2024/2659

16.10.2024 г.

ПРЕПОРЪКА (ЕС) 2024/2659 НА КОМИСИЯТА

от 11 октомври 2024 година

относно насоки за износа на изделия за кибернаблюдение съгласно член 5 от Регламент (ЕС) 2021/821 на Европейския парламент и на Съвета

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 292 от него,

като има предвид, че:

(1) с Регламент (ЕС) 2021/821 на Европейския парламент и на Съвета ([1]) се въвежда режим на Съюза за контрол на износа, брокерската дейност, техническата помощ, транзита и трансфера на изделия с двойна употреба.

(2) В Регламент (ЕС) 2021/821 се засяга рискът от използване на изделията за кибернаблюдение за вътрешни репресии и/или за сериозни нарушения на правата на човека и международното хуманитарно право.

(3) По силата на член 5, параграф 2 и член 26, параграф 1 от Регламент (ЕС) 2021/821 Комисията и Съветът предоставят насоки за износителите по отношение на неописани изделия за кибернаблюдение, предвид необходимостта да се гарантират ефективността на режима на Съюза за контрол върху износа в областта на киберсигурността и съгласуваността при прилагането на Регламент (ЕС) 2021/821.

(4) С настоящата препоръка и приложените към нея насоки се цели да се окаже съдействие на износителите при прилагането на контрол върху неописани изделия за кибернаблюдение, включително, *inter alia*, мерки за надлежна проверка за оценка на рисковете, свързани с износа на тези изделия.

(5) Насоките, приложени към настоящата препоръка, бяха предмет на задълбочени консултации през 2022 г. и 2023 г. в рамките на експертната група „Технологии за наблюдение“, като в тях са взети предвид коментарите, получени по време на общественото обсъждане ([2]), проведено през второто тримесечие на 2023 г.

(6) Следва да се припомни, че настоящата препоръка и приложените насоки са необвързващи. Следователно износителите продължават да бъдат отговорни за изпълнението на задълженията си съгласно Регламент (ЕС) 2021/821, като Комисията продължава да поддържа актуално съдържанието на настоящата препоръка с течение на времето,

([1]) Регламент (ЕС) 2021/821 на Европейския парламент и на Съвета от 20 май 2021 г. за въвеждане на режим на Съюза за контрол на износа, брокерската дейност, техническата помощ, транзита и трансфера на изделия с двойна употреба (ОВ L 206, 11.6.2021 г., стр. 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.

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

Препоръчва се държавите членки, компетентните органи и износителите да вземат предвид насоките, предоставени в приложението към настоящата препоръка, за да изпълнят задълженията си по силата на член 5, параграф 2 от Регламент (ЕС) 2021/821.

Съставено в Брюксел на 11 октомври 2024 година.

За Комисията
Valdis DOMBROVSKIS
Изпълнителен заместник-председател

ПРИЛОЖЕНИЕ

СЪДЪРЖАНИЕ

Стр.

Въведение ... 4

1. Приложими правни разпоредби, определения и основни понятия ... 4

1.1. Общ преглед на приложимите правни разпоредби ... 4

1.2. Ключови определения ... 5

1.2.1. „Специално проектирани“ ... 5

1.2.2. „Скрито наблюдение“ ... 6

1.2.3. „Физически лица“ ... 6

1.2.4. „Мониторинг, извличане, събиране или анализиране на данни“ ... 6

1.2.5. „От информационни и телекомуникационни системи“ ... 7

1.2.6. „Знание“ и „са предназначени за“ ... 7

1.3. Вътрешни репресии, сериозни нарушения на правата на човека и международното хуманитарно право ... 7

1.3.1. Вътрешни репресии ... 8

1.3.2. Извършване на сериозни нарушения на правата на човека ... 8

1.3.3. Извършване на сериозни нарушения на международното хуманитарно право ... 9

2. Технически обхват ... 9

2.1. Описани изделия за кибернаблюдение ... 9

2.2. Потенциални неописани изделия за кибернаблюдение 8 ... 9

2.2.1. Технологии за лицево разпознаване и разпознаване на емоции 9 ... 10

2.2.2. Устройства за проследяване на местоположението ... 10

2.2.3. Системи за видеонаблюдение ... 10

3. Мерки за надлежна проверка ... 10

Изисквания, посочени в член 5, параграф 2 от Регламент (ЕС) 2021/821 ... 12

4. Допълнение ... 12

Описани изделия за кибернаблюдение, подлежащи на контрол съгласно приложение I към Регламент (ЕС) 2021/821 ... 12

Телекомуникационни системи за прихващане (5A001.f.) ... 12

Системи за наблюдение в интернет (5A001.j.) ... 13

„Софтуер за проникване“ (4A005, 4D004 и свързаните с тях мерки за контрол по 4E001.a и 4E001.c.) ... 13

Софтуер за наблюдение на комуникациите (5D001.e.) ... 14

Изделия, използвани за извършване на криптоанализ (5A004.a.) ... 14

Инструменти за криминалистика/разследване (5A004.b., 5D002.a.3.b. и 5D002.c.3.b.) ... 14

ВЪВЕДЕНИЕ

С рамката на Съюза за контрол на износа, която е установена с Регламент (ЕС) 2021/821 („регламента“), се цели да се гарантира, че се изпълняват международните задължения и ангажименти на Съюза и неговите държави членки, включително по отношение на мира, сигурността и стабилността в регионален план и зачитането на правата на човека и международното хуманитарно право. В тази връзка Съюзът и неговите държави членки са приложили решенията, взети в рамките на многостранните режими за контрол върху износа, и съответно са актуализирали контролния списък на Съюза в приложение I към Регламента ([1]). Също така преди да започне да се прилага член 5 от Регламента, компетентните органи на държавите членки вече упражняваха контрол върху износа на определени описани изделия, които биха могли да се използват за наблюдение ([2]), отчитайки рисковете от злоупотреба при определени конкретни обстоятелства. При особено тежки обстоятелства Съюзът е налагал санкции, ограничаващи износа на определени видове оборудване за наблюдение ([3]).

