2024/2659

16.10.2024

KOMMISSIONENS HENSTILLING (EU) 2024/2659

af 11. oktober 2024

om retningslinjer for eksport af cyberovervågningsprodukter i henhold til artikel 5 i Europa-Parlamentets og Rådets forordning (EU) 2021/821

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 292, og

ud fra følgende betragtninger:

(1) Ved Europa-Parlamentets og Rådets forordning (EU) 2021/821 ([1]) blev der indført en EU-ordning for kontrol med eksport, mæglervirksomhed, teknisk bistand, transit og overførsel i forbindelse med produkter med dobbelt anvendelse.

(2) Forordning (EU) 2021/821 imødegår risikoen for, at cyberovervågningsprodukter bliver brugt til intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret.

(3) I henhold til artikel 5, stk. 2, og artikel 26, stk. 1, i forordning (EU) 2021/821 skal Kommissionen og Rådet udstikke retningslinjer for eksportører med hensyn til cyberovervågningsprodukter, som ikke er opført på listen, i betragtning af behovet for at sikre effektiviteten af Unionens eksportkontrolordning for så vidt angår cybersikkerhed og sikre en ensartet gennemførelse af forordning (EU) 2021/821.

(4) Denne henstilling og de dertil knyttede retningslinjer har til formål at støtte eksportørerne i deres kontrol af cyberovervågningsprodukter, der ikke er opført på listen, hvilket bl.a. omfatter foranstaltninger vedrørende passende omhu med henblik på at vurdere risiciene ved eksport af sådanne produkter.

(5) De retningslinjer, der er knyttet til denne henstilling, var i 2022 og 2023 genstand for omfattende høringer i ekspertgruppen vedrørende overvågningsteknologi og er udarbejdet under hensyntagen til de bemærkninger, der indkom under en offentlig høring, som blev afholdt i andet kvartal af 2023 ([2]).

(6) Det skal erindres, at denne henstilling og de tilknyttede retningslinjer ikke er bindende. Eksportørerne bør derfor fortsat have ansvaret for at opfylde deres forpligtelser i henhold til forordning (EU) 2021/821, mens Kommissionen bør sikre, at denne henstilling forbliver relevant også fremover —

([1]) Europa-Parlamentets og Rådets forordning (EU) 2021/821 af 20. maj 2021 om en EU-ordning for kontrol med eksport, mæglervirksomhed, teknisk bistand, transit og overførsel i forbindelse med produkter med dobbelt anvendelse (EUT L 206 af 11.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

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

VEDTAGET DENNE HENSTILLING:

Der henstilles til, at medlemsstaternes kompetente myndigheder og eksportører tager retningslinjerne i bilaget til denne henstilling til efterretning med henblik på at opfylde deres forpligtelser i henhold til artikel 5, stk. 2, i forordning (EU) 2021/821.

Udfærdiget i Bruxelles, den 11. oktober 2024.

På Kommissionens vegne
Valdis DOMBROVSKIS
Ledende næstformand

BILAG

INDHOLDSFORTEGNELSE

Side

Indledning ... 4

1. Relevante lovbestemmelser, definitioner og nøglebegreber ... 4

1.1. Oversigt over relevante lovbestemmelser ... 4

1.2. Vigtige definitioner ... 5

1.2.1. »Særligt udformet« ... 5

1.2.2. »Skjult overvågning« ... 6

1.2.3. »Fysiske personer« ... 6

1.2.4. »Overvågning, uddragelse, indsamling og analyse af data« ... 6

1.2.5. »Fra informations- og telekommunikationssystemer« ... 7

1.2.6. »Kendskab« og »er bestemt til« ... 7

1.3. Intern undertrykkelse, alvorlige krænkelser af menneskerettighederne og den humanitære folkeret ... 7

1.3.1. Intern undertrykkelse ... 8

1.3.2. Alvorlige krænkelser af menneskerettighederne ... 8

1.3.3. Alvorlige krænkelser af den humanitære folkeret ... 9

2. Teknisk anvendelsesområde ... 9

2.1. Cyberovervågningsprodukter, der er opført på listen ... 9

2.2. Potentielle cyberovervågningsprodukter, der ikke er opført på listen ... 9

2.2.1. Ansigts- og følelsesgenkendelsesteknologi ... 10

2.2.2. Lokaliseringssporingsanordninger ... 10

2.2.3. Videoovervågningssystemer ... 10

3. Foranstaltninger vedrørende passende omhu ... 10

Krav i artikel 5, stk. 2, i forordning (EU) 2021/821 ... 12

4. Tillæg ... 12

Cyberovervågningsprodukter, der er opført på listen i bilag I til forordning (EU) 2021/821 ... 12

Systemer til aflytning af telekommunikation (5A001.f.) ... 12

Internetovervågningssystemer (5A001.j.) ... 13

»Intrusionsoftware« (4A005, 4D004 og den tilhørende kontrol under 4E001.a. og 4E001.c.) ... 13

Software til overvågning af kommunikation (5D001.e.) ... 14

Produkter, der anvendes til at udføre kryptoanalyse (5A004.a.) ... 14

Kriminaltekniske redskaber og efterforskningsredskaber (5A004.b., 5D002.a.3.b. og 5D002.c.3.b.) ... 14

INDLEDNING

EU-rammen for eksportkontrol, der er oprettet ved forordning (EU) 2021/821 (»forordningen«), har til formål at sikre, at Unionens og medlemsstaternes internationale forpligtelser og tilsagn, herunder vedrørende regional fred, sikkerhed og stabilitet og respekt for menneskerettighederne og den humanitære folkeret, overholdes. Unionen og medlemsstaterne har derfor gennemført de beslutninger, der er truffet i de multilaterale eksportkontrolordninger, og ajourført EU-kontrollisten i bilag I til forordningen i overensstemmelse hermed ([1]). Før forordningens artikel 5 fandt anvendelse, kontrollerede medlemsstaternes kompetente myndigheder desuden allerede eksporten af visse produkter opført på listen, som kunne være omfattet af ansøgninger om overvågning ([2]), i betragtning af risikoen for misbrug under visse særlige omstændigheder. I tilfælde af usædvanligt alvorlige omstændigheder har Unionen indført sanktioner, der begrænser eksporten af visse former for overvågningsudstyr ([3]).

Forordningen afspejler Unionens tilsagn om effektivt at imødegå risikoen for, at cyberovervågningsprodukter bliver brugt til intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret. Forordningen indfører navnlig nye bestemmelser om kontrol med eksporten af cyberovervågningsprodukter, der ikke er opført på listen, herunder eksportørernes forpligtelse til at underrette den kompetente myndighed, hvis de i henhold til deres procedure for passende omhu har kendskab til, at cyberovervågningsprodukter, der ikke er opført på listen, og som eksportørerne agter at eksportere, helt eller delvis er bestemt til anvendelse i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret. I forordningen opfordres Kommissionen og Rådet endvidere til at udstikke retningslinjer for eksportører for at støtte en effektiv gennemførelse af den nye kontrol af cyberovervågningsprodukter, der ikke er opført på listen.

