EDRi

Spajver i državna zloupotreba: Argumenti za zabranu na nivou EU

Sadržaj

Izradu ovog pozicionog dokumenta koordinisao je **Aljoša Ajanović, savetnik za politike u mreži EDRi.**

Zahvaljujemo se svim članovima EDRi mreže, na čiji se rad oslanja ovaj izveštaj. Posebnu zahvalnost za doprinos izveštaju dugujemo:

→ Chloé Berthélémy, *EDRi*
→ Jesper Lund, *IT-Pol Denmark*
→ Bastien Le Querrec, *La Quadrature du Net*
→ Andrijana Ristić, *SHARE Fondacija*
→ Rand Hammoud, *Access Now*
→ Luzie Neyenhuys, *Gesellschaft für Freiheitsrechte*
→ Hannah Lichtenthäler, *SUPERRR Lab*
→ Rejo Zenger, *Bits of Freedom*
→ Michaela Nakyama Shapiro, *ARTICLE 19*
→ Walter van Holst, *Vrijschrift.org*

* Redakcija prevoda na srpski jezik: Milica Jovanović

REZIME

Upotreba spajvera[1] postaje jedna od najvećih pretnji demokratiji, osnovnim pravima i sajber bezbednosti ne samo u Evropskoj uniji, već širom sveta. I državni i privatni akteri koriste komercijalni spajver, često sa pogubnim posledicama po privatnost, političke slobode i ličnu bezbednost ljudi. Industrija spajvera razvila se zahvaljujući popustljivosti, pravnim prazninama i slaboj regulatornoj kontroli, dok se Evropa pretvara u centar za razvoj, trgovinu, primenu i izvoz ovih štetnih tehnologija.

Spajver funkcioniše tako što eksploatiše ranjivosti, narušava integritet uređaja i omogućava daljinski, često neprimetan pristup neograničenoj količini ličnih podataka. Bilo da ga koriste državne službe bezbednosti, privatne firme ili pojedinci, upotreba spajvera u osnovi krši principe neophodnosti i proporcionalnosti iz evropskog pravnog okvira o ljudskim pravima. Tržište komercijalnog spajvera ne samo da omogućava nezakoniti nadzor, već i podstiče rodno zasnovano nasilje, prisilnu kontrolu i destabilizaciju čitavih zajednica.

Proliferacija spajvera omogućena je pravilima unutrašnjeg tržišta EU, odsustvom ujednačene regulative i bujanjem tržišta ranjivosti. Države i privatni dobavljači profitiraju na ovom modelu „upada kao usluge“, dok su žrtve suočene sa ogromnim preprekama u ostvarivanju pravne zaštite. Neuspeh EU da reguliše ovu industriju ima globalne posledice, jer ohrabruje njeno širenje i u zemlje kandidate i dalje, dodatno urušavajući demokratske norme i bezbednost širom sveta.

S obzirom na inherentne rizike i sistemske zloupotrebe, zaključujemo da nikakve zaštitne mere ne mogu učiniti upotrebu spajvera usklađenom sa fundamentalnim pravima. Zato EDRi poziva na potpunu zabranu u EU – zabranu razvoja, proizvodnje, reklamiranja, prodaje, izvoza i upotrebe spajvera – na osnovu jasne i primenjive definicije koja obuhvata njegove osnovne karakteristike i funkcije. Samo potpuna zabrana može efikasno zaštititi ljudska prava, zatvoriti regulatorne rupe i zaustaviti učešće EU u globalnom širenju spajvera.

Pored toga, EU mora hitno da preduzme korake za suzbijanje šireg ekosistema spajvera:

→ **Zatvoriti tržište komercijalnog spajvera** kroz zabranu rada dobavljača i investitora, kao i izvoza spajvera iz EU. Poslovni model zasnovan na tajnosti, ranjivostima i zloupotrebi, mora biti razoren kako bi se sprečilo dalje širenje industrije.

→ **Zatvoriti tržište ranjivosti i eksploita** kroz zabranu komercijalne trgovine ranjivostima u ove svrhe. Javna sredstva i javne nabavke više ne smeju da podstiču razvoj novih eksploita. Resursi

[1] U prevodu ovog teksta koristimo izraz „spajver“, umesto tradicionalnog „špijunski softver“ (*spying software*). Mada najčešće jeste reč o računarskom programu, špijunska tehnologija danas daleko prevazilazi softverske aplikacije i obuhvata hardver i druga tehnološka rešenja. Termin „spajver“ bolje odražava ovu složenost i sve više se koristi u tehničkim i neformalnim kontekstima, omogućavajući neutralniji i fleksibilniji izraz za savremene oblike sajber špijunaže.

treba da budu usmereni na koordinisano otkrivanje ranjivosti, rad istraživača i jačanje sajber bezbednosti.

→ **Obezbediti pristup zaštiti žrtvama** koje su već pretrpele štetu zbog zloupotrebe spajvera, izradom jasnih zakonskih procedura za zadovoljenje pravde, uključujući sudsku zaštitu, mehanizme reparacije i odgovornost države za nezakonitu upotrebu spajvera. EU takođe mora da garantuje efikasnu istragu, krivično gonjenje i kažnjavanje počinilaca i investitora, uključujući političku i administrativnu odgovornost javnih funkcionera koji su omogućili zloupotrebe spajvera.

2. Šta je spajver? Postojana definicija

U ovom delu bavimo se definisanjem spajvera. Razmatramo alate za hakovanje koje koriste države u svrhe nadzora, ali i alate poput tzv. progoniteljskog softvera (*stalkerware*) i forenzičkih programa, da bi smo razjasnili opseg ovog dokumenta ali i svake buduće regulative koja se tiče spajvera.

2.1 Definisanje spajvera: holistički i održiv pristup

2.1.1 Definicija koja predviđa buduće pretnje

Kad se pomene „spajver“, mnogi pomisle na *Pegaz* zloglasne izraelske kompanije NSO Group, ili na slične programe o kojima se priča u medijima poslednjih godina. Međutim, postoji i mnogo drugih softverskih alata sa različitim mogućnostima koji spadaju u kategoriju spajvera. Novi tehnološki trendovi, poput *AdInt* koji može da zarazi uređaje preko naizgled bezazlenih ciljanih reklama,[2] pokazuju koliko brzo zastarevaju i sažete i detaljne definicije.

Industrija komercijalnog spajvera stalno se menja, iskorišćava pravne rupe i razvija specifične tehnologije da bi izbegla tradicionalnu klasifikaciju. Zato održiva, primenjiva i fleksibilna definicija mora da se fokusira na ono što spajver radi, umesto na to kako se reklamira ili ko ga koristi. Definicija takođe mora biti dovoljno široka da obuhvati svaki softver sa opisanim karakteristikama i tako spreči buduće štete. U suprotnom, ako se definicija ograniči samo na najinvazivnije vrste, mnogi alati koji krše privatnost ostaće izvan domašaja zakona, dok će pravnu prazninu moći da koriste i države i privatni zlonamerni akteri.

---

[2] *AdInt* se odnosi na novi oblik reklamnih praksi, „Ad intelligence“, odnosno tehnike koje podatke prikupljene za svrhe reklamiranja pretvaraju u obaveštajne podatke. Kako navode mediji, izraelske kompanije razvijaju softver koji može da inficira uređaj preko naizgled obične ciljane reklame. *Intelligence Online*, “Offensive AdInt Is Israeli Cyber Sector’s New Secret Weapon”, 15. februar, 2024. https://www.intelligenceonline.com/surveillance--interception/2024/02/15/offensive-adint-is-israeli-cyber-sector-s-new-secret-weapon,110159842-eve

2.1.2 Osnovne karakteristike: koja vrsta softvera se svrstava u spajver?

Kada se određuje obim zabrane upotrebe spajvera, neophodno je opisati tehnike i alate koje želimo da zabranimo. Na osnovu našeg uvida u postojeće i ranije alate za hakovanje, spajver se može definisati kao svaki softver koji ispunjava sledeće kumulativne uslove:

1. **Instalira se ili pokreće na uređaju bez slobodnog i informisanog pristanka korisnika.**

2. **Narušava integritet uređaja**, što znači da softver privremeno ili trajno menja jedan ili više elemenata uređaja, uključujući, između ostalog, nestabilnu (radnu) memoriju (RAM)[3] i druge interne memorije, unutrašnje čipove ili drajvove za skladištenje. Ova karakteristika razlikuje spajver od nekih tradicionalnih forenzičkih alata, koji su teoretski ograničeni na ekstrakciju podataka i ne menjaju uređaj ni podatke na njemu na način koji ovlašćeni korisnici ne mogu da otkriju, za razliku od forenzičkih alata (videti deo ispod). Ovaj princip očuvanja integriteta uređaja ključan je za ispunjavanje zahteva integriteta i validnosti dokaza tokom sudskih postupaka.[4]

3. Njegova **upotreba se** pretežno **omogućava eksploatacijom** postojećih ili namerno stvorenih **ranjivosti u digitalnim sistemima** (hardveru ili softveru), uključujući socijalni inženjering, fizičku implantaciju ili unapred instalirane mehanizme,[5] kao i obmanjujuće reklame.[6]

4. Nakon instalacije, njegove aktivnosti (tj. izdavanje komandi) vrše se **automatski ili na daljinu**. Pošto je instaliran, spajver radi bez potrebe za daljim fizičkim pristupom uređaju.

---

[3] Neki spajver alati funkcionišu tako što usađuju izvršni kod (exe) na RAM kako bi ostali neopaženi.

[4] U sudskim postupcima, dokazi moraju biti pouzdani, autentični i proverljivi. Ako je uređaj kompromitovan, postaje nejasno da li su dokazi izmenjeni, podmetnuti, izbrisani, niti da li je stanje uređaja autentično... Podacima se ne može verovati ako se ne može verovati uređaju s kojeg su dobijeni.

[5] Smatramo da razlika između fizičke implantacije i unapred instaliranih mehanizama, leži u znanju i saglasnosti proizvođača. Primer unapred instaliranog mehanizma je zloglasni *Clipper Chip*, čipset koji je razvila i promovisala američka Nacionalna bezbednosna agencija (NSA) tokom 1990-ih, da omogući federalnim, državnim i lokalnim organima za sprovođenje zakona da dešifruju presretnute glasovne i prenose podataka. Od proizvođača se očekivalo da ugrade *Clipper Chip* u svaki novi telefon ili drugi uređaj, u zamenu za blaže izvozne kontrole. Primer fizičke implantacije bila bi implantacija malih malicioznih čipova od strane Kine na matične ploče kompanije *Super Micro Computer Inc*. (*Supermicro*) počev od 2014, što je uticalo na najmanje 30 američkih kompanija u lancu snabdevanja od ove kompanije, uključujući *Apple* i *Amazon*. Vidi: *Bloomberg*, “How China Used a Tiny Chip in a Hack That Infiltrated Amazon and Apple”, 4. oktobar, 2018. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

[6] *Haaretz*, “Revealed: Israeli Cyber Firms Developed an ‘Insane’ New Spyware Tool – No Defense Exists”, 14. septembar, 2023. https://www.haaretz.com/israel-news/2023-09-14/ty-article-magazine/highlight/revealed-israeli-cyber-firms-developed-an-insane-new-spyware-tool-no-defense-exists/0000018a-93cb-de77-a98f-ffdf2fb60000

5. Može biti **ciljano usmeren** na pojedince ili grupe, ili **korišćen neselektivno**.

Pored toga, softver koji služi za instaliranje ovde definisanog spajvera, takođe spada pod tu definiciju (videti odeljak 2.1.4) – čak i ako mu to nije primarna namena.

Ovakvo određenje izbegava restriktivne kvalifikatore poput „dizajniran s namerom“ ili „posebno napravljen“, koji funkcionalno identičnim alatima omogućava zaobilaženje regulative samo zato što se drugačije reklamiraju.

Dobar presedan predstavlja Izvršna naredba 14093 u Sjedinjenim Američkim Državama, koja komercijalni spajver definiše kao bilo koji softver koji omogućava „daljinski pristup računaru, bez pristanka korisnika, administratora ili vlasnika“.[7] Ovako širok pristup obezbeđuje da regulatorni okvir obuhvati i tehnologije i metode nadzora koje u trenutku usvajanja nisu postojale. Slično tome, Agencija EU za sajber bezbednost (ENISA) definiše spajver kao „vrstu malvera koji špijunira aktivnosti korisnika bez njihovog znanja ili pristanka, uključujući snimanje klikova na tastaturi (*keylogging*), praćenje aktivnosti i prikupljanje podataka“.[8]

Nasuprot tome, uže definicije, poput onih u smernicama EU o primeni Uredbe o robi dvostruke namene na alate za sajber nadzor, ne uspevaju da obuhvate celokupan domet spajvera jer se fokusiraju na nameru programera i specifične karakteristike dizajna, umesto na funkcionalnosti samog alata.[9]

2.1.3 Kapaciteti spajvera: šta sve ovaj alat može?

Osim prema osnovnim karakteristikama, spajver treba definisati i prema onome što omogućava. Tehnologija se smatra špijunskom ako, uz ispunjene kriterijume iz tačke 2.1.2, omogućava jednu ili više od sledećih funkcionalnosti:

---

[7] Izvršna naredba 14093, “Prohibition on the Use of the United States Government of Commercial Spyware”, 27. mart, 2023. https://www.presidency.ucsb.edu/documents/executive-order-14093-prohibition-use-the-united-states-government-commercial-spyware-that

[8] Arhivirana stranica: *Enisa*, What is malware? https://web.archive.org/web/20230419091714/https://www.enisa.europa.eu/topics/incident-response/glossary/malware

[9] Komisija je predmete za sajber-nadzor opisala kao „predmete dvostruke namene posebno dizajnirane da omoguće tajni nadzor fizičkih lica putem praćenja, izdvajanja, prikupljanja ili analize podataka iz informacionih i telekomunikacionih sistema“. European Commission, “Commission Recommendation (EU) 2024/2659 of 11 October 2024 on guidelines on the export of cyber-surveillance items under Article 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council”, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402659

→ **Pristup i nadzor uređaja** (podaci u realnom vremenu), čime se operateru spajvera omogućava da posmatra aktivnosti, presreće komunikacije, prati lokaciju i slično, sa potencijalno neograničenim pristupom.

→ **Prikupljanje ili obrada korisničkih podataka** (istorijski podaci), kao što je izvlačenje starih poruka, istorije poziva, istorije pretraživanja, sačuvanih fajlova, biometrijskih podataka itd.

→ **Iznošenje (eksfiltracija) podataka** radi deljenja tih informacija sa trećom stranom.

→ **Kontrola ili manipulacija uređajem**, poput aktiviranja mikrofona ili kamera, izmene sistemskih podešavanja, isključivanja bezbednosnih funkcija itd.

→ **Menjanje ili falsifikovanje informacija**, uključujući izmenu, brisanje ili fabrikovanje poruka, fajlova ili logova, kako bi se prikrili tragovi ili čak podmetnuli dokazi.

Ovaj „ili-ili“ pristup je od ključnog značaja: alat ne mora istovremeno da obavlja sve ove radnje da bi bio klasifikovan kao spajver.[10] Svaki softver koji ispunjava osnovne karakteristike i poseduje makar jednu od ovih funkcionalnosti treba da potpada pod zabranu.

Karakteristike i kapaciteti spajvera čine njegovu upotrebu suštinski nespojivom sa pravom na privatnost. Razlog je u tome što spajver narušava integritet uređaja bez pristanka korisnika i omogućava pristup ogromnoj količini podataka na način koji nije u skladu sa principima neophodnosti i proporcionalnosti, a koji se zahtevaju za svako ograničenje fundamentalnih prava iz Povelje EU.[11]

2.1.4 Šta spada u kategoriju „spajvera“?

Slede primeri alata koje svrstavamo pod ovu definiciju spajvera (lista nije konačna):

→ **Komercijalni spajver**: softver koji razvijaju, proizvode i prodaju privatne kompanije za potrebe vlada, korporacija ili pojedinaca. Među poznatim primerima su *Pegasus* (NSO Group), *Predator* (Intellexa), *Graphite* (Paragon) ili *FinSpy/FinFisher* (Lench IT Solutions PLC).

