2024/2659

16.10.2024

# ODPORÚČANIE KOMISIE (EÚ) 2024/2659

## z 11. októbra 2024

## o usmerneniach o vývoze položiek kybernetického dohľadu podľa článku 5 nariadenia Európskeho parlamentu a Rady (EÚ) 2021/821

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 292,

keďže:

(1) Nariadením Európskeho parlamentu a Rady (EÚ) 2021/821 ([1]) sa stanovuje režim Únie na kontrolu vývozov, sprostredkovania, technickej pomoci, tranzitu a transferu položiek s dvojakým použitím.

(2) Nariadením (EÚ) 2021/821 sa rieši riziko používania položiek kybernetického dohľadu v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva.

(3) Podľa článku 5 ods. 2 a článku 26 ods. 1 nariadenia (EÚ) 2021/821 Komisia a Rada poskytnú vývozcom usmernenia, pokiaľ ide o položky kybernetického dohľadu, ktoré nie sú uvedené na zozname, vzhľadom na potrebu zabezpečiť efektívnosť režimu Únie na kontrolu vývozov, pokiaľ ide o kybernetickú bezpečnosť, a konzistentnosť vykonávania nariadenia (EÚ) 2021/821.

(4) Cieľom tohto odporúčania a k nemu pripojených usmernení je podporiť vývozcov pri vykonávaní kontrol položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, okrem iného vrátane opatrení náležitej starostlivosti na posúdenie rizík súvisiacich s vývozom takýchto položiek.

(5) Usmernenia pripojené k tomuto odporúčaniu boli v rokoch 2022 a 2023 predmetom rozsiahlych konzultácií v expertnej skupine pre technológie dohľadu a zohľadnili sa v nich pripomienky prijaté v rámci verejnej konzultácie ([2]), ktorá sa konala v druhom štvrťroku 2023.

(6) Treba pripomenúť, že toto odporúčanie a pripojené usmernenia nie sú záväzné. Vývozcovia by si preto mali zachovať zodpovednosť za plnenie svojich povinností podľa nariadenia (EÚ) 2021/821, zatiaľ čo Komisia by mala zabezpečiť, aby toto odporúčanie zostalo relevantné v priebehu času,

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2021/821 z 20. mája 2021, ktorým sa stanovuje režim Únie na kontrolu vývozov, sprostredkovania, technickej pomoci, tranzitu a transferu položiek s dvojakým použitím (Ú. v. EÚ 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.

PRIJALA TOTO ODPORÚČANIE:

Odporúča sa, aby príslušné orgány a vývozcovia z členských štátov pri plnení svojich povinností podľa článku 5 ods. 2 nariadenia (EÚ) 2021/821 zohľadnili usmernenia uvedené v prílohe k tomuto odporúčaniu.

V Bruseli 11. októbra 2024

*Za Komisiu*
Valdis DOMBROVSKIS
*výkonný podpredseda*

*PRÍLOHA*

**OBSAH**

*Strana*

Úvod ... 4

1. Príslušné právne ustanovenia, vymedzenia a kľúčové pojmy ... 4

1.1. Prehľad príslušných právnych ustanovení ... 4

1.2. Hlavné vymedzenia pojmov ... 5

1.2.1. „Osobitne navrhnuté“ ... 5

1.2.2. „Tajné sledovanie“ ... 6

1.2.3. „Fyzické osoby“ ... 6

1.2.4. „Monitorovanie, extrahovanie, zhromažďovanie, analýza údajov“ ... 6

1.2.5. „Z informačných a telekomunikačných systémov“ ... 7

1.2.6. „Informovanosť“ a „sú určené na“ ... 7

1.3. Vnútorná represia, závažné porušovanie ľudských práv a medzinárodného humanitárneho práva ... 7

1.3.1. Vnútorná represia ... 8

1.3.2. Závažné porušovanie ľudských práv ... 8

1.3.3. Závažné porušovanie medzinárodného humanitárneho práva ... 9

2. Technický rozsah pôsobnosti ... 9

2.1. Položky kybernetického dohľadu uvedené na zozname ... 9

2.2. Potenciálne položky kybernetického dohľadu, ktoré nie sú uvedené na zozname ... 9

2.2.1. Technológia rozpoznávania tváre a emócií ... 10

2.2.2. Zariadenia na sledovanie polohy ... 10

2.2.3. Systémy videomonitorovania ... 10

3. Opatrenia náležitej starostlivosti ... 10

Požiadavky stanovené v článku 5 ods. 2 nariadenia (EÚ) 2021/821 ... 12

4. Dodatok ... 12

Zoznam položiek kybernetického dohľadu, ktoré sa riadia prílohou I k nariadeniu (EÚ) 2021/821 ... 13

Telekomunikačné odpočúvacie systémy (5A001.f) ... 13

Systémy internetového sledovania (5A001.j) ... 13

„Narušiteľský softvér“ (4A005, 4D004 a súvisiace riadiace prvky podľa 4E001.a) a 4E001.c) ... 14

Softvér na monitorovanie komunikácie (5D001.e) ... 14

Položky používané na vykonávanie kryptoanalýzy (5A004.a) ... 14

Forenzné/vyšetrovacie nástroje (5A004.b, 5D002.a.3.b. a 5D002.c.3.b.) ... 15

## ÚVOD

Cieľom rámca Únie na kontrolu vývozu zriadeného nariadením (EÚ) 2021/821 (ďalej len „nariadenie“) je zabezpečiť dodržiavanie medzinárodných povinností a záväzkov Únie a jej členských štátov vrátane záväzkov týkajúcich sa mieru, bezpečnosti a stability v regióne a dodržiavania ľudských práv a medzinárodného humanitárneho práva. Únia a jej členské štáty preto vykonali rozhodnutia prijaté v rámci multilaterálnych režimov kontroly vývozu a zodpovedajúcim spôsobom aktualizovali kontrolný zoznam Únie uvedený v prílohe I k nariadeniu ([1]). Okrem toho predtým, ako sa začal uplatňovať článok 5 nariadenia, príslušné orgány členských štátov už kontrolovali vývoz určitých položiek uvedených na zozname, ktoré môžu mať uplatnenie pri dohľade ([2]), pričom zohľadnili riziká zneužitia za určitých osobitných okolností. V prípade mimoriadne závažných okolností Únia uložila sankcie obmedzujúce vývoz určitých sledovacích zariadení ([3]).

Nariadenie odzrkadľuje záväzok Únie účinne riešiť riziko používania položiek kybernetického dohľadu v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva. Nariadením sa zavádzajú najmä nové ustanovenia týkajúce sa kontroly vývozu položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, vrátane povinnosti vývozcov informovať príslušný orgán, ak si sú na základe svojich zistení v rámci náležitej starostlivosti vedomí, že položky kybernetického dohľadu, ktoré vývozcovia navrhujú vyvážať, sú vcelku alebo sčasti určené na použitie v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva. V nariadení sa ďalej vyzýva Komisia a Rada, aby poskytli vývozcom usmernenia na podporu účinného vykonávania nových kontrol položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname.

Cieľom týchto usmernení je preto podporiť vývozcov pri uplatňovaní kontrol položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, okrem iného vrátane opatrení náležitej starostlivosti, ktorými sa posudzujú riziká súvisiace s vývozom takýchto položiek koncovým používateľom a na koncové použitia podľa nových ustanovení nariadenia.

