2024/2659

16.10.2024

KOMISJONI SOOVITUS (EL) 2024/2659,

11. oktoober 2024,

Euroopa Parlamendi ja nõukogu määruse (EL) 2021/821 artikli 5 kohast küberseirekaupade eksporti käsitlevate suuniste kohta

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 292,

ning arvestades järgmist:

(1) Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/821 ([1]) on kehtestatud liidu kord kahesuguse kasutusega kaupade ekspordi, vahendamise, tehnilise abi, transiidi ja edasitoimetamise kontrollimiseks:

(2) Määruses (EL) 2021/821 käsitletakse küberseirekaupade siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsiseks rikkumiseks ja kuritarvitamiseks kasutamise riski.

(3) Vastavalt määruse (EL) 2021/821 artikli 5 lõikele 2 ja artikli 26 lõikele 1 teevad komisjon ja nõukogu eksportijatele kättesaadavaks suunised loetlemata küberseirekaupade kohta, et tagada liidu ekspordikontrolli korra tõhusus küberturvalisuse suhtes ning määruse (EL) 2021/821 järjepidev rakendamine.

(4) Käesoleva soovituse ja sellele lisatud suuniste eesmärk on toetada eksportijaid loetlemata küberseirekaupade kontrollimisel, muu hulgas seoses hoolsuskohustuse meetmetega, millega hinnatakse selliste kaupade ekspordiga seotud riske.

(5) Käesolevale soovitusele lisatud suuniste üle toimusid 2022. ja 2023. aastal laialdased konsultatsioonid seiretehnoloogia eksperdirühmas ning arvesse võeti 2023. aasta teises kvartalis toimunud avaliku konsultatsiooni ([2]) käigus saadud tähelepanekuid.

(6) Tuleks meenutada, et käesolev soovitus ja sellele lisatud suunised ei ole siduvad. Seega peaksid eksportijad jääma vastutavaks määrusest (EL) 2021/821 tulenevate kohustuste täitmise eest ning komisjon peaks tagama, et käesolev soovitus jääb aja jooksul asjakohaseks,

([1]) Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/821, millega kehtestatakse liidu kord kahesuguse kasutusega kaupade ekspordi, vahendamise, tehnilise abi, transiidi ja edasitoimetamise kontrollimiseks (ELT L 206, 11.6.2021, lk 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

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

ON VASTU VÕTNUD KÄESOLEVA SOOVITUSE:

Liikmesriikide pädevatel asutustel ja eksportijatel soovitatakse võtta määruse (EL) 2021/821 artikli 5 lõikest 2 tulenevate kohustuste täitmiseks arvesse käesoleva soovituse lisas esitatud suuniseid.

Brüssel, 11. oktoober 2024

Komisjoni nimel
juhtiv asepresident
Valdis DOMBROVSKIS

LISA

SISUKORD

Lk

Sissejuhatus ... 4

1. Asjakohased õigusnormid, määratlused ja põhimõisted ... 4

1.1. Ülevaade asjakohastest õigusnormidest ... 4

1.2. Põhimääratlused ... 5

1.2.1. „Spetsiaalselt kavandatud“ ... 5

1.2.2. „Varjatud jälgimine“ ... 6

1.2.3. „Füüsilised isikud“ ... 6

1.2.4. „Andmete jälgimine, ekstraheerimine, kogumine või analüüsimine“ ... 6

1.2.5. „Info- ja telekommunikatsioonisüsteemidest saadud“ ... 7

1.2.6. „Teadlikkus“ ja „ette nähtud“ ... 7

1.3. Siserepressioonid, inimõiguste ja rahvusvahelise humanitaarõiguse tõsine rikkumine ... 7

1.3.1. Siserepressioonid ... 8

1.3.2. Inimõiguste tõsine rikkumine ... 8

1.3.3. Rahvusvahelise humanitaarõiguse tõsine rikkumine ... 9

2. Tehniline kohaldamisala ... 9

2.1. Loetletud küberseirekaubad ... 9

2.2. Võimalikud loetlemata küberseirekaubad ... 9

2.2.1. Näo- ja emotsioonituvastustehnoloogia ... 10

2.2.2. Asukoha jälgimise seadmed ... 10

2.2.3. Videoseiresüsteemid ... 10

3. Hoolsuskohustuse meetmed ... 10

Määruse (EL) 2021/821 artikli 5 lõikes 2 sätestatud nõuded ... 12

4. Liide ... 12

Loetletud küberseirekaubad, mida kontrollitakse vastavalt määruse (EL) 2021/821 I lisale ... 12

Telekommunikatsiooni pealtkuulamise seadmed (5A001.f) ... 12

Interneti jälgimise süsteemid (5A001.j) ... 13

„Sissetungimistarkvara“ (4A005, 4D004 ja seotud kontrollid 4E001.a ja 4E001.c alusel) ... 13

Teabeedastuse seire tarkvara (5D001.e) ... 14

Krüptoanalüüsiks kasutatavad kaubad (5A004.a) ... 14

Kriminalistika-/uurimisvahendid (5A004.b, 5D002.a.3.b ja 5D002.c.3.b) ... 14

SISSEJUHATUS

Määrusega (EL) 2021/821 (edaspidi „määrus“) loodud liidu ekspordikontrolli raamistiku eesmärk on tagada liidu ja selle liikmesriikide rahvusvaheliste kohustuste ja lubaduste täitmine muu hulgas seoses piirkondliku rahu, turvalisuse ja stabiilsuse ning inimõiguste ja rahvusvahelise humanitaarõiguse austamisega. Seepärast on liit ja selle liikmesriigid rakendanud rahvusvahelise ekspordikontrollirežiimi otsused ja vastavalt ajakohastanud määruse I lisas olevat liidu kontrolliloetelu ([1]). Juba siis, kui määruse artiklit 5 veel ei kohaldatud, kontrollisid liikmesriikide pädevad asutused teatavate selliste loetletud kaupade eksporti, mida võib kasutada seireks, ([2]) võttes arvesse väärkasutuse riski teatavatel konkreetsetel asjaoludel. Liit on kehtestanud sanktsioone, ([3]) millega piiratakse teatavate seireseadmete eksporti eriti keerukate asjaolude korral.

Määrus peegeldab liidu meelekindlust võtta küberseirekaupade siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsiseks rikkumiseks ja kuritarvitamiseks kasutamise risk tulemuslikult käsile. Eeskätt kehtestati määrusega uued sätted loetlemata küberseirekaupade ekspordi kontrolli kohta, sealhulgas eksportija kohustus teatada pädevale asutusele, kui ta on nõuetekohase hoolsuse põhimõtte kohaselt tehtud järelduste põhjal teadlik, et loetlemata küberseirekaubad, mida ta kavatseb eksportida, on tervikuna või osaliselt ette nähtud kasutamiseks siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsisteks rikkumisteks. Lisaks sisaldab määrus üleskutset komisjonile ja nõukogule teha eksportijatele kättesaadavaks suunised, et toetada loetlemata küberseirekaupade uute kontrollide tulemuslikku rakendamist.

Seega on nende suuniste eesmärk toetada eksportijaid loetlemata küberseirekaupade kontrollimisel, muu hulgas seoses nõuetekohase hoolsuse meetmetega, mille abil hinnatakse selliste kaupade lõppkasutajatele eksportimise ja lõppkasutusega seotud riske määruse uute sätete alusel.

