Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/2659

2024 10 16

# KOMISIJOS REKOMENDACIJA (ES) 2024/2659

## 2024 m. spalio 11 d.

## dėl Europos Parlamento ir Tarybos reglamento (ES) 2021/821 5 straipsnyje aprašytų kibernetinio stebėjimo prekių eksporto gairių

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 292 straipsnį,

kadangi:

(1) Europos Parlamento ir Tarybos reglamentu (ES) 2021/821 ([1]) nustatytas Sąjungos dvejopo naudojimo prekių eksporto, persiuntimo, susijusių tarpininkavimo paslaugų, techninės pagalbos ir tranzito kontrolės režimas;

(2) Reglamentu (ES) 2021/821 sprendžiamas rizikos, kad kibernetinio stebėjimo prekės gali būti naudojamos vykdant vidaus represijas ir (arba) sunkius žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimus, klausimas;

(3) pagal Reglamento (ES) 2021/821 5 straipsnio 2 dalį ir 26 straipsnio 1 dalį Komisija ir Taryba eksportuotojams pateikia gaires dėl sąraše neišvardytų kibernetinio stebėjimo prekių, atsižvelgdamos į poreikį užtikrinti Sąjungos eksporto kontrolės režimo veiksmingumą kibernetinio saugumo srityje ir Reglamento (ES) 2021/821 įgyvendinimo nuoseklumą;

(4) šia rekomendacija ir kartu su ja pateikiamomis gairėmis siekiama padėti eksportuotojams taikyti sąraše neišvardytų kibernetinio stebėjimo prekių kontrolės priemones, įskaitant, *inter alia*, išsamaus patikrinimo priemones, kuriomis vertinama su tokių prekių eksportu susijusi rizika;

(5) dėl kartu su šia rekomendacija pateikiamų gairių 2022 ir 2023 m. vyko išsamios konsultacijos Stebėjimo technologijų ekspertų grupėje ir buvo atsižvelgta į antrąjį 2023 m. ketvirtį vykusių viešų konsultacijų ([2]) metu gautas pastabas;

(6) reikėtų priminti, kad ši rekomendacija ir kartu su ja pateikiamos gairės nėra privalomos. Todėl eksportuotojai turėtų ir toliau vykdyti savo įsipareigojimus pagal Reglamentą (ES) 2021/821, o Komisija turėtų užtikrinti, kad ši rekomendacija laikui bėgant išliktų aktuali,

([1]) 2021 m. gegužės 20 d. Europos Parlamento ir Tarybos reglamentas (ES) 2021/821, nustatantis Sąjungos dvejopo naudojimo prekių eksporto, persiuntimo, susijusių tarpininkavimo paslaugų, techninės pagalbos ir tranzito kontrolės režimą, (OL L 206, 2021 6 11, p. 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_lt.

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

Rekomenduojama, kad valstybių narių kompetentingos institucijos ir eksportuotojai, vykdydami savo įsipareigojimus pagal Reglamento (ES) 2021/821 5 straipsnio 2 dalį, atsižvelgtų į šios rekomendacijos priede pateikiamas gaires.

Priimta Briuselyje 2024 m. spalio 11 d.

*Komisijos vardu*
Valdis DOMBROVSKIS
*Vykdomasis pirmininko pavaduotojas*

*PRIEDAS*

**TURINYS**

*Puslapis*

Įvadas ..... 4

1. Aktualios teisinės nuostatos, apibrėžtys ir pagrindinės sąvokos ..... 4

1.1. Aktualių teisinių nuostatų apžvalga ..... 4

1.2. Pagrindinės apibrėžtys ..... 5

1.2.1. „Specialiai sukurta“ ..... 5

1.2.2. Slaptas stebėjimas ..... 6

1.2.3. Fiziniai asmenys ..... 6

1.2.4. Duomenų stebėjimas, išgavimas, rinkimas ar analizavimas ..... 6

1.2.5. „Iš informacinių ir telekomunikacijų sistemų“ ..... 7

1.2.6. „Žinojimas“ ir „ketinama naudoti“ ..... 7

1.3. Vidaus represijos, šiurkštūs žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimai ..... 7

1.3.1. Vidaus represijos ..... 8

1.3.2. Šiurkštūs žmogaus teisių pažeidimai ..... 8

1.3.3. Šiurkštūs tarptautinės humanitarinės teisės pažeidimai ..... 9

2. Techninė taikymo sritis ..... 9

2.1. Sąraše išvardytos kibernetinio stebėjimo prekės ..... 9

2.2. Galimos sąraše neišvardytos kibernetinio stebėjimo prekės ..... 9

2.2.1. Veido ir emocijų atpažinimo technologijos ..... 10

2.2.2. Vietos nustatymo įtaisai ..... 10

2.2.3. Stebėjimo vaizdo kameromis sistemos ..... 10

3. Išsamaus patikrinimo priemonės ..... 10

Reglamento (ES) 2021/821 5 straipsnio 2 dalyje nustatyti reikalavimai ..... 12

4. Priedėlis ..... 12

Sąraše išvardytos pagal Reglamento (ES) 2021/821 I priedą kontroliuojamos kibernetinio stebėjimo prekės ..... 12

Telekomunikacijos perėmimo sistemos (5A001.f.) ..... 12

Interneto stebėjimo sistemos (5A001.j.) ..... 13

Įsilaužimo programinė įranga (4A005, 4D004 ir susijusios kontrolės priemonės pagal 4E001.a. ir 4E001.c.) ..... 13

Ryšių stebėsenos programinė įranga (5D001.e.) ..... 14

Kriptoanalitinėms funkcijoms atlikti skirtos prekės (5A004.a.) ..... 14

Teismo ekspertizės / tyrimo priemonės (5A004.b., 5D002.a.3.b. ir 5D002.c.3.b.) ..... 14

## ĮVADAS

Reglamentu (ES) 2021/821 (toliau – Reglamentas) nustatyta Sąjungos eksporto kontrolės sistema siekiama užtikrinti, kad būtų laikomasi Sąjungos ir jos valstybių narių tarptautinių įsipareigojimų ir įsipareigojimų, be kita ko, susijusių su regionine taika, saugumu ir stabilumu, žmogaus teisių ir tarptautinės humanitarinės teisės paisymu. Todėl Sąjunga ir jos valstybės narės įgyvendino pagal daugiašalius eksporto kontrolės režimus priimtus sprendimus ir atitinkamai atnaujino Reglamento I priede pateiktą Sąjungos kontrolės priemonių sąrašą ([1]). Be to, prieš pradedant taikyti Reglamento 5 straipsnį, valstybių narių kompetentingos institucijos jau kontroliavo tam tikrų sąraše išvardytų prekių, kurios gali turėti stebėjimo funkcijų ([2]), eksportą, atsižvelgdamos į piktnaudžiavimo tam tikromis konkrečiomis aplinkybėmis riziką. Ypač rimtais atvejais Sąjunga nustatė sankcijas, kuriomis apribojo tam tikros stebėjimo įrangos eksportą ([3]).

Reglamentas atspindi Sąjungos įsipareigojimą veiksmingai mažinti riziką, kad kibernetinio stebėjimo prekės galėtų būti naudojamos vykdant vidaus represijas ir (arba) šiurkščius žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimus. Reglamentu visų pirma nustatomos naujos nuostatos dėl sąraše neišvardytų kibernetinio stebėjimo prekių eksporto kontrolės, įskaitant įpareigojimą eksportuotojams pranešti kompetentingai institucijai, kai jie, remdamiesi savo išsamaus patikrinimo metu nustatytais faktais, nustato, kad sąraše neišvardytos kibernetinio stebėjimo prekės, kurias siūlo eksportuoti eksportuotojai, bus visiškai arba iš dalies skirtos naudoti vykdant vidaus represijas ir (arba) šiurkščius žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimus. Be to, Reglamente Komisija ir Taryba raginamos eksportuotojams pateikti gaires, kuriomis būtų remiamas veiksmingas naujų sąraše neišvardytų kibernetinio stebėjimo prekių kontrolės priemonių įgyvendinimas.

Todėl šiomis gairėmis siekiama padėti eksportuotojams taikyti sąraše neišvardytų kibernetinio stebėjimo prekių kontrolę, įskaitant, be kita ko, išsamaus patikrinimo priemones, kuriomis vertinama rizika, susijusi su tokių prekių eksportu galutiniams naudotojams ir galutiniu naudojimu pagal naujas Reglamento nuostatas.