Disse retningslinjer har derfor til formål at støtte eksportører i anvendelsen af kontrol med cyberovervågningsprodukter, der ikke er opført på listen, herunder bl.a. foranstaltninger vedrørende passende omhu med henblik på at vurdere risiciene ved eksport af produkterne til slutbrugere og endelige anvendelsesformål i henhold til de nye bestemmelser i forordningen.

1. RELEVANTE LOVBESTEMMELSER, DEFINITIONER OG NØGLEBEGREBER

1.1. Oversigt over relevante lovbestemmelser

Forordningen indfører nye bestemmelser, der specifikt giver mulighed for kontrol med eksport af cyberovervågningsprodukter, der ikke er opført i bilag I til forordningen, og som helt eller delvis er eller kan være bestemt til anvendelse i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret. De relevante betragtninger og artikler er:

a) betragtning 8: For at imødegå risikoen for, at visse ikke opførte cyberovervågningsprodukter, der eksporteres fra Unionens toldområde, kan misbruges af personer, der har medvirket til eller været ansvarlige for at give ordre til eller for at begå alvorlige krænkelser af menneskerettighederne eller den humanitære folkeret, er det hensigtsmæssigt at bringe eksporten af sådanne produkter under kontrol. De dermed forbundne risici vedrører navnlig tilfælde, hvor cyberovervågningsprodukter er særligt udformet til at give mulighed for adgang til eller deep packet inspection i

([1]) Se navnlig kontrol i forbindelse med systemer til aflytning af telekommunikation (5A001.f), internetovervågningssystemer (5A001.j.), intrusionsoftware (4A005, 4D004 og den tilhørende kontrol under 4E001.a og 4E001.c) og software til retshåndhævelsesovervågning (5D001.e). Se endvidere på grundlag af en vurdering fra sag til sag kontrol vedrørende visse kriminaltekniske redskaber og efterforskningsredskaber (5A004.b 5D002.a.3.b og 5D002.c.3.b).

([2]) Især informationssikkerhedssystemer.

([3]) Jf. Rådets forordning (EF) nr. 765/2006 af 18. maj 2006 om restriktive foranstaltninger på baggrund af situationen i Belarus og Belarus' involvering i den russiske aggression mod Ukraine (EUT L 134 af 20.5.2006, s. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Rådets forordning (EU) nr. 359/2011 af 12. april 2011 om restriktive foranstaltninger over for visse personer, enheder og organer på baggrund af situationen i Iran (EUT L 100 af 14.4.2011, s. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Rådets forordning (EU) nr. 36/2012 af 18. januar 2012 om restriktive foranstaltninger på baggrund af situationen i Syrien og om ophævelse af forordning (EU) nr. 442/2011 (EUT L 16 af 19.1.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Rådets forordning (EU) nr. 401/2013 af 2. maj 2013 om restriktive foranstaltninger på baggrund af situationen i Myanmar/Burma og om ophævelse af forordning (EF) nr. 194/2008 (EUT L 121 af 3.5.2013, s. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj) og Rådets forordning (EU) 2017/2063 af 13. november 2017 om restriktive foranstaltninger på baggrund af situationen i Venezuela (EUT L 295 af 14.11.2017, s. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

informations- og telekommunikationssystemer med henblik på at foretage skjult overvågning af fysiske personer gennem overvågning, uddragelse, indsamling eller analyse af data fra informations- og telekommunikationssystemer. Produkter, der anvendes til rent kommercielle formål, såsom fakturering, markedsføring, kvalitetstjenester, brugertilfredshed eller netsikkerhed, anses normalt ikke for at indebære sådanne risici.

b) betragtning 9: »Med henblik på at styrke den effektive kontrol med eksporten af cyberovervågningsprodukter, der ikke er opført på listen, er det vigtigt yderligere at harmonisere anvendelsen af bredtfavnende kontrol (»catch-all control«) på dette område. Med henblik herpå er medlemsstaterne forpligtet til at støtte en sådan kontrol ved at udveksle oplysninger indbyrdes og med Kommissionen, navnlig om den teknologiske udvikling af cyberovervågningsprodukter, og ved at udvise omhu i forbindelse med anvendelsen af en sådan kontrol for at fremme en udveksling på EU-plan«.

c) Artikel 2, nr. 20), som indeholder en definition af cyberovervågningsprodukter som »produkter med dobbelt anvendelse, som er særligt udformet til at give mulighed for skjult overvågning af fysiske personer gennem overvågning, uddragelse, indsamling eller analyse af data fra informations- og telekommunikationssystemer«.

d) Ved artikel 5 indføres et krav om tilladelse til eksport af cyberovervågningsprodukter, der ikke er opført på listen, hvis eksportøren af den kompetente myndighed er blevet gjort bekendt med, at de pågældende produkter helt eller delvis er eller kan være bestemt til anvendelse i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret (artikel 5, stk. 1). Det kræves endvidere, at eksportører underretter den kompetente myndighed, hvis de i henhold til deres procedure for passende omhu har kendskab til, at produkterne helt eller delvis er bestemt til anvendelse i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret (artikel 5, stk. 2). Denne kompetente myndighed skal træffe afgørelse om, hvorvidt der skal kræves tilladelse til den pågældende eksport.

e) Det fastsættes endvidere i artikel 5, stk. 2, at »Kommissionen og Rådet stiller retningslinjer til rådighed for eksportører, jf. artikel 26, stk. 1«.

1.2. **Vigtige definitioner**

Forordningen indeholder særlige betragtninger og bestemmelser, der præciserer specifikke udtryk, som er relevante for kontrollen med eksporten af cyberovervågningsprodukter, der ikke er opført på listen, og det er vigtigt, at eksportørerne forstår disse klart, således at de kan udvise passende omhu og gennemføre en effektiv kontrol. Af særlig relevans indeholder artikel 2, nr. 20), følgende præcise definition af »cyberovervågningsprodukter«: »produkter med dobbelt anvendelse, som er særligt udformet til at give mulighed for skjult overvågning af fysiske personer gennem overvågning, uddragelse, indsamling eller analyse af data fra informations- og telekommunikationssystemer«.

Med henblik på disse retningslinjer bør specifikke aspekter af denne definition præciseres.

1.2.1. *»Særligt udformet«*

Et produkt er udformet til skjult overvågning, når dets tekniske karakteristika er egnede til og objektivt giver mulighed for skjult overvågning af fysiske personer. Ved udtrykket »særligt udformet« forstås derfor, at skjult overvågning af fysiske personer skal have været hovedformålet med udviklingen og udformningen af produktet. Det ligger imidlertid ikke i udtrykket, at produktet udelukkende kan anvendes til skjult overvågning af fysiske personer.

