2024/2659

16.10.2024.

PREPORUKA KOMISIJE (EU) 2024/2659

od 11. listopada 2024.

o smjernicama za izvoz robe za kibernetički nadzor u skladu s člankom 5. Uredbe (EU) 2021/821 Europskog parlamenta i Vijeća

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 292.,

budući da:

(1) Uredbom (EU) 2021/821 Europskog parlamenta i Vijeća ([1]) uspostavlja se režim Unije za kontrolu izvoza, brokeringa, tehničke pomoći, provoza i prijenosa robe s dvojnom namjenom.

(2) Uredbom (EU) 2021/821 nastoji se smanjiti rizik od upotrebe robe za kibernetički nadzor u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava.

(3) U skladu s člankom 5. stavkom 2. i člankom 26. stavkom 1. Uredbe (EU) 2021/821 Komisija i Vijeće stavljaju izvoznicima na raspolaganje smjernice o nenavedenoj robi za kibernetički nadzor, s obzirom na potrebu da se osigura učinkovitost režima Unije za kontrolu izvoza u pogledu kibernetičke sigurnosti i dosljednost provedbe Uredbe (EU) 2021/821.

(4) Cilj je ove Preporuke i smjernica koje su joj priložene poduprijeti izvoznike u primjeni kontrola nenavedene robe za kibernetički nadzor, uključujući među ostalim mjere dužne pažnje kojima se procjenjuju rizici povezani s izvozom takve robe.

(5) O smjernicama priloženima ovoj Preporuci 2022. i 2023. provedena su opsežna savjetovanja u okviru Stručne skupine za tehnologiju nadzora te su u njima uzete u obzir primjedbe zaprimljene tijekom javnog savjetovanja ([2]) održanog u drugom tromjesečju 2023.

(6) Treba napomenuti da ova Preporuka i priložene smjernice nisu obvezujuće. Stoga bi izvoznici trebali zadržati odgovornost za ispunjavanje svojih obveza na temelju Uredbe (EU) 2021/821, a Komisija bi trebala osigurati da ova Preporuka ostane relevantna kako vrijeme prolazi,

([1]) Uredba (EU) 2021/821 Europskog parlamenta i Vijeća od 20. svibnja 2021. o uspostavi režima Unije za kontrolu izvoza, brokeringa, tehničke pomoći, provoza i prijenosa robe s dvojnom namjenom (SL L 206, 11.6.2021., str. 1., ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

DONIJELA JE OVU PREPORUKU:

Preporučuje se da nadležna tijela i izvoznici iz država članica uzmu u obzir smjernice iz Priloga ovoj Preporuci kako bi ispunili svoje obveze iz članka 5. stavka 2. Uredbe (EU) 2021/821.

Sastavljeno u Bruxellesu 11. listopada 2024.

Za Komisiju
Valdis DOMBROVSKIS
Izvršni potpredsjednik

PRILOG

SADRŽAJ

Stranica

Uvod ... 4

1. Relevantne pravne odredbe, definicije i ključni pojmovi ... 4

1.1. Pregled relevantnih pravnih odredaba ... 4

1.2. Glavne definicije ... 5

1.2.1. „Posebno osmišljena” ... 5

1.2.2. „Prikriveni nadzor” ... 6

1.2.3. „Fizičke osobe” ... 6

1.2.4. „Praćenje, izdvajanje, prikupljanje, analiziranje podataka” ... 6

1.2.5. „Iz informacijskih i telekomunikacijskih sustava” ... 7

1.2.6. „Zna” i „namijenjena” ... 7

1.3. Unutarnja represija, ozbiljne povrede ljudskih prava i međunarodnog humanitarnog prava ... 7

1.3.1. Unutarnja represija ... 8

1.3.2. Počinjenje ozbiljnih povreda ljudskih prava ... 8

1.3.3. Počinjenje ozbiljnih povreda međunarodnog humanitarnog prava ... 9

2. Tehničko područje primjene ... 9

2.1. Navedena roba za kibernetički nadzor ... 9

2.2. Potencijalna nenavedena roba za kibernetički nadzor ... 9

2.2.1. Tehnologija prepoznavanja lica i emocija ... 10

2.2.2. Uređaji za praćenje lokacije ... 10

2.2.3. Sustavi videonadzora ... 10

3. Mjere dužne pažnje ... 10

Zahtjevi iz članka 5. stavka 2. Uredbe (EU) 2021/821 ... 12

4. Dodatak ... 12

Navedena roba za kibernetički nadzor kako je kontrolirana Prilogom I. Uredbi (EU) 2021/821 ... 12

Telekomunikacijski sustavi za presretanje (5A001.f.) ... 12

Sustavi za nadzor interneta (5A001.j.) ... 13

„Softver za neovlašteni ulazak” (4A005, 4D004 i povezane kontrole iz 4E001.a. i 4E001.c.) ... 13

Softver za praćenje komunikacije (5D001.e.) ... 14

Roba koja se upotrebljava za kriptoanalizu (5A004.a.) ... 14

Forenzički/istražni alati (5A004.b., 5D002.a.3.b. i 5D002.c.3.b.) ... 14

UVOD

Okvirom Unije za kontrolu izvoza uspostavljenim Uredbom (EU) 2021/821 („Uredba”) nastoji se osigurati da Unija i njezine države članice ispunjavaju međunarodne obveze, među ostalim u pogledu regionalnog mira, sigurnosti i stabilnosti te poštovanja ljudskih prava i međunarodnog humanitarnog prava. Unija i njezine države članice stoga su provele odluke donesene u okviru multilateralnih režima za kontrolu izvoza i u skladu s time ažurirale kontrolni popis Unije u Prilogu I. Uredbi ([1]). Nadalje, prije početka primjene članka 5. Uredbe nadležna tijela država članica već su kontrolirala izvoz određene robe s popisa koja može imati nadzorne primjene ([2]), uzimajući u obzir rizik zloupotrebe u određenim posebnim okolnostima. U iznimno teškim okolnostima Unija je uvela sankcije kojima se ograničava izvoz određene opreme za nadzor ([3]).

Uredba odražava namjeru Unije da uspješno smanji rizik od upotrebe robe za kibernetički nadzor u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava. Konkretno, u Uredbu su unesene nove odredbe za kontrolu izvoza nenavedene robe za kibernetički nadzor, uključujući obvezu za izvoznike da obavijeste nadležno tijelo ako na temelju rezultata dubinske analize znaju da je nenavedena roba za kibernetički nadzor koju izvoznici namjeravaju izvoziti namijenjena, u cijelosti ili djelomično, za upotrebu u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava. U Uredbi se uz to poziva Komisiju i Vijeće da izvoznicima stave na raspolaganje smjernice za potporu učinkovitoj provedbi novih kontrola za nenavedenu robu za kibernetički nadzor.

Stoga je cilj ovih smjernica poduprijeti izvoznike u primjeni kontrola nenavedene robe za kibernetički nadzor, uključujući, među ostalim, mjere dužne pažnje kojima se procjenjuju rizici povezani s izvozom takve robe krajnjim korisnicima i za krajnje upotrebe u skladu s novim odredbama Uredbe.

