2024/2659

16.10.2024

KOMISSION SUOSITUS (EU) 2024/2659,

annettu 11 päivänä lokakuuta 2024,

Euroopan parlamentin ja neuvoston asetuksen (EU) 2021/821 5 artiklan mukaista verkkovalvontatuotteiden vientiä koskevista suuntaviivoista

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 292 artiklan,

sekä katsoo seuraavaa:

(1) Euroopan parlamentin ja neuvoston asetuksella (EU) 2021/821 ([1]) perustetaan kaksikäyttötuotteiden vientiä, välitystä, teknistä apua, kauttakulkua ja siirtoa koskeva unionin valvontajärjestelmä.

(2) Asetuksella (EU) 2021/821 puututaan riskiin siitä, että verkkovalvontatuotteita käytetään kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin.

(3) Asetuksen (EU) 2021/821 5 artiklan 2 kohdan ja 26 artiklan 1 kohdan mukaisesti komissio ja neuvosto asettavat viejien saataville suuntaviivoja valvontaluetteloon sisältymättömistä verkkovalvontatuotteista, koska on tarpeen varmistaa unionin vientivalvontajärjestelmän tehokkuus kyberturvallisuuden osalta sekä asetuksen (EU) 2021/821 täytäntöönpanon yhdenmukaisuus.

(4) Tällä suosituksella ja liitteenä olevilla suuntaviivoilla pyritään tukemaan viejiä valvontaluetteloon sisältymättömien verkkovalvontatuotteiden valvonnan toteuttamisessa, mukaan lukien huolellisuusperiaatteen mukaiset toimenpiteet, joilla arvioidaan kyseisten tuotteiden vientiin liittyviä riskejä.

(5) Tähän suositukseen liitetyistä suuntaviivoista järjestettiin laajoja kuulemisia valvontateknologian asiantuntijaryhmässä vuosina 2022 ja 2023, ja suuntaviivoissa on otettu huomioon vuoden 2023 toisella vuosineljänneksellä järjestetyssä julkisessa kuulemisessa ([2]) saadut kommentit.

(6) On pidettävä mielessä, että tämä suositus ja siihen liitetyt suuntaviivat eivät ole sitovia. Viejien on sen vuoksi edelleen huolehdittava, että ne noudattavat asetuksen (EU) 2021/821 mukaisia velvoitteitaan, ja komission on puolestaan varmistettava, että tämä suositus on jatkuvasti ajantasainen,

([1]) Euroopan parlamentin ja neuvoston asetus (EU) 2021/821, annettu 20 päivänä toukokuuta 2021, kaksikäyttötuotteiden vientiä, välitystä, teknistä apua, kauttakulkua ja siirtoa koskevan unionin valvontajärjestelmän perustamisesta (EUVL L 206, 11.6.2021, s. 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 ANTANUT TÄMÄN SUOSITUKSEN:

Jäsenvaltioiden toimivaltaisia viranomaisia ja viejiä suositellaan ottamaan huomioon tämän suosituksen liitteessä annetut suuntaviivat voidakseen täyttää asetuksen (EU) 2021/821 5 artiklan 2 kohdan mukaiset velvoitteensa.

Tehty Brysselissä 11 päivänä lokakuuta 2024.

Komission puolesta
Valdis DOMBROVSKIS
Johtava varapuheenjohtaja

LIITE

SISÄLLYS

Sivu

Johdanto ... 4

1. Asian kannalta merkitykselliset säännökset, määritelmät ja keskeiset käsitteet ... 4

1.1 Yhteenveto asian kannalta merkityksellisistä säännöksistä ... 4

1.2 Keskeiset määritelmät ... 5

1.2.1 'Erityisesti suunniteltu' ... 5

1.2.2 'Salaa tarkkailu' ... 6

1.2.3 'Luonnolliset henkilöt' ... 6

1.2.4 'Tietojen seuraaminen, poimiminen, kerääminen ja analysointi' ... 6

1.2.5 'Tieto- ja televiestintäjärjestelmistä' ... 7

1.2.6 'Tietää' ja 'on tarkoitettu' ... 7

1.3 Kansalliset tukahduttamistoimet ja ihmisoikeuksien ja kansainvälisen humanitaarisen oikeuden vakavat loukkaukset ... 7

1.3.1 Kansalliset tukahduttamistoimet ... 8

1.3.2 Ihmisoikeuksien vakava loukkaus ... 8

1.3.3 Kansainvälisen humanitaarisen oikeuden vakava loukkaus ... 9

2. Tekninen soveltamisala ... 9

2.1 Valvontaluetteloon sisältyvät verkkovalvontatuotteet ... 9

2.2 Mahdolliset valvontaluetteloon sisältymättömät verkkovalvontatuotteet ... 9

2.2.1 Kasvojen- ja tunteentunnistusteknologia ... 10

2.2.2 Sijainninseurantalaitteet ... 10

2.2.3 Videovalvontajärjestelmät ... 10

3. Huolellisuusperiaatteen mukaiset toimenpiteet ... 10

Asetuksen (EU) 2021/821 5 artiklan 2 kohdassa säädetyt vaatimukset ... 12

4. Lisäys ... 12

Asetuksen (EU) 2021/821 liitteen I mukaisesti valvottavat valvontaluetteloon sisältyvät verkkovalvontatuotteet ... 12

Telekuuntelujärjestelmät (5A001.f) ... 12

Internetvalvontajärjestelmät (5A001.j) ... 13

"Tunkeutumisohjelmistot" (4A005, 4D004 ja vastaava 4E001.a ja 4E001.c kohdan mukainen valvonta) ... 13

Tietoliikenteen valvontaohjelmistot (5D001.e) ... 14

Salauksen analysointiin käytettävät tuotteet (5A004.a) ... 14

Rikostekniset välineet / tutkintavälineet (5A004.b, 5D002.a.3.b ja 5D002.c.3.b) ... 14

JOHDANTO

Asetuksella (EU) 2021/821, jäljempänä 'asetus', vahvistetaan unionin vientivalvontakehys, jonka tavoitteena on varmistaa, että unionin ja sen jäsenvaltioiden alueellista rauhaa, turvallisuutta ja vakautta sekä ihmisoikeuksien ja kansainvälisen humanitaarisen oikeuden kunnioittamista koskevia kansainvälisiä velvoitteita ja sitoumuksia noudatetaan. Unioni ja jäsenvaltiot ovat näin ollen panneet täytäntöön monenvälisissä vientivalvontajärjestelmissä tehdyt päätökset ja saattaneet asetuksen liitteessä I olevan unionin valvontaluettelon ([1]) vastaavasti ajan tasalle. Lisäksi ennen asetuksen 5 artiklan voimaantuloa jäsenvaltioiden toimivaltaiset viranomaiset olivat jo soveltaneet vientivalvontaa tiettyihin valvontaluetteloon sisältyviin tuotteisiin, joita saatetaan käyttää seurantaan ja valvontaan ([2]), ottaen huomioon väärinkäytön riskit tietyissä erityisolosuhteissa. Poikkeuksellisen vakavissa olosuhteissa unioni on määrännyt pakotteita, joilla rajoitetaan tiettyjen seuranta- ja valvontalaitteiden vientiä ([3]).

Asetus ilmentää unionin sitoutumista ehkäistä tehokkaasti riskiä siitä, että verkkovalvontatuotteita käytetään kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin. Erityisesti asetuksella annetaan uusia säännöksiä, jotka koskevat valvontaluetteloon sisältymättömien verkkovalvontatuotteiden vientivalvontaa, mukaan lukien viejien velvoite ilmoittaa toimivaltaiselle viranomaiselle, jos viejä tietää huolellisuusperiaatteen mukaisesti tehtyjen selvitystensä mukaan, että valvontaluetteloon sisältymättömät verkkovalvontatuotteet, jotka viejä aikoo viedä, on tarkoitettu kokonaan tai osittain käyttöön, joka liittyy kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin. Lisäksi asetuksessa kehotetaan komissiota ja neuvostoa asettamaan viejien saataville suuntaviivoja, joilla tuetaan valvontaluetteloon sisältymättömien verkkovalvontatuotteiden uusien valvontatoimien tehokasta toteuttamista.

Näillä suuntaviivoilla pyritäänkin tukemaan viejiä valvontaluetteloon sisältymättömien verkkovalvontatuotteiden valvonnan toteuttamisessa asetuksen uusien säännösten mukaisesti, mukaan lukien muun muassa huolellisuusperiaatteen mukaiset toimenpiteet, joilla arvioidaan riskejä, jotka liittyvät tuotteiden vientiin loppukäyttäjille ja tuotteiden loppukäyttöön.