Регламентът е израз на ангажимента на Съюза ефективно да преодолее риска от използването на изделията за кибернаблюдение за вътрешни репресии и/или за сериозни нарушения на правата на човека и международното хуманитарно право. По-специално с регламента се въвеждат нови разпоредби за контрол на износа на неописани изделия за кибернаблюдение, включително задължение за износителите да уведомяват компетентния орган, когато знаят, в съответствие с констатациите си от надлежната проверка, че неописани изделия за кибернаблюдение, които износителите възнамеряват да изнесат, са предназначени изцяло или частично за употреба, свързана с вътрешни репресии, и/или за извършване на сериозни нарушения на правата на човека и на международното хуманитарно право. Регламентът също така изисква от Комисията и Съвета да предоставят насоки за износителите, за да подпомогнат ефективното прилагане на новите мерки за контрол на неописани изделия за кибернаблюдение.

Следователно с настоящите насоки се цели да се окаже съдействие на износителите при прилагането на контрол върху неописани изделия за кибернаблюдение, включително, наред с другото, мерки за надлежна проверка за оценка на рисковете, свързани с износа на такива изделия до крайните потребители и крайната употреба на изделията съгласно новите разпоредби в регламента.

1. ПРИЛОЖИМИ ПРАВНИ РАЗПОРЕДБИ, ОПРЕДЕЛЕНИЯ И ОСНОВНИ ПОНЯТИЯ

1.1. Общ преглед на приложимите правни разпоредби

С регламента се въвеждат нови разпоредби, специално предвиждащи контрол върху износа на изделия за кибернаблюдение, които не са описани в приложение I към регламента и които са или могат да бъдат предназначени, изцяло или частично, за употреба, свързана с вътрешни репресии, и/или за извършване на сериозни нарушения на правата на човека и международното хуманитарно право. Става дума за следните съображения и членове:

а) съображение (8): „За справяне с риска от евентуални злоупотреби с някои изнасяни от митническата територия на Съюза неописани изделия за кибернаблюдение от лица, които са съучастници или отговорни за организирането или извършването на сериозни нарушения на правата на човека или на международното хуманитарно право, е целесъобразно износът на такива изделия да се постави под контрол. Свързаните с това рискове се отнасят по-специално до случаите, когато изделия за кибернаблюдение са специално проектирани за проникване или задълбочена проверка на пакети в информационни или телекомуникационни системи с цел скрито наблюдение на

([1]) Вж. по-конкретно мерките за контрол, касаещи телекомуникационните системи за прихващане (5A001.f), системите за наблюдение в интернет (5A001.j.), софтуера за проникване (4A005, 4D004 и свързаните с тях мерки за контрол по 4E001.a и 4E001.c) и софтуера за мониторинг на правоприлагането (5D001.e). Вж. още мерките за контрол, свързани с определени инструменти за криминалистика/разследване (5A004.b 5D002.a.3.b и 5D002.c.3.b), прилагани след оценка на всеки отделен случай.

([2]) Най-вече системите за информационна сигурност.

([3]) Вж. Регламент (ЕО) № 765/2006 на Съвета от 18 май 2006 г. относно ограничителни мерки с оглед на положението в Беларус и участието на Беларус в руската агресия срещу Украйна (ОВ L 134, 20.5.2006, стр. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Регламент (ЕС) № 359/2011 на Съвета от 12 април 2011 г. относно ограничителни мерки, насочени срещу определени лица, образувания и органи предвид ситуацията в Иран (ОВ L 100, 14.4.2011 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Регламент (ЕС) № 36/2012 на Съвета от 18 януари 2012 г. относно ограничителни мерки с оглед на положението в Сирия и за отмяна на Регламент (ЕС) № 442/2011 (ОВ L 16, 19.1.2012 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Регламент (ЕС) № 401/2013 на Съвета от 2 май 2013 г. относно ограничителни мерки по отношение на Мианмар/Бирма и за отмяна на Регламент (ЕО) № 194/2008 (ОВ L 121, 3.5.2013 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); и Регламент (ЕС) 2017/2063 на Съвета от 13 ноември 2017 г. относно ограничителни мерки с оглед на положението във Венесуела (ОВ L 295, 14.11.2017 г., стр. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

физически лица чрез мониторинг извличане, събиране или анализиране на данни, включително биометрични данни от тези системи. Изделията с чисто търговско приложение, които се използват за фактуриране, маркетинг, свързани с качеството услуги, определяне на удовлетвореността на ползвателите или сигурност на мрежата обикновено не се считат за криещи такива рискове.“;

б) съображение (9) „С оглед засилване на ефективния контрол върху износа на неописани изделия за кибернаблюдение е важно допълнително да се хармонизира прилагането на всеобхватен контрол в тази област. За тази цел държавите членки се ангажират да подкрепят осъществяването на такъв контрол като споделят информация помежду си и с Комисията, по-специално относно технологични разработки на изделия за кибернаблюдение, и като проявяват бдителност при осъществяването на проверките за насърчаване на обмена на равнището на Съюза.“;

в) член 2, точка 20, в която е предвидено определение на изделия за кибернаблюдение като „изделия с двойна употреба, специално проектирани, за да направят възможно скрито наблюдение на физически лица чрез мониторинг, извличане, събиране или анализиране на данни от информационни и телекомуникационни системи“;

г) С член 5 се внася изискване за разрешение за износ на неописани изделия за кибернаблюдение, ако износителят е бил уведомен от компетентния орган, че въпросните изделия са или могат да бъдат предназначени, изцяло или частично, за употреба, свързана с вътрешни репресии, и/или за извършване на сериозни нарушения на правата на човека и международното хуманитарно право (член 5, параграф 1). С него също така износителите се задължават да уведомяват компетентния орган, когато знаят, в съответствие с констатациите си от надлежната проверка, че изделията са предназначени изцяло или частично за употреба, свързана с вътрешни репресии и/или за извършване на сериозни нарушения на правата на човека и на международното хуманитарно право (член 5, параграф 2). Компетентният орган решава дали съответният износ да бъде предмет на разрешителен режим; и

д) член 5, параграф 2, където също така се предвижда, че: „Комисията и Съветът предоставят насоки за износителите, както е посочено в член 26, параграф 1“.

1.2. **Ключови определения**

Регламентът съдържа специални съображения и разпоредби, разясняващи специфични термини, които имат отношение към контрола върху износа на неописани изделия за кибернаблюдение и с които е важно износителите да са напълно наясно, за да бъдат в състояние да провеждат надлежни проверки и да упражняват ефективен контрол. Особено важно е следното определение в член 2, точка 20 на „изделия за кибернаблюдение“: *„изделия с двойна употреба, специално проектирани, за да направят възможно скрито наблюдение на физически лица чрез мониторинг, извличане, събиране или анализиране на данни от информационни и телекомуникационни системи“*.