1. RELEVANTNE PRAVNE ODREDBE, DEFINICIJE I KLJUČNI POJMOVI

1.1. Pregled relevantnih pravnih odredaba

U Uredbu su unesene nove odredbe koje izričito omogućuju kontrole izvoza robe za kibernetički nadzor koja nije navedena u Prilogu I. Uredbi i koja jest ili bi mogla biti, u cijelosti ili djelomično, namijenjena upotrebi u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava. Relevantne uvodne izjave i članci su:

(a) uvodna izjava 8.: „Kako bi se odgovorilo na rizik da određenu nenavedenu robu za kibernetički nadzor izvezenu iz carinskog područja Unije zloupotrijebe osobe umiješane u organizaciju i počinjenje teških povreda ljudskih prava ili međunarodnog humanitarnog prava, primjereno je kontrolirati izvoz te robe. Povezani rizici odnose se osobito na slučajeve u kojima je roba za kibernetički nadzor posebno osmišljena kako bi se omogućio neovlašten ulazak ili analiza paketnog prometa) u informacijskim i telekomunikacijskim sustavima kako bi se provodio prikriveni nadzor

([1]) Vidjeti posebno kontrole koje se odnose na telekomunikacijske sustave za presretanje (5A001.f), sustave za nadzor interneta (5A001.j.), softver za neovlašteni ulazak (4A005, 4D004 i povezane kontrole pod 4E001.a i 4E001.c) i softver za praćenje komunikacije koji koriste tijela kaznenog progona (5D001.e). Nadalje vidjeti, na temelju procjene svakog pojedinačnog slučaja, kontrole koje se odnose na određene forenzičke/istražne alate (5A004.b 5D002.a.3.b i 5D002.c.3.b).

([2]) Osobito sustavi za sigurnost informacija.

([3]) Vidjeti Uredbu Vijeća (EZ) br. 765/2006 od 18. svibnja 2006. o mjerama ograničavanja s obzirom na stanje u Bjelarusu i sudjelovanje Bjelarusa u ruskoj agresiji prema Ukrajini (SL L 134, 20.5.2006., str. 1., ELI: http://data.europa.eu/eli/reg/2006/765/oj); Uredbu Vijeća (EU) br. 359/2011 od 12. travnja 2011. o mjerama ograničavanja protiv određenih osoba, subjekata i tijela s obzirom na stanje u Iranu (SL L 100, 14.4.2011., str. 1., ELI: http://data.europa.eu/eli/reg/2011/359/oj); Uredbu Vijeća (EU) br. 36/2012 od 18. siječnja 2012. o mjerama ograničavanja s obzirom na stanje u Siriji i o stavljanju izvan snage Uredbe (EU) br. 442/2011 (SL L 16, 19.1.2012., str. 1., ELI: http://data.europa.eu/eli/reg/2012/36/oj); Uredbu Vijeća (EU) br. 401/2013 od 2. svibnja 2013. o mjerama ograničavanja s obzirom na stanje u Mjanmaru/Burmi i stavljanju izvan snage Uredbe (EZ) br. 194/2008 (SL L 121, 3.5.2013., str. 1., ELI: http://data.europa.eu/eli/reg/2013/401/oj); i Uredbu Vijeća (EU) 2017/2063 od 13. studenog 2017. o mjerama ograničavanja s obzirom na stanje u Venezueli (SL L 295, 14.11.2017., str. 21., ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

fizičkih osoba praćenjem, izdvajanjem, prikupljanjem i analiziranjem podataka, uključujući biometrijske podatke, iz tih sustava. Za robu koja se upotrebljava isključivo za komercijalnu primjenu kao što je plaćanje, stavljanje na tržište, usluge kvalitete, zadovoljstvo korisnika ili sigurnost mreže općenito se smatra da ne podrazumijeva te rizike”;

(b) uvodna izjava 9.: „Radi jačanja djelotvorne kontrole izvoza nenavedene robe za kibernetički nadzor nužno je dodatno uskladiti primjenu sveobuhvatnih kontrola u tom području. U tu su svrhu države članice predane podupiranju tih kontrola dijeljenjem informacija među sobom i s Komisijom, posebno u pogledu tehnoloških kretanja robe za kibernetički nadzor i postupajući s oprezom u primjeni tih kontrola kako bi se promicala razmjena na razini Unije.”;

(c) članak 2. točka 20., u kojem se roba za kibernetički nadzor definira kao „roba s dvojnom namjenom posebno osmišljena kako bi se omogućio prikriveni nadzor fizičkih osoba praćenjem, izdvajanjem, prikupljanjem ili analiziranjem podataka iz informacijskih i telekomunikacijskih sustava”;

(d) u članku 5. propisuje se da se za izvoz nenavedene robe za kibernetički nadzor zahtijeva dozvola ako je nadležno tijelo obavijestilo izvoznika da predmetna roba jest ili bi mogla biti, u cijelosti ili djelomično, namijenjena za upotrebu u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava (članak 5. stavak 1.). Nadalje, izvoznici su dužni obavijestiti nadležno tijelo ako na temelju rezultata svoje dubinske analize znaju da je roba namijenjena, u cijelosti ili djelomično, za upotrebu u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava (članak 5. stavak 2.). To nadležno tijelo odlučuje je li za taj izvoz potrebna dozvola; i

(e) u članku 5. stavku 2. nadalje se navodi da „Komisija i Vijeće stavljaju izvoznicima na raspolaganje smjernice, kako je navedeno u članku 26. stavku 1.”.

1.2. **Glavne definicije**

Uredba sadržava posebne uvodne izjave i odredbe u kojima se pojašnjavaju posebni uvjeti relevantni za kontrole izvoza nenavedene robe za kibernetički nadzor i važno je da ih izvoznici jasno razumiju kako bi poduzeli mjere dužne pažnje i učinkovito provodili kontrole. Od osobite je važnosti sljedeća precizna definicija „robe za kibernetički nadzor” u članku 2. točki 20.: „roba s dvojnom namjenom posebno osmišljena kako bi se omogućio prikriveni nadzor fizičkih osoba praćenjem, izdvajanjem, prikupljanjem ili analiziranjem podataka iz informacijskih i telekomunikacijskih sustava”.

Za potrebe ovih smjernica treba pojasniti specifične elemente te definicije.

1.2.1. *„Posebno osmišljena”*

Roba je namijenjena prikrivenom nadzoru kada su njezine tehničke značajke prikladne za prikriveni nadzor fizičkih osoba i objektivno ga omogućuju. Stoga izraz „posebno osmišljena” znači da je prikriveni nadzor fizičkih osoba morao biti glavna svrha razvoja i izrade proizvoda. Međutim, iz tog izraza ne proizlazi da se roba može koristiti samo za prikriveni nadzor fizičkih osoba.

Kako je pojašnjeno u uvodnoj izjavi 8. Uredbe, roba koja se upotrebljava isključivo za komercijalne primjene kao što su plaćanje, stavljanje na tržište, usluge kvalitete, zadovoljstvo korisnika ili sigurnost mreže, nije posebno osmišljena za prikriveni nadzor i stoga nije obuhvaćena definicijom robe za kibernetički nadzor. Na primjer, iako se roba za nadzor operativnih sustava u industriji ili za praćenje prometa korisnika može upotrijebiti za potrebe nadzora, ta roba nije prema definiciji roba za kibernetički nadzor jer nije posebno osmišljena da omogućuje prikriveni nadzor fizičkih osoba.

