Eiropas Savienības
Oficiālais Vēstnesis

LV
L sērija

2024/2659

16.10.2024.

KOMISIJAS IETEIKUMS (ES) 2024/2659

(2024. gada 11. oktobris)

par kibernovērošanas preču eksporta vadlīnijām, kas darītas pieejamas saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2021/821 5. pantu

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 292. pantu,

tā kā:

(1) Eiropas Parlamenta un Padomes Regula (ES) 2021/821 ([1]) izveido Savienības režīmu divējāda lietojuma preču eksporta, starpniecības, tehniskās palīdzības, tranzīta un pārvadājumu kontrolei.

(2) Regula (ES) 2021/821 vēršas pret risku, ka kibernovērošanas preces tiek izmantotas saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu.

(3) Kiberdrošības un Regulas (ES) 2021/821 konsekventas īstenošanas jautājumā jāgādā par Savienības eksporta kontroles režīma efektivitāti, tālab Komisija un Padome, ievērojot Regulas (ES) 2021/821 5. panta 2. punktu un 26. panta 1. punktu, dara eksportētājiem pieejamas vadlīnijas par sarakstā neminētām kibernovērošanas precēm.

(4) Šā ieteikuma un tam pievienoto vadlīniju mērķis ir atbalstīt eksportētājus kontroles piemērošanā sarakstā neminētām kibernovērošanas precēm, kā arī pienācīgas rūpības pasākumu veikšanā, ar ko novērtē riskus, kas saistīti ar tādu preču eksportu.

(5) Šim ieteikumam pievienotajās vadlīnijās, kuras tika plaši apspriestas Uzraudzības tehnoloģiju ekspertu grupā 2022. un 2023. gadā, ņemtas vērā piezīmes, kas saņemtas 2023. gada otrajā ceturksnī notikušajā sabiedriskajā apspriešanā ([2]).

(6) Būtu jāatgādina, ka šis ieteikums un tam pievienotās vadlīnijas nav saistošas. Tādējādi eksportētājiem arī turpmāk būtu jāpilda pienākumi, kurus tiem uzliek Regula (ES) 2021/821, savukārt Komisijai būtu jānodrošina, ka šis ieteikums laika gaitā aizvien būtu nozīmīgs,

([1]) Eiropas Parlamenta un Padomes Regula (ES) 2021/821 (2021. gada 20. maijs), ar ko izveido Savienības režīmu divējāda lietojuma preču eksporta, starpniecības, tehniskās palīdzības, tranzīta un pārvadājumu kontrolei (OV L 206, 11.6.2021., 1. lpp., 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.

IR PIEŅĒMUSI ŠO IETEIKUMU.

Dalībvalstu kompetentajām iestādēm un eksportētājiem tiek ieteikts tiem ar Regulas (ES) 2021/821 5. panta 2. punktu uzlikto pienākumu izpildē ņemt vērā šā ieteikuma pielikumā sniegtās vadlīnijas.

Briselē, 2024. gada 11. oktobrī

Komisijas vārdā –
priekšsēdētājas izpildvietnieks
Valdis DOMBROVSKIS

PIELIKUMS

SATURS

Lappuse

Ievads ... 4

1. Attiecīgās tiesību normas, definīcijas un galvenie jēdzieni ... 4

1.1. Attiecīgo tiesību normu pārskats ... 4

1.2 Galvenās definīcijas ... 5

1.2.1. “Īpaši izstrādāts” ... 5

1.2.2. “Slepena novērošana” ... 6

1.2.3. “Fiziskas personas” ... 6

1.2.4. “Uzraudzīt, izgūt, vākt, analizēt datus” ... 6

1.2.5. “Informācijas un telesakaru sistēmu” [dati] ... 7

1.2.6. “Informētība” un “ir paredzēts” ... 7

1.3. Iekšējās represijas, cilvēktiesību un starptautisko humanitāro tiesību nopietni pārkāpumi ... 7

1.3.1. Iekšējās represijas ... 8

1.3.2. Cilvēktiesību nopietnu pārkāpumu izdarīšana ... 8

1.3.3. Starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšana ... 9

2. Tehniskais tvērums ... 9

2.1. Sarakstā iekļautas kibernovērošanas preces ... 9

2.2. Sarakstā neminētas potenciālas kibernovērošanas preces ... 9

2.2.1. Sejas un emociju atpazīšanas tehnoloģija ... 10

2.2.2. Līdzsekošanas ierīces ... 10

2.2.3. Videonovērošanas sistēmas ... 10

3. Pienācīgas rūpības pasākumi ... 10

Regulas (ES) 2021/821 5. panta 2. punkta prasības ... 12

4. Papildinājums ... 12

Sarakstā iekļautas kibernovērošanas preces, kas tiek kontrolētas saskaņā ar Regulas (ES) 2021/821 I pielikumu ... 12

Telesakaru pārtveršanas sistēmas (5A001.f) ... 12

Interneta uzraudzības sistēmas (5A001.j) ... 13

“Ielaušanās programmatūra” (4A005, 4D004 un saistītā kontrole saskaņā ar 4E001.a un 4E001.c pozīciju) ... 13

Komunikācijas uzraudzības programmatūra (5D001.e) ... 14

Preces, ar kurām veic kriptoanalīzi (5A004.a) ... 14

Kriminālistikas/izmeklēšanas rīki (5A004.b, 5D002.a.3.b un 5D002.c.3.b) ... 14

IEVADS

Ar Regulu (ES) 2021/821 ("regula") izveidotā Savienības eksporta kontroles sistēma tiecas nodrošināt Savienības un tās dalībvalstu starptautisko pienākumu un saistību, tai skaitā attiecībā uz mieru, drošību un stabilitāti reģionos un cilvēktiesību un starptautisko humanitāro tiesību ievērošanu, izpildi. Savienība un tās dalībvalstis tāpēc ir īstenojušas daudzpusējos eksporta kontroles režīmos pieņemtos lēmumus un attiecīgi atjauninājušas Savienības kontroles ([1]) sarakstu, kas sniegts regulas I pielikumā. Turklāt, kad vēl nebija piemērojams regulas 5. pants, dalībvalstu kompetentās iestādes, ņemot vērā ļaunprātīgas izmantošanas risku zināmos īpašos apstākļos, jau bija kontrolējušas tādu konkrētu sarakstā iekļautu preču eksportu, kuras var tikt izmantotas novērošanai ([2]). Smagu ārkārtas apstākļu dēļ Savienība ir piespriedusi sankcijas, kas ierobežo konkrētu novērošanas aprīkojumu ([3]) eksportu.

Regula rāda Savienības apņemšanos efektīvi novērst risku, ka kibernovērošanas preces varētu tikt izmantotas saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu. Regula pirmām kārtām ievieš jaunus noteikumus par sarakstā neminētu kibernovērošanas preču eksporta kontroli, kā arī uzliek eksportētājiem pienākumu ziņot kompetentajai iestādei, ja, vadoties pēc pienācīgā pārbaudē gūtiem konstatējumiem, tie ir informēti, ka sarakstā neminētas kibernovērošanas preces, kuras eksportētāji ierosina eksportēt, pilnībā vai daļēji ir paredzētas lietošanai saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu. Turklāt regulā Komisija un Padome tiek aicinātas darīt pieejamas eksportētāju vadlīnijas, lai tiktu atbalstīta sarakstā neminētu kibernovērošanas preču jaunās kontroles efektīva izpilde.

Šo vadlīniju mērķis tādējādi ir, pamatojoties ar regulas jaunajiem noteikumiem, sniegt eksportētājiem atbalstu kontroles piemērošanā sarakstā neminētām kibernovērošanas precēm, kā arī tādu pienācīgas rūpības pasākumu veikšanā, ar kuriem tiek novērtēti ar preču eksportēšanu galalietotājiem un preču galalietojumiem saistīti riski.

