i proporcionalnošću, uključujući dostupnost odgovarajućih pravnih lijekova. Kao što je spomenuto, takve je zahtjeve promicao i Sud Europske unije u vezi s nadzorom u Sjedinjenim Državama (u spomenutim predmetima *Schrems I* i *II*). Kad bi se izvršila takva zakonodavna promjena, uporaba softvera poput Pegasusa u većini bi se slučajeva smatrala pravno manjkavom i prema pravu EU-a.

Potpora donošenju odgovarajućih pravnih okvira na nacionalnoj razini

Budući da je nacionalna sigurnost i dalje rezervirana nadležnost država članica, one moraju na djelotvoran način uskladiti svoje aktivnosti s temeljnim pravima i načelima prava EU-a. Međutim, institucije EU-a istovremeno bi trebale poticati države članice da donesu odgovarajući okvir za uporabu špijunskog softvera u svrhe nacionalne sigurnosti[124]:

1. **Zakonitost**. Za svaku uporabu špijunskog softvera u svrhe nacionalne sigurnosti trebala bi postojati pravna osnova koja je dovoljno jasna i precizna da bi pojedinci mogli razumjeti pod kojim bi uvjetima mogli biti podvrgnuti tajnom nadzoru i u koje svrhe.
2. **Zakonita svrha**. Špijunski softver trebao bi se upotrebljavati isključivo u stvarnu svrhu nacionalne sigurnosti na način kojim se doprinosi zaštiti demokratskog društva, a ne na način kojim se ona narušava.

[124] Za neke od tih zahtjeva vidjeti: Electronic Frontier Foundation i druge nevladine organizacije (2014.). „Necessary and Proportionate: On the application of human rights to communication surveillance" (Nužno i proporcionalno: o primjeni ljudskih prava na nadzor komunikacija). https://necessaryandproportionate.org.

3. **Nužnost**. Špijunski softver trebao bi se upotrebljavati isključivo kad se cilj nacionalne sigurnosti koji se nastoji ostvariti ne može u jednakoj mjeri ostvariti bilo kojim drugim manje narušavajućim sredstvima ili na bilo koji drugi manje narušavajući način. Pod time se podrazumijeva da bi podaci kojima se pristupa ili koji se na neki drugi način zadržavaju trebali biti ograničeni na podatke koji su relevantni za prijetnju i trebala bi im pristupati isključivo ovlaštena tijela i isključivo u svrhu i u trajanju za koje je ovlaštenje dano.
4. **Primjerenost**. Svaka uporaba špijunskog softvera trebala bi biti primjerena za cilj nacionalne sigurnosti koji se nastoji ostvariti.
5. **Proporcionalnost (uravnoteženje)**. Zadiranje u prava pojedinaca i demokratske vrijednosti ne bi trebalo nadilaziti korist za nacionalnu sigurnost koja se nastoji ostvariti. U tu svrhu moramo uzeti u obzir ozbiljnost apstraktno zamislivih scenarija rizika, ali i vjerojatnost da će takvi scenariji postati stvarnost. Stoga bi, kako bi zadiranje u prava i demokraciju bilo opravdano, trebala postojati velika vjerojatnost da će se neka određena prijetnja nacionalnoj sigurnosti izvršiti i velika vjerojatnost da će podaci dobiveni primjenom špijunskog softvera biti korisni u identificiranju i suzbijanju takve prijetnje.
6. **Nadležno tijelo**. Ovlaštenja i druga utvrđivanja povezana s uporabom špijunskog softvera trebalo bi davati nepristrano i neovisno tijelo koje raspolaže odgovarajućim vještinama i resursima.
7. **Pravičan sudski postupak**. Uporaba špijunskog softvera trebala bi podlijegati preispitivanju koje vrši neovisan, nadležan i nepristran sud osnovan temeljem zakona koji raspolaže potrebnim ovlastima za pravovremeno ostvarivanje prava svih pojedinaca koji su na meti softvera i pružanje pravnih lijekova za sva kršenja.
8. **Obavještavanje korisnika**. Kad se uređaji korisnika hakiranju, pojedinci na koje je to hakiranje usmjereno i kojima ti uređaji pripadaju trebali bi biti obaviješteni što je prije moguće bez da se pritom ugrozi svrha operacije nadzora.
9. **Transparentnost**. Države bi trebale pružati odgovarajuće javno dostupne informacije o pravnom okviru kojim je uređena uporaba špijunskog softvera (uključujući zakone, propise, aktivnosti, ovlasti ili tijela) te o načinima na koje državne agencije upotrebljavaju špijunski softver. Nadalje, trebalo bi objaviti informacije o otkrivenim zlouporabama proizvoda za kibernadzor.
10. **Javni nadzor**. Države bi trebale uspostaviti neovisne mehanizme nadzora kako bi se osigurala transparentnost i odgovornost pri uporabi špijunskog softvera. Parlamenti bi trebali imati mogućnosti provođenja djelotvornih kontrola nad tajnim aktivnostima koje provodi izvršna vlast. U tijela nadzora u okviru kojih se te kontrole provode trebali bi biti uključeni predstavnici opozicije.
11. **Sigurnost i certifikacija.** Trebalo bi uspostaviti precizne tehnološke zahtjeve za špijunski softver kako bi se zajamčio integritet podataka i povjerljivost operacija, koje bi u načelu trebali provoditi samo nadležni državni službenici.
12. **Tehnička prilagodljivost.** Funkcionalnosti alata špijunskog softvera trebalo bi ograničiti na pojedinačne funkcije ili bi one trebale biti prilagodljive kako bi se prije pokretanja špijunskog softvera mogle ograničiti na ono što je potrebno i zakonito odobreno u predmetnom slučaju.