1.2.2. *„Prikriveni nadzor”*

Roba omogućuje prikriveni nadzor prije svega kad nadzor nije očito zamjetljiv nadziranoj fizičkoj osobi. To bi bio slučaj kada te osobe nisu svjesne prisutnosti i/ili rada robe za kibernetički nadzor pa ne mogu izbjeći taj nadzor ili barem prilagoditi svoje ponašanje u skladu s tim. Čak i ako se nadzor provodi robom koja je postavljena ili radi u javnom prostoru, prikupljanje podataka u određenim se slučajevima može smatrati relevantnim za prikriveni nadzor, posebno ako se prikupljeni podaci mogu preusmjeriti, ocijeniti ili obrađivati u druge svrhe osim onih o kojima je dotična fizička osoba obaviještena. Drugim riječima, ako fizička osoba ne može objektivno očekivati da će biti pod nadzorom, nadzor se može smatrati prikrivenim u skladu s člankom 2. točkom 20. Uredbe.

1.2.3. *„Fizičke osobe”*

Pojam „fizička osoba” odnosi se na živog čovjeka, dakle ne na pravne osobe ili subjekte, na koje se odredbe stoga ne primjenjuju. Taj izraz ne obuhvaća nadzor nad predmetima, lokacijama ili strojevima kao takvima.

1.2.4. *„Praćenje, izdvajanje, prikupljanje, analiziranje podataka”*

Prema Oxfordovu engleskom rječniku riječi praćenje, izdvajanje, prikupljanje i analiziranje imaju sljedeće značenje:

— „praćenje”: motrenje; nadziranje, prisluškivanje,

— „izdvajanje”: odjeljivanje,

— „prikupljanje”: sabiranje, skupljanje,

— „analiziranje”: razlučivanje ili utvrđivanje elemenata nečega (složenog) kako bi se odredila njegova struktura ili priroda, i tako ga se objasnilo ili razumjelo; pomno i metodično ispitivanje u svrhu tumačenja; podvrgavanje kritičkoj ili računalnoj analizi.

Ti izrazi podrazumijevaju da bi roba koja se upotrebljava za nadzor trebala imati jasne tehničke mogućnosti za obradu podataka radi praćenja, prikupljanja, izdvajanja ili analiziranja podataka, kao što je, na primjer, sljedeća roba:

(a) roba koja se upotrebljava za praćenje podataka iz informacijskih i telekomunikacijskih sustava ([4]) (na primjer, veličine datoteke ili prometa paketa podataka koji se prenose u takvom sustavu);

(b) roba koja izdvaja podatke iz informacijskih i telekomunikacijskih sustava provođenjem neovlaštenog ulaska i izdvajanja (na primjer, softver za neovlašteni ulazak);

(c) roba koja omogućuje analizu podataka izdvojenih iz informacijskih i telekomunikacijskih sustava, uključujući onu koja može obrađivati slike kamere pohranjene u tim sustavima (na primjer, određene vrste tehnologija za analizu podataka koje se koriste u sustavima za prepoznavanje lica).

Roba koja se upotrebljava za jednostavno praćenje informacijskih sustava ili promatranje građana putem kamera za videonadzor i koja omogućuje snimanje razgovora, razmjena podataka, kretanja i ponašanja pojedinaca ne bi bila roba za kibernetički nadzor obuhvaćena definicijom iz Uredbe jer nije posebno osmišljena za tu svrhu i mora koristiti druge tehnologije, kao što su umjetna inteligencija ili velika količina podataka. Međutim, cijeli sustav (koji koristi druge tehnologije, kao što su umjetna inteligencija ili tehnologije velikih količina podataka) mogao bi biti roba za kibernetički nadzor prema definiciji iz članka 2. točke 20. Uredbe.

Važno je napomenuti da, iako se navode neki primjeri korisni za ilustraciju, definicija i područje primjene robe za kibernetički nadzor nisu ograničeni tim primjerima jer je cilj članka 5. omogućiti učinkovitu kontrolu izvoza nenavedene robe.

([4]) Za definiciju vidjeti točku 1.2.5. u nastavku.

Kao što je vidljivo iz upotrebe veznika „ili” u definiciji, navedene tehničke mogućnosti treba smatrati alternativama i nije potrebno da roba ima sve te tehničke mogućnosti za praćenje, izdvajanje, prikupljanje ili analiziranje podataka. Drugim riječima, dovoljno je da roba ima jednu od tih tehničkih mogućnosti da bude obuhvaćena definicijom robe za kibernetički nadzor iz članka 2. točke 20.

1.2.5. *„Iz informacijskih i telekomunikacijskih sustava”*

Ti se izrazi odnose na sustave koji elektronički obrađuju informacije, na primjer programiranje/kodiranje, operacije sustava osobnih računala (hardver) i drugo upravljanje informacijama, uključujući softversku tehnologiju, *web*-tehnologiju, računalnu tehnologiju, tehnologiju pohrane itd., te na neke sustave koji prenose informacije na daljinu, na primjer tehničke sustave koji prenose zvukove, signale, tekst, druge znakove i slike žičanim i bežičnim kanalima, optičkim vlaknima, radijskim i drugim elektromagnetskim sustavima. Ta dva koncepta zajedno obuhvaćaju širok raspon sustava za prijenos ili obradu informacija. Treba napomenuti da se taj izraz odnosi na sustave, a ne na opremu.

1.2.6. *„Zna” i „namijenjena”*

Prema članku 5. stavku 2. Uredbe izvoznik obavješćuje nadležno tijelo ako „zna […] da je roba za kibernetički nadzor […] namijenjena za upotrebu u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava”.

Izraz „zna” nije novi pravni koncept i upotrebljava se u kontekstu zahtjeva u pogledu dozvole koji su povezani s krajnjom upotrebom (tzv. sveobuhvatne kontrole) propisanih u člancima 4., 6., 7. i 8. Uredbe. Ako izvoznik „zna”, to znači da ima znanje koje potvrđuje namjeravanu zloupotrebu. Sama mogućnost takvog rizika nije dovoljna da bi se utvrdilo znanje. Međutim, izraz „znanje” ne može se izjednačiti s pasivnošću: on podrazumijeva da je izvoznik poduzeo korake kako bi stekao dostatno i odgovarajuće znanje za procjenu rizika povezanih s izvozom i kako bi osigurao poštovanje Uredbe.

To da roba mora biti „namijenjena” relevantnoj osjetljivoj krajnjoj upotrebi podrazumijeva da bi izvoznik trebao procijeniti krajnju upotrebu u svakom slučaju zasebno, s obzirom na specifične okolnosti konkretnog slučaja. Za razliku od toga, teoretski rizik, to jest rizik koji se ne temelji na ocjeni činjenica konkretnog slučaja, da se roba može upotrijebiti na način kojim se krše ljudska prava ne bi bio dovoljan da se podrazumijeva da je „namijenjena” konkretnoj zloupotrebi u skladu s člankom 5.