1. ASJAKOHASED ÕIGUSNORMID, MÄÄRATLUSED JA PÕHIMÕISTED

1.1. Ülevaade asjakohastest õigusnormidest

Määrusega kehtestatakse uued sätted, millega nähakse konkreetselt ette selliste määruse I lisas loetlemata küberseirevahendite ekspordi kontroll, mis on või mis võivad olla ette nähtud selleks, et kasutada neid tervikuna või osaliselt siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsisteks rikkumisteks. Asjaomased põhjendused ja artiklid on järgmised:

a) põhjendus 8: „Selleks et vähendada riski, et isikud, kes on olnud kaasosalised tõsistes inimõiguste või rahvusvahelise humanitaarõiguse rikkumistes või vastutavad nende korraldamise või toimepanemise eest, võivad teatavaid liidu tolliterritooriumilt eksporditud loetlemata küberseirekaupu väärkasutada, on asjakohane selliste kaupade ekspordi kontroll. Kaasnevad riskid on seotud eelkõige juhtumitega, kus küberseirekaubad on spetsiaalselt kavandatud info- ja telekommunikatsioonisüsteemidesse sissetungimiseks või nende andmepakettide süvaseireks, et füüsilisi isikuid

([1]) Vt eeskätt kontrollid, mis puudutavad telekommunikatsiooni pealtkuulamise seadmeid (5A001.f), interneti jälgimise süsteeme (5A001.j), sissetungimistarkvara (4A005, 4D004 ja seotud kontrollid 4E001.a ja 4E001.c alusel) ja õiguskaitsealase järelevalve tarkvara (5D001.e). Vt lisaks juhtumipõhisele hindamisele tuginevaid kontrolle seoses teatavate kriminalistika-/uurimisvahenditega (5A004.b, 5D002.a.3.b ja 5D002.c.3.b).

([2]) Eeskätt infoturbesüsteemid.

([3]) Vt nõukogu 18. mai 2006. aasta määrus (EÜ) nr 765/2006, mis käsitleb piiravaid meetmeid seoses olukorraga Valgevenes ja Valgevene osalemisega Venemaa agressioonis Ukraina vastu (ELT L 134, 20.5.2006, lk 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); nõukogu 12. aprilli 2011. aasta määrus (EL) nr 359/2011, mis käsitleb teatavate isikute, üksuste ja asutuste vastu suunatud piiravaid meetmeid seoses olukorraga Iraanis (ELT L 100, 14.4.2011, lk 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); nõukogu 18. jaanuari 2012. aasta määrus (EL) nr 36/2012, mis käsitleb piiravaid meetmeid seoses olukorraga Süürias ja millega tunnistatakse kehtetuks määrus (EL) nr 442/2011 (ELT L 16, 19.1.2012, lk 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); nõukogu 2. mai 2013. aasta määrus (EL) nr 401/2013, mis käsitleb Myanmari/Birma vastu suunatud piiravaid meetmeid ja millega tunnistatakse kehtetuks määrus (EÜ) nr 194/2008 (ELT L 121, 3.5.2013, lk 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj), ja nõukogu 13. novembri 2017. aasta määrus (EL) 2017/2063 piiravate meetmete kohta seoses olukorraga Venezuelas (ELT L 295, 14.11.2017, lk 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

varjatult jälgida nendes süsteemides sisalduvate andmete, sealhulgas biomeetriliste andmete jälgimise, ekstraheerimise, kogumise või analüüsimise teel. Kaupu, mida kasutatakse puhtäriliseks otstarbeks, nagu arveldamine, turundus, kvaliteeditеenused, kasutajate rahulolu või võrguturve, ei peeta üldiselt selliste riskidega seotuks.“;

b) põhjendus 9: „Loetlemata küberseirekaupade ekspordi tulemusliku kontrolli tugevdamiseks on oluline veelgi ühtlustada lauskontrolli kohaldamist kõnealuses valdkonnas. Selleks kohustuvad liikmesriigid sellist kontrollimist toetama, jagades omavahel ja komisjoniga teavet, eelkõige küberseirekaupade tehnoloogia arengu kohta, ning olles valvsad selliste kontrollide kohaldamisel, et edendada teabevahetust liidu tasandil.“;

c) artikli 2 punktis 20 on esitatud mõiste „küberseirekaubad“ määratlus: „kahesuguse kasutusega kaubad, mis on spetsiaalselt kavandatud füüsiliste isikute varjatud jälgimiseks info- ja telekommunikatsioonisüsteemidest saadud andmete jälgimise, ekstraheerimise, kogumise või analüüsimise teel“;

d) artikliga 5 kehtestatakse nõue, mille kohaselt on loetlemata küberseirevahendite eksportimiseks vaja luba juhul, kui pädev asutus on eksportijat teavitanud, et kõnealused kaubad on ette nähtud kasutamiseks või neid saab tervikuna või osaliselt kasutada siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsisteks rikkumisteks (artikli 5 lõige 1). Samuti sisaldab see nõuet, et eksportija peab teavitama pädevat asutust, kui ta on nõuetekohase hoolsuse põhimõtte kohaselt tehtud järelduste põhjal teadlik, et kaubad on tervikuna või osaliselt ette nähtud kasutamiseks siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsisteks rikkumisteks (artikli 5 lõige 2). Kõnealune pädev asutus peab otsustama, kas nõuda asjaomaseks eksportimiseks loa taotlemist või mitte, ning

e) artikli 5 lõikes 2 on ühtlasi sätestatud, et „komisjon ja nõukogu teevad eksportijatele kättesaadavaks artikli 26 lõikes 1 osutatud suunised“.

1.2. **Põhimääratlused**

Määrus sisaldab eraldi põhjendusi ja sätteid, milles selgitatakse konkreetseid mõisteid, mis puudutavad loetlemata küberseirekaupade ekspordi kontrolle ja mis on olulised, et eksportijatel oleks selge arusaam, mille põhjal täita hoolsuskohustust ja rakendada tõhusalt kontrolle. Eriti oluline on artikli 2 punktis 20 esitatud „küberseirekaupade“ täpne määratlus: „kahese kasutusega kaubad, mis on spetsiaalselt kavandatud füüsiliste isikute varjatud jälgimiseks info- ja telekommunikatsioonisüsteemidest saadud andmete jälgimise, ekstraheerimise, kogumise või analüüsimise teel“.

Käesolevate suuniste kohaldamiseks tuleks selgitada mõningaid selle määratluse konkreetseid aspekte.

1.2.1. *„Spetsiaalselt kavandatud“*

Kaup on kavandatud varjatud jälgimiseks, kui selle tehnilised omadused sobivad füüsiliste isikute varjatud jälgimiseks ja objektiivselt võimaldavad seda. Seega tähendab „spetsiaalselt kavandatud“, et füüsiliste isikute varjatud jälgimine pidi olema toote arendamise ja kavandamise peamine eesmärk. Samas ei eelda selline sõnakasutus, et sellist kaupa saab kasutada üksnes füüsiliste isikute varjatud jälgimiseks.

Nagu on selgitatud määruse põhjenduses 8, ei ole kaubad, mida kasutatakse puhtäriliseks otstarbeks, nagu arveldamine, turundus, kvaliteeditеenused, kasutajate rahulolu või võrguturve, kavandatud spetsiaalselt füüsiliste isikute varjatud jälgimiseks ega kuulu seega küberseirekaupade määratluse alla. Kuigi näiteks kaupu, mida tööstuses kasutatakse operatsioonisüsteemide seireks või kasutajate liikluse jälgimiseks, võidakse kasutada seire otstarbel ei ole need kaubad määratluse kohaselt küberseirekaubad, sest neid ei ole kavandatud spetsiaalselt füüsiliste isikute varjatud jälgimiseks.