За целите на настоящите насоки следва да се разяснят конкретни аспекти от това определение.

1.2.1. *„Специално проектирани“*

Дадено изделие се счита за специално проектирано, за да направи възможно скрито наблюдение, когато техническите му характеристики са подходящи за скрито наблюдение на физически лица и обективно го позволяват. Ето защо терминът „специално проектирани“ означава, че скритото наблюдение на физически лица трябва да е било основната цел, за която е разработен и проектиран продуктът. Този термин обаче не налага изискване изделието да може да се използва единствено за скрито наблюдение на физически лица.

Както е обяснено в съображение 8 от регламента, изделията с чисто търговско приложение, които се използват за фактуриране, маркетинг, свързани с качеството услуги, определяне на удовлетвореността на ползвателите или сигурност на мрежата, не са специално проектирани за скрито наблюдение на физически лица и следователно не попадат в определението за изделия за кибернаблюдение. Така например изделията за наблюдение на операционни системи в промишлеността или за мониторинг на трафика на потребителите, въпреки че могат да бъдат използвани с цел наблюдение, не са изделия за кибернаблюдение съгласно определението, тъй като не са специално проектирани

1.2.2. *„Скрито наблюдение“*

Изделията позволяват скрито наблюдение най-вече когато наблюдението не е ясно забележимо за засегнатото физическо лице. Такъв би бил случаят, ако съответните лица не предполагат за наличието и/или използването на изделия за кибернаблюдение и следователно нямат възможност да избегнат това наблюдение или поне подобаващо да адаптират поведението си. Дори наблюдението да се извършва посредством изделия, които са монтирани или експлоатирани на обществено достъпно място, в определени случаи получаването на данни може да се счете за свързано със скрито наблюдение, по-специално понеже събраните данни може да се отклоняват, подлагат на оценка или обработват за цели, различни от тези, съобщени на физическото лице. С други думи, ако дадено физическо лице няма обективни основания да очаква, че ще бъде наблюдавано, то наблюдението може да се счита за скрито в съответствие с член 2, точка 20 от Регламента.

1.2.3. *„Физически лица“*

С термина „физическо лице“ се назовава човешко същество, което се противопоставя на юридическо лице или субект, които следователно не са обект на разпоредбите. Поради това терминът не се отнася до наблюдението на предмети, обекти или машини.

1.2.4. *„Мониторинг, извличане, събиране или анализиране на данни“*

Съгласно Оксфордския речник на английския език думите мониторинг, извличане, събиране и анализиране имат следното езиково значение:

— „мониторинг“: надзор; наблюдение, подслушване,

— „извличане“: изтегляне,

— „събиране“: натрупване, организиране на едно място,

— „анализиране“: разграничаване или установяване на елементите на нещо (сложно) с цел да се определи структурата или естеството му и по този начин то да се обясни или разбере; внимателно и методично изследване с цел тълкуване; подлагане на критичен или изчислителен анализ.

Тези термини предполагат, че изделията, използвани за наблюдение, следва да разполагат с конкретни технически възможности за обработване на данни, за да се осъществява мониторинг, събиране, извличане или анализиране на данни, като например следните изделия:

а) Изделия, използвани за наблюдение на данни от информационни и телекомуникационни системи ([4]) (напр. размер на файловете или пакетен трафик на данните, които се предават в такива системи);

б) Изделия, които извличат данни от информационни и телекомуникационни системи, като извършват проникване или извличане (например „софтуер за проникване“);

в) Изделия, които позволяват анализ на данни, извлечени от информационни и телекомуникационни системи, включително такива, които могат да обработват фотографски изображения, съхранявани в тези системи (например определени видове технологии за анализ на данни, които се използват като част от системи за лицево разпознаване).

Изделия, използвани единствено за мониторинг на информационни системи или за наблюдение на населението чрез камери за видеонаблюдение, които също така позволяват улавяне на разговори, размяна на данни, движения и индивидуално поведение, не се считат за изделия за кибернаблюдение съгласно определението в регламента, тъй като не са специално проектирани за тази цел и трябва да работят с други технологии като изкуствен интелект или големи данни. Въпреки това цялата система (която работи с други технологии като изкуствен интелект или големи данни) потенциално би могла да представлява изделие за кибернаблюдение съгласно определението в член 2, точка 20 от Регламента.

Важно е да се отбележи, че макар даването на примери да е полезно за онагледяване, определението и обхватът на изделията за кибернаблюдение не се ограничават до тези примери, тъй като целта на член 5 е да се даде възможност за ефективен контрол върху износа на неописани изделия.

([4]) За определение, моля, вж. точка 1.2.5. по-долу.

Както е видно от използването на съюза „или“ в определението, изброените технически възможности следва да се считат за алтернативни, като не е задължително дадено изделие да предлага всички технически възможности за мониторинг, извличане, събиране или анализиране на данни. С други думи е достатъчно изделието да има една от тези технически възможности, за да попада в определението за изделие за кибернаблюдение по член 2, точка 20.

1.2.5. *„От информационни и телекомуникационни системи“*

Тези термини се отнасят до системи, които обработват информация електронно, например програмиране/кодиране, операции на компютърна система (хардуер) и други начини за управление на информация, включително софтуерни технологии, уеб технологии, компютърни технологии, технологии за съхранение и др., както и до някои системи, които предават информация от разстояние, например технически системи, които предават звуци, сигнали, текст, други означения и изображения както чрез кабелни, така и чрез безжични канали, чрез оптични влакна, чрез радио и други електромагнитни системи. Взети заедно, тези две понятия обхващат широк набор от системи за предаване или обработване на информация. Следва да се отбележи, че терминът се отнася до системи, а не до оборудване.

1.2.6. *„Знание“ и „са предназначени за“*

По силата на член 5, параграф 2 от регламента всеки износител следва да уведомява компетентния орган, когато *„знае, че изделия за кибернаблюдение (…) са предназначени (…) за употреба, свързана с вътрешни репресии и/или за извършване на сериозни нарушения на правата на човека и международното хуманитарно право“*.