1.3. **Unutarnja represija, ozbiljne povrede ljudskih prava i međunarodnog humanitarnog prava**

Na temelju članka 15. Uredbe, u kojem se navode čimbenici za procjenu treba li se izdati dozvola, države članice trebaju uzeti u obzir sve relevantne čimbenike, uključujući one obuhvaćene Zajedničkim stajalištem Vijeća 2008/944/ZVSP ([5]).

Člankom 5. Uredbe kontrole se proširuju na izvoz nenavedene robe za kibernetički nadzor s obzirom na rizik od njezine upotrebe u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava. Zajedničko stajalište 2008/944/ZVSP i Priručnik za provedbu tog Zajedničkog stajališta ([6]) pružaju korisne smjernice u tom pogledu.

([5]) Zajedničko stajalište Vijeća 2008/944/ZVSP od 8. prosinca 2008. o definiranju zajedničkih pravila kojima se uređuje kontrola izvoza vojne tehnologije i opreme (SL L 335, 13.12.2008., str. 99., ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Vidjeti Priručnik za provedbu Zajedničkog stajališta Vijeća 2008/944/ZVSP o definiranju zajedničkih pravila kojima se uređuje kontrola izvoza vojne tehnologije i opreme, https://data.consilium.europa.eu/doc/document/ST-12189-2019-INIT/hr/pdf.

1.3.1. *Unutarnja represija*

Prema članku 2. stavku 2. Zajedničkog stajališta 2008/944/ZVSP „u unutarnju represiju se, između ostalog, ubraja mučenje i drugo okrutno, neljudsko i ponižavajuće postupanje ili kažnjavanje, samovoljna smaknuća ili smaknuća po kratkom postupku, nestanci, samovoljna zatvaranja i druga gruba kršenja ljudskih prava i temeljnih sloboda utvrđenih odgovarajućim međunarodnim instrumentima humanitarnog prava, uključujući Opću deklaraciju o ljudskim pravima i Međunarodni pakt o građanskim i političkim pravima". U Priručniku za provedbu Zajedničkog stajališta 2008/944/ZVSP navode se smjernice o elementima koje treba uzeti u obzir u izvoznikovoj procjeni, uključujući „podatke o trenutačnom i prošlom postupanju predloženog krajnjeg korisnika i države primateljice općenito u odnosu na poštovanje ljudskih prava".

1.3.2. *Počinjenje ozbiljnih povreda ljudskih prava*

Zloupotreba nenavedene robe za kibernetički nadzor može negativno utjecati na širok spektar ljudskih prava i izravno otežavati ostvarivanje prava na privatnost i zaštitu podataka. Proizvoljnim ili nezakonitim nadzorom mogu se kršiti i druga ljudska prava, kao što su pravo na slobodu izražavanja, udruživanja i okupljanja, slobodu mišljenja, savjesti i vjeroispovijesti, kao i pravo na jednako postupanje ili zabranu diskriminacije te pravo na slobodne, ravnopravne i tajne izbore. U određenim slučajevima nadzor, uključujući praćenje ili prikupljanje informacija o fizičkim osobama kao što su borci za ljudska prava, aktivisti, političke ličnosti, ranjive skupine stanovništva i novinari, može dovesti do zastrašivanja, suzbijanja, proizvoljnog pritvaranja, mučenja ili čak izvansudskih pogubljenja. Stoga bi izvoznici u svoje procjene trebali uključiti te aspekte koji se odnose na ozbiljne povrede ljudskih prava.

Međunarodna praksa pokazuje da bilo kakva ograničenja ljudskih prava moraju biti „primjerena" i u skladu s međunarodnim standardima u području ljudskih prava. U praksi to znači da su uspostavljene odgovarajuće zaštitne mjere kojima se osigurava da su ograničenja zakonita i da štite bit pravâ. Podložno načelu proporcionalnosti, ograničenja su moguća samo ako su nužna i ako zaista služe legitimnoj svrsi, na primjer nacionalnoj ili javnoj sigurnosti, javnom poretku, zaštiti javnog zdravlja ili zaštiti prava i sloboda drugih osoba.

Roba za kibernetički nadzor može obuhvaćati legitimne i regulirane alate za suzbijanje kriminaliteta, kao što su alati za sprečavanje, istragu, otkrivanje ili progon kaznenih djela, među ostalim u području borbe protiv terorizma, ili za izvršavanje kaznenih sankcija. No kad se izvozi represivnim režimima ili privatnim krajnjim korisnicima i/ili u područja sukoba, ta se roba za kibernetički nadzor može zloupotrijebiti i za počinjenje ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava.

To zahtijeva procjenu okolnosti svakog pojedinačnog slučaja, što uključuje primjenu relevantnih propisa s obzirom na eventualne informacije o ozbiljnim povredama ljudskih prava o kojima su izvijestila nadležna tijela, primjerice Ujedinjenih naroda, Unije ili Vijeća Europe. Kao pokazatelj ozbiljnosti povreda ljudskih prava može poslužiti potvrda tih povreda u informacijama koje objavljuju nadležna tijela Ujedinjenih naroda, Unija ili Vijeće Europe. Takva izričita potvrda tih tijela nije nužna, ali je važan čimbenik za zadovoljenje tog kriterija.

Prema članku 5. povreda ljudskih prava mora biti „ozbiljna". Korisne smjernice za kategorizaciju mogućih povreda ljudskih prava kao „ozbiljnih" mogu se pronaći u Priručniku za provedbu Zajedničkog stajališta 2008/944/ZVSP. Prema tom priručniku, priroda i posljedice povrede odlučujuće su. Sustavne i/ili raširene povrede ljudskih prava redovito se smatraju ozbiljnima, ali „ozbiljnima" se mogu smatrati i povrede koje nisu sustavne ili raširene, primjerice zbog ozbiljnosti intervencije za pogođene osobe.

Prilog II. Priručniku za provedbu Zajedničkog stajališta 2008/944/ZVSP sadržava nepotpun popis glavnih međunarodnih i regionalnih instrumenata za ljudska prava, uključujući Međunarodni pakt o građanskim i političkim pravima (ICCPR), Konvenciju protiv mučenja i drugih okrutnih, neljudskih ili ponižavajućih postupaka ili kažnjavanja, Europsku konvenciju o ljudskim pravima (Konvencija) i Povelju o temeljnim pravima (Povelja), koji mogu dati važne smjernice za tumačenje i primjenu kriterija koji omogućuju pouzdane procjene ljudskih prava. Ti instrumenti i njihovi dodatni protokoli glavne su međunarodne norme i standardi u područjima ljudskih prava i temeljnih sloboda.

1.3.3. *Počinjenje ozbiljnih povreda međunarodnog humanitarnog prava*

Međunarodno humanitarno pravo (koje se naziva i „ženevsko pravo” ili „pravo oružanog sukoba”) razvijeno je nizom međunarodnih ugovora, prije svega Haškim pravilnikom, Ženevskim konvencijama i njihovim dvama dodatnim protokolima iz 1977., i njime se utvrđuju pravila koja u vrijeme oružanog sukoba služe za zaštitu osoba koje ne sudjeluju ili više ne sudjeluju u sukobima (na primjer civili i ranjeni, bolesni ili zarobljeni borci) i zaraćenim stranama nameću ograničenja u pogledu sredstava i metoda ratovanja (haško pravo).