Som præciseret i forordningens betragtning 8 er produkter, der anvendes til rent kommercielle formål, såsom fakturering, markedsføring, kvalitetstjenester, brugertilfredshed eller netsikkerhed, ikke særligt udformet til skjult overvågning af fysiske personer og falder derfor ikke ind under definitionen af cyberovervågningsprodukter. Selv om produkter til overvågning af operativsystemer i industrien eller overvågning af brugernes trafik f.eks. kan anvendes til overvågningsformål, er disse produkter ikke cyberovervågningsprodukter, der er omfattet af definitionen, da de ikke er særligt udformet til at muliggøre skjult overvågning af fysiske personer.

1.2.2. *»Skjult overvågning«*

Produkter, der giver mulighed for skjult overvågning, navnlig hvor overvågningen ikke er synlig for den berørte fysiske person. Dette vil være tilfældet, når de berørte personer ikke er bekendt med tilstedeværelsen af og/eller virkningen af cyberovervågningsprodukter og derfor ikke har mulighed for at unddrage sig denne overvågning eller i det mindste tilpasse deres adfærd i overensstemmelse hermed. Selv om overvågningen foretages ved hjælp af produkter, der er installeret eller anvendes i det offentlige rum, kan indsamlingen af data i visse tilfælde anses for at være relevant for skjult overvågning, idet de indsamlede data navnlig kan anvendes, evalueres eller behandles til andre formål end dem, som den berørte fysiske person er gjort bekendt med. Når en fysisk person ikke objektivt kan forvente at blive overvåget, kan overvågningen med andre ord anses for at være skjult i henhold til forordningens artikel 2, nr. 20).

1.2.3. *»Fysiske personer«*

Udtrykket »fysisk person« henviser til et levende menneske i modsætning til en juridisk person eller enhed, som derfor ikke er omfattet af bestemmelserne. Begrebet omfatter ikke overvågning af genstande, steder eller maskiner som sådan.

1.2.4. *»Overvågning, uddragelse, indsamling og analyse af data«*

Ifølge Oxford English Dictionary har ordene overvågning, uddragelse, indsamling og analyse følgende sproglige betydning:

— »overvågning«: tilsyn, overvågning, aflytning

— »uddragelse«: at udtrække

— »indsamling«: at indhente, at samle

— »analyse«: at skelne mellem eller undersøge elementerne i noget (komplekst) for at bestemme dets struktur eller karakter og dermed forklare eller forstå det, at foretage en grundig og metodisk undersøgelse med henblik på fortolkning, at underkaste noget en kritisk analyse eller en computeranalyse.

Disse udtryk indebærer, at de produkter, der anvendes til overvågning, skal have præcise tekniske kapaciteter til behandling af data med henblik på at overvåge, indsamle, uddrage eller analysere data, f.eks. følgende produkter:

a) Produkter, der anvendes til overvågning af data fra informations- og telekommunikationssystemer ([4]) (f.eks. filstørrelse eller pakketrafik for de data, der overføres i et sådant system).

b) Anordninger, der uddrager data fra informations- og telekommunikationssystemer gennem intrusion og uddragelse (f.eks. intrusionsoftware).

c) Produkter, der gør det muligt at analysere data fra informations- og telekommunikationssystemer, herunder systemer, der kan behandle kamerabilleder, som er lagret i disse systemer (f.eks. visse typer dataanalyseteknologier, der anvendes i ansigtsgenkendelsessystemer).

Produkter, der blot anvendes til at overvåge informationssystemer eller til at overvåge befolkningen via videoovervågningskameraer, og som gør det muligt at registrere samtaler, dataudvekslinger, bevægelser og individuel adfærd, vil ikke være cyberovervågningsprodukter som defineret i forordningen, da de ikke er særligt udformet til dette formål og skal anvendes sammen med andre teknologier såsom kunstig intelligens eller big data. Hele systemet (der arbejder sammen med andre teknologier såsom AI- eller big data-teknologier) kan imidlertid potentielt være et cyberovervågningsprodukt som defineret i forordningens artikel 2, nr. 20).

Det er vigtigt at bemærke, at selv om der gives nogle nyttige eksempler til illustration, er definitionen og omfanget af cyberovervågningsprodukter ikke begrænset til disse eksempler, da formålet med artikel 5 er at muliggøre effektiv eksportkontrol af produkter, der ikke er opført på listen.

([4]) Se 1.2.5 nedenfor for en definition.

Som det fremgår af anvendelsen af konjunktionen »eller« i definitionen, skal de anførte tekniske kapaciteter betragtes som alternativer, og et produkt skal ikke have alle disse tekniske kapaciteter for at overvåge, uddrage, indsamle eller analysere data. Det er med andre ord tilstrækkeligt, at et produkt har en af disse tekniske kapaciteter for at falde ind under definitionen af cyberovervågningsprodukter i artikel 2, nr. 20).

1.2.5. *»Fra informations- og telekommunikationssystemer«*

Disse udtryk henviser til systemer, der behandler information elektronisk, f.eks. programmering/kodning, drift af PC-system (hardware) og anden informationsforvaltning, herunder softwareteknologi, webteknologi, computerteknologi, lagringsteknologi osv., og til systemer, der transmitterer information over afstand, f.eks. tekniske systemer, der transmitterer lyde, signaler, tekst, andre tegn, billeder over ledningstråd, trådløst, optiske fibre, radio og andet elektromagnetisk system. Disse to begreber dækker over en bred vifte af systemer, der transmitterer eller behandler information. Det skal bemærkes, at udtrykket henviser til systemer og ikke til udstyr.

1.2.6. *»Kendskab« og »er bestemt til«*

I henhold til forordningens artikel 5, stk. 2, skal en eksportør underrette den kompetente myndighed, hvis eksportøren »har kendskab til cyberovervågningsprodukter«, som »er bestemt til anvendelse i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret«.

Udtrykket »kendskab« er ikke et nyt juridisk begreb, men er blevet anvendt i forbindelse med slutanvendelsesrelaterede tilladelseskrav (bredtfavnende kontrol (»catch-all« control)) i henhold til forordningens artikel 4, 6, 7 og 8. At have »kendskab« til indebærer, at eksportøren har positivt kendskab til det påtænkte misbrug. En sådan risiko er ikke i sig selv et tilstrækkeligt grundlag for at fastslå kendskab. Udtrykket »kendskab« kan imidlertid ikke sidestilles med passivitet, da det forudsætter, at eksportøren har taget skridt til at opnå tilstrækkelig og fyldestgørende viden til at vurdere risiciene ved eksporten og sikre, at forordningen overholdes.

Angivelsen af, at produkterne skal være »bestemt til« en relevant følsom endelig anvendelse, indebærer, at eksportøren bør vurdere den endelige anvendelse fra sag til sag i lyset af de særlige omstændigheder i den pågældende sag. Omvendt ville en teoretisk risiko, dvs. en risiko, der ikke er baseret på en faktuel vurdering af sagen, for, at produkterne kan anvendes på en måde, der krænker menneskerettighederne, ikke være tilstrækkelig til at antage, at de »er bestemt til« et specifikt misbrug i henhold til artikel 5.