→ **Državni spajver**: pojedine vlade razvijaju sopstveni spajver da se ne bi oslanjale na privatne dobavljače. Nemačka već godinama koristi svoj *Remote Communication Interception Software*

[10] Sličan pristup usvojila je Bajdenova administracija u Izvršnoj naredbi 14093, u kojoj su kapaciteti spajvera definisani kao: „(I) pristup, prikupljanje, iskorišćavanje, izdvajanje, presretanje, preuzimanje ili prenos sadržaja, uključujući informacije pohranjene na računaru povezanom na internet ili prenesene preko njega; (ii) snimanje audio ili video poziva računara ili korišćenje računara za snimanje zvuka ili videa; ili (iii) praćenje lokacije računara.“

[11] Povelja Evropske unije o osnovnim pravima, 2012/C 326/02, Član 52(1).

(RCIS)[12] u svrhe sprovođenja zakona, dok Francuska trenutno razvija sopstveni.[13] U decembru 2024. godine, međunarodna organizacija *Amnesty International* otkrila da i vlasti u Srbiji koriste domaći spajver nazvan „NoviSpy“.[14]

→ **Progoniteljski softver (*stalkerware*)**: spajver koji koriste pojedinci, često u intimnim odnosima sa partner(k)om, npr. u slučajevima porodičnog nasilja, kako bi nadzirali i kontrolisali drugu osobu. Ponekad se predstavlja kao softver za „roditeljsku kontrolu“.[15]

→ **Softver za roditeljsku kontrolu ili za nadzor zaposlenih**: mada ne moraju svi alati za roditeljsku kontrolu nužno biti spajver, oni koji omogućavaju trećoj strani (roditelju, staratelju ili menadžeru) daljinski, tajni i neovlašćeni pristup komunikacijama ili kontrolnim podešavanjima uređaja deteta ili zaposlenog, spadaju pod definiciju spajvera. Softver koji se strogo ograničava na blokiranje određenih funkcija (npr. instalaciju novih aplikacija) ili pristupa određenim onlajn sadržajima, ne smatra se spajverom. Kao što je navedeno, alati za roditeljsku kontrolu često mogu biti zloupotrebljeni u kontekstu digitalnog proganjanja ili prisilne kontrole.

→ **Kilogeri (*keyloggers*)**:[16] programi koji tajno beleže pritiske na tastaturi i na taj način služe za krađu lozinki ili uvid u finansijske informacije, privatnu komunikaciju i aktivnost zaposlenih.

→ **Infostileri (*infostealers*)**:[17] malver osmišljen za izvlačenje osetljivih korisničkih podataka, poput istorije pretraživanja, sačuvanih kredencijala i privatnih fajlova. Ove alate često koriste sajber-kriminalci, ali ih mogu upotrebljavati i državni akteri.

2.1.5 Šta nije spajver?

Slede primeri alata koji ne spadaju pod ovu definiciju spajvera (lista nije konačna):

→ **Softver za daljinski pristup**: alati kao što su KVM svičevi (*switches*),[18] *TeamViewer*,[19] *AnyDesk* ili *Microsoft Remote Desktop*, koji se koriste za legitimnu IT podršku i rad na daljinu.

---

[12] *Netzpolitik.org*, “Prüfbericht zum BKA-Staatstrojaner: Die Software ist [redacted]” 2022, https://netzpolitik.org/2022/die-software-ist-[redacted]-[redacted]-[redacted]/
[13] *Intelligence Online*, “French Intelligence Service Safeguards Funding for Developing In-House Spyware,” 3. februar, 2025. https://www.intelligenceonline.com/surveillance--interception/2025/02/03/french-intelligence-service-safeguards-funding-for-developing-in-house-spyware,110369360-eve
[14] *Amnesty International*, “Serbia: A Digital Prison: Surveillance and the Suppression of Civil Society,” decembar 2024. https://www.amnesty.org/en/documents/eur70/8813/2024/en/
[15] *National Cybersecurity Alliance*, “Stalkerware,” 2022, https://www.staysafeonline.org/articles/stalkerware
[16] *Malwarebytes*, “What Is a Keylogger?” 2024. https://www.malwarebytes.com/keylogger
[17] *Proton*, “What Are Infostealers?” 2024. https://proton.me/blog/infostealers
[18] *Wikipedia*, KVM switch https://en.wikipedia.org/wiki/KVM_switch
[19] *TeamViewer*, www.teamviewer.com

Ovi alati zahtevaju pristanak korisnika pre nego što im se omogući pristup, dok se pristanak može opozvati u bilo kom trenutku.

→ **Eksfiltracija telemetrijskih podataka niskog nivoa**: proizvođači softvera i operativnih sistema prikupljaju telemetrijske podatke (kao što su prijave grešaka, statistika korišćenja) radi analize i otklanjanja grešaka, u skladu sa svojim uslovima korišćenja i poslovnom praksom. Mada može doći do problema koji utiču na privatnost korisnika u slučajevima kada se ovo radi loše ili prekomerno, ti podaci su obično pseudonimizovani, a njihovo prikupljanje ne omogućava širi pristup uređaju.

→ **Forenzički alati**: ovi alati omogućavaju kopiranje ili izvlačenje podataka sa određenog uređaja, obično otključanog, bez narušavanja njegovog integriteta. Poštovanje integriteta uređaja tokom rada digitalnih forenzičkih alata, od ključnog je značaja za integritet i verodostojnost dokaza u krivičnom postupku: neophodno je da i odbrana i nezavisni tehnički stručnjaci mogu da provere i reprodukuju digitalne dokaze koje sakupe istražni organi. Ovi alati će se smatrati spajverom ako se koriste za instaliranje spajvera, u skladu sa definicijom iz odeljka 2.1.2.

→ **Tradicionalne metode nadzora**, kada se sprovode potpuno u skladu sa važećim zakonima i zaštitnim merama. Teoretski, prisluškivanje koje je odobrio sud ili zakonit pristup podacima koje čuva internet provajder, razlikuju se od spajvera jer podrazumevaju određeni nivo nadgledanja, transparentnosti i sudske kontrole; ograničeni su vremenski, kao i u odnosu na vrstu i količinu podataka kojima se pristupa,[20] što potencijalno ispunjava zahtev proporcionalnosti; pristup nije direktan u sam uređaj, već preko treće strane, obično telekomunikacionog provajdera.[21]

2.1.6 Da li zavisi od toga ko ga koristi?

Prilikom definisanja šta jeste „spajver“, fokus treba da bude na intruzivnim kapacitetima alata, a ne na tome ko ga koristi. Naš predlog za zabranu zasniva se na nesrazmernoj prirodi spajvera, jer upravo ona određuje posledice na privatnost i druga ljudska prava. Spajver ostaje spajver bez obzira na to da li ga koriste službe za sprovođenje zakona, obaveštajne agencije, privatne kompanije, sajber plaćenici ili pojedinci, uključujući nasilne emotivne partnere. Međutim, države imaju veću obavezu da poštuju, štite i ostvaruju ljudska prava, što znači da od državnih aktera

[20] Pogledati presudu francuskog suda kojom se proglašava nezakonitim francuski zakon koji policiji i tajnim službama dozvoljava upotrebu spajvera, posebno u vezi s aktiviranjem mikrofona ili kamera, zbog neusaglašenosti sa zahtevima neophodnosti i proporcionalnosti. Conseil Constitutionnel, “Décision n° 2023-855 DC du 16 novembre 2023 - Communiqué de presse,” 16. novembar, 2023. https://www.conseil-constitutionnel.fr/actualites/communique/decision-n-2023-855-dc-du-16-novembre-2023-communique-de-presse

[21] *European Digital Rights* (EDRi), “Do You Trust the Police? CJEU Advocate General Accepts Access to Phones for Any Type of Crime,” 10. maj, 2023. https://edri.org/our-work/eu-court-of-justice-advocate-general-accepts-access-to-phones-for-any-crime/

očekujemo proaktivne mere kako bi zaštitili našu privatnost od spajvera, i nametnuli kompanijama obavezu da ne razvijaju i ne prodaju alate koji krše ljudska prava.

2.1.7 Specifičan slučaj UFED uređaja

Mada se čuveni *Cellebrite Universal Forensics Extraction Device* (UFED)[22] reklamira kao tradicionalni forenzički alat, on zapravo ispunjava neke od osnovnih karakteristika spajvera, izuzev mogućnosti kontinuiranog izvlačenja podataka nakon instalacije (osim ako se Cellebrite koristi za instaliranje spajvera – videti odeljak 2.1.2 – kako su pokazala otkrića o spajveru u Srbiji 2024. godine).[23] *Cellebrite* i slični alati poput *XRY* (MSAB)[24] i *Graykey* (Magnet Forensics)[25] narušavaju integritet zaključanih uređaja iskorišćavanjem bezbednosnih ranjivosti. Na primer, na zaključanim uređajima *Cellebrite* instalira izvršni kod[26] ili da razbije lozinku metodom tzv. nasilnog probijanja (*brute force*)[27] ili da omogući ekstrakciju podataka u stanju iOS uređaja nakon prvog otključavanja (*After First Unlock*, AFU).[28] Dakle, *Cellebrite* se ne ograničava samo na prosto izvlačenje podataka sa uređaja, kao što to čine tradicionalni forenzički alati.

Iz tog razloga, kao i zbog rizika koje ovakvi alati nose za osnovna prava, EDRi smatra da bi upotreba *Cellebrite*a i sličnog softvera takođe trebalo da bude zabranjena. Mada Cellebrite UFED i sličan softver nisu direktno obuhvaćeni opsegom zabrane spajvera koju EDRi zagovara, predložena zabrana tržišta ranjivosti i eksploita (videti odeljak 3.4) takođe bi ograničila nekontrolisanu upotrebu UFED-ova za izvlačenje podataka, budući da se ona oslanja na iskorišćavanje ranjivosti uređaja.

---

[22] *Access Now*, "What spy firm Cellebrite can't hide from investors", 2021. https://www.accessnow.org/what-spy-firm-cellebrite-cant-hide-from-investors/
[23] *Amnesty International*, "Serbia: Authorities Using Spyware and Cellebrite Forensic Extraction Tools to Hack Journalists and Activists," 16. decembar, 2024. https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/
[24] *MSAB*, XRY – Mobile Forensics and Data Recovery Software https://www.msab.com/product/xry-extract
[25] *Magnet Forensics*, Graykey: Accelerate your mobile investigations https://www.magnetforensics.com/products/magnet-graykey
[26] Instalaciju binarnog fajla „falcon" za ekstrakciju podataka dokumentovala je organizacija *Amnesty International* u izveštaju: "Serbia: A Digital Prison: Surveillance and the Suppression of Civil Society," decembar 2024. https://www.amnesty.org/en/documents/eur70/8813/2024/en/
[27] Vidi *Rečnik pojmova*.
[28] Pametni telefoni imaju dva različita stanja koja mogu uticati na mogućnost njihovog otključavanja i izdvajanja podataka iz njih: „pre prvog otključavanja" (*Before First Unlock*, BFU) – pre nego što korisnik prvi put unese lozinku kada uključi uređaj – pohranjeni podaci su u potpunosti šifrovani; „posle prvog otključavanja" (*After First Unlock*, AFU), kada korisnik uspešno pristupi telefonu nakon što je uređaj bio isključen – određeni podaci su dešifrovani i mogu se lakše izvući pomoću nekih forenzičkih alata za uređaje, čak i ako je telefon zaključan. Za više detalja, vidi: *DigiForCE Lab Blog*, „BFU and AFU Lock States", 23. avgust 2023. https://blogs.dsu.edu/digforce/2023/08/23/bfu-and-afu-lock-states/

2.1.8 Poređenje sa tradicionalnim metodama nadzora poput prisluškivanja

Kao što fizički pretres nečijeg doma mora biti podvrgnut najstrožoj pravnoj zaštiti, isto važi i za digitalne upade u privatne uređaje – jer je pristup nečijem telefonu danas često dublje narušavanje privatnosti nego ulazak u nečiju kuću.

Međutim, spajver koji danas koriste evropske vlasti suštinski se razlikuje od tradicionalnih metoda nadzora, i po obimu i po invazivnosti. Dok su starije metode obično ograničene u pogledu trajanja, prostora i podataka, spajver funkcioniše kao „alat za sve“ koji omogućava trajni i potpuni pristup (digitalnom) životu određene osobe.

Uporedimo tradicionalne metode sa spajverom:

→ Mikrofoni i kamere koji se koriste za fizičko prisluškivanje, postavljaju se na fiksnim lokacijama. Njihova pozicija se obično bira tako da se smanji rizik od prikupljanja podataka o nekom drugom (npr. snimanje samo spavaće sobe osumnjičenog). Nasuprot tome, spajver može potajno da aktivira mikrofon ili kameru uređaja bez obzira na lokaciju korisnika, i na taj način kontinuirano prikuplja podatke iz bilo kog okruženja, bez ciljanja ili ograničenja, uključujući i podatke slučajnih prolaznika koji nemaju nikakve veze sa krivičnom istragom.

→ GPS praćenje omogućava nadzor lokacije, ali obično pruža samo jednu vrstu informacija, o lokaciji, a može biti fokusirano na uređaj ili objekat, a ne nužno za određenu osobu. Spajver, međutim, kombinuje podatke o lokaciji sa svim ostalim aktivnostima na uređaju, direktno vezujući nadzor za konkretnog pojedinca i mnoštvo raznih informacija.

→ Pretres doma, mada omogućava pristup velikoj količini istorijskih podataka, vremenski je i prostorno ograničen. Ovlašćeni službenici ulaze u određeni prostor i uzimaju ono što se tamo fizički zatekne u tom trenutku. To je potpuno različito od spajvera, koji omogućava kontinuiran nadzor i prikupljanje svih istorijskih i podataka u realnom vremenu, tokom produženog trajanja.

Spajver, dakle, nije tek digitalni ekvivalent ovih metoda – on može da ih kombinuje i daleko ih prevazilazi. Šteta koju izaziva ne može se ograničiti i često pogađa ne samo osobu na meti, već i ljude koji sa njom komuniciraju, i fizički i digitalno. Ova kolateralna intruzija posebno je problematična u krivičnom pravu, koje se zasniva na individualizovanoj sumnji i odgovornosti. Pojedini sudovi već su ocenili da je taj aspekt spajvera nezakonit.[29] Ključno je i to da spajver kompromituje uređaj, što znači da dokazi pribavljeni njegovom upotrebom ne mogu da prođu test integriteta dokaza na sudu. Njegove karakteristike i kapaciteti čine ga suštinski nespojivim sa principima neophodnosti, proporcionalnosti i pravne zaštite.

---

[29] *Conseil Constitutionnel*, ibidem.

2.2 Upotreba spajvera u slučaju nedržavnih aktera: tri studije slučaja

Državni organi nisu jedini korisnici spajvera. Široko je dostupan i sve češće se koristi u kontekstu privatnog sektora, gde su posledice po osnovna prava jednako ozbiljne.

A. Progoniteljski softver i rodno zasnovano nasilje

Posebno podmukla vrsta spajvera je tzv. progoniteljski softver (*stalkerware*), koji se često lažno reklamira kao softver za „roditeljsku kontrolu“ ili „nadzor zaposlenih“. Alati kao što su *PC Tattletale*,[30] *mSpy*[31] i *TheTruthSpy*[32] omogućavaju privatnim osobama i poslodavcima da tajno prate (bivše) partner(k)e, zaposlene i disidente. Razmere zloupotrebe ovih alata otkrivene su kroz curenje podataka – na primer, 2024. godine portal *TechCrunch* je izvestio da su sa *mSpy* „procurili“ milioni korisničkih evidencija,[33] čime je potvrđena njegova masovna upotreba u nadzoru intimnih partnera. Slično tome, 2023. hakovana je aplikacija *LetMeSpy*, koja je posebno reklamirana za praćenje ljudi, što je otkrilo na desetine hiljada žrtava.[34] U drugim slučajevima – *Spyhide*,[35] *Spytech*[36] i *PC Tattletale*[37] – procurili su podaci sa preko 100.000 kompromitovanih uređaja.