1. ASIAN KANNALTA MERKITYKSELLISET SÄÄNNÖKSET, MÄÄRITELMÄT JA KESKEISET KÄSITTEET

1.1 Yhteenveto asian kannalta merkityksellisistä säännöksistä

Asetuksella annetaan uusia säännöksiä, joilla säädetään vientivalvonnasta etenkin sellaisten asetuksen liitteeseen I sisältymättömien verkkovalvontatuotteiden osalta, jotka on tai on mahdollisesti tarkoitettu kokonaan tai osittain käyttöön, joka liittyy kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin. Asiaankuuluvat johdanto-osan kappaleet ja artiklat ovat seuraavat:

a) johdanto-osan 8 kappale: "Jotta voidaan ehkäistä riskiä siitä, että vakaviin ihmisoikeusloukkauksiin tai kansainvälisen humanitaarisen oikeuden loukkauksiin osallisina olevat tai tällaisten loukkausten määräämisestä tai toteuttamisesta vastuussa olevat henkilöt saattavat käyttää väärin tiettyjä valvontaluetteloon sisältymättömiä unionin tullialueelta vietyjä verkkovalvontatuotteita, on aiheellista valvoa tällaisten tuotteiden vientiä. Tähän liittyviä riskejä esiintyy

([1]) Ks. etenkin valvonta, joka koskee telekuuntelujärjestelmiä (5A001.f), internetvalvontajärjestelmiä (5A001.j), tunkeutumisohjelmistoja (4A005, 4D004 ja vastaava 4E001.a ja 4E001.c kohdan mukainen valvonta) sekä lainvalvontaviranomaisille tarkoitettuja valvontaohjelmistoja (5D001.e). Ks. myös tapauskohtaisen arvioinnin perusteella valvonta, joka koskee tiettyjä rikosteknisiä välineitä / tutkintavälineitä (5A004.b, 5D002.a.3.b ja 5D002.c.3.b).

([2]) Etenkin "tiedonsuojaus"järjestelmät.

([3]) Ks. neuvoston asetus (EY) N:o 765/2006, annettu 18 päivänä toukokuuta 2006, Valko-Venäjän tilanteen johdosta ja sen johdosta, että Valko-Venäjä on osallisena Venäjän Ukrainaa vastaan kohdistamassa hyökkäyksessä, määrättävistä rajoittavista toimenpiteistä (EUVL L 134, 20.5.2006, s. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); neuvoston asetus (EU) N:o 359/2011, annettu 12 päivänä huhtikuuta 2011, Iranin tilanteen johdosta tiettyihin henkilöihin, yhteisöihin ja elimiin kohdistettavista rajoittavista toimenpiteistä (EUVL L 100, 14.4.2011, s. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); neuvoston asetus (EU) N:o 36/2012, annettu 18 päivänä tammikuuta 2012, Syyrian tilanteen johdosta määrättävistä rajoittavista toimenpiteistä ja asetuksen (EU) N:o 442/2011 kumoamisesta (EUVL L 16, 19.1.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); neuvoston asetus (EU) N:o 401/2013, annettu 2 päivänä toukokuuta 2013, Myanmarin/Burman tilanteen johdosta määrättävistä rajoittavista toimenpiteistä ja asetuksen (EY) N:o 194/2008 kumoamisesta (EUVL L 121, 3.5.2013, s. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); ja neuvoston asetus (EU) 2017/2063, annettu 13 päivänä marraskuuta 2017, Venezuelan tilanteen johdosta määrättävistä rajoittavista toimenpiteistä (EUVL L 295, 14.11.2017, s. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

etenkin tapauksissa, joissa verkkovalvontatuotteet on erityisesti suunniteltu mahdollistamaan tieto- ja televiestintäjärjestelmiin tunkeutuminen tai pakettien syvätarkastus (DPI-tekniikka) luonnollisten henkilöiden salaa tarkkailemiseksi seuraamalla, poimimalla, keräämällä tai analysoimalla näistä järjestelmistä saatuja tietoja, biometriset tiedot mukaan lukien. Tuotteisiin, joita käytetään puhtaasti kaupallisiin sovelluksiin, kuten laskutus, markkinointi, laatupalvelut, käyttäjätyytyväisyys tai verkkoturvallisuus, ei yleisesti ottaen katsota liittyvän tällaisia riskejä.";

b) johdanto-osan 9 kappale: "Jotta voidaan edelleen tehostaa valvontaluetteloon sisältymättömien verkkovalvontatuotteiden viennin valvontaa, on olennaisen tärkeää yhdenmukaistaa entisestään valvontaluetteloon sisältymättömien tuotteiden valvontatoimia tällä alalla. Tätä varten jäsenvaltiot ovat sitoutuneet tukemaan tällaista valvontaa vaihtamalla tietoja keskenään ja komission kanssa erityisesti verkkovalvontatuotteiden teknologian kehityksestä ja seuraamalla valppaasti tällaisen valvonnan toteuttamista edistääkseen tietojenvaihtoa unionin tasolla.";

c) asetuksen 2 artiklan 20 kohta, jonka mukaan verkkovalvontatuotteilla tarkoitetaan "kaksikäyttötuotteita, jotka on erityisesti suunniteltu mahdollistamaan luonnollisten henkilöiden salaa tarkkailun seuraamalla, poimimalla, keräämällä tai analysoimalla tietoja tieto- ja televiestintäjärjestelmistä";

d) asetuksen 5 artikla, jolla säädetään luetteloon sisältymättömien verkkovalvontatuotteiden vientiä koskevasta lupavaatimuksesta, jos viejä on saanut toimivaltaiselta viranomaiselta tiedon, että kyseiset tuotteet on tai on mahdollisesti tarkoitettu kokonaan tai osittain käyttöön, joka liittyy kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin (5 artiklan 1 kohta). Lisäksi siinä edellytetään viejiä ilmoittamaan toimivaltaiselle viranomaiselle, jos viejä tietää huolellisuusperiaatteen mukaisesti tehtyjen selvitystensä mukaan, että tuotteet on tarkoitettu kokonaan tai osittain käyttöön, joka liittyy kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin (5 artiklan 2 kohta). Kyseinen toimivaltainen viranomainen päättää, onko aiheellista määrätä kyseinen vienti luvanvaraiseksi; ja

e) asetuksen 5 artiklan 2 kohta, jossa säädetään lisäksi, että "komissio ja neuvosto asettavat viejien saataville suuntaviivoja 26 artiklan 1 kohdan mukaisesti".

1.2 **Keskeiset määritelmät**

Asetuksessa on erityisiä johdanto-osan kappaleita ja säännöksiä, joilla selvennetään tiettyjä termejä, jotka ovat merkityksellisiä luetteloon sisältymättömien verkkovalvontatuotteiden vientivalvonnan kannalta ja jotka viejien on tärkeää ymmärtää selvästi, jotta asianmukaista huolellisuutta voidaan noudattaa ja valvonta panna tehokkaasti täytäntöön. Erityisen merkityksellinen on 2 artiklan 20 kohta, jossa annetaan seuraava täsmällinen määritelmä, jonka mukaan 'verkkovalvontatuotteilla' tarkoitetaan "kaksikäyttötuotteita, jotka on erityisesti suunniteltu mahdollistamaan luonnollisten henkilöiden salaa tarkkailun seuraamalla, poimimalla, keräämällä tai analysoimalla tietoja tieto- ja televiestintäjärjestelmistä".

Näissä suuntaviivoissa olisi selvennettävä määritelmän tiettyjä näkökohtia.

1.2.1 *'Erityisesti suunniteltu'*

Tuote on suunniteltu salaa tarkkailuun, jos tuotteen tekniset ominaisuudet soveltuvat luonnollisten henkilöiden salaa tarkkailuun ja tuote objektiivisesti mahdollistaa kyseisen tarkkailun. Siksi termillä 'erityisesti suunniteltu' tarkoitetaan, että tuotteen kehittämisen ja suunnittelun päätarkoituksena on täytynyt olla luonnollisten henkilöiden salaa tarkkailu. Termi ei kuitenkaan edellytä, että tuotetta voidaan käyttää yksinomaan luonnollisten henkilöiden salaa tarkkailuun.

