Uradni list
Evropske unije

SL
Serija L

2024/2659

16.10.2024

PRIPOROČILO KOMISIJE (EU) 2024/2659

z dne 11. oktobra 2024

o smernicah glede izvoza blaga za kibernetski nadzor iz člena 5 Uredbe (EU) 2021/821 Evropskega parlamenta in Sveta

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 292 Pogodbe,

ob upoštevanju naslednjega:

(1) Z Uredbo (EU) 2021/821 Evropskega parlamenta in Sveta ([1]) je bil vzpostavljen režim Unije za nadzor izvoza, posredovanja, tehnične pomoči, tranzita in prenosa blaga z dvojno rabo.

(2) V Uredbi (EU) 2021/821 je obravnavano tveganje uporabe blaga za kibernetski nadzor v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava.

(3) Na podlagi členov 5(2) in 26(1) Uredbe (EU) 2021/821 Komisija in Svet izvoznikom izdata smernice glede blaga za kibernetski nadzor, ki ni navedeno na seznamu, da se zagotovita učinkovitost režima Unije za nadzor izvoza v zvezi s kibernetsko varnostjo in doslednost izvajanja Uredbe (EU) 2021/821.

(4) Namen tega priporočila in priloženih smernic je podpreti izvoznike pri izvajanju nadzora nad blagom za kibernetski nadzor, ki ni navedeno na seznamu, med drugim z ukrepi skrbnih pregledov za oceno tveganj, povezanih z izvozom takega blaga.

(5) O smernicah, priloženih temu priporočilu, se je v letih 2022 in 2023 obsežno posvetovala strokovna skupina za tehnologijo nadzora, v njih pa so upoštevane tudi pripombe, prejete med javnim posvetovanjem ([2]), izvedenim v drugem četrtletju leta 2023.

(6) Opozoriti je treba, da to priporočilo in priložene smernice niso zavezujoči. Zato bi morali izvozniki ostati odgovorni za izpolnjevanje svojih obveznosti iz Uredbe (EU) 2021/821, Komisija pa bi morala zagotavljati, da bo to priporočilo ostalo relevantno –

([1]) Uredba (EU) 2021/821 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi režima Unije za nadzor izvoza, posredovanja, tehnične pomoči, tranzita in prenosa blaga z dvojno rabo (UL 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.

SPREJELA NASLEDNJE PRIPOROČILO:

Priporoča se, da pristojni organi držav članic in izvozniki za izpolnjevanje svojih obveznosti iz člena 5(2) Uredbe (EU) 2021/821 upoštevajo smernice iz Priloge k temu priporočilu.

V Bruslju, 11. oktobra 2024

Za Komisijo
Valdis DOMBROVSKIS
izvršni podpredsednik

PRILOGA

KAZALO

Stran

Uvod ... 4

1. Relevantne pravne določbe, opredelitev pojmov in ključni pojmi ... 4

1.1. Pregled relevantnih pravnih določb ... 4

1.2. Ključne opredelitve pojmov ... 5

1.2.1. „Posebej zasnovano“ ... 5

1.2.2. „Tajni nadzor“ ... 6

1.2.3. „Fizične osebe“ ... 6

1.2.4. „Spremljanje, pridobivanje, zbiranje in analiza podatkov“ ... 6

1.2.5. „Iz informacijskih in telekomunikacijskih sistemov“ ... 7

1.2.6. „Je znano“ in „je namenjeno za“ ... 7

1.3. Notranja represija, hude kršitve človekovih pravic in mednarodnega humanitarnega prava ... 7

1.3.1. Notranja represija ... 8

1.3.2. Huda kršitev človekovih pravic ... 8

1.3.3. Huda kršitev mednarodnega humanitarnega prava ... 9

2. Tehnično področje uporabe ... 9

2.1. Blago za kibernetski nadzor, navedeno na seznamu ... 9

2.2. Potencialno blago za kibernetski nadzor, ki ni navedeno na seznamu ... 9

2.2.1. Tehnologija za prepoznavanje obrazov in čustev ... 10

2.2.2. Naprave za sledenje lokaciji ... 10

2.2.3. Sistemi za videonadzor ... 10

3. Ukrepi izvajanja skrbnih pregledov ... 10

Zahteve iz člena 5(2) Uredbe (EU) 2021/821 ... 12

4. Dodatek ... 12

Blago za kibernetski nadzor, ki se nadzoruje v skladu s Prilogo I k Uredbi (EU) 2021/821 ... 12

Sistemi za prestrezanje telekomunikacij (5A001.f) ... 12

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

Vdorna programska oprema (4A005, 4D004 in povezani nadzor iz točk 4E001.a in 4E001.c) ... 13

Programska oprema za spremljanje komunikacij (5D001.e) ... 13

Blago, ki se uporablja za izvajanje kriptoanalize (5A004.a) ... 14

Forenzična/preiskovalna orodja (5A004.b, 5D002.a.3.b in 5D002.c.3.b) ... 14

UVOD

Namen okvira Unije za nadzor izvoza, vzpostavljenega z Uredbo (EU) 2021/821 (v nadaljnjem besedilu: Uredba), je zagotoviti spoštovanje mednarodnih obveznosti in zavez Unije in njenih držav članic, med drugim v zvezi z regionalnim mirom, varnostjo in stabilnostjo ter spoštovanjem človekovih pravic in mednarodnega humanitarnega prava. Unija in njene države članice so zato uresničile odločitve, sprejete v okviru večstranskih režimov za nadzor izvoza, in ustrezno posodobile seznam Unije za nadzor iz Priloge I k Uredbi ([1]). Poleg tega so pristojni organi držav članic že pred začetkom uporabe člena 5 Uredbe nadzirali izvoz določenega blaga s seznama, ki bi se lahko uporabljalo za nadzor ([2]), pri čemer so upoštevali tveganja zlorabe v nekaterih posebnih okoliščinah. V izjemno resnih okoliščinah je Unija uvedla sankcije za omejitev izvoza določene opreme za nadzor ([3]).

V Uredbi se odraža zaveza Unije k učinkovitemu odpravljanju tveganja, da bi se blago za kibernetski nadzor uporabljalo v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava. Z Uredbo so bile zlasti uvedene nove določbe za nadzor izvoza blaga za kibernetski nadzor, ki ni navedeno na seznamu, vključno z obveznostjo izvoznikov, da obvestijo pristojni organ, kadar jim je glede na ugotovitve iz skrbnega pregleda znano, da je blago za kibernetski nadzor, ki ni navedeno na seznamu in ga nameravajo izvozniki izvoziti, kot celota ali po delih namenjeno za uporabo v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava. Poleg tega sta v Uredbi Komisija in Svet pozvana, naj v podporo učinkovitemu izvajanju novega nadzora nad blagom za kibernetski nadzor, ki ni navedeno na seznamu, izdata smernice za izvoznike.

Namen smernic je torej podpreti izvoznike pri izvajanju nadzora nad blagom za kibernetski nadzor, ki ni navedeno na seznamu, med drugim vključno z ukrepi izvajanja skrbnih pregledov za oceno tveganj, povezanih z izvozom blaga končnim uporabnikom in končno uporabo v skladu z novimi določbami Uredbe.

