2024/2659

16.10.2024

DOPORUČENÍ KOMISE (EU) 2024/2659

ze dne 11. října 2024

o pokynech pro vývoz zboží kybernetického dohledu podle článku 5 nařízení Evropského parlamentu a Rady (EU) 2021/821

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 292 této smlouvy,

vzhledem k těmto důvodům:

(1) Nařízení Evropského parlamentu a Rady (EU) 2021/821 ([1]) zavádí režim Unie pro kontrolu vývozu, zprostředkování, technické pomoci, tranzitu a přepravy zboží dvojího užití:

(2) Nařízení (EU) 2021/821 řeší riziko použití zboží kybernetického dohledu ve spojení s vnitřními represemi nebo závažným porušováním lidských práv a mezinárodního humanitárního práva.

(3) Podle čl. 5 odst. 2 a čl. 26 odst. 1 nařízení (EU) 2021/821 vydají Komise a Rada pokyny pro vývozce, pokud jde o zboží kybernetického dohledu neuvedené na seznamu, s ohledem na potřebu zajistit účinnost režimu kontroly vývozu Unie, pokud jde o kybernetickou bezpečnost, a konzistentnost uplatňování nařízení (EU) 2021/821.

(4) Cílem tohoto doporučení a pokynů k němu připojených je podpořit vývozce při uplatňování kontrol zboží kybernetického dohledu, které není uvedeno na seznamu, mimo jiné včetně opatření náležité péče posuzujících rizika související s vývozem tohoto zboží.

(5) Pokyny připojené k tomuto doporučení byly v letech 2022 a 2023 předmětem rozsáhlých konzultací v rámci expertní skupiny pro sledovací technologie a zohlednily připomínky obdržené během veřejné konzultace ([2]) konané ve druhém čtvrtletí roku 2023.

(6) Je třeba připomenout, že toto doporučení a přiložené pokyny nejsou závazné. Vývozci by proto měli nadále nést zodpovědnost za plnění svých povinností podle nařízení (EU) 2021/821, zatímco Komise by měla zajistit, aby toto doporučení zůstalo v průběhu času relevantní,

([1]) Nařízení Evropského parlamentu a Rady (EU) 2021/821 ze dne 20. května 2021, kterým se zavádí režim Unie pro kontrolu vývozu, zprostředkování, technické pomoci, tranzitu a přepravy zboží dvojího užití (Úř. věst. L 206, 11.6.2021, s. 1, ELI: https://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.

PŘIJALA TOTO DOPORUČENÍ:

Doporučuje se, aby příslušné orgány a vývozci členských států při plnění svých povinností podle čl. 5 odst. 2 nařízení (EU) 2021/821 zohlednili pokyny uvedené v příloze tohoto doporučení.

V Bruselu dne 11. října 2024.

Za Komisi
Valdis DOMBROVSKIS
výkonný místopředseda

PŘÍLOHA

OBSAH

Strana

Úvod..... 4

1. Příslušná právní ustanovení, definice a klíčové pojmy 4

1.1 Přehled příslušných právních ustanovení 4

1.2 Klíčové definice 5

1.2.1 „Speciálně navržené“ 5

1.2.2 „Tajné sledování“ 6

1.2.3 „Fyzické osoby“ 6

1.2.4 „Monitorování, extrakce, shromažďování a analýza dat“ 6

1.2.5 „Z informačních a telekomunikačních systémů“ 7

1.2.6 „Vědomí“ a „je určeno k“ 7

1.3 Vnitřní represe, závažné porušování lidských práv a mezinárodního humanitárního práva 7

1.3.1 Vnitřní represe 8

1.3.2 Závažné porušování lidských práv 8

1.3.3 Závažné porušování mezinárodního humanitárního práva 9

2. Technická oblast působnosti 9

2.1 Zboží kybernetického dohledu, které je uvedeno na seznamu 9

2.2 Potenciální zboží kybernetického dohledu, které není uvedeno na seznamu 9

2.2.1 Technologie pro rozpoznávání tváří a emocí 10

2.2.2 Zařízení pro sledování polohy 10

2.2.3 Kamerové monitorovací systémy 10

3. Opatření náležité péče 10

Požadavky stanovené v čl. 5 odst. 2 nařízení (EU) 2021/821 12

4. Dodatek 12

Zboží kybernetického dohledu uvedené v příloze I nařízení (EU) 2021/821 12

Systémy k odposlechu telekomunikací (5A001.f.) 12

Systémy sledování internetu (5A001.j.) 13

„Software umožňující průnik do systému“ (4A005, 4D004 a související kontroly podle položek 4E001.a. a 4E001.c.) 13

Software pro sledování komunikace (5D001.e.) 14

Zboží používané k výkonu kryptoanalýzy (5A004.a.) 14

Forenzní/vyšetřovací nástroje (5A004.b., 5D002.a.3.b. a 5D002.c.3.b.) 14

ÚVOD

Cílem rámce Unie pro kontrolu vývozu stanoveného nařízením (EU) 2021/821 (dále jen „nařízení“) je zajistit dodržování mezinárodních závazků a povinností Unie a jejích členských států, včetně závazků týkajících se regionálního míru, bezpečnosti a stability a dodržování lidských práv a mezinárodního humanitárního práva. Unie a její členské státy proto provedly rozhodnutí přijatá v rámci mnohostranných režimů kontroly vývozu a odpovídajícím způsobem aktualizovaly kontrolní seznam Unie v příloze I nařízení ([1]). Kromě toho již před zahájením uplatňování článku 5 nařízení kontrolovaly příslušné orgány členských států vývoz určitého zboží, které je uvedeno na seznamu a které může mít sledovací využití ([2]), přičemž zohlednily rizika zneužití za určitých zvláštních okolností. V případě mimořádně závažných okolností zavedla Unie sankce omezující vývoz některých sledovacích zařízení ([3]).

Nařízení odráží závazek Unie účinně řešit riziko využívání zboží kybernetického dohledu ve spojení s vnitřními represemi a/nebo závažným porušováním lidských práv a mezinárodního humanitárního práva. Nařízení zejména zavádí nová ustanovení pro kontrolu vývozu zboží kybernetického dohledu, které není uvedeno na seznamu, včetně povinnosti vývozců informovat příslušný orgán, pokud jsou si podle svých zjištění učiněných po uplatnění náležité péče vědomi, že zboží kybernetického dohledu, které není uvedeno na seznamu a které mají v úmyslu vyvézt, je zcela nebo zčásti určeno k použití ve spojení s vnitřními represemi a/nebo se závažným porušováním lidských práv a mezinárodního humanitárního práva. Nařízení dále vyzývá Komisi a Radu, aby zpřístupnily pokyny pro vývozce, které podpoří účinné provádění nových kontrol zboží kybernetického dohledu, které není uvedeno na seznamu.