1.2.2. *„Varjatud jälgimine“*

Kaup võimaldab varjatud jälgimist eeskätt siis, kui jälgimine ei ole mõjutatud füüsilisele isikule ilmselgelt märgatav. Seda näiteks juhul, kui asjaomased isikud ei ole teadlikud küberseirekaupade kohalolust ja/või tööst ning seega ei ole neil võimalust sellest jälgimisest eemalduda või vähemalt oma käitumist vastavalt kohandada. Isegi kui jälgimine toimub avalikku ruumi paigaldatud või seal töötava seadme abil, võib andmete hankimist teatavatel juhtudel pidada varjatud jälgimise seisukohast asjakohaseks, eeskätt seetõttu, et kogutud andmeid võib ümber suunata, hinnata või töödelda muudel eesmärkidel kui need, millest mõjutatud füüsilist isikut on teavitatud. Teisisõnu võib jälgimist pidada varjatud jälgimiseks määruse artikli 2 punkti 20 tähenduses, kui füüsiline isik ei saa objektiivselt eeldada, et teda jälgitakse.

1.2.3. *„Füüsilised isikud“*

„Füüsiline isik“ viitab elus inimesele, keda vastandatakse juriidilisele isikule või üksusele, kelle suhtes neid sätteid seega ei kohaldata. See mõiste ei hõlma objektide, kohtade või masinate kui selliste jälgimist.

1.2.4. *„Andmete jälgimine, ekstraheerimine, kogumine või analüüsimine“*

Sõnaraamatutes on sõnadele „jälgimine“, „ekstraheerimine“, „kogumine“ ja „analüüsimine“ antud järgmised tähendused:

— „jälgimine“: järelevalve; vaatlemine, jälitamine;

— „ekstraheerimine“: väljavõtmine;

— „kogumine“: koondamine, kokku toomine;

— „analüüsimine“: millegi (keeruka) elementide eritlemine või kindlaks tegemine, et selgitada välja nähtuse ülesehitus või olemus ja sellest paremini aru saada või seda selgitada; millegi põhjalik ja metoodiline uurimine, et seda tõlgendada; kriitilise või arvutusliku analüüsi rakendamine.

Need terminid tähendavad, et seireks kasutataval kaubal peaks olema andmetöötluse täpne tehniline suutlikkus, et andmeid jälgida, koguda, ekstraheerida või analüüsida, nagu näiteks järgmistel kaupadel:

a) kaup, mida kasutatakse info- ja telekommunikatsioonisüsteemidest saadud andmete ([4]) jälgimiseks (näiteks sellises süsteemis edastatavate andmete failisuurus või pakettide liikumine);

b) kaubad, millega saab info- ja telekommunikatsioonisüsteemidest andmeid ekstraheerida sissetungi või ekstraheerimise teel (näiteks sissetungitarkvara);

c) kaubad, mis võimaldavad analüüsida info- ja telekommunikatsioonisüsteemidest saadud andmeid, kaasa arvatud kaubad, millega saab töödelda neis süsteemides olevaid kaameraga tehtud kujutisi (näiteks teatavat liiki andmeanalüüsi tehnoloogiad, mida kasutatakse näotuvastussüsteemide osana).

Kaubad, mida kasutatakse lihtsalt infosüsteemide jälgimiseks või elanikkonna vaatamiseks videovalvekaamerate kaudu ja mis võimaldavad salvestada vestlusi, andmevahetust, liikumist ja üksikisiku käitumist, ei ole küberseirekaubad selle määruse tähenduses, sest neid ei ole kavandatud spetsiaalselt selleks otstarbeks ja neid tuleb kasutada koos muude tehnoloogiatega, näiteks tehisintellekti või suurandmetega. Samas on võimalik, et kogu süsteemi näol (mis töötab koos muude tehnoloogiatega, nagu tehisintellekt või suurandmete tehnoloogiad) on tegemist küberseirekaubaga määruse artikli 2 punkti 20 tähenduses.

On oluline märkida, et kuigi toodud on mõningaid illustreerimise mõttes kasulikke näiteid, ei piirdu küberseirekaupade mõiste määratlus ja kohaldamisala nende näidetega, sest artikli 5 eesmärk on võimaldada loetlemata kauba tulemuslikku ekspordikontrolli.

([4]) Vt määratlus punktis 1.2.5.

Nagu näitab sidesõna „või“ kasutamine määratluses, tuleb loetletud tehnilisi võimalusi käsitada alternatiividena ning kaubal ei pea olema kõiki tehnilisi võimalusi andmete jälgimiseks, ekstraheerimiseks, kogumiseks või analüüsimiseks. Teisisõnu piisab sellest, kui kaubal on üks neist tehnilistest võimalustest, et kuuluda artikli 2 punktis 20 esitatud küberseirekauba määratluse alla.

1.2.5. *„Info- ja telekommunikatsioonisüsteemidest saadud“*

Nende fraasidega viidatakse süsteemidele, milles toimub teabe elektrooniline töötlemine, näiteks programmeerimine/kodeerimine, personaalarvutisüsteemide (riistvara) töö ja muu teabe haldamine, sealhulgas tarkvaratehnoloogia, veebitehnoloogia, arvutitehnoloogia, salvestustehnoloogia ja muu selline, ning mõningatele süsteemidele, mis edastavad teavet vahemaa tagant, näiteks tehnilised süsteemid, millega edastatakse heli, signaale, teksti, muid märke ja kujutisi nii traadiga kui ka traadita kanalites optilise kiu, raadio või muu elektroonilise süsteemi kaudu. Koos hõlmavad need kaks kategooriat mitmesuguseid teabe edastamise ja töötlemise süsteeme. Juhime tähelepanu sellele, et mõiste tähistab süsteeme, mitte seadmeid.

1.2.6. *„Teadlikkus“ ja „ette nähtud“*

Vastavalt määruse artikli 5 lõikele 2 peab eksportija teavitama pädevat asutust, kui ta on „teadlik, et küberseiretooted […] on ette nähtud kasutamiseks […] siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsisteks rikkumisteks“.

„Teadlikkus“ ei ole uus õigusmõiste, vaid seda on kasutatud lõppkasutusega seotud loanõuete puhul (nn üldkontroll) määruse artiklite 4, 6, 7 ja 8 alusel. Teadlikkus eeldab, et eksportija teab kavandatavast väärkasutamisest. Pelgalt sellise riski võimalus ei ole teadlikkuse tekkimiseks piisav. Samas ei saa teadlikkust samastada passiivsusega: see eeldab, et eksportija on midagi teinud, et tal oleksid piisavad ja pädevad teadmised, et hinnata ekspordiga seotud riske ja tagada määruse järgimine.

Viide sellele, et kaup peab olema „ette nähtud“ asjaomaseks tundlikuks lõppkasutuseks, tähendab, et eksportija peaks hindama lõppkasutust igal üksikjuhul eraldi, arvestades just selle juhtumi konkreetseid asjaolusid. Samas ei ole teoreetiline risk (st risk, mille aluseks ei ole juhtumi faktiline hindamine), et kaupu võidaks kasutada inimõigusi rikkuval viisil, piisav eeldamaks, et need on „ette nähtud“ konkreetseks väärkasutuseks artikli 5 tähenduses.

1.3. **Siserepressioonid, inimõiguste ja rahvusvahelise humanitaarõiguse tõsine rikkumine**

Vastavalt määruse artiklile 15, milles on sätestatud loa andmisele eelneva hindamisega seotud kaalutlused, peavad liikmesriigid võtma arvesse kõiki asjakohaseid kaalutlusi, kaasa arvatud neid, mis sisalduvad nõukogu ühises seisukohas 2008/944/ÜVJP ([5]).

Määruse artikliga 5 laiendatakse kontroll loetlemata küberseirekauba ekspordile, võttes arvesse riski, et sellist kaupa kasutatakse siserepressioonideks ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsisteks rikkumisteks. Selle kohta on kasulikke juhiseid ühises seisukohas 2008/944/ÜVJP ja selle ühise seisukoha kasutusjuhendis ([6]).