1. ATTIECĪGĀS TIESĪBU NORMAS, DEFINĪCIJAS UN GALVENIE JĒDZIENI

1.1. Attiecīgo tiesību normu pārskats

Regula ievieš jaunus noteikumus, kas īpaši paredz tādu regulas I pielikumā neminētu kibernovērošanas preču eksporta kontroli, kuras kopumā vai kādas to daļas ir vai varētu būt paredzētas lietošanai saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu. Attiecīgie apsvērumi un panti ir šādi:

a) 8. apsvērums: "Lai novērstu risku, ka personas, kuras ir līdzatbildīgas vai atbildīgas par cilvēktiesību vai starptautisko humanitāro tiesību smagu pārkāpumu vadīšanu vai izdarīšanu, varētu ļaunprātīgi izmantot konkrētas sarakstā neiekļautas kibernovērošanas preces, kas eksportētas no Savienības muitas teritorijas, ir lietderīgi veikt šādu preču eksporta kontroli. Saistītie riski jo īpaši attiecas uz gadījumiem, kad kibernovērošanas preces ir īpaši izstrādātas ar mērķi darīt iespējamu ielaušanos vai padziļinātu pakešu pārbaudi informācijas un telesakaru sistēmās, lai veiktu

([1]) Sk. īpaši kontroli, kas saistīta ar telesakaru pārtveršanas sistēmām (5A001.f), interneta uzraudzības sistēmām (5A001.j), ielaušanās programmatūru (4A005, 4D004 un saistītu kontroli 4E001.a un 4E001.c pozīcijā) un tiesībaizsardzības uzraudzības programmatūru (5D001.e). Bez tam sk. kontroli, kas saistīta ar konkrētiem kriminālistikas/izmeklēšanas rīkiem (5A004.b, 5D002.a.3.b un 5D002.c.3.b) un kur katru gadījumu novērtē atsevišķi.

([2]) Īpaši informācijas drošības sistēmas.

([3]) Sk. Padomes Regulu (EK) Nr. 765/2006 (2006. gada 18. maijs) par ierobežojošiem pasākumiem, ņemot vērā situāciju Baltkrievijā un Baltkrievijas iesaistīšanos Krievijas agresijā pret Ukrainu (OV L 134, 20.5.2006., 1. lpp., ELI: http://data.europa.eu/eli/reg/2006/765/oj); Padomes Regulu (ES) Nr. 359/2011 (2011. gada 12. aprīlis) par ierobežojošiem pasākumiem, kas vērsti pret konkrētām personām, vienībām un struktūrām saistībā ar situāciju Irānā (OV L 100, 14.4.2011., 1. lpp., ELI: http://data.europa.eu/eli/reg/2011/359/oj); Padomes Regulu (ES) Nr. 36/2012 (2012. gada 18. janvāris) par ierobežojošiem pasākumiem, ņemot vērā situāciju Sīrijā un ar ko atceļ Regulu (ES) Nr. 442/2011 (OV L 16, 19.1.2012., 1. lpp., ELI: http://data.europa.eu/eli/reg/2012/36/oj); Padomes Regulu (ES) Nr. 401/2013 (2013. gada 2. maijs) par ierobežojošiem pasākumiem, ņemot vērā situāciju Sīrijā un ar ko atceļ Regulu (EK) Nr. 194/2008 (OV L 121, 3.5.2013., 1. lpp., ELI: http://data.europa.eu/eli/reg/2013/401/oj), un Padomes Regulu (ES) 2017/2063 (2017. gada 13. novembris) par ierobežojošiem pasākumiem saistībā ar situāciju Venecuēlā (OV L 295, 14.11.2017., 21. lpp., ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

fizisku personu slepenu novērošanu, uzraugot, izgūstot, vācot vai analizējot minēto sistēmu datus, arī biometriskos datus. Preces, ko izmanto tikai komerciālos nolūkos, piemēram, rēķinu sagatavošanai, tirgvedībai, pakalpojumu kvalitātes, lietotāju gandarījuma vai tīkla drošības nodrošināšanai, parasti tiek uzskatītas par tādām, kas šādus riskus nerada.";

b) 9. apsvērums: "Lai stiprinātu sarakstā neiekļautu kibernovērošanas preču eksporta kontroles efektivitāti, ir svarīgi vēl vairāk saskaņot visaptverošas kontroles piemērošanu minētajā jomā. Šajā nolūkā dalībvalstis ir apņēmušās atbalstīt šādu kontroli, apmainoties ar informāciju savā starpā un ar Komisiju, jo īpaši attiecībā uz tehnoloģiju attīstību kibernovērošanas precēm, un modri uzraugot šādas kontroles piemērošanu, lai veicinātu apmaiņu Savienības līmenī.";

c) 2. panta 20. punkts, kur definēts, ka kibernovērošanas preces ir "divējāda lietojuma preces, kas īpaši izstrādātas, lai darītu iespējamu fizisku personu slepenu novērošanu, uzraugot, izgūstot, vācot vai analizējot informācijas un telesakaru sistēmu datus";

d) 5. pants ievieš prasību, kas nosaka, ka sarakstā neminētu kibernovērošanas preču eksportam ir vajadzīga atļauja, ja kompetentā iestāde ir informējusi eksportētāju par to, ka attiecīgās preces kopumā vai kādas to daļas ir vai varētu būt paredzētas lietošanai saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu (5. panta 1. punkts). Ja eksportētāji, vadoties pēc pienācīgā pārbaudē gūtiem secinājumiem, ir informēti, ka preces kopumā vai kādas to daļas ir paredzētas lietošanai saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu, tas turklāt prasa eksportētājiem to paziņot kompetentajai iestādei (5. panta 2. punkts). Minētā kompetentā iestāde pieņem lēmumu par to, vai uz attiecīgo eksportu jāattiecina prasība saņemt atļauju; un

e) 5. panta 2. punkts turklāt nosaka, ka "Komisija un Padome eksportētājiem dara pieejamas vadlīnijas, kā minēts 26. panta 1. punktā".

1.2. **Galvenās definīcijas**

Atsevišķos regulas apsvērumos un noteikumos skaidroti specifiski termini, kuri attiecas uz sarakstā neminētu kibernovērošanas preču kontroli un kuru skaidra izpratne ir svarīga, lai eksportētāji izpildītu pienācīgu pārbaudi un efektīvi īstenotu kontroli. Īpaši svarīgs ir 2. panta 20. punkts, kur "kibernovērošanas preces" precīzi definētas kā "divējāda lietojuma preces, kas īpaši izstrādātas, lai darītu iespējamu fizisku personu slepenu novērošanu, uzraugot, izgūstot, vācot vai analizējot informācijas un telesakaru sistēmu datus".

Šajās vadlīnijās precizējami konkrēti minētās definīcijas elementi.

1.2.1. *"Īpaši izstrādāts"*

Prece ir izstrādāta slepenai novērošanai, kad tās tehniskās iezīmes ir piemērotas fizisku personu slepenai novērošanai un to objektīvi dara iespējamu. Tāpēc termins "īpaši izstrādāts" nozīmē, ka produkta projektēšanas un izstrādes galvenais mērķis ir fizisku personu slepena novērošana. Tomēr tāds termins nenozīmē, ka fizisku personu slepena novērošana var būt vienīgais preces lietojums.

Regulas 8. apsvērumā paskaidrots – parasti tiek uzskatīts, ka preces, ko izmanto tikai komerciālos nolūkos, piemēram, rēķinu sagatavošanai, tirgvedībai, pakalpojumu kvalitātes, lietotāju gandarījuma vai tīkla drošības nodrošināšanai, nav īpaši izstrādātas slepenai novērošanai un tādējādi kibernovērošanas preču definīcijā neietilpst. Piemēram, lai arī nozares operētājsistēmu vai lietotāju datplūsmas novērošanai paredzētas preces var tikt izmantotas novērošanai, saskaņā ar definīciju šīs preces tomēr nav kibernovērošanas preces, jo tās nav īpaši izstrādātas fizisku personu slepenai novērošanai.