Cílem těchto pokynů je proto podpořit vývozce při uplatňování kontrol zboží kybernetického dohledu, které není uvedeno na seznamu, mimo jiné včetně opatření náležité péče posuzujících rizika související s vývozem tohoto zboží ke konečným uživatelům a pro konečná použití podle nových ustanovení nařízení.

1. PŘÍSLUŠNÁ PRÁVNÍ USTANOVENÍ, DEFINICE A KLÍČOVÉ POJMY

1.1 Přehled příslušných právních ustanovení

Nařízení zavádí nová ustanovení týkající se kontrol vývozu zboží kybernetického dohledu, které není uvedeno v příloze I nařízení a které je nebo může být zcela nebo zčásti určeno k použití ve spojení s vnitřními represemi a/nebo se závažným porušováním lidských práv a mezinárodního humanitárního práva. Příslušné body odůvodnění a články jsou následující:

a) 8. bod odůvodnění: „S cílem řešit riziko, že by určité zboží kybernetického dohledu, které není uvedeno na seznamu a které je vyváženo z celního území Unie, mohlo být zneužito osobami odpovědnými nebo spoluodpovědnými za nařizování či páchání závažného porušování lidských práv nebo mezinárodního humanitárního práva, je vhodné vývoz tohoto zboží kontrolovat. Související rizika se týkají zejména případů, kdy je zboží kybernetického dohledu speciálně navržené k tomu, aby umožňovalo průnik do informačních a telekomunikačních systémů nebo hloubkovou

([1]) Viz zejména kontroly týkající se systémů k odposlechu telekomunikací (5A001.f.), systémů sledování internetu (5A001.j.), softwaru umožňujícího průnik do systému (4A005, 4D004 a související kontroly podle položek 4E001.a. a 4E001.c.) a softwaru pro sledování ze strany donucovacích orgánů (5D001.e.). Dále viz kontroly týkající se některých forenzních/vyšetřovacích nástrojů (5A004.b., 5D002.a.3.b. a 5D002.c.3.b.) na základě posouzení jednotlivých případů.

([2]) Zejména systémy pro bezpečnost informací.

([3]) Viz nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006 o omezujících opatřeních s ohledem na situaci v Bělorusku a zapojení Běloruska do ruské agrese proti Ukrajině (Úř. věst. L 134, 20.5.2006, s. 1, ELI: https://eur-lex.europa.eu/eli/reg/2006/765/oj?locale=cs); Nařízení Rady (EU) č. 359/2011 ze dne 12. dubna 2011 o omezujících opatřeních namířených proti některým osobám, subjektům a orgánům s ohledem na situaci v Íránu (Úř. věst. L 100, 14.4.2011, s. 1, ELI: https://eur-lex.europa.eu/eli/reg/2011/359/oj?locale=cs); Nařízení Rady (EU) č. 36/2012 ze dne 18. ledna 2012 o omezujících opatřeních vzhledem k situaci v Sýrii a o zrušení nařízení (EU) č. 442/2011 (Úř. věst. L 16, 19.1.2012, s. 1, ELI: https://eur-lex.europa.eu/eli/reg/2012/36/oj?locale=cs); Nařízení Rady (EU) č. 401/2013 ze dne 2. května 2013 o omezujících opatřeních vůči Myanmaru/Barmě a o zrušení nařízení (ES) č. 194/2008 (Úř. věst. L 121, 3.5.2013, s. 1, ELI: https://eur-lex.europa.eu/eli/reg/2013/401/oj?locale=cs); a nařízení Rady (EU) 2017/2063 ze dne 13. listopadu 2017 o omezujících opatřeních vzhledem k situaci ve Venezuele (Úř. věst. L 295, 14.11.2017, s. 21, ELI: https://eur-lex.europa.eu/eli/reg/2017/2063/oj?locale=cs).

inspekci paketů s cílem provádět tajné sledování fyzických osob prostřednictvím monitorování, extrakce, shromažďování nebo analýzy dat z těchto systémů, včetně biometrických údajů. U zboží používaného pro čistě komerční účely, k nimž patří fakturace, marketing, kvalitní služby, spokojenost uživatelů nebo bezpečnost sítí, se má obecně za to, že taková rizika nepředstavuje“;

b) 9. bod odůvodnění: „V zájmu posílení účinné kontroly vývozu zboží kybernetického dohledu, které není uvedeno na seznamu, je nezbytné dále harmonizovat uplatňování kontrol vývozu zboží dvojího užití, které není uvedeno v příloze I (dále jen „univerzální kontroly“) v této oblasti. Za tímto účelem se členské státy zavazují podporovat tyto kontroly tak, že budou mezi sebou navzájem i s Komisí sdílet informace, zejména o technologickém vývoji zboží kybernetického dohledu, a že budou k uplatňování těchto kontrol přistupovat obezřetně s cílem podporovat výměnu informací na úrovni Unie“;

c) ustanovení čl. 2 bod 20, které uvádí tuto definici zboží kybernetického dohledu: „zboží dvojího užití, které je speciálně navržené k tomu, aby umožňovalo tajné sledování fyzických osob prostřednictvím monitorování, extrakce, shromažďování nebo analýzy dat z informačních a telekomunikačních systémů“;

d) ustanovení článku 5 zavádí požadavek na povolení pro vývoz zboží, které není uvedeno na seznamu, pokud byl vývozce příslušným orgánem informován, že dané zboží je nebo může být zcela nebo zčásti určeno k použití ve spojení s vnitřními represemi a/nebo se závažným porušováním lidských práv a mezinárodního humanitárního práva (čl. 5 odst. 1). Dále požaduje, aby vývozci uvědomili příslušný orgán, pokud jsou si na základě zjištění učiněných po uplatnění náležité péče vědomi toho, že zboží je zcela nebo zčásti určeno k použití ve spojení s vnitřními represemi a/nebo se závažným porušováním lidských práv a mezinárodního humanitárního práva (čl. 5 odst. 2). Tento příslušný orgán rozhodne, zda dotčený vývoz podmíní povolením; a

e) čl. 5 odst. 2 dále stanoví, že „Komise a Rada poskytnou vývozcům pokyny podle čl. 26 odst. 1.“

1.2 **Klíčové definice**

Nařízení obsahuje zvláštní body odůvodnění a ustanovení, jež objasňují konkrétní pojmy týkající se kontrol vývozu zboží, které není uvedeno na seznamu, a u nichž je důležité, aby je vývozci jasně pochopili, aby mohli vykonávat náležitou péči a účinně provádět kontroly. Zvláště důležitá je následující přesná definice „zboží kybernetického dohledu“ uvedená v čl. 2 bodě 20: „zboží dvojího užití, které je speciálně navržené k tomu, aby umožňovalo tajné sledování fyzických osob prostřednictvím monitorování, extrakce, shromažďování nebo analýzy dat z informačních a telekomunikačních systémů“.