## 1. PRÍSLUŠNÉ PRÁVNE USTANOVENIA, VYMEDZENIA A KĽÚČOVÉ POJMY

### 1.1. Prehľad príslušných právnych ustanovení

V nariadení sa zavádzajú nové ustanovenia konkrétne stanovujúce kontroly vývozu položiek kybernetického dohľadu neuvedených v prílohe I k nariadeniu, ktoré sú alebo môžu byť určené vcelku alebo sčasti na použitie v súvislosti s vnútornou represiou a/alebo so závažným porušovaním ľudských práv a medzinárodného humanitárneho práva. Príslušné odôvodnenia a články sú:

a) odôvodnenie 8: „S cieľom zamedziť riziku, že niektoré z položiek kybernetického dohľadu neuvedených na zozname, ktoré sú vyvezené z colného územia Únie, môžu byť zneužité osobami, ktoré sú spoluzodpovedné alebo zodpovedné za riadenie alebo páchanie závažného porušovania ľudských práv alebo medzinárodného humanitárneho práva, je vhodné zaviesť kontrolu vývozu takýchto položiek. Súvisiace riziká sa týkajú najmä prípadov, keď sú položky kybernetického dohľadu cielene navrhnuté tak, aby umožnili narušenie alebo hĺbkovú kontrolu paketov

([1]) Pozri najmä kontroly týkajúce sa telekomunikačných odpočúvacích systémov (5A001.f), systémov internetového sledovania (5A001.j), narušiteľského softvéru (4A005, 4D004 a súvisiacich kontrol podľa 4E001.a a 4E001.c) a softvéru na monitorovanie zo strany orgánov presadzovania práva (5D001.e). Pozri ďalej, na základe individuálneho posúdenia, kontroly týkajúce sa určitých forenzných/vyšetrovacích nástrojov (5A004.b, 5D002.a.3.b a 5D002.c.3.b).

([2]) Najmä systémy informačnej bezpečnosti.

([3]) Pozri nariadenie Rady (ES) č. 765/2006 z 18. mája 2006 o reštriktívnych opatreniach vzhľadom na situáciu v Bielorusku a zapojenie Bieloruska do ruskej agresie voči Ukrajine (Ú. v. EÚ L 134, 20.5.2006, s. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj), nariadenie Rady (EÚ) č. 359/2011 z 12. apríla 2011 o reštriktívnych opatreniach voči určitým osobám, subjektom a orgánom s ohľadom na situáciu v Iráne (Ú. v. EÚ L 100, 14.4.2011, s. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj), nariadenie Rady (EÚ) č. 36/2012 z 18. januára 2012 o reštriktívnych opatreniach s ohľadom na situáciu v Sýrii, ktorým sa zrušuje nariadenie (EÚ) č. 442/2011 (Ú. v. EÚ L 16, 19.1.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj), nariadenie Rady (EÚ) č. 401/2013 z 2. mája 2013 o reštriktívnych opatreniach vzhľadom na situáciu v Mjanmarsku/Barme a o zrušení nariadenia (ES) č. 194/2008 (Ú. v. EÚ L 121, 3.5.2013, s. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj) a nariadenie Rady (EÚ) 2017/2063 z 13. novembra 2017 o reštriktívnych opatreniach vzhľadom na situáciu vo Venezuele (Ú. v. EÚ L 295, 14.11.2017, s. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

informačných a telekomunikačných systémov s cieľom vykonávať utajené sledovanie fyzických osôb monitorovaním, extrahovaním, zhromažďovaním alebo analýzou údajov, vrátane biometrických údajov, z týchto systémov. Položky používané na čisto komerčné účely, napríklad na fakturáciu, marketing, služby kvality, spokojnosť používateľov alebo bezpečnosť siete, sa vo všeobecnosti považujú za položky, ktoré nezahŕňajú takéto riziká.“;

b) odôvodnenie 9: „V záujme posilnenia účinnej kontroly vývozov položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, je nevyhnutné ďalej harmonizovať uplatňovanie univerzálnych kontrol v uvedenej oblasti. Členské štáty sú preto odhodlané podporovať takéto kontroly výmenou informácií medzi sebou a s Komisiou, najmä pokiaľ ide o technologický vývoj položiek kybernetického dohľadu, a ostražitým vykonávaním takýchto kontrol v záujme podpory výmeny na úrovni Únie.“;

c) v článku 2 ods. 20 sa stanovuje vymedzenie pojmu „položky kybernetického dohľadu“ ako „položky s dvojakým použitím osobitne navrhnuté tak, aby umožňovali tajné sledovanie fyzických osôb monitorovaním, extrahovaním, zhromažďovaním alebo analýzou údajov z informačných a telekomunikačných systémov“;

d) v článku 5 sa zavádza požiadavka na povolenie vývozu položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, ak vývozcu príslušný orgán informoval, že dané položky sú alebo môžu byť určené vcelku alebo sčasti na použitie v súvislosti s vnútornou represiou a/alebo so závažným porušovaním ľudských práv a medzinárodného humanitárneho práva (článok 5 ods. 1). Ďalej sa v ňom vyžaduje, aby vývozcovia upovedomili príslušný orgán, ak sú si podľa zistení z postupu náležitej starostlivosti vedomí, že položky sú vcelku alebo sčasti určené na použitie v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva (článok 5 ods. 2). Uvedený príslušný orgán rozhodne, či príslušný vývoz bude alebo nebude podliehať povoleniu, a

e) v článku 5 ods. 2 sa ďalej stanovuje, že „Komisia a Rada poskytnú vývozcom usmernenia, ako sa uvádza v článku 26 ods. 1“.

## 1.2. **Hlavné vymedzenia pojmov**

Nariadenie obsahuje osobitné odôvodnenia a ustanovenia, v ktorých sa objasňujú konkrétne pojmy relevantné pre kontroly vývozu položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname a sú dôležité na to, aby vývozcovia jasne porozumeli ustanoveniam s cieľom vykonávať náležitú starostlivosť a účinne vykonávať kontroly. Osobitne dôležité je, že článok 2 bod 20 stanovuje toto presné vymedzenie pojmu „položky kybernetického dohľadu“: *„položky s dvojakým použitím osobitne navrhnuté tak, aby umožňovali tajné sledovanie fyzických osôb monitorovaním, extrahovaním, zhromažďovaním alebo analýzou údajov z informačných a telekomunikačných systémov*“.

Na účely týchto usmernení by sa mali objasniť osobitné aspekty tohto vymedzenia.

### 1.2.1. *„Osobitne navrhnuté“*

Položka je určená na tajné sledovanie, ak sú jej technické vlastnosti vhodné na tajné sledovanie fyzických osôb a objektívne ho umožňujú. Pojem „osobitne navrhnutý“ preto znamená, že tajný dohľad nad fyzickými osobami musí byť hlavným účelom vývoja a návrhu výrobku. Takýto pojem však nevyžaduje, aby sa položka mohla používať výlučne na tajné sledovanie fyzických osôb.

Ako sa objasňuje v odôvodnení 8 nariadenia, položky používané na čisto komerčné účely, napríklad na fakturáciu, marketing, služby kvality, spokojnosť používateľov alebo bezpečnosť siete, nie sú osobitne navrhnuté na utajené sledovanie fyzických osôb, a preto nepatria do vymedzenia položiek kybernetického dohľadu. Napríklad, aj keď položky určené na sledovanie operačných systémov v priemysle alebo na monitorovanie prevádzky používateľov môžu byť použité na účely sledovania, tieto položky nie sú položkami kybernetického dohľadu podľa vymedzenia, pretože nie sú osobitne navrhnuté tak, aby umožňovali tajné sledovanie fyzických osôb.