1.2.2. *"Slepena novērošana"*

Preces dara iespējamu slepenu novērošanu, īpaši ja slepenā novērošana skartajai fiziskajai personai nav acīmredzami nojaušama. Piemēram, kad skartās personas nenojauš kibernovērošanas preču atrašanos tuvumā un/vai darbību un tāpēc tām nav iespējas no novērošanas izvairīties vai vismaz attiecīgi pielāgoties. Pat ja novērošanu veic publiskajā telpā uzstādītas vai darbojošās preces, konkrētos gadījumos datu iegūšanu var uzskatīt par slepenai novērošanai būtisku, proti, savāktos datus var novirzīt, vērtēt vai apstrādāt citiem nolūkiem, ne tiem, par kuriem skartā fiziskā persona tikusi informēta. Citiem vārdiem sakot, kad fiziska persona nevar objektīvi paredzēt viņas novērošanu, novērošanu var uzskatīt par slēptu saskaņā ar regulas 2. panta 20. punktu.

1.2.3. *"Fiziskas personas"*

Termins "fiziska persona" attiecas uz dzīvu cilvēku, kas ir pretstatā juridiskai personai vai subjektam, uz kuriem noteikumi līdz ar to neattiecas. Termins neaptver priekšmetu, vietu vai iekārtu novērošanu.

1.2.4. *"Uzraudzīt, izgūt, vākt, analizēt datus"*

Skaidrojošajā un sinonīmu vārdnīcā "Tēzaurs" vārdiem "uzraudzīt", "izgūt", "vākt" un "analizēt" ir šāda nozīme:

— "uzraudzīt": 'skatīties'; 'vērot',

— "izgūt": 'izdabūt ārā', 'iegūt',

— "vākt": 'pārvietot', 'virzīt', 'novietot (vienkop)",

— "analizēt": 'pakļaut analīzei'; 'sīki, pamatīgi pētīt, raksturot'; 'izdarīt analīzi'.

Minētie termini nozīmē, ka novērošanai izmantotajām precēm jābūt ar precīzām tehniskām datu apstrādes spējām, kas ļauj uzraudzīt, vākt, izgūt vai analizēt datus, un tādas preces par piemēru ir:

a) preces, kuras izmanto, lai uzraudzītu informācijas un telesakaru sistēmu ([4]) datus (piemēram, tādā sistēmā pārraidīto datu datnes lielums vai pakešu datplūsma);

b) preces, kas izgūst informācijas un telesakaru sistēmu datus, veicot ielaušanos un izgūšanu (piemēram, ielaušanās programmatūra);

c) preces, kas dara iespējamu tādu datu analīzi, kuri izgūti no informācijas un telesakaru sistēmām, ieskaitot preces, kuras var apstrādāt minētajās sistēmās glabātos ar kameru iegūtus attēlus (piemēram, noteikta veida datu analīzes tehnoloģijas, ko izmanto sejas atpazīšanas sistēmās).

Preces, kuras ļauj uztvert sarunas, datu apmaiņu, kustības un individuālu uzvedību un kuras izmanto parastai informācijas sistēmu uzraudzībai vai sabiedrības locekļu vērošanai videonovērošanas kamerās, netiktu uzskatītas par regulā definētajām kibernovērošanas precēm, jo nav īpaši izstrādātas tādiem nolūkiem un darbojas ar citām tehnoloģijām, piemēram, mākslīgo intelektu vai lielo datu tehnoloģiju. Tomēr visa sistēma (kas darbojas kopā ar citām tehnoloģijām, piemēram, mākslīgo intelektu vai lielo datu tehnoloģijām) varētu būt kibernovērošanas prece saskaņā ar regulas 2. panta 20. punkta definīciju.

Ņemot vērā, ka 5. panta mērķis ir nodrošināt sarakstā neminēto preču efektīvu eksporta kontroli, jāuzsver, ka nedaudzie ilustratīviem nolūkiem sniegtie piemēri neierobežo kibernovērošanas preču definīciju un tvērumu.

([4]) Definīciju skatīt 1.2.5. punktā.

Definīcijā lietotais saiklis "vai" parāda, ka uzskaitītās tehniskās spējas uzskatāmas par alternatīvām un vienai precei nebūt nav jāpiemīt visām minētajām tehniskajām spējām, kas ļauj uzraudzīt, izgūt, vākt vai analizēt datus. Citiem vārdiem sakot, pietiek ar kādu no minētajām tehniskajām spējām, lai prece atbilstu kibernovērošanas preces definīcijai 2. panta 20. punktā.

1.2.5. *"Informācijas un telesakaru sistēmu" [dati]*

Minētais termins attiecas uz sistēmām, kas elektroniski apstrādā informāciju, piemēram, programmēšanu/kodēšanu, personālo datoru sistēmas (aparatūra) operācijas un cita informācijas vadība, ieskaitot programmatūras tehnoloģiju, tīmekļa tehnoloģiju, datortehnoloģiju, glabāšanas tehnoloģiju u. c., un uz dažām sistēmām, kas pārraida informāciju no attāluma, piemēram, tehniskām sistēmām, kas pārraida skaņas, signālus, tekstu, citas zīmes, attēlus gan vadu, gan bezvadu kanālos, izmantojot optiskās šķiedras, radiosakarus un citas elektromagnētiskās sistēmas. Abos minētajos jēdzienos kopā ietilpst plašs informācijas pārraides vai apstrādes sistēmu klāsts. Jāatzīmē, ka termins attiecas uz sistēmām, nevis iekārtām.

1.2.6. *"Informētība" un "ir paredzēts"*

Ievērojot regulas 5. panta 2. punktu, ja eksportētājs "ir informēts, ka kibernovērošanas preces [..] ir paredzētas [..] lietošanai saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu, eksportētājs to paziņo kompetentajai iestādei".

Termins "informēts" gan nav jauns juridisks jēdziens, bet tiek lietots galapatēriņa atļaujas prasību (tā sauktās "visaptverošās" kontroles) kontekstā saskaņā ar regulas 4., 6., 7. un 8. pantu. Būt "informētam" nozīmē, ka eksportētājam ir zināma informācija, kura apstiprina ļaunprātīga lietojuma nodomu. Tas vien, ka tāds risks ir iespējams, nav pietiekami, lai konstatētu informētību. Tomēr termins "informētība" nav pielīdzināms pasivitātei: eksportētājam ir jārīkojas, lai iegūtu pietiekamas un adekvātas zināšanas ar eksportu saistītu risku novērtēšanai un panāktu atbilstību regulai.

Norāde, ka precēm jābūt "paredzētām" attiecīgam paaugstināta riska galalietojumam, nozīmē, ka eksportētājam būtu jānovērtē galalietojums, skatot katru gadījumu atsevišķi un ņemot vērā konkrētā gadījuma specifiskos apstākļus. Turpretī teorētisks, proti, uz gadījuma faktu novērtējumu nebalstīts, risks, ka ar preču lietojumu var tikt pārkāptas cilvēktiesības, nebūtu pietiekams, lai liktu domāt, ka preces "ir paredzētas" konkrētam ļaunprātīgam lietojumam saskaņā ar 5. pantu.

1.3. **Iekšējās represijas, cilvēktiesību un starptautisko humanitāro tiesību nopietni pārkāpumi**

Ievērojot regulas 15. pantu, kur izklāstīti atļaujas novērtēšanas apsvērumi, dalībvalstīm ir jāņem vērā visi attiecīgie apsvērumi, ieskaitot tos, uz kuriem attiecas Padomes Kopējā nostāja 2008/944/KĀDP ([5]).

Regulas 5. pants paplašina kontroli, to attiecinot uz sarakstā neminētu kibernovērošanas preču eksportu, ņemot vērā risku, ka tās var tikt izmantotas saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu. Šajā jautājumā lietderīgi norādījumi atrodami Kopējā nostājā 2008/944/KĀDP un norādījumos par šo kopējo nostāju ([6]).