Терминът „знае“ не представлява ново правно понятие, а е използван във връзка с изискванията за наличие на разрешение предвид крайната употреба (т.нар. „всеобхватен контрол“) съгласно членове 4, 6, 7 и 8 от Регламента. Щом износителят „знае“, се предполага, че той разполага с недвусмислени сведения за предстояща злоупотреба. Само вероятността от такъв риск не е достатъчна, за да бъде налице „знание“. Терминът „знание“ обаче не може да се приравни към пасивно състояние — той изисква износителят да е предприел постъпки, за да получи достатъчни и подходящи сведения за преценка на рисковете, свързани с износа, и за да гарантира спазване на регламента.

Уточнението, че изделията трябва да „са предназначени за“ съответна чувствителна крайна употреба, предполага, че износителят следва да подлага крайната употреба на отделна оценка за всеки отделен случай, предвид конкретните обстоятелства по него. *От друга страна*, наличието на теоретичен риск (т.е. такъв, който не се основава на почиваща на факти оценка на случая), че изделията може да бъдат използвани по начин, който нарушава правата на човека, не би било достатъчно, за да се допусне, че те „са предназначени за“ конкретна злоупотреба по член 5.

1.3. **Вътрешни репресии, сериозни нарушения на правата на човека и международното хуманитарно право**

По силата на член 15 от регламента, в който се посочват съображенията при преценката дали да се предостави разрешение, държавите членки трябва да вземат предвид всички съответни съображения, включително тези, обхванати от Обща позиция 2008/944/ОВППС на Съвета ([5]).

С член 5 контролът се разширява, така че да обхване износа на неописани изделия за кибернаблюдение, като се има предвид рискът от използването им за вътрешни репресии и/или за сериозни нарушения на правата на човека и международното хуманитарно право. В Обща позиция 2008/944/ОВППС на Съвета и в съпътстващия я Справочник на потребителя ([6]) се съдържат полезни насоки в това отношение.

([5]) Обща позиция 2008/944/ОВППС на Съвета от 8 декември 2008 г., определяща общи правила за режим на контрол върху износа на военни технологии и оборудване (ОВ L 335, 13.12.2008 г., стр. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Вж. Справочник на потребителя към Обща позиция 2008/944/ОВППС на Съвета, определяща общи правила за режим на контрол върху износа на военни технологии и оборудване, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Вътрешни репресии*

По смисъла на член 2, параграф 2 от Обща позиция 2008/944/ОВППС на Съвета „вътрешните репресии включват, inter alia, изтезание и друго жестоко, нехуманно и унизително отношение или наказание, екзекуции, извършени по съкратена процедура или произволни такива, безследно изчезване на лица, произволно задържане и други сериозни нарушения на правата на човека и основните свободи, изложени в съответните международни инструменти за правата на човека, включително Всеобщата декларация за правата на човека и Международния пакт за граждански и политически права“ (МПГПП). Справочникът на потребителя към Обща позиция 2008/944/ОВППС на Съвета дава насоки относно елементите, които трябва да се вземат предвид при оценката на износителя, включително „настоящи и предишни данни за потенциалния краен потребител по отношение на зачитането на правата на човека, както и за получаващата държава като цяло“.

1.3.2. *Извършване на сериозни нарушения на правата на човека*

Злоупотребата с неописани изделия за кибернаблюдение може да окаже отрицателно въздействие върху широк спектър от права на човека и има пряко отношение към правото на неприкосновеност на личния живот и на защита на личните данни. Произволното или незаконосъобразно наблюдение също така може да наруши други права на човека, като правото на свобода на изразяване на мнение, на събранията и сдруженията, на свобода на мисълта, съвестта и религията, правото на равно третиране или забрана на дискриминацията, както и правото на свободни, равноправни и тайни избори. В определени случаи наблюдението, включително мониторингът или събирането на информация от физически лица, като защитници на правата на човека, активисти, политически фигури, уязвими групи от населението и журналисти, може да доведе до сплашване, потискане, произволно задържане, изтезание или дори до извънсъдебни екзекуции. Ето защо износителите следва да включват в оценките си тези аспекти, свързани със сериозните нарушения на правата на човека.

Международната практика сочи, че евентуалните ограничения на правата на човека трябва да бъдат „уместни“ и да съответстват на международните стандарти за правата на човека. На практика това означава да са били въведени подходящи предпазни мерки, за да се гарантира, че ограниченията са предвидени в закон и зачитат същността на правата. Съгласно принципа на пропорционалност ограничения може да се налагат само ако са необходими и действително допринасят за постигането на законна цел — например националната или обществената сигурност, обществения ред, опазването на общественото здраве или защитата на правата и свободите на други лица.

Изделията за кибернаблюдение може да включват законни и регулирани пособия, с приложение в областта на правоприлагането, например за предотвратяване, разследване, разкриване или наказателно преследване на престъпления, включително при борбата с тероризма или изпълнението на наказания. Същевременно са възможни и злоупотреби с изделия за кибернаблюдение за извършване на сериозни нарушения на правата на човека и международното хуманитарно право, ако бъдат изнесени за репресивни режими или крайни потребители и/или за засегнати от конфликти зони.

Това налага обстоятелствата по всеки отделен случай да се подлагат на отделна оценка, включително като се прилагат съответните нормативни разпоредби предвид евентуални доклади на компетентните органи, например ООН, Съюза или Съвета на Европа, сочещи сериозни нарушения на правата на човека. Представа за степента на „сериозност“ на нарушенията на правата на човека може да се получи от факта, че въпросните нарушения са признати в информация, публикувана от компетентните органи на ООН, от Съюза или от Съвета на Европа. Изричното признаване от страна на тези органи не е абсолютно необходимо, но е важен фактор с оглед изпълнението на критериите.

Съгласно условията в член 5 нарушението на правата на човека трябва да бъде „сериозно“. В Справочника на потребителя към Обща позиция 2008/944/ОВППС на Съвета се съдържат полезни насоки, що се отнася до категоризирането на възможните нарушения на правата на човека като „сериозни“. Съгласно Справочника определящи са естеството на нарушението и последиците от него. Системните и/или широкоразпространените нарушения на правата на човека обикновено се приемат за сериозни, но за „сериозни“ може да се считат и нарушения, които не са системни или широкоразпространени — например заради степента на тежест за засегнатите лица.