1. RELEVANTNE PRAVNE DOLOČBE, OPREDELITVE POJMOV IN KLJUČNI POJMI

1.1. Pregled relevantnih pravnih določb

Uredba vsebuje nove določbe, ki govorijo izrecno o nadzoru nad izvozom blaga za kibernetski nadzor, ki ni navedeno v Prilogi I k Uredbi ter je ali bi lahko bilo kot celota ali po delih namenjeno za uporabo v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava. Upoštevne uvodne izjave in členi so:

(a) uvodna izjava 8: „Da bi obravnavali tveganje, da bi blago za kibernetski nadzor, ki ni navedeno na seznamu in bi se izvozilo s carinskega območja Unije, lahko zlorabile osebe, ki so vpletene v ali odgovorne za vodenje ali izvajanje hudih kršitev človekovih pravic ali mednarodnega humanitarnega prava, je treba nadzorovati izvoz tega blaga. S tem povezana tveganja zadevajo zlasti primere, ko je blago za kibernetski nadzor posebej zasnovano tako, da omogoča vdiranje v informacijske in telekomunikacijske sisteme ali temeljit pregled paketov v njih za tajni nadzor fizičnih oseb s spremljanjem, pridobivanjem, zbiranjem ali analizo podatkov, vključno z biometričnimi podatki, iz teh sistemov. Za

([1]) Glej zlasti nadzor v zvezi s sistemi za prestrezanje telekomunikacij (5A001.f), sistemi za nadzor interneta (5A001.j), vdorno programsko opremo (4A005, 4D004 in povezan nadzor iz točk 4E001.a in 4E001.c) ter programsko opremo za spremljanje s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (5D001.e). Poleg tega glej na podlagi ocene posameznih primerov nadzor v zvezi z nekaterimi forenzičnimi/preiskovalnimi orodji (5A004.b, 5D002.a.3.b in 5D002.c.3.b).

([2]) Zlasti sistemi informacijske varnosti.

([3]) Glej Uredbo Sveta (ES) št. 765/2006 z dne 18. maja 2006 o omejevalnih ukrepih zaradi razmer v Belorusiji in vpletenosti Belorusije v rusko agresijo proti Ukrajini (UL L 134, 20.5.2006, str. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Uredbo Sveta (EU) št. 359/2011 z dne 12. aprila 2011 o omejevalnih ukrepih proti nekaterim osebam, subjektom in organom zaradi razmer v Iranu (UL L 100, 14.4.2011, str. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Uredbo Sveta (EU) št. 36/2012 z dne 18. januarja 2012 o omejevalnih ukrepih glede na razmere v Siriji in razveljavitvi Uredbe (EU) št. 442/2011 (UL L 16, 19.1.2012, str. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Uredbo Sveta (EU) št. 401/2013 z dne 2. maja 2013 o omejevalnih ukrepih v zvezi z Mjanmarom/Burmo in razveljavitvi Uredbe (ES) št. 194/2008 (UL L 121, 3.5.2013, str. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj), Uredbo Sveta (EU) 2017/2063 z dne 13. novembra 2017 o omejevalnih ukrepih glede na razmere v Venezueli (UL L 295, 14.11.2017, str. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

blago, ki se uporablja izključno za komercialne uporabe, na primer za obračunavanje, trženje, zagotavljanje kakovosti storitev, zadovoljstvo uporabnikov ali varnost omrežja, se na splošno šteje, da ne predstavlja takih tveganj“;

(b) uvodna izjava 9: „Za okrepitev učinkovitega nadzora nad izvozom blaga za kibernetski nadzor, ki ni navedeno na seznamu, je bistveno, da se na tem področju dodatno uskladi uporaba vsezajemajočega nadzora. V ta namen so se države članice zavezale, da bodo ta nadzor podprle z izmenjavo informacij med seboj in s Komisijo, zlasti o tehnološkem razvoju blaga za kibernetski nadzor, in s posvečanjem pozornosti temu, da pri izvajanju vsezajemajočega nadzora spodbujajo izmenjavo na ravni Unije“;

(c) člen 2, točka 20, v katerem je blago za kibernetski nadzor opredeljeno kot „blago z dvojno rabo, posebej zasnovano tako, da omogoča tajni nadzor fizičnih oseb s spremljanjem, pridobivanjem, zbiranjem ali analizo podatkov iz informacijskih in telekomunikacijskih sistemov“;

(d) člen 5, s katerim je uvedena zahteva po dovoljenju za izvoz blaga za kibernetski nadzor, ki ni navedeno na seznamu, če je pristojni organ izvoznika obvestil, da je ali bi lahko bilo zadevno blago kot celota ali po delih namenjeno za uporabo v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava (člen 5(1)). Poleg tega ta člen od izvoznikov zahteva, da obvestijo pristojni organ, kadar jim je glede na ugotovitve skrbnega pregleda znano, da je blago kot celota ali po delih namenjeno za uporabo v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava (člen 5(2)). Pristojni organ odloči, ali je za izvoz potrebno dovoljenje, ter

(e) člen 5(2), v katerem je nadalje določeno, da „Komisija in Svet izdata smernice za izvoznike iz člena 26(1)“.

1.2. **Ključne opredelitve pojmov**

Uredba vsebuje namenske uvodne izjave in določbe, ki pojasnjujejo določene izraze, ki so pomembni za nadzor izvoza blaga za kibernetski nadzor, ki ni navedeno na seznamu, ter jih morajo izvozniki jasno razumeti, da lahko izvajajo skrbni pregled in učinkovito izvajajo nadzor. Pomemben je zlasti člen 2, točka 20, v katerem je natančno opredeljen pojem „blago za kibernetski nadzor“: „blago z dvojno rabo, posebej zasnovano tako, da omogoča tajni nadzor fizičnih oseb s spremljanjem, pridobivanjem, zbiranjem ali analizo podatkov iz informacijskih in telekomunikacijskih sistemov“.

Za namene teh smernic bi bilo treba pojasniti določene vidike te opredelitve.

1.2.1. *„Posebej zasnovano“*

Blago je zasnovano za tajni nadzor, kadar so njegove tehnične značilnosti primerne za tajni nadzor fizičnih oseb in ga objektivno omogočajo. Zato izraz „posebej zasnovano“ pomeni, da mora biti tajni nadzor fizičnih oseb glavni namen razvoja in zasnove izdelka. Vendar izraz ne pomeni nujno, da se lahko blago uporablja samo za tajni nadzor fizičnih oseb.

Kot je pojasnjeno v uvodni izjavi 8 Uredbe, blago, ki se uporablja izključno za komercialne uporabe, na primer za obračunavanje, trženje, zagotavljanje kakovosti storitev, zadovoljstvo uporabnikov ali varnost omrežja, ni posebej zasnovano za tajni nadzor fizičnih oseb in zato ne spada v opredelitev blaga za kibernetski nadzor. Na primer, čeprav se blago za nadzor operacijskih sistemov v industriji ali spremljanje prometa uporabnikov lahko uporablja za namene nadzora, to blago ni blago za kibernetski nadzor v skladu z opredelitvijo, saj ni posebej zasnovano za omogočanje tajnega nadzora fizičnih oseb.