Između ostalog, umnožavanje progoniteljskog softvera omogućavaju nedostatak regulacije, agresivne marketinške kampanje koje normalizuju digitalni nadzor i proganjanje,[38] kao i niske

---

[30] *TechCrunch*, “Spyware maker pcTattletale says it’s ‘out of business’ and shuts down after data breach”, 2024. https://techcrunch.com/2024/05/28/pctattletale-spyware-shutters-data-breach/
[31] *mSpy* https://www.mspy.com/
[32] *Business and Human Rights Resources Centre*, “TheTruthSpy spyware found on 50,000 Android devices“, februar 2024. https://www.business-humanrights.org/fr/derni%C3%A8res-actualit%C3%A9s/thetruthspy-spyware-found-on-50000-android-devices
[33] *TechCrunch*, “Data Breach Exposes Millions of mSpy Spyware Customers,” 2024. https://techcrunch.com/2024/07/11/mspy-spyware-millions-customers-data-breach/
[34] *TechCrunch*, “LetMeSpy Hacked: Spyware App Breach Exposes Thousands,” 2023. https://techcrunch.com/2023/06/27/letmespy-hacked-spyware-thousands
[35] *TechCrunch*, “Spyhide Stalkerware is Spying on Tens of Thousands of Phones,” 2023. https://techcrunch.com/2023/07/24/spyhide-stalkerware-android/
[36] *TechCrunch*, “Spytech Data Breach Exposes Thousands of Compromised Devices,” 2024. https://techcrunch.com/2024/07/25/spytech-data-breach-windows-mac-android-chromebook-spyware/
[37] *IrpiMedia*, “PC Tattletale: Il Software di Spionaggio per Lavoratori,” 2024. https://irpimedia.irpi.eu/spiarelowcost-pc-tattletale-software-spyware-lavoratori
[38] *Gesellschaft für Freiheitsrechte*, “Cyberstalking-Apps: GFF reicht Beschwerde gegen Google bei der Bundesnetzagentur und der EU-Kommission ein,” 4. novembar, 2024. https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-cyberstalking-google

cene. „Jeftini“ alati za špijuniranje mogu se kupiti za svega nekoliko evra,[39] što ih čini dostupnim velikom broju zlostavljača. Istovremeno, rizici koje nose, od prisilne kontrole do čestih curenja podataka, predstavljaju ozbiljnu pretnju bezbednosti, privatnosti i drugim ljudskim pravima osoba na meti, posebno žena, LGBTQI+ osoba i drugih marginalizovanih grupa.

Progoniteljski softver se ponekad naziva i „bračni softver“ (*spouseware*)[40] jer dodatno podstiče rodno zasnovano nasilje, omogućavajući zlostavljačima da prate, kontrolišu i zastrašuju svoje partner(k)e. Istraživanja koja su sproveli *IrpiMedia*[41] i *Citizen Lab*[42] pokazuju da ove alate često tajno instaliraju intimni partneri ili bivši partneri, dodatno učvršćujući obrasce nasilja. Ovaj oblik digitalnog zlostavljanja najčešće vrše muškarci nad ženama,[43] koje uglavnom i ne znaju da su im uređaji kompromitovani.

Činjenica da EU (kao ni nacionalne vlade) nije zabranila komercijalni spajver omogućio je kompanijama da praktično nekažnjeno profitiraju na rodno zasnovanom nasilju. Žrtve digitalnog zlostavljanja suočavaju se sa ogromnim preprekama: otkriti spajver, dokazati kršenje prava, bezbedno ga ukloniti, probiti se kroz službe za sprovođenje zakona koje često ne preduzimaju ništa. Analiza sprovedena u sedam zemalja tzv. globalne većine pokazalo je da se 60% prijavljenih slučajeva onlajn nasilja nad ženama uopšte ne istražuje.[44] Prema podacima *Amnesty International* i UNDP-a, ovakav oblik nasilja ostavlja dugotrajne psihološke, socijalne i bezbednosne posledice.[45]

---

[39] *IrpiMedia*, “La Zona Grigia del Mercato degli Stalkerware,” 2024. https://irpimedia.irpi.eu/spiarelowcost-app-parental-control-sorveglianza-elettronica/

[40] *BBC News*, “Stalkerware: The Software That Spies on Your Partner,” 24. oktobar, 2019. https://www.bbc.com/news/technology-50166147

[41] *IrpiMedia*, “Uomini che Spiano le Donne,” 2024. https://irpimedia.irpi.eu/spiarelowcost-stalkerware-donne/

[42] *Citizen Lab*, “Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications,” 2019. https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/

[43] *Kaspersky*, “Global Kaspersky Report Reveals Digital Violence Has Increased,” 2024. https://www.kaspersky.com/about/press-releases/global-kaspersky-report-reveals-digital-violence-has-increased

[44] *GenderIT.org*, “Tracking Online Gender-Based Violence,” 2024. https://genderit.org/onlinevaw/state/

[45] *Amnesty International*, “An Urgent Call to Address Online Gender-Based Violence,” 2024. https://www.amnesty.org/en/documents/asa39/7955/2024/en/; *UNDP*, “Tackling Gender-Based Violence in the Digital Age,” 2024. https://www.undp.org/sites/g/files/zskgke326/files/2024-12/final-analysis-tf-gbv.pdf

B. Seksualna iznuda i ucena

Industrija komercijalnog spajvera doprinela je i porastu mreža za seksualnu iznudu (*sextortion*), gde se žrtve ucenjuju ukradenim ili iznuđenim ličnim podacima, najčešće seksualnih sadržaja, uključujući intimne slike, video snimke ili privatne razgovore.

Tako je 2020. tim *Lookout Threat Intelligence* otkrio špijunski paket pod nazivom *Goontact*, koji je preko ilegalnih sajtova za eskort usluge namamljivao korisnike i navodio ih da instaliraju zlonamerne aplikacije prikazane kao „bezbedne“ aplikacije za razmenu poruka.[46] Kada bi se instalirao, *Goontact* je eksfiltrirao lične podatke – SMS poruke, fotografije, kontakte, lokaciju – i koristio ih za iznudu. Žrtve su najčešće bile targetirane u Kini, Tajvanu, Južnoj Koreji i Japanu.

C. Spajver kao plaćeničko oružje u geopolitičkim sukobima

Spajver se koristi i kao oružje u nacionalnim i međunarodnim sukobima, a koriste ih plaćenički hakeri; često ih, mada ne uvek, angažuju države za pljačku ili nadzor određene grupe ljudi, kao i za hibridne kampanje destabilizacije. Na primer, kineska hakerska grupa APT15, navodno povezana sa kineskim vlastima,[47] koristila je špijunski alat *BadBazaar*[48] za targetiranje tibetanske i ujgurske zajednice.

Svi ovi slučajevi pokazuju kako se upotreba spajvera prostire daleko izvan navodno „legitimnih“ državnih aktivnosti – obično je to, u rukama službi za sprovođenje zakona ili obaveštajnih agencija, alat prinude i kontrole koji se koristi u javnom i privatnom domenu, ali i kao sredstvo lične, korporativne ili državne represije.

---

[46] Korisnici su podsticani da instaliraju zlonamernu aplikaciju pod raznim izgovorima, poput rešavanja problema sa zvukom ili videom. *Lookout Threat Intelligence*, “Lookout Discovers New Spyware ‘Goontact’ Used by Sextortionists for Blackmail,” decembar 2020. https://www.lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-goontact-used-by-sextortionists-for-blackmail

[47] *ZDNet*, “Connection Discovered Between Chinese Hacker Group APT15 and Defense Contractor,” 2020. https://www.zdnet.com/article/connection-discovered-between-chinese-hacker-group-apt15-and-defense-contractor/

[48] *Lookout Threat Intelligence*, “BadBazaar: Surveillanceware Used by APT15 to Target Tibetan and Uyghur Communities,” januar 2024. https://www.lookout.com/threat-intelligence/article/badbazaar-surveillanceware-apt15

2.3 Državna upotreba komercijalnog spajvera

Mnogi skandali vezani za državnu upotrebu spajvera obuhvataju programe kao što su *Pegasus*, *Graphite* ili *Predator*, koje razvijaju i prodaju privatni dobavljači, a koji imaju posebno zabrinjavajuće kapaciteta:[49]

→ Neograničen pristup podacima: Ovi komercijalni alati bez ograničenja pristupaju i izvlače sve istorijske i podatke u realnom vremenu.

→ Neproverljivost upotrebe: Ne ostavljaju jasne zapise o vremenu ili učestalosti infekcija, niti o tome koje podatke su preuzeli i gde su ih poslali.

→ Sposobnost samouništenja: Mnogi špijunski alati dizajnirani su tako da posle upotrebe sami obrišu tragove, što otežava forenzičku analizu i utvrđivanje odgovornosti.

→ Stalna kontrola: Spajver stvara „nevidljivo prisustvo“ koje prosečan korisnik ne može da otkrije ili ukloni, pa se može dugo zadržati na uređaju.

→ Vojni dizajn: Ovi alati su istorijski razvijani za vojne svrhe, a sada se koriste i u civilnim kontekstima.

Problem nije samo u tehničkim kapacitetima tih alata, već i u tome što nikada nisu zamišljeni da rade u zakonskim okvirima koji poštuju prava. Njihov razvoj i upotreba na okupiranim palestinskim teritorijama,[50] u kontekstu vojne okupacije, jasan je primer.

Iluzija o „dobrom“ spajveru

Ideja da može postojati „dobar spajver koji poštuje prava“ suštinski je pogrešna, jer sama priroda savremenog spajvera – njegov neograničen i tajni pristup uređajima, eksploatacija ranjivosti, narušavanje integriteta uređaja i njegovo vojno poreklo – direktno je u suprotnosti sa principima transparentnosti i odgovornosti i ne ispunjava standarde procene uticaja na osnovna prava. Prema sudskoj praksi Evropskog suda za ljudska prava,[51] svaki ciljani nadzor, zbog

---

[49] Ovo nije konačan popis i treba da istakne neke posebne pretnje po ljudska prava koje donose špijunski alati. Kao što smo već pomenuli, svemoćni pristup, ili bilo koja druga od navedenih sposobnosti, nije obavezna karakteristika spajvera. Špijunska tehnologija može imati ograničen pristup uređaju, ali i dalje može spadati pod definiciju 2.1 a time i obuhvaćen našim pozivom za zabranu.

[50] *The New Arab*, “How AI, Big Tech, and Spyware Power Israel’s Occupation,” 2023. https://www.newarab.com/analysis/how-ai-big-tech-and-spyware-power-israels-occupation

[51] „…u skladu sa praksom Evropskog suda za ljudska prava o ciljanom nadzoru, u pogledu zakonitosti, legitimiteta, nužnosti i proporcionalnosti bilo koje mere nadzora.“ *Council of Europe*, “Pegasus and Similar

posledica koje ima na ljudska prava, mora biti zasnovan na jasnom pravnom okviru, podložan nezavisnoj kontroli i strogoj proveri neophodnosti i proporcionalnosti. Međutim, spajver, po samom dizajnu, ne može da ispuni te zahteve.

Pojedini stručnjaci za ljudska prava razmatrali su kakve bi kapacitete spajver trebalo da ima, i na koji način bi trebalo da bude primenjen, da bi to bilo u skladu sa ljudskim pravima i uz *ex ante* zaštitne mere:[52]

→ mogućnost ciljanja samo vrlo specifičnih podataka („hirurška ekstrakcija podataka“), umesto automatskog praćenja i snimanja svih podataka i metapodataka;

→ izbegavanje automatskog pristupa podacima o kontaktima ciljanih osoba, osim ako je opravdano;

→ ugrađeni mehanizmi za sprečavanje štetne upotrebe, kao što su sistemi za označavanje i „prekidači za isključenje“ u slučajevima očigledne zloupotrebe;

→ beleženje svih radnji operatera u proverljivom, trajnom zapisu.

Realnost je da takva tehnologija danas ne postoji i da ostaje tehnički i praktično neizvodljiva. Štaviše, oslanjala bi se na poverenje u aktere koji su po svojoj prirodi skloni delovanju u senci. Ne postoje ni ekonomski ni politički podsticaji, ni za dobavljače ni za države, da razvijaju takva tehnička ograničenja. Konačno, oslanjanje samo na tehnička rešenja suštinski je neadekvatno za rešavanje složenih političkih pitanja, poput širokog spektra kršenja ljudskih prava kroz državnu upotrebu spajvera.

Pojam „spajvera usklađenog s ljudskim pravima“ stoga nije realističan put.

2.4 Preporuke javnih politika Evropskoj komisiji

Iako nacionalna bezbednost ostaje isključiva odgovornost država članica prema članu 4(2) Ugovora o Evropskoj uniji, to ne isključuje delovanje EU u donošenju zakona o spajveru. Pre

---

Spyware and Secret State Surveillance”, 2024. https://rm.coe.int/pegasus-and-similar-spyware-and-secret-state-surveillance/1680ac7f68rorism; “Position Paper on Global Regulation of Counter-Terrorism Spyware Technology Trade”, decembar 2022. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

[52] Ovaj sveobuhvatni spisak kapaciteta sastavio je specijalni izvestilac UN-a za borbu protiv terorizma: *UN Special Rapporteur on Counter-Terrorism*, “Position Paper on Global Regulation of Counter-Terrorism Spyware Technology Trade”, decembar 2022. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

svega, kao što je Evropska komisija nedavno navela, nacionalna bezbednost ne može biti opšte opravdanje, jer mora da ispuni specifičan visok prag.[53] Štaviše, razvoj, proizvodnja, marketing, prodaja, izvoz i upotreba spajvera direktno utiču na funkcionisanje unutrašnjeg tržišta, zaštitu osnovnih prava zagarantovanih Poveljom, zaštitu podataka, sajber bezbednost i spoljašnje odnose EU, što su sve oblasti koje jasno spadaju u nadležnost EU. Potpuna zabrana spajvera ne bi se mešala u prerogative nacionalne bezbednosti država članica, već bi uspostavila jedinstvena pravila kako bi se sprečilo širenje i zloupotreba ovih alata unutar i izvan Unije.

EDRi poziva na potpunu zabranu razvoja, proizvodnje, reklamiranja, prodaje, izvoza i upotrebe spajvera kao jedinog prihvatljivog rešenja u skladu sa ljudskim pravima.

1. Potpuna zabrana spajvera. Evropska komisija treba, što je hitnije moguće, da predloži potpunu zabranu razvoja, proizvodnje, reklamiranja, prodaje, izvoza i upotrebe spajvera.

2. Pravno čvrsto utemeljena definicija spajvera. Ova zabrana mora biti zasnovana na jasnoj i primenjivoj definiciji spajvera, fokusirajući se na njegove osnovne karakteristike i funkcionalnosti, a ne na njegov marketing ili nameravanu upotrebu. Samo takav sveobuhvatan pristup može sprečiti zloupotrebu, obezbediti pravnu sigurnost i podržati osnovna prava zagarantovana Poveljom o osnovnim pravima Evropske unije.

3. Sveobuhvatan opseg koji pokriva sve aktere. Zabrana mora obuhvatiti sve javne i privatne aktere koji deluju unutar EU ili podležu njenoj jurisdikciji. Ne sme se ograničiti na alate koje države koriste u kontekstu sprovođenja zakona ili nacionalne bezbednosti, već mora obuhvatiti i komercijalni spajver koji se prodaje za druge namene, uključujući korporativni i privatni nadzor.

3. Zloupotreba na prodaju: kako stati na kraj širenju komercijalnog spajvera

Tržište komercijalnog spajvera omogućava državama vrlo invazivne kapacitete za nadzor bez potrebe da ih same razvijaju. Sve veći broj privatnih kompanija gradi i prodaje ovakve alate, ponekad malom broju državnih aktera, a ponekad desetinama njih. Ovi akteri posluju u pravno i

[53] Prema Sudu pravde EU, pojam „nacionalna bezbednost“ odnosi se na „primarni interes zaštite osnovnih funkcija države i temeljnih interesa društva i obuhvata sprečavanje i kažnjavanje aktivnosti koje mogu ozbiljno destabilizovati osnovne ustavne, političke, ekonomske ili društvene strukture zemlje, a posebno direktno ugroziti društvo, stanovništvo ili samu državu, poput terorističkih aktivnosti“. *EU Commission*, “Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)”, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

etički sivoj zoni: formalno su privatni, često sastavljeni od bivših vojnih kadrova, i duboko povezani sa bezbednosnim strukturama.