## 1. AKTUALIOS TEISINĖS NUOSTATOS, APIBRĖŽTYS IR PAGRINDINĖS SĄVOKOS

### 1.1. Aktualių teisinių nuostatų apžvalga

Reglamentu nustatomos naujos nuostatos, kuriomis konkrečiai numatoma Reglamento I priede neišvardytų kibernetinio stebėjimo prekių, kurios visos ar iš dalies, yra arba gali būti naudojamos vidaus represijoms ir (arba) sunkiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti. Aktualios konstatuojamosios dalys ir straipsniai:

a) 8 konstatuojamoji dalis. „siekiant užkirsti kelią rizikai, kad asmenys, prisidedantys prie vadovavimo vykdant sunkius žmogaus teisių arba tarptautinės humanitarinės teisės pažeidimus arba prie jų vykdymo, arba atsakingi už nurodymą juos vykdyti arba už jų vykdymą, gali naudoti tam tikras į sąrašą neįtrauktas iš Sąjungos muitų teritorijos eksportuotas kibernetinio stebėjimo prekes, reikėtų kontroliuoti tokių prekių eksportą. Ši rizika visų pirma susijusi su atvejais, kai kibernetinio stebėjimo prekės yra specialiai sukurtos taip, kad būtų galima įsilaužti į informacines ir telekomunikacijų

([1]) Žr. visų pirma kontrolės priemones, susijusias su telekomunikacijos perėmimo sistemomis (5A001.f), interneto stebėjimo sistemomis (5A001.j.), įsilaužimo programine įranga (4A005, 4D004 ir susijusias kontrolės priemones pagal 4E001.a ir 4E001.c) ir teisėsaugos srityje naudojama stebėjimo programine įranga (5D001.e). Taip pat, atsižvelgiant į kiekvieno konkretaus atvejo vertinimą, žr. kontrolės priemones, susijusias su tam tikromis teismo ekspertizės / tyrimo priemonėmis (5A004.b 5D002.a.3.b ir 5D002.c.3.b).

([2]) Visų pirma informacijos saugumo sistemų.

([3]) Žr. 2006 m. gegužės 18 d. Tarybos reglamentą (EB) Nr. 765/2006 dėl ribojamųjų priemonių atsižvelgiant į padėtį Baltarusijoje ir į Baltarusijos įsitraukimą į Rusijos agresiją prieš Ukrainą (OL L 134, 2006 5 20, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); 2011 m. balandžio 12 d. Tarybos reglamentą (ES) Nr. 359/2011 dėl ribojamųjų priemonių, taikytinų tam tikriems asmenims, subjektams ir įstaigoms atsižvelgiant į padėtį Irane, (OL L 100, 2011 4 14, p. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); 2012 m. sausio 18 d. Tarybos reglamentą (ES) Nr. 36/2012 dėl ribojamųjų priemonių, atsižvelgiant į padėtį Sirijoje, kuriuo panaikinamas Reglamentas (ES) Nr. 442/2011, (OL L 16, 2012 1 19, p. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); 2013 m. gegužės 2 d. Tarybos reglamentą (ES) Nr. 401/2013 dėl ribojamųjų priemonių Mianmarui / Birmai, kuriuo panaikinamas Reglamentas (EB) Nr. 194/2008, (OL L 121, 2013 5 3, p. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj) ir 2017 m. lapkričio 13 d. Tarybos reglamentą (ES) 2017/2063 dėl ribojamųjų priemonių atsižvelgiant į padėtį Venesueloje (OL L 295, 2017 11 14, p. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

sistemas arba atlikti išsamų duomenų paketų patikrinimą, kad būtų galima slaptai stebėti fizinius asmenis stebint, išgaunant, renkant ar analizuojant duomenis, įskaitant biometrinius duomenis, iš tų sistemų. Prekės, naudojamos išimtinai komerciniais tikslais, pvz., sąskaitoms išrašyti, rinkodarai, kokybiškoms paslaugoms, vartotojų pasitenkinimui arba tinklo saugumui, paprastai nelaikomos keliančiomis tokią riziką“;

b) 9 konstatuojamoji dalis. „siekiant sustiprinti veiksmingą į sąrašą neįtrauktų kibernetinio stebėjimo prekių eksporto kontrolę, labai svarbu toliau derinti visa apimančios kontrolės taikymą toje srityje. Tuo tikslu valstybės narės yra įsipareigojusios remti tokią kontrolę dalydamosi tarpusavyje ir su Komisija informacija, visų pirma apie kibernetinio stebėjimo prekių technologinę plėtrą, ir budriai taikydamos tokią kontrolę skatinti keitimąsi informacija Sąjungos lygmeniu“;

c) 2 straipsnio 20 punktas, kuriame pateikiama kibernetinio stebėjimo prekių apibrėžtis: „dvejopo naudojimo prekės, specialiai sukurtos tam, kad būtų galima slaptai stebėti fizinius asmenis stebint, išgaunant, renkant ar analizuojant duomenis iš informacinių ir telekomunikacijų sistemų“;

d) 5 straipsnyje nustatoma, kad sąraše neišvardytoms kibernetinio stebėjimo prekėms eksportuoti reikia eksporto leidimo, jei kompetentinga institucija yra informavusi eksportuotoją, kad atitinkamos prekės, visos ar iš dalies, yra arba gali būti naudojamos vidaus represijoms ir (arba) sunkiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti (5 straipsnio 1 dalis). Jame taip pat reikalaujama, kad eksportuotojai praneštų kompetentingai institucijai, kai jie, remdamiesi savo išsamaus patikrinimo išvadomis, žino, kad prekes ketinama naudoti, visas arba iš dalies, vidaus represijoms ir (arba) šiurkštiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti (5 straipsnio 2 dalis). Ta kompetentinga institucija nusprendžia, ar atitinkamam eksportui reikia leidimo, ir

e) 5 straipsnio 2 dalyje taip pat nustatyta, kad „Komisija ir Taryba pateikia eksportuotojams skirtas gaires, kaip nurodyta 26 straipsnio 1 dalyje“.

## 1.2. **Pagrindinės apibrėžtys**

Reglamente pateikiamos specialios konstatuojamosios dalys ir nuostatos, kuriose paaiškinamos konkrečios sąraše neišvardytų kibernetinio stebėjimo prekių eksporto kontrolės sąlygos, kurios yra svarbios eksportuotojams, kad jie galėtų atlikti išsamius patikrinimus ir veiksmingai taikyti kontrolės priemones. Ypač svarbu, kad 2 straipsnio 20 punkte pateikiama tiksli kibernetinio stebėjimo prekių apibrėžtis: „dvejopo naudojimo prekės, specialiai sukurtos tam, kad būtų galima slaptai stebėti fizinius asmenis stebint, išgaunant, renkant ar analizuojant duomenis iš informacinių ir telekomunikacijų sistemų“.

Šiose gairėse turėtų būti paaiškinti konkretūs tos apibrėžties aspektai.

### 1.2.1. *„Specialiai sukurta“*

Prekė sukurta tam, kad būtų galima vykdyti slaptą stebėjimą, jeigu jos techninės savybės yra tinkamos ir dėl jų objektyviai galima vykdyti slaptą fizinių asmenų stebėjimą. Todėl terminas „specialiai sukurta“ reiškia, kad slaptas fizinių asmenų stebėjimas turi būti pagrindinis tokios prekės sukūrimo tikslas. Tačiau ši sąvoka nereiškia, kad prekė turi būti skirta tik slaptam fizinių asmenų stebėjimui.

Kaip paaiškinta Reglamento 8 konstatuojamojoje dalyje, prekės, naudojamos išimtinai komerciniai tikslais, pavyzdžiui, sąskaitoms išrašyti, rinkodarai, kokybiškoms paslaugoms, naudotojų pasitenkinimui ar tinklo saugumui užtikrinti, nėra specialiai sukurtos slaptam fizinių asmenų stebėjimui ir todėl nepatenka į kibernetinio stebėjimo prekių apibrėžtį. Pavyzdžiui, net jei prekės, skirtos operacinėms sistemoms stebėti pramonėje arba naudotojų srautui stebėti, galėtų būti naudojamos stebėjimo tikslais, šios prekės nėra kibernetinio stebėjimo prakės pagal apibrėžtį, nes jos nėra specialiai sukurtos slaptam fizinių asmenų stebėjimui.