Upotreba nenavedene robe za kibernetički nadzor kao sredstva i metode ratovanja u kontekstu oružanog sukoba trebala bi biti u skladu s međunarodnim humanitarnim pravom. U takvim je okolnostima rizik od ozbiljnih povreda međunarodnog humanitarnog prava čimbenik obuhvaćen Uredbom te bi ga, kao i za počinjenje ozbiljnih povreda ljudskih prava, trebalo procijeniti s obzirom na predviđenu krajnju upotrebu robe u konkretnom slučaju. U Priručniku za provedbu Zajedničkog stajališta 2008/944/ZVSP navode se smjernice o elementima koje treba uzeti u obzir, uključujući podatke o primateljevu poštovanju međunarodnog humanitarnog prava u prošlosti i danas, primateljeve namjere izražene formalnim obvezama i primateljevu sposobnost da osigura korištenje prenesene opreme ili tehnologije u skladu s međunarodnim humanitarnim pravom i spriječi njezino preusmjeravanje ili prenošenje na druga odredišta gdje bi se mogla upotrijebiti za ozbiljne povrede tog prava.

Prema članku 5. povreda međunarodnog humanitarnog prava mora biti „ozbiljna”. Smjernice se mogu pronaći u Priručniku za provedbu Zajedničkog stajališta 2008/944/ZVSP u kojima se potvrđuje da „izolirani slučajevi kršenja međunarodnog humanitarnog prava ne moraju neophodno ukazivati na odnos države primateljice prema međunarodnom humanitarnom pravu”, a „uzrok ozbiljne zabrinutosti trebao bi se odnositi na slučajeve u kojima je moguće razaznati određeni obrazac kršenja ili u kojima država primateljica nije poduzela odgovarajuće korake za kažnjavanje tih kršenja”. Međunarodni odbor Crvenog križa (ICRC) dao je smjernice za procjenu povreda međunarodnog humanitarnog prava u svrhu kontrole izvoza. Prema mišljenju Međunarodnog odbora Crvenog križa „povrede međunarodnog humanitarnog prava ozbiljne su ako ugrožavaju zaštićene osobe (na primjer civile, ratne zarobljenike, ranjenike i bolesnike) ili objekte (na primjer civilne objekte ili infrastrukturu) ili ako krše važne univerzalne vrijednosti”. Primjerice, ratni zločini su ozbiljne povrede međunarodnog humanitarnog prava. Međunarodni odbor Crvenog križa nadalje spominje slične čimbenike koje treba uzeti u obzir kao i Priručnik za provedbu Zajedničkog stajališta 2008/944/ZVSP, uključujući formalne obveze primjene pravila međunarodnog humanitarnog prava, odgovarajuće mjere kojima se osigurava odgovornost za povrede međunarodnog humanitarnog prava, educiranje pripadnika vojske o međunarodnom humanitarnom pravu i zabranu novačenja djece u oružane snage.

2. **TEHNIČKO PODRUČJE PRIMJENE**

2.1. **Navedena roba za kibernetički nadzor**

Dodatak ovim smjernicama sadržava informacije o robi za kibernetički nadzor navedenoj u Prilogu I. Uredbi kako bi se izvoznicima pomoglo u utvrđivanju potencijalne nenavedene robe za kibernetički nadzor.

2.2. **Potencijalna nenavedena roba za kibernetički nadzor**

Iako je po definiciji nemoguće sastaviti potpun popis proizvoda koji se mogu kontrolirati kao „nenavedena roba” na temelju članka 5., sljedeća roba mogla bi se koristiti za nadzor i zato prema Uredbi s njom treba biti posebno oprezan.

Kako je pojašnjeno u uvodnoj izjavi 8. Uredbe, za robu koja se upotrebljava isključivo za komercijalne primjene kao što su plaćanje, stavljanje na tržište, usluge kvalitete, zadovoljstvo korisnika ili sigurnost mreže općenito se smatra da ne nosi rizike od zloupotrebe relevantne u slučaju ozbiljnih povreda ljudskih prava ili međunarodnog humanitarnog prava, pa općenito ne podliježe kontroli na temelju članka 5. Mnogi od tih proizvoda imaju funkcionalnosti za sigurnost informacija (kriptografske ili čak kriptanalitičke) koje ispunjavaju kontrolne parametre iz kategorije 5. dijela 2. teksta o kontroli iz Priloga I. Uredbi. Ni sigurnosna mrežna oprema (uključujući rutere, preklopnike ili releje) nije obuhvaćena definicijom „robe za kibernetički nadzor” ako je funkcionalnost za sigurnost informacija ograničena na zadatke „rada, administriranja ili održavanja” kojima se provode samo objavljeni ili komercijalni kriptografski standardi, ali bi izvoznici ipak trebali ostati oprezni i uzeti u obzir da su zabilježene razne zloupotrebe takve robe za povrede ljudskih prava.

2.2.1. *Tehnologija prepoznavanja lica i emocija*

Tehnologije prepoznavanja lica i emocija imaju i druge namjene osim kibernetičkog nadzora, primjerice identifikaciju ili autentifikaciju, pa nisu automatski obuhvaćene definicijom. Međutim, u određenim okolnostima tehnologije prepoznavanja lica i emocija mogu biti obuhvaćene područjem primjene članka 2. točke 20. Uredbe.

Tehnologije prepoznavanja lica i emocija koje se mogu upotrebljavati za praćenje ili analizu pohranjenih videozapisa mogle bi biti obuhvaćene definicijom robe za kibernetički nadzor. Međutim, čak i ako su gore navedeni kriteriji ispunjeni, potrebno je pažljivo ispitati je li softver posebno osmišljen za prikriveni nadzor.

2.2.2. *Uređaji za praćenje lokacije*

Uređaji za praćenje lokacije omogućuju praćenje fizičke lokacije uređaja u određenom razdoblju, a tijela kaznenog progona i obavještajne agencije već neko vrijeme upotrebljavaju određene tehnologije za praćenje lokacije. Njihov potencijal za ciljani i masovni nadzor znatno se povećao otkako su uznapredovale tehnologije praćenja, među ostalim satelitskog praćenja lokacije, praćenja lokacije pomoću baznih postaja, Wi-Fi i Bluetooth primoodašiljača, i otkako su se „uređaji za praćenje" kao što su pametni telefoni i drugi elektronički uređaji (npr. sustavi ugrađeni u vozilo) uobičajili.

Tijela kaznenog progona i obavještajne agencije upotrebljavaju uređaje za praćenje lokacije primjerice za prikupljanje dokaza tijekom istrage ili za praćenje osumnjičenika, ali ih upotrebljavaju i poduzeća u komercijalne svrhe, na primjer za izvješćivanje o agregiranim obrascima kretanja u trgovačkim ulicama, praćenje zaposlenika na terenu ili za oglašavanje na temelju lokacije.

2.2.3. *Sustavi videonadzora*

Kako bi se izvoznicima pomoglo u utvrđivanju mogućeg kibernetičkog nadzora, korisno je pojasniti i koja roba ne bi bila obuhvaćena njegovom definicijom. U tom smislu, primjerice sustavi videonadzora i kamere (uključujući kamere visoke rezolucije) koji se upotrebljavaju za snimanje ljudi u javnim prostorima nisu obuhvaćeni definicijom robe za kibernetički nadzor jer se njima ne prate niti prikupljaju podaci iz informacijskih i telekomunikacijskih sustava.