Pro účely těchto pokynů je třeba objasnit konkrétní aspekty této definice.

1.2.1 *„Speciálně navržené“*

Zboží je navržené pro tajné sledování, pokud jsou jeho technické vlastnosti vhodné pro tajné sledování fyzických osob a objektivně ho umožňují. Pojem „speciálně navržené“ tedy znamená, že tajné sledování fyzických osob muselo být hlavním účelem vývoje a návrhu výrobku. Tento pojem však nevyžaduje, aby zboží mohlo být použito výhradně k tajnému sledování fyzických osob.

Jak je objasněno v 8. bodě odůvodnění nařízení, zboží používané pro čistě komerční účely, k nimž patří fakturace, marketing, řízení kvality, zajišťování spokojenosti uživatelů nebo bezpečnost sítí, není speciálně navržené pro tajné sledování fyzických osob, a proto nespadá do definice zboží kybernetického dohledu. Například i když zboží pro dohled nad operačními systémy v průmyslu nebo pro sledování síťové komunikace uživatelů může být použito pro účely dohledu, nejedná se o zboží kybernetického dohledu ve smyslu definice, neboť není speciálně navržené tak, aby umožňovalo skryté sledování fyzických osob.

1.2.2 *„Tajné sledování“*

Zboží umožňuje tajné sledování zejména v případech, kdy sledování není pro dotčenou fyzickou osobu zjevně patrné. Tak tomu je v případě, kdy si dotčené osoby neuvědomují přítomnost a/nebo činnost zboží kybernetického dohledu, a nemají tedy možnost se z tohoto dohledu vymanit nebo alespoň odpovídajícím způsobem upravit své chování. I když se sledování provádí pomocí zboží instalovaného nebo provozovaného ve veřejném prostoru, může být sběr dat v určitých případech považován za relevantní pro tajné sledování, zejména mohou být získané údaje zneužity, vyhodnocovány nebo zpracovány pro jiné účely, než o kterých je dotčená fyzická osoba informována. Jinými slovy, pokud fyzická osoba nemůže objektivně očekávat, že je pod dohledem, lze sledování považovat za tajné podle čl. 2 bodu 20 nařízení.

1.2.3 *„Fyzické osoby“*

Pojem „fyzická osoba“ označuje živou lidskou bytost, na rozdíl od právnické osoby nebo subjektu, na něž se tudíž tato ustanovení nevztahují. Tento pojem nezahrnuje sledování objektů, míst nebo přístrojů jako takových.

1.2.4 *„Monitorování, extrakce, shromažďování a analýza dat“*

Podle Oxfordského slovníku angličtiny mají slova „monitoring“ (monitorování), „extracting“ (extrakce), „collecting“ (shromažďování) a „analysing“ (analýza) následující jazykový význam:

— „monitoring“ (monitorování): dohled; sledování, odposlouchávání;

— „extracting“ (extrakce): přimět někoho k řeči;

— „collecting“ (shromažďování): získávat, sbírat;

— „analysing“ (analýza): odlišit nebo zjistit prvky něčeho (složitého) za účelem určení struktury nebo povahy dané věci, a tím ji vysvětlit nebo pochopit; důkladně a metodicky zkoumat za účelem výkladu; podrobit kritickému nebo výpočetnímu rozboru.

Z těchto pojmů vyplývá, že zboží používané ke sledování by mělo mít přesné technické schopnosti zpracování údajů za účelem monitorování, shromažďování, extrakce nebo analýzy dat, jako je např. toto zboží:

a) zboží použité k monitorování dat z informačních a telekomunikačních systémů ([4]) (například velikost souborů nebo provoz datových souborů přenášených v takovém systému);

b) zboží, které získává data z informačních a telekomunikačních systémů pomocí průniku do systému a extrakce dat (například software umožňující průnik do systému);

c) zboží, které umožňuje analýzu dat získaných z informačních a telekomunikačních systémů, včetně těch, které mohou zpracovávat záběry z kamer v těchto systémech (například určité typy technologií analýzy dat používaných jako součást systémů pro rozpoznávání tváří).

Zboží, které se používá k jednoduchému monitorování informačních systémů nebo ke sledování obyvatelstva prostřednictvím kamer a které umožňuje zachycovat rozhovory, výměnu údajů, pohyby a chování jednotlivců, není kybernetickým sledovacím zbožím ve smyslu definice nařízení, protože není speciálně navržené pro tento účel a musí spolupracovat s jinými technologiemi, jako je umělá inteligence nebo data velkého objemu. Celý systém (spolupracující s dalšími technologiemi, jako je umělá inteligence nebo technologie pracující s daty velkého objemu) by však potenciálně mohl být zbožím kybernetického dohledu podle definice v čl. 2 bodě 20 nařízení.

Důležité je, že ačkoli článek 5 uvádí několik příkladů užitečných pro ilustraci, definice a oblast působnosti zboží kybernetického dohledu nejsou těmito příklady omezeny, neboť cílem článku 5 je umožnit účinnou kontrolu vývozu zboží, které není uvedeno na seznamu.

([4]) Definice je uvedena níže v bodě 1.2.5.

Jak je patrné z použití spojky „nebo“ v definici, uvedené technické schopnosti je třeba považovat za alternativy a není nutné, aby zboží mělo všechny tyto technické možnosti monitorování, extrakce, shromažďování nebo analýzy dat. Jinými slovy, k tomu, aby zboží spadalo pod definici zboží kybernetického dohledu podle čl. 2 bodu 20, stačí, aby mělo jednu z těchto technických schopností.

1.2.5 *„Z informačních a telekomunikačních systémů“*

Tyto pojmy se vztahují na systémy, které elektronicky zpracovávají informace, například prostřednictvím programování/kódování, operací počítačového (hardwarového) systému a jiné správy informací, včetně softwarových technologií, webových technologií, počítačových technologií, technologií uchovávání atd., a na některé systémy, které přenášejí informace na dálku, například technické systémy pro přenos zvuku, signálů, textu, jiných znaků a obrazů prostřednictvím kabelových i bezdrátových kanálů, optických vláken, rádiového systému a jiných elektromagnetických systémů. Tyto dva pojmy zahrnují širokou škálu systémů, které přenášejí nebo zpracovávají informace. Je třeba poznamenat, že tento termín se vztahuje na systémy, nikoli na zařízení.

1.2.6 *„Vědomí“ a „je určeno k“*

Podle čl. 5 odst. 2 nařízení má vývozce uvědomit příslušný orgán, je-li si „vědom toho, že toto zboží kybernetického dohledu je (…) určeno k (…) použití ve spojení s vnitřními represemi a/nebo se závažným porušováním lidských práv a mezinárodního humanitárního práva“.