В приложение II към Справочника на потребителя към Обща позиция 2008/944/ОВППС на Съвета е представен неизчерпателен списък на основните международни и регионални инструменти за правата на човека, включително Международната конвенция за граждански и политически права (МКГПП), Конвенцията против изтезанията и други форми на жестоко, нечовешко или унизително отнасяне или наказание, Европейската конвенция за правата на човека („Конвенцията“) и Хартата на основните права („Хартата“), които може да дадат важни насоки относно тълкуването и прилагането на критериите и така да спомогнат за извършването на надеждни оценки на правата на човека. Тези инструменти и съответните допълнителни протоколи към тях представляват основните международни норми и стандарти в областта на правата на човека и основните свободи.

1.3.3. *Извършване на сериозни нарушения на международното хуманитарно право*

Международното хуманитарно право (наричано още „Женевско право“ или „право на въоръжените конфликти“) е разработено чрез редица международни договори, най-важните от които са Хагският правилник, Женевските конвенции и двата допълнителни протокола към тях от 1977 г., и определя правила, които по време на въоръжен конфликт служат за защита на лицата, които не участват или вече не участват във военни действия (например граждански лица, ранени, болни или пленени войници), и налагат на воюващите страни ограничения по отношение на средствата и методите на водене на война (Хагски закон).

Употребата на неописани изделия за кибернаблюдение следва да е в съответствие с международното хуманитарно право, когато се прилагат като средства и методи за водене на война в контекста на въоръжен конфликт. При такива обстоятелства рискът от сериозни нарушения на международното хуманитарно право е сред съображенията, които съгласно регламента се вземат предвид и що се отнася до извършването на сериозни нарушения на правата на човека, следва да се подлага на оценка предвид планираната крайна употреба на изделията в конкретния случай. Справочникът на потребителя към Обща позиция 2008/944/ОВППС на Съвета дава насоки относно елементите, които трябва да се вземат предвид, включително настоящи и предишни данни за получателя по отношение на зачитането на международното хуманитарно право, намеренията на получателя, изразени посредством официални ангажименти, и способността на получателя да гарантира, че трансферираното оборудване или технология се използват по начин, който съответства на международното хуманитарно право, както и че не се отклоняват или трансферират към други местоназначения, където биха могли да се използват за сериозни нарушения на това право.

Съгласно член 5 нарушението на международно хуманитарно право трябва да бъде „сериозно“. Насоки може да се намерят в Справочника на потребителя към Обща позиция 2008/944/ОВППС на Съвета, където се признава, че „изолираните случаи на нарушения на международното хуманитарно право не са непременно показателни за отношението на държавата получател към международното хуманитарно право“, докато „където обаче може да се установят определени модели на извършване на нарушенията или ако държавата получател не е предприела необходимите действия за наказване на нарушенията, следва да възникнат сериозни опасения“. Международният комитет на Червения кръст (МКЧК) е предоставил насоки във връзка с оценките на нарушенията на международното хуманитарно право за целите на контрола на износа. Според МКЧК „нарушенията на международно хуманитарното право са сериозни, ако застрашават защитени лица (например граждански лица, военнопленници, ранени и болни) или обекти (например граждански обекти или инфраструктура) или ако нарушават важни универсални ценности“. Военните престъпления например представляват сериозни нарушения на международното хуманитарно право. МКЧК споменава още фактори, които да се вземат предвид, сходни с тези в Справочника на потребителя към Обща позиция 2008/944/ОВППС на Съвета, включително официални ангажименти за прилагане на правилата на международното хуманитарно право, подходящи мерки, с които да се гарантира търсене на отговорност при нарушения на международното хуманитарно право, обучение на военните във връзка с международното хуманитарно право и забрана за набиране на деца във въоръжените сили.

2. **ТЕХНИЧЕСКИ ОБХВАТ**

2.1. **Описани изделия за кибернаблюдение**

В допълнението към настоящите насоки се съдържа информация относно изделията за кибернаблюдение, описани в приложение I към регламента, която да подпомогне износителите при идентифицирането на потенциални неописани изделия за кибернаблюдение.

2.2. **Потенциални неописани изделия за кибернаблюдение**

Макар по дефиниция да е невъзможно да се предостави изчерпателен списък на продуктите, които могат да се контролират като „неописани изделия“ съгласно член 5, при следните изделия е възможно да е налице потенциал за наблюдение и може да има основания за особено голяма бдителност съгласно регламента.

Както става ясно от съображение 8 от регламента, изделията с чисто търговско приложение, които се използват за фактуриране, маркетинг, свързани с качеството услуги, определяне на удовлетвореността на ползвателите или във връзка със сигурността на мрежата, обикновено не се считат за криещи рискове от злоупотреби, които да имат отношение към сериозните нарушения на правата на човека или на международното хуманитарно право, и следователно като цяло не подлежат на контрол съгласно член 5. Много от тези изделия имат функции, свързани с информационната сигурност (криптографски или дори криптоаналитични), които отговарят на параметрите за контрол за категория 5, част 2 от касаещия контрола текст в приложение I към регламента. Оборудването за мрежова сигурност, включително маршрутизатори (рутери), мрежови комутатори или релейни станции, при което функционалността за „информационна сигурност“ е ограничена до изпълнението на задачи по „експлоатация, администриране или поддръжка“ и се прилагат само публикувани или търговски криптографски стандарти, също не попада в определението за „изделия за кибернаблюдение“, въпреки че износителите следва да не губят бдителност, предвид наличието на различни доклади за злоупотреба с подобни изделия с цел нарушаване на правата на човека.

2.2.1. *Технологии за лицево разпознаване и разпознаване на емоции*

Технологиите за лицево разпознаване и разпознаване на емоции имат множество приложения освен кибернаблюдението — например за идентификация и удостоверяване на автентичността, и не попадат автоматично в определението. Въпреки това при определени обстоятелства технологиите за лицево разпознаване и разпознаване на емоции може да попаднат в обхвата на член 2, точка 20 от регламента.

Технологиите за лицево разпознаване и разпознаване на емоции, които могат да се използват за мониторинг или анализ на запазени видео изображения, биха могли да попаднат в обхвата на определението за изделие за кибернаблюдение. Дори обаче горепосочените критерии да са изпълнени, трябва внимателно да се анализира дали софтуерът е специално проектиран за скрито наблюдение.