1.2.2. *„Slaptas stebėjimas“*

Naudojant prekę sudaromos sąlygos vykdyti slaptą stebėjimą, visų pirma tais atvejais, kai tokio stebėjimo akivaizdžiai nepastebi fizinis asmuo, kurio atžvilgiu jis vykdomas. Taip būtų tais atvejais, kai atitinkami asmenys nežinotų, kad naudojamos tokios kibernetinio stebėjimo prekės ir (arba) vykdomi tokie veiksmai ir todėl neturėtų galimybės nutraukti tokį stebėjimą ar bent jau atitinkamai pakoreguoti savo elgesį. NET jei stebėjimas vykdomas naudojant viešojoje erdvėje įrengtus ar veikiančius objektus, duomenų gavimas tam tikrais atvejais gali būti laikomas svarbiu slapto stebėjimo aspektu, visų pirma todėl, kad surinkti duomenys gali būti nukreipiami, vertinami arba tvarkomi kitais tikslais nei tie, apie kuriuos buvo informuotas nukentėjęs fizinis asmuo. Kitaip tariant, jeigu fizinis asmuo negali objektyviai tikėtis, kad bus stebimas, pagal reglamento 2 straipsnio 20 punktą gali būti laikoma, kad vykdomas slaptas stebėjimas.

1.2.3. *„Fiziniai asmenys“*

„Fizinis asmuo“ yra tikras žmogus, t. y. ne juridinis asmuo ir ne subjektas, kuriam nuostatos netaikomos. Ši sąvoka neapima objektų, vietų ar mašinų stebėjimo.

1.2.4. *„Duomenų stebėjimas, išgavimas, rinkimas ar analizavimas“*

Remiantis Oksfordo anglų kalbos žodynu, žodžiai „stebėjimas“, „išgavimas“, „rinkimas“ ir „analizavimas“ turi šią kalbinę reikšmę:

— „stebėjimas“ – (slaptas) sekimas, priežiūra, slaptas klausymasis;

— „išgavimas“ – ištraukimas;

— „rinkimas“ – kaupimas, susirinkimas;

— „analizavimas“ – ko nors (sudėtinio) elementų atskyrimas ar nustatymas, kad būtų galima nustatyti nagrinėjamo objekto struktūrą ar pobūdį ir taip jį paaiškinti arba suprasti; atidus ir metodiškas nagrinėjimas aiškinimo tikslais; svarbios arba skaičiuojamosios analizės atlikimas.

Šie terminai reiškia, kad stebėjimui naudojamos prekės turėtų suteikti tikslias technines galimybes tvarkyti duomenis siekiant stebėti, rinkti, išgauti ar analizuoti duomenis. Tai, pavyzdžiui, gali būti prekės, kurios:

a) naudojamos informacinių ir telekomunikacijų sistemų duomenims stebėti ([4]), (pavyzdžiui, tokiose sistemose perduodamų duomenų rinkmenų dydžiams arba duomenų rinkinių srautams stebėti);

b) naudojamos siekiant išgauti duomenis iš informacinių ir telekomunikacijų sistemų įsilaužiant ir išgaunant duomenis, (pavyzdžiui, įsilaužimo programinė įranga);

c) naudojamos analizuojant iš informacinių ir telekomunikacijų sistemų išgautus duomenis, įskaitant prekes, kurios gali būti naudojamos apdorojant tose sistemose saugomus atvaizdus, (pavyzdžiui, tam tikrų rūšių duomenų analizės technologijos, naudojamos veido atpažinimo sistemose).

Prekės, naudojamos tik informacinėms sistemoms stebėti arba gyventojams stebėti naudojant vaizdo stebėjimo kameras ir pokalbiams, keitimuisi duomenimis, judėjimui bei individualiam elgesiui fiksuoti, pagal Reglamente pateiktą apibrėžtį nebūtų laikomos kibernetinio stebėjimo prekėmis, nes jos nėra specialiai šiems tikslams sukurtos prekės ir turi būti naudojamos kartu su kitomis technologijomis, pavyzdžiui, dirbtiniu intelektu ar didžiaisiais duomenimis. Tačiau visa sistema (kurioje tokios prekės naudojamos kartu su kitomis technologijomis, pavyzdžiui, dirbtiniu intelektu ar didžiųjų duomenų technologijomis) galėtų būti laikoma kibernetinio stebėjimo preke, atitinkančia Reglamento 2 straipsnio 20 punkte pateiktą apibrėžtį.

Svarbu tai, kad kibernetinio stebėjimo prekių apibrėžtis ir taikymo sritis nėra ribojamos tik šiais naudingais pavyzdžiais, nes 5 straipsnio tikslas – sudaryti sąlygas veiksmingai sąraše neišvardytų prekių eksporto kontrolei.

([4]) Žr. 1.2.5 skirsnyje pateikiamą apibrėžtį.

Kaip matyti iš apibrėžtyje vartojamo jungtuko „arba“, išvardyti techniniai pajėgumai turi būti laikomi alternatyvomis ir norint stebėti, išgauti, rinkti ar analizuoti duomenis nebūtina, kad objektas turėtų visus šiuos techninius pajėgumus. Kitaip tariant, pakanka, kad vienas iš tų techninių pajėgumų atitiktų 2 straipsnio 20 punkte pateiktą kibernetinio stebėjimo prekės apibrėžtį.

1.2.5. *„Iš informacinių ir telekomunikacijų sistemų“*

Tai sistemos, kurios elektroniniu būdu apdoroja informaciją, pavyzdžiui, programavimo / kodavimo, asmeninių kompiuterių sistemų (aparatinės įrangos) operacijų ir kitos informacijos administravimo, įskaitant programinės įrangos technologijas, žiniatinklio technologijas, kompiuterių technologijas, saugojimo technologijas ir kt., taip pat kai kurias sistemas, kuriomis informacija perduodama per atstumą, pavyzdžiui, technines sistemas, kurias naudojant laidiniais ir belaidžiais kanalais, optinėmis skaidulomis, radijo ir kitomis elektromagnetinėmis sistemomis perduodami garsai, signalai, tekstas, kiti ženklai arba vaizdai. Šios dvi sąvokos kartu apima įvairias informacijos perdavimo arba apdorojimo sistemas. Reikėtų pažymėti, kad šis terminas naudojamas sistemoms, o ne įrangai, apibūdinti.

1.2.6. *„Žinojimas“ ir „ketinama naudoti“*

Pagal reglamento 5 straipsnio 2 dalį eksportuotojas turi pranešti kompetentingai institucijai, kai eksportuotojas „žino, kad <...> kibernetinio stebėjimo prekes ketinama naudoti <...> vidaus represijoms ir (arba) šiurkštiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti“.

Terminas „žinojimas“ nėra nauja teisinė sąvoka, jis vartojamas kalbant apie su galutiniu naudojimu susijusius leidimų reikalavimus (vadinamąją visa apimančią kontrolę) pagal Reglamento 4, 6, 7 ir 8 straipsnius. Žinojimas reiškia, kad eksportuotojas turi informacijos, kuria remdamasis gali patvirtinti, kad prekes ketinama naudoti netinkamai. Žinojimui užtikrinti vien tokios rizikos galimybės nepakanka. Tačiau terminas „žinojimas“ negali būti prilyginamas pasyvumui: eksportuotojas turi imtis veiksmų, kad gautų pakankamos ir tinkamos informacijos, reikalingos su eksportu susijusiai rizikai įvertinti ir užtikrinti, kad būtų laikomasi Reglamento.

Nuoroda, kad prekes turi būti ketinama naudoti atitinkamais su probleminiais vartotojais susijusiais tikslais, reiškia, kad eksportuotojas turėtų įvertinti prekių naudojimą kiekvienu konkrečiu atveju, atsižvelgdamas į konkrečias to atvejo aplinkybes. *A contrario*, teorinės rizikos, t. y. rizikos, kurios negalima pagrįsti faktiniu bylos vertinimu, kad prekės gali būti naudojamos pažeidžiant žmogaus teises, nepakanka, kad būtų galima laikyti, jog jas „ketinama naudoti“ konkrečiam netinkamam tikslui pagal 5 straipsnį.