([5]) Padomes 2008. gada 8. decembra Kopējā nostāja 2008/944/KĀDP, ar ko izveido kopīgus noteikumus, kas reglamentē militāru tehnoloģiju un ekipējuma eksporta kontroli (OV L 335, 13.12.2008., 99. lpp., ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Sk. Norādījumus par Padomes Kopējo nostāju 2008/944/KĀDP, ar ko izveido kopīgus noteikumus, kas reglamentē militāru tehnoloģiju un ekipējuma eksporta kontroli (https://www.consilium.europa.eu/media/40659/st12189-en19.pdf).

1.3.1. *Iekšējas represijas*

Kopējās nostājas 2008/944/KĀDP 2. panta 2. punkts: "Iekšējas represijas, *inter alia*, ir arī spīdzināšana un citi nežēlīgas, necilvēcīgas vai pazemojošas attieksmes vai sodīšanas veidi, nāvessodi bez tiesas sprieduma vai patvaļīgi nāvessodi, cilvēku pazušanas gadījumi, patvaļīga aizturēšana un citi smagi cilvēktiesību un pamatbrīvību pārkāpumi, kā norādīts attiecīgos starptautiskos cilvēktiesību instrumentos, tostarp Vispārējā cilvēktiesību deklarācijā un Starptautiskajā paktā par pilsoniskajām un politiskajām tiesībām" *(ICCPR)*. Norādījumi par Kopējo nostāju 2008/944/KĀDP skaidro, kādi elementi, ieskaitot "paredzētā īstā lietotāja [galalietotāja], kā arī saņēmējas valsts reputāciju un pagātni no cilvēktiesību ievērošanas viedokļa", ņemami vērā eksportētāja novērtējumā.

1.3.2. *Cilvēktiesību nopietnu pārkāpumu izdarīšana*

Sarakstā neminētu kibernovērošanas preču ļaunprātīga izmantošana var negatīvi ietekmēt daudzas cilvēktiesību normas un tieši aizskart tiesības uz privātumu un datu aizsardzību. Patvaļīga vai nelikumīga novērošana var pārkāpt arī citas cilvēktiesības, piemēram, tiesības uz vārda, biedrošanās un pulcēšanās brīvību, domu, pārliecības un ticības brīvību, kā arī tiesības uz vienlīdzīgu attieksmi vai diskriminācijas aizliegumu un tiesības uz brīvām, vienlīdzīgām un aizklātām vēlēšanām. Konkrētos gadījumos fizisku personu, piemēram, cilvēktiesību aizstāvju, aktīvistu, politiķu, neaizsargātu iedzīvotāju grupu un žurnālistu, novērošana, kā arī uzraudzība vai to informācijas vākšana var izraisīt iebiedēšanu, apspiešanu, patvaļīgu aizturēšanu, spīdzināšanu vai pat sodīšanu ar nāvi bez tiesas sprieduma. Tādēļ eksportētājiem savos novērtējumos būtu jāiekļauj minētie ar nopietniem cilvēktiesību pārkāpumiem saistītie elementi.

Starptautiskā prakse liecina, ka visiem cilvēktiesību ierobežojumiem jābūt "samērīgiem" un jāatbilst starptautiskajiem cilvēktiesību standartiem. Praksē tas nozīmē, ka pastāv adekvātas garantijas, lai nodrošinātu, ka ierobežojumi ir noteikti tiesību aktos un tiek saglabāta tiesību būtība. Ievērojot proporcionalitātes principu, ierobežojumus var noteikt tikai tad, ja tie ir vajadzīgi un tik tiešām kalpo likumīgam mērķim, piemēram, valsts vai sabiedrības drošībai, sabiedriskajai kārtībai, sabiedrības veselības aizsardzībai vai citu personu tiesību un brīvību aizsardzībai.

Kibernovērošanas precēs var ietilpt likumīgi un reglamentēti rīki tiesībaizsardzības pielietojumiem, piemēram, noziedzīgu nodarījumu novēršanai, izmeklēšanai, atklāšanai vai saukšanai pie atbildības par tiem, arī terorisma apkarošanas jomā, vai kriminālsodu izpildei. Tajā pašā laikā kibernovērošanas preces, tās eksportējot uz represīviem režīmiem vai privātiem galalietotājiem un/vai uz konfliktu zonām, var tikt lietotas arī ļaunprātīgi, lai izdarītu cilvēktiesību un starptautisko humanitāro tiesību nopietnus pārkāpumus.

Tādēļ ir jāizvērtē katra atsevišķā gadījuma apstākļi, kā arī jāpiemēro attiecīgi noteikumi, ņemot vērā visus kompetento struktūru, piemēram, Apvienoto Nāciju Organizācijas, Savienības vai Eiropas Padomes, sniegtos ziņojumus par nopietniem cilvēktiesību pārkāpumiem. Minēto pārkāpumu atzīšana Apvienoto Nāciju Organizācijas kompetento struktūru, Savienības vai Eiropas Padomes publiskotā informācijā var palīdzēt nonākt pie secinājuma par cilvēktiesību pārkāpumu "nopietnību". Tāds skaidrs minēto struktūru sniegts atzinums gan nav obligāts, taču ir būtisks faktors, lai kritēriji tiktu izpildīti.

Saskaņā ar 5. panta noteikumiem cilvēktiesību pārkāpumam jābūt "nopietnam". Norādījumos par Kopējo nostāju 2008/944/KĀDP atrodama lietderīga informācija, kad klasificēt iespējamu cilvēktiesību pārkāpumu par "smagu". No minētajiem norādījumiem izriet, ka galvenā nozīme ir pārkāpuma raksturam un sekām. Sistemātiski un/vai plaša mēroga cilvēktiesību pārkāpumi regulāri tiek uzskatīti par nopietniem; bet pret skartajām personām izdarītā pārkāpuma smaguma dēļ par "nopietniem" var uzskatīt arī tādus pārkāpumus, kas nav sistemātiski vai plaša mēroga.

II pielikumā Norādījumiem par Kopējo nostāju 2008/944/KĀDP ir iekļauts neizsmeļošs saraksts ar galvenajiem starptautiskajiem un reģionālajiem cilvēktiesību instrumentiem, to skaitā Starptautiskais pakts par pilsoniskajām un politiskajām tiesībām ("*ICCPR*"), Konvencija pret spīdzināšanu un citu nežēlīgu, necilvēcīgu vai pazemojošu rīcību vai sodīšanu, Eiropas Cilvēktiesību konvencija ("Konvencija") un Pamattiesību harta ("Harta"), un tas var sniegt svarīgu informāciju, kā rūpīgu cilvēktiesību novērtējumu vajadzībām interpretēt un piemērot kritērijus. Minētajos instrumentos un to attiecīgajos papildprotokolos ir norādītas galvenās starptautiskās normas un standarti cilvēktiesību un pamatbrīvību jomā.

1.3.3. *Starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšana*

Starptautiskās humanitārās tiesības (sauktas arī par "Ženēvas tiesībām" vai "Bruņotu konfliktu tiesībām") ir izstrādātas no virknes starptautisku līgumu, īpaši Hāgas noteikumiem, Ženēvas konvencijām un to diviem 1977. gada papildprotokoliem, un nosaka noteikumus, kuri bruņotu konfliktu laikā tiecas aizsargāt cilvēkus, kas nepiedalās vai vairs nepiedalās karadarbībā (piemēram, civiliedzīvotājus un ievainotus, slimus vai sagūstītus kaujiniekus), un kuri nosaka karojošajām pusēm ierobežojumus attiecībā uz karadarbības līdzekļiem un metodēm ("Hāgas tiesības").