Pojem „vědom“ není nový právní pojem, ale používá se v souvislosti s požadavky na povolení související s konečným použitím (tzv. „univerzální kontroly“) podle článků 4, 6, 7 a 8 nařízení. Být si „vědom“ znamená, že vývozce pozitivně ví o zamýšleném zneužití. Pouhá možnost takového rizika k prokázání vědomí nestačí. Pojem „vědomí“ však nelze ztotožňovat s pasivitou: vyžaduje, aby vývozce podnikl kroky vedoucí k získání dostatečných a přiměřených znalostí potřebných k posouzení rizik spojených s vývozem a k zajištění souladu s nařízením.

Údaj o tom, že zboží musí být „určeno k“ příslušnému citlivému konečnému použití, znamená, že vývozce by měl posoudit konečné použití jednotlivě s ohledem na konkrétní okolnosti daného případu. Naopak teoretické riziko, tj. nezaložené na faktickém posouzení případu, že by zboží mohlo být použito způsobem, který porušuje lidská práva, nestačí k tomu, aby bylo možné doložit, že je „určeno“ ke konkrétnímu zneužití podle článku 5.

1.3 **Vnitřní represe, závažné porušování lidských práv a mezinárodního humanitárního práva**

Podle článku 15 nařízení, který stanoví kritéria pro posouzení povolení, mají členské státy vzít v úvahu všechna relevantní hlediska, včetně těch, na která se vztahuje společný postoj Rady 2008/944/SZBP ([5]).

Článek 5 nařízení rozšiřuje kontroly na vývoz zboží, které není uvedeno na seznamu, s ohledem na riziko jeho použití ve spojení s vnitřními represemi a/nebo závažným porušováním lidských práv a mezinárodního humanitárního práva. Společný postoj 2008/944/SZBP a uživatelská příručka k tomuto společnému postoji ([6]) poskytují v tomto ohledu užitečné pokyny.

([5]) Společný postoj Rady 2008/944/SZBP ze dne 8. prosince 2008, kterým se stanoví společná pravidla pro kontrolu vývozu vojenských technologií a vojenského materiálu (Úř. věst. L 335, 13.12.2008, s. 99, ELI: https://eur-lex.europa.eu/eli/compos/2008/944/oj?locale=cs).

([6]) Viz uživatelská příručka ke společnému postoji Rady 2008/944/SZBP, kterým se stanoví společná pravidla pro kontrolu vývozu vojenských technologií a vojenského materiálu, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1 *Vnitřní represe*

Podle čl. 2 odst. 2 společného postoje 2008/944/SZBP „vnitřní represe zahrnuje mimo jiné mučení a jiné kruté, nelidské a ponižující zacházení nebo trestání, okamžité nebo svévolné popravy, zmizení, svévolné zadržení nebo jiné významné porušování lidských práv a základních svobod, jak jsou stanoveny v příslušných mezinárodních nástrojích týkajících se lidských práv, včetně Všeobecné deklarace lidských práv a Mezinárodního paktu o občanských a politických právech“. Uživatelská příručka ke společnému postoji 2008/944/SZBP obsahuje pokyny k prvkům, které je třeba vzít v úvahu při posuzování vývozce, včetně „dosavadního jednání navrhovaného konečného uživatele, pokud jde o dodržování lidských práv, a dosavadního jednání přijímající země obecně“.

1.3.2 *Závažné porušování lidských práv*

Zneužití zboží, které není uvedeno na seznamu, může mít negativní dopad na širokou škálu lidských práv a přímo narušuje právo na soukromí a ochranu údajů. Svévolné nebo nezákonné sledování může porušovat i další lidská práva, jako je právo na svobodu projevu, sdružování a shromažďování, svobodu myšlení, svědomí a náboženského vyznání, jakož i právo na rovné zacházení nebo zákaz diskriminace a právo na svobodné, rovné a tajné volby. V konkrétních případech může sledování, včetně monitorování nebo shromažďování informací o fyzických osobách, jako jsou obránci lidských práv, aktivisté, politické osobnosti, zranitelné skupiny obyvatel a novináři, vést k zastrašování, potlačování, svévolnému zadržování, mučení nebo dokonce popravám bez řádného soudu. Vývozci by proto měli tyto aspekty týkající se závažného porušování lidských práv zahrnout do svých posouzení.

Mezinárodní zkušenosti ukazují, že jakákoli omezení lidských práv musí být „přiměřená“ a v souladu s mezinárodními normami v oblasti lidských práv. V praxi to znamená, že jsou zavedeny dostatečné záruky, které zajišťují, že omezení jsou stanovena zákonem a zachovávají podstatu práv. Při dodržení zásady proporcionality lze omezení provést pouze tehdy, pokud jsou nezbytná a skutečně slouží legitimnímu cíli – například národní či veřejné bezpečnosti, veřejnému pořádku, ochraně veřejného zdraví nebo ochraně práv a svobod druhých.

Zboží kybernetického dohledu může zahrnovat legitimní a regulované nástroje pro použití v oblasti prosazování práva, jako je prevence, vyšetřování, odhalování nebo stíhání trestných činů, a to i v oblasti boje proti terorismu, nebo výkon trestů. Zároveň může být zboží kybernetického dohledu zneužito k závažnému porušování lidských práv a mezinárodního humanitárního práva, pokud jeho vývoz směřuje do zemí s represivními režimy, k soukromým konečným uživatelům a/nebo do konfliktních oblastí.

To vyžaduje individuální posouzení okolností jednotlivých případů, včetně uplatnění příslušných předpisů s ohledem na případné zprávy o závažném porušování lidských práv ze strany příslušných orgánů, například Organizace spojených národů, Unie nebo Rady Evropy. Vodítkem pro „závažnost“ porušování lidských práv může být uznání těchto porušení v rámci informací zveřejněných příslušnými orgány Organizace spojených národů, Unie nebo Rady Evropy. Takové výslovné uznání ze strany těchto orgánů není nezbytně nutné, ale je významným faktorem pro splnění kritérií.

Podle ustanovení článku 5 musí být porušení lidských práv „závažné“. Užitečné pokyny týkající se kategorizace možných porušení lidských práv jako „závažných“ lze nalézt v uživatelské příručce ke společnému postoji 2008/944/SZBP. Podle této příručky jsou rozhodující povaha a důsledky porušení. Systematické a/nebo rozsáhlé porušování lidských práv je považováno za závažné; za „závažná“ však mohou být považována i porušení, která nejsou systematická nebo rozsáhlá – například vzhledem k závažnosti zásahu pro postižené osoby.