1.3. **Vidaus represijos, šiurkštūs žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimai**

Pagal Reglamento 15 straipsnį, kuriame išdėstyti vertinimo, ar išduoti leidimą, aspektai, valstybės narės turi atsižvelgti į visus svarbius aspektus, įskaitant tuos, kuriems taikoma Tarybos bendroji pozicija 2008/944/BUSP ([5]).

Reglamento 5 straipsniu išplečiama sąraše neišvardytų kibernetinio stebėjimo prekių eksporto kontrolė, atsižvelgiant į riziką, kad jos galėtų būti naudojamos vidaus represijoms ir (arba) sunkiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti. Šiuo atžvilgiu naudingų gairių pateikiama Bendrojoje pozicijoje 2008/944/BUSP ir šios bendrosios pozicijos naudojimo vadove ([6]).

([5]) 2008 m. gruodžio 8 d. Tarybos bendroji pozicija 2008/944/BUSP, nustatanti bendrąsias taisykles, reglamentuojančias karinių technologijų ir įrangos eksporto kontrolę, (OL L 335, 2008 12 13, p. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Žr. Tarybos bendrosios pozicijos 2008/944/BUSP, nustatančios bendrąsias taisykles, reglamentuojančias karinių technologijų ir įrangos eksporto kontrolę, naudojimo vadovą, skelbiamą adresu https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Vidaus represijos*

Pagal Bendrosios pozicijos 2008/944/BUSP 2 straipsnio 2 dalį „[v]idaus represijoms, inter alia, yra priskiriami kankinimai ir kitoks žiaurus, nežmoniškas ar žeminantis elgesys arba baudimas, mirties nuosprendžio įvykdymas be teismo ar savavališkai, asmenų dingimas, nesankcionuotas sulaikymas ir kiti rimti žmogaus teisių ir pagrindinių laisvių pažeidimai, nustatyti atitinkamuose tarptautiniuose žmogaus teisių dokumentuose, tarp jų Visuotinėje žmogaus teisių deklaracijoje bei Tarptautiniame pilietinių ir politinių teisių pakte“ (TPPTP). Bendrosios pozicijos 2008/944/BUSP naudojimo vadove pateikiamos gairės dėl elementų, į kuriuos turi būti atsižvelgiama eksportuotojo vertinime, be kita ko, „einamojo ir ankstesnių laikotarpių duomenų apie taip, kaip siūlomas galutinis naudotojas paiso žmogaus teisių ir kaip šių teisių paisoma šalyje gavėjoje apskritai“.

1.3.2. *Šiurkštūs žmogaus teisių pažeidimai*

Netinkamas sąraše neišvardytų kibernetinio stebėjimo prekių naudojimas gali turėti neigiamą poveikį įvairioms žmogaus teisėms ir tiesiogiai pažeisti teisę į privatumą ir teisę į duomenų apsaugą. Savavališkai ar neteisėtai vykdant stebėjimą taip pat gali būti pažeidžiamos kitos žmogaus teisės, pavyzdžiui, teisės į saviraiškos, asociacijų ir susirinkimų laisvę, minties, sąžinės ir religijos laisvę, taip pat teisė į vienodą požiūrį arba nediskriminavimą bei teisė į laisvus, vienodus ir slaptus rinkimus. Tam tikrais atvejais fizinių asmenų, pavyzdžiui, žmogaus teisių gynėjų, aktyvistų, politinių veikėjų, pažeidžiamų gyventojų ir žurnalistų, stebėjimas, įskaitant jų stebėseną ar informacijos rinkimą, gali tapti bauginimo, teisių atėmimo, savavališko kalinimo, kankinimo ar net neteisminių egzekucijų priežastimi. Todėl atlikdami savo vertinimus eksportuotojai turėtų atsižvelgti į šiuos su sunkiais žmogaus teisių pažeidimais susijusius aspektus.

Iš tarptautinės praktikos matyti, kad bet kokie žmogaus teisių apribojimai turi būti tinkami ir atitikti tarptautinius žmogaus teisių standartus. Praktiškai tai reiškia, kad turi būti taikomos tinkamos apsaugos priemonės, kuriomis būtų galima užtikrinti, kad teisės aktuose būtų numatomi apribojimai ir kad būtų išsaugoma teisių esmė. Remiantis proporcingumo principu, apribojimai gali būti nustatomi tik tuo atveju, jei jie būtini ir jais tikrai siekiama teisėto tikslo, pavyzdžiui, nacionalinio ar visuomenės saugumo, viešosios tvarkos, visuomenės sveikatos apsaugos ar kitų asmenų teisių ir laisvių apsaugos.

Kibernetinio stebėjimo prekės gali apimti teisėtas ir reguliuojamas teisėsaugos tikslais naudojamas priemones, pavyzdžiui, nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, be kita ko, kovos su terorizmu srityje, arba baudžiamųjų sankcijų vykdymo priemones. Tačiau kibernetinio stebėjimo prekės taip pat gali būti netinkamai naudojamos sunkiems žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimams vykdyti, kai jos eksportuojamos represiniams režimams ar privatiems galutiniams naudotojams ir (arba) į konfliktines zonas.

Todėl reikia įvertinti kiekvieno konkretaus atvejo aplinkybes, įskaitant atitinkamų taisyklių taikymą, atsižvelgiant į bet kokius, pavyzdžiui, Jungtinių Tautų, Sąjungos ar Europos Tarybos, kompetentingų įstaigų pranešimus apie sunkius žmogaus teisių pažeidimus. Žmogaus teisių pažeidimų sunkumas gali būti grindžiamas tų pažeidimų pripažinimu Jungtinių Tautų, Sąjungos ar Europos Tarybos kompetentingų įstaigų paskelbtoje informacijoje. Toks aiškus šių įstaigų pripažinimas nėra absoliuti būtinybė, tačiau tai yra svarbus veiksnys siekiant užtikrinti, kad kriterijai būtų įvykdyti.

Pagal 5 straipsnio nuostatas žmogaus teisių pažeidimas turi būti sunkus. Naudingų rekomendacijų dėl galimų žmogaus teisių pažeidimų priskyrimo galimiems sunkiems žmogaus teisių pažeidimams galima rasti Bendrosios pozicijos 2008/944/BUSP naudojimo vadove. Vadovaujantis šiuo vadovu, lemiamieji veiksniai yra pažeidimo pobūdis ir pasekmės. Paprastai sunkiais pažeidimais laikomi sistemingi ir (arba) plačiai paplitę žmogaus teisių pažeidimai. Tačiau tai gali būti ir ne tik sistemingi ar plačiai paplitę pažeidimai, pavyzdžiui, vertinant pagal intervencinio veiksmo poveikio nukentėjusiems asmenims sunkumą.

Bendrosios pozicijos 2008/944/BUSP naudojimo vadovo II priede pateikiamas nebaigtinis pagrindinių tarptautinių ir regioninių žmogaus teisių dokumentų, įskaitant Tarptautinį pilietinių ir politinių teisių paktą (TPPTP), Jungtinių Tautų konvenciją prieš kankinimą ir kitokį žiaurų, nežmonišką ar žeminantį elgesį ar baudimą, Europos žmogaus teisių konvenciją (toliau – Konvencija) ir Pagrindinių teisių chartiją (toliau – Chartija), sąrašas, kuriame galima rasti svarbių gairių, kaip aiškinti ir taikyti kriterijus, kuriais grindžiami patikimi žmogaus teisių vertinimai. Šie dokumentai ir jų atitinkami papildomi protokolai yra pagrindinės tarptautinės normos ir standartai žmogaus teisių ir pagrindinių laisvių srityse.

1.3.3. *Šiurkštūs tarptautinės humanitarinės teisės pažeidimai*

Tarptautinė humanitarinė teisė (taip pat vadinama Ženevos teise arba ginkluotųjų konfliktų teise) buvo išplėtota įvairiomis tarptautinėmis sutartimis, visų pirma Hagos taisyklėmis, Ženevos konvencijomis ir jų dviem 1977 m. paskelbtais papildomais protokolais, ir joje nustatytos taisyklės, kuriomis vadovaujantis ginkluoto konflikto metu turi būti apsaugomi asmenys, kurie nedalyvauja arba nebedalyvauja karo veiksmuose, (pavyzdžiui, civiliai gyventojai ir sužeisti sergantys ar į nelaisvę paimti kovotojai) ir kuriomis kariaujančiosioms šalims nustatomi su karo priemonėms ir metodais susiję apribojimai (Hagos teisė).