3. **MJERE DUŽNE PAŽNJE**

U skladu s uvodnom izjavom 7. Uredbe „doprinos izvoznika […] općem cilju trgovinskih kontrola je ključan. Kako bi mogli djelovati u skladu s ovom Uredbom, procjenu rizika povezanih s transakcijama na koje se odnosi ova Uredba treba provoditi mjerama provjere transakcija, poznatima i kao načelo dužne pažnje, kao dio programa unutarnje usklađenosti".

U članku 2. točki 21. program unutarnje usklađenosti definira se kao „trajne učinkovite, primjerene i razmjerne politike i postupci koje su donijeli izvoznici kako bi omogućili usklađenost s odredbama i ciljevima iz ove Uredbe te s uvjetima dozvola koji se provode u skladu s ovom Uredbom, uključujući, među ostalim, mjere dužne pažnje kojima se ocjenjuju rizici povezani s izvozom robe krajnjim korisnicima i krajnjim upotrebama".

Preporuka Komisije (EU) 2019/1318 ([7]) je okvir koji izvoznicima pomaže u utvrđivanju, upravljanju i ublažavanju rizika povezanih s kontrolama trgovine robom s dvojnom namjenom i okvir za jamčenje usklađenosti s relevantnim Unijinim i nacionalnim zakonima i propisima.

Ove smjernice izvoznicima mogu pomoći u provedbi mjera provjere transakcija, poznatih i kao načelo dužne pažnje, u okviru programa unutarnje usklađenosti.

U skladu s člankom 5. stavkom 2. Uredbe (EU) 2021/821 izvoznici nenavedene robe za kibernetički nadzor dužni su provesti dubinsku analizu mjerama provjere transakcija, što znači poduzimanje koraka za klasifikaciju robe i procjenu rizika transakcije. U praksi se izvoznike potiče na sljedeće:

([7]) Preporuka Komisije (EU) 2019/1318 od 30. srpnja 2019. o programima unutarnjeg usklađivanja za kontrole trgovine robom s dvojnom namjenom u skladu s Uredbom Vijeća (EZ) br. 428/2009 (SL L 205, 5.8.2019., str. 15., ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Provjera je li nenavedena roba koja se izvozi možda „roba za kibernetički nadzor”, tj. posebno osmišljena kako bi se omogućio prikriveni nadzor fizičkih osoba praćenjem, izdvajanjem, prikupljanjem ili analiziranjem podataka iz informacijskih i telekomunikacijskih sustava**

Ovaj se korak odnosi na utvrđivanje robe u skladu s odredbama koje se primjenjuju na robu za kibernetički nadzor. To uključuje provjeru tehničkih karakteristika robe s obzirom na tehničke parametre iz Priloga I. Uredbi ako je riječ o robi navedenoj na popisu, odnosno s obzirom na specifične izraze i koncepte iz definicije robe za kibernetički nadzor ako je riječ o nenavedenoj robi, i s obzirom na naknadnu klasifikaciju robe (roba, tehnologija ili softver).

3.2. **Pregled mogućnosti predmetne robe kako bi se utvrdio potencijal zloupotrebe u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava od strane inozemnih krajnjih korisnika**

Izvoznici bi trebali procijeniti može li se proizvod zloupotrijebiti za unutarnju represiju, kršenje ili povredu ljudskih prava, uključujući pravo na život, slobodu od mučenja, nečovječnog i ponižavajućeg postupanja, pravo na privatnost, pravo na slobodu govora, pravo na udruživanje i okupljanje, pravo na slobodu mišljenja, savjesti i vjeroispovijesti, pravo na jednako postupanje ili zabranu diskriminacije ili pravo na slobodne, jednake i tajne izbore.

To uključuje i procjenu može li se proizvod upotrebljavati kao dio ili komponenta sustava koji bi mogao dovesti do istih kršenja i/ili zloupotrebe.

Izvoznici bi u svojoj procjeni trebali koristiti tzv. znakove upozorenja, odnosno sve neuobičajene okolnosti u transakciji koje upućuju na to da bi krajnja upotreba, krajnji korisnik ili odredište robe koja se izvozi mogli biti neprimjereni.

Znakovi upozorenja:

(a) roba se stavlja na tržište s informacijama povezanima s njezinom mogućom upotrebom za prikriveni nadzor;

(b) informacije koje upućuju na to da se slična roba zloupotrebljavala u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava (vidjeti odjeljak 1.3.);

(c) informacije koje upućuju na to da je roba nezakonito korištena u aktivnostima nadzora usmjerenima protiv države članice ili u vezi s nezakonitim nadzorom građanina EU-a;

(d) informacije koje upućuju na to da transakcija uključuje robu koja bi se mogla upotrijebiti za uspostavu, prilagodbu ili konfiguraciju sustava za koji je poznato da je zloupotrijebljen u vezi s unutarnjom represijom i/ili počinjenjem ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava (vidjeti odjeljak 1.3.);

(e) roba ili slična roba nalazi se na popisu objavljenom u seriji C *Službenog lista Europske unije* u skladu s člankom 5. stavkom 6. Uredbe.

3.3. **Provjera dionika uključenih u transakciju (uključujući krajnjeg korisnika i primatelje kao što su distributeri i preprodavači) kao pomoć nadležnim tijelima**

Kao pomoć nadležnim tijelima, i u mjeri u kojoj je to moguće izvoznici bi trebali:

(a) prije i tijekom bilo koje transakcije provjeriti kako primatelji i/ili krajnji korisnici namjeravaju upotrebljavati proizvod ili uslugu, na temelju izjava o krajnjoj upotrebi;

(b) upoznati se sa situacijom u relevantnom odredištu robe, posebno s općim stanjem ljudskih prava, jer je to važan pokazatelj rizika od ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava povezanih s izvozom;

(c) razmotriti rizik da će proizvod ili usluga biti preusmjereni drugom neovlaštenom krajnjem korisniku, na temelju znakova upozorenja navedenih u nastavku.

Znakovi upozorenja:

(a) krajnji korisnik ima očit odnos sa stranom vladom koja je u prošlosti počinila unutarnju represiju i/ili ozbiljne povrede ljudskih prava i međunarodnog humanitarnog prava;

(b) krajnji korisnik je strukturni dio oružanih snaga ili druge skupine uključene u oružani sukob koji obuhvaća mjere unutarnje represije i/ili ozbiljne povrede ljudskih prava i međunarodnog humanitarnog prava u prošlosti;

(c) krajnji korisnik u prošlosti je izvozio robu za kibernetički nadzor u zemlje u kojima je upotreba takve robe dovela do mjera unutarnje represije i/ili ozbiljnih povreda ljudskih prava i međunarodnog humanitarnog prava.