([5]) Nõukogu 8. detsembri 2008. aasta ühine seisukoht 2008/944/ÜVJP, millega määratletakse sõjatehnoloogia ja -varustuse ekspordi kontrolli reguleerivad ühiseeskirjad (ELT L 335, 13.12.2008, lk 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Vt nõukogu ühise seisukoha 2008/944/ÜVJP (millega määratletakse sõjatehnoloogia ja -varustuse ekspordi kontrolli reguleerivad ühiseeskirjad) kasutusjuhend, https://data.consilium.europa.eu/doc/document/ST-12189-2019-INIT/et/pdf.

1.3.1. *Siserepressioonid*

Ühise seisukoha 2008/944/ÜVJP artikli 2 lõikes 2 on sätestatud, et „siserepressioonid hõlmavad muu hulgas isikute piinamist ja muul julmal, ebainimlikul või alandaval viisil kohtlemist või karistamist, kiirkorras ja omavolilist hukkamist, kadumist, omavolilist kinnipidamist ja muid olulisi inimõiguste ja põhivabaduste rikkumisi, mis on sätestatud asjakohastes inimõigusi käsitlevates rahvusvahelistes õigusaktides, sealhulgas inimõiguste ülddeklaratsioonis ning kodaniku- ja poliitiliste õiguste rahvusvahelises paktis“. Ühise seisukoha 2008/944/ÜVJP kasutusjuhendis on esitatud juhiseid elementide kohta, mida tuleb eksportija hindamisel arvesse võtta, sealhulgas „väidetava lõppkasutaja praegust ja varasemat tegevust inimõiguste austamise seisukohast ning vastuvõtjariigi praegust ja varasemat tegevust üldiselt“.

1.3.2. *Inimõiguste tõsine rikkumine*

Loetletud küberseirekauba väärkasutamisel võib olla negatiivne mõju mitmesugustele inimõigustele ning see rikub otseselt õigust eraelu puutumatusele ja andmekaitsele. Meelevaldne või ebaseaduslik jälgimine võib rikkuda ka muid inimõigusi, näiteks õigust väljendusvabadusele, ühinemise ja kogunemise vabadusele, mõtte-, südametunnistuse- ja usuvabadusele, aga ka õigust võrdsele kohtlemisele või diskrimineerimise keeldu ning õigust vabadele, võrdsetele ja salajastele valimistele. Konkreetsetel juhtudel võib seire, sealhulgas füüsiliste isikute, näiteks inimõiguste kaitsjate, aktivistide, poliitikategelaste, haavatavate elanikkonnarühmade ja ajakirjanike jälgimine või nende teabe kogumine viia hirmutamise, allasurumise, meelevaldse kinnipidamise, piinamise või isegi kohtuvälise hukkamiseni. Seepärast peaksid eksportijad oma hinnangutes neid inimõiguste tõsise rikkumisega seotud aspekte arvesse võtma.

Rahvusvahelised tavad näitavad, et igasugune inimõiguste piiramine peab olema „asjakohane“ ja kooskõlas rahvusvaheliste inimõiguste standarditega. Praktikas tähendab see, et kehtivad piisavad kaitsemeetmed tagamaks, et piirangud on seadusega ette nähtud ja et säilib õiguste põhiolemus. Proportsionaalsuse põhimõtte kohaselt võib piiranguid kehtestada üksnes siis, kui need on vajalikud ja kui neil on tõeliselt õiguspärane eesmärk, nagu riiklik või avalik julgeolek, avalik kord, rahvatervise kaitse või teiste õiguste ja vabaduste kaitse.

Küberseirekaupade hulka võivad kuuluda õiguspärased ja reguleeritud töövahendid, mida kasutatakse õiguskaitseks, näiteks süütegude tõkestamiseks, uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks muu hulgas terrorismivastases võitluses või kriminaalkaristuste täitmisele pööramise eesmärgil. Samas, kui küberseirekaupu eksporditakse repressiivsetele režiimidele või eraisikutest lõppkasutajatele ja/või konfliktipiirkondadesse, võidakse neid ka väärkasutada, et panna toime inimõiguste ja rahvusvahelise humanitaarõiguse tõsiseid rikkumisi.

See tähendab, et eraldi tuleb hinnata iga üksikjuhu asjaolusid, kaasa arvatud seda, kuidas kohaldatakse asjaomaseid õigusnorme, arvestades näiteks ÜRO, liidu ja Euroopa Nõukogu pädevate asutuste võimalikke aruandeid inimõiguste tõsise rikkumise kohta. Inimõiguste rikkumise „tõsiduse“ kohta võib teha järeldusi selle põhjal, kas neid rikkumisi on tunnistatud ÜRO, liidu või Euroopa Nõukogu pädevate asutuste avaldatud teabes. Ei ole ilmtingimata vaja, et sellised asutused on neid rikkumisi sõnaselgelt tunnistanud, kuid see on oluline tegur, mille põhjal hinnata, kas kriteeriumid on täidetud.

Artikli 5 sõnastuse kohaselt peab tegemist olema „tõsise“ inimõiguste rikkumisega. Kasulikke juhiseid võimaliku inimõiguste rikkumise „tõsiseks“ liigitamise kohta leiab ühise seisukoha 2008/944/ÜVJP kasutusjuhendist. Vastavalt sellele kasutusjuhendile on määrava tähtsusega rikkumise laad ja tagajärjed. Süstemaatilisi ja/või laiaulatuslikke inimõiguste rikkumisi peetakse tavapäraselt tõsiseks, kuid tõsiseks võib pidada ka rikkumisi, mis ei ole süstemaatilised ega laialt levinud, kui selleks annab alust näiteks see, kui raskelt on tegevus mõjunud asjaomastele isikutele.

Ühise seisukoha 2008/944/ÜVJP kasutusjuhendi II lisas on esitatud peamiste rahvusvaheliste ja piirkondlike inimõigustealaste õigusaktide mittetäielik loetelu, millesse kuuluvad muu hulgas kodaniku- ja poliitiliste õiguste rahvusvaheline konventsioon (ICCPR), piinamise ning muu julma, ebainimliku või inimväärikust alandava kohtlemise ja karistamise vastane konventsioon, Euroopa inimõiguste konventsioon (konventsioon) ja põhiõiguste harta (harta), mis sisaldavad olulisi juhiseid selle kohta, kuidas tõlgendada ja kohaldada kriteeriume, et inimõigusi usaldusväärselt hinnata. Need õigusaktid ja nende vastavad lisaprotokollid kujutavad endast inimõiguste ja põhivabaduste valdkonna peamisi rahvusvahelisi norme ja standardeid.

1.3.3. *Rahvusvahelise humanitaarõiguse tõsine rikkumine*

Rahvusvaheline humanitaarõigus, mida nimetatakse ka Genfi õiguseks või relvakonfliktiõiguseks, on välja töötatud mitmete rahvusvaheliste lepingutega, millest olulisimad on Haagi konventsioonid, Genfi konventsioonid ja nende kaks lisaprotokolli aastast 1977, ning selles on esitatud õigusnormid, mis kaitsevad relvakonflikti ajal inimesi, kes ei osale või enam ei osale vaenutegevuses (nt tsiviilisikud ja haavatud, haiged või kinnipeetud võitlejad), ja millega on vaenupooltele kehtestatud sõjapidamise vahendite ja meetodite piirangud (Haagi õigus).