Příloha II uživatelské příručky ke společnému postoji 2008/944/SZBP obsahuje neúplný seznam hlavních mezinárodních a regionálních nástrojů v oblasti lidských práv, včetně Mezinárodního paktu o občanských a politických právech, Úmluvy proti mučení a jinému krutému, nelidskému či ponižujícímu zacházení nebo trestání, Evropské úmluvy o lidských právech a Listiny základních práv, které mohou být důležitým vodítkem pro výklad a uplatňování kritérií na podporu důkladného posouzení lidských práv. Tyto nástroje a jejich dodatkové protokoly představují hlavní mezinárodní normy a standardy v oblasti lidských práv a základních svobod.

1.3.3 *Závažné porušování mezinárodního humanitárního práva*

Mezinárodní humanitární právo (nazývané také „ženevské právo“ nebo „právo ozbrojených konfliktů“), jež bylo vypracováno prostřednictvím řady mezinárodních smluv, především Haagského řádu, Ženevských úmluv a jejich dvou dodatkových protokolů z roku 1977, určuje pravidla, která v době ozbrojeného konfliktu slouží k ochraně osob, které se neúčastní nebo již neúčastní páchání násilností (například civilistů a raněných, nemocných nebo zajatých bojovníků), a ukládá válčícím stranám omezení, pokud jde o prostředky a způsoby vedení boje (haagské právo).

Používání zboží kybernetického dohledu, které není uvedeno na seznamu, by mělo být v souladu s mezinárodním humanitárním právem, pokud je nasazeno jako prostředek nebo způsob vedení boje v rámci ozbrojeného konfliktu. Za těchto okolností je třeba zohlednit riziko závažného porušení mezinárodního humanitárního práva na základě nařízení a stejně jako v případě závažného porušení lidských práv by mělo být posuzováno s ohledem na zamýšlené konečné použití zboží v konkrétním případě. Uživatelská příručka ke společnému postoji 2008/944/SZBP obsahuje pokyny k prvkům, které je třeba vzít v úvahu, včetně dosavadního jednání příjemce, pokud jde o dodržování mezinárodního humanitárního práva, záměrů příjemce vyjádřených prostřednictvím formálních závazků a schopnosti příjemce zajistit, aby se převedené zařízení nebo technologie použily způsobem, který je v souladu s mezinárodním humanitárním právem, a aby nebyly odkloněny nebo převedeny na jiná místa určení, kde by mohly být použity k závažnému porušení tohoto práva.

Podle článku 5 musí být porušení mezinárodního humanitárního práva „závažné“. V uživatelské příručce ke společnému postoji 2008/944/SZBP lze nalézt pokyny, které uznávají, že „ojedinělé případy porušení mezinárodního humanitárního práva nutně nevypovídají o postoji přijímající země k mezinárodnímu humanitárnímu právu“, zatímco „příčinou k vážným obavám by mělo být odhalení určitých modelů porušování práva nebo skutečnost, že přijímající země neučinila příslušná opatření, aby porušování práva potrestala“. Mezinárodní výbor Červeného kříže poskytl pokyny týkající se posuzování případů porušení mezinárodního humanitárního práva pro účely kontroly vývozu. Podle Mezinárodního výboru Červeného kříže je „porušení mezinárodního humanitárního práva závažné, pokud ohrožuje chráněné osoby (například civilisty, válečné zajatce, raněné a nemocné) nebo objekty (například civilní objekty nebo infrastrukturu) nebo pokud porušuje důležité univerzální hodnoty“. Například válečné zločiny představují závažné porušení mezinárodního humanitárního práva. Mezinárodní výbor Červeného kříže dále uvádí podobné faktory, které je třeba zvážit, jako uživatelská příručka ke společnému postoji 2008/944/SZBP, včetně formálních závazků k uplatňování pravidel mezinárodního humanitárního práva, vhodných opatření zajišťujících odpovědnost za porušování mezinárodního humanitárního práva, školení ozbrojených sil v oblasti mezinárodního humanitárního práva a zákazu náboru dětí do ozbrojených sil.

2. TECHNICKÁ OBLAST PŮSOBNOSTI

2.1 Zboží kybernetického dohledu, které je uvedeno na seznamu

V dodatku k těmto pokynům jsou uvedeny informace o zboží kybernetického dohledu uvedeném v příloze I nařízení, které mají vývozcům pomoci při identifikaci potenciálního zboží kybernetického dohledu, které není uvedeno na seznamu.

2.2 Potenciální zboží kybernetického dohledu, které není uvedeno na seznamu

Ačkoli je ze samé podstaty věci nemožné poskytnout vyčerpávající seznam výrobků, které mohou být kontrolovány jako „zboží, které není uvedeno na seznamu“ podle článku 5, následující zboží by mohlo potenciálně sloužit k dohledu a může vyžadovat zvláštní pozornost na základě nařízení.

Podle upřesnění v 8. bodě odůvodnění nařízení se zboží používané pro čistě komerční účely, jako je fakturace, marketing, kvalitní služby, spokojenost uživatelů nebo bezpečnost sítí, obecně nepovažuje za zboží, které by mohlo být zneužito v rámci závažného porušení lidských práv nebo mezinárodního humanitárního práva, a proto obecně nepodléhá kontrole podle článku 5. Mnohé z tohoto zboží má funkci v oblasti bezpečnosti informací (šifrovací nebo dokonce kryptoanalytickou), která splňuje kontrolní parametry podle kategorie 5 části 2 kontrolního textu v příloze I nařízení. Vybavení pro síťové zabezpečení – včetně routerů, spínačů nebo relé, u nichž je funkce zabezpečení informací omezena na úkoly „provozu, správy nebo údržby“ používající pouze veřejné nebo komerční šifrovací standardy – rovněž nespadá pod definici „zboží kybernetického dohledu“, ačkoli vývozci by měli nadále bedlivě sledovat různé zprávy o zneužití takového zboží k porušování lidských práv.

2.2.1 *Technologie pro rozpoznávání tváří a emocí*

Technologie pro rozpoznávání tváří a emocí mají mnohostranné využití, které se netýká kybernetického dohledu (jedná se například o identifikaci nebo autentizaci), a nespadají automaticky do definice. Za určitých okolností však mohou technologie pro rozpoznávání tváří a emocí spadat do oblasti působnosti čl. 2 bodu 20 nařízení.

Technologie pro rozpoznávání tváří a emocí, které lze použít k monitorování nebo analýze uložených videozáznamů, by mohly spadat do definice zboží kybernetického dohledu. Nicméně i v případě, že jsou výše uvedená kritéria splněna, je třeba pečlivě prověřit, zda je software určený speciálně pro skryté sledování.