3.4. Upotreba rezultata dubinske analize za izradu planova za sprečavanje i ublažavanje potencijalnih budućih štetnih učinaka

Izvoznici bi, na temelju rezultata svoje dubinske analize, trebali obustaviti aktivnosti koje uzrokuju štetne učinke povezane s ljudskim pravima ili im doprinose, te izraditi i provesti korektivni akcijski plan. Taj plan može uključivati:

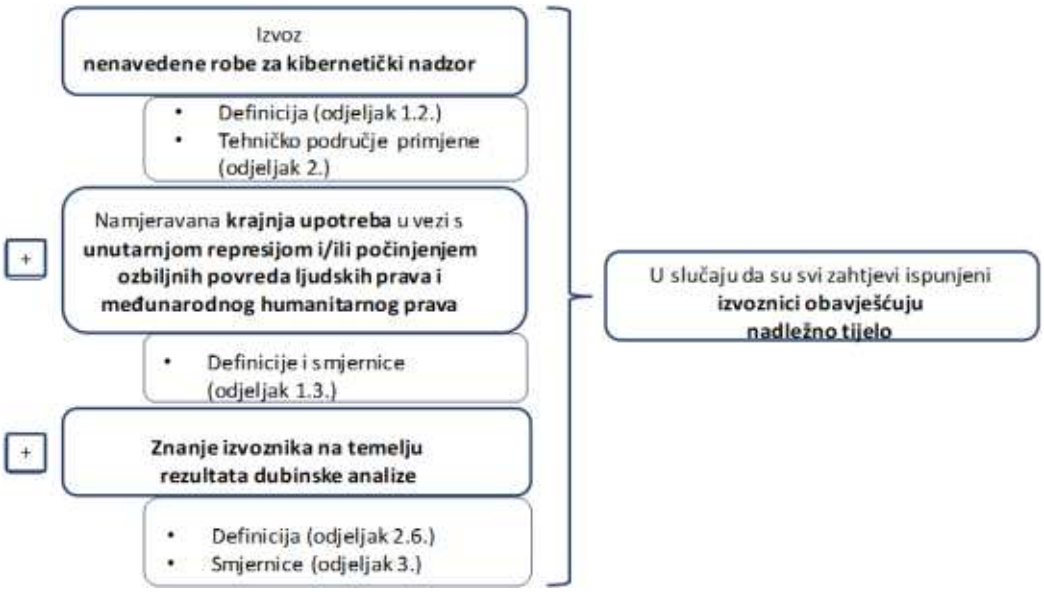
(a) ažuriranje politika poduzeća tako da se daju smjernice o tome kako izbjeći i ukloniti štetne učinke u budućnosti i osigura njihova provedba;

(b) ažuriranje i poboljšanje sustava upravljanja na temelju rezultata procjene rizika kako bi se bolje pratile informacije i upozorilo na rizike prije pojave štetnih učinaka;

(c) prikupljanje informacija kako bi se razumjeli veliki rizici štetnih učinaka povezanih sa sektorom;

(d) obavješćivanje nadležnih tijela država članica o rezultatima dubinske analize kako bi se olakšao protok informacija o određenoj robi, krajnjim korisnicima i odredištima.

Zahtjevi iz članka 5. Stavka 2. Uredbe (EU) 2021/821



4. DODATAK

Navedena roba za kibernetički nadzor kako je kontrolirana Prilogom I. Uredbi (EU) 2021/821

— **Sustavi za presretanje telekomunikacija (5A001.f.)**

U većini zemalja, uključujući države članice, povjerljivost komunikacija zaštićena je zakonom, ali prikriveni elektronički nadzor komunikacija koji provode državna tijela može se odobriti u skladu s propisima (tzv. zakonito presretanje). Međutim, digitalno doba omogućilo je da se tehnologije za presretanje koriste nad velikim brojem ljudi. Način na koji je libijski režim koristio alate za presretanje pokazao je da te tehnologije imaju potencijal za primjenu u velikim razmjerima i potaknuo uvođenje kontrola izvoza sustava za presretanje telekomunikacija 2012.

Ta kontrola primjenjuje se na opremu namijenjenu izdvajanju sadržaja komunikacije (glasa ili podataka), kao i identifikatora pretplatnika ili drugih metapodataka koji se prenose zrakom putem bežične komunikacije te na opremu za radiofrekvencijsko praćenje. Ta se kontrola primjenjuje, na primjer, na uređaje za presretanje međunarodnog identifikatora pokretnog pretplatnika (IMSI *catcher*) koji presreću promet mobilnih telefona i prate kretanje korisnika mobilnih telefona ili na opremu koja stvara lažne pristupne točke za Wi-Fi i koja može izdvojiti IMSI brojeve s telefona, kao i na određene vrste robe posebno osmišljene da omoguće dubinsku analizu sadržaja paketa u telekomunikacijskim sustavima. Oprema za ometanje mobilnih telekomunikacija nije obuhvaćena područjem primjene robe za kibernetički nadzor jer se njome ne prikupljaju podaci.

Iako je takve sustave moguće izraditi korištenjem tehnologija opće namjene, njihove mogućnosti masovnog presretanja ovisit će o specifičnim dijelovima i komponentama, npr. o specifičnom softveru, naprednim integriranim sklopovima ili integriranim sklopovima specifične namjene (primjerice FPGA, ASIC itd.) za povećanje broja paketa ili komunikacijskih sesija koji se mogu obraditi u sekundi.

— **Sustavi za nadzor interneta (5A001.j.)**

Iako se danas mnoge internetske komunikacije obično automatski šifriraju, presretanje komunikacijskih podataka (metapodataka) iz internetskog prometa, kao što su IP adrese te učestalost i veličina razmjene podataka, i dalje se može upotrebljavati da se utvrde veze između osoba i naziva domena. Vlade se mogu koristiti tim sustavima zakonito i uz sudski nadzor u legitimne svrhe, kao što je identifikacija osoba koje posjećuju domene povezane s kriminalnim ili terorističkim sadržajem. No, praćenje i analiza internetskog prometa na temelju etničkih, vjerskih, političkih ili društvenih obilježja mogu se iskoristiti za sveobuhvatno mapiranje pojedinaca i društva neke zemlje radi kontrole stanovništva i represije, kao i u druge svrhe, primjerice za identificiranje političkih disidenata. Uz to što je sporna u pogledu ljudskih prava i unutarnje represije, ta roba može doprinijeti i jačanju sigurnosnih i vojnih sposobnosti.

Kontrola na temelju stavke 5A001.j primjenjuje se na sustave za kontrolu interneta koji rade na „carrier-class IP mreži (npr. okosnica IP mreže nacionalne kategorije)" radi analize, izdvajanja i indeksiranja prenesenog sadržaja metapodataka (glas, videozapis, poruke, privitci) na temelju „trajnih selektora" te mapiranja relacijske mreže ljudi. Riječ je o robi koja izvodi „prikriveni nadzor" jer ciljane osobe nisu svjesne presretanja komunikacije. S druge strane, kontrole ne zahvaćaju sustave u kojima postoji aktivnost korisnika ili pretplatnika ili interakcija s njim te se, na primjer, ne primjenjuju na društvene mreže ili komercijalne tražilice. Nadalje, kontrole se primjenjuju na sustave koji obrađuju podatke koji dolaze iz jezgrene mreže pružatelja internetskih usluga i ne primjenjuju se na društvene mreže ili komercijalne tražilice koje obrađuju podatke koje su korisnici dali.