Kui loetlemata küberseirekaupu kasutatakse relvakonfliktis sõjapidamise vahendite ja meetoditena, peaks nende kasutamine olema kooskõlas rahvusvahelise humanitaarõigusega. Selliste asjaolude korral on rahvusvahelise humanitaarõiguse tõsise rikkumise risk kaalutlus määruse tähenduses ning, nagu ka inimõiguste tõsise rikkumise puhul, tuleks seda hinnata, võttes arvesse kauba kavandatud lõppkasutust konkreetsel juhul. Ühise seisukoha 2008/944/ÜVJP kasutusjuhend sisaldab juhiseid elementide kohta, mida tuleb arvesse võtta, sealhulgas vastuvõtja varasem ja praegune tegevus seoses rahvusvahelise humanitaarõiguse austamisega, vastuvõtja ametlikult võetud kohustustest ilmnevad kavatsused ja vastuvõtja võime tagada, et edasi toimetatavat varustust või tehnoloogiat kasutatakse kooskõlas rahvusvahelise humanitaarõigusega ning seda ei suunata kõrvale ega toimetata edasi sihtkohtadesse, kus seda võidakse kasutada nimetatud õiguse raskete rikkumiste toimepanekuks.

Vastavalt määruse artiklile 5 peab tegemist olema rahvusvahelise humanitaarõiguse „tõsise“ rikkumisega. Ühise seisukoha 2008/944/ÜVJP kasutusjuhendist võib leida juhiseid, milles tunnistatakse, et „rahvusvahelise humanitaarõiguse rikkumise üksikjuhtumid ei näita tingimata vastuvõtjariigi suhtumist rahvusvahelisse humanitaarõigusesse“, kuid „murettekitavaks asjaoluks tuleks pidada seda, kui võib tuvastada rikkumiste seaduspärasust või kui vastuvõtjariik ei ole astunud sobivaid samme rikkujate karistamiseks“. Rahvusvaheline Punase Risti Komitee (RPRK) on andnud suunised selle kohta, kuidas hinnata rahvusvahelise humanitaarõiguse rikkumisi ekspordikontrolli kohaldamisel. RPRK seisukoht on, et „rahvusvahelise humanitaarõiguse rikkumine on tõsine, kui see ohustab kaitstavaid isikuid (näiteks tsiviilisikuid, sõjavange, haavatuid või haigeid) või objekte (näiteks tsiviilobjekte või -taristut) või kui need rikuvad olulisi universaalseid väärtusi“. Näiteks sõjakuritegude näol on tegemist rahvusvahelise humanitaarõiguse tõsise rikkumisega. Ühtlasi nimetab RPRK samalaadseid tegureid, mida kaaluda, nagu on nimetatud ühise seisukoha 2008/944/ÜVJP kasutusjuhendis, näiteks ametlikult võetud kohustus kohaldada rahvusvahelise humanitaarõiguse norme, asjakohased meetmed, millega tagatakse vastutus rahvusvahelise humanitaarõiguse rikkumiste eest, rahvusvahelise humanitaarõiguse alane koolitus sõjaväele ja keeld värvata lapsi relvajõududesse.

2. **TEHNILINE KOHALDAMISALA**

2.1. **Loetletud küberseirekaubad**

Käesolevate suuniste liites on esitatud teave määruse I lisas loetletud küberseirekaupade kohta, et aidata eksportijatel kindlaks teha võimalikud loetlemata küberseirekaubad.

2.2. **Võimalikud loetlemata küberseirekaubad**

Põhimõtteliselt on võimatu esitada ammendavat loetelu toodetest, mida võib artikli 5 kohaselt kontrollida kui loetlemata kaupa, kuid järgmisi kaupu on võimalik seireks kasutada ning nende puhul võib eriline valvsus olla määrusest lähtuvalt õigustatud.

Nagu on selgitatud määruse põhjenduses 8, ei peeta kaupu, mida kasutatakse puhtäriliseks otstarbeks, nagu arveldamine, turundus, kvaliteeditеenused, kasutajate rahulolu või võrguturve, üldiselt seotuks sellise väärkasutamise riskidega, mis on inimõiguste või rahvusvahelise humanitaarõiguse tõsise rikkumise seisukohast asjakohased, ning seega ei kohaldata nende suhtes üldiselt artikli 5 kohast kontrolli. Mitmel kõnealusel kaubal on (krüptograafia või isegi krüptoanalüüsi) infoturbefunktsioonid, mis vastavad määruse I lisa kontrollitavaid kaupu käsitleva teksti 5. kategooria 2. osas nimetatud kontrolliparameetritele. Küberseirekauba määratlus ei hõlma ka julgeolekuga seotud võrguseadmeid, sh marsruuterid, kommutaatorid ja releed, mille infoturbefunktsioonid piirduvad käitamise, juhtimise ja hooldamisega ja millega rakendatakse üksnes avaldatud või kommertskasutuseks mõeldud krüptograafilisi standardeid, kuid eksportijad peaksid siiski säilitama valvsuse, arvestades et mitmel korral on teatatud selliste kaupade väärkasutamisest seoses inimõiguste rikkumisega.

2.2.1. *Näo- ja emotsioonituvastustehnoloogia*

Näo- ja emotsioonituvastustehnoloogial on lisaks küberseirele mitu muud kasutusotstarvet, näiteks identimine või autentimine, ning tavapäraselt need määratluse alla ei kuuluks. Samas võib näo- ja emotsioonituvastustehnoloogia teatavatel asjaoludel kuuluda määruse artikli 2 punkti 20 kohaldamisalasse.

Küberseirekauba määratluse alla võiks kuuluda näo- ja emotsioonituvastustehnoloogia, mida saab kasutada salvestatud videokujutiste jälgimiseks või analüüsimiseks. Isegi kui eespool nimetatud kriteeriumid on täidetud, tuleb hoolega uurida, kas tarkvara on spetsiaalselt kavandatud varjatud jälgimise jaoks.

2.2.2. *Asukoha jälgimise seadmed*

Asukoha jälgimise seadmetega saab jälgida seadme asukohta aja jooksul ning õiguskaitse- ja luureasutused on mõningaid asukoha jälgimise tehnoloogiaid kasutanud juba mõnda aega. Võimalus, et selliseid seadmeid kasutatakse massilise ja suunatud jälgimise jaoks, on jälgimisseadmete keerukamaks muutumise (nt satelliidipõhine asukohajälgimine, mobiilsidemastide põhine asukohajälgimine, WiFi ja Bluetoothi transiiverid) ja selliste nn jälgimisseadmete nagu nutitelefonid ja muud elektroonikaseadmed (nt autodes kasutatavad sõidukisisesed süsteemid) laialdase leviku tõttu märkimisväärselt kasvanud.

Õiguskaitse- ja luureasutused kasutavad asukoha jälgimise seadmeid näiteks selleks, et koguda uurimise käigus tõendeid või jälitada kahtlusaluseid, kuid neid kasutavad ka ettevõtted ärilisel otstarbel, näiteks selleks, et saada ülevaade koondandmetel põhinevatest liikumismustritest kaubandustänavatel, jälgida väljaspool töökohta töötavaid töötajaid või pakkuda asukohapõhist reklaami.

2.2.3. *Videoseiresüsteemid*

Et eksportijatel oleks lihtsam võimalikku küberseiret ära tunda, oleks kasulik selgitada, millised kaubad mõiste alla ei kuulu. Selles tähenduses ei ole küberseirekauba määratlusega hõlmatud näiteks videoseiresüsteemid ja -kaamerad (kaasa arvatud suure eraldusvõimega kaamerad), mida kasutatakse inimeste filmimiseks avalikus ruumis, sest sellised seadmed ei jälgi ega kogu info- ja telekommunikatsioonisüsteemidest saadud andmeid.

