Europeiska unionens
officiella tidning

SV
L-serien

2024/2659

16.10.2024

KOMMISSIONENS REKOMMENDATION (EU) 2024/2659

av den 11 oktober 2024

om riktlinjer för export av cyberövervakningsprodukter i enlighet med artikel 5 i Europaparlamentets och rådets förordning (EU) 2021/821

THE EUROPEAN COMMISSION,

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 292, och

av följande skäl:

(1) Genom Europaparlamentets och rådets förordning (EU) 2021/821 ([1]) upprättas en unionsordning för kontroll av export, förmedling, transitering och överföring av samt tekniskt bistånd för produkter med dubbla användningsområden.

(2) Förordning (EU) 2021/821 åtgärdar risken för att cyberövervakningsprodukter används för att främja internt förtryck och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt.

(3) Enligt artiklarna 5.2 och 26.1 i förordning (EU) 2021/821 ska kommissionen tillgängliggöra riktlinjer för exportörer med avseende på cyberövervakningsprodukter som inte förtecknas, för att säkerställa att unionsordningen för exportkontroll på cybersäkerhetsområdet är effektiv och för att säkerställa ett konsekvent genomförande av förordning (EU) 2021/821.

(4) Denna rekommendation och den bifogade vägledningen syftar till att stödja exportörer i tillämpningen av kontroller på cyberövervakningsprodukter som inte förtecknas, bland annat genom due diligence-åtgärder för att bedöma riskerna i samband med exporten av sådana produkter.

(5) Den vägledning som bifogas denna rekommendation var föremål för omfattande samråd i expertgruppen för övervakningsteknik under 2022 och 2023 och tar hänsyn till synpunkter som inkom under ett offentligt samråd ([2]) som hölls andra kvartalet 2023.

(6) Det bör erinras om att denna rekommendation och den bifogade vägledningen inte är bindande. Exportörerna bör därför behålla ansvaret för att fullgöra sina skyldigheter enligt förordning (EU) 2021/821 medan kommissionen bör säkerställa att denna rekommendation behåller sin relevans över tid.

([1]) Europaparlamentets och rådets förordning (EU) 2021/821 av den 20 maj 2021 om upprättande av en unionsordning för kontroll av export, förmedling, transitering och överföring av samt tekniskt bistånd för produkter med dubbla användningsområden (EUT L 206, 11.6.2021, s. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

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

HÄRIGENOM REKOMMENDERAS FÖLJANDE.

Det rekommenderas att medlemsstaternas behöriga myndigheter och exportörerna tar hänsyn till vägledningen i bilagan till denna rekommendation för att fullgöra sina skyldigheter enligt artikel 5.2 i förordning (EU) 2021/821.

Utfärdad i Bryssel den 11 oktober 2024.

På kommissionens vägnar
Valdis DOMBROVSKIS
Verkställande vice ordförande

BILAGA

INNEHÅLL

INLEDNING

Unionens ram för exportkontroll som inrättades genom förordning (EU) 2021/821 (*förordningen*) syftar till att säkerställa att unionens och dess medlemsstaters internationella skyldigheter och åtaganden uppfylls, bland annat när det gäller regional fred, säkerhet och stabilitet samt respekt för mänskliga rättigheter och internationell humanitär rätt. Unionen och dess medlemsstater har därför genomfört de beslut som fattats inom ramen för de multilaterala exportkontrollsystemen och uppdaterat unionens kontrollförteckning i bilaga I till förordningen i enlighet med detta ([1]). Vidare hade de behöriga myndigheterna i medlemsstaterna redan innan artikel 5 blev tillämplig kontrollerat exporten av vissa förtecknade produkter som kan ha övervakningstillämpningar ([2]), med beaktande av riskerna för missbruk under vissa särskilda omständigheter. Vid exceptionellt allvarliga omständigheter har unionen infört sanktioner som begränsat exporten av viss övervakningsutrustning ([3]).

Förordningen är ett uttryck för unionens beslutsamhet att effektivt motverka risken för att cyberövervakningsprodukter används för att främja internt förtryck och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt. Genom förordningen införs i synnerhet nya bestämmelser om kontroll av export av cyberövervakningsprodukter som inte förtecknas, däribland en skyldighet för exportörer att underrätta den behöriga myndigheten ifall de känner till, enligt sina due diligence-resultat, att de ej förtecknade cyberövervakningsprodukter som exportörerna vill exportera helt eller delvis är avsedda för användning i samband med internt förtryck och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt. Förordningen uppmanar vidare kommissionen och rådet att tillgängliggöra riktlinjer för exportörer till stöd för ett effektivt genomförande av de nya kontrollerna av cyberövervakningsprodukter som inte förtecknas.