Sąraše neišvardytų kibernetinio stebėjimo prekių naudojimas turėtų atitikti tarptautinę humanitarinę teisę, jei tos prekės naudojamos kaip karo priemonės ir metodai ginkluoto konflikto metu. Tokiomis aplinkybėmis pagal Reglamentą atsižvelgiama į šiurkščių tarptautinės humanitarinės teisės pažeidimų riziką ir, kaip ir šiurkščių žmogaus teisių pažeidimų atveju, ši rizika turėtų būti vertinama atsižvelgiant į numatomą prekių naudojimo būdą konkrečiu atveju. Bendrosios pozicijos 2008/944/BUSP naudojimo vadove pateikiamos gairės dėl elementų, į kuriuos reikia atsižvelgti, įskaitant duomenis apie tai, kaip gavėjas anksčiau ir šiuo metu laikosi tarptautinės humanitarinės teisės aktų, gavėjo ketinimus, kurie turi būti išreikšti oficialiais įsipareigojimais, ir gavėjo gebėjimą užtikrinti, kad perduota įranga ar technologijos būtų naudojamos laikantis tarptautinės humanitarinės teisės aktų ir nebūtų nukreipiamos ar perkeliamos į kitas paskirties vietas, kuriose jos galėtų būti naudojamos sunkiems šių teisės aktų pažeidimams vykdyti.

Pagal 5 straipsnį tarptautinės humanitarinės teisės pažeidimas turi būti sunkus. Gairių pateikiama Bendrosios pozicijos 2008/944/BUSP naudojimo vadove, kuriame pripažįstama, kad „atskiri tarptautinės humanitarinės teisės pažeidimų incidentai nebūtinai atspindi šalies gavėjos požiūrį į tarptautinę humanitarinę teisę“ ir „jeigu galima pastebėti tam tikrą pažeidimų modelį arba jeigu šalis gavėja nesiima tinkamų priemonių nubausti už pažeidimus, tai turėtų kelti didelį susirūpinimą“. Tarptautinis Raudonojo Kryžiaus komitetas (TRKK) yra pateikęs gaires dėl tarptautinės humanitarinės teisės pažeidimų vertinimo vykdant eksporto kontrolę. Tarptautinio Raudonojo Kryžiaus komiteto teigimu, „laikoma, kad tarptautinės humanitarinės teisės pažeidimai yra sunkūs, jei dėl jų atsiranda pavojus asmenims, kuriems suteikiama tarptautinė apsauga, (pavyzdžiui, civiliams, karo belaisviams, sužeistiesiems ir sergantiesiems) arba objektams (pavyzdžiui, civiliniams objektams ar infrastruktūrai) arba jeigu dėl jų pažeidžiamos svarbios visuotinės vertybės“. Pavyzdžiui, karo nusikaltimai yra sunkūs tarptautinės humanitarinės teisės pažeidimai. TRKK taip pat nurodo panašius veiksnius, į kuriuos turėtų būti atsižvelgiama Bendrosios pozicijos 2008/944/BUSP naudojimo vadove, įskaitant oficialius įsipareigojimus taikyti tarptautinės humanitarinės teisės taisykles, tinkamas priemones, kuriomis užtikrinama atskaitomybė už tarptautinės humanitarinės teisės pažeidimus, kariuomenei skirtus tarptautinės humanitarinės teisės srities mokymus ir draudimą verbuoti vaikus į ginkluotąsias pajėgas.

## 2. **TECHNINĖ TAIKYMO SRITIS**

### 2.1. **Sąraše išvardytos kibernetinio stebėjimo prekės**

Šių gairių priedėlyje pateikiama informacija apie Reglamento I priede išvardytas kibernetinio stebėjimo prekes, taip siekiant padėti eksportuotojams nustatyti galimas sąraše neišvardytas kibernetinio stebėjimo prekes.

### 2.2. **Galimos sąraše neišvardytos kibernetinio stebėjimo prekės**

Nors iš esmės neįmanoma pateikti išsamaus prekių, kurios pagal 5 straipsnį gali būti kontroliuojamos kaip sąraše neišvardytos prekės, sąrašo, toliau nurodytos prekės galėtų būti naudojamos stebėjimui vykdyti, todėl pagal Reglamentą joms reikėtų taikyti ypatingo budrumo priemones.

Kaip paaiškinta Reglamento 8 konstatuojamojoje dalyje, prekės, naudojamos išimtinai komerciniais tikslais, pavyzdžiui, sąskaitoms išrašyti, rinkodarai, kokybiškoms paslaugoms, naudotojų pasitenkinimui ar tinklo saugumui užtikrinti, paprastai nelaikomos keliančiomis riziką, kad jos bus naudojamos netinkamai ir kad jos bus panaudotos sunkiems žmogaus teisių arba tarptautinės humanitarinės teisės pažeidimams, todėl paprastai joms netaikomos 5 straipsnyje nustatytos kontrolės priemonės. Daug šių prekių turi Reglamento I priedo kontrolinio teksto 5 kategorijos 2 dalyje nurodytus kontrolės parametrus atitinkančias informacijos saugumo (kriptografijos ar net kriptoanalizės) funkcijas. Tinklų saugumo tinklo įrangai, įskaitant maršruto parinktuvus, jungiklius ar persiuntimo mazgus, kurių informacijos saugumo funkcijos yra susijusios tik su operacijų, administravimo ar techninės priežiūros užduotimis, įgyvendinant tik paskelbtus arba komercinius kriptografijos standartus, kibernetinio stebėjimo prekių apibrėžtis taip pat netaikoma, nors eksportuotojai turėtų išlikti budrūs ir atsižvelgti į įvairius pranešimus apie netinkamą tokių objektų naudojimą vykdant žmogaus teisių pažeidimus.

2.2.1. *Veido ir emocijų atpažinimo technologijos*

Veido ir emocijų atpažinimo technologijos gali būti naudojamos ne tik kibernetiniam stebėjimui, bet ir įvairioms reikmėms, pavyzdžiui, atpažinimui ar autentiškumui nustatyti, todėl kibernetinio stebėjimo prekių apibrėžtis joms automatiškai netaikoma. Tačiau tam tikromis aplinkybėmis veido ir emocijų atpažinimo technologijos gali būti laikomos Reglamento 2 straipsnio 20 punkte apibrėžtomis prekėmis.

Veido ir emocijų atpažinimo technologijos, kurios gali būti naudojamos saugomiems nufilmuotiems vaizdams stebėti arba analizuoti, galėtų būti laikomos kibernetinio stebėjimo prekėmis. Tačiau net jei programinė įranga atitinka pirmiau minėtus kriterijus, reikia atidžiai išnagrinėti, ar tokia įranga yra specialiai sukurta slaptam stebėjimui.

2.2.2. *Vietos nustatymo įtaisai*

Vietos nustatymo įtaisai suteikia galimybę stebėti fizinę įrenginio buvimo vietą laikui bėgant, o teisėsaugos ir žvalgybos agentūros kai kurias vietos nustatymo technologijas naudoja jau kurį laiką. Galimybės naudojant šiuos įtaisus vykdyti tikslinį ir masinį stebėjimą buvo labai išplėtotos, nes sekimo technologijos tapo pažangesnės: plačiai paplito galimybės naudoti palydovinio ryšio vietos nustatymo sistemas, mobiliojo ryšio bokštų vietos nustatymo sistemas, belaidžio vietinio ryšio ir „Bluetooth“ siųstuvus-imtuvus, taip pat sekimo prietaisus, pvz., išmaniuosius telefonus ir kitus elektroninius prietaisus (pvz., automobiliuose montuojamas transporto priemonėms skirtas sistemas).

Vietos nustatymo prietaisus naudoja teisėsaugos ir žvalgybos agentūros, pavyzdžiui, rinkdamos įrodymus tyrimo metu arba sekdamos įtariamuosius, taip pat bendrovės komerciniais tikslais, pavyzdžiui, teikdamos ataskaitas dėl bendrų judėjimo modelių parduotuvių rajono gatvėse, sekdamos už darbo vietos ribų dirbančius darbuotojus arba pagal vietą parenkamos reklamos tikslais.