1.3. **Intern undertrykkelse, alvorlige krænkelser af menneskerettighederne og den humanitære folkeret**

I henhold til forordningens artikel 15 vedrørende betragtningerne i forbindelse med vurderingen af en tilladelse, skal medlemsstaterne tage hensyn til alle relevante betragtninger, herunder betragtningerne i Rådets fælles holdning 2008/944/FUSP ([5]).

I forordningens artikel 5 udvides kontrollen til at omfatte eksport af cyberovervågningsprodukter, der ikke er opført på listen, i betragtning af risikoen for, at de bliver brugt til intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret. Fælles holdning 2008/944/FUSP og brugervejledningen til denne fælles holdning ([6]) giver nyttig vejledning i denne henseende.

([5]) Rådets fælles holdning 2008/944/FUSP af 8. december 2008 om fælles regler for kontrol med eksport af militærteknologi og -udstyr (EUT L 335 af 13.12.2008, s. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Se brugervejledningen til Rådets fælles holdning 2008/944/FUSP om fælles regler for kontrol med eksport af militærteknologi og -udstyr: https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Intern undertrykkelse*

I henhold til artikel 2, stk. 2, i Rådets fælles holdning 2008/944/FUSP omfatter intern undertrykkelse »bl.a. tortur og anden grusom, umenneskelig og nedværdigende behandling eller straf, summariske eller vilkårlige henrettelser, forsvindinger, vilkårlige arrestationer og andre alvorlige krænkelser af menneskerettighederne og de grundlæggende frihedsrettigheder som fastsat i relevante internationale menneskerettighedsinstrumenter, herunder verdenserklæringen om menneskerettigheder og den internationale konvention om borgerlige og politiske rettigheder« (ICCPR). Brugervejledningen til fælles holdning 2008/944/FUSP indeholder vejledning om de elementer, der skal tages i betragtning ved eksportørens vurdering, herunder »den foreslåede slutbrugers tidligere og nuværende overholdelse af menneskerettighederne og modtagerlandets overholdelse generelt«.

1.3.2. *Alvorlige krænkelser af menneskerettighederne*

Misbrug af cyberovervågningsprodukter, der ikke er opført på listen, kan have en negativ indvirkning på et bredt spektrum af menneskerettigheder og griber direkte ind i retten til privatlivets fred og databeskyttelse. Vilkårlig eller ulovlig overvågning kan også krænke andre menneskerettigheder såsom ytrings-, forenings- og forsamlingsfriheden, tanke-, samvittigheds- og religionsfriheden samt retten til ligebehandling eller forbud mod forskelsbehandling og retten til frie, lige og hemmelige valg. I særlige tilfælde kan overvågning, herunder overvågning eller indsamling af oplysninger om fysiske personer såsom menneskerettighedsforkæmpere, aktivister, politikere, sårbare befolkningsgrupper og journalister føre til intimidering, undertrykkelse, vilkårlig tilbageholdelse, tortur eller endog udenretslige drab. Eksportører bør derfor medtage disse aspekter vedrørende alvorlige krænkelser af menneskerettighederne i deres vurderinger.

Ifølge international praksis skal enhver begrænsning af menneskerettighederne være »passende« og i overensstemmelse med de internationale menneskerettighedsstandarder. I praksis betyder dette, at der skal indføres passende garantier for at sikre, at begrænsninger er fastsat ved lov, og at rettighedernes væsentligste indhold respekteres. Under iagttagelse af proportionalitetsprincippet kan der kun indføres begrænsninger, hvis de er nødvendige og faktisk opfylder et legitimt formål — f.eks. national eller offentlig sikkerhed, den offentlige orden, beskyttelsen af folkesundheden eller beskyttelsen af andres rettigheder og friheder.

Cyberovervågningsprodukter kan omfatte lovlige og regulerede redskaber til retshåndhævende anvendelser, f.eks. med henblik på forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger, herunder inden for terrorbekæmpelse, eller fuldbyrdelse af strafferetlige sanktioner. Cyberovervågningsprodukter kan også samtidigt misbruges til at begå alvorlige krænkelser af menneskerettighederne og den humanitære folkeret, når de eksporteres til undertrykkende regimer eller private slutbrugere og/eller til konfliktområder.

Dette kræver en vurdering fra sag til sag af omstændighederne i en sag, herunder anvendelse af relevante bestemmelser på baggrund af rapporter om alvorlige krænkelser af menneskerettighederne fra FN's kompetente organer, EU eller Europarådet. Anerkendelsen af disse krænkelser i rapporter offentliggjort af FN's kompetente organer, EU og Europarådet, kan indikere, at krænkelserne af menneskerettighederne er »alvorlige«. Disse organers udtrykkelige anerkendelse er ikke absolut nødvendig, men den er en væsentlig faktor for opfyldelsen af kriterierne.

I henhold til ordlyden i artikel 5 skal krænkelsen af menneskerettighederne være »alvorlig«. Nyttig vejledning til kategorisering af mulige krænkelser af menneskerettighederne som »alvorlige« findes i brugervejledningen til fælles holdning 2008/944/FUSP. Ifølge denne vejledning er krænkelsens karakter og konsekvenser afgørende. Systematiske og/eller udbredte krænkelser af menneskerettighederne betragtes normalt som alvorlige, men krænkelser, der ikke er systematiske eller udbredte, kan også betragtes som »alvorlige« — f.eks. hvis krænkelsen er alvorlig for de berørte personer.

Bilag II til brugervejledningen til fælles holdning 2008/944/FUSP indeholder en ikkeudtømmende liste over de vigtigste internationale og regionale menneskerettighedsinstrumenter, herunder den internationale konvention om borgerlige og politiske rettigheder (ICCPR), konventionen mod tortur og anden grusom, umenneskelig eller nedværdigende behandling eller straf, den europæiske menneskerettighedskonvention (konventionen) og chartret om grundlæggende rettigheder (chartret), som kan give vigtig vejledning om fortolkningen og anvendelsen af kriterierne til støtte for solide vurderinger af menneskerettighederne. Disse instrumenter og deres respektive tillægsprotokoller udgør de vigtigste internationale normer og standarder inden for menneskerettigheder og grundlæggende frihedsrettigheder.

1.3.3. *Alvorlige krænkelser af den humanitære folkeret*

Den humanitære folkeret (også kaldet »Genèveloven« eller »loven om væbnet konflikt«) er blevet udviklet gennem en række internationale traktater, navnlig Haagforskrifterne, Genèvekonventionerne og de to tillægsprotokoller hertil fra 1977, og fastlægger regler, der i tilfælde af væbnet konflikt beskytter personer, der ikke eller ikke længere deltager i fjendtligheder (f.eks. civile og sårede, syge eller krigsfanger), og pålægger de krigsførende parter begrænsninger med hensyn til krigsførelsens midler og metoder (Haagloven).