Dessa riktlinjer syftar därför till att stödja exportörer i tillämpningen av kontroller på cyberövervakningsprodukter som inte förtecknas, bland annat genom due diligence-åtgärder för att bedöma riskerna i samband med export av sådana produkter till slutanvändare och för slutanvändning i enlighet med de nya bestämmelserna i förordningen.

1. RELEVANTA RÄTTSLIGA BESTÄMMELSER, DEFINITIONER OCH CENTRALA BEGREPP

1.1 Översikt över relevanta rättsliga bestämmelser

Genom förordningen införs nya bestämmelser som specifikt föreskriver kontroll av export av cyberövervakningsprodukter som inte förtecknas i bilaga I till den förordningen och som helt eller delvis är, eller kan vara, avsedda för användning i samband med internt förtryck och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt. Det handlar om följande skäl och artiklar:

a) Skäl 8: ”För att hantera risken för att vissa cyberövervakningsprodukter som inte tas upp i förteckningen och som exporteras från unionens tullområde skulle kunna missbrukas av personer som medverkar till eller är ansvariga för att leda eller begå allvarliga kränkningar av mänskliga rättigheter eller internationell humanitär rätt är det lämpligt att införa kontroll av sådana produkter. Riskerna i samband med detta gäller särskilt fall där cyberövervakningsutrustning

([1]) Se i synnerhet kontroller avseende system för avlyssning av telekommunikation (5A001.f), system för internetövervakning (5A001.j.), intrångsprogram (4A005, 4D004 och relaterade kontroller enligt 4E001.a och 4E001.c) och programvara för övervakning som utförs av rättsväsendet (5D001.e). Se vidare, baserat på en bedömning från fall till fall, kontroller avseende vissa forensiska verktyg/utredningsverktyg (5A004.b 5D002.a.3.b och 5D002.c.3.b).

([2]) I synnerhet system för informationssäkerhet.

([3]) Se rådets förordning (EG) nr 765/2006 av den 18 maj 2006 om restriktiva åtgärder med anledning av situationen i Belarus och Belarus inblandning i Rysslands aggression mot Ukraina (EUT L 134, 20.5.2006, s. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Rådets förordning (EU) nr 359/2011 av den 12 april 2011 om restriktiva åtgärder mot vissa personer, enheter och organ med hänsyn till situationen i Iran (EUT L 100, 14.4.2011, s. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Rådets förordning (EU) nr 36/2012 av den 18 januari 2012 om restriktiva åtgärder med hänsyn till situationen i Syrien och om upphävande av förordning (EU) nr 442/2011 (EUT L 16, 19.1.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Rådets förordning (EU) nr 401/2013 av den 2 maj 2013 om restriktiva åtgärder mot Myanmar/Burma och om upphävande av förordning (EG) nr 194/2008 (EUT L 121, 3.5.2013, s. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); och rådets förordning (EU) 2017/2063 av den 13 november 2017 om restriktiva åtgärder med anledning av situationen i Venezuela (EUT L 295, 14.11.2017, s. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

är särskilt utformad för att möjliggöra intrång eller djup paketinspektion i informations- och telekommunikationssystem för att utföra dold övervakning av fysiska personer genom övervakning, extraktion, insamling eller analys av data, inbegripet biometriska uppgifter, från dessa system. Produkter som används för rent kommersiella tillämpningar såsom fakturering, marknadsföring, kvalitetstjänster, användarnöjdhet eller nätsäkerhet anses i allmänhet inte medföra sådana risker."

b) Skäl 9: "För att stärka den effektiva kontrollen av export av cyberövervakningsprodukter som inte tas upp i förteckningen och är det viktigt att ytterligare harmonisera tillämpningen av övergripande kontroller (*catch-all controls*) på detta område. I detta syfte har medlemsstaterna åtagit sig att stödja sådana kontroller genom att utbyta information sinsemellan och med kommissionen, särskilt när det gäller den tekniska utvecklingen av cyberövervakningsprodukter, och genom att vara vaksamma vid tillämpningen av sådana kontroller för att främja ett utbyte på unionsnivå."

c) I artikel 2.20 definieras cyberövervakningsprodukter som "produkter med dubbla användningsområden som är särskilt konstruerade för att möjliggöra dold övervakning av fysiska personer genom monitorering, extraktion, inhämtning eller analys av data från informations- och telekommunikationssystem".

d) Genom artikel 5 införs ett tillståndskrav för export av cyberövervakningsprodukter som inte förtecknas i bilaga I om exportören har informerats av den behöriga myndigheten om att produkterna i fråga helt eller delvis är, eller kan vara, avsedda för användning i samband med internt förtryck och/eller för att begå allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt (artikel 5.1). Vidare åläggs exportörer att underrätta den behöriga myndigheten om de känner till, enligt sina due diligence-resultat, att de cyberövervakningsprodukter som de avser att exportera helt eller delvis är avsedda för användning i samband med internt förtryck och/eller för att begå allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt (artikel 5.2). Den behöriga myndigheten ska besluta om tillstånd ska krävas för exporten i fråga.

e) I artikel 5.2 föreskrivs vidare att "[k]ommissionen och rådet ska tillgängliggöra riktlinjer för exportörer som avses i artikel 26.1".