2.2.2. *Устройства за проследяване на местоположението*

Устройствата за проследяване на местоположението позволяват проследяване на физическото положение на дадено устройство във времето, като определени технологии за проследяване на местоположението вече се използват от правоприлагащи и разузнавателни ведомства. Техният потенциал за насочено и масово наблюдение претърпя значително развитие, тъй като при технологиите за проследяване настъпи напредък — включително във връзка с проследяването на местоположение въз основа на спътникови данни, проследяването на местоположение въз основа на данни от базови станции, приемно-предавателните устройства, свързани с WLAN или блутут, и тъй като устройствата за проследяване, като смартфони и други електронни устройства (например бордови системи в автомобилите) придобиха голямо разпространение.

Устройствата за проследяване на местоположението се използват от правоприлагащи и разузнавателни ведомства например за събиране на доказателства в хода на разследване или за проследяване на заподозрени лица, но и от дружества за търговски цели, например за отчитане на модели на съвкупното движение по търговски улици, за проследяване на служители, работещи извън основния обект, или за реклама въз основа на местоположението.

2.2.3. *Системи за видеонаблюдение*

С цел да се окаже съдействие на износителите при идентифициране на потенциални възможности за кибернаблюдение е от полза да се изясни и кои изделия не попадат в обхвата на определението. Така например системите и камерите за видеонаблюдение, включително камери с висока разделителна способност, които се използват за заснемане на хора на обществени места, не попадат в обхвата на определението за изделия за кибернаблюдение, тъй като с тях не се наблюдават или събират данни от информационни и телекомуникационни системи.

3. **МЕРКИ ЗА НАДЛЕЖНА ПРОВЕРКА**

Съгласно съображение 7 от регламента „[п]риносът на износителите […] за постигането на общата цел за контрол върху търговията е от решаващо значение. За да могат те да действат в съответствие с настоящия регламент, оценката на рисковете от сделките, попадащи в обхвата на настоящия регламент, трябва да се прави чрез мерки за скрининг на сделките, известни също като принцип на надлежната проверка, като част от вътрешните програми за съответствие (ВПС)“.

В член 2, точка 21 „вътрешна програма за съответствие“ (ВПС) се определя като „действащи ефективни, целесъобразни и пропорционални политики и процедури, приети от износителите, за улесняване на спазването на разпоредбите и целите на настоящия регламент и на реда и условията относно прилаганите съгласно настоящия регламент разрешения, включително, *inter alia*, мерки за надлежна проверка за оценка на рисковете, свързани с износа на изделията до крайните потребители и крайната употреба на изделията“.

С Препоръка (ЕС) 2019/1318 ([7]) на Комисията се осигурява рамка, която да помогне на износителите да идентифицират, управляват и намаляват рисковете, свързани с контрола на търговията с изделия с двойна употреба, и да гарантира спазването на съответното законодателство на Съюза и националните законови и подзаконови актове.

Тези насоки биха могли да подпомогнат износителите при прилагане на мерки за скрининг на сделките (известни също като принцип на надлежната проверка) като част от ВПС.

По силата на член 5, параграф 2 от Регламент (ЕС) 2021/821 износителите на неописани изделия за кибернаблюдение са длъжни да извършват надлежна проверка чрез мерки за скрининг на сделките, което означава да работа по класификацията на изделията и оценка на риска във връзка със сделките. На практика износителите биват насърчавани да анализират следното:

([7]) Препоръка (ЕС) 2019/1318 на Комисията от 30 юли 2019 г. относно вътрешните програми за съответствие във връзка с контрола на търговията с изделия с двойна употреба съгласно Регламент (ЕО) № 428/2009 на Съвета (ОВ L 205, 5.8.2019 г., стр. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Да анализират дали неописаните изделия, които ще се изнасят, може да представляват „изделия за кибернаблюдение“, тоест дали са специално проектирани, за да направят възможно скрито наблюдение на физически лица чрез мониторинг, извличане, събиране или анализиране на данни от информационни и телекомуникационни системи.**

Тази стъпка е свързана с определяне на вида на изделието съгласно разпоредбите, които се отнасят до изделията за кибернаблюдение. Това включва разглеждане на техническите характеристики на изделията въз основа на техническите параметри, посочени за описаните изделия в приложение I към регламента, както и с оглед на конкретните термини и понятия от определението за изделия за кибернаблюдение, касаещи неописаните изделия, както и последваща класификация на изделието (стока, технология или софтуер).

3.2. **Да анализират възможностите на въпросното изделие, за да определят потенциала за злоупотреба за вътрешни репресии и/или извършване на сериозни нарушения на правата на човека и международното хуманитарно право от крайни потребители в други държави.**

Износителите следва да извършват оценка, за да определят дали е възможна злоупотреба с продукта с цел извършване на вътрешни репресии, нарушаване или злоупотреба с права на човека, включително правото на живот, правото на защита от изтезания, нечовешко или унизително отнасяне, правото на неприкосновеност на личния живот, правото на свобода на изразяване на мнение, на събранията и сдруженията, правото на свобода на мисълта, съвестта и религията, правото на равно третиране или забрана на дискриминацията или правото на свободни, равноправни и тайни избори.

Тук се включва и оценка за определяне дали продуктът би могъл да се използва като част или компонент на система, която би могла да доведе до същите нарушения и/или злоупотреба.

В оценката си износителите следва да се ръководят от т.нар. „червени флагчета“, които се отнасят до необичайни обстоятелства по дадена сделка, сочещи, че износът може да е предназначен за неподходяща крайна употреба, краен потребител или местоназначение.

изделието се Червени флагчета:

а) предлага на пазара с информация, свързана с потенциалната му употреба за скрито наблюдение;

б) информация, указваща, че с подобно изделие е извършена злоупотреба, свързана с вътрешни репресии и/или с извършване на сериозни нарушения на правата на човека и международното хуманитарно право (вж. точка 1.3);

в) информация, указваща, че изделието е използвано незаконосъобразно за дейности по наблюдение, насочени срещу държава членка, или във връзка с незаконосъобразно наблюдение на гражданин на ЕС;

г) информация, указваща, че сделката включва изделия, които биха могли да се използват за създаване, персонализиране или конфигуриране на система, за която се знае, че се използва за злоупотреба, свързана с вътрешни репресии и/или с извършване на сериозни нарушения на правата на човека и международното хуманитарно право (вж. точка 1.3);

д) изделието или сходно изделие фигурира в списъка, публикуван в серия C на *Официален вестник на Европейския съюз* в съответствие с член 5, параграф 6 от регламента.