Pošto su privatno vlasništvo, komercijalne firme koje prave spajver pre svega slede profitni motiv. U praksi, to znači poslovanje u tajnosti, eksploataciju ljudskih prava radi zarade i omogućavanje masovnih kršenja prava širom različitih jurisdikcija. Industrija spajvera nije samo inherentno štetna po svojim posledicama, već je opasna po samom dizajnu. Njen poslovni model zasniva se na zloupotrebi ranjivosti softvera, praksi koja slabi sajber bezbednost svih nas. Kršenja ljudskih prava ne dešavaju se samo u trenutku kada se alat upotrebljava, već tokom čitavog njegovog životnog ciklusa – od razvoja do marketinga, prodaje i post-prodajne „podrške".

3.1 Problem širenja: kako je komercijalno tržište učinilo spajver jeftinijim i dostupnijim

Provaljivanje u uređaje nikada nije bilo jednostavan zadatak za državne organe. Operativni plan upada obično podrazumeva potragu za ranjivostima u digitalnoj infrastrukturi (hardveru, softveru i mrežama), razvoj eksploita i špijunskih implantata, kao i identifikaciju odgovarajućih vektora napada. To zahteva značajna finansijska sredstva, vreme i stručnost, pre nego što se ciljani sistem uspešno kompromituje. Zbog toga postoji velika razlika u kapacitetima različitih država u ovoj oblasti; neke imaju naprednije tehnike, dok druge zaostaju.

Pojava i ekspanzija tržišta komercijalnog spajvera značajno utiču na ovaj jaz.[54] Kupovina „gotovog" softvera sada je relativno jeftina – naročito za državne aktere. Prema izveštajima medija, *Pegasus* košta nešto više od milion dolara za deset meta.[55]

Britanska obaveštajna, bezbednosna i sajber agencija izvestila je da je više od 80 država kupilo spajver i „upozorila da proliferacija ovih komercijalnih hakerskih alata i usluga dodatno snižava prag za ulazak i državnih i nedržavnih aktera u sajber prostor".[56] To je u skladu sa podacima

---

[54] Navodi se da izraelska *NSO Group* za klijente ima 60 vladinih službi u 40 zemalja. *The Washington Post*, "On the list: Ten prime ministers, three presidents and a king", 20. juli 2021. https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/

[55] Po cenovniku iz 2016, list *New York Times* izvestio je da je *NSO Group* u to vreme naplaćivala svojim klijentima 650.000 dolara za infiltraciju na 10 uređaja, plus naknadu za instalaciju od 500.000 dolara. *New York Times*, "How Spy Tech Firms Let Governments See Everything on a Smartphone", 2. septembar 2016. https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smart-phone.html

[56] *The Record*, "More than 80 countries have purchased spyware, British cyber agency warns", 19. april 2023. https://therecord.media/spyware-purchased-by-eighty-countries-gchq-warns. Svesni smo da, kao članica saveza "Pet očiju" i kao jedna od retkih država na svetu sa dovoljno kapaciteta i resursa za razvoj

Carnegijevog[57] globalnog inventara komercijalnog spajvera i digitalne forenzike, koji pokazuju da su 74 zemlje nabavile ovakve alate.

Države koje ranije nisu imale resurse ni kapacitete da samostalno razvijaju ovakve tehnologije (uključujući diktatorske ili represivne režime) sada mogu da se okrenu industriji komercijalnog nadzora da bi sprovodile nezakonit nadzor uz pomoć spajvera.

S druge strane, komercijalni spajver postao je veoma unosan biznis koji generiše oko 12 milijardi dolara godišnje.[58] Na primer, izraelsku firmu *Paragon* 2024. godine kupila je investiciona kompanija za oko 900 miliona dolara.[59] Uporedo s tim, raste tržište ranjivosti,[60] uz stalno rastuću potražnju. Startap *Crowdfense* godinama podiže cene svojih eksploita „nultog-dana“:[61] između 5 i 7 miliona dolara za *iPhone* ranjivosti; do 5 miliona za Android telefone; oko 3 do 3,5 miliona za *Chrome* i *Safari*; od 3 do 5 miliona za *WhatsApp* i *iMessage*. To je stvorilo izuzetno unosne prilike za razvoj i prodaju spajvera.[62]

Privatne kompanije stoje iza najsofisticiranijih alata za hakovanje i nadzor koji su trenutno prisutni na tržištu i time predstavljaju ozbiljnu pretnju kolektivnoj bezbednosti i privatnosti na internetu. Međutim, nekontrolisano širenje ovakvih oružja[63] i normalizacija njihove upotrebe predstavljaju odgovornost država, koje nisu preduzele mere da eliminišu profitne podsticaje za ovo tržište „upada kao usluge“. Na očigledan primer odsustva kontrole ukazuje Googlova grupa za analizu pretnji, koja je pratila 40 komercijalnih dobavljača: „Iako ovi dobavljači tvrde da pažljivo proveravaju svoje klijente i upotrebu, sa obećanjem da se alati koriste samo protiv

---

sopstvenih hakerskih tehnika, Ujedinjeno Kraljevstvo ima snažan interes da zadrži ovu komparativnu prednost i stoga brine što su i druge zemlje sada u stanju da nabave slične kapacitete za nadzor.

[57] *Mendeley Data* Feldstein, S.; Kot, B. “Global Inventory of Commercial Spyware & Digital Forensics”, 2023. https://data.mendeley.com/datasets/csvhpkt8tm/10

[58] *Carnegie Endowment for International Peace*, “Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses,” 14. mart, 2023. https://carnegieendowment.org/research/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses

[59] *Calcalistech*, “Spyware startup Paragon acquired for up to $900M by investment firm AE”, 2024. https://www.calcalistech.com/ctechnews/article/s1ucev64kg

[60] Vidi *Rečnik pojmova*.

[61] Vidi *Rečnik pojmova* i: *EDRi*, “State access to encrypted data”, oktobar 2022. https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf

[62] *TechCrunch*, “Price of zero-day exploits rises as companies harden products against hackers”, 6. april 2024. https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/. U tekstu se primećuje da “*Crowdfense* trenutno nudi najviše javno poznate cene dosad”, osim za jednu rusku kompaniju.

[63] Namerno koristimo ovaj izraz s obzirom na ulogu koju spajver ima u ozbiljnim represivnim i ofanzivnim operacijama, poput ubistava Džamala Kašogdžija i Sesilija Pinjede Birta – vidi: *The Guardian*, “Revealed: murdered journalist’s number selected by Mexican NSO client”, 18. juli 2021. https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto

kriminalaca i terorista, ono što smo iznova uočavali jeste da vlade zapravo koriste alate u svrhe koje su u sukobu sa demokratskim vrednostima.“[64]

Dok se EU ponosi svojim naprednim pravilima zaštite podataka i privatnosti, izveštaji ukazuju na zabrinjavajuće povoljne poslovne uslove koje Unija nudi dobavljačima spajvera.[65] Evropski parlament je 2023. godine naveo da „mnogi proizvođači i dobavljači spajvera jesu ili su bili registrovani u jednoj ili više država članica“, navodeći kao primere *Thalestris Limited* (matičnu kompaniju firme *Intellexa*) u Irskoj, Grčkoj, Švajcarskoj i na Kipru, *DSIRF* u Austriji, *QuaDream* na Kipru, *Amesys* i *Nexa Technologies* u Francuskoj, i *FinFisher* u Nemačkoj.[66] Danas se toj listi mogu dodati kompanije poput Paragona u Nemačkoj[67] ili kompanije *Paradigm Shift*, *Palm Beach Networks* i *Epsilon*, sa sedištem u Barseloni.[68]

To je i razlog iz kog je Italija poslednjih godina na meti kritike, budući da je ugostila šest poznatih proizvođača spajvera u Evropi.[69] U tom kontekstu, jedno istraživanje je otkrilo ulogu koju javne nabavke imaju u razvoju štetnog tržišta spajvera, kao i u dostupnosti i raznovrsnosti alata.[70] S druge strane, tužilački organi u Italiji odobravaju znatno više mera nadzora godišnje nego druge evropske službe.[71] Drugim rečima, čini se da ponuda oblikuje potražnju.

Tokom 2024. mediji su otkrili da su izraelski hakeri preselili poslovanje i osnovali nove kompanije za spajver u Kataloniji.[72] Jedan od razloga za ovo preseljenje u Evropu jeste pooštravanje izvoznih pravila u Izraelu, nakon skandala vezanih za NSO Group. Kako se navodi, „kompanijama je sada teže da izvoze spajver iz Izraela u ostatak sveta, uključujući EU,

---

[64] *The Record*, “Commercial spyware on the agenda as UN Security Council members meet”, 2024. https://therecord.media/commercial-spyware-meeting-un-security-council-members. Šejn Hantli je takođe rekao: “Udarne naslove zauzimaju dobro poznate kompanije koje prodaju spajver, kao što je *NSO Group* … ali desetine manjih dobavljača doprinose problemu”.
[65] *Politico*, “How Europe Became the Wild West of Spyware”, 25. oktobar 2023. https://www.politico.eu/article/how-europe-became-wild-west-spyware/
[66] *European Parliament*, “Recommendation of 15 June 2023 to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware (2023/2500(RSP))”, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html
[67] *Euractiv*, “EXCLUSIVE: Spyware firm behind new surveillance of journalists, civil society operates from the EU”, 2025. https://www.euractiv.com/section/tech/news/exclusive-spyware-firm-behind-new-surveillance-of-journalists-civil-society-operates-from-the-eu/
[68] *TechCrunch*, “How Barcelona became an unlikely hub for spyware startups”, 13. januar 2025. https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/
[69] *IrpiMedia*, “Italian spyware on the international market”, 21. mart 2023. https://irpimedia.irpi.eu/en-italian-spyware-on-the-international-market
[70] *IrpiMedia*, Ibid.
[71] *IrpiMedia*, Ibid.
[72] *Haaretz*, “’Expulsion to Spain’: Israeli Hackers Flock to Barcelona in Big Spyware Shift”, 26. decembar 2024. https://www.haaretz.com/israel-news/security-aviation/2024-12-26/ty-article/.premium/israeli-hackers-flock-to-barcelona-as-spyware-industry-shifts/00000193-fec4-df5b-a9b3-fec5d9dc0000

nego iz same Unije".[73] Dakle, u trenutku pisanja ovog izveštaja, EU nudi pogodnije uslove za ove kompanije zahvaljujući niskim trgovinskim barijerama unutar Unije i slabim kontrolama izvoza robe dvostruke namene. Umesto da to sprečava, regulativa EU zapravo podstiče širenje komercijalnog spajvera, koji se potom koristi za kršenje ljudskih prava širom sveta.

Razvoj spajvera oslanja se na tzv. ranjivosti „nultog dana" preko kojih se mete mogu inficirati neopaženo. Takve ranjivosti – koje ugrožavaju sve nas, jer se mogu iskoristiti protiv bilo koga, uključujući i same državne interese – ključne su za industriju spajvera. Paradoksalno, javna sredstva u velikoj meri podstiču tržište ranjivosti „nultog dana", ne samo kroz rast potražnje za komercijalnim spajverom, već i kroz direktne investicije u otkrivanje ranjivosti. Što se tiče potonjeg, neke vlade država članica EU izdvajaju deo svog budžeta za plaćanje istraživača bezbednosti kako bi pronašli ranjivosti „nultog dana" za eksploataciju i internu primenu spajvera. Na primer, kompanija *Zerodium* deluje kao posrednik između bezbednosnih istraživača i državnih institucija, uglavnom u Evropi i Severnoj Americi, garantujući međusobnu anonimnost učesnicima transakcije.[74] *Zerodium* trenutno nudi i do 2,5 miliona dolara za informacije o ranjivostima – znatno više nego što nude programi nagrade za bagove (*bug bounty*)[75] koje vodi industrija softvera. Javna sredstva koja danas posredno podržavaju ove transakcije *Zerodiuma* (i drugih posrednika u unosnoj trgovini informacijama o ranjivostima za eksploataciju) trebalo bi, gde god je to moguće, preusmeriti na otklanjanje ranjivosti pre nego što ih zloupotrebe maliciozni akteri.

Aktuelna pravna i politička situacija, u najboljem slučaju, ignoriše – a u najgorem, podstiče i podržava – dizajn, razvoj i upotrebu tehnologija komercijalnog spajvera. To se mora hitno promeniti kroz zabranu tržišta komercijalnog spajvera.

3.2 Neprihvatljivi rizici tržišta komercijalnog spajvera

„Time što ostavljaju ranjivosti [u računarskim sistemima] otvorenim, ili ih čak namerno stvaraju, oni koji pribegavaju hakovanju doprinose pretnjama po bezbednost i privatnost miliona korisnika, kao i šireg digitalnog informacionog ekosistema." (Izveštaj Kancelarije visokog komesara Ujedinjenih nacija za ljudska prava, 2022.)[76]

Industrija komercijalnog spajvera po svojoj prirodi predstavlja sistemsku pretnju ne samo ljudskim pravima, već i sajber bezbednosti, stabilnosti demokratije i globalnoj sigurnosti. Problem se ne odnosi samo na to kako se ovakav softver koristi, već i na to kako se on dizajnira

[73] *TechCrunch*, Ibid.
[74] *Zerodium*, "Zero-day Exploit Acquisition Platform", accessed 2025. https://zerodium.com
[75] Vidi *Rečnik pojmova*.
[76] *Office of the United Nations High Commissioner for Human Rights*, "The Right to Privacy in the Digital Age", 4. avgust 2022. https://docs.un.org/en/A/HRC/51/17

i kako funkcioniše industrija u celini. Od razvoja, do marketinga i upotrebe, poslovni model spajvera zasniva se na tajnosti, nekažnjivosti i eksploataciji ranjivosti.

A. Tržište ranjivosti kao pretnja sajber i nacionalnoj bezbednosti

Spajver funkcioniše pre svega tako što iskorišćava ranjivosti. To podrazumeva namerno stvorene propuste, kao što je državni „propust" (*backdoor*), ali i one kupljene na tržištu koje se razvilo oko eksploatacije bezbednosnih rupa, poput „nultog dana" i drugih nezakrpljenih ranjivosti. Umesto da ih isprave, prodavci spajvera – a često i same države – odlučuju da ih pretvore u oružje. Time korisnici, uključujući i državne službenike, ostaju trajno ranjivi.

Nedavni izveštaji potvrđuju koliko je opasan pristup obaveznog „propusta": kineska hakerska grupa *Salt Typhoon* uspela je da pristupi „propustima" napravljenim za zakonito presretanje i održavala je pristup kritičnoj američkoj telekomunikacionoj infrastrukturi „mesecima ili duže", sa nepoznatim posledicama.[77] Takav opasan ishod nije izuzetak, već je ugrađen u dizajn.

Uticaj komercijalnih dobavljača spajvera na tržište ranjivosti je očigledan: oni ne samo da ga koriste, već ga i aktivno podstiču. Prema podacima Googleove grupe za analizu pretnji (*Threat Analysis Group*, TAG), dvadeset od dvadeset pet ranjivosti „nultog dana" identifikovanih 2023. godine iskoristili su upravo komercijalni prodavci spajvera.[78] Ova zapanjujuća brojka jasno pokazuje da je komercijalni spajver glavni pokretač potražnje za eksploatacijom ranjivosti.

Rezultat je sistemski slom bezbednosti, gde vlade i privatni akteri podstiču nesigurnost umesto da jačaju digitalni ekosistem. Umnožavanje komercijalnih prodavaca spajvera povećava broj nepoznatih ranjivosti u digitalnim sistemima, što predstavlja direktnu i ozbiljnu pretnju po bezbednost i privatnost svih nas. To uključuje i državne zvaničnike i vladine administracije koji se i sami oslanjaju na iste te digitalne sisteme u svom radu da zaštite poverljive i tajne informacije.