3. **HOOLSUSKOHUSTUSE MEETMED**

Määruse põhjenduses 7 on öeldud, et „väga oluline on, et eksportijad […] aitaksid kaasa kaubanduskontrolli üldisele eesmärgile. Selleks et nad saaksid tegutseda kooskõlas käesoleva määrusega, tuleb määrusega hõlmatud tehingutega seotud riske hinnata ettevõttesiseste nõuetele vastavuse programmide raames tehingute järelevalve meetmete abil, mida tuntakse ka nõuetekohase hoolsuse põhimõttena."

Artikli 2 punktis 21 on ettevõttesisene nõuetele vastavuse programm defineeritud järgmiselt: „eksportijate poolt käesoleva määruse sätete ja eesmärkide ning määruse kohaselt rakendatavate lubade andmise tingimuste ja nõuete täitmise hõlbustamiseks kasutusele võetud pidev, tulemuslik, asjakohane ja proportsionaalne poliitika ja protseduurid, mis muu hulgas hõlmavad nõuetekohase hoolsuse meetmeid, mille abil hinnatakse kaupade lõppkasutajatele eksportimise ja lõppkasutusega seotud riske".

Komisjoni soovitusega (EL) 2019/1318 on loodud raamistik, ([7]) mis aitab eksportijatel kindlaks teha, hallata ja maandada kahesuguse kasutusega kaupadega kauplemise kontrollimisega seotud riske ning tagada asjakohaste liidu ja siseriiklike õigus- ja haldusnormide järgimise.

Need suunised võivad olla eksportijatele abiks, kui nad viivad ettevõttesiseste nõuetele vastavuse programmide alusel ellu tehingute järelevalve meetmeid, mida nimetatakse ka hoolsuskohustuse põhimõtteks.

Vastavalt määruse (EL) 2021/821 artikli 5 lõikele 2 peavad loetlemata küberseirekaupade eksportijad teostama hoolsuskohustust tehingute järelevalve meetmete abil, mis tähendab, et nad peavad tegelema kaupade klassifitseerimise ja tehinguriski hindamisega. Praktikas julgustatakse eksportijaid tegelema järgmiste teemadega.

([7]) Komisjoni 30. juuli 2019. aasta soovitus (EL) 2019/1318 ettevõttesiseste nõuetele vastavuse programmide kohta kahesuguse kasutusega kaupadega kauplemise kontrollimiseks vastavalt nõukogu määrusele (EÜ) nr 428/2009 (ELT L 205, 5.8.2019, lk 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Vaatama üle, kas eksporditava kauba näol võiks olla tegemist küberseirekaubaga, st kaubaga, mis on spetsiaalselt kavandatud füüsiliste isikute varjatud jälgimiseks info- ja telekommunikatsioonisüsteemidest saadud andmete jälgimise, ekstraheerimise, kogumise või analüüsimise teel.**

See samm puudutab kauba kindlaksmääramist küberseirekauba suhtes kohaldatavate sätete alusel. See hõlmab kauba tehniliste omaduste hindamist määruse I lisas loetletud kaupade tehniliste näitajate põhjal ning võttes arvesse küberseirekauba määratluses kasutatud konkreetseid termineid ja mõisteid loetlemata kaupade kohta ja kauba edasist klassifitseerimist (kaup, tehnoloogia või tarkvara).

3.2. **Vaatama üle asjaomase kauba funktsioonid, et teha kindlaks, milline on võimalus, et välisriigi lõppkasutajad hakkavad seda väärkasutama seoses siserepressioonide ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsise rikkumisega.**

Eksportijad peaksid teostama hindamise, et teha kindlaks, kas toodet võidaks väärkasutada, et panna toime siserepressioone, rikkuda inimõigusi, kaasa arvatud õigust elule, õigust olla kaitstud piinamise, ebainimliku ja alandava kohtlemise eest, õigust sõnavabadusele, ühinemise ja kogunemise õigust, mõtte-, südametunnistuse- ja usuvabadust, õigust võrdsele kohtlemisele või diskrimineerimise keeldu või õigust vabadele, võrdsetele ja salajastele valimistele.

See hõlmab ka hindamist, et teha kindlaks, kas toodet võidaks kasutada sellise süsteemi osa või komponendina, mis võiks põhjustada samasuguseid rikkumisi ja/või väärkasutust.

Eksportijad peaksid hindamisel kasutama nn ohumärke, mis viitavad tehingu ebatavalistele asjaoludel ja annavad märku sellest, et eksport võib olla mõeldud sobimatu lõppkasutuse, lõppkasutaja või sihtkoha jaoks.

Ohumärgid:

a) kauba turustamisel kasutatakse teavet selle kohta, kuidas seda on võimalik kasutada varjatud jälgimise jaoks;

b) teave, mis annab märku sellest, et sarnast kaupa on väärkasutatud seoses siserepressioonide ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsise rikkumisega (vt punkt 1.3);

c) teave, mis annab märku sellest, et kaupa on ebaseaduslikult kasutatud jälgimistegevuses, mis on suunatud liikmesriigi vastu või seotud ELi kodaniku ebaseadusliku jälgimisega;

d) teave, mis annab märku sellest, et tehing hõlmab kaupu, mida võidakse kasutada sellise süsteemi loomiseks, kohandamiseks või konfigureerimiseks, mida teadaolevalt väärkasutatakse seoses siserepressioonide ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsise rikkumisega (vt punkt 1.3);

e) kaupa või samalaadset kaupa on nimetatud määruse artikli 5 lõike 6 kohaselt *Euroopa Liidu Teataja* C-seerias avaldatud loetelus.

3.3. **Vaatama pädevate asutuste toetamiseks üle, millised sidusrühmad tehingus osalevad (sealhulgas lõppkasutaja ja kaubasaajad, nt levitajad ja edasimüüjad).**

Eksportijad peaksid pädevate asutuste toetamiseks tegema võimaluste piires järgmist:

a) vaatama enne iga tehingut ja selle ajal üle, kuidas kaubasaajad ja/või lõppkasutajad kavatsevad toodet või teenust kasutada, lähtudes lõppkasutust käsitlevatest avaldustest;

b) viima ennast kurssi olukorraga, eriti inimõiguste üldtingimusega, kauba asjaomases sihtkohas, sest see on oluline näitaja, mille põhjal hinnata inimõiguste ja rahvusvaheline humanitaarõiguse rikkumise riski seoses ekspordiga;

c) vaatama allpool loetletud ohumärkide põhjal läbi, millised on riskid, et kaup või toode suunatakse kõrvale mõnele teisele volitamata lõppkasutajale.

Ohumärgid:

a) lõppkasutajal on ilmne seos välisriigi valitsusega, mis on varem pannud toime siserepressioone ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsiseid rikkumisi;

b) lõppkasutaja on selliste relvajõudude või muu rühmituse struktuuriline osa, mis osalevad relvastatud konfliktis, millega on varasemalt kaasnenud siserepressioonid ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsised rikkumised;

c) lõppkasutaja on varasemalt eksportinud küberseirekaupu riikidesse, kus sellise kauba kasutamine on toonud kaasa siserepressioone ja/või inimõiguste ja rahvusvahelise humanitaarõiguse tõsiseid rikkumisi.