2.2.3. *Stebėjimo vaizdo kameromis sistemos*

Siekiant padėti eksportuotojams nustatyti kibernetinio stebėjimo galimybę, taip pat naudinga paaiškinti, kokioms prekėms ši apibrėžtis nebūtų taikoma. Šiuo požiūriu, kibernetinio stebėjimo prekių apibrėžtis netaikoma, pavyzdžiui, vaizdo stebėjimo sistemoms ir kameroms, įskaitant didelės skiriamosios gebos kameras, kurios naudojamos žmonėms filmuoti viešosiose erdvėse, nes jas naudojant nevykdoma stebėsena ir nerenkami duomenys iš informacinių ir telekomunikacijų sistemų.

## 3. **IŠSAMAUS PATIKRINIMO PRIEMONĖS**

Kaip nurodyta Reglamento 7 konstatuojamojoje dalyje, „labai svarbu, kad eksportuotojai <...> prisidėtų prie bendro prekybos kontrolės tikslo. Kad jie galėtų veikti laikydamiesi šio reglamento, su sandoriais, kuriems taikomas šis reglamentas, susijęs rizikos vertinimas turi būti atliekamas taikant sandorių tikrinimo priemones, dar vadinamas deramo tikrinimo principu, kurios yra vidaus atitikties užtikrinimo programų dalis“.

2 straipsnio 21 punkte vidaus atitikties užtikrinimo programa (angl. ICP) apibrėžta kaip „vykdoma veiksminga, tinkama ir proporcinga politika ir procedūros, kurias eksportuotojai patvirtino, kad palengvintų atitiktį šio reglamento nuostatoms ir tikslams ir pagal šį reglamentą įgyvendinamoms leidimų sąlygoms, įskaitant, be kita ko, išsamaus patikrinimo priemones vertinant riziką, susijusią su atitinkamų prekių eksportu galutiniams naudotojams ir galutiniu naudojimu“.

Komisijos rekomendacijoje (ES) 2019/1318 ([7]) nustatyta sistema, skirta padėti eksportuotojams nustatyti, valdyti ir sušvelninti su prekybos dvejopo naudojimo prekėmis kontrole susijusią riziką ir užtikrinti, kad būtų laikomasi atitinkamų Sąjungos ir nacionalinių įstatymų ir kitų teisės aktų.

Šios gairės gali padėti eksportuotojams taikyti sandorių tikrinimo priemones, dar vadinamas deramo tikrinimo principu, kurios yra vidaus atitikties užtikrinimo programų dalis.

Pagal Reglamento (ES) 2021/821 5 straipsnio 2 dalį sąraše neišvardytų kibernetinio stebėjimo prekių eksportuotojai privalo atlikti išsamų patikrinimą taikydami sandorių tikrinimo priemones, t. y. jie privalo imtis veiksmų, susijusių su prekių klasifikacija ir sandorių rizikos vertinimu. Praktiškai eksportuotojai raginami patikrinti toliau išvardytus aspektus.

([7]) 2019 m. liepos 30 d. Komisijos rekomendacija (ES) 2019/1318 dėl prekybos dvejopo naudojimo prekėmis kontrolės vidaus atitikties užtikrinimo programų pagal Tarybos reglamentą (EB) Nr. 428/2009 (OL L 205, 2019 8 5, p. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Patikrinti, ar sąraše nenurodyta prekė, kurią ketinama eksportuoti, gali būti kibernetinio stebėjimo prekė, specialiai sukurta tam, kad būtų galima slaptai stebėti fizinius asmenis stebint, išgaunant, renkant ar analizuojant duomenis iš informacinių ir telekomunikacijų sistemų.**

Šiuo etapu turi būti atliekamas prekės apibrėžimas pagal kibernetinio stebėjimo prekėms taikomas nuostatas. Tai, be kita ko, yra prekių techninių savybių išnagrinėjimas remiantis Reglamento I priede nustatytais sąraše išvardytų prekių techniniais parametrais ir atsižvelgiant į konkrečius sąraše neišvardytoms prekėms taikomos kibernetinio stebėjimo prekių apibrėžties terminus bei sąvokas ir paskesnį prekės klasifikavimą (prekė, technologija ar programinė įranga).

3.2. **Patikrinti atitinkamos prekės galimybes siekiant nustatyti, ar ją netinkamai naudojant būtų galima vykdyti vidaus represijas ir (arba) sunkius žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimus.**

Eksportuotojai turėtų atlikti vertinimą ir nustatyti, ar prekė galėtų būti netinkamai naudojama vidaus represijoms vykdyti arba žmogaus teisėms, įskaitant teisę į gyvybę, laisvę nepatirti kankinimo, nežmoniško ar žeminančio elgesio, teisę į privatumą, teisę į žodžio laisvę, teisę jungtis į asociacijas ir teisę į susirinkimus, teisę į minties, sąžinės ir religijos laisvę, teisę į vienodą požiūrį ar diskriminacijos draudimą arba teisę į laisvus, vienodus ir slaptus rinkimus, pažeisti ar jomis piktnaudžiauti.

Taip pat turi būti įvertinama, ar prekė galėtų būti naudojama kaip sistemos dalis ar komponentas, dėl kurio galėtų būti padaromi tie patys pažeidimai ir (arba) būti netinkamai naudojama tokia sistema.

Atlikdami šį vertinimą eksportuotojai turėtų naudoti vadinamuosius grėsmės ženklus, kuriais būtų pažymimos bet kokios neįprastos sandorio aplinkybės, iš kurių matyti, kad eksportuojamos prekės gali būti skirtos netinkamam naudojimui, galutiniam naudotojui arba paskirties vietai.

Grėsmės ženklai:

a) prekė parduodama kartu su informacija apie galimą jos naudojimą vykdant slaptą stebėjimą;

b) turima informacijos, kad panaši prekė buvo netinkamai panaudota vykdant vidaus represijas ir (arba) sunkius žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimus (žr. 1.3 skirsnį);

c) turima informacijos, kad prekė buvo neteisėtai panaudota vykdant prieš valstybę narę nukreiptą sekimo veiklą arba vykdant neteisėtą ES piliečio sekimą;

d) turima informacijos, kad sandoris yra susijęs su prekėmis, kurios galėtų būti naudojamos sistemai, kuri, kaip žinoma, netinkamai naudojama vykdant vidaus represijas ir (arba) sunkius žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimus, kurti, pritaikyti arba konfigūruoti (žr. 1.3 skirsnį);

e) prekė arba panaši prekė yra nurodyta *Europos Sąjungos oficialiojo leidinio* C serijoje pagal Reglamento 5 straipsnio 6 dalį paskelbtame sąraše.

3.3. **Padedant kompetentingoms institucijoms, peržiūrėti sandoryje dalyvaujančias suinteresuotąsias šalis (įskaitant galutinius naudotojus ir gavėjus, pavyzdžiui, platintojus ir perpardavėjus).**

Padedant kompetentingoms institucijoms, eksportuotojai kiek įmanoma turėtų:

a) prieš bet kokį sandorį ir jo metu, remdamiesi galutinio naudojimo pareiškimais, peržiūrėti, kaip gavėjai ir (arba) galutiniai naudotojai ketina naudoti prekę arba paslaugą;

b) susipažinti su padėtimi atitinkamoje prekių paskirties vietoje, visų pirma su bendra žmogaus teisių padėtimi, nes tai yra svarbus su eksportuojamomis prekėmis susijusių sunkių žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimų rizikos rodiklis;

c) vadovaudamiesi toliau išvardytais grėsmės ženklais, peržiūrėti, ar esama rizikos, kad prekė arba paslauga bus nukreiptos kitam neteisėtam galutiniam naudotojui.

Grėsmės ženklai:

a) galutinis naudotojas turi akivaizdžių ryšių su užsienio Vyriausybe, kuri vykdo vidaus represijas ir (arba) šiurkščiai pažeidžia žmogaus teises ir tarptautinę humanitarinę teisę;

b) galutinis naudotojas pagal struktūrą priklauso ginkluotosioms pajėgoms ar kitai grupei, dalyvaujančiai ginkluotame konflikte, susijusiame su vidaus represinėmis priemonėmis ir (arba) praeityje padarytais rimtais žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimais;

c) galutinis naudotojas anksčiau eksportavo kibernetinio stebėjimo prekes į šalis, kuriose dėl tokių prekių naudojimo buvo pradėta taikyti vidaus represines priemones ir (arba) vykdyti sunkius žmogaus teisių ir tarptautinės humanitarinės teisės pažeidimus.