[77] *Techdirt*, "A 25-Year-Old Is Writing Backdoors Into The Treasury's $6 Trillion Payment System. What Could Possibly Go Wrong?", 5. februar 2025. https://www.techdirt.com/2025/02/05/a-25-year-old-is-writing-backdoors-into-the-treasurys-6-trillion-payment-system-what-could-possibly-go-wrong
[78] *The Record*, "Commercial spyware on the agenda as UN Security Council members meet", 2024. https://therecord.media/commercial-spyware-meeting-un-security-council-members

Potreba za programima nagrade za bagove

Ova zabrinjavajuća dinamika takođe potiskuje etička istraživanja u oblasti sajber bezbednosti. Brokeri ranjivosti poput kompanija *Zerodium* i *Crowdfense* nude milione dolara za eksploite „nultog dana“,[79] višestruko veće iznose od javnih programa nagrada za bagove.[80]

Na taj način se programerima uskraćuje prilika da zakrpe propuste, jer istraživači imaju mnogo veću finansijsku korist da uočene ranjivosti zadrže u tajnosti nego da ih prijave. Posledično, bezbednost država i građana zavisi od spremnosti proizvođača i dobavljača da pronađu ranjivosti i brzo izdaju bezbednosne zakrpe.

Ova industrija vredna milijarde dolara[81] urušava same temelje sajber bezbednosti time što ostavlja ranjivosti otvorenim, legitimizuje ofanzivna sajber oružja, a kontrolu autsorsuje privatnim akterima koji nemaju nikakav interes da vode računa o pravima ili o otpornosti sistema.

EU ne sme da doprinosi slabljenju sajber prostora

Naravno, ako EU zabrani ovo tržište kompanije i programeri će se preseliti na drugo mesto. Oslanjanje industrije spajvera na jurisdikcijsku arbitražu omogućava dobavljačima da iskorišćavaju regulatorne praznine, perpetuirajući tržište ranjivosti.[82] Preseljenjem u zemlje sa slabim nadzorom, ove kompanije mogu da nastave trgovinu eksploitima uz minimalnu odgovornost. Međutim, EU to ne može da koristi kao izgovor za popustljivost, budući da to tržište potkopava njen unutrašnji bezbednosni i globalni sajberbezbednosni scenario. EU ipak ima određenu moć: kompanije biraju lokaciju i prema tome gde su njihovi programeri voljni da žive. Kada bi ovim kompanijama bilo zabranjeno da se nastane u Evropi, to bi ih učinilo manje privlačnim za programere.

Učestvujući aktivno ili pasivno u tržištu ranjivosti – kroz odsustvo jasnih regulatornih procesa i tolerisanje investitora – EU sama sebi nanosi štetu i slabi sopstvenu bezbednost.

---

[79] *TechCrunch*, “Price of zero-day exploits rises as companies harden products against hackers”, 6. april 2024. https://techcrunch.com/2024/04/06/price-of-zero-day-exploits-rises-as-companies-harden-products-against-hackers/
[80] Vidi *Rečnik pojmova*.
[81] Vidi odeljak 3.1 za podatke o prihodima tržišta.
[82] *Atlantic Council*, “Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights”, 2023. https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them

B. Problemi transparentnosti i pravne odgovornosti

Kada je reč o obavezama u oblasti ljudskih prava i uprkos deklarativnoj posvećenosti korporativnoj odgovornosti (kao što su Vodeći principi UN za poslovanje i ljudska prava), komercijalni dobavljači spajvera posluju gotovo potpuno bez nadzora i u uslovima potpune netransparentnosti.[83]

Industriji spajvera pogoduje rad u senci. Dobavljači prikrivaju svoje alate pod nejasnim etiketama poput „zakonitog pristupa" ili „istraživačkih tehnologija"[84] i operišu zaštićeni mrežama fantomskih firmi kroz koje se kanališu investicije i izbegava pravna odgovornost.[85] Zahvaljujući tome, gotovo je nemoguće uspostaviti transparentnost, a većinu informacija koje imamo otkrivaju istraživački novinari. Pored toga, investitori u potpunosti podržavaju netransparentnu ekonomiju spajvera. Nedavna akvizicija kompanije *Paragon* od strane američke privatne investicione firme za čak 900 miliona dolara pokazuje ogroman obim ovog modela nadzora kao usluge.[86] Profit pokreće širenje ovog tržišta, a ne bezbednost ili pravda.

Dodatni problem predstavlja složenost utvrđivanja odgovornosti: često nije jasno ko snosi odgovornost za šta u međunarodnom lancu proizvodnje, što praktično onemogućava žrtve da ostvare pravnu zaštitu i odgovorne privedu pravdi.[87]

3.3 Kako važeća regulativa EU omogućava širenje komercijalnog spajvera?

Dok pratimo trendove preseljenja i uspostavljanja kompanija u Evropi, potrebno je da sagledamo postojeći zakonodavni okvir EU kako bismo razumeli pravne uslove pod kojima tržište komercijalnog spajvera cveta na teritoriji Unije.

[83] *UN Human Rights Council*, "Report on Business and Human Rights", A/HRC/41/25, maj 2019. https://undocs.org/A/HRC/41/25
[84] *Atlantic Council*, Ibid.
[85] *Politico*, "Europe's Pegasus scandal: EU probe targets NSO", 2022. https://www.politico.eu/article/europe-pegasus-spyware-eu-probe-nso/
[86] *The Record*, "Paragon bought by U.S. private equity", 2024. https://therecord.media/paragon-bought-private-equity-american
[87] *UN Special Rapporteur on Counter-Terrorism*, "Position Paper on Global Regulation of Counter-Terrorism Spyware Technology Trade", decembar 2022. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

A. Uredba o robi dvostruke namene i njeni nedostaci

Od 1994. godine, EU reguliše izvoz „robe dvostruke namene“ – dobara, softvera i tehnologija koje se mogu koristiti i u civilne i u vojne svrhe.[88] Poslednje izmene zakona usvojene su 2021. godine. U ovu kategoriju formalno spadaju i alati za sajber nadzor,[89] uključujući „intruzivni softver“, „softver za nadzor komunikacija“ i „forenzičke alate“.[90] Evropska komisija je 2024. izdala posebne smernice o tome kako se Uredba primenjuje na izvoz sredstava za sajber nadzor, a samim tim i na izvoz spajvera.[91]

Međutim, uprkos tim smernicama, Uredba u osnovi nije u stanju da reši problem proliferacije komercijalnog spajvera, i to iz sledećih razloga:

1. Ograničen obim: samo kontrola izvoza. Uredba se primenjuje isključivo na izvoz van EU. Takođe, režim EU nema ekstrateritorijalni domet, što dodatno ograničava kontrolu proliferacije spajvera preko filijala ili preprodavaca.

2. Unutrašnja trgovina je slobodna. Samo proizvodi navedeni u Aneksu IV – Vrlo osetljiva roba, podležu licenciranju kada se izvoze iz jedne države članice u drugu. Dakle, unutrašnje tržište komercijalnog spajvera, koje je deo Aneksa I – Lista robe dvostruke namene, trenutno je potpuno slobodno, bez regulacije i bez obaveznog licenciranja.

3. Slaba primena pravila i kontrola. Smernice Komisije iz 2024. ne uvode snažne zaštitne mere. Konkretno:

→ Kontrola izvoza odnosi se samo na proizvode koji su izazvali ili mogu izazvati „ozbiljna kršenja ljudskih prava ili međunarodnog humanitarnog prava“ u trećim zemljama. To stvara veliku prazninu u slučajevima kada je do štete došlo unutar EU. U načelu, kako ističu mnoge organizacije civilnog društva, tekst ne pruža kriterijume za tumačenje šta znači „ozbiljno“ kršenje ljudskih prava, dok postojećim kriterijumima za vojnu tehnologiju ili opremu nedostaju strogo tumačenje, primena i kontrola širom EU.[92]

---

[88] *European Union*, “Regulation (EU) 2021/821”, https://eur-lex.europa.eu/eli/reg/2021/821/oj

[89] Michel, Quentin et al., “A Decade of Evolution of Dual-Use Trade Control Concepts”, European Studies Unit, University of Liège, 2020. https://orbi.uliege.be/bitstream/2268/246711/1/full.pdf

[90] Terminologija za delove opreme za sajber nadzor apdejtovana je 2024. *European Commission*, “RECOMMENDATION (EU) 2024/214 of 10 January 2024 on guidelines setting out the methodology for data gathering and processing for the preparation of the annual report on the control of exports, brokering, technical assistance, transit and transfer of dual-use items”, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32024H0214

[91] *European Commission*, “Guidelines for Cyber-Surveillance Exporters”, 16. oktobar 2024. https://policy.trade.ec.europa.eu/news/commission-publishes-guidelines-cyber-surveillance-exporters-2024-10-16_en

[92] *Access Now*, “Analysis of EU Surveillance Tech Export Rules”, 2021. https://www.accessnow.org/wp-content/uploads/2021/03/Analysis-EU-Surveillance-Tech-Export-Rules.pdf

→ Čak i kada takvi rizici postoje, ne postoji automatski mehanizam za obustavu izvoza, dok su izvoznici obavezani tek da sami procene rizik od kršenja ljudskih prava.

4. Sprovođenje pravila je takođe slabo delimično zato što su odluke o implementaciji i izdavanju licenci prepuštene državama članicama, kao i primena „uopštene klauzule o ljudskim pravima“,[93] pa ne postoje zajednički kriterijumi u vezi s tim.

Vasenarski aranžman (*Wassenaar Arrangement*),[94] prema kom se sačinjavaju kontrolne liste u skladu sa regulativom EU o dvostrukoj nameni, takođe je vrlo problematičan. Opisuje se kao neefikasan[95] – pod snažnim uticajem geopolitike, pri čemu ključni akteri poput Kine uopšte ne učestvuju, a zemlje poput Rusije sprečavaju svako ažuriranje. U trenutku pisanja ovog dokumenta, Aranžman je i dalje neobavezujuća lista koja je zamrznuta već godinama.

Jedan od lakših prvih koraka za unapređenje trenutne situacije bilo bi strože sprovođenje Uredbe o robi dvostruke namene i smernica Komisije iz 2024. godine, uz striktno tumačenje u skladu sa ljudskim pravima. Drugo, kontrole i nadzor mogli bi da se pojačaju dodavanjem spajvera u Aneks IV, čime bi i unutrašnja trgovina ovim alatima bila podvrgnuta licenciranju.

Međutim, imajući u vidu njen uski obim, slabe interne kontrole i odsustvo sprovođenja, Uredba o robi dvostruke namene nije prikladan pravni instrument za efikasno regulisanje tržišta komercijalnog spajvera, te ne sprečava snabdevanje autoritarnih režima širom sveta ovim alatima.[96]

B. Propisi o oružju – propuštena prilika?

Države bi trebalo da tretiraju spajver na sličan način kao konvencionalno oružje,[97] a da regulišu njegovu komercijalnu proliferaciju strogim pravnim režimom.

---

[93] *BAFA*, “Leaflet on Art. 5 of the EU Dual-Use Regulation (Regulation (EU) 2021/821)” https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_leaflet_art-5_eu-dual-use-regulation.pdf?__blob=publicationFile&v=2

[94] Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, https://www.wassenaar.org

[95] *Austin Lewis*, “The Effectiveness of the Wassenaar Arrangement as the Non-Proliferation Regime for Conventional Weapons”, 2015. https://stacks.stanford.edu/file/druid:mz349xm4602/The%20Effectiveness%20of%20the%20Wassenaar%20Arrangement%20as%20the%20Non-proliferation%20Regime%20for%20Conventional%20Weapons%20-%20Austin%20Lewis.pdf

[96] *Spiegel*, “The Predator Files: European Spyware Consortium Supplied Despots and Dictators”, 2023. https://www.spiegel.de/international/business/the-predator-files-european-spyware-consortium-supplied-despots-and-dictators-a-2fd8043f-c5c1-4b05-b5a6-e8f8b9949978

[97] Kako je pomenuto u fusnoti 72, spajver se može izjednačiti sa oružjem zbog svog ozbiljnog i često nepovratnog uticaja na žrtve: korišćen je za suzbijanje kritike, razbijanje demokratske opozicije i doprineo je teškim kršenjima ljudskih prava, uključujući proizvoljna hapšenja, pa čak i ubistva.

EU je vremenom razvila okvir za trgovinu i civilnim i vojnim oružjem. Civilno vatreno oružje obuhvaćeno je Direktivom o oružju (Direktiva (EU) 2021/555),[98] koja uspostavlja određene kontrolne mehanizme za nabavku, posedovanje i transfer unutar EU. Vojno oružje uređeno je Zajedničkim stavom Saveta 2008/944/ZSBP,[99] koji teoretski nalaže državama članicama EU da procenjuju svaki izvoz prema kriterijumima kao što su ljudska prava, bezbednost i regionalna stabilnost. Ovaj okvir obuhvata i „Zajedničku vojnu listu", u kojoj se „spajver" ne navodi izričito, ali sadrži kategorije (poput „intruzivni softver") koje bi mogle obuhvatiti i spajver.[100]

Spajver vodi poreklo iz vojnog obaveštajnog rada i okupacionih praksi, posebno u kontekstima poput okupiranih palestinskih teritorija,[101] i koristi se u ratnim zonama[102] i protiv branilaca ljudskih prava i populacija koje teže oslobođenju od okupacionih snaga.[103] Međutim, integracija spajvera u postojeći okvir vojnog izvoza imala bi slične nedostatke kao i Regulativa o dvostrukoj nameni:

→ Unutrašnja trgovina oružjem u EU ostaje bez sistema licenci – samo se izvoz u zemlje izvan EU kontroliše ovim zakonodavstvom; unutrašnja trgovina vojnim sredstvima u načelu ne zahteva licence,[104] osim ako se ne primenjuju nacionalna pravila ili bezbednosni izuzeci.

→ Odgovornost za izdavanje izvoznih dozvola leži na državama članicama, na osnovu „prethodnog znanja o krajnjoj upotrebi u zemlji konačnog odredišta". U praksi, države članice EU često odobravaju takve dozvole čak i kada postoje uverljivi rizici od kršenja ljudskih prava.[105]

---

[98] *European Union*, "Directive (EU) 2021/555", https://eur-lex.europa.eu/eli/dir/2021/555/oj/eng
[99] *European Union*, "Council Common Position 2008/944/CFSP" https://eur-lex.europa.eu/eli/compos/2008/944/oj/eng
[100] *European Union*, "Common Military List of the European Union", adopted on February 2020 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XG0313(07)
[101] *Chatham House*, "Review: Why Israel tests its spyware on Palestinians", novembar 2023. https://www.chathamhouse.org/publications/the-world-today/2023-06/review-why-israel-tests-its-spyware-palestinians
[102] *Access Now*, "Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict", maa 2023. https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict
[103] *Amnesty International*, "Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict", 2021 https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2
[104] Transfer vojne opreme unutar EU regulisan je Direktivom 2009/43/EC. Licenca za izvoz nije potrebna za transfere unutar EU za mnoge vojne stavke ako dobavljač koristi opštu ili globalnu licencu za transfer.
[105] *Chiara Bonaiutti*, "Arms Transfers and Human Rights: Assessing the Impact and Enforcement of the EU Common Position on Arms Exports in a Multilevel Analysis", 2024. https://www.researchgate.net/publication/366958609_Article_Arms_Transfers_and_Human_Rights_Assessing_the_Impact_and_Enforcement_of_the_EU_Common_Position_on_Arms_Exports_in_a_Multilevel_Analysis

C. Pall Mall proces

Pall Mall proces,[106] koji su u februaru 2024. godine pokrenuli Ujedinjeno Kraljevstvo i Francuska, ima za cilj da se pozabavi „širenjem i neodgovornom upotrebom komercijalnih sajber intruzivnih kapaciteta (*commercial cyber intrusion capabilities*, CCICs)“.[107] Pažnja je usmerena na to „kako komercijalni spajver potkopava nacionalnu bezbednost, ljudska prava, međunarodni mir i stabilnost sajber prostora“.

Međutim, do prve polovine 2025. godine *Pall Mall* proces je proizveo samo dva neobavezujuća dokumenta: deklaraciju i kodeks prakse za države.[108] Mada su ovi dokumenti izraz dobre namere, njihova dobrovoljna priroda izaziva ozbiljne sumnje u pogledu njihove delotvornosti za suzbijanje zloupotreba ili uvođenje promena u politike i prakse u dvadeset pet država učesnica (od kojih su osamnaest članice EU). Štaviše, čini se i da legitimizuju određene vrste spajvera i slučajeve upotrebe.