— **„Softver za neovlašteni ulazak" (4A005, 4D004 i povezane kontrole iz 4E001.a. i 4E001.c.)**

Softver za neovlašteni ulazak omogućuje osobi koja ga koristi da prikriveno dobije daljinski pristup elektroničkom uređaju (kao što je pametni telefon, prijenosno računalo, poslužitelj ili uređaj koji koristi internet stvari), da pribavlja podatke pohranjene na uređaju, da prisluškuje putem kamere ili mikrofona koji su ugrađeni u uređaj ili povezani s njim te da koristi uređaj kao sredstvo za izvođenje napada na opremu na koju se uređaj spaja ili na kontakte korisnika („hakiranje putem uređaja treće strane"). Iako postoje legitimne upotrebe ([8]) softvera za neovlašteni ulazak, primjerice „softver za daljinski pristup" koji se upotrebljava za podršku na daljinu informatičkih službi, prikrivena priroda nadzora i količina informacija koje se mogu prikupiti predstavljaju visok rizik od povrede prava na privatnost i zaštitu osobnih podataka te mogu ozbiljno ugroziti pravo na slobodu izražavanja.

([8]) Radi jasnoće, dozvola za izvoz u treće zemlje bila bi potrebna za robu za kibernetički nadzor navedenu na popisu koja je pod kontrolom u okviru Priloga I. Uredbi o robi s dvojnom namjenom, bez obzira na to je li upotreba te robe legitimna.

Kontrola na temelju stavke 4A005 i dr. obuhvaća softver te sustave, opremu, komponente i s njima povezanu tehnologiju, posebno osmišljene ili preinačene za stvaranje, naredbe i kontrolu ili isporuku „softvera za neovlašteni ulazak”, ali se ne odnosi na sam „softver za neovlašteni ulazak”, kako je definiran u Prilogu I. Uredbi. Ti kibernetički alati kontroliraju se uzimajući u obzir moguće poremećaje i štetu koje mogu uzrokovati ako se uspješno upotrebljavaju i izvršavaju, ali kontrole nisu namijenjene tome da, primjerice, utječu na aktivnost istraživača i sektora kibernetičke sigurnosti jer oni moraju razmjenjivati informacije o softveru za neovlašteni ulazak kako bi mogli izrađivati zakrpe za svoje proizvode i instalirati ih prije objave ranjivosti.

— **Softver za praćenje komunikacije (5D001.e.)**

Taj softver služi ovlaštenim tijelima kaznenog progona za praćenje i analiziranje podataka prikupljenih ciljanim mjerama presretanja koje su zatražili od pružatelja komunikacijskih usluga. Omogućuje pretraživanje na temelju „trajnih selektora” komunikacijskog sadržaja ili metapodataka, pomoću sučelja za zakonito presretanje, i mapiranje relacijske mreže ili praćenje kretanja ciljanih pojedinaca na temelju rezultata pretraživanja. Taj je softver namijenjen „prikrivenom nadzoru” jer koristi podatke prikupljene presretanjem komunikacije bez znanja nadziranih osoba. Nadalje, on „analizira” podatke prikupljene putem „telekomunikacijskih sustava”. Softver se instalira u državnom tijelu (na primjer, operativno-tehničkom centru za nadzor telekomunikacija (*Law Enforcement Monitoring Facility* – LEMF)), a kontrola se ne primjenjuje na sustave za sukladnost zakonitog presretanja s propisima (npr. sustavi za upravljanje zakonitim presretanjem i uređaji za posredovanje) koji su komercijalno razvijeni i instalirani u prostorima pružatelja komunikacijskih usluga (npr. integrirani u komunikacijsku mrežu), kojima pružatelj usluga upravlja i održava ih. Kako je pojašnjeno u tekstu o kontroli, kontrole se ne primjenjuju na „softver” posebno osmišljen ili izmijenjen za isključivo komercijalne svrhe kao što su plaćanje, kvaliteta usluge u mreži (QoS), kvaliteta iskustva (QoE), uređaji za posredovanje ili mobilno plaćanje ili upotreba u bankarstvu.

— **Roba koja se upotrebljava za kriptoanalizu (5A004.a.)**

Ta kontrola primjenjuju se na robu osmišljenu za probijanje kriptografskih mehanizama kako bi se dobile povjerljive varijable ili osjetljivi podaci, uključujući nekriptirani tekst, lozinke ili kriptografske ključeve. Kriptografija se upotrebljava za zaštitu povjerljivosti informacija u prijenosu i u stanju mirovanja. Kriptoanaliza služi za narušavanje te povjerljivosti i prema tome ta tehnologija „omogućuje” prikriveni nadzor praćenjem, izdvajanjem, prikupljanjem ili analiziranjem podataka iz informacijskih i telekomunikacijskih sustava.

— **Forenzički/istražni alati (5A004.b., 5D002.a.3.b. i 5D002.c.3.b.)**

Forenzički/istražni alati osmišljeni su za izdvajanje neobrađenih podataka iz uređaja (primjerice računalnog ili komunikacijskog) tako da se podaci ne mijenjaju neovlašteno niti oštećuju i da se mogu upotrebljavati u sudske svrhe, tj. u kaznenoj istrazi ili na sudu. Ti proizvodi zaobilaze „autentifikaciju” ili autorizacijske kontrole uređaja kako bi se neobrađeni podaci mogli izdvojiti iz proizvoda. Državna tijela i tijela kaznenog progona, ali i vojne snage upotrebljavaju te proizvode za izdvajanje i analizu podataka iz zaplijenjenih uređaja. Iako imaju legitimne primjene, mogu se zloupotrijebiti pa su rizične za osjetljive ili komercijalne podatke.

Međutim, forenzički/istražni alati koji nisu „posebno osmišljeni” za prikriveni nadzor nisu obuhvaćeni definicijom robe za kibernetički nadzor iz članka 2. točke 20. Osim toga, forenzički/istražni alati koji samo izdvajaju korisnikove podatke ili ako su podaci nezaštićeni na uređaju nisu obuhvaćeni tekstom o kontroli u stavci 5A004.b. i drugima. Istodobno se kontrole ne primjenjuju na proizvodnu ili ispitnu opremu proizvođača, alate za administratore sustava ili proizvode isključivo namijenjene komercijalnom maloprodajnom sektoru, primjerice proizvode za otključavanje mobilnih telefona. Stoga, s obzirom na raznolikost tih vrsta tehnologije, primjena kontrola ovisi o pojedinačnoj procjeni svakog proizvoda.

Naposljetku, treba napomenuti da je u Prilogu I. Uredbi navedena druga roba povezana s nadzorom koju ne bi trebalo smatrati obuhvaćenom definicijom robe za kibernetički nadzor, kao što je mobilna telekomunikacijska oprema za ometanje (5A001.f.) namijenjena oštećivanju ili ometanju komunikacije ili sustava, softver za neovlašteni ulazak kojim se mijenja sustav (4D004) i laserska oprema za otkrivanje zvuka (6A005.g.) koja laserom prikuplja audiopodatke ili omogućuje daljinsko prisluškivanje (ponekad se naziva „laserski mikrofon”). Slično tome, ako se navedene bespilotne zračne letjelice upotrebljavaju za potrebe nadzora, to ne znači da su obuhvaćene definicijom robe za kibernetički nadzor.