2.2.2 *Zařízení pro sledování polohy*

Zařízení pro sledování polohy umožňují sledovat fyzickou polohu zařízení v průběhu času a některé technologie pro sledování polohy již nějakou dobu používají donucovací a zpravodajské orgány. Jejich potenciál pro cílené a hromadné sledování se značně rozšířil spolu s tím, jak se zdokonalily monitorovací technologie – včetně satelitního sledování polohy, sledování polohy pomocí vysílačů, vysílačů Wi-Fi a Bluetooth – a jak se rozšířila „sledovací zařízení“, jako jsou chytré telefony a další elektronická zařízení (například palubní systémy ve vozidlech).

Zařízení pro sledování polohy používají donucovací a zpravodajské orgány, například ke shromažďování důkazů v průběhu vyšetřování nebo ke sledování podezřelých osob, ale také společnosti pro komerční účely, například pro podávání zpráv o souhrnných vzorcích pohybu v ulicích s obchody, pro sledování zaměstnanců pracujících na dálku nebo pro reklamu založenou na lokalitě.

2.2.3 *Kamerové monitorovací systémy*

Za účelem pomoci vývozcům identifikovat potenciální kybernetický dohled je také užitečné objasnit, na jaké zboží se definice nebude vztahovat. V tomto smyslu se definice zboží kybernetického dohledu nevztahuje například na kamerové monitorovací systémy a kamery – včetně kamer s vysokým rozlišením – používané k natáčení osob na veřejných prostranstvích, protože nemonitorují ani neshromažďují údaje z informačních a telekomunikačních systémů.

3. **OPATŘENÍ NÁLEŽITÉ PÉČE**

Podle 7. bodu odůvodnění nařízení je „zásadně důležité, aby k plnění celkového cíle kontrol obchodu přispívali vývozci“. Aby mohli jednat v souladu s tímto nařízením, je třeba provést posouzení rizik souvisejících s transakcemi, na něž se toto nařízení vztahuje, a to pomocí opatření pro prověřování transakcí, známých také pod označením „zásada náležité péče“, jež jsou součástí interních programů dodržování předpisů (dále rovněž jako „ICP“).

Ustanovení čl. 2 bodu 21 definuje interní program dodržování předpisů („ICP“) jako „průběžné, účinné, vhodné a přiměřené politiky a postupy, které přijmou vývozci, aby usnadnili dodržování ustanovení a cílů tohoto nařízení a podmínek povolení uplatňovaných podle tohoto nařízení, včetně opatření náležité péče posuzujících rizika související s vývozem zboží konečným uživatelům a ke konečným použitím“.

Doporučení Komise (EU) 2019/1318 ([7]) poskytuje rámec, jehož cílem je pomoci vývozcům určit, řídit a zmírňovat rizika související s kontrolami zboží dvojího užití a zajistit dodržování příslušných právních předpisů Unie a vnitrostátních právních předpisů.

Tyto pokyny mohou být vývozcům oporou při provádění opatření v oblasti prověřování transakcí, známých také jako zásada náležité péče, v rámci ICP.

Podle čl. 5 odst. 2 nařízení (EU) 2021/821 jsou vývozci zboží, které není uvedeno na seznamu, povinni provádět náležitou péči prostřednictvím opatření v oblasti prověřování transakcí, což znamená podniknout kroky ve věci klasifikace zboží a posouzení rizik transakcí. Z praktického hlediska se vývozcům doporučuje, aby provedli následující přezkumy:

([7]) Doporučení Komise (EU) 2019/1318 ze dne 30. července 2019 k vnitropodnikovým programům pro kontrolu vývozu pro kontroly obchodu se zbožím dvojího užití podle nařízení Rady (ES) č. 428/2009 (Úř. věst. L 205, 5.8.2019, s. 15, ELI: https://eur-lex.europa.eu/eli/reco/2019/1318/oj?locale=cs).

3.1 **Přezkoumat, zda zboží určené k vývozu, které není uvedeno na seznamu, může být „zbožím kybernetického dohledu“, tj. speciálně navržené k tomu, aby umožňovalo tajné sledování fyzických osob prostřednictvím monitorování, extrakce, shromažďování nebo analýzy dat z informačních a telekomunikačních systémů.**

Tento krok se týká určení zboží podle ustanovení vztahujících se na zboží kybernetického dohledu. To zahrnuje posouzení technických vlastností zboží na základě technických parametrů stanovených v příloze I nařízení pro zboží, které je uvedeno na seznamu, a s ohledem na specifické termíny a pojmy v definici zboží kybernetického dohledu pro zboží, které není uvedeno na seznamu, a na následnou klasifikaci dané položky (zboží, technologie nebo software).

3.2 **Přezkoumat schopnosti daného zboží za účelem zjištění, zda může být zneužito ve spojení s vnitřními represemi a/nebo závažným porušováním lidských práv a mezinárodního humanitárního práva ze strany zahraničních konečných uživatelů.**

Vývozci by měli provést posouzení, zda by výrobek nemohl být zneužit k vnitřním represím, porušování nebo zneužívání lidských práv, včetně práva na život, zákazu mučení a nelidského a ponižujícího zacházení, práva na soukromí, práva na svobodu projevu, práva na sdružování a shromažďování, práva na svobodu myšlení, svědomí a náboženského vyznání, práva na rovné zacházení nebo zákazu diskriminace nebo práva na svobodné, rovné a tajné volby.

Sem spadá rovněž posouzení toho, zda by výrobek mohl být použit jako díl nebo konstrukční část systému, který by mohl způsobit některé ze zmíněných porušení a/nebo zneužití.

Vývozci by měli při posuzování věnovat pozornost tzv. varovným signálům, které poukazují na jakékoliv neobvyklé okolnosti transakce a naznačují, že vývoz může být určen pro nevhodné konečné použití, nevhodného konečného uživatele nebo nevhodné místo určení.

Varovné signály:

a) zboží je uváděno na trh s informacemi o jeho možném použití pro tajné sledování;

b) s informacemi, jež naznačují, že podobné zboží bylo zneužito ve spojení s vnitřními represemi a/nebo závažným porušováním lidských práv a mezinárodního humanitárního práva (viz oddíl 1.3);

c) s informacemi, jež naznačují, že zboží bylo nezákonně použito při sledování zaměřeném proti členskému státu nebo ve spojení s nezákonným sledováním občana EU;

d) s informacemi, které naznačují, že součástí transakce je zboží, které by mohlo být použito k vytvoření, přizpůsobení nebo konfiguraci systému, o němž je známo, že se zneužívá ve spojení s vnitřními represemi a/nebo závažným porušováním lidských práv a mezinárodního humanitárního práva (viz oddíl 1.3);

e) dané zboží nebo podobné zboží se nachází na seznamu zveřejněném v řadě C *Úředního věstníku Evropské unie* v souladu s čl. 5 odst. 6 nařízení.