Pored toga, *Pall Mall* proces predviđa i dobrovoljni kodeks prakse za dobavljače spajvera. Međutim, efikasna primena takvih kodeksa od strane dobavljača krajnje je neizvesna. Kako napominje jedna od kompanija koje učestvuju u procesu, „još uvek je pitanje kako će *Pall Mall* proces […] zapravo dopreti do onih čije ponašanje i postupci treba da se promene da bi se situacija zaista popravila“.[109]

Činjenica da je proces zapadno-centričan, predvođen Ujedinjenim Kraljevstvom i Francuskom, takođe ograničava globalno učešće; u trenutku pisanja ovog dokumenta, tek oko dvadeset država je potpisalo dobrovoljni kodeks. Kako se ističe u rezimeu konsultacija, manjak reprezentativnosti u procesu nosi rizik od obeshrabrivanja učesnika: „Ako se države ili akteri iz različitih regiona ne osećaju zastupljeno, to može dovesti do povlačenja i odustajanja.“[110]

---

[106] Ministry for Europe and Foreign Affairs (France), “The Pall Mall Process”, 2024. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of

[107] Prema Kodeksu prakse za države, „tržište za CCIC obuhvata širok spektar kompanija za sajber upade koje nude proizvode i usluge koje se neprestano razvijaju i diversifikuju, uključujući one za prodiranje u računarske sisteme ili ometanje u zamenu za komercijalnu korist i/ili objavljene pod licencom slobodnog i otvorenog koda, kao što su komercijalni softver za intruzivni nadzor (ponekad nazvan komercijalni špijunski softver), te tržište ranjivosti i eksploita“. *UK Government*, “The Pall Mall Process: Code of Practice for States”, https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states

[108] Ibid.

[109] *The Record*, “Pall Mall Process to tackle commercial hacking proliferation raises more concerns than solutions“, 2025. https://therecord.media/pall-mall-process-commercial-hacking-concerns

[110] Pall Mall Process, Consultation on good practices: summary report. 2025. https://assets.publishing.service.gov.uk/media/677e486ed721a08c00665555/Pall-Mall-Process-Consultation-Summary-Report.pdf

U svom sadašnjem obliku, *Pall Mall* proces rizikuje da drastično podbaci u odnosu na svoje ciljeve. Da bi zaista bio delotvoran, mora da prevaziđe dobrovoljne okvire i preraste u obavezujući, primenjiv sporazum koji se direktno bavi posledicama po ljudska prava koje izazivaju prakse komercijalnog spajvera. U suprotnom, ostaće diplomatska vežba odvojena od stvarnosti industrije i dubokih povreda prava koje prouzrokuje.

D. Da li su CRA i NIS2 korisna sredstva za regulisanje tržišta ranjivosti?

Kao odgovor na rastuće pretnje sajber bezbednosti, EU je uvela nove instrumente poput Zakona o sajber otpornosti (*Cyber Resilience Act*, CRA) i revidirane Direktive o bezbednosti mreža i informacija (NIS2). Mada oba propisa imaju cilj da ojačaju digitalni ekosistem i pruže rešenje za sistemske ranjivosti, ne dosežu nivo potreban za regulisanje tržišta komercijalnog spajvera.

CRA, usvojen 2024. godine, uvodi osnovne zahteve sajber bezbednosti za „proizvode sa digitalnim elementima“.[111] Zakon obavezuje proizvođače da zakrpe poznate ranjivosti, sprovode procene rizika i obezbede transparentnost u vezi sa integritetom softvera. CRA predstavlja značajan i pozitivan korak napred za digitalnu politiku EU – ali sadrži i neka suštinska ograničenja kada je reč o spajveru:

→ Isključenje iz obima primene: CRA se ne primenjuje na proizvode povezane sa nacionalnom bezbednošću ili odbranom. Time je izuzet spajver koji razvijaju ili koriste javni organi. Dobavljači komercijalnog spajvera često pozicioniraju svoje alate kao „sredstva za sprovođenje zakona“ ili „istraživačka rešenja“, čime se izuzimaju iz obima potrošačkih proizvoda.

→ Nedostatak sprovođenja u slučaju namernih ranjivosti: CRA je primarno usmeren na slučajne propuste i nemar. Ne obuhvata dobavljače koji namerno eksploatišu ranjivosti ili njima komercijalno trguju u ofanzivne svrhe. Jedna od mogućih mera bila bi da se istraži da li se CRA može iskoristiti za jačanje otpornosti uređaja na eksploite, kao i za zabranu proizvoda poput progoniteljskog softvera, koji su običnim potrošačima lako dostupni na tržištu. Međutim, ni to ne bi predstavljalo sveobuhvatno rešenje.

Direktiva NIS2, usvojena 2022. godine, proširuje obaveze u oblasti sajber bezbednosti za subjekte koji posluju u osamnaest sektora širom tržišta EU – uključujući digitalne usluge, energetiku, zdravstvo i javnu upravu. Ovaj propis uvodi strože zahteve za izveštavanje o incidentima, upravljanje rizicima i transparentnost lanca snabdevanja. Međutim, baš kao i CRA, ima ograničenu primenu kada je reč o spajveru:

→ Fokus na otpornost, a ne na zloupotrebu: NIS2 teži da spreči poremećaje u infrastrukturi, a ne da se bavi tajnim nadzorom pojedinaca ili kršenjem ljudskih prava.

[111] The CRA, explained https://www.cyberresilienceact.eu/the-cra-explained/

→ Nema posebnih pravila za tehnologije nadzora: Ne postoji obaveza za regulisanje dobavljača koji razvijaju alate kojima se narušava bezbednost ili eksploatišu ranjivosti.

→ Izuzeci za državnu upotrebu: Operacije u okviru nacionalne bezbednosti – što je način na koji se državna upotreba spajvera često predstavlja – isključene su iz obima direktive.

Mada su i CRA i NIS2 ključni za unapređenje digitalnog ekosistema EU, to nisu prikladni mehanizmi za regulisanje tržišta komercijalnog spajvera. Njihov fokus je na prevenciji rizika i jačanju otpornosti, dok je spajver namerna i sistemska pretnja koja cilja prava korisnika, njihovu bezbednost i digitalnu infrastrukturu. Takođe je važno istaći da oba teksta sadrže ogromne rupe zasnovane na izuzecima za nacionalnu bezbednost, što sprečava da ova dva propisa (kao i drugi pravni instrumenti EU) delotvorno i sveobuhvatno utiču na tržište spajvera.

E. Sankcije protiv dobavljača i investitora

Sankcije protiv dobavljača i investitora komercijalnog spajvera možda nisu dugoročno rešenje, ali mogu imati neke pozitivne kratkoročne efekte, poput onih koje je uvela Bajdenova administracija,[112] a koji mogu poslužiti kao koristan model za delovanje EU:

→ Odgovornost. Sankcije bar šalju poruku žrtvama da se teži uspostavljanju odgovornosti, a istovremeno prouzrokuju ekonomsku, operativnu i reputacionu štetu dobavljačima i investitorima, što može imati odvraćajući efekat.

→ Reforme korporativne politike. Suočene sa američkim sankcijama, neke kompanije su bile prinuđene da se prilagode. Na primer, kompanija *Sandvine*[113] je restrukturirala svoje poslovanje i bar tvrdi da je počela da „tretira ljudska prava kao prioritet“ pošto je Bajdenova administracija stavila ovu kompaniju na listu zabranjenih zbog isporuke tehnologije korišćene za masovni nadzor i cenzuru u Egiptu. Ovakve reakcije pokazuju da pritisak putem sankcija može dovesti makar do delimičnih promena u ponašanju dobavljača.

→ Povlačenje sa tržišta autoritarnih režima. U nekim slučajevima sankcije su direktno uticale na poslovne odluke. *Sandvine* je najavio povlačenje iz pedeset šest zemalja koje je označio kao „nedemokratske“ – uključujući i Egipat – navodeći da će prodaju ograničiti isključivo na demokratije. Iako ovaj pristup nije savršen (jer spajver krši ljudska prava i u demokratijama, a pristup se oslanja na tumačenje samog dobavljača šta se smatra demokratijom), ipak je doprineo smanjenju štete i usporavanju širenja.

---

[112] *Politico*, “Commerce Department blacklists dozens of groups over weapons-related violations”, 2024. https://www.politico.com/news/2024/10/21/commerce-dept-blacklist-groups-00184628.POLITICO
[113] *Reuters*, “U.S. removes Sandvine from trade restriction list after corporate reforms”, 2024. https://www.reuters.com/technology/us-removes-sandvine-trade-restriction-list-after-corporate-reforms-2024-10-21

→ Odvraćanje. Pravni postupci i stavljanje dobavljača na liste zabranjenih takođe služe kao važan faktor odvraćanja. Značajna presuda u slučaju *WhatsApp* protiv *NSO Group*, kada je sud utvrdio da je NSO prekršio zakone o hakovanju, uspostavila je presedan koji može obeshrabriti slične zloupotrebe drugih dobavljača spajvera.[114] Ako bi sankcije bile usmerene i na investitore, to bi moglo imati odvraćajući efekat od ključnog značaja za američki i evropski kapital, čak i ako se kompanije presele u inostranstvo.

Sankcije moraju biti deo šire strategije koja ima za cilj da podstakne odgovornost dobavljača i investitora i uspori proliferaciju spajvera. Mada same po sebi ne mogu da razgrade čitavu industriju, sankcije mogu da utiču na podsticaje, ograniče prodaju i stigmatizuju aktere koji zloupotrebljavaju tehnologiju – naročito ako se uspostave na nivou cele Unije. Štaviše, sankcije bi otežale programerima iz EU da rade za dobavljače spajvera, čak i ako im je sedište u inostranstvu. Važno je i to da se sankcije mogu uvesti odmah.

3.4 Preporuke javnih politika za institucije EU i države članice

Kako bi se rešio regulatorni vakuum koji omogućava nekontrolisani rast industrije komercijalnog spajvera, hitno su potrebne sledeće mere institucija EU i država članica:

1. Potpuna zabrana komercijalnog spajvera. Evropska komisija mora da zabrani razvoj, proizvodnju, reklamiranje, prodaju, izvoz i upotrebu komercijalnog spajvera od strane privatnih kompanija, u skladu sa zahtevima organizacija civilnog društva koje se bave digitalnim pravima.[115]

2. Zabrana tržišta ranjivosti i eksploita. Evropska komisija treba da uvede zabranu komercijalne trgovine ranjivostima u bilo koje svrhe osim jačanja bezbednosti sistema. Paralelno s tim, treba da propiše obavezno odgovorno prijavljivanje rezultata istraživanja ranjivosti kroz jedinstven proces izveštavanja i da zabrani autsorsovanje istraživanja ranjivosti u ofanzivne svrhe od strane država prema privatnim profitnim dobavljačima.

3. Zaštita etičkog istraživanja u oblasti sajber bezbednosti i odgovornog prijavljivanja ranjivosti. EU treba da ulaže u istraživačke institucije i inicijative koje se fokusiraju na sajber bezbednost u javnom interesu, sa prioritetom na digitalna prava, privatnost i demokratsku sigurnost. Na nivou država, zaštita uzbunjivača mora biti proširena, a vlade i akteri iz industrije treba da uspostave snažne podsticaje – poput dobro finansiranih programa nagrada za bagove – za etičko

---

[114] *Financial Times*, “Trump’s ‘big, beautiful’ tax bill heightens concerns over US debt”, 2025. https://www.ft.com/content/e5b770d7-07af-4e27-a686-a0c473e93770

[115] *Center for Democracy & Technology*, “Civil Society Joint Statement on the Use of Surveillance Spyware in the EU and Beyond”, 2024. https://cdt.org/insights/civil-society-joint-statement-on-the-use-of-surveillance-spyware-in-the-eu-and-beyond/

prijavljivanje bezbednosnih propusta proizvođačima softvera. Istraživači u oblasti bezbednosti koji rade u dobroj veri, a ne u ime dobavljača spajvera, moraju biti slobodni od krivične i građanske odgovornosti kada sprovode istraživanja ili kada dele informacije o ranjivostima sa proizvođačima softvera i drugim bezbednosnim istraživačima.

4. Ukinuti finansijske podsticaje koji pokreću proliferaciju spajvera. Države članice EU moraju zabraniti javne nabavke od komercijalnih dobavljača spajvera i zabraniti javna i privatna ulaganja u kompanije koje proizvode spajver, na bilo kom nivou korporativne strukture.

5. Ciljane sankcije protiv aktera iz industrije komercijalnog spajvera. Visoki predstavnik Unije za spoljne poslove i bezbednosnu politiku i Savet treba odmah da se usaglase o sledećim sankcijama: zabrana ulaska za državljane trećih zemalja i pravna lica uključena u industriju komercijalnog spajvera, uključujući rukovodioce i investitore; ciljano uskraćivanje viza – za one koji već imaju sedište u Evropi – i zabrane putovanja za one koji posluju van EU; zamrzavanje imovine kompanija i pojedinaca,[116] uključujući i državljane EU koji rade u inostranstvu; stavljanje na listu zabranjenih dobavljača umešanih u bilo koji skandal sa spajverom; zabrana izvoza kompanijama sa sedištem u EU u bilo koju zemlju.

6. Odgovornost dobavljača, investitora i država koje omogućavaju sporno poslovanje. Dobavljači komercijalnog spajvera moraju se suočiti sa pravnim posledicama zbog omogućavanja kršenja ljudskih prava. Investitori koji svesno finansiraju te firme takođe moraju biti pozvani na odgovornost pred nadležnim sudovima. Isto tako, strane države koje omogućavaju izvoz i upotrebu spajvera u represivne svrhe moraju se suočiti sa diplomatskim i ekonomskim sankcijama. Države članice EU treba da prilagode svoje zakonodavstvo, da obavežu svoje tužilačke istrage da prate ove slučajeve, kao i da preduzmu korake da zaobiđu netransparentne strukture ovih kompanija.

7. Uvesti obaveznu retroaktivnu transparentnost. Dobavljači komercijalnog spajvera koji su poslovali unutar ili iz EU, njihovi klijenti i investitori moraju biti obavezani na retroaktivno javno objavljivanje svih svojih vlasnika i akcionara, ugovora, prodaje i sporazuma sa krajnjim korisnicima. Ova retroaktivna objava mora biti propisana zakonima država članica ili ostvarena putem sudskih mehanizama, kako bi se u potpunosti razotkrila razmera i obim zloupotreba koje je spajver omogućio i kako bi se žrtvama obezbedila delotvorna pravna zaštita. Ovi podaci trebalo bi da budu dostupni u centralnim, pretraživim registrima, otvorenim za organizacije civilnog društva, pravosudne organe i zakonodavce.

Dobavljači komercijalnog spajvera često se rebrendiraju, sele ili otvaraju fantomske kompanije kako bi izbegli regulaciju. Industriju spajvera ne održavaju samo programeri, već i prateći akteri:

[116] *European Parliament*, “Enhancing research security”, 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760416/EPRS_BRI(2024)760416_EN.pdf

pružaoci hosting usluga, preprodavci, finansijske institucije i konsultantske firme. Svi akteri koji omogućavaju razvoj ili primenu komercijalnog spajvera moraju biti obuhvaćeni ovim regulatornim merama.

4. Zaštita za žrtve

Upotreba spajvera imala je razorne posledice po ljude, organizacije i demokratske institucije. Međutim, uprkos očiglednim kršenjima osnovnih prava, u većini slučajeva žrtve nisu imale pristup delotvornoj zaštiti. U ovom delu predstavljamo pravne i vanpravne mere koje je neophodno sprovesti kako bi se ispravile nepravde, obezbedila odgovornost za prouzrokovanu štetu i pružila zaštita pojedincima i grupama.

4.1 Kršenja ljudskih prava

Upotreba spajvera izaziva ozbiljnu zabrinutost u vezi sa kršenjem osnovnih ljudskih prava, pre svega zbog njegove intruzivne i neselektivne prirode. Kao što smo ustanovili u Poglavlju 2, njegova upotreba je u suštini nespojiva sa osnovnim pravnim principima neophodnosti i proporcionalnosti, koji se moraju poštovati za svako zakonito ograničenje osnovnih prava, u skladu sa članom 52(1) Povelje o osnovnim pravima Evropske unije.