3.4. **Naudojantis išsamaus patikrinimo metu nustatytais faktais parengti planus, kaip užkirsti kelią galimam neigiamam poveikiui ateityje ir jį sušvelninti.**

Eksportuotojai, remdamiesi savo išsamaus patikrinimo išvadomis, turėtų nutraukti veiklą, dėl kurios daromas neigiamas poveikis žmogaus teisėms arba kuria prisidedama prie tokio poveikio, ir parengti ir įgyvendinti taisomųjų veiksmų planą. Tai gali būti:

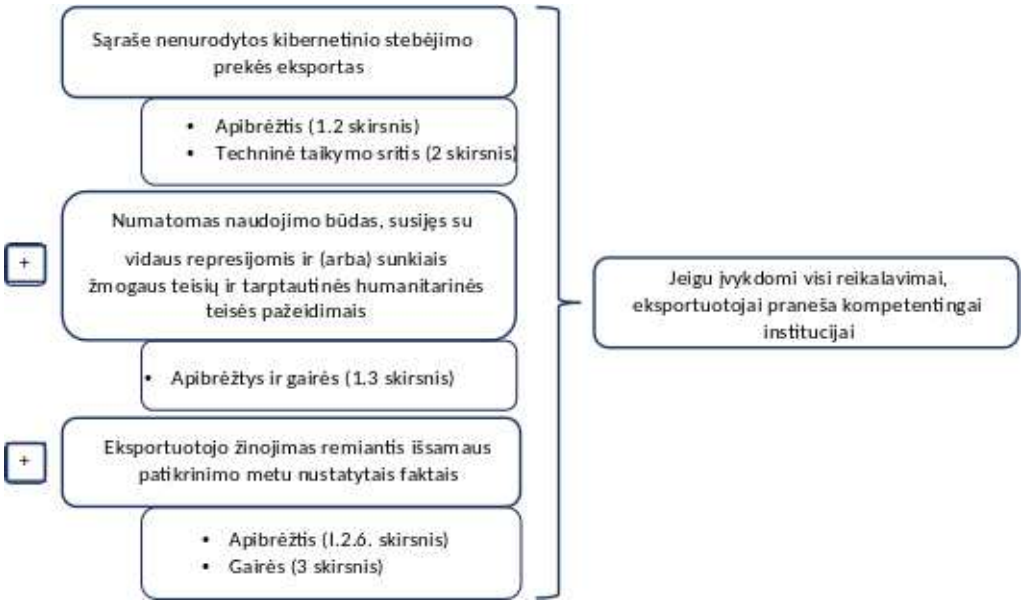
a) įmonės politikos atnaujinimas pateikiant gaires, kaip ateityje išvengti neigiamo poveikio, su juo kovoti ir užtikrinti šių veiksmų įgyvendinimą;

b) remiantis rizikos vertinimo išvadomis atliekamas valdymo sistemų atnaujinimas ir sustiprinimas, kad būtų galima geriau stebėti informaciją ir pažymėti grėsmes prieš atsirandant neigiamam poveikiui;

c) informacijos rinkimas siekiant suprasti, kokios aukšto lygio neigiamo poveikio grėsmės gali būti būdingos atitinkamam sektoriui;

d) valstybių narių kompetentingų institucijų informavimas apie išsamaus patikrinimo išvadas, taip sudarant palankesnes sąlygas su tam tikrais objektais, galutiniais naudotojais ir paskirties vietomis susijusios informacijos srautui.

**Reglamento (ES) 2021/821 5 straipsnio 2 dalyje nustatyti reikalavimai**




4. **PRIEDĖLIS**

**Sąraše išvardytos pagal Reglamento (ES) 2021/821 I priedą kontroliuojamos kibernetinio stebėjimo prekės**

— **Telekomunikacijos perėmimo sistemos (5A001.f.)**

Daugumoje šalių, įskaitant valstybes nares, ryšių konfidencialumas saugomas teisės aktais, tačiau valdžios institucijoms pagal teisinę sistemą gali būti leidžiama slaptai vykdyti elektroninį ryšių stebėjimą (vadinamąjį teisėtą perėmimą). Tačiau skaitmeniniame amžiuje atsirado galimybė masiniu mastu naudoti perėmimo technologijas. Libijos režimo naudojimosi perėmimo priemonėmis pavyzdys parodė, kad šios technologijos gali būti naudojamos masiškai, ir paskatino 2012 m. pradėti taikyti telekomunikacijų perėmimo sistemų eksporto kontrolę.

Ši kontrolė taikoma ryšio turinio (balso ar duomenų), taip pat abonento identifikatorių ar kitų metaduomenų, kurie belaidžiu ryšiu perduodami oru, išgavimo ir radijo dažnių stebėjimo įrangai. Ši kontrolė taikoma, pavyzdžiui, IMSI (tarptautinių judriojo ryšio abonento identifikatorių) gaudyklėms, kuriomis perimamas mobiliųjų telefonų duomenų srautas ir sekamas mobiliųjų telefonų naudotojų judėjimas, arba įrangai, kurią naudojant sukuriamos netikros belaidžio interneto zonos, kuriose iš telefonų galima išgauti IMSI duomenis, taip pat tam tikrų rūšių prekėms, kurios specialiai kuriamos taip, kad būtų galima atlikti išsamų telekomunikacijų sistemų duomenų paketų patikrinimą. Mobilioji telekomunikacijų trukdymo įranga kibernetinio stebėjimo prekėms nepriskiriama, nes ją naudojant nerenkami duomenys.

Nors tokioms sistemoms kurti gali būti naudojamos bendrosios paskirties technologijos, jų masinio perėmimo galimybės priklauso nuo konkrečių dalių ir komponentų, įskaitant, pavyzdžiui, specialią programinę įrangą, pažangiuosius arba specialiosios paskirties integrinius grandynus (pvz., programuojamosios loginės matricos, ASIC ir kt.), skirtas padidinti paketų arba ryšio seansų, kuriuos galima apdoroti per sekundę, skaičiui.

— **Interneto stebėjimo sistemos (5A001.j.)**

Nors didžioji dalis internetinių ryšių dabar paprastai užšifruojami automatiškai, siekiant nustatyti sąsajas tarp asmenų ir domenų vardų vis dar galima naudoti srauto duomenų (metaduomenų) apie ryšius, pvz., IP adresų ir keitimosi duomenimis dažnio ir apimties, perėmimo technologijas. Valdžios institucijos gali teisėtai ir su teisminių institucijų priežiūra naudotis šiomis sistemomis teisėtais tikslais, pavyzdžiui, siekdamos nustatyti asmenų, kurie lankosi su nusikalstamu ar teroristiniu turiniu susijusiose erdvėse, tapatybę. Tačiau vykdant etniniais, religiniais, politiniais ar socialiniais kriterijais grindžiamą interneto duomenų srauto stebėseną ir analizę gali būti sudaromi išsamūs šalies žmonių ir socialinių grupių žemėlapiai, kurie gali būti naudojami gyventojų kontrolės ir represijų ar kitais tikslais, pavyzdžiui, siekiant nustatyti politinius disidentus. Šios prekės gali ne tik padėti vykdyti su žmogaus teisėmis susijusius pažeidimus ir vidaus represijas, bet ir sustiprinti saugumą ir karinius pajėgumus.

5A001.j punkte nustatyta kontrolės priemonė taikoma interneto kontrolės sistemoms, kurios veikia saitų klasės IP tinkle (pavyzdžiui, nacionalinio lygio pagrindiniame IP tinkle), skirtoms analizuoti, išgauti ir indeksuoti perduodamų metaduomenų turiniui (balsui, vaizdo įrašams, pranešimams, priedams) remiantis nekintamaisiais selektoriais ir sudaryti žmonių ryšių tinklo žemėlapiui. Tai prekės, kurias naudojant vykdomas slaptas sekimas, nes asmenys, kuriems taikomos priemonės, nežino, kad jų ryšiai yra perimami. Ir priešingai, kontrolės priemonių nesiekiama taikyti sistemoms, kuriose vykdomi naudotojų ar abonentų veiksmai ar sąveika, ir, pavyzdžiui, socialiniams tinklams ar komercinėms paieškos sistemoms. Be to, kontrolė taikoma sistemoms, kuriose tvarkomi interneto paslaugų teikėjo pagrindinio tinklo duomenys, ir netaikoma socialiniams tinklams ar komercinėms paieškos sistemoms, kuriose tvarkomi naudotojų pateikiami duomenys.