Kuten asetuksen johdanto-osan kahdeksannessa perustelukappaleessa selvennetään, tuotteita, joita käytetään puhtaasti kaupallisiin sovelluksiin, kuten laskutukseen, markkinointiin, laatupalveluihin, käyttäjätyytyväisyyteen tai verkkoturvallisuuteen, ei ole erityisesti suunniteltu luonnollisten henkilöiden salaa tarkkailuun, joten ne eivät kuulu verkkovalvontatuotteiden määritelmän piiriin. Vaikka esimerkiksi teollisuuden käyttöjärjestelmien valvontaan tai käyttäjäliikenteen valvontaan tarkoitettuja tuotteita voidaan käyttää valvontatarkoituksiin, ne eivät ole määritelmän mukaisia verkkovalvontatuotteita, koska niitä ei ole erityisesti suunniteltu mahdollistamaan luonnollisten henkilöiden salaa tarkkailua.

1.2.2 *'Salaa tarkkailu'*

Tuotteet mahdollistavat salaa tarkkailun etenkin siinä tapauksessa, että asianomainen luonnollinen henkilö ei voi selvästi havaita tarkkailua. Näin on silloin, kun asianomaiset henkilöt eivät ole tietoisia verkkovalvontatuotteiden olemassaolosta ja/tai toiminnasta, eikä heillä näin ollen ole mahdollisuutta estää itseensä kohdistuvaa tarkkailua tai edes muuttaa käyttäytymistään. Vaikka tarkkailu toteutetaan julkiseen tilaan asennettujen tai julkisessa tilassa käytettävien tuotteiden avulla, tällaisen tietojen hankkimisen voidaan tietyissä tapauksissa katsoa olevan salaa tarkkailua, ja erityisesti on huomattava, että kerättyjä tietoja voidaan siirtää, arvioida tai käsitellä muihin tarkoituksiin kuin niihin, joista asianomainen luonnollinen henkilö on saanut tiedon. Toisin sanoen silloin, kun luonnollinen henkilö ei voi objektiivisesti olettaa olevansa tarkkailun kohteena, tarkkailu voidaan katsoa asetuksen 2 artiklan 20 kohdan mukaiseksi salaa tarkkailuksi.

1.2.3 *'Luonnolliset henkilöt'*

Termillä 'luonnollinen henkilö' tarkoitetaan elävää ihmistä vastakohtana oikeushenkilöille tai yhteisöille, joihin ei sovelleta näitä säännöksiä. Termi ei koske tavaroiden, sijaintien tai koneiden tarkkailua sellaisenaan.

1.2.4 *'Tietojen seuraaminen, poimiminen, kerääminen ja analysointi'*

Oxford English Dictionary -sanakirjan mukaan ilmaisujen 'seuraaminen', 'poimiminen', 'kerääminen' ja 'analysointi' englanninkielisillä vastineilla (monitoring, extracting, collecting ja analysing, tässä järjestyksessä) tarkoitetaan seuraavaa:

— 'seuraaminen': valvonta; tarkkailu, kuuntelu;

— 'poimiminen': valikointi joukosta;

— 'kerääminen': kokoaminen yhteen, yhdistäminen;

— 'analysointi': eritellä tai selvittää jonkin (monitahoisen) osatekijät sen rakenteen tai luonteen määrittämiseksi, jotta se voitaisiin selittää tai sitä voitaisiin ymmärtää; tutkia tarkasti ja järjestelmällisesti tulkitsemista varten; teettää kriittinen tai tietokoneavusteinen analyysi.

Nämä termit implikoivat, että tarkkailuun käytettävissä tuotteissa olisi oltava määrätyt tietojen käsittelyyn tarvittavat tekniset valmiudet, jotta niillä voidaan seurata, poimia, kerätä ja analysoida tietoja, mistä esimerkkinä ovat seuraavat tuotteet:

a) tuotteet, joita käytetään tieto- ja televiestintäjärjestelmistä ([4]) peräisin olevien tietojen valvontaan (esimerkiksi kyseisessä järjestelmässä siirrettävien tietojen tiedostokoot tai pakattu liikenne);

b) tuotteet, jotka poimivat tietoja tieto- ja televiestintäjärjestelmistä tunkeutumisen ja poimimisen avulla (esimerkiksi tunkeutumisohjelmistot);

c) tuotteet, jotka mahdollistavat tieto- ja televiestintäjärjestelmistä poimittujen tietojen analysoinnin, mukaan lukien tuotteet, joilla voidaan käsitellä kyseisiin järjestelmiin tallennettuja kamerakuvia (esimerkiksi tietyntyyppiset data-analyysitekniikat, joita käytetään kasvojentunnistusjärjestelmissä).

Tuotteet, joita käytetään pelkästään tietojärjestelmien seurantaan tai väestön tarkkailuun videovalvontakameroiden avulla ja jotka mahdollistavat keskustelujen, tiedonsiirron, liikkumisen ja yksittäisen käyttäytymisen tallentamisen, eivät olisi asetuksen määritelmän mukaisia verkkovalvontatuotteita, koska niitä ei ole erityisesti suunniteltu tähän tarkoitukseen ja niiden on toimittava muun teknologian, kuten tekoälyn tai massadatan, kanssa. Kyseinen järjestelmä kokonaisuudessaan (käyttö yhdessä muun teknologian kuten tekoäly- tai massadatateknologian kanssa) voisi kuitenkin mahdollisesti olla asetuksen 2 artiklan 20 kohdan määritelmän mukainen verkkovalvontatuote.

Vaikka muutamat esimerkit ovat hyödyllisiä havainnollistamisen kannalta, on tärkeää, että esimerkeillä ei rajoiteta verkkovalvontatuotteiden määritelmää ja soveltamisalaa, koska 5 artiklan tavoitteena on mahdollistaa valvontaluetteloon sisältymättömien tuotteiden tehokas vientivalvonta.

([4]) Katso jäljempänä 1.2.5 kohdassa annettu määritelmä.

Kuten määritelmässä käytetty konjunktio ”tai” osoittaa, luetellut tekniset valmiudet on katsottava vaihtoehdoiksi, eikä tietyllä tuotteella tarvitse olla kaikkia mainittuja teknisiä valmiuksia tietojen seuraamiseen, poimimiseen, keräämiseen tai analysointiin. Toisin sanoen riittää, että tuotteella on jokin mainituista teknisistä valmiuksista, jotta se on 2 artiklan 20 kohdassa annetun verkkovalvontatuotteen määritelmän mukainen.

1.2.5 *'Tieto- ja televiestintäjärjestelmistä'*

Näillä termeillä tarkoitetaan järjestelmiä, jotka käsittelevät sähköisesti tietoja, kuten ohjelmointia/koodausta, mikrotietokonejärjestelmän (laitteiston) toimintoja ja muuta tiedonhallintaa, mukaan lukien esimerkiksi ohjelmistoteknologia, verkkoteknologia, tietokoneteknologia ja tallennusteknologia, sekä joitakin järjestelmiä, jotka välittävät tietoja välimatkan päästä, esimerkiksi teknisiä järjestelmiä, jotka siirtävät ääntä, signaaleja, tekstiä, muita merkkejä tai kuvia niin langallisia kuin langattomia kanavia pitkin optisten kuitujen, radion ja muun sähkömagneettisen järjestelmän avulla. Yhdessä nämä kaksi käsitettä kattavat useita erilaisia tietojen siirtämiseen tai käsittelyyn tarkoitettuja järjestelmiä. On huomattava, että termi ei viittaa laitteisiin vaan järjestelmiin.

1.2.6 *'Tietää' ja 'on tarkoitettu'*

Asetuksen 5 artiklan 2 kohdan mukaan viejän on ilmoitettava toimivaltaiselle viranomaiselle, jos viejä tietää, että verkkovalvontatuotteet on tarkoitettu käyttöön, joka liittyy kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin.

Termi 'tietää' ei ole uusi oikeudellinen käsite, vaan sitä on käytetty asetuksen 4, 6, 7 ja 8 artiklan mukaisten loppukäyttöön liittyvien lupavaatimusten yhteydessä (niin kutsutut valvontaluetteloon sisältymättömien tuotteiden valvontatoimet). 'Tietäminen' implikoi, että viejällä on positiivista tietoa aiotusta väärinkäytöstä. Pelkkä riskin mahdollisuus ei tarkoita, että asiasta tiedettäisiin. Termiä 'tietää' ei voida myöskään rinnastaa passiivisuuteen: se edellyttää, että viejä on toteuttanut toimia hankkiakseen riittävät ja asianmukaiset tiedot vientiin liittyvien riskien arviointia varten ja varmistaakseen asetuksen noudattamisen.