1.2.2. *„Tajni nadzor“*

Blago omogoča tajni nadzor zlasti, kadar nadzor za zadevno fizično osebo ni očitno zaznaven. Tako je, kadar se zadevne osebe ne zavedajo prisotnosti in/ali delovanja blaga za kibernetski nadzor ter se zato nadzoru ne morejo izogniti ali vsaj ustrezno prilagoditi svojega vedenja. Tudi če se nadzor izvaja z blagom, ki je nameščeno ali se uporablja v javnem prostoru, se lahko pridobivanje podatkov v nekaterih primerih šteje za pomembno za tajni nadzor, zlasti če se lahko zbrani podatki preusmerjajo, ocenjujejo ali obdelujejo za namene, s katerimi zadevna fizična oseba ni seznanjena. Povedano drugače: kadar fizična oseba ne more objektivno pričakovati, da bo pod nadzorom, se lahko šteje, da je nadzor tajen v skladu s členom 2, točka 20, Uredbe.

1.2.3. *„Fizične osebe“*

Izraz „fizična oseba“ se nanaša na živega človeka, torej ne na pravne osebe ali subjekte, za katere torej določbe ne veljajo. Izraz ne zajema nadzora predmetov, lokacij ali strojev kot takih.

1.2.4. *„Spremljanje, pridobivanje, zbiranje in analiza podatkov“*

Prosto povzeto po *Slovarju slovenskega knjižnega jezika* imajo besede „spremljanje“, „pridobivanje“, „zbiranje“ in „analiziranje“ naslednje splošnojezikovne pomene:

— spremljanje: dojemanje, zaznavanje vsebine česa z gledanjem, poslušanjem,

— pridobivanje: delanje, da prihaja kaj iz česa kot rezultat določenega postopka,

— zbiranje: delanje, da prihaja skupaj večja količina česa,

— analiziranje: ugotavljanje sestavnih delov česa, razčlenjevanje; temeljit, izčrpen pregled.

Ti izrazi pomenijo, da bi moralo imeti blago, ki se uporablja za nadzor, natančne tehnične zmogljivosti za obdelavo podatkov, namenjene spremljanju, zbiranju, pridobivanju ali analizi podatkov, kot na primer naslednje blago:

(a) blago, ki se uporablja za spremljanje podatkov iz informacijskih in telekomunikacijskih sistemov ([4]) (na primer velikosti datotek ali prometa podatkovnih paketov, ki se prenašajo v takem sistemu);

(b) blago, s katerim se pridobivajo podatki iz informacijskih in telekomunikacijskih sistemov z vdorom in ekstrakcijo (na primer vdorna programska oprema);

(c) blago, ki omogoča analizo podatkov, pridobljenih iz informacijskih in telekomunikacijskih sistemov, vključno z blagom, ki lahko obdeluje posnetke kamer, shranjene v teh sistemih (na primer nekatere vrste tehnologij za analizo podatkov, ki se uporabljajo kot del sistemov za prepoznavanje obrazov).

Blago, ki se uporablja zgolj za spremljanje informacijskih sistemov ali prebivalstva s kamerami za videonadzor in ki omogoča zajemanje pogovorov, izmenjav podatkov, gibanja in vedenja posameznikov, ne bi ustrezalo opredelitvi blaga za kibernetski nadzor iz Uredbe, saj ni posebej zasnovano za ta namen in mora delovati z drugimi tehnologijami, kot so umetna inteligenca ali velepodatki. Vendar bi lahko bil celoten sistem (ki deluje skupaj z drugimi tehnologijami, kakršne so umetna inteligenca ali tehnologije velepodatkov) blago za kibernetski nadzor v skladu z opredelitvijo iz člena 2, točka 20, Uredbe.

Pomembno je poudariti, da so navedeni primeri sicer koristni za ponazoritev, vendar opredelitev in obseg blaga za kibernetski nadzor nista omejena na te primere, saj je cilj člena 5 omogočiti učinkovit nadzor izvoza blaga, ki ni navedeno na seznamu.

([4]) Za opredelitev glej točko 1.2.5.

Kot je razvidno iz uporabe veznika „ali“ v opredelitvi, je treba navedene tehnične zmogljivosti obravnavati kot alternative in ni nujno, da ima blago vse navedene tehnične zmogljivosti za spremljanje, pridobivanje, zbiranje ali analiziranje podatkov. Povedano drugače: da blago spada v opredelitev blaga za kibernetski nadzor iz člena 2, točka 20, zadostuje ena od navedenih tehničnih zmogljivosti.

1.2.5. *„Iz informacijskih in telekomunikacijskih sistemov“*

Ta izraza se nanašata na sisteme, ki elektronsko obdelujejo informacije, na primer s programiranjem/kodiranjem, operacijami sistemov osebnih računalnikov (strojne opreme) in drugim upravljanjem informacij, vključno s programsko tehnologijo, spletno tehnologijo, računalniško tehnologijo, tehnologijo shranjevanja itd., ter na nekatere sisteme, ki prenašajo informacije na daljavo, na primer tehnične sisteme, ki prek žičnih in brezžičnih kanalov, kot so optična vlakna, radio in drugi elektromagnetni sistemi, prenašajo zvok, signale, besedilo ali druge znake oziroma slike. Ta pojma skupaj zajemata širok nabor sistemov, ki prenašajo ali obdelujejo informacije. Opozoriti je treba, da se izraza nanašata na sisteme in ne na opremo.

1.2.6. *„Je znano“ in „je namenjeno za“*

V skladu s členom 5(2) Uredbe izvoznik uradno obvesti pristojni organ, če mu „je […] znano“, da je „blago za kibernetski nadzor“ „namenjeno“ „za uporabo v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava“.

Izraz „je znano“ ni nov pravni pojem, temveč se uporablja v povezavi z obveznostmi pridobitve dovoljenja v zvezi s končno uporabo (t. i. „vsezajemajoči“ nadzor) iz členov 4, 6, 7 in 8 Uredbe. „Je znano“ pomeni, da je nameravana zloraba uvozniku poznana. Zgolj možnost tveganja zlorabe ne zadostuje za ugotovitev, da je znana. Vendar izraza „je znano“ ni mogoče enačiti s pasivnostjo: izraz predpostavlja, da je izvoznik izvedel ukrepe za pridobitev zadostnega in ustreznega poznavanja za oceno tveganj, povezanih z izvozom, in za zagotovitev skladnosti z Uredbo.

Navedba, da mora biti blago „namenjeno za“ ustrezno občutljivo končno uporabo, pomeni, da bi moral izvoznik končno uporabo oceniti za vsak primer posebej glede na specifične okoliščine primera. Nasprotno pa teoretično tveganje – torej tveganje, ki ne temelji na dejanski presoji zadeve – da bi se blago lahko uporabilo v nasprotju s človekovimi pravicami, ni dovolj za domnevo, da „je namenjeno za“ določeno zlorabo v skladu s členom 5.

1.3. **Notranja represija, hude kršitve človekovih pravic in mednarodnega humanitarnega prava**

V skladu s členom 15 Uredbe, v katerem so navedeni razmisleki za oceno dovoljenja, morajo države članice upoštevati vse ustrezne razmisleke, vključno z vprašanji, ki so zajeta v Skupnem stališču Sveta 2008/944/SZVP ([5]).