1.2 **Centrala definitioner**

Förordningen innehåller skäl och bestämmelser som klargör specifika begrepp av betydelse för kontrollen av export av cyberövervakningsprodukter som inte förtecknas. Det är viktigt att exportörerna har en tydlig förståelse av dessa begrepp så att de på ett effektivt sätt kan genomföra due diligence och kontroller. Av särskild relevans är artikel 2.20 som omfattar följande exakta definition av 'cyberövervakningsprodukter': 'produkter med dubbla användningsområden som är särskilt konstruerade för att möjliggöra dold övervakning av fysiska personer genom monitorering, extraktion, inhämtning eller analys av data från informations- och telekommunikationssystem'.

Vid tillämpningen av dessa riktlinjer bör specifika aspekter av den definitionen förtydligas.

1.2.1 *'Särskilt konstruerade/särskilt utformade'*

En produkt är konstruerad/särskilt utformad för dold övervakning när dess tekniska egenskaper är lämpliga för och objektivt sett möjliggör dold övervakning av fysiska personer. Därför betyder begreppet 'särskilt konstruerade/särskilt utformade' att dold övervakning av fysiska personer ska vara det huvudsakliga syftet med utvecklingen och konstruktionen/utformningen av produkten. Ett sådant begrepp förutsätter dock inte att produkten uteslutande kan användas för dold övervakning av fysiska personer.

Såsom klargörs i skäl 8 i förordningen är produkter som används för rent kommersiella tillämpningar, exempelvis fakturering, marknadsföring, kvalitetstjänster, användarnöjdhet eller nätsäkerhet, inte särskilt utformade för hemlig övervakning av fysiska personer och omfattas därför inte av definitionen av cyberövervakningsprodukter. Även om produkter för övervakning av operativsystem inom industrin eller övervakning av användarnas trafik kan användas för övervakningsändamål, är dessa produkter till exempel inte it-övervakningsprodukter enligt definitionen, eftersom de inte är särskilt utformade för att möjliggöra hemlig övervakning av fysiska personer.

1.2.2 *'Dold övervakning'*

Produkter möjliggör dold övervakning i synnerhet i de fall då övervakningen inte är uppenbar för den berörda fysiska personen. Detta skulle vara fallet när de berörda personerna inte är medveten om förekomsten av cyberövervakningsprodukter och/eller dessas aktivitet och därmed inte har möjlighet att avlägsna sig från denna övervakning eller åtminstone anpassa sitt beteende till övervakningen. Även om övervakningen sker med hjälp av produkter som installerats eller används på offentlig plats kan insamlingen av data i vissa fall anses relevant för dold övervakning, i synnerhet om insamlade data kan omdirigeras, utvärderas eller behandlas för andra ändamål än de som den berörda fysiska personen har kännedom om. Med andra ord kan övervakningen anses som dold i enlighet med artikel 2.20 i förordningen om en fysisk person inte objektivt sett kan förvänta sig vara under övervakning.

1.2.3 *'Fysiska personer'*

Begreppet 'fysisk person' avser en levande människa i motsats till en juridisk person eller enhet, som därför inte omfattas av bestämmelserna. Begreppet omfattar inte övervakning av objekt, platser eller maskiner som sådana.

1.2.4 *'Monitorering, extraktion, inhämtning, analys av data'*

Enligt *Oxford English Dictionary* har de engelska orden *monitoring* (monitorering), *extracting* (extraktion), *collecting* (inhämtning) och *analysing* (analys) följande språkliga innebörd:

— *'monitoring'*: tillsyn, övervakning, avlyssning;

— *'extracting'*: hämtning;

— *'collecting'*: inhämtning, insamling;

— *'analysing'*: att fastställa eller skilja mellan delarna av någonting (komplext) för att avgöra dess struktur eller art och därmed förklara eller förstå det; att noggrant och metodiskt granska något i tolkningssyfte; att göra en kritisk analys eller dataanlalys av något.