1.2.2. *„Tajné sledovanie“*

Položky umožňujú tajné sledovanie, najmä ak sledovanie zjavne nie je pre dotknutú fyzickú osobu vnímateľné. Tak by to bolo v prípade, keď dotknuté osoby nevedia o prítomnosti a/alebo činnosti položiek kybernetického dohľadu, a teda nemajú možnosť vyhnúť sa tomuto sledovaniu alebo aspoň zodpovedajúcim spôsobom prispôsobiť svoje správanie. Aj keď sa sledovanie vykonáva prostredníctvom položiek namontovaných alebo prevádzkovaných vo verejnom priestore, získavanie údajov sa môže v určitých prípadoch považovať za relevantné pre utajené sledovanie, najmä zhromaždené údaje sa môžu odkloniť, vyhodnotiť alebo spracovať na iné účely, ako sú tie, o ktorých je dotknutá fyzická osoba informovaná. Inými slovami, ak fyzická osoba nemôže objektívne očakávať, že bude sledovaná, sledovanie možno považovať za tajné podľa článku 2 bodu 20 nariadenia.

1.2.3. *„Fyzické osoby“*

Pojem „fyzická osoba“ sa vzťahuje na živú ľudskú bytosť na rozdiel od právnickej osoby alebo subjektu, na ktoré sa preto ustanovenia nevzťahujú. Tento pojem sa nevzťahuje na dohľad nad predmetmi, miestami alebo strojmi ako takými.

1.2.4. *„Monitorovanie, extrahovanie, zhromažďovanie, analýza údajov“*

Podľa slovníka Oxford English Dictionary majú slová „monitorovanie, extrakcia, zhromažďovanie a analýza“ tento význam:

— „monitorovanie“: dohľad, sledovanie, odpočúvanie,

— „extrahovanie“: vytiahnutie,

— „zhromažďovanie“: získavanie, zber,

— „analýza“: rozlišovanie alebo zisťovanie prvkov niečoho (komplexného) s cieľom určenia jeho štruktúry alebo povahy, a teda vysvetlenia alebo pochopenia daného javu; podrobné a metodické preskúmanie na účely interpretácie; podrobenie kritickej alebo numerickej analýze.

Z týchto pojmov vyplýva, že položky používané na sledovanie by mali mať presné technické kapacity na spracovanie údajov s cieľom monitorovať, zhromažďovať, extrahovať alebo analyzovať údaje, ako sú napríklad tieto položky:

a) položky používané na monitorovanie údajov z informačných a telekomunikačných systémov ([4]) (napríklad veľkosť súboru alebo prenos paketov prenášaných v takomto systéme);

b) položky, ktoré extrahujú údaje z informačných a telekomunikačných systémov vniknutím a extrakciou (napríklad narušiteľský softvér);

c) položky, ktoré umožňujú analýzu údajov extrahovaných z informačných a telekomunikačných systémov vrátane tých, ktoré môžu spracúvať kamerové snímky uložené v týchto systémoch (napríklad určité typy technológií analýzy údajov používaných ako súčasť systémov rozpoznávania tváre).

Položky, ktoré sa používajú len na monitorovanie informačných systémov alebo sledovanie obyvateľstva prostredníctvom videokamier a ktoré umožňujú zachytiť konverzácie, výmeny údajov, pohyby a správanie jednotlivcov, nie sú položkami kybernetického dohľadu v rámci vymedzenia v nariadení, keďže nie sú osobitne navrhnuté na tento účel a musia pracovať s inými technológiami, ako je umelá inteligencia alebo veľké dáta. Celý systém (spolupracujúci s inými technológiami, ako je umelá inteligencia alebo technológie veľkých dát) by však mohol byť položkou kybernetického dohľadu podľa vymedzenia v článku 2 bode 20 nariadenia.

Dôležité je, že hoci sa uvádza niekoľko príkladov užitočných na ilustračné účely, vymedzenie a rozsah položiek kybernetického dohľadu nie sú týmito príkladmi obmedzené, keďže cieľom článku 5 je umožniť účinnú kontrolu vývozu položiek, ktoré nie sú uvedené na zozname.

([4]) Vymedzenie pojmu je uvedené ďalej v bode 1.2.5.

Ako vyplýva z použitia spojky „alebo“ vo vymedzení pojmu, uvedené technické spôsobilosti sa majú považovať za alternatívy a nie je potrebné, aby položka mala všetky tieto technické spôsobilosti na monitorovanie, extrakciu, zhromažďovanie alebo analýzu údajov. Inými slovami stačí, aby určitá položka mala jednu z týchto technických spôsobilostí, na ktorú sa vzťahuje vymedzenie položky kybernetického dohľadu v článku 2 bode 20.

1.2.5. *„Z informačných a telekomunikačných systémov“*

Tieto pojmy sa vzťahujú na systémy, ktoré elektronicky spracúvajú informácie, napríklad programovanie/kódovanie, prevádzku systému osobných počítačov (hardvér) a inú správu informácií vrátane softvérovej technológie, webovej technológie, počítačovej technológie, technológie ukladania atď., a na niektoré systémy, ktoré prenášajú informácie na diaľku, napríklad technické systémy, ktoré prenášajú zvuky, signály, texty, iné znaky, obrázky drôtovými aj bezdrôtovými kanálmi, optickými vláknami, rádiovým a iným elektromagnetickým systémom. Tieto dva pojmy spoločne zahŕňajú širokú škálu systémov na prenos alebo spracovanie informácií. Treba poznamenať, že tento pojem sa vzťahuje na systémy, a nie na zariadenia.

1.2.6. *„Informovanosť“ a „sú určené na“*

Podľa článku 5 ods. 2 nariadenia vývozca upovedomí príslušný orgán, ak si je vývozca *„vedomý toho, dané položky sú alebo môžu byť určené vcelku alebo sčasti na použitie v súvislosti s vnútornou represiou a/alebo so závažným porušovaním ľudských práv a medzinárodného humanitárneho práva“*.

Pojem „informovanosť“ nie je novým právnym pojmom, ale používa sa v súvislosti s požiadavkami na povolenia týkajúce sa konečného použitia (tzv. univerzálne kontroly) podľa článkov 4, 6, 7 a 8 nariadenia. „Informovaný“ znamená, že vývozca si je skutočne vedomý zamýšľaného zneužitia. Samotná možnosť takéhoto rizika nestačí na preukázanie informovanosti. Pojem „informovanosť“ však nie je možné zamieňať s pasivitou: vyžaduje, aby vývozca podnikol kroky na získanie dostatočných a primeraných informácií na hodnotenie rizík spojených s vývozom a na zaistenie súladu s nariadením.

Údaj, že položky musia byť „určené na“ relevantné citlivé konečné použitie znamená, že vývozca by mal posúdiť konečné použitie na individuálnom základe vzhľadom na osobitné okolnosti daného prípadu. Naproti tomu teoretické riziko, t. j. také, ktoré nie je založené na skutkovom posúdení veci, že položky by mohli byť použité spôsobom, ktorý porušuje ľudské práva, by nestačilo na to, aby z nich vyplývalo, že „sú určené“ na konkrétne zneužitie podľa článku 5.