Člen 5 Uredbe ob upoštevanju tveganja, da se bo blago uporabljalo v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava, razširja nadzor na izvoz blaga za kibernetski nadzor, ki ni navedeno na seznamu. Koristne smernice v zvezi s tem so Skupno stališče 2008/944/SZVP in navodila za uporabnike tega skupnega stališča ([6]).

([5]) Skupno stališče Sveta 2008/944/SZVP z dne 8. decembra 2008, ki opredeljuje skupna pravila glede nadzora izvoza vojaške tehnologije in opreme (UL L 335, 13.12.2008, str. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Glej Navodila za uporabnike za Skupno stališče Sveta 2008/944/SZVP, ki opredeljuje skupna pravila glede nadzora izvoza vojaške tehnologije in opreme, https://data.consilium.europa.eu/doc/document/ST-12189-2019-INIT/sl/pdf.

1.3.1. *Notranja represija*

V skladu s členom 2(2) Skupnega stališča 2008/944/SZVP „[n]otranja represija med drugim zajema mučenje in druga okrutna, nečloveška in ponižujoča ravnanja ali kaznovanja, hitre ali samovoljne usmrtitve, izginotja, samovoljne pripore ali druge večje kršitve človekovih pravic in temeljnih svoboščin, kakor so določene v ustreznih instrumentih o človekovih pravicah, vključno s Splošno deklaracijo o človekovih pravicah in z Mednarodnim paktom o državljanskih in političnih pravicah“. Navodila za uporabnike za Skupno stališče 2008/944/SZVP vsebujejo smernice o elementih, ki jih je treba upoštevati pri oceni izvoznika, vključno s „sedanjo in preteklo evidenco predlaganega končnega uporabnika v zvezi s spoštovanjem človekovih pravic ter evidenco države prejemnice na splošno“.

1.3.2. *Huda kršitev človekovih pravic*

Zloraba blaga za kibernetski nadzor, ki ni navedeno na seznamu, lahko negativno vpliva na širok spekter človekovih pravic ter neposredno posega v pravico do zasebnosti in varstva podatkov. Poleg tega lahko samovoljen ali nezakonit nadzor pomeni kršitev drugih človekovih pravic, kot so pravica do svobode izražanja, združevanja in zbiranja, svoboda veroizpovedi in prepričanja, pravica do enake obravnave ali prepoved diskriminacije ter pravica do svobodnih, enakih in tajnih volitev. V določenih primerih lahko nadzor, vključno s spremljanjem fizičnih oseb, kot so zagovorniki človekovih pravic, aktivisti, politične osebnosti, ranljivo prebivalstvo in novinarji, ali zbiranjem informacij o njih, privede do ustrahovanja, zatiranja, samovoljnih pridržanj, mučenja ali celo izvensodnih pobojev. Zato bi morali izvozniki te vidike v zvezi s hudimi kršitvami človekovih pravic vključiti v svoje ocene.

Mednarodna praksa kaže, da mora biti kakršno koli omejevanje človekovih pravic „ustrezno“ in v skladu z mednarodnimi standardi na področju človekovih pravic. V praksi to pomeni, da so vzpostavljeni zadostni zaščitni ukrepi, ki zagotavljajo, da je omejevanje določeno z zakonodajo in da se ohrani bistvo pravic. Ob upoštevanju načela sorazmernosti je omejevanje dovoljeno le, če je nujno in resnično služijo zakonitemu namenu – na primer nacionalni ali javni varnosti, javnemu redu, varovanju javnega zdravja ali varstvu pravic in svoboščin drugih.

Blago za kibernetski nadzor lahko vključuje zakonita in regulirana orodja za organe kazenskega pregona, na primer za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj, tudi na področju boja proti terorizmu, ali izvrševanje kazenskih sankcij. Hkrati se lahko blago za kibernetski nadzor zlorabi tudi za hude kršitve človekovih pravic in mednarodnega humanitarnega prava, kadar se izvozi represivnim režimom ali zasebnim končnim uporabnikom in/ali na konfliktna območja.

Zato je treba v vsakem primeru posebej oceniti okoliščine, vključno z uporabo ustreznih predpisov glede na morebitna poročila o hudih kršitvah človekovih pravic, ki jih izdajo pristojni organi, na primer Združeni narodi, Unija ali Svet Evrope. Kot podlaga za ugotavljanje, ali gre za „hudo“ kršitev človekovih pravic, lahko služi ugotovitev o kršitvah, navedena v informacijah, ki jih objavijo pristojni organi Združenih narodov, Unija ali Svet Evrope. Taka izrecna ugotovitev navedenih organov ni absolutno nujna, vendar je pomemben dejavnik za izpolnitev meril.

V skladu s členom 5 mora biti kršitev človekovih pravic „huda“. Koristne smernice za opredelitev morebitnih kršitev človekovih pravic kot „hudih“ so na voljo v Navodilih za uporabnike za Skupno stališče 2008/944/SZVP. V skladu z navedenimi navodili so odločilne narava in posledice kršitve. Sistematične in/ali razširjene kršitve človekovih pravic se običajno obravnavajo kot hude; vendar se lahko za „hude“ štejejo tudi kršitve, ki niso sistematične ali razširjene – na primer zaradi resnosti posega za zadevne osebe.

Priloga II k Navodilom za uporabnike za Skupno stališče 2008/944/SZVP vsebuje neizčrpen seznam glavnih mednarodnih in regionalnih instrumentov človekovih pravic, vključno z Mednarodnim paktom o državljanskih in političnih pravicah, Konvencijo proti mučenju in drugim krutim, nečloveškim ali poniževalnim kaznim ali ravnanju, Evropsko konvencijo o človekovih pravicah in Listino o temeljnih pravicah, ki lahko služijo kot pomembne smernice za razlago in uporabo meril v podporo zanesljivim ocenam glede človekovih pravic. Ti instrumenti in njihovi dodatni protokoli predstavljajo glavne mednarodne norme in standarde na področjih človekovih pravic in temeljnih svoboščin.

1.3.3. *Huda kršitev mednarodnega humanitarnega prava*

Mednarodno humanitarno pravo (imenovano tudi „ženevsko pravo“ ali „pravo oboroženih spopadov“), ki je bilo razvito z vrsto mednarodnih pogodb, predvsem Haaškim pravilnikom, Ženevskimi konvencijami in njihovima dodatnima protokoloma iz leta 1977, opredeljuje pravila, ki v času oboroženih spopadov ščitijo ljudi, ki ne sodelujejo ali ne sodelujejo več v sovražnostih (na primer civilisti in ranjeni, bolni ali ujeti borci), ter vpletenim stranem nalaga omejitve glede sredstev in načinov vojskovanja (haaško pravo).