Kad sarakstā neminētas kibernovērošanas preces bruņota konflikta kontekstā tiek lietotas kā karadarbības līdzekļi un karadarbības metožu vajadzībām, to lietojumam būtu jāatbilst starptautiskajām humanitārajām tiesībām. Tādos apstākļos starptautisko humanitāro tiesību nopietnu pārkāpumu risks ir jāņem vērā saskaņā ar regulu, un tas, tāpat kā cilvēktiesību nopietnu pārkāpumu izdarīšana, būtu jānovērtē, ņemot vērā preču paredzēto galalietojumu konkrētajā gadījumā. Norādījumi par Kopējo nostāju 2008/944/KĀDP sniedz informāciju par apsveramiem elementiem, to skaitā par to, vai saņēmējs iepriekš ir ievērojis un pašreiz ievēro starptautiskās humanitārās tiesības, saņēmēja iecerēm, kas izteiktas oficiālās saistībās un par saņēmēja spēju nodrošināt, lai nodoto ekipējumu vai tehnoloģiju izmanto saskaņā ar starptautiskajām humanitārajām tiesībām un nenovirza vai nenodod citiem galamērķiem, kur to varētu izmantot, lai izdarītu nopietnus minēto tiesību pārkāpumus.

Ievērojot 5. pantu, starptautisko humanitāro tiesību pārkāpumam jābūt "nopietnam". Informācija atrodama Norādījumos par Kopējo nostāju 2008/944/KĀDP, kur atzīts, ka "atsevišķi starptautisko humanitāro tiesību pārkāpumu gadījumi ne vienmēr liecina par saņēmējas valsts attieksmi pret starptautiskajām humanitārajām tiesībām", lai gan "pamatots iemesls nopietnām bažām ir, ja atklājas zināmas pārkāpumu izdarīšanas tendences vai tas, ka saņēmēja valsts nav veikusi pietiekamus pasākumus, lai sodītu par pārkāpumiem". Starptautiskā Sarkanā Krusta komiteja ("SSKK") ir sniegusi vadlīnijas par starptautisko humanitāro tiesību pārkāpumu novērtēšanu eksporta kontroles nolūkos. SSKK uzskata, ka "starptautisko humanitāro tiesību pārkāpumi ir nopietni, ja tie apdraud aizsargājamās personas (piemēram, civiliedzīvotājus, karagūstekņus, ievainotos un slimos) vai objektus (piemēram, civilos objektus vai infrastruktūru) vai ja tie iznīcina svarīgas universālās vērtības". Piemēram, kara noziegumi ir starptautisko humanitāro tiesību nopietni pārkāpumi. SSKK pie tam min Norādījumos par Kopējo nostāju 2008/944/KĀDP sniegtajiem līdzīgus faktorus, to skaitā oficiālas saistības piemērot starptautisko humanitāro tiesību noteikumus, atbilstīgus pasākumus, kuri nodrošina atbildību par starptautisko humanitāro tiesību pārkāpumiem, militārajiem spēkiem izstrādātu mācību kursu par starptautiskajām humanitārajām tiesībām un aizliegumu vervēt bērnus bruņotajos spēkos.

2. **TEHNISKAIS TVĒRUMS**

2.1. **Sarakstā iekļautas kibernovērošanas preces**

Lai palīdzētu eksportētājiem apzināt sarakstā neminētas potenciālas kibernovērošanas preces, šo vadlīniju papildinājumā sniegta informācija par regulas I pielikumā iekļautajām kibernovērošanas precēm.

2.2. **Sarakstā neminētas potenciālas kibernovērošanas preces**

Lai gan pēc definīcijas nav iespējams izveidot sarakstu ar pilnīgi visiem produktiem, kurus drīkst kontrolēt kā "sarakstā neminētas preces" saskaņā ar 5. pantu, tālāk minētās preces var tikt izmantotas novērošanai un atbilstoši regulai var būt pamatota īpaša modrība.

Regulas 8. apsvērumā paskaidrots – parasti tiek uzskatīts, ka preces, ko izmanto tikai komerciālos nolūkos, piemēram, rēķinu sagatavošanai, tirgvedībai, pakalpojumu kvalitātes, lietotāju gandarījuma vai tīkla drošības nodrošināšanai, nerada ļaunprātīgas lietošanas riskus, kuri kā nopietni pārkāpumi ir būtiski cilvēktiesību un starptautisko humanitāro tiesību izpratnē, un tāpēc parasti uz tām neattiecas kontrole saskaņā ar 5. pantu. Daudzām no minētajām precēm ir informācijas drošības (kriptogrāfijas vai pat kriptoanalīzes) funkcionalitāte, kas atbilst kontroles parametriem, kuri minēti regulas I pielikuma kontroles apraksta 5. kategorijas 2. daļā. "Kibernovērošanas preču" definīcijā neietilpst arī drošības tīkla aprīkojums, ieskaitot maršrutētājus, slēdžus vai relejus, gadījumos kad "informācijas drošības" funkcionalitāte ietver tikai "ekspluatācijas, administrēšanas, uzturēšanas" uzdevumus un ar tiem tiek ievēroti tikai publicēti vai komerciāli kriptogrāfijas standarti, tomēr eksportētājiem būtu jāsaglabā modrība, ņemot vērā dažādus ziņojumus par šādu priekšmetu ļaunprātīgu izmantošanu cilvēktiesību pārkāpumos.

2.2.1. *Sejas un emociju atpazīšanas tehnoloģija*

Vēl bez kibernovērošanas sejas un emociju atpazīšanas tehnoloģijām ir daudzi citi lietojumi, piemēram, identifikācija vai autentifikācija, un definīcija uz tām neattiektos automātiski. Tomēr zināmos apstākļos sejas un emociju atpazīšanas tehnoloģijas var ietilpt regulas 2. panta 20. punkta tvērumā.

Tā kibernovērošanas preces definīcijas tvērumā varētu ietilpt sejas un emociju atpazīšanas tehnoloģijas, kas var tikt izmantotas glabātu videoattēlu pārraudzībai vai analīzei. Tomēr arī tad, ja izpildīti iepriekš minētie kritēriji, rūpīgi jāpārbauda, vai programmatūra īpaši izstrādāta slepenai novērošanai.

2.2.2. *Līdzsekošanas ierīces*

Līdzsekošanas ierīces ļauj sekot līdzi ierīces fiziskajai atrašanās vietai laika gaitā, un tiesībaizsardzības iestādes un izlūkdienesti jau kādu laiku izmanto dažas līdzsekošanas tehnoloģijas. Līdzsekošanas tehnoloģijām kļūstot progresīvākām un izplatoties tādām "līdzsekošanas ierīcēm" kā, piemēram, viedtālruņi un citas elektroniskās ierīces (piemēram, transportlīdzekļos iebūvētas sistēmas), ievērojami ir audzis to potenciāls mērķētai un plaša mēroga novērošanai, arī atrašanās vietas meklēšanai ar satelītiem, mobilo sakaru torņiem, *Wi-Fi* un *Bluetooth* raiduztvērējiem.

Piemēram, tiesībaizsardzības iestādes un izlūkdienesti izmanto līdzsekošanas ierīces, lai izmeklēšanas gaitā vāktu pierādījumus vai izsekotu aizdomās turētos, tāpat arī uzņēmumi tās izmanto komerciālos nolūkos, piemēram, pārskatam par kopējiem pārvietošanās modeļiem iepirkšanās ielās, ārpus darbavietas strādājošu darbinieku izsekošanai vai reklāmai pēc atrašanās vietas.

2.2.3. *Videonovērošanas sistēmas*

Lai palīdzētu eksportētājiem identificēt potenciālu kibernovērošanu, ir lietderīgi precizēt arī to, uz kurām precēm definīcija neattiektos. Šajā ziņā kibernovērošanas preču definīcija neattiecas, piemēram, uz videonovērošanas sistēmām un kamerām, to skaitā augstas izšķirtspējas kamerām, kuras izmanto personu filmēšanai publiskās vietās, jo tās neuzrauga un nevāc datus no informācijas un telesakaru sistēmām.