3.3. **В помощ на компетентните органи да анализират заинтересованите страни, които участват в сделката (включително крайните потребители и получатели като дистрибутори и препродавачи).**

В подкрепа на компетентните органи износителите следва, доколкото е възможно:

а) преди и по време на всяка сделка да анализират как възнамеряват получателите и/или крайните потребители да използват продукта или услугата въз основа на декларации за крайната употреба;

б) да се запознаят със ситуацията в съответното местоназначение на изделията, най-вече с положението по отношение на правата на човека като цяло, тъй като това предоставя важен показател за риска от сериозни нарушения на правата на човека и международното хуманитарно право, свързани с износа;

в) да анализират рисковете от това продуктът или услугата да бъдат отклонени към различни неупълномощени крайни потребители въз основа на червените флагчета, посочени по-долу.

Червени флагчета:

а) крайният потребител има очевидна връзка с чуждо правителство, за което има данни, че е извършвало вътрешни репресии и/или сериозни нарушения на правата на човека и международното хуманитарно право;

б) крайният потребител структурно е част от въоръжените сили или друга група, която преди е участвала във въоръжен конфликт, включващ мерки за вътрешни репресии и/или сериозни нарушения на правата на човека и международното хуманитарно право;

в) крайният потребител преди е изнасял изделия за кибернаблюдение в държави, където използването на такива изделия е породило мерки за вътрешни репресии и/или сериозни нарушения на правата на човека и международното хуманитарно право.

3.4. **Да използват констатациите си от надлежната проверка за изготвяне на планове за предотвратяване и намаляване на възможните неблагоприятни последици в бъдеще.**

Въз основа на констатациите си от надлежната проверка износителите следва да преустановяват дейностите, които причиняват или допринасят за неблагоприятни въздействия върху правата на човека, както и да разработват и прилагат план за корективни действия. Тези действия може да включват:

а) актуализиране на политиките на предприятието, така че да предоставят насоки за начините, по които в бъдеще да се избягват и преодоляват неблагоприятните въздействия, и да се гарантира приложението на тези насоки;

б) използване на констатациите от оценката на риска с оглед актуализиране и укрепване на системите за управление с цел по-успешно проследяване на информация и обозначаване на рискове, преди да са възникнали неблагоприятни въздействия;

в) събиране на информация с цел разбиране на рисковете от високо ниво за неблагоприятни въздействия, свързани със сектора;

г) уведомяване на компетентните органи на държавата членка за констатациите от надлежната проверка с цел улесняване на информационния поток по отношение на определени изделия, крайни потребители и местоназначения.

Изисквания, посочени в член 5, параграф 2 от Регламент (ЕС) 2021/821



4. **ДОПЪЛНЕНИЕ**

Описани изделия за кибернаблюдение, подлежащи на контрол съгласно приложение I към Регламент (ЕС) 2021/821

— **Телекомуникационни системи за прихващане (5A001.f.)**

В повечето държави, включително в държавите членки, поверителният характер на комуникациите е защитен от закона, но скритото електронно наблюдение на комуникациите от страна на държавните органи може да бъде разрешено в определена законова рамка (т.нар. „законно прихващане“ (ЗП). Ерата на цифровите технологии обаче направи възможно масовото използване на технологии за прихващане. Използването на инструменти за прихващане от либийския режим насочи вниманието към потенциала за масово използване на такива технологии и ускори въвеждането през 2012 г. на мерки за контрол върху износа на телекомуникационни системи за прихващане.

Този контрол се отнася до оборудване, проектирано за извличането на съдържание от комуникация (глас или данни), както и на идентификационни данни за абонати или други метаданни, предавани по въздуха чрез безжична комуникация, и оборудване за радиочестотно наблюдение. Този контрол се отнася например до устройства за улавяне на IMSI (международна идентификация на мобилния абонат), които прихващат трафика през мобилни телефони и проследяват движението на потребителите на тези телефони, или до оборудване, създаващо фалшиви точки за безжичен достъп до интернет, които могат да извличат IMSI номерата на дадени телефони, както и до определени типове изделия, специално проектирани, за да направят възможна „задълбочената проверка на пакети“ в телекомуникационни системи. Оборудване за създаване на изкуствени смущения в мобилните далекосъобщения не попада в обхвата на изделията за кибернаблюдение, тъй като не събира данни.

Макар за изграждането на такива системи да могат да се използват технологии с общо предназначение, техните способности за масово прихващане зависят от конкретни части и компоненти, включително например специален софтуер и авангардни или специфични за съответното приложение интегрални схеми (например FPGA, ASIC и т.н.) за увеличаване на броя на пакетите или комуникационните сесии, които могат да се обработят за една секунда.

— **Системи за наблюдение в интернет (5A001.j.)**

Макар голяма част от осъществяващата се в интернет комуникация да е криптирана по подразбиране, прихващането на данни за трафика (метаданни) при комуникациите, като IP адреси и честота и размер на обменените данни, може да се използва с цел установяване наличието на връзки между лица и имена на домейни. Правителствата могат законно и в условията на съдебен надзор да използват тези системи за законни цели, като идентифицирането на лица, които посещават домейни, свързани с престъпно или терористично съдържание. Мониторингът и анализът на интернет трафик въз основата на профилиране по етнически, религиозни, политически или социални признаци обаче може да доведе до значително човешко и социално „картографиране“ на дадена държава с цел контрол и репресия на населението, както и за други цели, например идентифициране на политически дисиденти. Освен че пораждат въпроси, свързани с правата на човека и вътрешните репресии, тези изделия биха могли да допринесат и за повишаване на възможностите в областта на сигурността и военните действия.

Контролът съгласно 5A001.j се отнася до системи за контрол в интернет, които функционират в „IP carrier class мрежа (напр. IP опорна мрежа на национално равнище)“ и извършват анализ, извличане и индексиране на съдържанието на предадените метаданни (глас, видео, съобщения, прикачени файлове) въз основа на „рестриктивни критерии“ и изобразяват мрежата с контакти на дадени лица. Това са изделия, чрез които се осъществява „скрито наблюдение“, тъй като определените лица не знаят за прихващането на комуникацията. За разлика от тях контролът не е насочен към системи, при които е налице действие на потребителя или абоната или взаимодействие с него, и например не се отнася до социални мрежи или търсачки с търговска цел. Освен това контролът се отнася до системи, които обработват данни с произход от опорната мрежа на доставчика на интернет услуги, и не включва социални мрежи или търсачки с търговска цел, в които се обработват данни, предоставени от потребителите.