Uporaba blaga za kibernetski nadzor, ki ni navedeno na seznamu, bi morala biti v skladu z mednarodnim humanitarnim pravom, kadar se uporablja kot sredstvo in metode vojskovanja v okviru oboroženega spopada. V takih okoliščinah se v skladu z Uredbo upošteva tveganje hudih kršitev mednarodnega humanitarnega prava, ki bi ga bilo treba, kar zadeva hude kršitve človekovih pravic, oceniti glede na končno uporabo, za katero je blago namenjeno v posameznem primeru. Navodila za uporabnike za Skupno stališče 2008/944/SZVP vsebujejo smernice o elementih, ki jih je treba upoštevati, in sicer med drugim zgodovino preteklega in sedanjega spoštovanja mednarodnega humanitarnega prava s strani prejemnika, njegove namere, izražene v formalnih zavezah, in njegovo zmožnost zagotoviti, da bo prenesena oprema ali tehnologija uporabljena na način, skladen z mednarodnim humanitarnim pravom, in ne bo preusmerjena ali prenesena v druge namembne kraje, kjer bi bila lahko uporabljena za resne kršitve tega prava.

V skladu s členom 5 mora biti kršitev mednarodnega humanitarnega prava „huda“. Smernice so v Navodilih za uporabnike za Skupno stališče 2008/944/SZVP, v katerih je priznano, da „[p]osamezni incidenti v zvezi s kršitvami mednarodnega humanitarnega prava niso nujno pokazatelj odnosa države prejemnice do mednarodnega humanitarnega prava“, vendar „[č]e je opazen določen vzorec kršitev ali država prejemnica ni ustrezno ukrepala, da bi kaznovala kršitve, je to razlog za resen pomislek“. Mednarodni odbor Rdečega križa (ICRC) je pripravil smernice za ocenjevanje kršitev mednarodnega humanitarnega prava za namene nadzora izvoza. Po mnenju ICRC so „kršitve mednarodnega humanitarnega prava hude, če ogrožajo zaščitene osebe (na primer civiliste, vojne ujetnike, ranjene in bolne) ali objekte (na primer civilne objekte ali infrastrukturo) ali če so v nasprotju s pomembnimi univerzalnimi vrednotami“. Huda kršitev mednarodnega humanitarnega prava so na primer vojni zločini. Poleg tega ICRC navaja podobne dejavnike, ki jih je treba upoštevati kot Navodila za uporabnike za Skupno stališče 2008/944/SZVP, vključno s formalnimi zavezami za uporabo pravil mednarodnega humanitarnega prava, ustreznimi ukrepi za zagotavljanje odgovornosti za kršitve mednarodnega humanitarnega prava, usposabljanjem vojske o mednarodnem humanitarnem pravu in prepovedjo novačenja otrok za oborožene sile.

2. **TEHNIČNO PODROČJE UPORABE**

2.1. **Blago za kibernetski nadzor, navedeno na seznamu**

Za pomoč izvoznikom pri prepoznavanju potencialnega blaga za kibernetski nadzor, ki ni navedeno na seznamu, Dodatek k tem smernicam vsebuje informacije o blagu za kibernetski nadzor, navedenem v Prilogi I k Uredbi.

2.2. **Potencialno blago za kibernetski nadzor, ki ni navedeno na seznamu**

Čeprav je po definiciji nemogoče sestaviti izčrpen seznam izdelkov, ki jih je mogoče nadzirati kot blago, ki ni navedeno na seznamu, v skladu s členom 5, bi se naslednje blago lahko uporabljalo za nadzor in bi bila v skladu z Uredbo pri njem potrebna posebna pozornost.

Kot je pojasnjeno v uvodni izjavi 8 Uredbe, se za blago, ki se uporablja izključno za komercialne namene, na primer za obračunavanje, trženje, zagotavljanje kakovosti storitev, zadovoljstvo uporabnikov ali varnost omrežja, na splošno šteje, da ne predstavlja tveganj za zlorabo, ki bi bila pomembna v okviru hudih kršitev človekovih pravic ali mednarodnega humanitarnega prava, in zato na splošno ni predmet nadzora v skladu s členom 5. Mnogo takega blaga ima funkcije informacijske varnosti (kriptografske ali celo kriptoanalitične), ki ustrezajo kontrolnim parametrom skupine 5 v delu 2 besedila o nadzoru iz Priloge I k Uredbi. Varnostna omrežna oprema – vključno z usmerjevalniki, stikali ali releji, pri katerih je funkcionalnost informacijske varnosti omejena na naloge „delovanje, upravljanje ali vzdrževanje“, ki uporabljajo samo objavljene ali komercialne kriptografske standarde – prav tako ni zajeta v opredelitvi pojma „blago za kibernetski nadzor“, vendar bi morali izvozniki ostati pozorni glede na različna poročila o zlorabi takih predmetov za kršitve človekovih pravic.

2.2.1. *Tehnologija za prepoznavanje obrazov in čustev*

Tehnologije za prepoznavanje obrazov in čustev se ne uporabljajo le za kibernetski nadzor, temveč tudi na primer za identifikacijo ali avtentikacijo, in v opredelitev ne spadajo samodejno. Vendar lahko tehnologije za prepoznavanje obrazov in čustev v nekaterih okoliščinah spadajo na področje uporabe člena 2, točka 20, Uredbe.

Tehnologije za prepoznavanje obrazov in čustev, ki se lahko uporabljajo za spremljanje ali analizo shranjenih videoposnetkov, bi lahko spadale na področje uporabe opredelitve blaga za kibernetski nadzor. Vendar tudi če so zgoraj navedena merila izpolnjena, je treba skrbno preveriti, ali je programska oprema posebej zasnovana za tajni nadzor.

2.2.2. *Naprave za sledenje lokaciji*

Naprave za sledenje lokaciji omogočajo sledenje fizični lokaciji naprave skozi čas, nekatere tehnologije za sledenje lokaciji pa organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter obveščevalne službe uporabljajo že nekaj časa. Njihov potencial za ciljno usmerjen in množični nadzor je znatno napredoval z razvojem tehnologij za sledenje, vključno s satelitskim sledenjem lokaciji, sledenjem lokaciji na podlagi telekomunikacijskih stolpov, oddajniki-sprejemniki Wi-Fi in Bluetooth, ter razširjenostjo „sledilnih naprav“, kot so pametni telefoni in druge elektronske naprave (na primer informacijski sistemi v avtomobilih).

Naprave za sledenje lokaciji organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter obveščevalne agencije na primer uporabljajo za zbiranje dokazov med preiskavo ali sledenje osumljencem, uporabljajo pa se tudi za komercialne namene, na primer za poročanje o zbirnih vzorcih gibanja na nakupovalnih ulicah, sledenje zaposlenim, ki delajo zunaj lokacije, ali oglaševanje na podlagi lokacije.

2.2.3. *Sistemi za videonadzor*

Da bi izvoznikom pomagali pri prepoznavanju potencialnega blaga za kibernetski nadzor, je koristno tudi pojasniti, katero blago ni zajeto v opredelitvi. V tem smislu na primer sistemi za videonadzor in kamere, vključno s kamerami visoke ločljivosti, ki se uporabljajo za snemanje ljudi na javnih mestih, niso zajeti v opredelitvi blaga za kibernetski nadzor, saj ne spremljajo ali zbirajo podatkov iz informacijskih in telekomunikacijskih sistemov.