3.4. **Kasutama nõuetekohase hoolsuse põhimõtte kohaselt tehtud järeldusi selliste plaanide koostamiseks, millega hoida ära võimalikku edasist kahjulikku mõju ja seda leevendada.**

Eksportijad peaksid nõuetekohase hoolsuse põhimõtte kohaselt tehtud järelduste põhjal lõpetama tegevuse, mis põhjustab või suurendab kahjulikku mõju inimõigustele, ning töötama välja ja rakendama parandusmeetmete kava. Sellised meetmed võivad hõlmata järgmist:

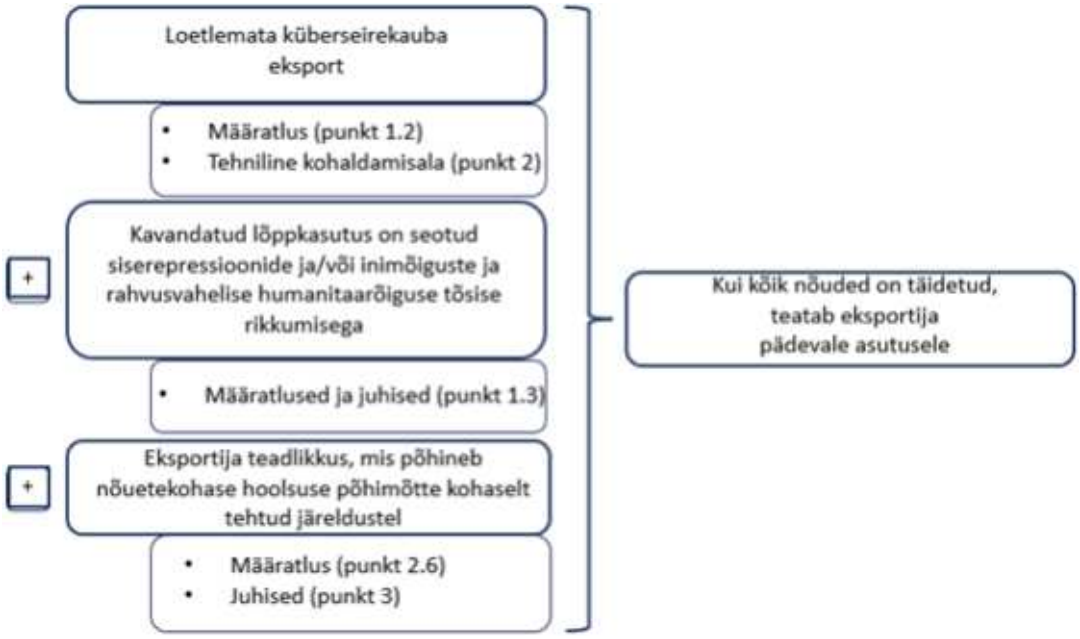
a) ettevõtte põhimõtete ajakohastamine, et pakkuda suuniseid selle kohta, kuidas vältida tulevikus kahjulikku mõju ja sellega toime tulla, ning nende rakendamine;

b) riskihindamise järelduste kasutamine juhtimissüsteemide ajakohastamiseks ja tugevdamiseks, et paremini teavet jälgida ja märgata riske enne kahjuliku mõju tekkimist;

c) teabe kogumine, et mõista kahjuliku mõju suuri riske antud sektoris;

d) liikmesriikide pädevate asutuste teavitamine nõuetekohase hoolsuse põhimõtte kohaselt tehtud järeldustest, et hõlbustada teabe liikumist teatavate kaupade lõppkasutajate ja sihtkohtade kohta.

Määruse (EL) 2021/821 artikli 5 lõikes 2 sätestatud nõuded



4. **LIIDE**

Loetletud küberseirekaubad, mida kontrollitakse vastavalt määruse (EL) 2021/821 I lisale

— **Telekommunikatsiooni pealtkuulamise seadmed (5A001.f)**

Enamikus riikides, sealhulgas liikmesriikides, on side konfidentsiaalsus seadusega kaitstud, kuid õigusraamistikuga võib olla lubatud side varjatud elektrooniline jälgimine valitsusasutuste poolt (nn seaduslik pealtkuulamine). Ent digiajastu on teinud võimalikuks pealtkuulamistehnoloogia massilise kasutamise. See, kuidas Liibüa režiim kasutas pealtkuulamisvahendeid, tõi esile sellise tehnoloogia massilise kasutuselevõtmise potentsiaali ja andis hoogu telekommunikatsiooni pealtkuulamise süsteemide ekspordikontrolli kehtestamisele 2012. aastal.

Sellist kontrolli kohaldatakse seadmete suhtes, mis on kavandatud side (hääl- või andmeside) sisu, aga ka abonentide tunnuste või muude traadita side kaudu eetrisse antavate metaandmete ekstraheerimiseks, ning raadiosageduse jälgimise seadmete suhtes. Sellist kontrolli kohaldatakse näiteks IMSI-püüdurite (IMSI ehk helistaja ja vastuvõtja rahvusvaheline mobiilside tunnus) suhtes, mis kuulavad pealt mobiiltelefoniliiklust ja jälgivad mobiiltelefonikasutajate liikumist, ja seadmete suhtes, mis tekitavad liba-WiFi-kuumkohti ja suudavad telefonist ekstraheerida IMSI numbrid, kui ka teatavat liiki kaupade suhtes, mis on kavandatud selleks, et teha telekommunikatsioonisüsteemides pakettide süvaseiret. Mobiilside segajad ei kuulu küberseirekaupade hulka, sest need ei kogu andmeid.

Selliste süsteemide loomiseks võib küll kasutada üldotstarbelist tehnoloogiat, kuid selleks, et neil oleks massilise pealtkuulamise võimekus, on vaja spetsiifilisi osi ja komponente, muu hulgas näiteks spetsiifilist tarkvara, täiustatud või rakendusspetsiifilisi kiipe (näiteks FGPA, ASIC jne), et sekundis töödeldavate pakettide või sideseansside arv oleks suurem.

— **Interneti jälgimise süsteemid (5A001.j)**

Kuigi suur osa internetipõhisest andmevahetusest on praegusel ajal tavaliselt vaikimisi krüpteeritud, saab andmeliiklusest side kohta püütud andmete (metaandmed), nt IP-aadresside, andmete vahetamise sageduse ja vahetatud andmete mahu põhjal siiski kindlaks teha isikute ja domeeninimede vahelisi seoseid. Valitsused võivad kasutada neid süsteeme seaduslikult ja kohtuliku järelevalve all õiguspärastel eesmärkidel, nt selliste isikute tuvastamiseks, kes külastavad kuritegeliku või terroristliku sisuga seotud domeene. Internetiliikluse jälgimine ja analüüsimine etniliste, religioossete, poliitiliste või sotsiaalsete omaduste põhjal võib aga viia riigi inimeste ja ühiskonna laialdase kaardistamiseni nii rahvastiku kontrollimiseks ja represseerimiseks kui ka muudel eesmärkidel, näiteks poliitiliste teisitimõtlejate tuvastamiseks. Lisaks inimõiguste ja siserepressioonidega seotud teemadele võivad need kaubad aidata parandada julgeoleku- ja sõjalist võimet.

Punkti 5A001.j alusel kohaldatakse kontrolli internetikontrollisüsteemide suhtes, mis töötavad „kandja klassi IP-võrgus (nt näiteks riigi ulatusega klassi IP-magistraal)“, et analüüsida, ekstraheerida ja indekseerida edastatud metaandmete sisu (heli, video, sõnumid, manused) nn kindlate selektorite põhjal ja kaardistada inimeste suhtevõrgustik. Neid kaupu kasutatakse varjatud jälgimiseks, sest sihtmärgiks olevad isikud ei ole side pealtkuulamisest teadlikud. Seevastu ei kohaldata kontrolli süsteemide suhtes, milles leiab aset kasutaja või abonendi tegevus või suhtlus temaga, ning neid ei kohaldata näiteks sotsiaalvõrgustike või kommertsotsingumootorite suhtes. Peale selle kohaldatakse kontrolli süsteemide suhtes, mida kasutatakse internetiteenuse pakkuja tuumikvõrgust pärit andmete töötlemiseks, kuid neid ei kohaldata sotsiaalvõrgustike ega kommertsotsingumootorite suhtes, mis töötlevad kasutajate esitatud andmeid.