Vaatimus siitä, että tuotteet 'on tarkoitettu' asiaankuuluvaan arkaluonteiseen loppukäyttöön, tarkoittaa, että viejän olisi arvioitava loppukäyttöä tapauskohtaisesti ottaen huomioon kunkin tapauksen erityisolosuhteet. Riski siihen, että tuotteita voidaan käyttää tavalla, joka loukkaa ihmisoikeuksia, voi olla myös teoreettinen, millä tarkoitetaan, että riski ei perustu tapauksen tosiseikkojen arviointiin. Tällainen teoreettinen riski ei riitä osoittamaan, että tuotteet 'on tarkoitettu' 5 artiklassa määritettyyn erityiseen väärinkäyttöön.

1.3 **Kansalliset tukahduttamistoimet ja ihmisoikeuksien ja kansainvälisen humanitaarisen oikeuden vakavat loukkaukset**

Asetuksen 15 artiklassa säädetään luvan arviointiin liittyvistä näkökohdista, ja artiklan mukaan jäsenvaltioiden on otettava huomioon kaikki asian kannalta merkitykselliset näkökohdat, mukaan lukien neuvoston yhteisessä kannassa 2008/944/YUTP ([5]) esitetyt näkökohdat.

Asetuksen 5 artiklalla valvonta laajennetaan koskemaan myös valvontaluetteloon sisältymättömien verkkovalvontatuotteiden vientiä ottaen huomioon riski siitä, että niitä käytetään kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin. Yhteisessä kannassa 2008/944/YUTP ja kyseiseen yhteiseen kantaan liittyvässä käyttäjän oppaassa ([6]) annetaan tältä osin hyödyllisiä ohjeita.

([5]) Neuvoston yhteinen kanta 2008/944/YUTP, vahvistettu 8 päivänä joulukuuta 2008, sotilasteknologian ja puolustustarvikkeiden viennin valvontaa koskevien yhteisten sääntöjen määrittämisestä (EUVL L 335, 13.12.2008, s. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Ks. sotilasteknologian ja puolustustarvikkeiden viennin valvontaa koskevien yhteisten sääntöjen määrittämisestä hyväksyttyyn neuvoston yhteiseen kantaan 2008/944/YUTP liittyvä käyttäjän opas, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1 *Kansalliset tukahduttamistoimet*

Yhteisen kannan 2008/944/YUTP 2 artiklan 2 kohdan mukaan ”kansallista sortotoimintaa ovat muun muassa kidutus ja muu julma, epäinhimillinen ja halventava kohtelu tai rangaistus, ilman oikeudenkäyntiä toteutetut tai mielivaltaiset teloitukset, katoamiset, mielivaltaiset vangitsemiset ja muut niiden ihmisoikeuksien ja perusvapauksien törkeät loukkaukset, jotka on määritelty kansainvälisissä ihmisoikeussopimuksissa, joihin kuuluvat ihmisoikeuksien yleismaailmallinen julistus sekä kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus” (ICCPR). Yhteiseen kantaan 2008/944/YUTP liittyvässä käyttäjän oppaassa annetaan ohjeita osatekijöistä, jotka on otettava huomioon viejän tekemässä arvioinnissa, mukaan lukien tiedot ”siitä, miten ilmoitettu loppukäyttäjä ja yleensä vastaanottajamaa ovat kunnioittaneet ihmisoikeuksia”.

1.3.2 *Ihmisoikeuksien vakava loukkaus*

Valvontaluetteloon sisältymättömien verkkovalvontatuotteiden väärinkäyttö voi vaikuttaa kielteisesti moniin eri ihmisoikeuksiin ja heikentää suoraan yksityisyyteen ja tietosuojaan liittyvän oikeuden toteutumista. Mielivaltainen tai lainvastainen tarkkailu ja valvonta voi loukata myös muita ihmisoikeuksia, kuten oikeutta sananvapauteen, yhdistymis- ja kokoontumisvapauteen ja ajatuksen-, omantunnon- ja uskonnonvapauteen sekä oikeutta yhdenvertaiseen kohteluun tai syrjinnän kieltoon sekä oikeutta vapaisiin, yhdenvertaisiin ja salaisiin vaaleihin. Erityistapauksissa tarkkailu ja valvonta, myös seuranta tai tietojen kerääminen, joka kohdistuu luonnollisiin henkilöihin, kuten ihmisoikeuksien puolustajiin, aktivisteihin, poliitikkoihin, haavoittuvassa asemassa oleviin väestöryhmiin ja toimittajiin, voi johtaa uhkailuun, sortamiseen, mielivaltaiseen vangitsemiseen, kidutukseen tai jopa laittomiin teloituksiin. Viejien olisikin sisällytettävä arviointeihinsa nämä vakaviin ihmisoikeusloukkauksiin liittyvät näkökohdat.

Kansainväliset käytännöt osoittavat, että ihmisoikeuksien minkä tahansa rajoituksen on oltava ”tarkoituksenmukainen” ja kansainvälisten ihmisoikeusnormien mukainen. Käytännössä tämä tarkoittaa, että käytössä on riittävät suojatoimet sen varmistamiseksi, että rajoitus on sallittu lainsäädännön nojalla ja oikeuksien olennaista sisältöä kunnioitetaan. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan asettaa vain, jos ne ovat välttämättömiä ja aidosti palvelevat oikeutettua tarkoitusta – esimerkiksi kansallista tai yleistä turvallisuutta, yleistä järjestystä, kansanterveyden suojelua tai muiden oikeuksien ja vapauksien suojelua.

Verkkovalvontatuotteisiin voi kuulua lainmukaisia ja säänneltyjä työkaluja, jotka on tarkoitettu lainvalvontaviranomaisten käyttöön, kuten rikosten ennalta estämiseen, tutkimiseen, havaitsemiseen tai syytteeseenpanoon, myös terrorismin torjunnan alalla, tai rikosoikeudellisten seuraamusten toimeenpanoon. Toisaalta verkkovalvontatuotteita voidaan myös väärinkäyttää vakaviin ihmisoikeusloukkauksiin ja kansainvälisen humanitaarisen oikeuden loukkauksiin, kun tuotteita viedään sortohallinnoille tai yksityisille loppukäyttäjille ja/tai konfliktialueille.

Tämän takia on arvioitava tapauskohtaisesti kunkin yksittäistapauksen olosuhteita, mukaan lukien asiaa koskevien säännösten soveltaminen, ottaen huomioon esimerkiksi Yhdistyneiden kansakuntien, unionin tai Euroopan neuvoston toimivaltaisten elinten raportoimat vakavat ihmisoikeusloukkaukset. Ihmisoikeusloukkausten vakavuus voidaan päätellä siitä, miten loukkaukset on luokiteltu Yhdistyneiden kansakuntien toimivaltaisten elinten, unionin tai Euroopan neuvoston julkaisemissa tiedoissa. Kyseisten elinten tekemä nimenomainen luokittelu ei ole ehdottoman välttämätöntä, mutta se on merkittävä tekijä, jotta perusteiden voidaan katsoa täyttyvän.

Asetuksen 5 artiklan mukaan ihmisoikeuksien loukkauksen on oltava vakava. Hyödyllisiä ohjeita mahdollisten ihmisoikeusloukkausten luokittelemiseksi vakaviksi on yhteiseen kantaan 2008/944/YUTP liittyvässä käyttäjän oppaassa. Oppaan mukaan ratkaisevia ovat loukkauksen luonne ja seuraukset. Järjestelmälliset ja/tai laajamittaiset ihmisoikeusloukkaukset katsotaan yleensä vakaviksi; toisaalta vakaviksi voidaan katsoa myös loukkaukset, jotka eivät ole järjestelmällisiä tai laajamittaisia – esimerkiksi siksi, että teko on vakava asianomaisten henkilöiden kannalta.

Yhteiseen kantaan 2008/944/YUTP liittyvän käyttäjän oppaan liitteessä II on ohjeellinen luettelo tärkeimmistä kansainvälisistä ja alueellisista ihmisoikeusvälineistä, joihin kuuluvat esimerkiksi kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus, kidutuksen ja muun julman, epäinhimillisen tai halventavan kohtelun tai rangaistuksen vastainen yleissopimus, Euroopan ihmisoikeussopimus, jäljempänä ’yleissopimus’, ja perusoikeuskirja, jäljempänä ’perusoikeuskirja’, ja joissa voi olla tärkeitä ohjeita perusteiden tulkinnasta ja soveltamisesta luotettavien ihmisoikeusarviointien tekemiseksi. Nämä välineet ja niihin liittyvät lisäpöytäkirjat ovat tärkeimpiä kansainvälisiä normeja ja vaatimuksia ihmisoikeuksien ja perusvapauksien alalla.