3. UKREPI IZVAJANJA SKRBNIH PREGLEDOV

V skladu z uvodno izjavo 7 Uredbe je „prispevek izvoznikov […] k splošnemu cilju nadzora trgovine […] ključnega pomena. Da bi lahko delovali v skladu s to uredbo, je treba v okviru programov notranje skladnosti oceniti tveganja, povezana s transakcijami, na katere se nanaša ta uredba, na podlagi ukrepov pregleda transakcij, znanimi tudi kot načelo ravnanja s primerno skrbnostjo.“

V skladu s členom 2, točka 21, program notranje skladnosti „pomeni stalne učinkovite, ustrezne in sorazmerne politike in postopke, ki jih izvozniki sprejmejo za lažje izpolnjevanje določb in ciljev te uredbe ter pogojev za dovoljenja, ki se izvajajo v skladu s to uredbo, med drugim vključno z ukrepi izvajanja skrbnih pregledov za oceno tveganj, povezanih z izvozom blaga končnim uporabnikom in končno uporabo“.

Priporočilo Komisije (EU) 2019/1318 ([7]) zagotavlja okvir za pomoč izvoznikom pri ugotavljanju, obvladovanju in zmanjševanju tveganj, povezanih z nadzorom trgovine z blagom z dvojno rabo, ter zagotavljanju skladnosti z ustreznimi zakoni in predpisi Unije ter nacionalnimi zakoni in predpisi.

Te smernice lahko podpirajo izvoznike pri izvajanju ukrepov pregleda transakcij, znanih tudi kot načelo ravnanja s primerno skrbnostjo, v okviru programov notranje skladnosti.

V skladu s členom 5(2) Uredbe (EU) 2021/821 morajo izvozniki blaga za kibernetski nadzor, ki ni navedeno na seznamu, izvajati skrbne preglede z ukrepi pregleda transakcij, kar pomeni sprejemanje ukrepov v zvezi z razvrstitvijo blaga in oceno tveganj transakcij. V praksi se izvoznike spodbuja, da opravijo naslednje:

([7]) Priporočilo Komisije (EU) 2019/1318 z dne 30. julija 2019 o programih notranje skladnosti za nadzor trgovine z blagom z dvojno rabo v skladu z Uredbo Sveta (ES) št. 428/2009 (UL L 205, 5.8.2019, str. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **pregledajo, ali je blago, ki se izvaža in ni navedeno na seznamu, morda „blago za kibernetski nadzor“, kar pomeni, da je blago z dvojno rabo, posebej zasnovano tako, da omogoča tajni nadzor fizičnih oseb s spremljanjem, pridobivanjem, zbiranjem ali analizo podatkov iz informacijskih in telekomunikacijskih sistemov;**

ta korak zadeva določitev blaga v skladu z določbami, ki se uporabljajo za blago za kibernetski nadzor. To vključuje pregled tehničnih značilnosti blaga na podlagi tehničnih parametrov iz Priloge I k Uredbi za blago, ki je navedeno na seznamu, in glede na specifične izraze in pojme iz opredelitve blaga za kibernetski nadzor za blago, ki ni navedeno na seznamu, ter glede na poznejšo razvrstitev blaga (blago, tehnologija ali programska oprema).

3.2. **pregledajo zmogljivosti zadevnega blaga, da se ugotovi možnost zlorabe v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava s strani tujih končnih uporabnikov;**

izvozniki bi morali oceniti, ali bi se izdelek lahko zlorabil za izvajanje notranje represije ali kršitev oziroma zlorabo človekovih pravic, vključno s pravico do življenja, prepovedjo mučenja, nečloveškega in ponižujočega ravnanja, pravico do zasebnosti, pravico do svobode govora, pravico do združevanja in zbiranja, pravico do svobode veroizpovedi ali prepričanja, pravico do enake obravnave ali prepovedjo diskriminacije ter pravico do svobodnih, enakih in tajnih volitev.

To vključuje tudi oceno, s katero se ugotovi, ali bi se izdelek lahko uporabljal kot del ali sestavni del sistema, ki bi lahko povzročil take kršitve in/ali zlorabo.

Izvozniki bi morali pri svoji oceni paziti na tako imenovane opozorilne znake za kakršne koli neobičajne okoliščine transakcije, ki kažejo, da je izvoz lahko namenjen neprimerni končni uporabi, končnemu uporabniku ali namembni državi.

Opozorilni znaki:

(a) blago se trži z informacijami o njegovi morebitni uporabi za tajni nadzor;

(b) informacije o pretekli zlorabi podobnega blaga v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava (glej oddelek 1.3);

(c) informacije o pretekli nezakoniti rabi blaga v dejavnostih nadzora, usmerjenih zoper državo članico, ali v povezavi z nezakonitim nadzorom državljana EU;

(d) informacije, da transakcija vključuje blago, ki bi se lahko uporabilo za vzpostavitev, prilagoditev ali konfiguracijo sistema, za katerega je znano, da se zlorablja v povezavi z notranjo represijo in/ali hudimi kršitvami človekovih pravic in mednarodnega humanitarnega prava (glej oddelek 1.3);

(e) zadevno blago ali podobno blago je na seznamu, objavljenem v seriji C *Uradnega lista Evropske unije* v skladu s členom 5(6) Uredbe;

3.3. **v podporo pristojnim organom pregledajo deležnike transakcije (vključno s končnimi uporabniki in prejemniki, kot so distributerji in preprodajalci);**

V podporo pristojnim organom bi, kolikor je mogoče, izvozniki morali:

(a) pred in med kakršno koli transakcijo na podlagi izjav o končni uporabi pregledati, kako nameravajo prejemniki in/ali končni uporabniki izdelek ali storitev uporabljati;

(b) se seznaniti z razmerami v zadevni namembni državi blaga, zlasti s splošnim stanjem človekovih pravic, saj je to pomemben kazalnik tveganja hudih kršitev človekovih pravic in mednarodnega humanitarnega prava, povezanega z izvozom;

(c) na podlagi opozorilnih znakov, navedenih v nadaljevanju, pregledati tveganja, da bo izdelek ali storitev preusmerjena do drugega nepooblaščenega končnega uporabnika.

Opozorilni znaki:

(a) končni uporabnik ima očiten odnos s tujo vlado, ki je v preteklosti izvajala notranjo represijo in/ali hude kršitve človekovih pravic in mednarodnega humanitarnega prava;

(b) končni uporabnik je strukturno del oboroženih sil ali druge skupine, ki je bila v preteklosti vpletena v oborožen spopad, ki je vključeval ukrepe notranje represije in/ali hude kršitve človekovih pravic in mednarodnega humanitarnega prava;

(c) končni uporabnik je v preteklosti izvažal blago za kibernetski nadzor v države, v katerih je uporaba takega blaga privedla do ukrepov notranje represije in/ali hudih kršitev človekovih pravic in mednarodnega humanitarnega prava;

3.4. **uporabijo ugotovitve iz skrbnega pregleda za pripravo načrtov za preprečevanje in ublažitev morebitnih prihodnjih negativnih vplivov.**

Izvozniki bi morali na podlagi ugotovitev iz skrbnega pregleda prenehati z dejavnostmi, ki povzročajo negativne vplive, povezane s človekovimi pravicami, ali prispevajo k njim, ter pripraviti in izvajati načrt popravljalnih ukrepov. Ti ukrepi lahko vključujejo:

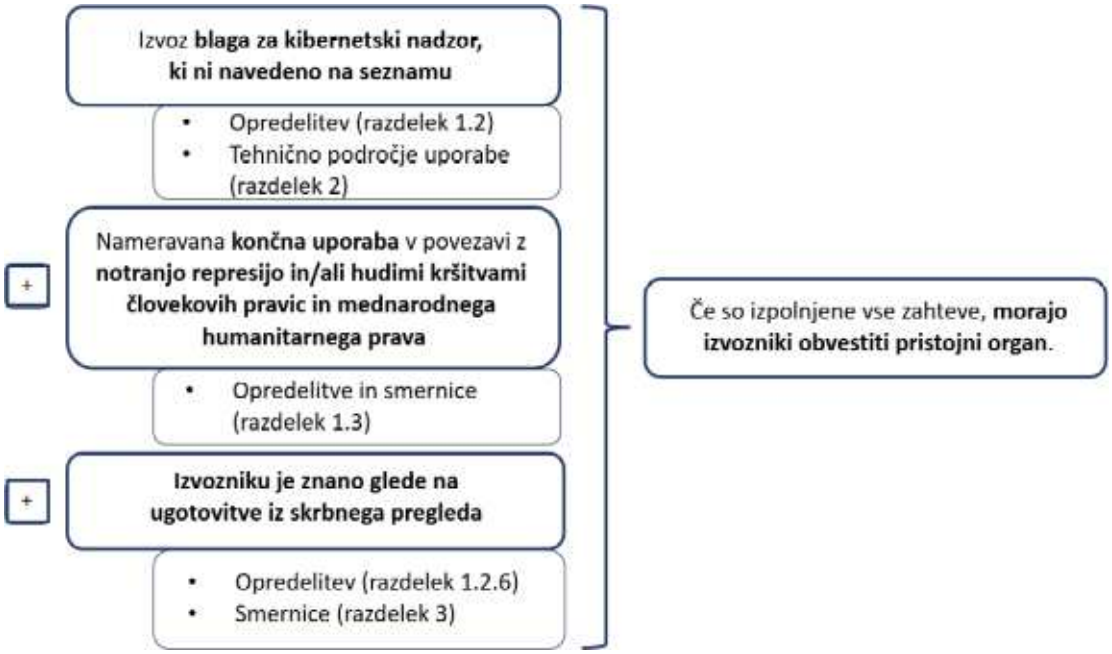
(a) posodobitev politik podjetja, da se zagotovijo smernice, kako v prihodnosti preprečevati in odpravljati negativne vplive, ter zagotavljanje njihovega izvajanja;

(b) uporaba ugotovitev iz ocene tveganja za posodobitev in okrepitev sistemov upravljanja za boljše spremljanje informacij in opozarjanje na tveganja, preden se pojavijo škodljivi vplivi;

(c) zbiranje informacij za razumevanje velikih tveganj škodljivih vplivov, povezanih s sektorjem;

(d) obveščanje pristojnih organov držav članic o ugotovitvah iz skrbnih pregledov, da se olajša pretok informacij v zvezi z določenim blagom, končnimi uporabniki in namembnimi državami.

Zahteve iz člena 5(2) Uredbe (EU) 2021/821



4. **DODATEK**

Blago za kibernetski nadzor, ki se nadzoruje v skladu s Prilogo I k Uredbi (EU) 2021/821

— **Sistemi za prestrezanje telekomunikacij (5A001.f)**

V večini držav, vključno z državami članicami, je zaupnost komunikacij zaščitena z zakonom, vendar je v pravnem okviru lahko dovoljen tajni elektronski nadzor komunikacij, ki ga izvajajo vladni organi (t. i. zakonito prestrezanje). V digitalni dobi pa je postala mogoča množična uporaba tehnologij prestrezanja. Uporaba orodij za prestrezanje s strani libijskega režima je opozorilo glede možnosti za množično uporabo teh tehnologij in je spodbudila k temu, da se je leta 2012 uvedel nadzor izvoza sistemov za prestrezanje telekomunikacij.

Nadzor se uporablja za opremo, zasnovano za pridobivanje vsebine komunikacije (glasu ali podatkov) ter identifikatorjev naročnikov ali drugih metapodatkov, ki se prenašajo po zraku prek brezžične komunikacije, in opremo za spremljanje radijskih frekvenc. Ta nadzor se na primer uporablja za IMSI lovilce (mednarodna identiteta mobilnega naročnika), ki prestrezajo promet z mobilnih telefonov in spremljajo gibanje njihovih uporabnikov, ali opremo za ustvarjanje lažnih dostopnih točk Wi-Fi, ki lahko iz telefona pridobijo številke IMSI, ter za nekatere vrste blaga, posebej zasnovanega, da omogoča „temeljit pregled paketov“ v telekomunikacijskih sistemih. Oprema za motenje mobilnih telekomunikacij ne spada v opredelitev blaga za kibernetski nadzor, saj ne zbira podatkov.

Medtem ko se za vzpostavitev takih sistemov lahko uporabi tehnologija splošnega namena, bodo za njihove zmogljivosti za množično prestrezanje potrebni posebni deli in komponente, vključno na primer s posebno programsko opremo, naprednimi integriranimi vezji ali integriranimi vezji za specifično uporabo (na primer FPGA, ASIC itd.), da se poveča število paketov ali komunikacijskih sej, ki jih je mogoče obdelati na sekundo.

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

Čeprav je veliko internetnih komunikacij dandanes običajno privzeto šifriranih, se lahko prestrezanje podatkov o prometu (metapodatkov) v zvezi s komunikacijami, kot so naslovi IP ter pogostost in obseg izmenjave podatkov, še vedno uporablja za identifikacijo povezav med osebami in domenskimi imeni. Vlade lahko te sisteme zakonito in pod sodnim nadzorom uporabljajo za zakonite namene, kot je identifikacija oseb, ki obiščejo domene, povezane s kriminalnimi ali terorističnimi vsebinami. Spremljanje in analiza internetnega prometa na podlagi etničnih, verskih, političnih ali družbenih značilnosti pa lahko vodita k celovitemu človeškemu in socialnemu popisovanju države za nadzor in represijo prebivalstva ter druge namene, na primer za prepoznavanje političnih disidentov. Poleg vprašanj v zvezi s človekovimi pravicami in notranjo represijo lahko to blago prispeva tudi h krepitvi varnostnih in vojaških zmogljivosti.

Nadzor iz točke 5A001.j se uporablja za sisteme za nadzor interneta, ki delujejo v „nosilnem omrežju internetnega protokola (IP) (npr. nacionalna hrbtenica IP)“ za izvajanje analize, pridobivanja in indeksiranja posredovanih metapodatkovnih vsebin (glas, video, sporočila, priponke) na podlagi „trdih selektorjev“ ter določanje omrežja razmerij ljudi. To je blago, s katerim se izvaja tajni nadzor, ker zadevne osebe niso seznanjene s prestrezanjem komunikacij. Nasprotno pa nadzor nad izvozom ne zadeva sistemov, ki vključujejo dejanje uporabnika oziroma naročnika ali interakcijo z njim, in se na primer ne uporablja za družbena omrežja ali komercialne iskalnike. Poleg tega se nadzor izvoza uporablja za sisteme, ki obdelujejo podatke iz jedrnega omrežja ponudnika interneta, ne pa tudi za družbena omrežja ali komercialne iskalnike, ki obdelujejo podatke, ki jih predložijo uporabniki.