3. **PIENĀCĪGAS RŪPĪBAS PASĀKUMI**

Saskaņā ar regulas 7. apsvērumu "eksportētāju [..] ieguldījums, lai īstenotu vispārējo tirdzniecības kontroles mērķi, ir ļoti svarīgs. Lai šīs personas varētu rīkoties saskaņā ar šo regulu, jāveic ar darījumiem, uz kuriem attiecas šī regula, saistītu risku novērtējums, kā to paredz iekšējās atbilstības programma (IAP) un kas īstenojams, veicot darījumu izvērtēšanas pasākumus, ko dēvē arī par pienācīgas rūpības principu".

2. panta 21. punktā definēts, ka iekšējās atbilstības programma ("IAP") ir "pastāvīgi efektīvi, piemēroti un samērīgi politikas pasākumi un procedūras, ko eksportētāji pieņēmuši, lai veicinātu atbilstību šīs regulas noteikumiem un mērķiem un tādu atļauju noteikumiem, kuras īstenotas saskaņā ar šo regulu, cita starpā pienācīgas rūpības pasākumi, ar ko novērtē ar preču eksportēšanu galalietotājiem un preču galalietojumiem saistītos riskus".

Komisijas Ieteikums (ES) 2019/1318 ([7]) ir pamats, kas palīdz eksportētājiem apzināt, pārvaldīt un mazināt riskus, kas saistīti ar divējāda lietojuma preču kontroli, un nodrošināt atbilstību attiecīgajiem ES un valstu normatīvajiem aktiem.

Minētās vadlīnijas var palīdzēt eksportētājiem īstenot iekšējās atbilstības programmā paredzētos darījumu izvērtēšanas pasākumus (ko dēvē arī par pienācīgas rūpības principu).

Sarakstā neminētu kibernovērošanas preču eksportētāji saskaņā ar Regulas (ES) 2021/821 5. panta 2. punktu ievēro pienācīgu rūpīgu, īstenojot darījumu izvērtēšanas pasākumus, proti, sper soļus attiecībā uz preču klasifikāciju un darījuma riska novērtējumu. Faktiski eksportētāji tiek mudināti veikt turpmāk minēto.

([7]) Komisijas Ieteikums (ES) 2019/1318 (2019. gada 30. jūlijs) par iekšējās atbilstības programmām divējāda lietojuma preču tirdzniecības kontrolei saskaņā ar Regulu (EK) Nr. 428/2009 (OV L 205, 5.8.2019., 15. lpp., ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Pārbaudīt, vai sarakstā neminētā prece varētu būt "divējāda lietojuma prece", proti, īpaši izstrādāta, lai darītu iespējamu fizisku personu slepenu novērošanu, uzraugot, izgūstot, vācot vai analizējot informācijas un telesakaru sistēmu datus.**

Šis solis attiecas uz preces veida noteikšanu saskaņā ar noteikumiem, kurus piemēro kibernovērošanas precēm. Noteikšanā ietilpst preces tehnisko raksturlielumu pārbaude, uzskaitīto preču gadījumā – pamatojoties uz regulas I pielikumā izklāstītajiem tehniskajiem parametriem, bet sarakstā neminēto preču gadījumā – ņemot vērā kibernovērošanas preču definīcijā lietotos īpašos terminus un jēdzienus, un pēcāka preces (preču, tehnoloģijas vai programmatūras) klasifikācija.

3.2. **Pārbaudīt, vai attiecīgajai precei ir spējas, kuras ārvalstu galalietotāji varētu ļaunprātīgi izmantot saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietniem pārkāpumiem.**

Eksportētājiem būtu jānovērtē, vai produkts var tikt ļaunprātīgi izmantots, lai veiktu iekšējas represijas, pārkāptu vai ļaunprātīgi izmantotu cilvēktiesības, tai skaitā tiesības uz dzīvību, tiesības būt pasargātam no spīdzināšanas, necilvēcīgas un pazemojošas attieksmes, tiesības uz privātumu, tiesības uz runas brīvību, tiesības uz biedrošanās un pulcēšanās brīvību, tiesības uz domu, pārliecības un ticības brīvību, kā arī tiesības uz vienlīdzīgu attieksmi vai diskriminācijas aizliegumu un tiesības uz brīvām, vienlīdzīgām un aizklātām vēlēšanām.

Tāpat jānovērtē, vai produkts var tikt izmantots kā sistēmas daļa vai komponents, izraisot tos pašus pārkāpumus un/vai ļaunprātīgu izmantošanu.

Eksportētājiem novērtējumā būtu jāizmanto tā dēvētie brīdinājuma signāli, kas norāda uz jebkādiem neierastiem darījuma apstākļiem, kuri liecina, ka eksports var būt paredzēts nepiemērotam galapatēriņam, galalietotājam vai galamērķim.

Brīdinājuma signāli:

a) tirgotajai precei pievienota informācija par tās potenciālu lietojumu slepenai novērošanai;

b) informācija par līdzīgas preces ļaunprātīgu izmantošanu saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietniem pārkāpumiem (sk. 1.3. iedaļu);

c) informācija par preces ļaunprātīgu izmantošanu novērošanas darbībās, kas vērstas pret dalībvalsti vai saistītas ar ES pilsoņa nelikumīgu novērošanu;

d) informācija, kas norāda, ka darījums aptver priekšmetus, kas var tikt izmantoti tādas sistēmas izveidei, pielāgošanai vai konfigurācijai, par kuru zināma tās ļaunprātīga izmantošana saistībā ar iekšējām represijām un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu izdarīšanu (sk. 1.3. iedaļu);

e) konstatēts, ka prece vai līdzīga prece ir minēta sarakstā, kas saskaņā ar regulas 5. panta 6. punktu publicēts *Eiropas Savienības Oficiālā Vēstneša* C sērijā.

3.3. **Lai atbalstītu kompetentās iestādes, pārbaudīt darījumā iesaistītās ieinteresētās personas (ieskaitot galalietotājus un saņēmējus, piemēram, izplatītājus un tālākpārdevējus).**

Eksportētājiem, atbalstot kompetentās iestādes, cik vien iespējams, būtu:

a) pirms darījuma un tā laikā, pamatojoties uz galapatēriņa deklarācijām, jāpārbauda, kā saņēmēji un/vai galalietotāji ir nodomājuši izmantot produktu vai pakalpojumu;

b) jāgūst priekšstats par attiecīgajā preču galamērķī esošo situāciju, īpaši cilvēktiesību vispārējo stāvokli, jo tas ir svarīgs cilvēktiesību un starptautisko humanitāro tiesību nopietnu pārkāpumu risku rādītājs saistībā ar eksportu;

c) pamatojoties uz tālāk uzskaitītajiem brīdinājuma signāliem, jāpārbauda, vai pastāv riski produktam vai pakalpojumam tikt novirzītam citam neatļautam galalietotājam.

Brīdinājuma signāli:

a) galalietotājam ir acīmredzama saistība ar ārvalstu valdību, kas ir veikusi iekšējas represijas un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnus pārkāpumus;

b) galalietotājs strukturāli ietilpst bruņotajos spēkos vai citā grupējumā, kas iepriekš bijis iesaistīts bruņotā konfliktā, kas ietver iekšējas represijas un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnus pārkāpumus;

c) galalietotājs agrāk ir eksportējis kibernovērošanas preces uz valstīm, kurās šādu preču lietošana ir izraisījusi iekšējas represijas un/vai cilvēktiesību un starptautisko humanitāro tiesību nopietnus pārkāpumus.