1.3.3 *Kansainvälisen humanitaarisen oikeuden vakava loukkaus*

Kansainvälinen humanitaarinen oikeus (jota kutsutaan myös 'Geneven oikeudeksi' tai 'aseellisia konflikteja koskevaksi oikeudeksi') perustuu erilaisiin kansainvälisiin sopimuksiin, joista tärkeimpiä ovat Haagin asetukset sekä Geneven yleissopimukset ja niiden kaksi lisäpöytäkirjaa vuodelta 1977. Kansainvälisessä humanitaarisessa oikeudessa määritetään säännöt, joiden tarkoituksena on suojella aseellisten konfliktien aikana ihmisiä, jotka eivät osallistu tai eivät enää osallistu vihamielisyyksiin (esimerkiksi siviilit ja haavoittuneet, sairaat tai vangitut taistelijat), ja joilla asetetaan taistelukeinoihin ja -menetelmiin liittyviä rajoituksia konfliktin osapuolille (Haagin laki).

Valvontaluetteloon sisältymättömien verkkovalvontatuotteiden käytössä olisi noudatettava kansainvälistä humanitaarista oikeutta, jos niitä käytetään taistelukeinoina ja -menetelminä aseellisessa konfliktissa. Asetuksen mukaan tällaisissa olosuhteissa on otettava huomioon kansainvälisen humanitaarisen oikeuden vakavien loukkausten riski, ja – kuten ihmisoikeuksien vakavien loukkausten tapauksessa – riskiä olisi arvioitava tapauskohtaisesti ottaen huomioon tuotteiden ilmoitettu loppukäyttö. Yhteiseen kantaan 2008/944/YUTP liittyvässä käyttäjän oppaassa annetaan ohjeita huomioon otettavista osatekijöistä, mukaan luettuina tiedot siitä, miten vastaanottaja noudattaa ja on noudattanut kansainvälistä humanitaarista oikeutta, sekä vastaanottajan aikeet virallisina sitoumuksina ilmaistuina ja vastaanottajan kyky varmistaa, että siirrettyjä tarvikkeita tai siirrettyä teknologiaa käytetään kansainvälisen humanitaarisen oikeuden mukaisesti eikä niitä suunnata tai siirretä muuhun määräpaikkaan, jossa niitä saatettaisiin käyttää edellä mainitun oikeuden vakaviin loukkauksiin.

Asetuksen 5 artiklan mukaan kansainvälisen humanitaarisen oikeuden loukkauksen on oltava vakava. Yhteiseen kantaan 2008/944/YUTP liittyvässä käyttäjän oppaassa annetaan ohjeita, joiden mukaan "yksittäiset kansainvälisen humanitaarisen oikeuden loukkaukset eivät välttämättä ole osoitus vastaanottajamaan suhtautumisesta kansainväliseen humanitaariseen oikeuteen", ja todetaan, että "mikäli loukkauksissa voidaan havaita tietty kaava tai vastaanottajamaa ei ole toteuttanut loukkauksen johdosta asianmukaisia rankaisutoimia, asiaa olisi pidettävä erittäin huolestuttavana". Punaisen Ristin kansainvälinen komitea (ICRC) on antanut ohjeita kansainvälisen humanitaarisen oikeuden loukkausten arvioinnista vientivalvonnan yhteydessä. ICRC:n mukaan "kansainvälisen humanitaarisen oikeuden loukkaukset ovat vakavia, jos niistä aiheutuu vaaraa suojeltaville henkilöille (esimerkiksi siviileille, sotavangeille, haavoittuneille ja sairailla) tai kohteille (esimerkiksi siviilikohteille tai infrastruktuurille) tai ne rikkovat tärkeitä yleismaailmallisia arvoja". Esimerkiksi sotarikokset ovat vakavia kansainvälisen humanitaarisen oikeuden loukkauksia. Huomioon otettavien seikkojen osalta ICRC mainitsee tekijöitä, jotka ovat samankaltaisia kuin yhteiseen kantaan 2008/944/YUTP liittyvässä käyttäjän oppaassa, mukaan lukien viralliset sitoumukset, jotka koskevat kansainvälisen humanitaarisen oikeuden sääntöjen soveltamista, asianmukaiset toimenpiteet, joilla varmistetaan vastuuvelvollisuus kansainvälisen humanitaarisen oikeuden loukkauksista, kansainvälisen humanitaarisen oikeuden opettaminen sotilaille sekä kielto, joka koskee lasten värväämistä asevoimiin.

2. TEKNINEN SOVELTAMISALA

2.1 Valvontaluetteloon sisältyvät verkkovalvontatuotteet

Näiden ohjeiden lisäyksessä annetaan tietoa asetuksen liitteessä I luetelluista verkkovalvontatuotteista, jotta viejät voivat tunnistaa mahdollisia valvontaluetteloon sisältymättömiä verkkovalvontatuotteita.

2.2 Mahdolliset valvontaluetteloon sisältymättömät verkkovalvontatuotteet

Vaikka on määritelmänkin mukaan mahdotonta laatia tyhjentävä luettelo tuotteista, joita voidaan valvoa 5 artiklan mukaisina 'valvontaluetteloon sisältymättöminä tuotteina', seuraavia tuotteita voitaisiin mahdollisesti käyttää tarkkailuun ja valvontaan, ja ne saattavat edellyttää erityistä valppautta asetuksen nojalla.

Kuten asetuksen johdanto-osan 8 kappaleessa selvennetään, tuotteisiin, joita käytetään puhtaasti kaupallisiin sovelluksiin, kuten laskutus, markkinointi, laatupalvelut, käyttäjätyytyväisyys tai verkkoturvallisuus, ei yleisesti ottaen katsota liittyvän väärinkäyttöriskejä ihmisoikeuksien tai kansainvälisen humanitaarisen oikeuden vakavien loukkausten osalta, eikä niihin siksi yleensä sovelleta 5 artiklan mukaista valvontaa. Monissa näistä tuotteista on tiedonsuojaustoimintoja (salaustoimintoja tai jopa salauksen analysointitoimintoja), jotka täyttävät asetuksen liitteessä I olevan valvontaa koskevan tekstin 5 ryhmän 2 osassa esitetyt valvontaparametrit. 'Verkkovalvontatuotteiden' määritelmä ei myöskään kata turvallisuusverkon laitteita, mukaan lukien reitittimet, kytkimet tai releet, joissa tiedonsuojaustoimintoa käytetään vain "toimintaan, hallintoon tai ylläpitoon" ja jotka perustuvat ainoastaan julkaistuihin tai kaupallisiin salausstandardeihin, mutta viejien olisi hyvä pysyä valppaina, koska tällaisten tuotteiden väärinkäytöstä ihmisoikeusloukkauksiin on tehty ilmoituksia.

2.2.1 *Kasvojen- ja tunteentunnistusteknologia*

Kasvojen- ja tunteentunnistusteknologioilla on lukuisia muitakin käyttötarkoituksia kuin verkkovalvonta – esimerkiksi tunnistaminen tai todentaminen – eivätkä nämä teknologiat automaattisesti kuulu määritelmän soveltamisalaan. Tietyissä olosuhteissa kasvojen- ja tunteentunnistusteknologiat voivat kuitenkin kuulua asetuksen 2 artiklan 20 kohdan soveltamisalaan.

Kasvojen- ja tunteentunnistusteknologiat, joita voidaan käyttää tallennetun videokuvan seurantaan tai analysointiin, voisivat kuulua verkkovalvontatuotteen määritelmän soveltamisalaan. Vaikka edellä mainitut perusteet täyttyvät, on kuitenkin tutkittava huolellisesti, onko ohjelmisto erityisesti suunniteltu salaa tarkkailuun.

2.2.2 *Sijainninseurantalaitteet*

Sijainninseurantalaitteet mahdollistavat laitteen fyysisen sijainnin seurannan ajan mittaan, ja jotkut sijainninseurantateknologiat ovat jo jonkin aikaa olleet lainvalvonta- ja tiedusteluviranomaisten käytössä. Mahdollisuus käyttää laitteita kohdennettuun valvontaan ja joukkovalvontaan on kehittynyt merkittävästi, koska seurantateknologiat ovat huomattavasti aiempaa kehittyneempiä – mukaan lukien satelliittipohjainen sijainninseuranta, tukiasemapohjainen sijainninseuranta, Wi-Fi- ja Bluetooth-lähetin-vastaanottimet – ja koska 'seurantalaitteet', kuten älypuhelimet ja muut elektroniset laitteet (esimerkiksi autoihin asennetut ajoneuvojärjestelmät), ovat yleistyneet.