— **„Sissetungimistarkvara“ (4A005, 4D004 ja seotud kontrollid 4E001.a ja 4E001.c alusel)**

Sissetungimistarkvara võimaldab selle käitajal saada varjatult kaugjuurdepääsu elektroonilisele seadmele, näiteks nutitelefonile, sülearvutile, serverile või asjade interneti seadmele, et saada sellesse seadmesse salvestatud andmeid, kuulata seadmesse sisseehitatud või seadmega ühendatud kaamera või mikrofoni kaudu pealt ning kasutada seadet hüppelauana, et rünnata selle seadmega ühendatud seadmeid või kasutaja kontaktisikuid („kolmanda isiku seadme kaudu häkkimine“). Sissetungimistarkvara kasutatakse ka seaduslikul otstarbel, ([8]) näiteks siis, kui tegemist on kaugjuurdepääsu tarkvaraga, mida IT-töötajad kasutavad kaugkasutajatoe pakkumiseks, kuid seire varjatuse ja potentsiaalselt kogutava teabe suure hulga puhul on suur oht, et rikutakse õigust privaatsusele ja isikuandmete kaitsele, ning ühtlasi võib see tõsiselt kahjustada õigust sõnavabadusele.

([8]) Selguse huvides olgu öeldud, et kahesuguse kasutusega kaupade määruse I lisa alusel kontrollitavate loetletud küberseirekaupade eksportimiseks kolmandatesse riikidesse on vaja luba ka siis, kui kauba kasutusotstarve on seaduslik.

Punkti 4A005 jt alusel toimuv kontroll hõlmab tarkvara ning süsteeme, seadmeid, komponente ja nendega seotud tehnoloogiat, mis on kavandatud või mida on kohandatud selleks, et saaks luua, juhtida ja kontrollida või kohale toimetada sissetungimistarkvara, kuid seda ei kohaldata sissetungimistarkvara enda suhtes määruse I lisa tähenduses. Neid kübervahendeid kontrollitakse, arvestades häireid ja kahju, mida need võivad eduka kasutamise ja rakendamise korral põhjustada, kuid kontrollimine ei peaks mõjutama näiteks küberturvalisusega tegelevate teadlaste ja tööstuse tegevust, kui neil on vaja jagada sissetungimistarkvara kohta käivat teavet, et töötada oma toodete jaoks välja parandusi ja paigaldada need enne, kui avalikkust nõrkusest teavitatakse.

— **Teabeedastuse seire tarkvara (5D001.e)**

See tarkvara on kavandatud selleks, et volitatud õiguskaitseasutused saaksid jälgida ja analüüsida andmeid, mis on kogutud kommunikatsiooniteenuse osutajalt taotletud sihtotstarbeliste sekkumismeetmete kaudu. See tarkvara võimaldab teha sidesisu või metaandmete nn kindlate selektorite põhjal otsinguid, kasutades seadusliku pealtkuulamise liidest, ning kaardistada suhete otsingutulemuste põhjal asjassepuutuvate isikute kontaktide võrgu või jälgida nende liikumist. Selline tarkvara on mõeldud varjatud jälgimiseks, sest see kasutab side pealtkuulamisel kogutud andmeid ilma, et isikud oleksid sellest teadlikud. Ühtlasi analüüsib see andmeid, mis on kogutud telekommunikatsioonisüsteemide kaudu. See tarkvara on paigaldatud valitsusasutuses (näiteks õiguskaitsealase järelevalve rajatises) ning kontrolli ei kohaldata seadusliku pealtkuulamise vastavussüsteemide suhtes (nt seadusliku pealtkuulamise juhtimise süsteemid ja vahendamise seadmed), mis on kommertsotstarbel välja töötatud ja paigaldatud sideteenuse osutaja ruumi (näiteks integreeritud sidevõrku) ning mida teenuseosutaja käitab ja hooldab. Nagu kontrollitavaid kaupu käsitlevas tekstis selgitatud, ei kohaldata kontrolli tarkvara suhtes, mis on spetsiaalselt kavandatud või mida on muudetud puhtärilisel otstarbel, näiteks arvete esitamise, võrguteenuse kvaliteedi, kogemuse kvaliteedi, vahendamisseadmete või mobiilimaksete või panganduse jaoks.

— **Krüptoanalüüsiks kasutatavad kaubad (5A004.a)**

Sellist kontrolli kohaldatakse kauba suhtes, mis on kavandatud krüptograafiliste süsteemide ületamiseks, et saada kätte salamuutujaid või tundlikku teavet, kaasa arvatud selge tekst, paroolid või krüptograafilised võtmed. Krüptograafiat kasutatakse edastatavate ja jõudeolekus andmete konfidentsiaalsuse kaitsmiseks. Krüptoanalüüsi kasutatakse kõnealuse konfidentsiaalsuse rikkumiseks ja seega võimaldab selline tehnoloogia varjatud jälgimist info- ja telekommunikatsioonisüsteemidest saadud andmete jälgimise, ekstraheerimise, kogumise või analüüsimise teel.

— **Kriminalistika-/uurimisvahendid (5A004.b, 5D002.a.3.b ja 5D002.c.3.b)**

Kriminalistika-/uurimisvahendid on kavandatud toorandmete ekstraheerimiseks seadmest (näiteks andmetöötluses või sides) nii, et andmeid ei manipuleerita ega rikuta ning neid saab kasutada kohtulikul eesmärgil, näiteks kriminaaluurimises või kohtus. Sellised tooted hiilivad seadme autentimis- või volituskontrollist mööda, nii et seadmest saab ekstraheerida toorandmed. Valitsusasutused ja õiguskaitseasutused, aga ka relvajõud kasutavad selliseid tooteid arestitud seadmetest andmete ekstraheerimiseks ja analüüsimiseks. Selliseid tooteid saab kasutada õiguspärasel otstarbel, kuid neid on siiski võimalik ka väärkasutada ja seega kujutavad need endast ohtu tundlikele andmetele ja äriandmetele.

Samas ei kuulu kriminalistika-/uurimisvahendid, mis ei ole kavandatud spetsiaalselt varjatud jälgimise jaoks, artikli 2 punktis 20 esitatud küberseirekaupade määratluse alla. Punkti 5A004.b kontrollitavaid kaupu käsitlev tekst ei käi siiski kriminalistika-/uurimisvahendite kohta, millega ekstraheeritakse üksnes kasutaja andmeid või seadmes olevaid kaitsmata andmeid. Samas ei kohaldata kontrolle tootjate tootmis- või testimisseadmete, süsteemihaldusvahendite või toodete suhtes, mis on mõeldud üksnes jaemüügisektorile, näiteks mobiiltelefonide avamistooted. Võttes arvesse sellist liiki tehnoloogiavahendite mitmekesisust, oleneb kontrolli kohaldamine seega iga toote juhtumipõhisest hindamisest.

Lõpuks juhime tähelepanu sellele, et määruse I lisas on loetletud muid seirega seotud kaupu, mida ei tuleks pidada küberseireseadmete määratluse alla kuuluvaks, näiteks mobiilside segajad (5A001.f), mis on kavandatud kahjustama või häirima sidet või süsteeme, sissetungimistarkvara, millega muudetakse mingit süsteemi (4D004), ja laserakustilised avastamisseadmed (6A005.g), mis koguvad audioandmeid laseri abiga või võimaldavad vestlusi distantsilt pealt kuulata (vahel nimetatakse neid ka lasermikrofonideks). Samuti ei tähenda loetletud mehitamata õhusõidukite seireotstarbeline kasutamine, et need kaubad kuuluksid küberseirekaupade määratluse alla.