— **Įsilaužimo programinė įranga (4A005, 4D004 ir susijusios kontrolės priemonės pagal 4E001.a. ir 4E001.c.)**

Įsilaužimo programinės įrangos naudotojas gali slapta įgyti nuotolinę prieigą prie elektroninio įrenginio, pvz., išmaniojo telefono, nešiojamojo kompiuterio, serverio ar daiktų interneto įrenginio, gauti įrenginyje saugomus duomenis, vykdyti pasiklausymą per įrenginyje įrengtą arba prie jo prijungtą kamerą ar mikrofoną ir naudoti prietaisą kaip tarpinį elementą atakoms prieš įrangą, prie kurios prijungiamas toks prietaisas, arba prieš jo naudotojo kontaktus (įsilaužimas naudojant trečiųjų šalių prietaisus). Nors esama ir teisėtų įsilaužimo programinės įrangos naudojimo būdų ([8]) (pavyzdžiui, IT specialistų naudojama nuotolinės prieigos programinė įranga), dėl jai būdingo slapto sekimo pobūdžio ir informacijos, kuri gali būti renkama, masto atsiranda didelė teisės į privatumą ir asmens duomenų apsaugą pažeidimų grėsmė ir gali būti daroma didelė žala teisei į saviraiškos laisvę.

([8]) Siekiant aiškumo, neatsižvelgiant į tai, ar prekės naudojimo būdas yra teisėtas, eksportuojant pagal Dvejopo naudojimo prekių reglamento I priedą kontroliuojamas sąraše išvardytas kibernetinio stebėjimo prekes reikėtų gauti leidimą eksportuoti į trečiąsias šalis.

4A005 *et al* nurodytos kontrolės priemonės taikomos programinei įrangai ir sistemoms, įrangai, komponentams ir susijusioms technologijoms, specialiai sukurtoms arba modifikuotoms įsilaužimo programinei įrangai gaminti, valdyti ir kontroliuoti arba tiekti, tačiau netaikomos pačiai Reglamento I priede apibrėžtai įsilaužimo programinei įrangai. Šios kibernetinės priemonės yra kontroliuojamos atsižvelgiant į galimą sutrikdymų mastą ir žalą, kurią būtų galima padaryti sėkmingai jas panaudojus ir įdiegus, tačiau kontrolės priemonėmis nesiekiama daryti poveikio, pavyzdžiui, kibernetinio saugumo srities tyrėjų ir pramonės veiklai, nes jie turi dalytis informacija, susijusia su įsilaužimo programine įranga, kad galėtų atlikti savo produktų korekcijas ir užtikrinti, kad jie būtų įdiegiami anksčiau, nei viešai paskelbiama apie nustatytą pažeidžiamumą.

— **Ryšių stebėsenos programinė įranga (5D001.e.)**

Ši programinė įranga skirta įgaliotoms teisėsaugos institucijoms stebėti ir analizuoti duomenims, kurie surenkami ryšių paslaugų teikėjui taikant privalomas tikslines perėmimo priemones. Ši programinė įranga suteikia galimybę vykdyti paiešką remiantis ryšių turinio arba metaduomenų nekintamaisiais selektoriais, naudojant teisėtam informacijos perėmimui skirtą sąsają ir sudarant žmonių ryšių tinklo žemėlapį arba sekant tikslinių asmenų judėjimą remiantis paieškų rezultatais. Ši programinė įranga skirta vykdyti slaptam stebėjimui, nes ją naudojant duomenys renkami perimant ryšių informaciją, o asmenys apie tai nežino. Be to, naudojant šią programinę įrangą analizuojami per telekomunikacijų sistemas surenkami duomenys. Ši programinė įranga įdiegiama Vyriausybinėje institucijoje (pvz., teisėsaugos stebėsenos įstaigoje) ir kontrolė nėra susijusi su teisėto perėmimo reikalavimų laikymosi užtikrinimo sistemomis (pavyzdžiui, teisėto perėmimo valdymo sistemomis ir tarpininkavimo prietaisais), kurios yra kuriamos komerciniu lygmeniu ir diegiamos ryšių paslaugų teikėjo erdvėje (pavyzdžiui, integruojant jas į ryšių tinklą) ir kurias eksploatuoja ir prižiūri paslaugų teikėjas. Kaip paaiškinta kontrolės priemonių aprašyme, kontrolės priemonės netaikomos programinei įrangai, specialiai sukurtai ar modifikuotai išimtinai komerciniais tikslais, pavyzdžiui, sąskaitų išrašymo tinklo paslaugų kokybės, patirties kokybės, tarpininkavimo prietaisų, mokėjimo mobiliuoju telefonu ar bankininkystės programinei įrangai.

— **Kriptoanalitinėms funkcijoms atlikti skirtos prekės (5A004.a.)**

Ši kontrolės priemonė taikoma kriptografiniams mechanizmams iššifruoti skirtoms prekėms, norint gauti slaptus kintamuosius arba neskelbtinus duomenis, įskaitant atvirąjį tekstą, slaptažodžius arba šifravimo raktus. Kriptografija naudojama siekiant užtikrinti informacijos konfidencialumą. Kriptoanalizė naudojama siekiant panaikinti tą konfidencialumą, todėl ši technologija suteikia galimybę vykdyti slaptą stebėjimą stebint, išgaunant, renkant ar analizuojant duomenis iš informacinių ir telekomunikacijų sistemų.

— **Teismo ekspertizės / tyrimo priemonės (5A004.b., 5D002.a.3.b. ir 5D002.c.3.b.)**

Teismo ekspertizės / tyrimo priemonės skirtos neapdorotiems (pvz., skaičiavimo arba ryšio) duomenims iš įrenginio išgauti taip, kad duomenų nebūtų galima suklastoti ar sugadinti ir juos būtų galima naudoti teisminiams tikslams, t. y. atliekant baudžiamąjį tyrimą ar vykstant teismo procesui. Naudojant šias prekes išvengiama prietaiso autentiškumo patvirtinimo arba autorizavimo kontrolės ir iš prietaiso išgaunami neapdoroti duomenys. Šiuos produktus naudoja ne tik valdžios ir teisėsaugos institucijos, bet ir ginkluotosios pajėgos, norėdamos išgauti ir analizuoti konfiskuotų prietaisų duomenis. Nors šios priemonės naudojamos teisėtai, jos taip pat gali būti naudojamos netinkamai ir todėl gali atsirasti pavojus neskelbtiniems ar komerciniams duomenims.

Tačiau teismo ekspertizės / tyrimo priemonėms, kurios nėra specialiai sukurtos slaptam sekimui, netaikoma 2 straipsnio 20 punkte nustatyta kibernetinio stebėjimo prekių apibrėžtis. Be to, 5A004.b. *et al*. kontrolės priemonių aprašyme neminimos teismo ekspertizės / tyrimo priemonės, kurias taikant išgaunami tik naudotojo duomenys arba neapsaugoti prietaiso duomenys. Kontrolės priemonės taip pat netaikomos gamintojo gamybos ar bandymo įrangai, sistemų administratorių priemonėms ar tik komercinės mažmeninės prekybos sektoriui skirtiems gaminiams, pavyzdžiui, mobiliųjų telefonų atrakinimo gaminiams. Todėl, atsižvelgiant į šių technologijų rūšių įvairovę, kontrolės priemonių taikymas priklauso nuo kiekvieno produkto įvertinimo kiekvienu konkrečiu atveju.

Galiausiai atkreipiame dėmesį, kad esama ir kitų Reglamento I priede išvardytų su stebėjimu susijusių prekių, kurioms neturėtų būti taikoma kibernetinio stebėjimo prekių apibrėžtis (pavyzdžiui, mobiliųjų telekomunikacijų trukdymo įranga (5A001.f.), skirta komunikacijoms ar sistemoms gadinti arba trikdyti, įsilaužimo programinė įranga, kurią naudojant galima modifikuoti sistemą (4D004), ir lazerinė akustinė aptikimo įranga (6A005.g.), kurią naudojant pasitelkiant lazerį galima rinkti garso duomenis arba klausytis pokalbių nuotoliniu būdu (kartais vadinama lazeriniu mikrofonu). Panašiai, kibernetinio stebėjimo prekių apibrėžtis nebūtų taikoma ir sąraše išvardytiems stebėjimo tikslais naudojamiems bepiločiams orlaiviams.