— **Vdorna programska oprema (4A005, 4D004 in povezani nadzor iz točk 4E001.a in 4E001.c)**

Vdorna programska oprema operaterju omogoča, da tajno pridobi oddaljeni dostop do elektronske naprave, kot je pametni telefon, prenosni računalnik, strežnik ali naprava, povezana v internet stvari, da pridobi podatke, shranjene na napravi, prisluškuje ali opazuje z vgrajeno ali povezano kamero oziroma mikrofonom ter napravo uporablja kot odskočno desko za napade na opremo, s katero je naprava povezana, ali na stike uporabnika (vdor prek naprav tretjih oseb). Čeprav obstajajo primeri zakonite rabe ([8]) vdorne programske opreme, na primer programska oprema za oddaljeni dostop, ki jo oddelki IT uporabljajo za podporo na daljavo, tajnost nadzora in obseg informacij, ki jih je mogoče zbrati, pomenita veliko tveganje kršitve pravice do zasebnosti in varstva osebnih podatkov ter lahko resno ogrozita pravico do svobode izražanja.

([8]) Za izvoz blaga za kibernetski nadzor, ki se nadzoruje v skladu s Prilogo I k uredbi o blagu z dvojno rabo, v tretje države bi bilo potrebno dovoljenje, ne glede na to, ali je raba blaga zakonita.

Nadzor iz točke 4A005 in drugih vključuje programsko opremo ter sisteme, opremo, komponente in sorodno tehnologijo, posebej razvito ali prirejeno za oblikovanje, upravljanje in zagotavljanje vdorne programske opreme ali nadzor nad njo, kot je opredeljeno v Prilogi I k Uredbi. Ta kibernetska orodja so predmet nadzora zaradi morebitnih motenj in škode, ki jih lahko povzročijo, če se uspešno uporabljajo in izvajajo, vendar namen nadzora ni vplivati na dejavnost raziskovalcev in industrije na področju kibernetske varnosti, ki morajo deliti informacije, povezane z vdorno programsko opremo, da bi lahko razvili in namestili popravke za svoje izdelke pred javno objavo ranljivosti.

— **Programska oprema za spremljanje komunikacij (5D001.e)**

Ta programska oprema je zasnovana, da pooblaščenim organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj omogoči spremljanje in analizo podatkov, zbranih s ciljno usmerjenimi ukrepi prestrezanja, ki jih zahtevajo od ponudnika komunikacijskih storitev. Omogoča iskanje po vsebini komunikacije ali metapodatkih na podlagi „trdih selektorjev“ z uporabo vmesnika za zakonito prestrezanje ter določanje omrežja razmerij ali sledenje gibanju ciljnih posameznikov na podlagi rezultatov iskanja. Namenjena je tajnemu nadzoru, saj uporablja podatke, zbrane s prestrezanjem komunikacij, ki se ga osebe ne zavedajo. Poleg tega analizira podatke, zbrane prek telekomunikacijskih sistemov. Programska oprema je nameščena pri vladnem organu (na primer enota za spremljanje za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (LEMF)) in nadzor se ne uporablja za sisteme za zagotavljanje skladnosti v zvezi z zakonitim prestrezanjem (na primer sisteme za upravljanje zakonitega prestrezanja in posredniške naprave), ki so komercialno razviti in nameščeni v prostoru ponudnika komunikacijskih storitev (na primer vključeni v komunikacijsko omrežje) ter jih ta upravlja in vzdržuje. Kot je pojasnjeno v besedilu o nadzoru, se nadzor ne uporablja za programsko opremo, posebej zasnovano ali prilagojeno za izključno komercialne namene, kot so na primer izstavitev računov, kakovost storitev (QoS) v omrežju, kakovost izkušnje (QoE), posredniške naprave ali mobilna plačila oziroma bančna raba.

— **Blago, ki se uporablja za izvajanje kriptoanalize (5A004.a)**

Nadzor se uporablja za blago, namenjeno premagovanju kriptografskih mehanizmov zaradi pridobivanja zaupnih spremenljivk ali občutljivih podatkov, vključno z odprtim besedilom, gesli ali kriptografskimi ključi. Kriptografija se uporablja za varovanje zaupnosti informacij med prenašanjem in v hrambi. Kriptoanaliza se uporablja za premagovanje te zaupnosti, zato ta tehnologija omogoča tajni nadzor s spremljanjem, pridobivanjem, zbiranjem ali analizo podatkov iz informacijskih in telekomunikacijskih sistemov.

— **Forenzična/preiskovalna orodja (5A004.b, 5D002.a.3.b in 5D002.c.3.b)**

Forenzična/preiskovalna orodja so zasnovana za ekstrakcijo surovih podatkov iz naprave (na primer računalniške ali komunikacijske) tako, da podatki niso spremenjeni ali poškodovani in se lahko uporabijo za sodne namene, tj. v kazenski preiskavi ali na sodišču. Ti izdelki zaobidejo avtentikacijo oziroma kontrolne elemente naprave za avtorizacijo, tako da je iz naprave mogoče pridobiti surove podatke. Te izdelke uporabljajo vladni organi, organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter oborožene sile za pridobivanje in analizo podatkov iz zaseženih naprav. Sicer se lahko uporabljajo zakonito, vendar jih je mogoče zlorabiti, zato pomenijo tveganje za občutljive ali komercialne podatke.

Vendar forenzična/preiskovalna orodja, ki niso posebej zasnovana za tajni nadzor, ne spadajo v opredelitev blaga za kibernetski nadzor iz člena 2, točka 20. Poleg tega forenzična/preiskovalna orodja, s katerimi se podatki uporabnikov samo pridobijo ali kadar podatki na napravi niso zaščiteni, niso zajeta v besedilu o nadzoru iz točke 5A004.b *et al*. Hkrati se nadzor ne uporablja za proizvajalčevo proizvodno ali preskusno opremo, orodja za skrbnike sistemov ali izdelke izključno za komercialni maloprodajni sektor, na primer za odklepanje mobilnih telefonov. Torej je glede na raznolikost teh vrst tehnologij uporaba nadzora odvisna od ocene vsakega posameznega izdelka v vsakem primeru posebej.

Nazadnje, upoštevajte, da obstaja drugo blago, povezano z nadzorom in navedeno v Prilogi I k Uredbi, ki se ne sme šteti za zajeto v opredelitvi blaga za kibernetski nadzor, kot so oprema za motenje mobilnih telekomunikacij (5A001.f), izdelana za poškodovanje ali motenje komunikacij ali sistemov, vdorna programska oprema, ki spreminja sistem (4D004), in laserska oprema za zaznavanje zvoka (6A005.g), ki zbira zvočne podatke z laserjem ali omogoča poslušanje pogovorov na daljavo (imenovana tudi laserski mikrofon). Podobno se zaradi uporabe zrakoplovov brez posadke, navedenih na seznamu, za namene nadzora to blago ne bi vključilo v opredelitev blaga za kibernetski nadzor.