8.3. A što je s Pegasusom?

Kao što smo upravo napomenuli, države članice mogu zakonito upotrebljavati alate za hakiranje uređaja za sigurnosne svrhe ili svrhe kaznenog progona isključivo u primjerenim okolnostima. Njihova bi uporaba trebala biti strogo ograničena na ono što je potrebno za legitimnu svrhu koja se nastoji ostvariti, trebala bi biti podložna strogim i nepristranim kontrolama i u konačnici sudskom preispitivanju i trebala bi biti usklađena s tehničkim zahtjevima kojima se jamči sigurnost i djelotvornost njihova rada.

Komisija bi kao čuvarica Ugovorâ trebala aktivno sudjelovati u istrazi uporabe špijunskog softvera i pobrinuti se da se pravo EU-a poštuje i da se vrijednosti EU-a provode. Europski parlament u tom smislu treba odigrati temeljnu ulogu sudjelujući u donošenju relevantnih zakonodavnih instrumenata (kao što je predložena Uredba o e-privatnosti), provodeći vlastite istražne radnje i surađujući s nacionalnim parlamentima i vladama, medijima i javnošću. Odbor PEGA bio je zaista vrlo učinkovit u prikupljanju i obradi dokaza o uporabi Pegasusa i pružanju opsežnih javno dostupnih informacija i kritičkih perspektiva[125]. Aktivnost tog odbora uistinu je pokazala koliko je važno priznati široke istražne ovlasti Europskog parlamenta kao nužnu nadopunu njegovim zakonodavnim i političkim odgovornostima[126].

U vezi s uporabom alata za hakiranje uređaja trebalo bi poduzeti različite inicijative:

- Dosljedno primjenjivati postojeće nacionalno pravo i pravo EU-a (uključujući Ugovore, Povelju i Europsku konvenciju o ljudskim pravima) za ocjenjivanje zakonitosti postojećih praksi.
- Poticati države koje primjenjuju alate špijunskog softvera da donesu odgovarajuće organizacijske, tehnološke i pravne okvire bez kojih bi svaka uporaba softvera za hakiranje uređaja bila nezakonita i stoga bi je trebalo zaustaviti.
- Uključiti stručnjake i civilno društvo u političku, etičku i tehnološku raspravu o uporabi sustava za hakiranje uređaja, njihovim utjecajima i alternativama.

Kao što je već spomenuto, posebni izvjestitelj o promicanju i zaštiti prava na slobodu mišljenja i izražavanja predložio je moratorij na uporabu špijunskog softvera[127]. To je stajalište s kojim se u načelu možemo složiti: prema procjeni proporcionalnosti kojom se odgovara na empirijske situacije, samo postojanje široko rasprostranjenih zlouporaba u uporabi sustava za hakiranje uređaja moglo bi opravdati obustavu njihove uporabe dok se sva tehnološka, pravna ili organizacijska pitanja koja su omogućila takve zlouporabe ne riješe na zadovoljavajući način. Globalna, iako privremena, zabrana hakiranja uređaja nesumnjivo bi bila najdjelotvorniji način da se spriječe široko rasprostranjene zlouporabe kojima smo svjedočili.