Anvendelsen af cyberovervågningsprodukter, der ikke er opført på listen, bør være i overensstemmelse med den humanitære folkeret, når de anvendes som midler og metoder i krigsførelsen i forbindelse med en væbnet konflikt. Under sådanne omstændigheder skal der tages hensyn til risikoen for alvorlige krænkelser af den humanitære folkeret i henhold til forordningen, og hvad angår alvorlige krænkelser af menneskerettigheder, bør risikoen vurderes i lyset af den tilsigtede endelige anvendelse af produkterne i den konkrete sag. Brugervejledningen til fælles holdning 2008/944/FUSP indeholder vejledning om de elementer, der skal tages i betragtning, herunder modtagerens tidligere og nuværende overholdelse af den humanitære folkeret, modtagerens hensigter som udtrykt gennem formelle forpligtelser og modtagerens evne til at sikre, at det overførte udstyr eller den overførte teknologi anvendes på en måde, der er i overensstemmelse med den humanitære folkeret, og ikke omdirigeres eller overføres til andre bestemmelsessteder, hvor udstyret eller teknologien kan anvendes til alvorlige overtrædelser af denne lov.

I henhold til artikel 5 skal krænkelsen af den humanitære folkeret være »alvorlig«. Vejledning findes i brugervejledningen til fælles holdning 2008/944/FUSP, hvori det anerkendes, at »isolerede tilfælde af krænkelser af den humanitære folkeret ikke nødvendigvis er udtryk for modtagerlandets holdning til den humanitære folkeret«, men »at det bør give anledning til alvorlig bekymring, hvis der kan konstateres et vist overtrædelsesmønster, eller hvis modtagerlandet ikke har truffet passende foranstaltninger til at straffe overtrædelser«. Den Internationale Røde Kors Komité (ICRC) har udstukket retningslinjer for vurderingen af krænkelser af den humanitære folkeret med henblik på eksportkontrol. Ifølge ICRC er »krænkelser af den humanitære folkeret alvorlige, hvis de bringer beskyttede personer (f.eks. civile, krigsfanger, sårede og syge) eller genstande (f.eks. civile genstande eller civil infrastruktur) i fare, eller hvis de udgør en krænkelse af vigtige universelle værdier«. Krigsforbrydelser udgør f.eks. alvorlige krænkelser af den humanitære folkeret. ICRC nævner endvidere lignende faktorer, som der skal tages hensyn til, såsom brugervejledningen til fælles holdning 2008/944/FUSP, herunder formelle tilsagn om at anvende reglerne i den humanitære folkeret, passende foranstaltninger til at sikre ansvarlighed for krænkelser af den humanitære folkeret, uddannelse af militæret i den humanitære folkeret og forbud mod at rekruttere børn til væbnede styrker.

2. TEKNISK ANVENDELSESOMRÅDE

2.1. Cyberovervågningsprodukter, der er opført på listen

Tillægget til disse retningslinjer indeholder oplysninger om cyberovervågningsprodukter, der er opført i bilag I til forordningen, og skal hjælpe eksportører med at identificere potentielle cyberovervågningsprodukter, der ikke er opført på listen.

2.2. Potentielle cyberovervågningsprodukter, der ikke er opført på listen

Selv om det pr. definition er umuligt at opstille en udtømmende liste over de produkter, der kan kontrolleres som »produkter, der ikke er opført på listen« i henhold til artikel 5, kan følgende produkter potentielt overvåges og berettige særlig årvågenhed i henhold til forordningen.

Som præciseret i betragtning 8 i forordningen anses produkter, der anvendes til rent kommercielle formål, såsom fakturering, markedsføring, kvalitetstjenester, brugertilfredshed eller netværkssikkerhed, normalt ikke for at indebære risici for misbrug, som relevante i forbindelse med alvorlige krænkelser af menneskerettighederne eller den humanitære folkeret, og de er derfor generelt ikke underlagt kontrol i henhold til artikel 5. Mange af disse produkter har informationssikkerhedsmæssige (kryptografiske eller endda kryptoanalytiske) funktioner, der opfylder kontrolparametrene i kategori 5, del 2, i kontrolteksten i bilag I til forordningen. Sikkerhedsnetværksudstyr — herunder routere, omkoblere eller relæer, hvor informationssikkerhedsfunktionen er begrænset til opgaverne »drift, administration eller vedligeholdelse«, og som kun anvender offentliggjorte eller kommercielle kryptografiske standarder — er heller ikke omfattet af definitionen af »cyberovervågningsprodukter«, selv om eksportørerne fortsat bør være opmærksomme på forskellige rapporter om misbrug af sådanne produkter til menneskerettighedskrænkelser.

2.2.1. *Ansigts- og følelsesgenkendelsesteknologi*

Ansigts- og følelsesgenkendelsesteknologier har flere andre anvendelser end cyberovervågning — f.eks. identifikation eller autentifikation — og falder ikke automatisk ind under definitionen. Under visse omstændigheder kan ansigts- og følelsesgenkendelsesteknologier dog være omfattet af anvendelsesområdet for forordningens artikel 2, nr. 20).

Ansigts- og følelsesgenkendelsesteknologier, der kan anvendes til at overvåge eller analysere lagrede videobilleder, kan falde ind under definitionen af cyberovervågningsprodukter. Selv om ovennævnte kriterier er opfyldt, skal det imidlertid nøje undersøges, om softwaren er særligt udformet til skjult overvågning.

2.2.2. *Lokaliseringssporingsanordninger*

Lokaliseringssporingsanordninger gør det muligt at spore en enheds fysiske placering over tid, og nogle lokaliseringssporingsteknologier er blevet brugt af retshåndhævende myndigheder og efterretningstjenester i nogen tid. Deres potentiale for målrettet overvågning og masseovervågning har udviklet sig betydeligt, efterhånden som sporingsteknologier er blevet mere avancerede — herunder satellitbaseret lokaliseringssporing, mobilmastbaseret lokaliseringssporing, Wi-Fi- og Bluetooth-transceivere — og efterhånden som »sporingsanordninger« såsom smartphones og andre elektroniske anordninger (f.eks. køretøjsmonterede systemer i biler) er blevet udbredt.

Lokaliseringssporingsanordninger anvendes af retshåndhævende myndigheder og efterretningstjenester, f.eks. til at indsamle bevismateriale i forbindelse med en efterforskning eller til at spore mistænkte, men også af virksomheder til kommercielle formål, f.eks. rapportering om aggregerede bevægelsesmønstre i handelsgader, sporing af medarbejdere, der arbejder uden for virksomheden, eller til lokaliseringsbaseret reklame.

2.2.3. *Videoovervågningssystemer*

For at hjælpe eksportørerne med at identificere potentiel cyberovervågning er det også nyttigt at præcisere, hvilke produkter der ikke er omfattet af definitionen. I denne forbindelse er videoovervågningssystemer og -kameraer — herunder kameraer med høj opløsning — der anvendes til at filme personer i det offentlige rum, f.eks. ikke omfattet af definitionen af cyberovervågningsprodukter, da de ikke overvåger eller indsamler data fra informations- og telekommunikationssystemer.