1.3. **Vnútorná represia, závažné porušovanie ľudských práv a medzinárodného humanitárneho práva**

Podľa článku 15 nariadenia, v ktorom sa uvádzajú úvahy na posúdenie poverenia, majú členské štáty zohľadniť všetky relevantné aspekty vrátane tých, na ktoré sa vzťahuje spoločná pozícia Rady 2008/944/SZBP ([5]).

Článkom 5 nariadenia sa rozširujú kontroly na vývoz položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, vzhľadom na riziko, že sa použijú v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva. V tejto súvislosti poskytuje užitočné usmernenie spoločná pozícia 2008/944/SZBP a používateľská príručka k tejto spoločnej pozícii ([6]).

([5]) Spoločná pozícia Rady 2008/944/SZBP z 8. decembra 2008, ktorou sa vymedzujú spoločné pravidlá upravujúce kontrolu vývozu vojenskej technológie a materiálu (Ú. v. EÚ L 335, 13.12.2008, s. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Pozri Používateľskú príručku k spoločnej pozícii Rady 2008/944/SZBP, ktorou sa vymedzujú spoločné pravidlá upravujúce kontrolu vývozu vojenskej technológie a materiálu, https://data.consilium.europa.eu/doc/document/ST-12189-2019-INIT/sk/pdf.

1.3.1. *Vnútorná represia*

Podľa článku 2 ods. 2 spoločnej pozície Rady 2008/944/SZBP *„vnútorná represia okrem iného zahŕňa mučenie a iné kruté, neľudské a ponižujúce zaobchádzanie alebo trestanie, hromadné alebo svojvoľné popravy, zmiznutia, svojvoľné zadržania a iné vážne porušovanie ľudských práv a základných slobôd, ktoré sú uvedené v príslušných medzinárodných nástrojoch v oblasti ľudských práv vrátane Všeobecnej deklarácie ľudských práv a Medzinárodného paktu o občianskych a politických právach“*. V používateľskej príručke k spoločnej pozícii 2008/944/SZBP sa uvádzajú usmernenia týkajúce sa prvkov, ktoré sa majú zohľadniť pri hodnotení vývozcu, vrátane otázky, či *„navrhovaný koncový používateľ a prijímajúca krajina vo všeobecnosti dodržiavajú a dodržiavali ľudské práva“*.

1.3.2. *Závažné porušovanie ľudských práv*

Zneužívanie položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, môže mať negatívny vplyv na široké spektrum ľudských práv a priamo zasahuje do práva na súkromie a ochranu údajov. Svojvoľné alebo nezákonné sledovanie môže porušovať aj iné ľudské práva, ako je právo na slobodu prejavu, združovania a zhromažďovania, slobodu myslenia, svedomia a náboženského vyznania, ako aj právo na rovnaké zaobchádzanie alebo zákaz diskriminácie a právo na slobodné, rovnoprávne a tajné voľby. Sledovanie vrátane monitorovania alebo zhromažďovania informácií fyzických osôb, ako sú obhajcovia ľudských práv, aktivisti, politické osobnosti, zraniteľní obyvatelia a novinári, môže v konkrétnych prípadoch viesť k zastrašovaniu, potláčaniu, svojvoľnému zadržiavaniu, mučeniu alebo dokonca k mimosúdnym popravám. Vývozcovia by preto mali tieto aspekty týkajúce sa závažného porušovania ľudských práv zahrnúť do svojich hodnotení.

Medzinárodná prax ukazuje, že akékoľvek obmedzenia ľudských práv musia byť „primerané“ a v súlade s medzinárodnými normami v oblasti ľudských práv. V praxi to znamená, že sú zavedené primerané záruky na zabezpečenie toho, aby boli obmedzenia stanovené zákonom a aby sa zachovala podstata práv. Za predpokladu dodržiavania zásady proporcionality možno obmedzenia stanoviť len vtedy, ak je to nevyhnutné a skutočne slúžia legitímnemu účelu, napríklad národnej alebo verejnej bezpečnosti, verejnému poriadku, ochrane verejného zdravia alebo ochrane práv a slobôd iných.

Položky kybernetického dohľadu môžu zahŕňať legitímne a regulované nástroje na účely presadzovania práva, napríklad na predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie, a to aj v oblasti boja proti terorizmu, alebo na výkon trestných sankcií. Zároveň sa položky kybernetického dohľadu môžu zneužiť aj na závažné porušovanie ľudských práv a medzinárodného humanitárneho práva pri vývoze do represívnych režimov alebo súkromným koncovým používateľom a/alebo do konfliktných oblastí.

Vyžaduje si to individuálne posúdenie okolností prípadu vrátane uplatňovania príslušných predpisov vzhľadom na všetky správy o závažnom porušovaní ľudských práv od príslušných orgánov, napríklad Organizácie Spojených národov, Únie alebo Rady Európy. „Závažnosť“ porušovania ľudských práv možno vyvodiť z uznania týchto porušení v informáciách uverejnených príslušnými orgánmi Organizácie Spojených národov, Úniou alebo Radou Európy. Nejde o absolútnu nevyhnutnosť takéhoto výslovného uznania týmito orgánmi, ale predstavuje významný faktor na splnenie kritérií.

Podľa článku 5 musí byť porušovanie ľudských práv „závažné“. Užitočné usmernenia na kategorizáciu možného porušovania ľudských práv ako „závažného“ možno nájsť v Užívateľskej príručke k spoločnej pozícii 2008/944/SZBP. Podľa uvedenej príručky má povaha a dôsledky porušenia rozhodujúci význam. Systematické a/alebo rozsiahle porušovanie ľudských práv sa pravidelne považuje za závažné, ale aj porušenia, ktoré nie sú systematické alebo rozšírené, sa môžu považovať za „závažné“, napríklad z dôvodu závažnosti zásahu pre dotknuté osoby.

V prílohe II k Užívateľskej príručke k spoločnej pozícii 2008/944/SZBP sa uvádza neúplný zoznam hlavných medzinárodných a regionálnych nástrojov v oblasti ľudských práv vrátane Medzinárodného paktu o občianskych a politických právach (ICCPR), Dohovoru proti mučeniu a inému krutému, neľudskému alebo ponižujúcemu zaobchádzaniu alebo trestaniu, Európskeho dohovoru o ľudských právach (ďalej len „dohovor“) a Charty základných práv (ďalej len „charta“), ktoré môžu poskytnúť dôležité usmernenie pre výklad a uplatňovanie kritérií na podporu dôkladného hodnotenia ľudských práv. Tieto nástroje a ich príslušné dodatkové protokoly predstavujú hlavné medzinárodné normy v oblasti ľudských práv a základných slobôd.

1.3.3. *Závažné porušovanie medzinárodného humanitárneho práva*

Medzinárodné humanitárne právo (nazývané aj „ženevské právo“ alebo „vojnové právo“) bolo vytvorené prostredníctvom celého radu medzinárodných zmlúv, predovšetkým Haagskych dohovorov, Ženevských dohovorov a ich dvoch dodatkových protokolov z roku 1977, a určujú sa v ňom pravidlá, ktoré v čase ozbrojeného konfliktu slúžia na ochranu ľudí, ktorí sa nezúčastňujú alebo sa už nezúčastňujú na nepriateľských akciách (napríklad civilistov a zranených, chorých alebo zadržaných bojovníkov) a ukladajú bojujúcim stranám obmedzenia, pokiaľ ide o prostriedky a metódy vojny (haagske právo).