Međutim, ako podržimo ideju o općem moratoriju na uporabu softvera za hakiranje uređaja – shvaćenu kao globalnu zabranu njegove uporabe dok se ne razviju mjere kojima će se spriječiti zlouporaba u cijelom svijetu – moramo uzeti u obzir činjenicu da većina država na svijetu, uključujući sve države članice EU-a, trenutačno upotrebljava špijunski softver. Hakiranje uređaja izričito se priznaje u

[125] https://www.europarl.europa.eu/committees/hr/pega/home/highlights.

[126] Moglo bi biti korisno povući paralelu s SAD-om, čiji se Vrhovni sud već odavno složio s Kongresom da je istražna ovlast toliko neophodna za zakonodavnu funkciju da se podrazumijeva iz općenitog povjeravanja zakonodavne ovlasti Kongresu. Vidjeti McGrain protiv Daughertyja, 273 U.S. 174 (1927.): „istražna ovlast i proces za njezino izvršavanje neophodna je i primjerena pomoćna funkcija zakonodavne funkcije."

[127] Ujedinjeni narodi. Izvješće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, 2014.; Kaye, David. „The impact of spyware on fundamental rights" (Utjecaj špijunskog softvera na temeljna prava).

određenim nacionalnim zakonodavstvima, na primjer talijanskom[128], te ga mnogi pripadnici policijskih i sigurnosnih snaga smatraju važnim dijelom svojeg paketa instrumenata, a s tom se prosudbom slažu i brojni političari.

Stoga umjesto preporuke svim državama članicama da se odmah i bezuvjetno odreknu svih alata za hakiranje uređaja smatramo politički izvedivijim moratorij na uporabu tih alata koji bi se sastojao od snažne pretpostavke protiv zakonitosti njihove uporabe. Ta se pretpostavka temelji na opsežnim dokazima o njihovoj nezakonitoj primjeni u mnogim zemljama i trebalo bi je ukinuti tek nakon što neka država uvjerljivo pokaže volju i kapacitet za sprečavanje svih zlouporaba dosljednom i djelotvornom provedbom svih potrebnih mjera (vidjeti poglavlja 8.1. i 8.2.) kako bi se zajamčila usklađenost s temeljnim pravima, demokracijom i vladavinom prava.

Nadalje, sve države članice trebalo bi potaknuti da zabrane uporabu konkretnih alata špijunskog softvera za koje postoje snažni dokazi da su već upotrebljavani za nezakonite aktivnosti, posebno na području EU-a. U slučaju Pegasusa možemo postaviti pitanje treba li te zlouporabe pripisati samoj prirodi Pegasusa – njegovim tehničkim značajkama kao što je njegov općenit opseg, koji ga čini maksimalno narušavajućim, te odsustvu odgovarajućih jamstava o sigurnosti i integritetu podataka koji se prikupljaju i šalju s pomoću tog softvera – ili su zlouporabe ipak posljedica komercijalnih, institucijskih, organizacijskih i političkih okvira u kojima je ta tehnologija upotrebljavana. U svakom slučaju, sam razmjer tih zlouporaba opravdava zabranu uporabe Pegasusa (uključujući kupnju, prodaju, uvoz i izvoz). Sve dok ne postoje jasni dokazi da se takve neprihvatljive prakse više ne provode, nastavak uporabe Pegasusa, čak i u okviru zakonitih aktivnosti, ekvivalentan je pružanju potpore njegovoj proizvodnji i distribuciji te stoga uključuje političko (iako ne i pravno) sudioništvo u takvim praksama.

[128] Zakonodavni ukaz od 29. prosinca 2017, br. 216., izmijenjen zakonom od 28 veljače 2020., br. 7.