Lainvalvonta- ja tiedusteluviranomaiset käyttävät sijainninseurantalaitteita esimerkiksi todisteiden keräämiseen tutkinnan aikana tai epäiltyjen jäljittämiseen. Yritykset puolestaan käyttävät laitteita kaupallisiin tarkoituksiin, esimerkiksi raportointiin, joka koskee ylätason liikkuvuusmalleja ostoskaduilla, etätöitä tekevien työntekijöiden seurantaan tai sijaintiin perustuvaan mainontaan.

2.2.3 *Videovalvontajärjestelmät*

Jotta viejät voisivat tunnistaa mahdollisen verkkovalvonnan, on myös hyödyllistä selventää, mitkä tuotteet eivät kuulu määritelmän soveltamisalaan. Tältä osin esimerkiksi videovalvontajärjestelmät ja -kamerat – myös korkean resoluution kamerat – joita käytetään ihmisten kuvaamiseen julkisissa tiloissa, eivät kuulu verkkovalvontatuotteiden määritelmän soveltamisalaan, koska niillä ei valvota tai kerätä tietoa tieto- ja televiestintäjärjestelmistä.

3. HUOLELLISUUSPERIAATTEEN MUKAISET TOIMENPITEET

Asetuksen johdanto-osan 7 kappaleen mukaan "on ratkaisevan tärkeää, että viejät […] edistävät yleistä kaupan valvonnan tavoitetta. Jotta ne voivat toimia tämän asetuksen mukaisesti, tämän asetuksen soveltamisalaan kuuluvien liiketapahtumien riskit on arvioitava toteuttamalla sisäiseen vaatimustenmukaisuusohjelmaan kuuluvia liiketapahtumien seurantatoimenpiteitä niin kutsutun huolellisuusperiaatteen (due diligence) mukaisesti."

Asetuksen 2 artiklan 21 kohdassa annetun määritelmän mukaan sisäisellä vaatimustenmukaisuusohjelmalla tarkoitetaan "jatkuvia vaikuttavia, asianmukaisia ja oikeasuhteisia toimintatapoja ja menettelyjä, joita viejät ovat ottaneet käyttöön helpottaakseen tämän asetuksen säännösten ja tavoitteiden sekä tämän asetuksen nojalla täytäntöönpantujen lupien ehtojen noudattamista ja joihin kuuluvat muun muassa huolellisuusperiaatteen mukaiset toimenpiteet, joilla arvioidaan riskejä, jotka liittyvät tuotteiden vientiin loppukäyttäjille ja tuotteiden loppukäyttöön".

Komission suosituksella (EU) 2019/1318 ([7]) luodaan puitteet, joilla viejiä autetaan tunnistamaan, hallitsemaan ja vähentämään kaksikäyttötuotteiden kaupan valvontaan liittyviä riskejä ja varmistamaan, että asiaan liittyviä unionin ja kansallisia lakeja ja asetuksia noudatetaan.

Nämä ohjeet voivat tukea viejiä, kun ne toteuttavat sisäiseen vaatimustenmukaisuusohjelmaan kuuluvia liiketapahtumien seurantatoimenpiteitä niin kutsutun huolellisuusperiaatteen mukaisesti.

Asetuksen (EU) 2021/821 5 artiklan 2 kohdan mukaan valvontaluetteloon sisältymättömien verkkovalvontatuotteiden viejien on noudatettava huolellisuusperiaatetta toteuttamalla liiketapahtumien seurantatoimenpiteitä eli toteutettava toimia, jotka koskevat tuotteiden luokittelua ja liiketapahtumien riskien arviointia. Käytännössä viejiä kannustetaan tarkastelemaan seuraavaa:

([7]) Komission suositus (EU) 2019/1318, annettu 30 päivänä heinäkuuta 2019, sisäisistä vaatimustenmukaisuusohjelmista asetuksen (EY) N:o 428/2009 mukaisessa kaksikäyttötuotteiden kaupan valvonnassa (EUVL L 205, 5.8.2019, s. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1 **Tarkastellaan, voisiko valvontaluetteloon sisältymätön vietävä tuote olla ’verkkovalvontatuote’ eli onko se erityisesti suunniteltu mahdollistamaan luonnollisten henkilöiden salaa tarkkailu seuraamalla, poimimalla, keräämällä tai analysoimalla tietoja tieto- ja televiestintäjärjestelmistä**

Tässä vaiheessa on kyse tuotteen määrittämisestä verkkovalvontatuotteisiin sovellettavien säännösten mukaisesti. Tarkastelun yhteydessä muun muassa tutkitaan tuotteiden tekniset ominaisuudet käyttäen lueteltujen tuotteiden osalta lähtökohtana teknisiä parametrejä, jotka annetaan asetuksen liitteessä I, ja ottaen valvontaluetteloon sisältymättömien tuotteiden osalta huomioon verkkovalvontatuotteiden määritelmässä käytetyt erityiset termit ja käsitteet, minkä jälkeen tuote luokitellaan (tavara, teknologia tai ohjelmisto).

3.2 **Tarkastellaan kyseisen tuotteen valmiuksia, jotta voidaan määrittää ulkomaisten loppukäyttäjien mahdollisuus väärinkäyttää tuotteita kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin**

Viejien olisi tehtävä arviointi sen määrittämiseksi, voitaisiinko tuotetta väärinkäyttää kansallisiin tukahduttamistoimiin tai voitaisiinko tuotteella loukata tai rikkoa ihmisoikeuksia, mukaan lukien oikeus elämään, vapaus kidutuksesta ja epäinhimillisestä ja halventavasta kohtelusta, oikeus yksityisyyteen, oikeus sananvapauteen, oikeus yhdistymis- ja kokoontumisvapauteen, oikeus ajatuksen-, omantunnon- ja uskonnonvapauteen, oikeus yhdenvertaiseen kohteluun tai syrjinnän kieltoon tai oikeus vapaisiin, yhdenvertaisiin ja salaisiin vaaleihin.

Tässä yhteydessä olisi myös arvioitava, voitaisiinko tuotetta käyttää jonkin järjestelmän osana tai komponenttina niin, että käyttö voisi johtaa samoihin loukkauksiin ja/tai väärinkäyttöön.

Viejien olisi käytettävä arvioinnissa niin sanottuja varoitusmerkkejä, jotka viittaavat liiketapahtuman epätavallisiin olosuhteisiin, joiden perusteella vientiä saatetaan tehdä epäasianmukaiseen loppukäyttöön tai määräpaikkaan tai epäasianmukaiselle loppukäyttäjälle.

Varoitusmerkkejä:

a) tuotetta markkinoidaan tiedoilla, jotka koskevat mahdollisuutta käyttää tuotetta salaa tarkkailuun;

b) tiedot, jotka osoittavat, että samankaltaista tuotetta on väärinkäytetty kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin (ks. 1.3 kohta);

c) tiedot, jotka osoittavat, että tuotetta on käytetty lainvastaisesti jäsenvaltioon kohdistuneissa valvontatoimissa tai EU:n kansalaisen lainvastaisessa tarkkailussa;

d) tiedot, jotka osoittavat, että liiketapahtumaan sisältyy tuotteita, joiden avulla voitaisiin perustaa, mukauttaa tai konfiguroida järjestelmä, jota tietojen mukaan on väärinkäytetty kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksia koskevan oikeuden ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin (ks. 1.3 kohta);

e) tuote tai vastaava tuote mainitaan valvontaluettelossa, joka on julkaistu *Euroopan unionin virallisen lehden* C-sarjassa asetuksen 5 artiklan 6 kohdan mukaisesti.

3.3 **Tarkastellaan toimivaltaisten viranomaisten tueksi liiketapahtumaan liittyviä osapuolia (mukaan lukien loppukäyttäjä ja vastaanottajat, kuten jakelijat ja jälleenmyyjät)**

Viejien olisi toimivaltaisten viranomaisten tueksi ja mahdollisuuksien mukaan

a) tarkasteltava ennen liiketapahtumaa ja sen aikana, miten vastaanottajat ja/tai loppukäyttäjät aikovat käyttää tuotetta tai palvelua loppukäyttöä koskevien ilmoitusten perusteella;

b) perehdyttävä tuotteiden asianomaisessa määräpaikassa vallitsevaan tilanteeseen, erityisesti yleiseen ihmisoikeustilanteeseen, koska se on tärkeä indikaattori vientiin liittyvästä ihmisoikeuksien ja kansainvälisen humanitaarisen oikeuden vakavien loukkausten riskistä;

c) tarkasteltava riskejä siitä, että alla lueteltujen varoitusmerkkien perusteella tuote tai palvelu siirretään toiselle hyväksymättömälle loppukäyttäjälle.