Používanie položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, by malo byť v súlade s medzinárodným humanitárnym právom, keď sa nasadzujú ako prostriedky a metódy vedenia vojny v kontexte ozbrojeného konfliktu. Za takýchto okolností sa riziko závažného porušovania medzinárodného humanitárneho práva zvažuje podľa nariadenia a pokiaľ ide o spáchanie závažného porušovania ľudských práv, malo by sa posudzovať z hľadiska zamýšľaného konečného použitia položiek v konkrétnom prípade. V Užívateľskej príručke k spoločnej pozícii 2008/944/SZBP sa uvádzajú usmernenia týkajúce sa prvkov, ktoré sa majú zohľadniť, vrátane minulých i súčasných záznamov príjemcu v súvislosti s dodržiavaním medzinárodného humanitárneho práva, zámerov príjemcu vyjadrených prostredníctvom formálnych záväzkov a spôsobilosti príjemcu zabezpečiť, že sa technológia alebo vybavenie na transfer použijú v súlade s medzinárodným humanitárnym právom a že sa nepoužijú na iné účely ani sa neuskutoční ich transfer na iné miesta určenia, kde by sa mohli použiť na závažné porušenie tohto práva.

Podľa článku 5 musí byť porušenie medzinárodného humanitárneho práva „závažné“. Usmernenie možno nájsť v Užívateľskej príručke k spoločnej pozícii 2008/944/SZBP, v ktorej sa uznáva, že „izolované prípady porušenia medzinárodného humanitárneho práva nemusia vždy naznačovať postoj prijímajúcej krajiny k medzinárodnému humanitárnemu právu“, zatiaľ čo „vážne obavy by malo vyvolať, ak je možné pozorovať určité vzorce porušovania alebo ak prijímajúca krajina neprijala príslušné opatrenia na potrestanie porušenia“. Medzinárodný výbor Červeného kríža (MVČK) poskytol usmernenia týkajúce sa posudzovania porušovania medzinárodného humanitárneho práva na účely kontroly vývozu. Podľa Medzinárodného výboru Červeného kríža „porušenia medzinárodného humanitárneho práva sú závažné, ak ohrozujú chránené osoby (napríklad civilistov, vojnových zajatcov, zranených a chorých) alebo objekty (napríklad civilné objekty alebo infraštruktúru) alebo ak porušujú dôležité univerzálne hodnoty“. Napríklad vojnové zločiny predstavujú závažné porušenie medzinárodného humanitárneho práva. MVČK ďalej uvádza ďalšie faktory, ktoré sa majú zvážiť, ako Užívateľskú príručku k spoločnej pozícii 2008/944/SZBP vrátane formálnych záväzkov uplatňovať pravidlá medzinárodného humanitárneho práva, primeraných opatrení na zabezpečenie zodpovednosti za porušovanie medzinárodného humanitárneho práva, výcviku armády v oblasti medzinárodného humanitárneho práva a zákazu náboru detí do ozbrojených síl.

## 2. TECHNICKÝ ROZSAH PÔSOBNOSTI

### 2.1. Položky kybernetického dohľadu uvedené na zozname

V dodatku k týmto usmerneniam sa uvádzajú informácie o položkách kybernetického dohľadu uvedených v prílohe I k nariadeniu s cieľom pomôcť vývozcom pri identifikácii potenciálnych položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname.

### 2.2. Potenciálne položky kybernetického dohľadu, ktoré nie sú uvedené na zozname

Hoci zo svojej podstaty nie je možné poskytnúť vyčerpávajúci zoznam tých výrobkov, ktoré možno kontrolovať ako položky, ktoré nie sú uvedené na zozname podľa článku 5, tieto položky by mohli mať potenciál využitia na sledovanie a môžu si vyžadovať osobitnú ostražitosť podľa nariadenia.

Ako sa objasňuje v odôvodnení 8 nariadenia, položky používané na čisto komerčné účely, napríklad na fakturáciu, marketing, služby kvality, spokojnosť používateľov alebo bezpečnosť siete, sa vo všeobecnosti považujú za položky, ktoré nezahŕňajú riziká zneužitia relevantné v rámci závažného porušovania ľudských práv alebo medzinárodného humanitárneho práva, a preto vo všeobecnosti nepodliehajú kontrole podľa článku 5. Mnohé z týchto položiek majú funkcie informačnej bezpečnosti (kryptografické alebo dokonca kryptoanalytické), ktoré spĺňajú kontrolné parametre podľa kategórie 5 časti 2 kontrolného textu v prílohe I k nariadeniu. Bezpečnostné sieťové zariadenia vrátane smerovačov, prepínačov alebo relé, pri ktorých je funkcia informačnej bezpečnosti obmedzená na úlohy „prevádzky, správy alebo údržby“, v ktorých sú implementované len zverejnené alebo komerčné kryptografické štandardy, nie sú zachytené ani vo vymedzení pojmu „položky kybernetického dohľadu“, hoci vývozcovia by mali zostať obozretní pri posudzovaní rôznych správ o zneužití takýchto položiek na porušovanie ľudských práv.

2.2.1. *Technológia rozpoznávania tváre a emócií*

Technológie rozpoznávania tváre a emócií majú viaceré použitia okrem kybernetického dohľadu, napríklad na identifikáciu alebo autentifikáciu, a toto vymedzenie by sa na ne automaticky nevzťahovalo. Za určitých okolností však technológie rozpoznávania tváre a emócií môžu patriť do rozsahu pôsobnosti článku 2 bodu 20 nariadenia.

Technológie rozpoznávania tváre a emócií, ktoré možno použiť na monitorovanie alebo analýzu uložených obrazov, by mohli patriť do rozsahu vymedzenia položky kybernetického dohľadu. Aj keď sú uvedené kritériá splnené, je však potrebné dôkladne preskúmať, či je softvér špeciálne navrhnutý na tajné sledovanie.

2.2.2. *Zariadenia na sledovanie polohy*

Zariadenia na sledovanie polohy umožňujú sledovanie fyzickej polohy zariadenia v priebehu času a niektoré technológie sledovania polohy už určitý čas používajú orgány presadzovania práva a spravodajské služby. Ich potenciál cieleného a hromadného sledovania sa značne rozvinul, keďže technológie sledovania sa stali vyspelejšími, vrátane satelitného sledovania polohy, sledovania polohy na základe stožiarov s mobilnými vysielačmi, vysielačov Wi-Fi a Bluetooth, a keďže sa rozšírili „sledovacie zariadenia“, ako sú smartfóny a iné elektronické zariadenia (napríklad palubné systémy v automobiloch).

Zariadenia na sledovanie polohy používajú orgány presadzovania práva a spravodajské orgány napríklad na zhromažďovanie dôkazov v priebehu vyšetrovania alebo na sledovanie podozrivých osôb, ale aj spoločnosti na komerčné účely, napríklad na podávanie správ o agregovaných modeloch pohybu v nákupných uliciach, sledovanie zamestnancov pracujúcich mimo pracoviska alebo na lokalizovanú reklamu.

2.2.3. *Systémy videomonitorovania*

S cieľom pomôcť vývozcom identifikovať potenciálny kybernetický dohľad je tiež užitočné objasniť, na ktoré položky by sa vymedzenie pojmu nevzťahovalo. V tomto zmysle sa napríklad na systémy videomonitorovania a kamery – vrátane kamier s vysokým rozlíšením – používané na filmovanie ľudí na verejných priestranstvách nevzťahuje definícia položiek kybernetického dohľadu, pretože nemonitorujú ani nezbierajú údaje z informačných a telekomunikačných systémov.