Dessa begrepp innebär att de produkter som används för övervakning bör ha exakta tekniska kapaciteter för behandling av data för monitorering, inhämtning, extraktion eller analys av data, såsom t.ex. följande produkter:

a) Produkter som används för monitorering av data från informations- och telekommunikationssystem ([4]) (t.ex. filstorlek eller pakettrafik för de data som överförs i ett sådant system).

b) Produkter som extraherar data från informations- och telekommunikationssystem genom att de gör intrång och utför extraktioner (t.ex. intrångsprogram).

c) Produkter som möjliggör en analys av data som extraherats från informations- och telekommunikationssystem, inbegripet sådana som kan behandla kamerabilder som lagras i dessa system (t.ex. vissa typer av dataanalysteknik som används som en del av ansiktsigenkänningssystem).

Produkter som används för att endast monitorera informationssystem eller bevaka befolkningen via videoövervakningskameror och som gör det möjligt att fånga samtal, datautbyten, rörelser och individuella beteenden skulle inte utgöra cyberövervakningsprodukter enligt definitionen i förordningen, eftersom de inte är särskilt konstruerade för detta ändamål och måste användas tillsammans med annan teknik, såsom artificiell intelligens eller stordata. Systemet som helhet (där produkten används tillsammans med annan teknik som AI-teknik eller stordatateknik) kan dock potentiellt utgöra en cyberövervakningsprodukt enligt definitionen i artikel 2.20 i förordningen.

Det bör framhållas att även om det ges några exempel som är användbara som illustration ska definitionen och tillämpningsområdet för cyberövervakningsprodukter inte begränsas av dessa exempel, eftersom syftet med artikel 5 är att möjliggöra effektiv exportkontroll av produkter som inte förtecknas.

([4]) Se definitionen i 1.2.5 nedan.

Såsom framgår av användningen av konjunktionen ’eller’ i definitionen ska de förtecknade tekniska funktionerna anses som alternativ, och en produkt måste inte ha alla dessa tekniska kapaciteter för monitorering, extraktion inhämtning eller analys av data. Med andra ord räcker det att en produkt har en av dessa tekniska kapaciteter för att omfattas av definitionen av en cyberövervakningsprodukt enligt artikel 2.20.

1.2.5 *’Från informations- och telekommunikationssystem’*

Dessa begrepp avser system som elektroniskt behandlar information från t.ex. programmering/kodning, drift av PC-system (hårdvara) och annan informationshantering, inbegripet programvaruteknik, webbteknik, datateknik, lagringsteknik etc. samt vissa system som förmedlar information på distans, t.ex. tekniska system för överföring av ljud, signaler, text, andra tecken och bilder genom både trådbundna och trådlösa kanaler, via optiska fibrer, radio och andra elektromagnetiska system. Tillsammans innefattar dessa två begrepp en mängd olika system för överföring eller behandling av information. Det bör noteras att begreppen avser system och inte utrustning.

1.2.6 *’Medvetenhet’ och ’är avsedda för’*

Enligt artikel 5.2 i förordningen ska en exportör underrätta den behöriga myndigheten om exportören ’känner till […] att de cyberövervakningsprodukter som denna avser att exportera […] är avsedda’ för ’användning i samband med internt förtryck och/eller för att begå allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt’.

Begreppet ’känner till’ är inte ett nytt rättsligt begrepp utan har använts i samband med slutanvändarrelaterade tillståndskrav (s.k. övergripande kontroller, *catch-all controls*) enligt artiklarna 4, 6, 7 och 8 i förordningen). Att ’känna till’ innebär att exportören har säker kunskap om det avsedda missbruket. Enbart möjligheten för en sådan risk är inte tillräcklig för att fastställa medvetenhet. Begreppet ’medvetenhet’ kan dock inte likställas med passivitet. Det förutsätter att exportören har vidtagit åtgärder för att erhålla tillräcklig och adekvat kunskap för att bedöma riskerna i samband med exporten och säkerställa att förordningen efterlevs.

Angivelsen att produkterna måste vara ’avsedda för’ en relevant känslig slutanvändning innebär att exportören bör bedöma slutanvändningen från fall till fall, mot bakgrund av de särskilda omständigheterna i det enskilda fallet. *E contrario* skulle en teoretisk risk, alltså en risk som inte baseras på en faktabaserad bedömning av ett fall, för att produkterna skulle kunna användas på ett sätt som kränker de mänskliga rättigheterna inte vara tillräcklig för att anse att de är ’avsedda för’ ett specifikt missbruk enligt artikel 5.

1.3 **Internt förtryck, allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt**

Enligt artikel 15 i förordningen, där de aspekter som ska beaktas vid bedömningen av ett tillstånd fastställs, ska medlemsstaterna beakta alla relevanta aspekter, inbegripet de som täcks av rådets gemensamma ståndpunkt 2008/944/Gusp ([5]).