Varoitusmerkkejä:

a) loppukäyttäjällä on ilmeinen suhde ulkomaan hallitukseen, joka on syyllistynyt kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksien ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin;

b) loppukäyttäjä on rakenteellisesti osa asevoimia tai muuta ryhmää, joka on aiemmin osallistunut aseelliseen konfliktiin, johon on liittynyt kansallisia tukahduttamistoimia ja/tai ihmisoikeuksien ja kansainvälisen humanitaarisen oikeuden vakavia loukkauksia;

c) loppukäyttäjä on aiemmin vienyt verkkovalvontatuotteita maihin, joissa kyseisten tuotteiden käyttö on johtanut kansallisiin tukahduttamistoimiin ja/tai ihmisoikeuksien ja kansainvälisen humanitaarisen oikeuden vakaviin loukkauksiin.

3.4 **Laaditaan huolellisuusperiaatteen mukaisesti tehtyjen selvitysten perusteella suunnitelmia mahdollisten tulevien haitallisten vaikutusten ehkäisemiseksi ja lieventämiseksi**

Viejien olisi huolellisuusperiaatteen mukaisesti tehtyjen selvitystensä perusteella lopetettava toiminta, joka aiheuttaa tai edesauttaa ihmisoikeuksiin liittyviä haitallisia vaikutuksia, sekä laadittava ja pantava täytäntöön korjaavien toimien suunnitelma. Näitä toimia voivat olla seuraavat:

a) saatetaan yrityksen toimintaperiaatteet ajan tasalle niin, että niissä annetaan ohjeita siitä, miten haitallisia vaikutuksia jatkossa voidaan välttää ja käsitellä, ja varmistetaan niiden täytäntöönpano;

b) hyödynnetään riskinarvioinnin tuloksia hallintajärjestelmien päivittämisessä ja vahvistamisessa, jotta tietoja voidaan seurata paremmin ja varoitusmerkkejä tunnistaa jo ennen haitallisten vaikutusten ilmenemistä;

c) kerätään tietoa alaan liittyvien haitallisten vaikutusten korkean tason riskien ymmärtämiseksi;

d) ilmoitetaan jäsenvaltioiden toimivaltaisille viranomaisille huolellisuusperiaatteen mukaisesti tehtyjen selvitysten tuloksista, millä edistetään tiettyjä tuotteita, loppukäyttäjiä ja määräpaikkoja koskevaa tiedonkulkua.

Asetuksen (EU) 2021/821 5 artiklan 2 kohdassa säädetyt vaatimukset



4. **LISÄYS**

Asetuksen (EU) 2021/821 liitteen I mukaisesti valvottavat valvontaluetteloon sisältyvät verkkovalvontatuotteet

— **Telekuuntelujärjestelmät (5A001.f)**

Useimmissa valtioissa, myös jäsenvaltioissa, viestinnän luottamuksellisuus on turvattu lailla, mutta viranomaisten suorittama viestinnän sähköinen salaa tarkkailu voidaan sallia oikeudellisen kehyksen puitteissa (niin kutsuttu laillinen telekuuntelu). Digitaalinen aikakausi on tuonut mukanaan mahdollisuuden sieppausteknologioiden laajamittaiseen käyttöön. Sieppausvälineiden käyttö Libyan hallinnon toimesta on hyvä esimerkki siitä, että kyseisiä teknologioita on mahdollista käyttää myös laajamittaisesti, ja vauhditti telekuuntelujärjestelmien vientivalvonnan käyttöönottoa vuonna 2012.

Valvonta koskee laitteita, joilla on tarkoitus poimia viestinnän sisältöä (ääntä tai tietoja) sekä tilaajatunnisteita tai muita metatietoja, joita lähetetään langattomana viestintänä ilman kautta, sekä radiotaajuuksien valvontalaitteita. Valvonta koskee esimerkiksi IMSI-sieppareita (International Mobile Subscriber Identity eli kansainvälinen matkaviestintilaajan tunnus), jotka sieppaavat matkapuhelinliikenteen ja jäljittävät matkapuhelinten käyttäjien liikkeitä, tai laitteita, jotka luovat väärennettyjä Wi-Fi-tukiasemia, jotka voivat poimia puhelimesta IMSI-numeroita, sekä tietyntyyppisiä tuotteita, jotka on erityisesti suunniteltu mahdollistamaan pakettien syvätarkastus (DPI-tekniikka) televiestintäjärjestelmissä. Matkaviestinyhteyksien häirintälaitteet eivät kuulu verkkovalvontatuotteiden soveltamisalaan, koska ne eivät kerää tietoja.

Vaikka tällaisten järjestelmien valmistamiseen voidaan käyttää yleiskäyttöistä teknologiaa, järjestelmien valmiudet siepata viestintää laajassa mittakaavassa perustuvat tiettyihin osiin ja komponentteihin, kuten tiettyihin ohjelmistoihin tai kehittyneisiin tai sovelluskohtaisiin integroituihin piireihin (esim. FPGA, ASIC), joilla lisätään niiden pakettien tai viestintäistuntojen määrää, jotka voidaan käsitellä yhden sekunnin kuluessa.

— **Internetvalvontajärjestelmät (5A001.j)**

Vaikka monet internetpohjaiset tietoliikenneyhteydet salataan nykyisin oletusarvoisesti, viestintään liittyviä liikennetietoja (metatietoja) – kuten IP-osoitteita sekä tiedonsiirron säännöllisyyttä ja siirrettyjen tietojen kokoa – voidaan kuitenkin edelleen siepata henkilöiden ja verkkotunnusten välisten yhteyksien määrittämiseksi. Hallitukset saattavat käyttää näitä järjestelmiä laillisesti ja – oikeudellisen valvonnan tapauksessa – laillisiin tarkoituksiin, esimerkiksi niiden henkilöiden tunnistamiseen, jotka vierailevat rikolliseen tai terroristiseen sisältöön liittyvillä verkkosivustoilla. Etniseen, uskonnolliseen, poliittiseen tai sosiaaliseen profilointiin perustuva verkkoliikenteen seuranta ja analysointi voi kuitenkin johtaa valtiossa ihmisten ja yhteisöjen kattavaan kartoittamiseen väestön valvontaa ja sortoa ja muita tarkoituksia varten, esimerkiksi poliittisten toisinajattelijoiden tunnistamista varten. Ihmisoikeuksiin ja kansallisiin tukahduttamistoimiin liittyvien kysymysten lisäksi on otettava huomioon, että tuotteet voivat osaltaan lisätä turvallisuuspalvelujen valmiuksia ja sotilaallisia valmiuksia.

Kohdan 5A001.j mukainen valvonta koskee internetvalvontajärjestelmiä, jotka toimivat ”IP-runkoverkossa (esimerkiksi kansallisen tason IP-runkoverkko)” ja analysoivat, poimivat ja indeksoivat lähetettyjen metatietojen sisältöä (ääntä, videokuvaa, viestejä ja liitteitä) ”kiinteiden kriteereiden” perusteella ihmisten suhdeverkoston kartoittamiseksi. Nämä ovat tuotteita, joita käytetään ”salaa tarkkailuun”, koska kohteena olevat henkilöt eivät ole tietoisia viestinnän sieppauksesta. Valvontaa ei kuitenkaan ole tarkoitus soveltaa järjestelmiin, joissa käyttäjä tai tilaaja toteuttaa toimia tai käyttäjän tai tilaajan kanssa ollaan vuorovaikutuksessa, eikä valvonta siksi koske esimerkiksi sosiaalisia verkostoja tai kaupallisia hakukoneita. Valvontaa sovelletaan järjestelmiin, jotka käsittelevät internetpalveluntarjoajan runkoverkosta saatavia tietoja, eikä valvontaa sovelleta sosiaalisiin verkostoihin tai kaupallisiin hakukoneisiin, jotka käsittelevät käyttäjien antamia tietoja.