## 3. OPATRENIA NÁLEŽITEJ STAROSTLIVOSTI

Podľa odôvodnenia 7 nariadenia *„zásadný význam má prínos vývozcov […] k celkovému cieľu, ktorým je kontrola obchodu. Aby mohli konať v súlade s týmto nariadením, posudzovanie rizík súvisiacich s transakciami, na ktoré sa vzťahuje toto nariadenie, sa má vykonávať prostredníctvom opatrení na preverovanie transakcií, ktoré sú známe aj ako zásada náležitej starostlivosti, ako časť programu vnútorného súladu“*.

V článku 2 bode 21 sa program vnútorného súladu vymedzuje ako *„nepretržité účinné, náležité a primerané politiky a postupy prijaté vývozcami na zabezpečenie súladu s ustanoveniami a cieľmi tohto nariadenia a s podmienkami povolení zavedených podľa tohto nariadenia, vrátane okrem iného opatrení náležitej starostlivosti na posúdenie rizík súvisiacich s vývozom položiek koncovým používateľom a ich konečným použitím“*.

Odporúčanie Komisie (EÚ) 2019/1318 ([7]) predstavuje rámec, ktorý vývozcom pomôže identifikovať, riadiť a zmierňovať riziká spojené s kontrolami obchodovania s položkami s dvojakým použitím a zabezpečiť súlad s príslušnými právnymi predpismi EÚ a jednotlivých členských štátov.

Tieto usmernenia môžu podporovať vývozcov pri vykonávaní opatrení na preverovanie transakcií známych aj ako zásada náležitej starostlivosti ako súčasť programu vnútorného súladu.

Podľa článku 5 ods. 2 nariadenia (EÚ) 2021/821 sa od vývozcov položiek kybernetického dohľadu, ktoré nie sú uvedené na zozname, vyžaduje, aby vykonali náležitú starostlivosť prostredníctvom opatrení na preverovanie transakcií, čo znamená prijatie krokov týkajúcich sa klasifikácie položiek a posúdenia rizika transakcií. V praxi sa vývozcom odporúča, aby:

([7]) Odporúčanie Komisie (EÚ) 2019/1318 z 30. júla 2019 o interných programoch dodržiavania pravidiel, pokiaľ ide o kontroly obchodovania s položkami s dvojakým použitím podľa nariadenia (ES) č. 428/2009 (Ú. v. EÚ L 205, 5.8.2019, s. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Preskúmali, či položka, ktorá nie je uvedená na zozname, môže byť „položka kybernetického dohľadu“, teda osobitne navrhnutá tak, aby umožňovala tajné sledovanie fyzických osôb monitorovaním, extrahovaním, zhromažďovaním alebo analýzou údajov z informačných a telekomunikačných systémov.**

Tento krok sa týka určenia položky podľa ustanovení, ktoré sa vzťahujú na položky kybernetického dohľadu. To zahŕňa preskúmanie technických charakteristík položiek na základe technických parametrov stanovených v prílohe I k nariadeniu pre uvedené položky a vzhľadom na osobitné pojmy a pojmy vo vymedzení položiek kybernetického dohľadu pre položky, ktoré nie sú uvedené na zozname, a na následnú klasifikáciu položky (tovar, technológia alebo softvér).

3.2. **Preskúmali schopnosti danej položky určiť možnosť zneužitia v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva zahraničnými koncovými používateľmi.**

Vývozcovia by mali vykonať posúdenie s cieľom určiť, či by sa výrobok mohol zneužiť na vnútornú represiu, porušovanie alebo zneužívanie ľudských práv vrátane práva na život, ochrany pred mučením, neľudským a ponižujúcim zaobchádzaním, práva na súkromie, práva na slobodu prejavu, združovania a zhromažďovania, práva na slobodu myslenia, svedomia a náboženského vyznania, práva na rovnaké zaobchádzanie alebo zákazu diskriminácie, alebo práva na slobodné, rovnoprávne a tajné voľby.

Zahŕňa aj posúdenie s cieľom určiť, či by sa výrobok mohol použiť ako súčasť alebo komponent systému, ktorý by mohol viesť k rovnakým porušeniam a/alebo zneužitiu.

Vývozcovia by pri posudzovaní mali používať tzv. varovné signály, ktoré odkazujú na akékoľvek abnormálne okolnosti pri transakcii, ktoré naznačujú, že vývoz môže byť určený na nevhodné konečné použitie, pre nevhodného konečného používateľa alebo na nevhodné miesto určenia.

Varovné signály:

a) položka sa uvádza na trh s informáciami týkajúcimi sa jej možného použitia na tajné sledovanie;

b) informácie naznačujúce, že podobná položka bola zneužitá v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva (pozri bod 1.3);

c) informácie o tom, že položka bola nezákonne použitá na sledovanie zamerané proti členskému štátu alebo v súvislosti s nezákonným sledovaním občana EÚ;

d) informácie o tom, že transakcia zahŕňa položky, ktoré by sa mohli použiť na zriadenie, prispôsobenie alebo konfiguráciu systému, o ktorom je známe, že sa zneužíva v súvislosti s vnútornou represiou a/alebo závažným porušovaním ľudských práv a medzinárodného humanitárneho práva (pozri bod 1.3);

e) položka alebo podobná položka sa nachádza na zozname uverejnenom v sérii C *Úradného vestníka Európskej únie* v súlade s článkom 5 ods. 6 nariadenia.

3.3. **Na podporu príslušných orgánov preskúmali zainteresované strany zapojené do transakcie (vrátane koncových používateľov a príjemcov, ako sú distribútori a ďalší predajcovia).**

Vývozcovia by mali na podporu príslušných orgánov a v možnom rozsahu:

a) pred každou transakciou a počas nej preskúmať, ako príjemcovia a/alebo koncoví používatelia zamýšľajú používať výrobok alebo službu na základe vyhlásení o konečnom použití;

b) oboznámiť sa so situáciou v príslušnom mieste určenia položiek, najmä so všeobecným stavom ľudských práv, keďže to predstavuje dôležitý ukazovateľ rizika závažného porušovania ľudských práv a medzinárodného humanitárneho práva v súvislosti s vývozom;

c) preskúmať riziká, že výrobok alebo služba budú presmerované na iného neoprávneného koncového používateľa na základe varovných signálov uvedených nižšie.

Varovné signály:

a) koncový používateľ má zjavný vzťah so zahraničnou vládou, ktorá sa preukázateľne dopúšťa vnútornej represie a/alebo závažného porušovania ľudských práv a medzinárodného humanitárneho práva;

b) koncový používateľ je štrukturálne súčasťou ozbrojených síl alebo inej skupiny zapojenej do ozbrojeného konfliktu zahŕňajúceho vnútorné represie a/alebo závažné porušovanie ľudských práv a medzinárodného humanitárneho práva v minulosti;

c) koncový používateľ v minulosti vyvážal položky kybernetického dohľadu do krajín, v ktorých použitie takýchto položiek viedlo k opatreniam vnútornej represie a/alebo k závažnému porušovaniu ľudských práv a medzinárodného humanitárneho práva.