Genom artikel 5 i förordningen utvidgas kontrollerna till exporten av cyberövervakningsprodukter som inte förtecknas mot bakgrund av risken för att de ska användas i samband med internt förtryck, allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt. Gemensam ståndpunkt 2008/944/Gusp och användarguiden till denna gemensamma ståndpunkt ([6]) ger användbar vägledning i detta hänseende.

([5]) Rådets gemensamma ståndpunkt 2008/944/Gusp av den 8 december 2008 om fastställande av gemensamma regler för kontrollen av export av militär teknik och krigsmateriel (EUT L 335, 13.12.2008, s. 99, http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Se användarguiden till rådets gemensamma ståndpunkt 2008/944/Gusp om fastställande av gemensamma regler för kontrollen av export av militär teknik och krigsmateriel, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1 *Internt förtryck*

I artikel 2.2 i gemensam ståndpunkt 2008/944/Gusp fastställs att ’Internt förtryck anses inbegripa bl.a. tortyr och annan grym, omänsklig och förnedrande behandling eller bestraffning, summariska eller godtyckliga avrättningar, försvinnanden, godtyckliga gripanden och andra allvarliga kränkningar av de mänskliga rättigheter och de grundläggande friheter som anges i de relevanta internationella instrument som rör de mänskliga rättigheterna, inklusive den allmänna förklaringen om de mänskliga rättigheterna och den internationella konventionen om medborgerliga och politiska rättigheter’. Användarguiden till gemensam ståndpunkt 2008/944/Gusp ger vägledning om de faktorer som ska beaktas vid exportörens bedömning, däribland ’den tilltänkta slutanvändarens och generellt mottagarlandets nuvarande och tidigare uppförande vad gäller mänskliga rättigheter’.

1.3.2 *Allvarliga kränkningar av mänskliga rättigheter*

Missbruk av cyberövervakningsprodukter som inte förtecknas kan ha en negativ inverkan på ett brett spektrum av mänskliga rättigheter och direkt inkräkta på rätten till integritet och dataskydd. Godtycklig eller olaglig övervakning kan också kränka andra mänskliga rättigheter, såsom rätten till yttrandefrihet, föreningsfrihet, mötesfrihet, tankefrihet, samvetsfrihet och religionsfrihet samt rätten till likabehandling och förbud mot diskriminering och rätten till fria, rättvisa och hemliga val. I enskilda fall kan övervakning, inbegripet monitorering och inhämtande av information om fysiska personer, såsom människorättsförsvarare, aktivister, politiska personer, utsatta befolkningsgrupper och journalister, leda till hot, förtryck, godtyckliga frihetsberövanden, tortyr eller till och med utomrättsliga avrättningar. Därför bör exportörer i sina bedömningar beakta dessa aspekter relaterade till allvarliga kränkningar av mänskliga rättigheter.

Enligt internationell praxis måste alla begränsningar av mänskliga rättigheter vara ’lämpliga’ och i enlighet med internationella människorättsnormer. I praktiken betyder detta att det ska finnas ändamålsenliga skyddsmekanismer som säkerställer att begränsningarna föreskrivs i lagstiftning och upprätthåller det väsentliga innehållet i dessa rättigheter. I enlighet med proportionalitetsprincipen får inskränkningar endast göras om de är nödvändiga och verkligen tjänar ett legitimt syfte – till exempel nationell eller allmän säkerhet, allmän ordning, skydd av folkhälsan eller skydd av andras rättigheter och friheter.

Cyberövervakningsprodukter kan innefatta legitima och reglerade verktyg för brottsbekämpningstillämpningar, såsom tillämpningar för att förebygga, förhindra, utreda, avslöja eller lagföra brott, inbegripet på området terrorismbekämpning, eller för att verkställa straffrättsliga påföljder. Samtidigt kan cyberövervakningsprodukter också missbrukas och användas för allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt när de exporteras till förtryckande regimer eller privata slutanvändare och/eller till konfliktområden.

Därför behövs en bedömning av omständigheterna från fall till fall, inbegripet tillämpning av relevanta bestämmelser mot bakgrund av eventuella rapporter om allvarliga kränkningar av mänskliga rättigheter från behöriga organ såsom Förenta nationerna, unionen eller Europarådet. Det faktum att en kränkning av mänskliga rättigheter erkänns i information som offentliggörs av Förenta nationernas, unionens eller Europarådets behöriga organ kan tjäna som vägledning när ’allvarlighetsgraden’ i kränkningarna ska fastställas. Ett sådant uttryckligt erkännande från dessa organ är inte någon absolut nödvändighet, men en viktig faktor för att kriteriet ska uppfyllas.