— **”Tunkeutumisohjelmistot” (4A005, 4D004 ja vastaava 4E001.a ja 4E001.c kohdan mukainen valvonta)**

Tunkeutumisohjelmiston avulla sen käyttäjä voi muodostaa salaa etäyhteyden elektroniseen laitteeseen, kuten älypuhelimeen, kannettavaan tietokoneeseen, palvelimeen tai esineiden internetin laitteeseen, saada laitteeseen tallennettuja tietoja, salakuunnella laitteeseen sisäänrakennetun tai siihen kytketyn kameran tai mikrofonin avulla ja hyödyntää laitetta hyökkäyksissä, joiden kohteena ovat muut laitteet, joihin kyseinen laite muodostaa yhteyden, tai käyttäjän kontaktit (”hakkerointi kolmannen osapuolen laitteiden kautta”). Vaikka tunkeutumisohjelmistoja voidaan käyttää myös laillisiin tarkoituksiin ([8]), mistä esimerkkinä ovat tietoteknisten yksiköiden etätukipalveluissa käytetyt ”etäyhteysohjelmistot”, tarkkailun salaisen luonteen ja mahdollisesti kerättyjen tietojen laajuuden takia on suuri riski siihen, että yksityisyyttä ja henkilötietojen suojaa koskevaa oikeutta loukataan, ja ohjelmistojen käyttö voi myös vakavasti heikentää oikeutta sananvapauteen.

([8]) Selvyyden vuoksi todetaan, että kaksikäyttöasetuksen liitteen I mukaisesti valvottavien luetteloon sisältyvien verkkovalvontatuotteiden vienti kolmansiin maihin edellyttäisi lupaa huolimatta siitä, onko niiden käyttö lainmukaista.

Kohdan 4A005 ym. mukainen valvonta koskee ohjelmistoja sekä järjestelmiä, laitteita, komponentteja ja niihin liittyviä teknologioita, jotka on erityisesti suunniteltu tai mukautettu ”tunkeutumisohjelmistojen” tuottamiseen, ohjaamiseen, hallintaan tai toimittamiseen, mutta se ei koske itse ”tunkeutumisohjelmistoja”, sellaisina kuin ne määritellään asetuksen liitteessä I. Näitä kybervälineitä valvotaan ottaen huomioon mahdolliset häiriöt ja vahingot, joita niiden onnistuneesta käytöstä ja toteutuksesta voi aiheutua, mutta valvonnan tarkoituksena ei ole vaikuttaa esimerkiksi kyberturvallisuuden tutkijoiden ja kyberturvallisuusalan toimintaan, koska niiden on voitava jakaa tunkeutumisohjelmistoihin liittyvää tietoa, jotta ne voivat kehittää tuotteilleen korjauksia ja saada ne käyttöön ennen haavoittuvuuden julkistamista.

— **Tietoliikenteen valvontaohjelmistot (5D001.e)**

Tämä ohjelmisto on suunniteltu kohdennettujen sieppaustoimenpiteiden avulla kerättyjen, viestintäpalvelun tarjoajalta pyydettyjen tietojen valvontaan ja analysointiin, jota tekee valtuutettu lainvalvontaviranomainen. Ohjelmisto mahdollistaa viestinnän sisällön tai metatietojen hakemisen ”kiinteiden kriteereiden” perusteella käyttämällä laillisen telekuuntelun rajapintaa sekä kohteena olevien yksittäisten henkilöiden suhdeverkoston kartoittamisen tai heidän liikkeidensä jäljittämisen hakutulosten perusteella. Ohjelmisto on tarkoitettu ”salaa tarkkailuun”, koska siinä käytetään viestintää sieppaamalla kerättyjä tietoja ilman, että henkilöt tietävät tarkkailusta. Lisäksi sillä ”analysoidaan” tietoja, joita on kerätty ”televiestintäjärjestelmistä”. Ohjelmisto asennetaan valtion viranomaiselle (esimerkiksi lainvalvontaviranomaisten valvontayksikölle), eikä valvonta koske laillisten sieppausjärjestelmien vaatimustenmukaisuusjärjestelmiä (esimerkiksi laillisten sieppausjärjestelmien hallintajärjestelmiä ja mediaattoreita), jotka on kehitetty kaupallisesti ja asennettu viestintäpalvelun tarjoajan tiloihin (esimerkiksi integroitu viestintäverkkoon) ja joita palveluntarjoaja käyttää ja ylläpitää. Kuten valvontaa koskevassa tekstissä selvennetään, valvonta ei koske ”ohjelmistoa”, joka on erityisesti suunniteltu tai muunnettu puhtaasti kaupallisiin tarkoituksiin, kuten laskutukseen, verkkopalvelujen laatuun (Quality of Service, QoS), käyttäjäkokemuksen laatuun (Quality of Experience, QoE), mediaattoreihin tai mobiilimaksu- tai pankkikäyttöön.

— **Salauksen analysointiin käytettävät tuotteet (5A004.a)**

Tämä valvonta koskee tuotteita, jotka on suunniteltu salausmekanismien estämiseksi, jotta voidaan selvittää luottamuksellisia muuttujia tai sensitiivistä tietoa, mukaan luettuna selväkielinen teksti, salasanat tai salausavaimet. Salauksella turvataan tiedon luottamuksellisuus siirron ja säilyttämisen aikana. Salauksen analysointia käytetään luottamuksellisuuden kumoamiseen, ja siksi tämä teknologia ”mahdollistaa” salaa tarkkailun seuraamalla, poimimalla, keräämällä tai analysoimalla tietoja tieto- ja televiestintäjärjestelmistä.

— **Rikostekniset välineet / tutkintavälineet (5A004.b, 5D002.a.3.b ja 5D002.c.3.b)**

Rikostekniset välineet / tutkintavälineet on suunniteltu poimimaan raakatietoa laitteesta (esimerkiksi tietojenkäsittely- tai viestintälaitteesta) niin, että tietoja ei voida muuttaa, ne eivät korruptoidu ja niitä voidaan käyttää oikeudellisiin tarkoituksiin eli rikostutkinnassa tai tuomioistuimessa. Nämä tuotteet kiertävät laitteen ”todentamis-” tai valtuutuskontrollin, jotta raakatieto voidaan poimia laitteesta. Näitä tuotteita käyttävät viranomaiset ja lainvalvontaviranomaiset, mutta myös sotilaalliset joukot, jotka poimivat ja analysoivat takavarikoitujen laitteiden tietoja. Lainmukaisista käyttötarkoituksista huolimatta tuotteita voidaan käyttää myös väärin, ja ne voivat siksi vaarantaa arkaluonteiset tai kaupalliset tiedot.

Rikostekniset välineet / tutkintavälineet, joita ei ole ”erityisesti suunniteltu” salaa tarkkailuun, eivät kuitenkaan kuulu 2 artiklan 20 kohdassa annetun verkkovalvontatuotteiden määritelmän soveltamisalaan. Valvontaa koskeva kohdan 5A004.b ym. teksti ei kata rikosteknisiä välineitä / tutkintavälineitä, jotka ainoastaan poimivat käyttäjätietoja, eikä tapauksia, joissa tietoja ei ole suojattu laitteella. Valvonta ei myöskään koske valmistajan tuotanto- tai testauslaitteita, järjestelmänvalvojille tarkoitettuja välineitä eikä tuotteita, jotka on tarkoitettu yksinomaan kaupalliseen vähittäismyyntiin, esimerkiksi matkapuhelinten lukituksen avaamiseen tarkoitettuja tuotteita. Kun otetaan huomioon tämäntyyppisten teknologioiden kirjo, valvonta sovelletaan kunkin tuotteen tapauskohtaisen arvion mukaan.

Lopuksi on syytä huomata, että asetuksen liitteessä I luetellaan muitakin valvontaan liittyviä tuotteita, joiden ei pitäisi katsoa kuuluvan verkkovalvontatuotteiden määritelmän soveltamisalaan. Näitä ovat esimerkiksi matkaviestinyhteyksien häirintälaitteet (5A001.f), jotka on suunniteltu tietoliikenteen tai järjestelmien vahingoittamiseen tai häiritsemiseen, järjestelmää muokkaavat tunkeutumisohjelmistot (4D004) sekä laserakustiset havainnointilaitteet (6A005.g), jotka keräävät äänidataa laserilla tai joiden avulla voidaan kuunnella keskusteluja etäältä (kutsutaan toisinaan ”lasermikrofoneiksi”). Samaan tapaan myöskään lueteltujen miehittämättömien ilma-alusten käyttö valvontatarkoituksiin ei tarkoita, että tuotteet kuuluisivat verkkovalvontatuotteiden määritelmän soveltamisalaan.