3. FORANSTALTNINGER VEDRØRENDE PASSENDE OMHU

Betragtning 7 i forordningen har følgende ordlyd: »Det er afgørende, at eksportører […] bidrager til det overordnede mål om handelskontrol. For at de kan handle i overensstemmelse med denne forordning, skal vurderingen af risici i forbindelse med transaktioner, der er omfattet af denne forordning, foretages ved hjælp af foranstaltninger til screening af transaktioner, også kaldet princippet om passende omhu, som en del af et internt program til sikring af overholdelse (ICP)«.

I artikel 2, nr. 21), defineres et internt program til sikring af overholdelse (ICP) som »løbende effektive, passende og forholdsmæssige politikker og procedurer, der er vedtaget af eksportører for at fremme overholdelse af bestemmelserne og målene i denne forordning samt vilkårene og betingelserne for de tilladelser, der gennemføres i henhold til denne forordning, herunder foranstaltninger vedrørende passende omhu til vurdering af risici i forbindelse med eksport af produkterne til slutbrugere og endelige anvendelsesformål«.

Kommissionens henstilling (EU) 2019/1318 ([7]) danner en ramme, der skal hjælpe eksportørerne med at identificere, håndtere og begrænse risici, der er forbundet med kontrol af handel med produkter med dobbelt anvendelse, og sikre overholdelse af Unionens og medlemsstaternes relevante love eller bestemmelser.

Disse retningslinjer kan støtte eksportører, der gennemfører foranstaltninger til screening af transaktioner, også kaldet princippet om passende omhu, som en del af et internt program til sikring af overholdelse (ICP).

I henhold til artikel 5, stk. 2, i forordning (EU) 2021/821 skal eksportører af cyberovervågningsprodukter, der ikke er opført på listen, udvise passende omhu ved hjælp af foranstaltninger til screening af transaktioner, herunder ved at tage skridt til produktklassificering og risikovurdering af transaktioner. I praksis opfordres eksportørerne til at tage følgende op til fornyet overvejelse:

([7]) Kommissionens henstilling (EU) 2019/1318 af 30. juli 2019 om interne programmer til sikring af overholdelse af kontrol af handel med produkter med dobbelt anvendelse i henhold til forordning (EF) nr. 428/2009 (EUT L 205 af 5.8.2019, s. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Overveje, om et produkt, der ikke er opført på listen, og som skal eksporteres, kan være et »cyberovervågningsprodukt«, dvs. et produkt, som er særligt udformet til at give mulighed for skjult overvågning af fysiske personer gennem overvågning, uddragelse, indsamling eller analyse af data fra informations- og telekommunikationssystemer.**

Dette trin vedrører bestemmelsen af produktet i henhold til de bestemmelser, der gælder for cyberovervågningsprodukter. Dette omfatter en undersøgelse af produkternes tekniske karakteristika på grundlag af de tekniske parametre, der er fastsat i bilag I til forordningen for de produkter, der er opført på listen, og i lyset af de specifikke udtryk og begreber i definitionen af cyberovervågningsprodukter for produkter, der ikke er opført på listen, og den efterfølgende klassificering af produktet (varer, teknologi eller software).

3.2. **Undersøge det pågældende produkts kapaciteter for at fastslå risikoen for udenlandske slutbrugeres misbrug i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret.**

Eksportører bør foretage en vurdering for at fastslå, om produktet kan misbruges i forbindelse med intern undertrykkelse, krænkelser eller misbrug af menneskerettigheder, herunder retten til liv, frihed for tortur, umenneskelig og nedværdigende behandling, retten til privatlivets fred, retten til ytringsfrihed, retten til forenings- og forsamlingsfrihed, retten til tanke-, samvittigheds- og religionsfrihed, retten til ligebehandling eller forbud mod forskelsbehandling eller retten til frie, lige og hemmelige valg.

Det omfatter også en vurdering af, om produktet kan anvendes som en del af eller en komponent i et system, der kan resultere i de samme krænkelser og/eller det samme misbrug.

Eksportører bør i deres vurdering anvende såkaldte faresignaler, som indikerer, at der er unormale omstændigheder i en transaktion, som tyder på, at eksporten kan være bestemt til en uhensigtsmæssig slutanvendelse eller slutbruger eller et uhensigtsmæssigt bestemmelsessted.

Faresignaler:

a) produktet markedsføres med oplysninger om dets potentielle anvendelse til skjult overvågning

b) oplysninger om, at et lignende produkt er blevet misbrugt i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret (se afsnit 1.3)

c) oplysninger om, at produktet er blevet anvendt ulovligt i forbindelse med overvågningsaktiviteter rettet mod en medlemsstat eller i forbindelse med ulovlig overvågning af en EU-borger

d) oplysninger om, at transaktionen omfatter produkter, der kan anvendes til at oprette, tilpasse eller konfigurere et system, som man ved bliver misbrugt i forbindelse med intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret (se afsnit 1.3)

e) produktet eller et lignende produkt er opført på listen offentliggjort i C-udgaven af *Den Europæiske Unions Tidende*, jf. forordningens artikel 5, stk. 6.

3.3. **Til støtte for de kompetente myndigheder undersøge de interessenter, der er involveret i transaktionen (herunder slutbrugere og modtagere såsom distributører og forhandlere).**

Eksportørerne bør til støtte for de kompetente myndigheder og så vidt muligt:

a) før og under enhver transaktion undersøge, hvordan modtagerne og/eller slutbrugerne agter at anvende produktet eller tjenesten, på grundlag af erklæringer om den endelige anvendelse

b) gøre sig bekendt med situationen på det relevante bestemmelsessted for produkterne, navnlig med den generelle menneskerettighedssituation, da dette er en vigtig indikator for risikoen for alvorlige krænkelser af menneskerettighederne og den humanitære folkeret i forbindelse med en eksport

c) undersøge risici for, at produktet eller tjenesten omdirigeres til en anden uautoriseret slutbruger, baseret på nedenstående faresignaler.

Faresignaler:

a) Slutbrugeren har et åbenlyst forhold til en udenlandsk regering, der tidligere har tyet til intern undertrykkelse og/eller begået alvorlige krænkelser af menneskerettighederne og den humanitære folkeret.

b) Slutbrugeren er strukturelt en del af de væbnede styrker eller en anden gruppe, der er involveret i en væbnet konflikt, hvor der gøres brug af intern undertrykkelse, og/eller som tidligere har begået alvorlige krænkelser af menneskerettighederne og den humanitære folkeret.

c) Slutbrugeren har tidligere eksporteret cyberovervågningsprodukter til lande, hvor anvendelsen af sådanne produkter har medført intern undertrykkelse og/eller alvorlige krænkelser af menneskerettighederne og den humanitære folkeret.