Enligt villkoren i artikel 5 måste kränkningarna av mänskliga rättigheter vara ’allvarliga’. Användbar vägledning för kategoriseringen av möjliga kränkningar av mänskliga rättigheter som ’allvarliga’ finns i användarguiden till gemensam ståndpunkt 2008/944/Gusp. Enligt den användarguiden är det kränkningens art och konsekvenser som är avgörande, Systematiska och/eller utbredda kränkningar av mänskliga rättigheter brukar betraktas som allvarliga, men även kränkningar som inte är systematiska eller utbredda kan anses vara ’allvarliga’ – mot bakgrund av hur allvarlig handlingen är för de berörda personerna.

I bilaga II till användarguiden till gemensam ståndpunkt 2008/944/Gusp finns en icke uttömmande förteckning över de viktigaste internationella och regionala människorättsinstrumenten, däribland den internationella konventionen om medborgerliga och politiska rättigheter (ICCPR), konventionen mot tortyr och annan grym, omänsklig eller förnedrande behandling eller bestraffning, den europeiska konventionen om de mänskliga rättigheterna (konventionen) Europeiska unionens stadga om de grundläggande rättigheterna (stadgan), som kan ge viktig vägledning för tolkningen och tillämpningen av kriterierna till stöd för robusta människorättsbedömningar. Dessa instrument och deras respektive tilläggsprotokoll utgör de viktigaste normerna och standarderna på områdena mänskliga rättigheter och grundläggande friheter.

1.3.3 *Allvarliga kränkningar av internationell humanitär rätt*

Internationell humanitär rätt ('Genèverätten' eller 'krigets lagar') har utvecklats genom en rad internationella fördrag, framför allt Haagkonventionen, Genèvekonventionerna och deras två tilläggsprotokoll från 1977, och identifierar regler som i tider av väpnad konflikt syftar till att skydda människor som inte – eller inte längre – deltar i fientligheterna (t.ex. civila och sårade, sjuka eller tillfångatagna stridande) och ålägger krigförande parter begränsningar vad gäller medel och metoder för krigföring (Haagrätten).

Användningen av cyberövervakningsprodukter som inte förtecknas bör vara förenlig med internationell humanitär rätt vid användning som medel och metoder för krigföring i samband med en väpnad konflikt. Under sådana omständigheter ska risken för allvarliga kränkningar av internationell humanitär rätt beaktas inom ramen för förordningen och ska, precis som risken för allvarliga kränkningar av mänskliga rättigheter, bedömas mot bakgrund av den avsedda slutanvändningen för produkterna i det specifika fallet. Användarguiden till gemensam ståndpunkt 2008/944/Gusp ger vägledning om de faktorer som ska beaktas, däribland mottagarens aktuella och tidigare agerande i fråga om respekt för internationell humanitär rätt, mottagarens avsikter såsom de uttrycks genom formella åtaganden och mottagarens förmåga att garantera att överförd materiel eller teknik används på ett sätt som är förenligt med internationell humanitär rätt och inte avleds eller överförs till andra bestämmelseorter där den kan användas för allvarliga kränkningar av denna lag.

Enligt artikel 5 måste kränkningarna av internationell humanitär rätt vara 'allvarliga'. Vägledning finns i användarguiden till gemensam ståndpunkt 2008/944/Gusp, där det erkänns att '[i]solerade incidenter med kränkningar av internationell humanitär rätt ger inte med nödvändighet en rättvisande bild av mottagarlandets hållning till internationell humanitär rätt', men om 'det går att urskilja ett mönster av kränkningar eller om mottagarlandet inte har vidtagit lämpliga åtgärder för att bestraffa kränkningar bör detta anses vara grund för allvarliga farhågor'. Internationella rödakorskommittén (ICRC) har utfärdat riktlinjer för bedömningen av kränkningar av internationell humanitär rätt för exportkontrolländamål. Enligt Internationella rödakorskommittén är kränkningar av internationell humanitär rätt allvarliga om de utgör en risk för skyddade personer (t.ex. civilbefolkning, krigsfångar, sårade och sjuka) eller objekt (t.ex. civila objekt eller infrastruktur) eller om de strider mot viktiga universella värden. Krigsbrott utgör exempelvis allvarliga kränkningar av internationell humanitär rätt. Internationella rödakorskommittén nämner också liknande faktorer som bör beaktas som användarguiden till gemensam ståndpunkt 2008/944/Gusp, däribland formella åtaganden om att tillämpa den internationella humanitära rättens regler, ändamålsenliga åtgärder som säkerställer ansvarsskyldighet vid kränkningar av internationell humanitär rätt, utbildning i internationell humanitär rätt för militären och förbud mot att rekrytera barn till väpnade styrkor.