IZVORI

- Amnesty International. *„Forensic Methodology Report. How to Catch NSO Group's Pegasus*" (Izvješće o forenzičkoj metodologiji. Kako uhvatiti Pegasus Grupe NSO). 2021.
  *„Lessons from the Stasi – a cautionary tale on mass surveillance (*Što smo naučili od Stasija – poučna priča o masovnom nadzoru). 2015.,
  url: https://www.amnesty.org/en/latest/news/2015/03/lessons-from-the-stasi/.
- Arendt, H. „The Crisis in Education" (Kriza u obrazovanju). *U „Between Past and Future – Six Exercises in Political Thought" (Između prošlosti i budućnosti: šest primjena političke misli).* Viking, 1961. [1954.].
- Auriel, P., Beaud, O., i Wellman, C. *„The Rule of Crisis: Terrorism, Emergency Legislation and the Rule of Law*" (Pravilo krize: terorizam, izvanredno zakonodavstvo i vladavina prava). Springer, 2018.
- Beckman, L. „Democracy" (Demokracija). U *Oxford Research Encyclopedias, Politics.* Oxford University Press, 2021.
- Benjakob, O. „As Israel Reins in Its Cyberarms Industry, an Ex-intel Officer is Building a New Empire" (Dok Izrael obuzdava svoju industriju kiberoružja, bivši obavještajac gradi novo carstvo), *Haaretz* (20. rujna 2022.).
- Boffey, D. „EU Commissioner calls for urgent action against Pegasus spyware" (Povjerenik EU-a poziva na hitno djelovanje protiv špijunskog softvera Pegasus). *The Guardian* (15. rujna 2021.).
- Buchta, A. i Kranenborg, H. „Institutional report topic 2: The new EU data protection regime" (Institucijsko izvješće o temi 2.: novi mehanizam EU-a za zaštitu podataka). U The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection" (Novi mehanizam EU-a za zaštitu podataka: utvrđivanje globalnih standarda prava na zaštitu osobnih podataka). XXIX. kongres FIDE-a u Haagu. Eleven, 2020.,str. 79–105.
- Christiano, T. i Sameer B. „Democracy" (Demokracija). U *The Stanford Encyclopedia of Philosophy*. Stanford University, 2022.
- Clarke, R. A. i dr. *„The NSA Report, Liberty and Security in a Changing World" (NSA-ovo izvješće, Sloboda i sigurnost u svijetu koji se mijenja).* Princeton University Press, 2014.
- Komisija Europskih zajednica. *Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija o akcijskom planu za europsku demokraciju.* COM(2020) 790 final, 2020.
- Vijeće Europe. *„Mass surveillance: Who is watching the watchers?" (Masovni nadzor: tko promatra promatrače?)* Council of Europe Publishing, 2016.
- De Witte, B. „Exclusive Member State Competences – Is There Such a Thing?" (Isključive kompetencije država članica – postoje li uopće). U *„The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*" (Podjela nadležnosti između EU-a i država članica: razmatranja o prošlosti, sadašnjosti i budućnosti). Hart, 2017., str. 59–73.
- Europski nadzornik za zaštitu podataka. *„Preliminary Remarks on Modern Spyware*" (Preliminarne opaske o modernom špijunskom softveru), 2022. https://edps.europa.eu/system/files/2022-02/22-02-15edpspreliminaryremarksonmodernspywareen0.pdf
- Electronic Frontier Foundation i druge nevladine organizacije. *„Necessary and Proportionate: On the application of human rights to communication surveillance"* (Nužno i proporcionalno: o primjeni ljudskih prava na nadzor komunikacija). 2014.,

url https://necessaryandproportionate.org/principles/.