3.4. **Využiť zistenia náležitej starostlivosti na vypracovanie plánov na predchádzanie potenciálnym nepriaznivým vplyvom v budúcnosti a ich zmiernenie.**

Vývozcovia by mali na základe svojich zistení v oblasti náležitej starostlivosti ukončiť činnosti, ktoré spôsobujú nepriaznivé vplyvy súvisiace s ľudskými právami alebo k nim prispievajú, ako aj vypracovať a vykonávať plán nápravných opatrení. Tieto činnosti môžu zahŕňať:

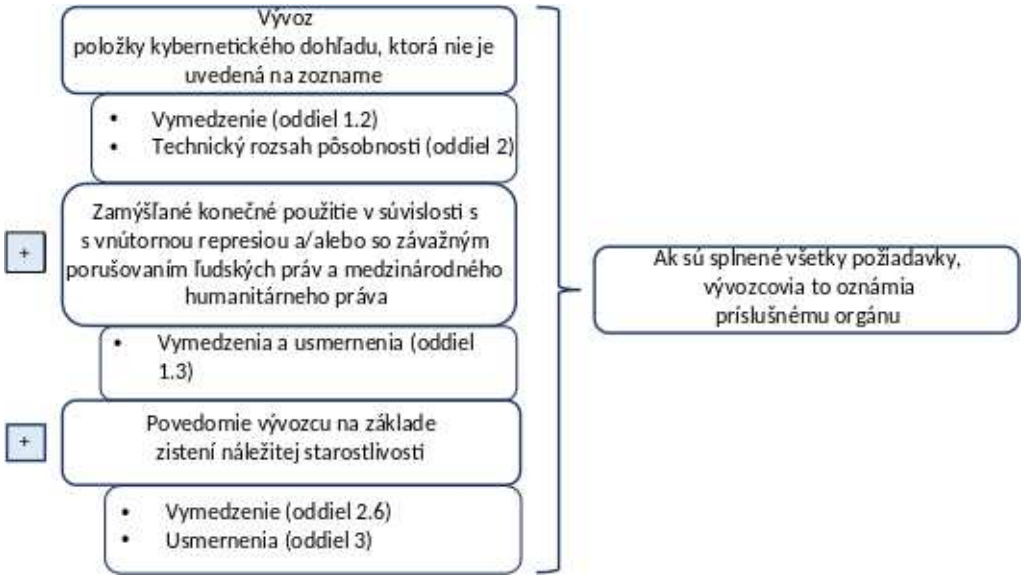
a) aktualizáciu podnikových politík s cieľom poskytnúť usmernenia o tom, ako predchádzať nepriaznivým vplyvom a riešiť ich v budúcnosti a zabezpečiť ich vykonávanie;

b) čerpanie zo zistení posúdenia rizík s cieľom aktualizovať a posilniť systémy riadenia s cieľom lepšie sledovať informácie a označovať riziká pred výskytom nepriaznivých vplyvov;

c) zhromažďovanie informácií s cieľom pochopiť vysoké riziká nepriaznivých vplyvov súvisiacich s odvetvím;

d) informovanie príslušných orgánov členských štátov o zisteniach náležitej starostlivosti s cieľom uľahčiť tok informácií, pokiaľ ide o určité položky, koncových používateľov a miesta určenia.

**Požiadavky stanovené v článku 5 ods. 2 nariadenia (EÚ) 2021/821**




4. **DODATOK**

**Zoznam položiek kybernetického dohľadu, ktoré sa riadia prílohou I k nariadeniu I k nariadeniu (EÚ) 2021/821**

— **Odpočúvacie telekomunikačné systémy (5A001.f)**

Vo väčšine krajín vrátane členských štátov je dôvernosť komunikácie chránená zákonom, ale tajné elektronické sledovanie komunikácie vládnymi orgánmi môže byť povolené v právnom rámci (tzv. zákonné odpočúvanie). Digitálna éra však priniesla možnosť využívať technológie odpočúvania v masovom meradle. Využívanie nástrojov na odpočúvanie zo strany líbyjského režimu poukázalo na potenciál zaviesť tieto technológie vo veľkom rozsahu a podnietilo zavedenie kontrol vývozu telekomunikačných odpočúvacích systémov v roku 2012.

Táto kontrola sa vzťahuje na zariadenia určené na extrakciu obsahu komunikácie (hlasovej alebo dátovej), ako aj na identifikátory zákazníkov alebo iné metaúdaje, ktoré sa prenášajú vzduchom prostredníctvom bezdrôtovej komunikácie, a na zariadenia na monitorovanie rádiových frekvencií. Táto kontrola sa vzťahuje napríklad na vybavenie na monitorovanie medzinárodného identifikačného kódu mobilných účastníkov (IMSI), ktoré zachytáva komunikáciu mobilných telefónov a sleduje pohyb používateľov mobilných telefónov, alebo na zariadenia vytvárajúce falošné Wi-Fi hotspoty, ktoré môžu extrahovať čísla IMSI z telefónu, ako aj na určité typy položiek osobitne navrhnutých tak, aby umožňovali hĺbkovú kontrolu paketov v telekomunikačných systémoch. Zariadenia na rušenie mobilných telekomunikácií nepatria do rozsahu položiek kybernetického dohľadu, pretože nezbierajú údaje.

Hoci na vybudovanie takýchto systémov možno použiť univerzálnu technológiu, ich schopnosť zachytávania v masovom meradle sa bude opierať o konkrétne časti a komponenty vrátane napríklad špecifického softvéru, pokročilých integrovaných obvodov alebo integrovaných obvodov pre špecifické použitie (napríklad FPGA, ASIC atď.) na zvýšenie počtu paketov alebo komunikačných relácií, ktoré možno spracovať za sekundu.

— **Systémy internetového sledovania (5A001.j.)**

Hoci väčšina internetovej komunikácie je v súčasnosti zvyčajne šifrovaná štandardne, zachytávanie prevádzkových údajov (metaúdajov) o komunikácii, ako sú IP adresy a frekvencia a veľkosť výmeny údajov, sa stále môže používať na identifikáciu prepojení medzi osobami a názvami domén. Vlády môžu tieto systémy používať zákonne a pod súdnym dohľadom na legitímne účely, ako je identifikácia osôb, ktoré navštevujú domény spojené s trestným alebo teroristickým obsahom. Monitorovanie a analýza internetovej prevádzky na základe etnickej, náboženskej, politickej alebo sociálnej charakteristiky však môže viesť ku komplexnému ľudskému a sociálnemu mapovaniu krajiny na účely kontroly obyvateľstva a represií, ako aj na iné účely, napríklad na identifikáciu politických disidentov. Okrem otázok týkajúcich sa ľudských práv a vnútornej represie môžu tieto položky prispieť aj k posilneniu bezpečnostných a vojenských spôsobilostí.

Kontrola podľa bodu 5A001.j) sa vzťahuje na systémy kontroly internetu, ktoré fungujú v carrier class IP sieťach (napríklad chrbticová IP sieť na celoštátnej úrovni) na vykonávanie analýzy, extrakcie a indexácie prenášaného obsahu metaúdajov (hlas, video, správy, prílohy) na základe pevných selektorov (hard selectors) a mapovanie vzťahovej siete ľudí. Ide o položky, ktoré vykonávajú tajné sledovanie, pretože cieľové osoby nevedia o odpočúvaní komunikácie. Naopak, kontroly nie sú zamerané na systémy, v ktorých existuje činnosť alebo interakcia s používateľom alebo účastníkom a ktoré sa napríklad nevzťahujú na sociálne siete alebo komerčné vyhľadávače. Okrem toho sa kontroly vzťahujú na systémy, ktoré spracúvajú údaje pochádzajúce z chrbticovej siete poskytovateľa internetu a nevzťahujú sa na sociálne siete alebo komerčné vyhľadávače, ktoré spracúvajú údaje poskytnuté používateľmi.