A. Direktan uticaj na targetirane pojedince

Najteža kršenja osnovnih ljudskih prava dešavaju se na individualnom nivou – čak i kada osobe nisu direktne mete. Upotreba spajvera nesrazmerno ograničava više osnovnih prava:

→ Pravo na privatni život i zaštitu podataka.[117] U svojoj suštini, spajver direktno zadire u pravo pojedinca na privatnost i zaštitu podataka. Venecijanska komisija ističe da upotreba spajvera direktno ugrožava pravo na privatnost zaštićeno međunarodnim ugovorima.[118] Pored toga,

[117] Članovi 7 i 8 Povelje o osnovnim pravima Evropske unije; članovi 7 i 8 Evropske konvencije o ljudskim pravima; član 17 Međunarodnog pakta o građanskim i političkim pravima; član 12 Univerzalne deklaracije o ljudskim pravima. *European Union*, “Charter of Fundamental Rights of the European Union”, 2012. https://www.europarl.europa.eu/charter/pdf/text_en.pdf; *United Nations*, “Universal Declaration of Human Rights”, 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights

[118] Venice Commission, “Report on a rule of law and human rights compliant regulation of spyware”, 2024. https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2024)043-e

značaj prava na zaštitu podataka u EU naglašen je dvostrukim okvirom EU,[119] koji odražava priznanje da je zaštita podataka fundamentalno pravo samo po sebi, ključno za očuvanje dostojanstva, autonomije i demokratskog učešća. Kada je reč o spajveru, Evropski supervizor za zaštitu podataka (*European Data Protection Supervisor*, EDPS) upozorava da je „nivo zadiranja u pravo na privatnost toliko ozbiljan da je osoba na metu u suštini lišena tog prava. Drugim rečima, ugrožena je sama suština prava. Stoga se njegova upotreba ne može smatrati proporcionalnom – bez obzira na to da li se mera može smatrati nužnom."[120]

→ Pravo na slobodu izražavanja, mirnog okupljanja i udruživanja.[121] Ova prava čine ključni temelj demokratskog društva. Kako se ističe u izveštaju Saveta Evrope o posledicama upotrebe spajvera na ljudska prava, „nadzor novinara i drugih medijskih aktera, kao i praćenje njihovih aktivnosti na mreži, može ugroziti legitimno ostvarivanje slobode izražavanja".[122] Na ova prava utiče i širi društveni efekat zebnje koji spajver proizvodi (vidi Odeljak B).

→ Pravo na pravično suđenje.[123] Spajver omogućava vlastima pristup poverljivim komunikacijama, što potencijalno narušava poverljivost odnosa između advokata i klijenta i potkopava pravičnost sudskog postupka. Advokati političkih disidenata u mnogim slučajevima bili su meta, kao u Španiji[124] ili Jordanu.[125] U pojedinim incidentima, poput onog sa Žordijem Kvišartom u Kataloniji,[126] žrtve su targetirane dok su pripremale strategiju za suđenje, što izaziva ozbiljne sumnje u valjanost procesa zbog povrede prava na odbranu.

---

119 Opšta uredba o zaštiti podataka (*General Data Protection Regulation*, GDPR) za privatni i javni sektor, i Direktiva za službe sprovođenja zakona (*Law Enforcement Directive*, LED) namenjena policijskim i pravosudnim organima.

120 *European Data Protection Supervisor*, "Preliminary Remarks on Modern Spyware", 15. februar 2022. str. 8 https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

121 Član 11 Povelje o osnovnim pravima EU; Član 10 Evropske konvencije o ljudskim pravima.

122 *Council of Europe*, "Pegasus Spyware and Its Impacts on Human Rights", 2022. https://rm.coe.int/pegasus-spyware-report-en/1680a6f5d8

123 Član 47 Povelje o osnovnim pravima EU; Član 6 Evropske konvencije o ljudskim pravima.

124 *TechCrunch*, "Lawyer allegedly hacked with spyware names NSO founders in lawsuit", 13. novembar 2024. https://techcrunch.com/2024/11/13/lawyer-allegedly-hacked-with-spyware-names-nso-founders-in-lawsuit/

125 *Security Week*, "At Least 30 Journalists, Lawyers and Activists Hacked With Pegasus in Jordan, Forensic Probe Finds", februar 2024. https://www.securityweek.com/at-least-30-journalists-lawyers-and-activists-hacked-with-pegasus-in-jordan-forensic-probe-finds/

126 *Front Line Defenders*, "Jordi Cuixart released from prison on pardon", 2021. https://www.frontlinedefenders.org/en/case/jordi-cuixart-released-prison-pardon

→ Pravo na jednakost i nediskriminaciju.[127] Žene, LGBTIQ+ i zajednice rodno raznolikih osoba izložene su specifičnom, rodno zasnovanom strahu kada otkriju da im je digitalna privatnost ugrožena, u riziku da se njihovi podaci koriste za onlajn uznemiravanje, naročito „doksovanje“.[128]

B. Posredni uticaj na ljude i zajednice

Kršenja ljudskih prava izazvana spajverom nisu jednodimenzionalna, naprotiv, odvijaju se na više nivoa. Posredno, ispoljavaju se kroz tri nivoa uticaja:

1. Uticaj na ljude povezane sa targetiranim osobama

Spajver zadire i u privatnost osoba povezanih sa onima koji su direktno na meti, uključujući „kolateralnu štetu“ nanetu poverljivim izvorima, advokatima, kolegama, članovima porodice i deci, čijim se ličnim podacima i komunikaciji nezakonito pristupa.[129]

2. Društveni uticaj kroz efekat zebnje

Upotreba spajvera takođe može proizvesti tzv. efekat zebnje (*chilling effect*),[130] posredno potkopavajući i druga osnovna prava poput slobode izražavanja, slobode udruživanja i okupljanja, prava na pravično suđenje i druga. Kada pojedinci sumnjaju da su pod nadzorom ili to pouzdano znaju, manje je verovatno da će javno istupati, iznositi kritiku, organizovati proteste ili učestvovati u građanskim aktivnostima, praktično sprovodeći autocenzuru iz straha od odmazde ili razotkrivanja. Na taj način, spajver ne samo da zadire u individualna prava, već i slabi kolektivno demokratsko učešće. Takođe može imati ozbiljne posledice po mentalno zdravlje, poput nesanice, noćnih mora i psihološke traume, a u nekim slučajevima dovesti i do potrebe za terapijom ili odustajanja od aktivizma.[131] Ovo povlačenje ili autocenzura ostavlja teške posledice na prostor za građansko učešće.

3. Uticaj na ljude nad kojima se vrši testiranje ili preko kojih se razvija

[127] Članovi 20 i 21 Povelje o osnovnim pravima EU; Član 14 Evropske konvencije o ljudskim pravima.
[128] *Amnesty International*, “Being ourselves is too dangerous: Digital violence and the silencing of women and LGBTI activists in Thailand”, 2024.
https://www.amnesty.org/en/wp-content/uploads/2024/05/ASA3979552024ENGLISH.pdf.
Druga prava na koja upotreba spajvera može da utiče, a koja su zaštićena Poveljom o osnovnim pravima Evropske unije, uključuju princip nepovredivnosti ljudskog dostojanstva (član 1), pravo na slobodu i bezbednost (član 6), slobodu misli, savesti i veroispovesti (član 10), pravo na kolektivno pregovaranje i delovanje (član 28) kada su meta radnici i njihove organizacije, kao i pretpostavku nevinosti i pravo na odbranu (član 48) jer se informacije prikupljaju preventivno, a kontrola nad uređajima može da se koristi za fabrikovanje lažnih dokaza.
[129] *Conseil Constitutionnel France*, Ibidem.
[130] *Amnesty International*, Ibidem.
[131] To je slučaj, na primer, aktivistkinje Pansire Džirathakun, koju je vlada Tajlanda targetirala Pegasus softverom. *Amnesty International*, Ibidem.

Štaviše, zloupotrebe spajvera protežu se duž čitavog lanca vrednosti: kompanije, investitori i države izvoznice imaju ulogu u perpetuiranju kršenja ljudskih prava, od razvoja do primene. Jasan primer je slučaj Izraela, vodećeg izvoznika komercijalnog spajvera i alata za digitalnu forenziku. U neprekidnom nizu izveštaja poslednjih godina navodi se da su mnogi komercijalni špijunski alati, proizvedeni u Izraelu i zatim prodavani u inostranstvu, testirani na Palestincima[132] pre plasiranja na tržište.[133] Čak i u slučajevima kada kompanije napuštaju Izrael da bi uspostavile poslovanje u EU, dokumentovano je da 56 od 74 vlade nabavljaju tehnologije za nadzor od firmi povezanih s tom zemljom.[134] Kompanije su ili bazirane u Izraelu (*NSO Group*, *Cellebrite*, *Cytrox* i *Candiru*), ili među vodećim rukovodiocima imaju bivše pripadnike Izraelskih odbrambenih snaga (IDF)[135] koji donose tehničku ekspertizu, kao u slučaju kompanije *Intellexa*.[136]

4.2 Zaštita

Odsustvo efektivnih pravnih lekova u Evropi ostavilo je žrtve bez mogućnosti zaštite, jačajući nekažnjivost dobavljača i korisnika spajvera. Potreban je čvrst okvir pravnih i vanpravnih lekova kako bi se obezbedila pravda, odgovornost i podrška za pogođene pojedince i zajednice.

A. Pravna zaštita

Država, koja je često i sama korisnik spajvera, teško da će pružiti nepristrasna pravna sredstva, dok se žrtve suočavaju sa značajnim preprekama u ostvarivanju pravde. Međutim, zemlje EU

[132] *Chatham House*, "Review: Why Israel tests its spyware on Palestinians", 2023. https://www.chathamhouse.org/publications/the-world-today/2023-06/review-why-israel-tests-its-spyware-palestinians
[133] *Foreign Policy*, "How the Occupation Fuels Tel Aviv's Booming AI Sector", 2022. https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/
[134] *Carnegie Endowment for International Peace*, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses", 2023. https://carnegieendowment.org/research/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229
[135] IDF je bio glavni akter u razvoju praksi koje, prema UN-u, „odgovaraju karakteristikama genocida" u Pojasu Gaze, u kontekstu rata od 2023. do 2025. godine. *United Nations General Assembly*, "Report of the Special Committee to Investigate Israeli Practices Affecting the Human Rights of the Palestinian People and Other Arabs of the Occupied Territories", 2024. https://docs.un.org/en/A/79/363
[136] Osnovana 2019. godine od strane bivšeg izraelskog vojnog oficira Tala Jonatana Dilijana, Intellexa se istakla kao ključni igrač na globalnom tržištu komercijalnog spajvera. *Turkiye Today*, "US imposes sanctions on Greece-based company founded by ex-Israeli military officer", 2024. https://www.turkiyetoday.com/world/us-imposes-sanctions-on-greece-based-company-founded-by-ex-israeli-military-officer-8398/

obavezane su da obezbede pravo na delotvornu pravnu zaštitu[137] koje, prema međunarodnom pravu ljudskih prava, obuhvata tri glavne komponente:[138]

→ Pristup relevantnim informacijama o kršenjima i mehanizmima reparacije

→ Jednak i delotvoran pristup pravdi

→ Odgovarajuća, delotvorna i brza reparacija za pretrpljenu štetu

Stoga, sledeća pravna sredstva zaštite predstavljaju minimum koji države članice EU moraju obezbediti, ex post, žrtvama spajvera kako bi se poštovalo pravo ljudskih prava.

1. **Pravo na obaveštenost: transparentnost i pristup informacijama.** Žrtve moraju imati potpun pristup detaljnim informacijama o operacijama spajvera, uključujući ko je primenio spajver protiv njih, koji sudski organ je odobrio njegovu upotrebu i po kom pravnom osnovu. Ovaj pravni lek obuhvata i transparentnost u vezi sa dobavljačima spajvera, kao što je navedeno u Poglavlju 3.

2. **Pravo na zaštitu podataka i informacije o čuvanju podataka.** Pojedinci moraju tačno znati obim zadiranja u njihove istorijske i podatke u realnom vremenu. To uključuje informacije o tome koje lične podatke su nadležni videli, nadzirali ili izvukli; kada; od strane koga (uz iscrpnu evidenciju); gde se podaci čuvaju; i kako su zaštićeni. Ovo pravo takođe obuhvata razumevanje postojećih bezbednosnih mera, protokola za zadržavanje i brisanje podataka, kao i svih slučajeva u kojima su podaci mogli biti presretnuti ili izmenjeni.

3. **Pravo na odgovornost i sudsku zaštitu.** Mora postojati jasan i dostupan pravosudni put koji omogućava žrtvama da pozovu na odgovornost i državne aktere i privatne kompanije. Pravni postupci treba da razjasne nadležnost, obezbede odgovarajuću kontrolu i izreknu sankcije odgovornima, pri čemu tužilaštva moraju aktivno pokretati gonjenje.

4. **Pravo na nezavisnu istragu.** Kao što je zahtevao istražni komitet Evropskog parlamenta o Pegazusu i sličnom softveru za nadzor (PEGA), žrtve treba da imaju pravo na nepristrasnu, nezavisnu istragu navedenih zloupotreba spajvera.[139] Takve istrage moraju imati ovlašćenje da prikupljaju dokaze – čak i kada su zaštićeni zakonima o tajnosti – da ispitaju relevantne strane, uključujući državne zvaničnike, zaposlene u kompanijama i investitore, kao i da rade slobodne od političkog ili komercijalnog upliva, kako bi se obezbedilo da istina bude u potpunosti razotkrivena.

---

[137] Član 47 Povelje o osnovnim pravima EU; Član 13 Evropske konvencije o ljudskim pravima.
[138] *Amnesty International*, Ibidem.
[139] PEGA Committee of inquiry
https://www.europarl.europa.eu/committees/en/archives/9/pega/home/welcome-words

5. **Pravo na naknadu štete.** Naknada mora obuhvatiti ne samo finansijske gubitke već i nematerijalnu štetu, poput posledica po mentalno zdravlje. Ovaj oblik reparacije služi i kao pravni lek za pojedinca i kao sredstvo odvraćanja od buduće upotrebe tehnologija spajvera.

6. **Pravo na neponavljanje.** Pravni okviri moraju obezbediti sistemske reforme kako bi se sprečila buduća kršenja od strane državnih organa ili drugih aktera, kao i da se sudska praksa razvija na način koji sprečava buduća kršenja ljudskih prava.

Iako su ova pravna sredstva od suštinskog značaja za zaštitu prava žrtava u slučaju zloupotrebe spajvera, ona predstavljaju privremene mere koje ne mogu zameniti osnovni cilj: potpunu zabranu spajvera u skladu sa obavezama poštovanja osnovnih prava.

B. Vanpravna zaštita

Dodatno, države članice EU moraju obezbediti primenu sledećih vanpravnih mera u javnim upravama u odnosu na žrtve spajvera:

1. **Psihološka podrška.** Obezbediti besplatne i nezavisne resurse za mentalno zdravlje i podršku žrtvama koje su doživele traumu usled nadzora i represije.[140]

2. **Briga o tražiocima azila i ljudima bez dokumenata.** Pružiti podršku žrtvama čija je bezbednost ugrožena spajverom i koje moraju potražiti utočište drugde, obezbeđivanjem azila i zaštite.

3. **Olakšati pristup podršci za žrtve.** Pokrenuti javne informativne kampanje usmerene na rizike spajvera, digitalnu samoodbranu i vrste pomoći (npr. telefonske linije, pravna pomoć i podrška civilnog društva). Obezbediti da pogođeni pojedinci znaju svoja prava i gde mogu da potraže pomoć.

4.3 Uloga strateške parnice u borbi protiv zloupotrebe spajvera

Sudske odluke su neophodne za uspostavljanje snažnog pravnog režima protiv upotrebe spajvera, jer sudovi često predstavljaju poslednji bastion zaštite ljudskih prava. Strateška parnica pruža više mogućih načina za uspostavljanje odgovornosti: osporavanje zakonskih

[140] *Forbes Technology Council*, “Recognizing and Preventing the Psychological Toll of Spyware”, 2022. https://www.forbes.com/councils/forbestechcouncil/2022/08/12/recognizing-and-preventing-the-psychological-toll-of-spyware/

odredbi koje dozvoljavaju upotrebu spajvera, razotkrivanje slučajeva u kojima vlade koriste takve alate, kao i pokretanje postupaka protiv kompanija.