3.4. **Balstoties uz pienācīgā pārbaudē gūtiem secinājumiem, izstrādāt plānu, kā novērst potenciālu nelabvēlīgu ietekmi un to mazināt nākotnē.**

Eksportētājiem uz pienācīgā pārbaudē gūtu secinājumu pamata būtu jāpārtrauc darbības, kas izraisa vai veicina nelabvēlīgu ietekmi saistībā ar cilvēktiesībām, kā arī būtu jāizstrādā un jāīsteno korektīvo pasākumu plāns. Iespējamie pasākumi ir šādi:

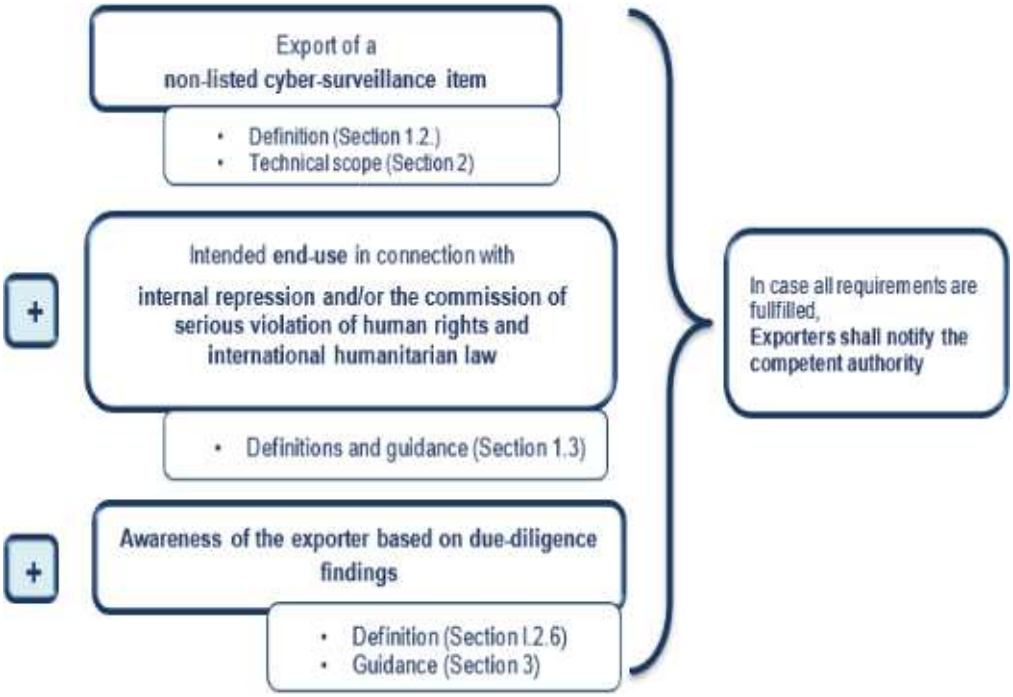
a) atjaunināt uzņēmuma stratēģiju, lai sniegtu norādījumus, kā nākotnē izvairīties no nelabvēlīgās ietekmes, novērst to un gādāt par stratēģijas īstenošanu;

b) balstoties uz riska novērtējuma konstatējumiem, atjaunināt un stiprināt vadības sistēmas, lai, iekams rodas nelabvēlīga ietekme, tiktu labāk izsekota informācija un brīdinātu par riskiem;

c) vākt informāciju, lai izprastu augsta līmeņa nelabvēlīgas ietekmes riskus, kas saistīti ar sektoru;

d) darīt zināmus dalībvalstu kompetentajām iestādēm pienācīgā pārbaudē gūtos konstatējumus, lai atvieglotu informācijas plūsmu attiecībā uz konkrētām precēm, galalietotājiem un galamērķiem.

Regulas (ES) 2021/821 5. panta 2. punkta prasības



4. **PAPILDINĀJUMS**

Sarakstā iekļautas kibernovērošanas preces, kas tiek kontrolētas saskaņā ar Regulas (ES) 2021/821 I pielikumu

— **Telesakaru pārtveršanas sistēmas (5A001.f)**

Lielākajā daļā valstu, to skaitā dalībvalstu, saziņas konfidencialitāti aizsargā likums, bet saskaņā ar tiesisko regulējumu var atļaut valdības iestāžu veiktu komunikācijas slepenu elektronisko novērošanu(t. s. likumīga datu pārtveršana (*LI*)). Tomēr digitālais laikmets radījis iespēju plaši izmantot noklausīšanās tehnoloģijas. To, ka noklausīšanās rīkus iespējams izmantot plašā mērogā, parādīja Lībijas režīms, kurš izmantoja minētās tehnoloģijas, un tādējādi 2012. gadā paātrināti tika ieviesta telesakaru pārtveršanas sistēmu eksporta kontrole.

Šāda kontrole tiek attiecināta uz aprīkojumu, kas izstrādāts saziņas (balss vai datu) satura, kā arī abonentu identifikatoru vai citu, izmantojot bezvadu savienojumu sakarus, pa gaisu pārraidītu metadatu izgūšanai, un radiofrekvenču uzraudzības iekārtām. Tā attiecas uz, piemēram, *IMSI* (starptautiskā mobilo sakaru abonenta identitāte) uztvērējiem, kas pārtver mobilo tālruņu datplūsmu un izseko mobilo tālruņu lietotāju pārvietošanos, vai iekārtām, kas izveido neīstus *Wi-Fi* tīklājus *IMSI* numuru izgūšanai no tālruņa, kā arī konkrētiem preču veidiem, kas īpaši izstrādāti, lai telesakaru sistēmās liktu veikt "padziļinātu pakešu pārbaudi". Tā kā mobilo telesakaru traucētājiekārtas nevāc datus, tās neietilpst kibernovērošanas preču tvērumā.

Tādas sistēmas var izveidot ar vispārējas nozīmes tehnoloģiju, taču tas, vai tādām sistēmām būs plaša mēroga pārtveršanas spējas, būs atkarīgs no konkrētām daļām un komponentiem, to skaitā, piemēram, konkrētām programmatūrām, modernām vai konkrētam pielietojumam paredzētām integrālshēmām (piem., *FPGA*, *ASIC* utt.), kas palielina sekundē apstrādājamu pakešu vai komunikācijas sesiju skaitu.

— **Interneta uzraudzības sistēmas (5A001.j)**

Lai gan nu ir parasts pēc noklusējuma šifrēt uz interneta bāzētu komunikāciju, vēl aizvien var tikt pārtverti komunikācijas datplūsmas dati (metadati), piemēram, IP adreses, datu apmaiņas biežums un datu apmaiņas lielums nolūkā identificēt saikni starp personām un domēnu nosaukumiem. Valdības var izmantot minētās sistēmas likumīgiem mērķiem, piemēram, tādu personu identificēšanai, kuras apmeklē domēnus, kas saistīti ar noziedzīgu vai teroristisku saturu. Tomēr interneta datplūsmas uzraudzība un analīze pēc etniskām, reliģiskām, politiskām vai sociālām pazīmēm var izraisīt cilvēku un sabiedrības visaptverošu kartēšanu valstī iedzīvotāju kontroles un represiju nolūkiem, kā arī citiem mērķiem, piemēram, politisko disidentu identificēšanai. Minētās preces, kuras raisa arī ar cilvēktiesībām un iekšējām represijām saistītus jautājumus, var arī palīdzēt stiprināt drošības un militārās spējas.

Kontrole, kas tiek attiecināta uz 5A001.j pozīciju, attiecas uz interneta kontroles sistēmām, kas darbojas "nesējklases IP tīklā (piemēram, valsts mēroga IP pamats)", lai analizētu, izgūtu un indeksētu pārraidīto metadatu saturu (balss, video, ziņojumi, pielikumi) atbilstīgi "konkrētām pazīmēm" un kartētu personu attiecību tīklu. Ar minētajām precēm veiktā novērošana ir "slepena" tāpēc, ka novērotās personas nav informētas par komunikācijas pārtveršanu. Turpretim kontrole nav vērsta uz sistēmām, kurās notiek lietotāja vai abonenta darbība vai mijiedarbība, piemēram, uz sociālajiem tīkliem vai komerciālām meklētājprogrammām. Turklāt kontrole attiecas uz sistēmām, kas apstrādā no interneta sniedzēja pamattīkla ņemtus datus, bet neattiecas uz sociālajiem tīkliem vai komerciālām meklētājprogrammām, kas apstrādā lietotāju sniegtus datus.