— **„Narušiteľský softvér“ (4A005, 4D004 a súvisiace kontroly podľa 4E001. a a 4E001.c)**

Narušiteľský softvér umožňuje svojmu operátorovi skryte získať vzdialený prístup k elektronickému zariadeniu, ako je smartfón, laptop, server alebo zariadenie internetu vecí, získať údaje uložené v zariadení, odpočúvať prostredníctvom kamery alebo mikrofónu zabudovaného alebo pripojeného k zariadeniu a používať zariadenie ako odrazový mostík na vykonanie útokov na zariadenie, ku ktorému sa zariadenie pripája, alebo proti kontaktom používateľa (hackerské útoky cez zariadenia tretích strán). Hoci existuje legitímne použitie ([8]) narušiteľského softvéru, napríklad softvéru na vzdialený prístup používaného IT oddeleniami na podporu na diaľku, utajená povaha sledovania a rozsah informácií, ktoré sa môžu zhromaždiť, predstavujú vysoké riziko porušenia práva na súkromie a ochranu osobných údajov a môžu vážne ohroziť právo na slobodu prejavu.

([8]) V záujme jasnosti by položky kybernetického dohľadu, ktoré sa riadia prílohou I k nariadeniu o položkách s dvojakým použitím potrebovali povolenie na vývoz do tretích krajín bez ohľadu na to, či je použitie položky legitímne.

Kontrola podľa bodu 4A005 a ostatných zahŕňa softvér, ako aj systémy, zariadenia, súčasti a súvisiace technológie osobitne navrhnuté alebo upravené na tvorbu, ovládanie a riadenie alebo dodávanie narušiteľského softvéru, ale nevzťahuje sa na samotný narušiteľský softvér vymedzený v prílohe I k nariadeniu. Tieto kybernetické nástroje sa kontrolujú s ohľadom na možné narušenie a škody, ktoré môžu spôsobiť, ak sa používajú a úspešne vykonávajú, ale cieľom kontrol nie je napríklad ovplyvniť činnosť výskumných pracovníkov v oblasti kybernetickej bezpečnosti a priemyslu, pretože si musia vymieňať informácie týkajúce sa narušiteľského softvéru, aby mohli vyvinúť riešenia pre svoje produkty a zabezpečiť ich zavedenie pred zverejnením zraniteľnosti.

— **Softvér na monitorovanie komunikácie (5D001.e)**

Tento softvér je určený na monitorovanie a analýzu údajov zozbieraných prostredníctvom cielených opatrení na odpočúvanie požadovaných od poskytovateľa komunikačných služieb zo strany oprávnených orgánov presadzovania práva. Tento softvér umožňuje vyhľadávanie na základe pevných selektorov komunikačného obsahu alebo metaúdajov s použitím rozhrania na zákonné odpočúvanie a mapovanie vzťahovej siete alebo sledovanie pohybu cieľových osôb na základe výsledkov vyhľadávaní. Tento softvér je určený na tajné sledovanie, pretože využíva údaje získané pri odpočúvaní komunikačnej prevádzky bez toho, aby o tom osoby vedeli. Okrem toho analyzuje údaje zozbierané prostredníctvom telekomunikačných systémov. Softvér je nainštalovaný v systémoch štátneho orgánu (napríklad orgán monitorujúci presadzovanie práva) a kontrola sa nevzťahuje na systémy na zaistenie súladu zákonného odpočúvania (napríklad systémy riadenia zákonného odpočúvania a sprostredkujúce zariadenia), ktoré sú komerčne vyvinuté a nainštalované v priestoroch poskytovateľa komunikačných služieb (napríklad integrované do komunikačnej siete) a ktoré poskytovateľ služieb prevádzkuje a udržiava. Ako sa objasňuje v texte opisujúcom kontrolnú položku, kontroly sa nevzťahujú na softvér osobitne navrhnutý alebo upravený na čisto komerčné účely, ako je kvalita služieb siete (QoS), kvalita skúseností (QoE), sprostredkujúce zariadenia alebo mobilné platby alebo bankové použitie v prípade fakturácie.

— **Položky používané na vykonanie kryptoanalýzy (5A004.a)**

Táto kontrolná položka sa uplatňuje na položky určené na prekonanie kryptografických mechanizmov s cieľom odvodiť dôverné premenné alebo citlivé údaje vrátane nezašifrovaného textu, hesiel alebo kryptografických kľúčov. Kryptografia sa používa na zabezpečenie dôvernosti prenášaných informácií a informácií v pokoji. Na potlačenie tejto dôvernosti sa používa kryptoanalýza, a preto táto technológia umožňuje tajné sledovanie monitorovaním, extrakciou, zberom alebo analýzou údajov z informačných a telekomunikačných systémov.

— **Forenzné/vyšetrovacie nástroje (5A004.b., 5D002.a.3.b. a 5D002.c.3.b.)**

Forenzné/vyšetrovacie nástroje sú navrhnuté tak, aby získavali nespracované údaje zo zariadenia (napríklad počítača alebo komunikačného zariadenia) tak, aby sa s týmito údajmi nemanipulovalo ani sa nepoškodzovali a aby sa mohli použiť na justičné účely, t. j. pri vyšetrovaní trestného činu alebo na súde. Tieto výrobky obchádzajú autentifikáciu alebo autorizačné kontroly zariadenia tak, aby sa nespracované údaje mohli extrahovať zo zariadenia. Tieto produkty používajú štátne orgány a orgány presadzovania práva, ale aj vojenské sily na získavanie a analýzu údajov zo zaistených zariadení. Hoci majú legitímne použitie, môžu byť zneužité, a teda predstavujú riziko pre citlivé alebo obchodné údaje.

Na forenzné/vyšetrovacie nástroje, ktoré nie sú osobitne navrhnuté na tajné sledovanie, sa však nevzťahuje vymedzenie položiek kybernetického dohľadu v článku 2 bode 20. Text kontrolnej položky v bode 5A004.b. a ďalších nezachytáva ani forenzné/vyšetrovacie nástroje, ktoré extrahujú len údaje o používateľoch, alebo ak údaje nie sú na zariadení chránené. Zároveň sa kontroly nevzťahujú na výrobné alebo skúšobné zariadenia výrobcu, nástroje správcu systému alebo výrobky výlučne pre komerčný maloobchodný sektor, napríklad na odblokovanie mobilných telefónov. Preto vzhľadom na rôznorodosť týchto druhov technológií závisí uplatňovanie kontrol od individuálneho posúdenia každého výrobku.

Na záver upozorňujeme, že v prílohe I k nariadeniu sú uvedené ďalšie položky súvisiace so sledovaním, ktoré by sa nemali považovať za položky, na ktoré sa vzťahuje vymedzenie položiek kybernetického dohľadu, ako sú zariadenia na rušenie mobilnej telekomunikácie (5A001.f.) určené na poškodzovanie alebo prerušenie komunikácie alebo systémov, narušiteľský softvér, ktorý upravuje systém (4D004), a laserové akustické detekčné zariadenia (6A005.g) zbierajúce zvukové údaje laserom alebo umožňujúce počúvanie konverzácií na diaľku (niekedy nazývané laserový mikrofón). Podobne by používanie bezpilotných vzdušných prostriedkov uvedených na zozname na účely sledovania neznamenalo, že tieto položky patria do vymedzenia položiek kybernetického dohľadu.