Značajan primer je slučaj *FinFisher* u Nemačkoj. Posle krivične prijave koju su podnele organizacije poput *Gesellschaft für Freiheitsrechte e.V.*, *Reporters Without Borders*, *European Centre for Constitutional and Human Rights* i *netzpolitik.org*, kancelarija javnog tužioca u Minhenu zaplenila je imovinu grupacije *FinFisher*.[141] Usled toga, kompanija *FinFisher GmbH* i njene partnerske firme podnele su zahtev za stečaj. Još jedan primer je odluka nemačkog saveznog ustavnog suda iz 2008, kojom su postavljeni visoki standardi za upotrebu državnog spajvera (*Staatstrojaner*).[142] Ovi slučajevi pokazuju kako strateška parnica može poslužiti kao efikasno sredstvo u borbi protiv zloupotrebe spajvera.

Međutim, na svom putu ka pravdi i promenama, žrtve širom Evrope nailaze na slične prepreke:

→ Tajnost i uskraćivanje informacija. Vlade se često pozivaju na zakone o tajnosti koji sprečavaju da ključne informacije dođu do javnosti, kao u slučaju Grčke[143] ili u Nemačkoj, povodom izveštaja o korišćenju Pegasusa u saveznom kriminalističkom uredu (*Bundeskriminalamt*, BKA).

→ Nečinjenje tužilaštva. Ovo nepostupanje države – koja je često upravo akter odgovoran za nezakoniti nadzor – ne samo da primorava žrtve da troše značajne resurse, vreme i energiju, već može dovesti i do sekundarne viktimizacije – pri čemu propust države da reaguje produbljuje pretrpljenu štetu. To je, na primer, slučaj u Kataloniji, gde su španski javni tužioci sistematski blokirali sudski postupak[144] četiri godine posle otkrića da su španske vlasti hakovale katalonske organizacije civilnog društva, advokate i političare, u skandalu nazvanom „Catalangate“.[145]

→ Komplikovana nadležnost. Globalna priroda dobavljača spajvera unosi dodatni sloj poteškoća. Kada kompanije imaju sedište u jednoj zemlji, podružnice u drugoj (npr. kompanija sa sedištem u Izraelu i podružnicama u Luksemburgu),[146] a njihove žrtve se nalaze u trećoj

141 *Netzpolitik*, “German Made State Malware Company FinFisher Raided”, 2020. https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/

142 *Bundesverfassungsgericht*, “Urteil vom 27. Februar 2008 – 1 BvR 370/07”, 2008. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

143 *Politico*, “Greece leaves spy services unchecked on Predator hacks”, 2024. https://www.politico.eu/article/greek-spyware-predatorgate-government-court-report-telephone/

144 *Politico*, “Catalonia reignites its court fight with Spain over spyware“, 2025. https://www.politico.eu/article/catalonia-reignite-court-fight-spain-israel-pegasus-candiru-spyware-hacking/

145 *The Citizen Lab*, “CatalanGate Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Candiru”, 2022. https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru

146 To je slučaj s NSO Grupom, za koju je katalonska organizacija *Iridia* uspela da izdejstvuje optužnicu posle tri godine pravne borbe. *Iridia*, “Three executives of the NSO Group charged for their responsibility

zemlji, uspostavljanje jasne nadležnosti postaje problematično. Usled ovakvih komplikacija, mnogi sudovi odbijaju da se bave tim slučajevima, pozivajući se na ograničenja nadležnosti. Čak i kada sudovi prihvate predmete, i dalje je veoma teško sprovesti odluke protiv kompanija koje nisu registrovane u EU.

Još jedna prepreka nalazi se i u nedostatku evropske sudske prakse u pogledu upotrebe spajvera. Ako Evropski sud za ljudska prava i Sud pravde Evropske unije ostanu dosledni svojoj odlučnoj posvećenosti zaštiti ljudskih prava, kada pred njih stignu slučajevi upotrebe spajvera, ovi sudovi će pružiti ključni pravni oslonac za zaštitu i utvrđivanje odgovornosti u slučajevima kada države koriste spajver.

4.4 Zaštita organizacija civilnog društva koje se bave slučajevima spajvera

Organizacije civilnog društva i istraživački novinari koji rade na otkrivanju spajvera, digitalnoj forenzici i reagovanju na incidente, često su jedini akteri koji razotkrivaju upotrebu spajvera od strane država, te ih stoga treba adekvatno zaštititi od pravnih zastrašivanja i potencijalnih posledica koje nameće država. Ove organizacije pružaju usluge i zaštitu novinarima, aktivistima, članovima civilnog društva i drugim nepravedno targetiranim žrtvama državne represije zbog posla koji obavljaju. Sposobnost organizacija civilnog društva da efikasno funkcionišu ozbiljno je ograničena u autoritarnim i hibridnim režimima, gde vlasti deluju izvan zakona i daju prednost interesima vladajućih stranaka nad interesima građana, ali sve više i u zemljama koje se formalno smatraju demokratskim.

Organizacije nisu samo direktno na meti državnih organa, već se suočavaju i sa dodatnim pretnjama, uključujući ucene, zastrašivanje i lične napade u medijima. Kao je pokazao slučaj u Srbiji, ove organizacije i njihovi zaposleni izloženi su kampanjama blaćenja i dezinformisanja – koje često orkestriraju tabloidi blisko povezani sa vladom.[147]

---

in the Pegasus espionage case", 2025.
https://iridia.cat/en/three-executives-of-the-nso-group-charged-for-their-responsibility-in-the-pegasus-espionage-case

[147] Dobar primer je kampanja blaćenja koju su poveli režimski mediji protiv SHARE Fondacije, koja je pomogla u otkrivanju skandala sa špijunskim softverom u Srbiji. *Novosti*, "SHARE FONDACIJA DOBILA VIŠE OD ČETIRI MILIONA EVRA: Izmislili priču o špijunaži novinara, a finansira ih Švajcarska", decembar 2024.
https://www.novosti.rs/vesti/politika/1444129/share-fondacija-dobila-vise-cetiri-miliona-evra-izmislili-pricu-spijunazi-novinara-finansira-svajcarska

Pored toga, pokušaji da se diskredituju i same organizacije i njihovi zaposleni dodatno potkopavaju njihov rad, stvarajući klimu straha i neprijateljstva koja otežava njihove napore da razotkriju i dokumentuju zloupotrebe koje istražuju. Dodatna strategija diskreditacije jeste zahtev državnih organa za pristup uređajima žrtava – upravo onih organa koji su ih prethodno podvrgli zloupotrebi. Ova praksa mora biti obeshrabrena, a organizacije civilnog društva i nezavisni forenzički stručnjaci treba da budu priznati i legitimni akteri za obavljanje takvih analiza umesto državnih organa.

Zajedno sa novinarima, organizacije civilnog društva obično su jedini akteri koji mogu da otkriju slučajeve kršenja ljudskih prava povezanih sa spajverom i stoga često predstavljaju jedini delotvorni oblik zaštite dostupan targetiranim pojedincima. Stoga je od najvećeg značaja da nezavisna nacionalna i međunarodna tela – uključujući nacionalne ombudsmane, poverenike za zaštitu podataka, institucije Evropske unije, Savet Evrope i Ujedinjene nacije – blagovremeno i odlučno reaguju na svaki zlonamerni napad na organizacije civilnog društva koje se bave slučajevima spajvera. Ova potreba je još urgentnija u kontekstu šireg talasa, obično među akterima krajnje desnice, širom Evrope i sveta, napada, omalovažavanja i delegitimizacije civilnog društva i demokratskog suprotstavljanja govoru mržnje i dezinformacija.

4.5 Preporuke institucijama Evropske unije i državama članicama

Kako bi se odgovorilo na stvarne posledice spajvera i obezbedila delotvorna zaštita, uz garancije da će svi koji učestvuju u kršenju ljudskih prava biti pozvani na odgovornost, potrebno je sprovesti sledeće mere:

1. Pun pristup pravnim i vanpravnim sredstvima zaštite za sve žrtve

→ Države članice moraju obezbediti da sva pravna i vanpravna sredstva zaštite izložena u ovom poglavlju budu dostupna svakoj osobi izloženoj spajveru, bez obzira na državljanstvo ili status. To obuhvata:

> → Pravna sredstva zaštite: pravo na obaveštenost, pravo na zaštitu podataka i informacije o njihovom čuvanju, sudska zaštita, nezavisna istraga, naknada štete i garancije neponavljanja.
>
> → Vanpravna sredstva zaštite: psihološka podrška, mehanizmi za tražioce azila, javne kampanje podizanja svesti i olakšan pristup podršci za žrtve.

2. Ukloniti pravosudne prepreke za postojeće žrtve

→ Savet Evropske unije i države članice moraju uvesti obavezujuću dužnost za tužioce da istražuju pritužbe žrtava spajvera, ukloniti mogućnost proizvoljnog nepostupanja i obezbediti podršku sudovima kroz specijalizovane jedinice ili nezavisne istražitelje osposobljene za ovako složene slučajeve.

→ Države članice moraju uspostaviti adekvatno finansirane nezavisne istražne organe za ispitivanje slučajeva zloupotrebe spajvera, izvan političkog uticaja, i kako bi se izbeglo da žrtve moraju predavati svoje uređaje organima kojima možda ne veruju.

→ Garantovati podršku žrtvama koje su već upletene u dugotrajne, opstruisane ili obustavljene sudske postupke, uključujući ubrzani pregled predmeta, procesnu podršku i pristup pomoći iz oblasti digitalne forenzike, kao i reformu pravila o nadležnosti kako bi se žrtvama sa prebivalištem u EU omogućilo da pokreću transnacionalne slučajeve spajvera, naročito u slučajevima kada dobavljači posluju u više država.

3. Obezbediti političku odgovornost i strukturnu reformu

→ Evropska komisija mora sprovesti preporuke PEGA komiteta. Posebno bi trebalo da obaveže države članice EU da odmah sprovedu nezavisne, transparentne i nepristrasne istrage svih slučajeva nezakonitog nadzora, po potrebi uz inicijativu državnih tužilaca, pod pretnjom primene mehanizma vladavine prava ili pokretanja postupaka zbog povrede prava ukoliko se mere ne sprovedu.

→ Evropska komisija treba da zahteva od država članica da obezbede potpunu transparentnost u javnim nabavkama i primeni alata spajvera, uključujući obavezno javno izveštavanje o njihovoj upotrebi.

→ Države članice pogođene skandalima treba da formiraju parlamentarne istražne odbore sa dovoljnim ovlašćenjima da ispitaju razmere, troškove i pravne osnove državne upotrebe spajvera, kao i detalje o javnim nabavkama.

→ Države članice takođe treba da sprovedu reformu propisa o tajnosti podataka na osnovu kojih se, pod opravdanjem „tajnosti“, skrivaju podaci o nezakonitom nadzoru, koji su od ključnog značaja za pravo žrtava na obaveštenost, naročito kada se te odredbe koriste da bi se žrtvama uskratila zaštita.

4. Zaštititi branitelje ljudskih prava, novinare, advokate i organizacije civilnog društva

→ Evropska komisija mora razviti i finansirati mehanizam hitne zaštite na nivou cele EU[148] za novinare, branitelje ljudskih prava, advokate i uzbunjivače koji su izloženi pretnji spajvera u EU i šire. Takav mehanizam treba da obezbedi:

[148] Dobar model bi bila inicijativa protectdefenders.eu, namenjena zaštiti branitelja ljudskih prava izloženih riziku, koja se finansira sredstvima EU, ali koju koordiniraju specijalizovane organizacije civilnog društva.

→ preventivnu podršku u oblasti digitalne bezbednosti, uključujući provere bezbednosti uređaja, obuke za komunikaciju i detekciju spajvera u realnom vremenu;

→ nezavisnu forenzičku pomoć i pouzdane telefonske linije za osobe u riziku;

→ hitno preseljenje, pravnu pomoć i finansijsku podršku za one koji su u neposrednoj opasnosti.

→ Evropska komisija takođe treba da uspostavi fond EU za organizacije civilnog društva i pojedince, poput novinara, koji se bave otkrivanjem spajvera, forenzikom i podrškom žrtvama, uključujući i fond za hitne slučajeve dostupan ne samo u državama članicama, već i u zemljama kandidatima za EU, u svrhe operativne podrške.

→ Države članice treba da učine korak više od obaveza propisanih zakonom o slobodi medija (*European Media Freedom Act*, EMFA) tako što će izričito zabraniti upotrebu spajvera protiv bilo koga (uključujući novinare, advokate i branitelje ljudskih prava), ali i garantovati pristup mehanizmima brze zaštite i pravne pomoći za one koji su već bili meta. Ove mere treba da budu komplementarne pravima žrtava izloženim u Preporukama 1 i 2.

→ Paralelno s tim, države članice moraju hitno da u svoje zakonodavstvo prenesu i efikasno primene Direktivu o sprečavanju SLAPP tužbi, kao i da usvoje ambiciozne sudske i vansudske mere radi bolje zaštite ljudi i organizacija civilnog društva od SLAPP tužbi. To obuhvata integrisanje odredbi iz povezanih neobavezujućih tekstova, poput Preporuke Evropske komisije protiv SLAPP tužbi iz 2022. godine i Preporuke Saveta Evrope iz 2024. godine, kao i obezbeđivanje javnog finansiranja za organizacije civilnog društva koje se bave forenzikom i podrškom žrtvama.

5. Rečnik pojmova

→ **Daljinski pristup** (*remote access*): mogućnost nadzora ili kontrole uređaja na daljinu, bez direktnog fizičkog kontakta sa uređajem.

→ **Dobavljači komercijalnog spajvera**: privatne kompanije koje zarađuju na razvoju i ponudi ofanzivnih sajber kapaciteta (za potrebe ometanja ili nadzora). Takođe se nazivaju „dobavljači komercijalnih tehnologija nadzora“ ili „sajber plaćeničke firme“, a mogu nuditi razne tehnologije nadzora, uključujući (ili ne) spajver. U ovom dokumentu koristimo specifičan izraz „dobavljači komercijalnog spajvera“ kako bismo označili samo one aktere u industriji koji prodaju spajver kao komercijalni proizvod.

→ **Eksploit** (*exploit*): segment koda ili program koji zlonamerno iskorišćava ranjivosti ili bezbednosne propuste u softveru, a često se koristi za instalaciju spajvera.

→ **Evidentiranje** (*logging*): proces beleženja svake aktivnosti na uređaju. Spajver često onemogućava ili zaobilazi logove kako bi njegovo prisustvo i upotreba ostali prikriveni.

→ **Nagrada za bagove** (*bug bounty*): ponuda koju sajtovi, organizacije, vlade i proizvođači softvera nude pojedincima u vidu priznanja i naknade za prijavu bagova, posebno onih koji se odnose na bezbednosne propuste i ranjivosti.

→ **Ranjivost nultog dana** (*zero-days*): vrsta bezbednosne ranjivosti koju hakeri koriste za napad na sisteme. Izraz „zero-day" označava činjenicu da proizvođači ili programeri još uvek nisu svesni greške i da imaju „nula dana" da je isprave.

→ **Obaveza propusta u enkripciji**: ranjivost ubačena po instrukciji vlasti, da bi se trećim stranama omogućio pristup šifrovanim podacima, što podriva poverenje i bezbednost za sve korisnike.

→ **Ranjivost** (*vulnerability*): softverska ranjivost je strukturna ili razvojna greška u aplikaciji koju napadači mogu iskoristiti da ugroze bezbednost i funkcionalnost sistema, mreže ili podataka sa kojima je u interakciji.

→ **Nasilno probijanje** (*brute force*): metod za zaobilaženje bezbednosnih zaštita kroz sistematsko i automatsko isprobavanje svih mogućih kombinacija kredencijala, lozinki, pristupnih kodova ili drugih faktora autentifikacije dok se ne dobije pristup uređaju.

→ **Telemetrija**: podaci koje prikuplja softver ili sistemi, poput lokacije ili statistike korišćenja, a koji se često koriste u svrhe nadzora bez jasnog pristanka korisnika.

→ **Upad kao usluga** (*intrusion-as-a-service*): komercijalni model prodaje kapaciteta privatnih aktera – uključujući i spajver – za upad na zahtev.

→ **Vektor napada**: metod ili „put" koji se koristi za isporuku spajvera u ciljani uređaj; npr. zlonamerni linkovi, obmanjujuće reklame, fizički pristup ili specifična ranjivost.