- Agencija EU-a za temeljna prava. *„Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU" (Nadzor koji provode obavještajne službe: mjere zaštite temeljnih prava i pravni lijekovi u EU-u). Svezak II.: „Field perspectives and legal update*" (Perspektive s terena i pravne novosti). Ured za publikacije Europske unije, 2017.
- Europska komisija. *Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija naslovljena „Suzbijanje dezinformacija na internetu: europski pristup"*. COM(2018) 236 final, 2018.
- Europsko vijeće. *Strategija unutarnje sigurnosti Europske unije – oblikovanje europskog modela sigurnosti.* Ured za publikacije Europske unije, 2010.
- Europski sud za ljudska prava. *Vodič kroz sudsku praksu Europskog suda za ljudska prava. Zaštita podataka.* Council of Europe Publishing, 2022.
- Europski parlament. *Rezolucija o programu nadzora američke Nacionalne sigurnosne agencije (NSA), o nadzornim tijelima u različitim državama članicama i njihovom utjecaju na temeljna prava građana EU-a i o transatlantskoj suradnji u pravosuđu i unutarnjim poslovima.* 2013/2188(INI), P7-TA (2014)0230, 2014.
- Europski parlament. Istražni odbor za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor, izvjestiteljica: Sophie in 't Veld (2022.). *Nacrt izvješća*.
- Glavno tajništvo Vijeća. *Europska sigurnosna strategija.* Sigurna Europa u boljem svijetu. 2009.
- Gutheil, M., Liger, Q., Heetman, A., Eager, J., i Crawford, M. *„Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices" (Pravni okviri za hakiranje koje provode tijela kaznenog progona: utvrđivanje, ocjenjivanje i usporedba praksi).* Studija koju je naručio odbor LIBE. Europski parlament, 2017.
- Habermas, J. *„Legitimation Crisis" (Kriza legitimacije)*. Beacon Press, 1975.
  – „Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research" (Politička komunikacija u medijskom društvu: uživa li demokracija i dalje epistemičku dimenziju? Utjecaj normativne teorije na empirijsko istraživanje). U *Communication Theory* (2006.), str. 411–426.
- Odbor za ljudska prava. *Opća napomena br. 34. o čl. 19.: sloboda mišljenja i izražavanja.* Ujedinjeni narodi. CCPR/C/GC/34, 2011.
- Kathrine, G.J.W., Praise, P.M., Rose, A.A. i Kalaivani, E.C., 2019. „Variants of phishing attacks and their detection techniques" (Varijante *phishing* napada i tehnika za njihovo otkrivanje). U *3rd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2019., str. 255-259.
- Kaye, David. *„The impact of spyware on fundamental rights" (Utjecaj špijunskog softvera na temeljna prava)*. Svjedočenje pred odborom PEGA u Europskom parlamentu, 27. listopada 2022.
- Legrand, T. „National Security and Public Policy: Exceptionalism Versus Accountability" (Nacionalna sigurnost i javna politika: iznimnost nasuprot odgovornosti). U *The Palgrave Handbook of National Security*. Ur. Michael Clarke i dr. 2022., poglavlje 3.
- Litwiński, P. *Opinia prawna w sprawie naruszeń, w związku z ujawnionymi przypadkami użycia oprogramowania szpiegującego Pegasus w świetle prawa ochrony danych osobowych, przepisów Karty Praw Podstawowych UE i Konstytucji RP*, Kancelaria Senatu, Varšava 2022.

- Liu, W. i Zhong, S. „Web malware spread modelling and optimal control strategies" (Modeliranje širenja mrežnog zlonamjernog softvera i optimalne strategije za kontrolu). *Scientific reports,* 2017., 7.(1.), str. 1-19.
- Lyon, D. *„Surveillance Studies" (Studije o nadzoru).* Polity Press, 2007.
- Mansbridge, J. i dr. „A systemic approach to deliberative democracy" (Sustavni pristup deliberativnoj demokraciji). U *„Deliberative Systems: Deliberative Democracy at the Large Scale*" (Deliberativni sustavi: deliberativna demokracija u velikim razmjerima). Ur. John Parkinson i Jane Mansbridge. Cambridge University Press, 2012., str. 1-26.
- Marx, G. T. *„Windows into the Soul. Surveillance and Society in an Age of High Technology" (Prozori duše. Nadzor i društvo u doba visoke tehnologije).* Chicago University Press, 2016.
- Marzocchi, O. i Mazzini, M. *„Pegasus and surveillance spyware" (Pegasus i špijunski softver za nadzor).* Europski parlament. Odbor PEGA-a, 2022.
- Mazetti, M., Bergman, R., i Sevis-Grindneff, M. „US strains to control spyware, but uses it" (SAD se trsi kontrolirati špijunski softver, ali se koristi njime). *The New York Times.* (1. prosinca 2022.).
- Newman, Lily Hay. „Google Warns That NSO Hacking Is On Par With Elite Nation-State Spies" (Google upozorava da je hakiranje koje provodi NSO usporedivo s elitnim špijunima nacionalnih država). *Wired* (15. prosinca 2021.).
- Monti, A. i Wacks, R. *„National Security in the New World Order*" (Nacionalna sigurnost u novom svjetskom poretku). Routledge, 2022.
- Nisha, T.N. i Kulkarni, M.S., „Zero click attacks – a new cyber threat for the e-banking sector" (Napadi bez klika – nova kibernetička prijetnja sektoru e-bankarstva). *Journal of Financial Crime*, (prije tiska), 2022.
- NSO. „Pegasus – *Product Description*" (Pegasus – Opis proizvoda).
- Rankin, Jennifer. „Dutch MEP says illegal spyware 'a grave threat to democracy'" (Nizozemska europarlamentarka tvrdi da je nezakonit špijunski softver „ozbiljna prijetnja" demokraciji). *The Guardian* (8. studenoga 2022.).
- Rijpma, J. J. „The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection" (Novi mehanizam EU-a za zaštitu podataka: utvrđivanje globalnih standarda prava na zaštitu osobnih podataka). *XXIX. kongres FIDE-a u Haagu*. Eleven, 2020.
- Rodotà, S. „Data Protection as a Fundamental Right" (Zaštita podataka kao temeljno pravo). U *Reinventing Data Protection*? (Preobrazba zaštite podataka). Ur. Serge Gutwirth i dr. Springer, 2009., str. 77–82.
- Saeed, I.A., Selamat, A. i Abuagoub, A.M. "A survey on malware and malware detection systems" (Pregled zlonamjernog softvera i sustava za njegovo otkrivanje). *International Journal of Computer Applications* (2013.), 67.(16.).
- Sahani, R. i Randhawa, S. „Clickjacking: Beware of Clicking" (Clickjacking: klikajte oprezno). *Wireless Personal Communications* (2021.) 121(4), str. 2845-2855.
- Salahdine, F. i Kaabouch, N., „Social engineering attacks: A survey" (Napadi društvenim inženjeringom: pregled). *Future Internet* (2019.), 11.(4.), str. 89.