— **"Ielaušanās programmatūra" (4A005, 4D004 un saistīta kontrole atbilstoši 4E001.a un 4E001.c pozīcijai)**

Ar ielaušanās programmatūras palīdzību operators var attālināti slepeni piekļūt elektroniskai ierīcei, piemēram, viedtālrunim, klēpjdatoram, serverim vai lietu interneta ierīcei, iegūt ierīcē glabātus datus, noklausīties ar ierīcē iebūvētu vai ar to savienotu mikrofonu un izmantot ierīci par līdzekli uzbrukumiem iekārtām, ar kurām ierīce savienojas, vai pret lietotāja kontaktiem ("uzlaušana, izmantojot trešās personas ierīces"). Lai gan ielaušanās programmatūrai ir likumīgi lietojumi ([8]), piemēram, IT nodaļas izmanto tālpiekļuves programmatūru attālinātam atbalstam, novērošanas slepenais raksturs un potenciāli savāktās informācijas apjoms rada augstu risku, ka tiks pārkāptas tiesības uz privātumu un personas datu aizsardzību, un var nopietni apdraudēt tiesības uz vārda brīvību.

([8]) Skaidrības labad jānorāda, ka sarakstā iekļautajām kibernovērošanas precēm, kas tiek kontrolētas saskaņā ar Divējāda lietojuma preču regulas I pielikumu, būtu vajadzīga atļauja to eksportam uz trešām valstīm neatkarīgi no tā, vai preces lietojums ir likumīgs.

Kontrole, kas minēta 4A005. pozīcijā un citviet, attiecas uz programmatūru, kā arī sistēmām, iekārtām, komponentiem un saistītu tehnoloģiju, kas speciāli izstrādāta vai pārveidota "ielaušanās programmatūras" izstrādāšanai, vadībai un kontrolei vai piegādei, bet neattiecas uz pašu "ielaušanās programmatūru", kā tā definēta regulas I pielikumā. Minētie kiberrīki tiek kontrolēti, ņemot vērā iespējamos traucējumus un kaitējumu, ko tie var radīt pie sekmīgas izmantošanas un izpildes, bet nav paredzēts, ka kontrole skar, piemēram, kiberdrošības pētnieku un nozares darbību, jo tiem jādalās informācijā, kas saistīta ar ielaušanās programmatūru, lai varētu izstrādāt produktu defektu labojumus un tos instalēt, iekams ievainojamība kļūst publiski zināma.

— **Komunikācijas uzraudzības programmatūra (5D001.e)**

Šī programmatūra ir paredzēta, lai pilnvarotas tiesībaizsardzības iestādes uzraudzītu un analizētu datus, kas tiek vākti pārtveršanas pasākumos, kuri tiek prasīti no sakaru pakalpojumu sniedzēja. Ar programmatūru iespējama meklēšana atbilstīgi "konkrētai pazīmei" komunikācijas saturā vai metadatos, izmantojot likumīgas pārtveršanas saskarni un kartējot cilvēku attiecību tīklu vai izsekojot mērķpersonu pārvietošanos, pamatojoties uz meklēšanas rezultātiem. Programmatūra ir paredzēta "slepenai novērošanai", jo izmanto komunikācijas pārtveršanā vāktus datus, skartajām personām par to neesot informētām. Turklāt tā "analizē" datus, kas vākti "telesakaru sistēmās". Programmatūra ir instalēta valdības iestādē (piemēram, tiesībaizsardzības uzraudzības objektā (*law enforcement monitoring facility* ("*LEMF*")), un kontrole neattiecas uz likumīgas datu pārtveršanas ("LI") atbilstības sistēmām (piemēram, LI pārvaldības sistēmām un starpniecības ierīcēm), kuras ir komerciāli izstrādātas un instalētas sakaru pakalpojumu sniedzēja telpā (piemēram, integrētas sakaru tīklā) un kuras pakalpojumu sniedzējs izmanto un uztur. Kā precizēts kontroles aprakstā, kontroli neattiecina uz "programmatūru", kas speciāli izstrādāta vai pielāgota tikai komerciāliem mērķiem, piemēram, rēķinu sagatavošanai, tīkla pakalpojumu kvalitātei (*QoS*), pieredzes kvalitātei (*QoE*), starpniecības ierīcēm vai mobilajiem maksājumiem vai bankas darbībām.

— **Preces, ko izmanto kriptoanalīzei (5A004.a)**

Šī kontrole tiek attiecināta uz precēm, kas ir izstrādātas tam, lai neitralizētu kriptogrāfijas mehānismus nolūkā iegūt konfidenciālus mainīgos lielumus vai sensitīvus datus, tostarp lasāmu tekstu, paroles un kriptogrāfijas kodu atslēgas. Kriptogrāfiju izmanto, lai nodrošinātu informācijas konfidencialitāti informācijas sūtīšanas un pārējā laikā. Kriptoanalīze tiek izmantota konfidencialitātes neitralizēšanai, un tādējādi šī tehnoloģija "iespējo" slepenu novērošanu, uzraugot, izgūstot, vācot vai analizējot informācijas un telesakaru sistēmu datus.

— **Kriminālistikas/izmeklēšanas rīki (5A004.b, 5D002.a.3.b un 5D002.c.3.b)**

Kriminālistikas/izmeklēšanas rīki ir izstrādāti neapstrādātu datu izgūšanai no ierīces (piemēram, skaitļošanas vai saziņas) tā, ka dati netiek grozīti vai sabojāti un tos var izmantot tiesiskiem nolūkiem, t. i., kriminālizmeklēšanā vai tiesā. Lai no ierīces izgūtu neapstrādātus datus, minētie produkti apiet ierīces "autentifikācijas" vai autorizācijas kontroli. Ne tikai valdība un tiesībaizsardzības iestādes, bet arī bruņotie spēki izmanto minētos produktus datu izgūšanai no konfiscētām ierīcēm un analīzei. Lai gan tiem ir likumīgi lietojumi, tos tomēr var izmantot ļaunprātīgi un tādējādi apdraudēt sensitīvus vai komerciālus datus.

Tomēr tādi kriminālistikas/izmeklēšanas rīki, kas nav "īpaši izstrādāti" slepenai novērošanai, neietilpst 2. panta 20. punkta kibernovērošanas preču definīcijā. Bez tam kontroles aprakstā attiecībā uz 5A004.b un citām pozīcijām neietilpst kriminālistikas/izmeklēšanas rīki, kuri tikai izgūst lietotāja datus vai kuru gadījumā ierīcē esošie dati nav aizsargāti. Līdztekus kontrole neattiecas uz ražotāja ražošanas vai testēšanas iekārtām, sistēmas administratora rīkiem vai produktiem, kas paredzēti tikai mazumtirdzniecībai, piemēram, uz mobilo tālruņu atbloķētājiem. Ņemot vērā minēto tehnoloģiju daudzveidību, kontroles piemērošana tādējādi ir atkarīga no novērtējuma, kas veikts par katru produktu atsevišķi.

Visbeidzot, jāņem vērā, ka regulas I pielikumā iekļautas vēl citas ar novērošanu saistītas preces, kuras nav uzskatāmas par tādām, uz kurām attiecas kibernovērošanas preču definīcija, piemēram, mobilo telesakaru traucētājiekārtas (5A001.f), kas konstruētas sakaru vai sistēmu bojāšanai vai traucēšanai, ielaušanās programmatūra sistēmu pārveidei (4D004) un lāzera akustiskās uztveršanas iekārtas (6A005.g), kas vāc audiodatus ar lāzeru vai ļauj noklausīties sarunas no attāluma (dažreiz sauktas par "lāzera mikrofonu"). Kibernovērošanas preču definīcija tāpat neattiektos uz sarakstā iekļautiem bezpilota lidaparātiem, kurus izmanto novērošanas nolūkos.