2. TEKNISKT TILLÄMPNINGSOMRÅDE

2.1 Cyberövervakningsprodukter som förtecknas

Tillägget till dessa riktlinjer innehåller information om cyberövervakningsprodukter som förtecknas i bilaga I till förordningen, för att hjälpa exportörerna identifiera potentiella cyberövervakningsprodukter som inte förtecknas.

2.2 Potentiella icke-förtecknade cyberövervakningsprodukter

Det är per definition omöjligt att tillhandahålla en uttömmande förteckning över produkter som får kontrolleras som 'produkter som inte förtecknas' i enlighet med artikel 5, men följande produkter kan ha potential för övervakning och kan kräva särskild vaksamhet inom ramen för förordningen.

Såsom klargörs i skäl 8 i förordningen anses produkter som används för rent kommersiella tillämpningar, exempelvis fakturering, marknadsföring, kvalitetstjänster, användarnöjdhet eller nätsäkerhet, i allmänhet inte medföra sådana risker för missbruk som är relevanta för allvarliga kränkningar av mänskliga rättigheter eller internationell humanitär rätt och omfattas därför inte av kontroll enligt artikel 5. Många av dessa produkter har informationssäkerhetsfunktioner (kryptografiska eller till och med kryptoanalytiska) som uppfyller kontrollparametrarna enligt kategori 5 del 2 i texten om kontroll i bilaga I till förordningen. Säkerhetsnätsutrustning – däribland routrar, switchar eller reläer, där funktionaliteten för informationssäkerhet är begränsad till "drift, administration eller underhåll" som enbart tillämpar publicerade eller kommersiella kryptografiska standarder – omfattas inte heller av definitionen av 'cyberövervakningsprodukter', även om exportörer ändå bör vara vaksamma och beakta olika rapporter om missbruk av sådana produkter för kränkningar av de mänskliga rättigheterna.

2.2.1 *Teknik för ansiktsigenkänning och känsloigenkänning*

Teknik för ansiktsigenkänning och känsloigenkänning har många andra användningsområden än cyberövervakning – t.ex. identifiering eller autentisering – och skulle inte automatiskt omfattas av definitionen. Under vissa omständigheter kan dock ansiktsigenkänning och känsloigenkänning omfattas av artikel 2.20 i förordningen.

Teknik för ansiktsigenkänning och känsloigenkänning som kan användas för att monitorera eller analysera lagrade videobilder kan omfattas av definitionen av cyberövervakningsprodukter. Även om ovannämnda kriterier uppfylls måste det dock noggrant undersökas om programvaran utformats specifikt för dold övervakning.

2.2.2 *Utrustning för positionsspårning*

Utrustning för positionsspårning tillåter spårning av en enhets fysiska position över tid, och viss positionsspårningsteknik har redan använts sedan en tid tillbaka av brottsbekämpande myndigheter och underrättelsetjänster. Utrustningens potential för riktad övervakning och massövervakning har utvecklats avsevärt i takt med att spårningstekniken blivit mer avancerad – inklusive satellitbaserad positionsspårning, basstationsbaserad positionsspårning, wifi- och bluetooth-sändare – och 'spårningsutrustning', såsom smarttelefoner och annan elektronisk utrustning (t.ex. fordonssystem i bilar) börjat användas mer allmänt.

Utrustning för positionsspårning används av brottsbekämpande myndigheter och underrättelsetjänster för att t.ex. samla in bevis under en utredning eller för att spåra misstänkta, men även av företag för kommersiella ändamål, t.ex. rapportering om aggregerade rörelsemönster på affärsgator, spårning av anställda som arbetar utanför arbetsplatsen eller för platsbaserad reklam.

2.2.3 *Videoövervakningssystem*

För att hjälpa exportörer identifiera potentiell cyberövervakning kan det också vara till nytta att klargöra vilka produkter som inte omfattas av definitionen. I detta hänseende omfattas inte exempelvis videoövervakningssystem och kameror – inbegripet kameror med hög upplösning – som används för att filma personer på offentlig plats – av definitionen av cyberövervakningsprodukter, eftersom de inte monitorerar eller inhämtar data från informations- och telekommunikationssystem.

3. DUE DILIGENCE-ÅTGÄRDER

I skäl 7 i förordning fastställs att 'Det är av avgörande betydelse att exportörer […] bidrar till det övergripande målet för handelskontrollerna. För att de ska kunna agera i enlighet med denna förordning måste bedömningen av risker i samband med transaktioner som omfattas av denna förordning göras genom transaktionsgranskningsåtgärder, även kallad due diligence-principen, som en del av interna efterlevnadsprogram'.