3.3 **S cílem podpořit příslušné orgány přezkoumat zúčastněné strany zapojené do transakce (včetně konečného uživatele a příjemců, jako jsou distributoři a prodejci).**

Vývozci by měli s cílem podpořit příslušné orgány a v rámci možností:

a) před každou transakcí a v jejím průběhu zkontrolovat, jakým způsobem hodlají příjemci a/nebo koneční uživatelé výrobek nebo službu používat, a to na základě prohlášení o konečném užití;

b) seznámit se se situací v příslušném místě určení zboží, zejména s obecným stavem lidských práv, neboť to je důležitým ukazatelem rizika závažného porušování lidských práv a mezinárodního humanitárního práva spojeného s vývozem;

c) přezkoumat rizika, že výrobek nebo služba budou dodány jinému neoprávněnému konečnému uživateli, na základě níže uvedených varovných signálů.

Varovné signály:

a) konečný uživatel má zřejmý vztah k zahraniční vládě státu, který se dopouští vnitřních represí a/nebo závažného porušování lidských práv a mezinárodního humanitárního práva;

b) konečný uživatel je strukturálně součástí ozbrojených sil nebo jiné skupiny zapojené do ozbrojeného konfliktu, při němž dochází k vnitřním represím a/nebo závažnému porušování lidských práv a mezinárodního humanitárního práva;

c) konečný uživatel v minulosti vyvezl zboží kybernetického dohledu do zemí, kde používání tohoto zboží vedlo k vnitřním represím a/nebo závažnému porušování lidských práv a mezinárodního humanitárního práva.

3.4 **Využít zjištění učiněná po uplatnění náležité péče k vypracování plánů na prevenci a zmírnění možných budoucích nepříznivých dopadů.**

Vývozci by měli na základě svých zjištění učiněných po uplatnění náležité péče ukončit činnosti, které mají nepříznivé dopady související s lidskými právy nebo k nim přispívají, a vypracovat a provést plán nápravných opatření. Na základě těchto opatření může být nutno:

a) aktualizovat firemní politiku tak, aby poskytovala návod, jak se v budoucnu vyhnout těmto nepříznivým dopadům a jak je řešit, a zajistit provádění těchto přístupů;

b) čerpat ze závěrů posouzení rizik za účelem aktualizace a posílení systémů řízení, aby bylo možné lépe sledovat informace a upozorňovat na rizika dříve, než k nepříznivým dopadům dojde;

c) shromažďovat informace pro pochopení rizik nepříznivých dopadů na vysoké úrovni souvisejících s daným odvětvím;

d) oznamovat příslušným orgánům členských států zjištění učiněná po uplatnění náležité péče, aby se usnadnil tok informací ohledně určitého zboží, konečných uživatelích a místech určení.

Požadavky stanovené v čl. 5 odst. 2 nařízení (EU) 2021/821



4. **DODATEK**

Zboží kybernetického dohledu uvedené v příloze I nařízení (EU) 2021/821

— **Systémy k odposlechu telekomunikací (5A001.f.)**

Ve většině zemí, včetně členských států, je důvěrnost komunikace chráněna zákonem, ale tajné elektronické sledování komunikace ze strany státních orgánů může být povoleno v rámci právního rámce (tzv. zákonný odposlech). Digitální éra však přinesla možnost masového využití odposlechových technologií. Používání odposlechových nástrojů libyjským režimem poukázalo na možnost masového nasazení těchto technologií a podnítilo zavedení kontroly vývozu systémů pro odposlech telekomunikací v roce 2012.

Tato kontrola se vztahuje na zařízení určená k extrakci obsahu komunikace (hlasové nebo datové), jakož i identifikátorů účastníků nebo jiných metadat, která jsou přenášena vzduchem prostřednictvím bezdrátové komunikace, a na zařízení pro radiofrekvenční monitorování. Tato kontrola se vztahuje například na zachytávače IMSI (International Mobile Subscriber Identity – mezinárodní identifikace mobilního účastníka), které zachycují provoz mobilních telefonů a sledují pohyb uživatelů mobilních telefonů, nebo na zařízení vytvářející falešné Wi-Fi hotspoty, jež mohou z telefonu získat čísla IMSI, a také na určité typy zboží speciálně navrženého tak, aby umožňovalo „hloubkovou inspekci paketů“ v telekomunikačních systémech. Rušicí zařízení pro mobilní komunikace nespadají do oblasti zboží kybernetického dohledu, protože neshromažďují údaje.

K vytvoření takových systémů lze sice použít univerzální technologii, ale jejich schopnost masového odposlechu bude záviset na specifických dílech a konstrukčních částech, mimo jiné včetně specifického softwaru a pokročilých nebo aplikačně specifických integrovaných obvodů (například FPGA, ASIC a další), aby se zvýšil počet paketů nebo komunikačních spojení, jež lze zpracovat za sekundu.

— **Systémy sledování internetu (5A001.j.)**

Přestože je dnes velká část internetové komunikace obvykle automaticky šifrovaná, lze k identifikaci vazeb mezi osobami a názvy domén stále využít zachycení provozních údajů (metadat) o komunikaci – jako jsou IP adresy a četnost a objem výměny dat. Vlády mohou tyto systémy používat legálně a pod soudním dohledem k legitimním účelům, například k identifikaci osob, které navštěvují domény spojené s kriminálním nebo teroristickým obsahem. Monitorování a analýza internetové komunikace na základě etnické, náboženské, politické nebo sociální charakterizace však může vést ke komplexnímu lidskému a sociálnímu mapování země za účelem kontroly a represe obyvatelstva, jakož i k jiným účelům, například k identifikaci politických disidentů. Kromě otázek týkajících se lidských práv a vnitřních represí může toto zboží rovněž přispět k posílení bezpečnostních a vojenských kapacit.

Kontrola podle položky 5A001.j. se vztahuje na systémy pro kontrolu internetu, které jsou provozovány na „carrier class IP sítích (např. celostátní páteřní IP síť)“ pro analýzu, extrakci a indexaci přenášeného obsahu metadat (hlas, video, zprávy, přílohy) na základě „zřejmých kritérií“ a mapují vztahovou síť osob. Jedná se o zboží, které provádí „tajné sledování“, protože dotčené osoby o odposlechu komunikace nevědí. Naproti tomu nejsou kontroly zaměřeny na systémy, kde probíhá činnost uživatele či účastníka nebo interakce s ním, a nevztahují se například na sociální sítě nebo komerční vyhledávače. Kromě toho se kontroly vztahují na systémy, které zpracovávají data pocházející z páteřní sítě poskytovatele internetu, a nevztahují se na sociální sítě nebo komerční vyhledávače, jež zpracovávají data zadaná uživateli.