3.4. **Anvende proceduren for passende omhu til at udarbejde planer for at forebygge og afbøde potentielle fremtidige negative indvirkninger.**

Eksportører bør på grundlag af deres procedure for passende omhu indstille aktiviteter, der forårsager eller bidrager til negative indvirkninger på menneskerettigheder, og udvikle og gennemføre en korrigerende handlingsplan. Sådanne foranstaltninger kan omfatte:

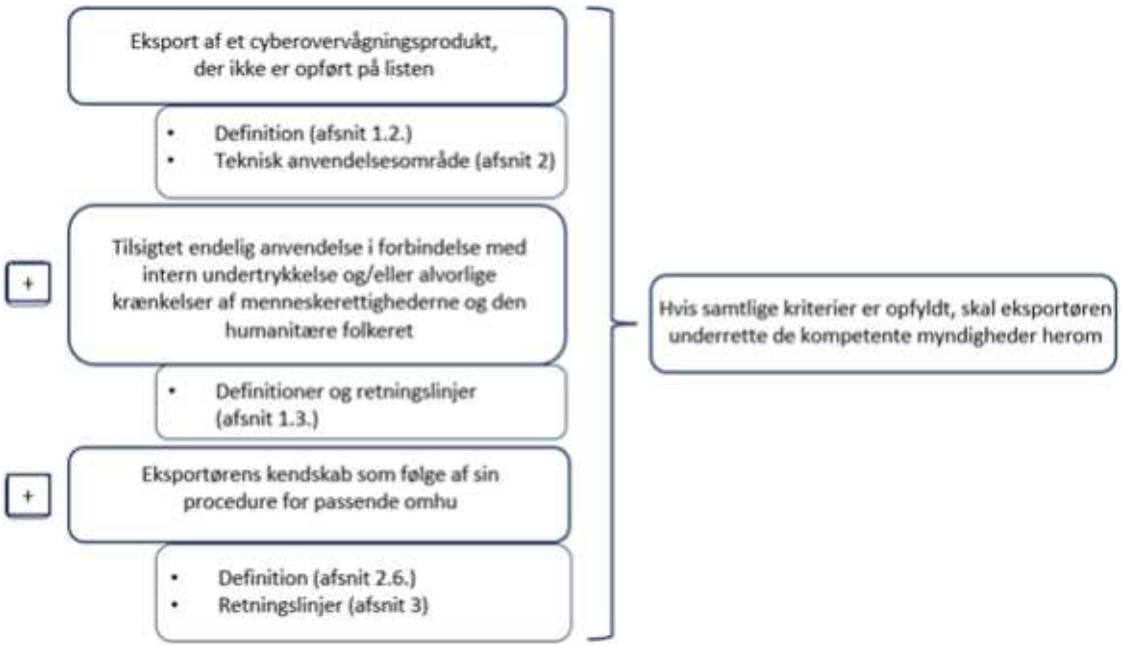
a) ajourføring af virksomhedens politikker for at vejlede om, hvordan de negative indvirkninger kan undgås og håndteres i fremtiden, og sikre, at de gennemføres

b) anvendelse af resultaterne af risikovurderingen til at ajourføre og styrke forvaltningssystemerne for bedre at kunne spore oplysninger og advare om risici, inden der opstår negative indvirkninger

c) indsamling af oplysninger for at få afdækket de overordnede risici for negative indvirkninger på sektoren

d) underretning af medlemsstaternes kompetente myndigheder om deres procedure for passende omhu for at lette informationsstrømmen vedrørende visse produkter, slutbrugere og bestemmelsessteder.

Krav i artikel 5, stk. 2, i forordning (EU) 2021/821



4. **TILLÆG**

Cyberovervågningsprodukter, der er opført på listen i bilag I til forordning (EU) 2021/821

— **Systemer til aflytning af telekommunikation (5A001.f.)**

I de fleste lande, herunder medlemsstaterne, er kommunikationshemmeligheden beskyttet ved lov, men offentlige myndigheders skjulte elektroniske overvågning af kommunikation kan tillades inden for lovens rammer (lovlig aflytning — Lawful Interception (LI)). Den digitale tidsalder indvarslede imidlertid muligheden for at anvende aflytningsteknologier i stor skala. Det libyske regimes anvendelse af aflytningsværktøjer fremhævede potentialet for at anvende disse teknologier i stor skala og ansporede til indførelse af eksportkontrol af systemer til aflytning af telekommunikation i 2012.

Denne kontrol anvendes på udstyr, der er beregnet til at udtrække indholdet af en kommunikation (tale eller data) samt identifikatorer for abonnementer eller andre metadata, der sendes via trådløs kommunikation, og radiofrekvensovervågningsudstyr. Denne kontrol gælder f.eks. for IMSI-fangere (International Mobile Subscriber Identity), der opfanger mobiltelefontrafik og sporer mobiltelefonbrugernes færden, eller for udstyr, der opretter falske Wi-Fi-hotspots, som kan uddrage IMSI-numre fra en telefon, samt for visse typer produkter, der er særligt udformet til at give mulighed for »deep packet inspection« i telekommunikationssystemer. Jammingudstyr til mobil telekommunikation er ikke omfattet af cyberovervågningsprodukter, da det ikke indsamler data.

Selv om teknologi til generelle formål kan anvendes til at opbygge sådanne systemer, vil systemernes aflytningskapacitet i stor skala afhænge af specifikke dele og komponenter, herunder f.eks. speciel software, eller applikationsspecifikke integrerede kredsløb, (f.eks. FPGA'er, ASIC'er osv.), der kan øge antallet af pakker, eller kommunikationssessioner, der kan behandles pr. sekund.

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

Selv om meget internetbaseret kommunikation nu typisk er krypteret som standard, kan aflytning af trafikdata (metadata) om kommunikation — såsom IP-adresser og hyppigheden og størrelsen af dataudvekslinger — stadig bruges til at identificere forbindelser mellem personer og domænenavne. Regeringer kan bruge disse systemer lovligt og med retsligt tilsyn til legitime formål, f.eks. til at identificere personer, der besøger domæner med tilknytning til kriminelt eller terrorrelateret indhold. Overvågning og analyse af internettrafik på grundlag af etnisk, religiøs, politisk eller social karakterisering kan imidlertid føre til en omfattende kortlægning af befolkningen og sociale forhold i et land med henblik på kontrol og undertrykkelse af befolkningen og andre formål, f.eks. identifikation af politiske systemkritikere. Ud over spørgsmål vedrørende menneskerettigheder og intern undertrykkelse kan disse produkter også bidrage til at øge den sikkerhedsmæssige og militære kapacitet.

Kontrollen under 5A001.j anvendes på internetkontrolsystemer, der opererer i et »carrier class-IP-net (f.eks. national IP-backbone)« med henblik på analyse, udtræk og indeksering af fremsendt metadataindhold (stemmer, videoer, beskeder, vedhæftede filer) på grundlag af »hard selectors« og kortlægning af enkeltpersoners sociale netværk. Disse produkter foretager »skjult overvågning«, fordi målpersonerne ikke er bekendt med aflytningen af kommunikationen. Kontrollen er derimod ikke rettet mod systemer, hvor en bruger eller en abonnent foretager en handling, eller hvor systemet interagerer med en bruger eller en abonnent, og anvendes f.eks. ikke på sociale netværk eller kommercielle søgemaskiner. Desuden anvendes kontrollen på systemer, der behandler data fra en internetudbyders kernenet, men den anvendes ikke på sociale netværk eller kommercielle søgemaskiner, der behandler data fra brugere.