— **„Софтуер за проникване“ (4A005, 4D004 и свързаните с тях мерки за контрол по 4E001.a и 4E001.c.)**

Софтуерът за проникване дава възможност на своя оператор по скрит начин да получи достъп от разстояние до електронно устройство като смартфон, лаптоп, сървър или устройство от интернета на нещата, за да придобие данни, съхранявани на устройството, да подслушва чрез камера или микрофон, вградени в устройството или свързани с него, както и да използва устройството като посредник за атаки, насочени към оборудване, с което е свързано устройството, или към контакти на потребителя („хакерска атака чрез устройства на трети лица“). Макар да има законни начини на използване ([8]) на софтуер за проникване, например „софтуер за достъп от разстояние“, който се използва за поддръжка от разстояние от страна на ИТ отделите, скритото естество на наблюдението и мащабът на потенциално събраната информация пораждат висок риск от нарушаване на правото на неприкосновеност на личния живот и на защита на личните данни и може сериозно да подкопаят свободата на изразяване.

([8]) За по-голяма яснота за описаните изделия за кибернаблюдение, подлежащи на контрол съгласно приложение I към Регламента за изделията с двойна употреба, се изисква разрешение за износ в трети страни, независимо дали употребата на изделието е законна.

Контролът по 4A005 и др. включва софтуер, както и системи, оборудване, компоненти и свързани технологии, специално проектирани или модифицирани за генериране, управление и контрол или за доставяне на „софтуер за проникване“, но не се прилага спрямо самия „софтуер за проникване“ така, както е определен в приложение I към регламента. Тези киберинструменти се контролират предвид потенциалните смущения и вреди, които могат да причинят, ако бъдат използвани и приложени успешно, но контролът не засяга изследователите в областта на киберсигурността и бранша на киберсигурността например, тъй като те трябва да споделят информация, свързана със софтуера за проникване, за да бъдат в състояние да разработват коригиращи програми за продуктите си и да ги внедряват преди дадена уязвимост да стане публично известна.

— **Софтуер за наблюдение на комуникациите (5D001.e.)**

Този софтуер е проектиран за наблюдение и анализ от страна на оправомощените правоприлагащи органи на данни, събрани чрез мерки за насочено прихващане, изисквани от доставчик на съобщителни услуги. Този софтуер позволява търсене въз основа на „рестриктивни критерии“ за съдържание на съобщение или за метаданни, като се използва интерфейс за законно прихващане и изобразяване на мрежата с контакти или проследяване на движението на определени лица въз основа на резултатите от търсене. Този софтуер е предназначен за „скрито наблюдение“, тъй като използва данни, събрани при прихващането на комуникация, без лицата да знаят за това. Той освен това „анализира“ данни, събрани чрез „телекомуникационни системи“. Този софтуер се инсталира в държавния орган (например държавно съоръжение за наблюдение) и контролът не се прилага спрямо системи, които са в съответствие със законното прихващане (ЗП) (например системи за управление на ЗП и устройства за съгласуване), които са разработени с търговска цел и са инсталирани в пространството на доставчик на съобщителни услуги (например интегрирани в комуникационната мрежа) и които доставчикът на съобщителни услуги експлоатира и поддържа. Както се уточнява в касаещия контрола текст, мерките за контрол не се прилагат по отношение на „софтуер“, специално проектиран или модифициран за чисто търговски цели, като фактуриране, качество на услугата в мрежата — Network Quality of Service (QoS), степен на удовлетвореност — Quality of Experience (QoE), устройства за съгласуване, мобилно плащане или банкиране.

— **Изделия, използвани за извършване на криптоанализ (5A004.a.)**

Този контрол се отнася до изделия, предназначени за компрометиране на криптографски механизми с цел извличане на поверителни променливи или чувствителни данни, включително чист текст, пароли или криптографски ключове. Криптографията се използва за гарантиране на поверителността на информацията както при предаване, така и при съхранение. Криптоанализът се използва за компрометиране на тази поверителност, поради което технологията „прави възможно“ скритото наблюдение чрез мониторинг, извличане, събиране или анализиране на данни от информационни и телекомуникационни системи.

— **Инструменти за криминалистика/разследване (5A004.b., 5D002.a.3.b. и 5D002.c.3.b.)**

Инструментите за криминалистика/разследване са предназначени за извличане на необработени данни от устройство (например изчислително или комуникационно), така че данните да не бъдат подправяни или компрометирани и да могат да се използват за съдебни цели, т.е. в наказателни разследвания или в съда. Тези продукти заобикалят „удостоверяването на автентичността“ или проверките за разрешаване на ниво устройство, така че от устройството да могат да се извлекат необработените данни. Тези продукти се използват от държавни и правоприлагащи ведомства, но и от въоръжените сили за извличане и анализ на данни от иззети устройства. Макар да имат законни употреби, с тях могат да се извършат и злоупотреби, а това поражда риск за чувствителни или търговски данни.

Въпреки това инструментите за криминалистика/разследване, които не са „специално проектирани“ за скрито наблюдение, не попадат в обхвата на определението за изделия за кибернаблюдение по член 2, точка 20. Инструментите за криминалистика/разследване, които само извличат данни на потребители, или когато данните върху устройството не са защитени, също не са обхванати от касаещия контрола текст по 5A004.b. и др. Същевременно мерките за контрол не се отнасят до оборудването за производство и изпитване на производителя, до инструментите на системния администратор или до продукти, предназначени изключително за сектора за търговия на дребно, например продукти за отключване на мобилни телефони. Ето защо, като се има предвид многообразието на тези видове технологии, прилагането на мерки за контрол зависи от индивидуалната оценка на всеки продукт.

И накрая, имайте предвид, че има други изделия, свързани с наблюдението, описани в приложение I към регламента, за които не следва да се счита, че попадат в определението за изделия за кибернаблюдение, като оборудване за създаване на изкуствени смущения в мобилните далекосъобщения (5A001.f.), проектирано за нанасяне на щети или смущаване на комуникации или системи, софтуер за проникване, който модифицира дадена система (4D004), и лазерно акустично детекторно оборудване (6A005.g.), което събира аудио данни с лазер или позволява да се слуша разговор от разстояние (наричано понякога „лазерен микрофон“). По подобен начин използването на описани безпилотни летателни апарати (БЛА) с цел наблюдение не ги включва в определението за изделия за кибернаблюдение.