— **„Software umožňující průnik do systému“ (4A005, 4D004 a související kontroly podle položek 4E001.a. a 4E001.c.)**

Software umožňující průnik do systému umožňuje svému provozovateli tajně získat vzdálený přístup k elektronickému zařízení, jako je chytrý telefon, notebook, server nebo zařízení pro internet věcí, získat data uložená v zařízení, odposlouchávat prostřednictvím kamery nebo mikrofonu zabudovaného v zařízení nebo k němu připojeného a použít zařízení jako prostředek k provedení útoků na přístroje, ke kterým se zařízení připojuje, nebo na kontakty uživatele („napadení prostřednictvím zařízení třetích stran“). Ačkoli pro software umožňující průnik do systému existuje legitimní využití ([8]), například „software umožňující vzdálený přístup“ používaný IT odděleními pro poskytování vzdálené podpory, tajná povaha sledování a rozsah případně shromážděných informací představuje vysoké riziko porušení práva na soukromí a ochranu osobních údajů a může vážně narušit právo na svobodu projevu.

([8]) Pro vyjasnění by zboží kybernetického dohledu uvedené v příloze I nařízení o zboží dvojího užití potřebovalo povolení k vývozu do třetích zemí bez ohledu na to, zda je jeho použití legitimní.

Kontrola podle položky 4A005 a dalších zahrnuje software, jakož i systémy, zařízení, konstrukční části a související technologie, speciálně navržené nebo upravené pro vytváření, řízení a kontrolu nebo dodávání „softwaru umožňujícího průnik do systému“, ale nevztahuje se na samotný „software umožňující průnik do systému“, jak je definován v příloze I nařízení. Tyto kybernetické nástroje jsou kontrolovány s ohledem na potenciální narušení a škody, jež mohou způsobit v případě úspěšného nasazení a použití, ale cílem kontrol není ovlivňovat např. činnost výzkumných pracovníků v oblasti kybernetické bezpečnosti a průmyslu, kteří potřebují sdílet informace týkající se softwaru umožňujícího průnik do systému, aby mohli vyvíjet opravy pro své produkty a mít je k dispozici před zveřejněním zranitelnosti.

— **Software pro sledování komunikace (5D001.e.)**

Tento software je navržený pro monitorování a analýzu údajů shromážděných oprávněnými donucovacími orgány prostřednictvím cílených odposlechů vyžádaných od poskytovatele komunikačních služeb. Umožňuje vyhledávat na základě „zřejmých kritérií“ obsahu komunikace nebo metadat, používat rozhraní pro zákonné odposlechy a mapovat vztahovou síť nebo sledovat pohyb cílových jednotlivců na základě výsledků vyhledávání. Tento software je určen k „tajnému sledování“, protože využívá data získaná z odposlechu komunikace, aniž by si toho byly dotyčné osoby vědomy. Dále „analyzuje“ údaje shromážděné prostřednictvím „telekomunikačních systémů“. Tento software je instalován ve vládním orgánu (například v monitorovacím zařízení k prosazování práva) a kontrola se nevztahuje na systémy pro dodržování zákonného odposlechu (například systémy pro řízení zákonného odposlechu a zařízení pro zprostředkování), které jsou vyvinuty ke komerčním účelům a instalovány v prostoru poskytovatele komunikačních služeb (například jsou začleněny do komunikační sítě) a které poskytovatel služeb provozuje a udržuje. Jak objasňuje kontrolní text, kontroly se nevztahují na „software“ speciálně navržený nebo upravený pro čistě komerční účely, jako je fakturace, zajišťování kvality služeb sítě, kvality poskytované služby, zařízení pro zprostředkování nebo mobilní platby či bankovnictví.

— **Zboží používané k výkonu kryptoanalýzy (5A004.a.)**

Tato kontrola se vztahuje na zboží navržené k deaktivaci kryptografických mechanismů za účelem odvození utajovaných proměnných nebo citlivých dat, včetně srozumitelného textu, hesel nebo šifrovacích klíčů. Šifrování se používá k zabezpečení důvěrnosti informací při přenosu i uchovávání. Kryptoanalýza se používá k narušení této důvěrnosti, a proto tato technologie „umožňuje“ tajné sledování prostřednictvím monitorování, extrakce, shromažďování nebo analýzy dat z informačních a telekomunikačních systémů.

— **Forenzní/vyšetřovací nástroje (5A004.b., 5D002.a.3.b. a 5D002.c.3.b.)**

Forenzní/vyšetřovací nástroje jsou navržené k takové extrakci nezpracovaných údajů ze zařízení (například z výpočetního nebo komunikačního zařízení), aby nebyly pozměněny nebo poškozeny a mohly být použity pro soudní účely, tj. při vyšetřování trestné činnosti nebo u soudu. Tyto produkty obcházejí kontroly „autentizace“ nebo ověřování zařízení, aby z něj bylo možné získat nezpracované údaje. Používají je vládní a donucovací orgány a také vojenské síly k extrakci a analýze dat ze zabavených zařízení. Mají sice legitimní využití, ale mohou být zneužity, a představují tak riziko pro citlivé nebo komerční údaje.

Forenzní/vyšetřovací nástroje, které nejsou „speciálně navržené“ k tajnému sledování, však nespadají do definice zboží kybernetického dohledu podle čl. 2 bodu 20. Kontrolní text v položce 5A004.b. a dalších se nevztahuje ani na forenzní/vyšetřovací nástroje, jež slouží pouze k extrakci uživatelských údajů nebo dat, která jsou v zařízení nechráněná. Zároveň se kontroly nevztahují na výrobní nebo testovací nástroje výrobce, nástroje pro správu systému nebo produkty určené výhradně pro komerční maloobchodní odvětví, například produkty pro odblokování mobilních telefonů. Vzhledem k různorodosti těchto typů technologií proto uplatnění kontrol závisí na individuálním posouzení každého výrobku.

V neposlední řadě upozorňujeme, že existuje další zboží, které souvisí s dohledem a je uvedeno v příloze I nařízení, a přitom by nemělo být považováno za zboží spadající do definice kybernetického dohledu, jako jsou například rušicí zařízení pro mobilní komunikace (5A001.f.) určená k poškození nebo narušení komunikace nebo systémů, software umožňující průnik do systému, který modifikuje systém (4D004), a laserová zařízení pro detekci zvuku (6A005.g.), která shromažďují zvukové údaje pomocí laseru nebo umožňují odposlouchávat hovory na dálku (někdy nazývané „laserové mikrofony“). Stejně tak používání bezpilotních vzdušných prostředků uvedených na seznamu pro účely sledování nevede k tomu, aby toto zboží spadalo do definice zboží kybernetického dohledu.