— **Intrusionsoftware (4A005, 4D004 og den tilhørende kontrol under 4E001.a. og 4E001.c.)**

Intrusionsoftware gør det muligt for operatøren i det skjulte at få fjernadgang til en elektronisk enhed såsom en smartphone, bærbar computer, server eller en enhed, der er forbundet til tingenes internet, at få adgang til data, der er lagret på enheden, at aflytte via et kamera eller en mikrofon, der er indbygget i eller tilsluttet enheden, og at bruge enheden som et springbræt til at udføre angreb på udstyr, som enheden forbinder til, eller mod brugerens kontakter (»hacking via tredjepartsenheder«). Intrusionsoftware, f.eks. »software til fjernadgang«, der anvendes af IT-afdelinger i forbindelse med fjernsupport, kan anvendes til lovlige formål ([8]), men overvågningens skjulte karakter og omfanget af de oplysninger, der eventuelt indsamles, er forbundet med en høj risiko for krænkelse af retten til privatlivets fred og beskyttelse af personoplysninger og kan i alvorlig grad undergrave retten til ytringsfrihed.

([8]) Af klarhedshensyn skal der i forbindelse med cyberovervågningsprodukter, som er opført på listen i bilag I til forordningen om produkter med dobbelt anvendelse, indhentes en tilladelse til eksport til tredjelande, uanset om anvendelsen af produktet er lovlig.

Kontrollen under 4A005 omfatter software samt systemer, udstyr, komponenter og tilknyttet teknologi, som er specielt udviklet eller modificeret til generering, kommando og kontrol eller levering af »intrusionsoftware«, men anvendes ikke på selve »intrusionsoftwaren« som defineret i bilag I til forordningen. Disse cyberværktøjer kontrolleres som følge af den potentielle forstyrrelse og skade, de kan forårsage, hvis de anvendes og virker efter hensigten, men det er ikke hensigten med kontrollen, at den skal påvirke f.eks. cybersikkerhedsforskeres og industriens aktiviteter, da de har behov for at dele oplysninger vedrørende intrusionsoftware for at kunne udvikle rettelser til deres produkter og indføre dem inden offentliggørelsen af sårbarheder.

— **Software til overvågning af kommunikation (5D001.e.)**

Denne software er udformet med henblik på at blive brugt af bemyndigede retshåndhævende myndigheder til at overvåge og analysere data, der indsamles gennem målrettede foranstaltninger til opfangning af kommunikation, som en kommunikationstjenesteyder anmodes om. Denne software giver mulighed for søgninger på basis af »hard selectors« i kommunikationsindhold eller metadata ved anvendelse af en interface til lovlig aflytning og kortlægning af sociale netværk eller sporing af bestemte personers bevægelser baseret på resultaterne af søgningen. Denne software er bestemt til »skjult overvågning«, fordi den anvender data, der er indsamlet ved opfangning af kommunikation uden den pågældendes vidende. Den »analyserer« endvidere data indsamlet via »telekommunikationssystemer«. Softwaren installeres i systemer i statslige myndigheder (f.eks. faciliteten til retshåndhævelsesovervågning (LEMF)), og kontrollen anvendes ikke i systemer til sikring af overholdelse med lovlig aflytning (f.eks. styringssystemer og formidlingsanordninger med lovlig aflytning), der er kommercielt udviklet og installeret i kommunikationstjenesteyders systemer (f.eks. integreret i kommunikationsnetværket), og som tjenesteyderen driver og vedligeholder. Som præciseret i kontrol teksten underlægges »software«, der er specielt konstrueret eller modificeret til rent kommercielle formål såsom fakturering, Network Quality of Service (QoS), Quality of Experience (QoE), formidlingsanordninger eller mobilbetaling eller -banking, ikke eksportkontrol.

— **Produkter, der anvendes til at udføre kryptoanalyse (5A004.a.)**

Denne kontrol anvendes på produkter, der er udviklet til at sætte kryptografiske mekanismer ud af kraft med det formål at udlede konfidentielle variabler eller følsomme data, herunder klar tekst, kodeord eller krypteringsnøgler. Kryptografi bruges til at sikre fortroligheden af oplysninger, som er under overførsel og inaktive. Kryptoanalyse anvendes til at bryde denne fortrolighed, og denne teknologi giver derfor »mulighed« for skjult overvågning gennem overvågning, uddragelse, indsamling eller analyse af data fra informations- og telekommunikationssystemer.

— **Kriminaltekniske redskaber og efterforskningsredskaber (5A004.b., 5D002.a.3.b. og 5D002.c.3.b.)**

Kriminaltekniske redskaber og efterforskningsredskaber er udformet til at udtrække rådata fra en anordning (f.eks. en computer- eller kommunikationsanordning), således at dataene ikke manipuleres eller ødelægges og kan anvendes til retslige formål, dvs. i en strafferetlig efterforskning eller ved en domstol. Disse produkter omgår anordningens »autentifikation« eller adgangskontrol, således at rådata kan udtrækkes fra anordningen. Disse produkter anvendes af statslige og retshåndhævende myndigheder, men også af militære styrker til at udtrække og analysere data fra beslaglagt udstyr. Selv om de kan anvendes til lovlige formål, kan de imidlertid misbruges og dermed udgøre en risiko for følsomme eller kommercielle data.

Kriminaltekniske redskaber og efterforskningsredskaber, der ikke er »særligt udformet« til skjult overvågning, falder imidlertid ikke ind under definitionen af cyberovervågningsprodukter i artikel 2, nr. 20). Kriminaltekniske redskaber og efterforskningsredskaber, der kun udtrækker brugerdata, eller hvor dataene er ubeskyttede på anordningen, underlægges f.eks. ikke eksportkontrol i medfør af 5A004.b., og kontrollen anvendes heller ikke på fabrikantens produktions- eller prøvningsudstyr, systemadministratorværktøjer eller produkter, der udelukkende er rettet mod den kommercielle detailsektor, f.eks. produkter til oplåsning af mobiltelefoner. I betragtning af de mange forskellige typer teknologi afhænger anvendelsen af kontrol derfor af en vurdering af hvert enkelt produkt fra sag til sag.

Endelig skal det bemærkes, at der er andre overvågningsrelaterede produkter opført i bilag I til forordningen, som ikke bør anses for at falde ind under definitionen af cyberovervågningsprodukter, f.eks. jammingudstyr til mobil telekommunikation (5A001.f.), der er designet til at beskadige eller afbryde kommunikation eller systemer, intrusionsoftware, der ændrer et system (4D004), og akustisk laser detektionsudstyr (6A005.g.), der indsamler lyddata med en laser eller gør det muligt at lytte til samtaler på afstand (kaldes somme tider en »lasermikrofon«). På samme måde vil anvendelsen af UAV'er opført på listen til overvågningsformål ikke indebære, at disse produkter omfattes af definitionen af cyberovervågningsprodukter.