- Sanders, B. „Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections" (Demokracija pod utjecajem: paradigme odgovornosti države za operacije kibernetičkog utjecaja na izbore). U Chinese Journal of International Law (2019.), str. 1–56.
- Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. i Ng, A. „Cybersecurity data science: an overview from machine learning perspective" (Kibersigurnosna podatkovna znanost: pregled iz perspektive strojnog učenja). *Journal of Big data* (2020.), 7.(1.), str. 1-29.
- Schmitt, C. *Political Theology* (Politička teologija). MIT, 1985. [1922.].
- Simitis, S. „Reviewing Privacy in the Information Age" (Preispitivanje privatnosti u informacijskom dobu). U *University of Pennsylvania Law Review* (1987.), str. 707-46.
- Singh, U.K., Joshi, C. i Kanellopoulos, D., 2019. „A framework for zero-day vulnerabilities detection and prioritization" (Okvir za otkrivanje i određivanje prioriteta dosad nepoznatih nedostataka). Journal of Information Security and Applications (2019.), 46., str. 164-172.
- Ujedinjeni narodi. *Izvješće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, Frank La Rue.* A/HRC/23/40, 2013.
- Ujedinjeni narodi, Opća skupština. *„The right to privacy in the digital age: resolution" (Pravo na privatnost u digitalnom dobu: rezolucija).* Ujedinjeni narodi. A/RES/73/179, 2019.
- Ujedinjeni narodi. *Izvješće posebnog izvjestitelja o promicanju i zaštiti prava na slobodu mišljenja i izražavanja, David Kaye.* A/HRC/41/35, 2019.

  Izvješće posebnog izvjestitelja za promicanje i zaštitu ljudskih prava i temeljnih sloboda u borbi protiv terorizma. Utjecaj mjera za suzbijanje terorizma i nasilnog ekstremizma na prostor za građansko djelovanje i prava aktera civilnog društva i boraca za ljudska prava. A/HRC/40/52, 2019.

  Izvješće posebnog izvjestitelja o pravu na privatnost, Joseph A. Cannataci. A/HRC/34/60, 2017.
- Vogiatzoglou, P., Marquenie, T., i Valke. P. *„Assessment of the implementation of the Law Enforcement Directive" (Procjena provedbe Direktive o provedbi zakona). Studija koju je naručio odbor LIBE.* Europski parlament, 2022.
- Watt, E. *„State Sponsored Cyber Surveillance"* (Kibernadzor pod pokroviteljstvom države). Elgar, 2021.

U ovoj studiji, koju je naručio Resorni odjel Europskog parlamenta za prava građana i ustavna pitanja na zahtjev Istražnog odbora za ispitivanje uporabe Pegasusa i jednakovrijednog špijunskog softvera za nadzor (PEGA), analizira se učinak uporabe Pegasusa i sličnog špijunskog softvera za nadzor na vrijednosti utvrđene u članku 2. Ugovora o Europskoj uniji, privatnost i zaštitu podataka i demokratske procese u državama članicama.

PE 740.514
IP/C/PEGA/IC/2022-071

Tisak ISBN 978-92-848-0261-6 | doi: 10.2861/947663 | QA-03-22-291-HR-C
PDF ISBN 978-92-848-0266-1 | doi: 10.2861/349448 | QA-03-22-291-HR-N