I artikel 2.21 definieras ett internt efterlevnadsprogram som 'fortlöpande effektiva, ändamålsenliga och proportionella policyer och förfaranden som antagits av exportörer för att underlätta efterlevnaden av bestämmelserna och målen i denna förordning och av villkoren i de tillstånd som genomförs enligt denna förordning, inbegripet, bland annat, due diligence-åtgärder för bedömning av risker relaterade till export av produkterna till slutanvändare och slutanvändningar'.

Kommissionens rekommendation (EU) 2019/1318 ([7]) ger en ram för att hjälpa exportörerna att identifiera, hantera och mildra risker i samband med kontroller av handel med produkter med dubbla användningsområden och att säkerställa förenlighet med relevanta lagar och andra författningar på unionsnivå och nationell nivå.

Denna vägledning kan stödja exportörer vid genomförandet av transaktionsgranskningsåtgärder, även kallad due diligence-principen, som en del av interna efterlevnadsprogram.

I enlighet med artikel 5.2 i förordning (EU) 2021/821 är en exportör av ej förtecknade cyberövervakningsprodukter skyldig att utföra due diligence genom transaktionsgranskningsåtgärder, vilket innebär att vidta åtgärder avseende produktklassificering och transaktionsriskbedömning. Rent konkret uppmanas exportörer att granska följande:

([7]) Kommissionens rekommendation (EU) 2019/1318 av den 30 juli 2019 om interna efterlevnadsprogram för kontroll av handel med produkter med dubbla användningsområden enligt rådets förordning (EG) nr 428/2009 (EUT L 205, 5.8.2019, s. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1 **Granska om den produkt som inte förtecknas kan vara en ’cyberövervakningsprodukt’, alltså särskilt konstruerad för att möjliggöra dold övervakning av fysiska personer genom monitorering extraktion, inhämtning eller analys av data från informations- och telekommunikationssystem**

Detta steg rör fastställandet av produkten enligt de bestämmelser som är tillämpliga på cyberövervakningsprodukter. Detta innefattar en undersökning av produkternas tekniska egenskaper, på grundval av de tekniska parametrar som anges i bilaga I till förordningen för de produkter som förtecknas, och mot bakgrund av de särskilda termerna och begreppen i definitionen av cyberövervakningsprodukter för produkter som inte förtecknas, samt mot bakgrund av den klassificering som sedan görs av produkten (varor, teknik eller programvara).

3.2 **Granska den berörda produktens kapaciteter, för att fastställa potentialen för missbruk i samband med internt förtryck och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt hos utländska slutanvändare**

Exportörer bör göra en bedömning för att fastställa om produkten skulle kunna missbrukas för internt förtryck, kränkningar av eller brott mot de mänskliga rättigheterna, inbegripet rätten till liv, frihet från tortyr och annan grym, omänsklig eller förnedrande behandling föreningsfrihet och mötesfrihet, tankefrihet, samvetsfrihet och religionsfrihet, rätten till likabehandling eller förbud mot diskriminering eller rätten till fria, jämlika och hemliga val.

Detta inbegriper också en bedömning för att fastställa om produkten kan användas som del eller komponent i ett system som kan resultera i samma kränkningar och/eller missbruk.

Exportörerna bör i sin bedömning använda så kallade varningsflaggor, som hänvisar till eventuella onormala omständigheter i en transaktion som tyder på att exporten kan vara avsedd för en olämplig slutanvändning, olämpliga slutanvändare eller en olämplig destination.

Varningsflaggor:

a) Produkten marknadsförs med information som rör dess potentiella användning för dold övervakning.

b) Det finns information som visar att en liknande produkt har missbrukats i samband med internt förtryck och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt (se avsnitt 1.3).

c) Information som visar att produkten olagligt har använts i övervakningsverksamhet riktad mot en medlemsstat eller vid olaglig övervakning av en EU-medborgare.

d) Information som visar att transaktionen omfattar produkter som skulle kunna användas för att inrätta, anpassa eller konfigurera ett system där det finns kännedom om missbruk i samband med internt förtryck och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt (se avsnitt 1.3).

e) Produkten eller en liknande produkt finns med i den förteckning som offentliggörs i C-serien av *Europeiska unionens officiella tidning* i enlighet med artikel 5.6 i förordningen.

3.3 **Till stöd för behöriga myndigheter, granska berörda parter som är involverade i transaktionen (däribland slutanvändare och mottagare såsom distributörer och återförsäljare)**

Exportörer bör, för att stödja de behöriga myndigheterna och i möjligaste mån göra följande:

a) Före och under varje transaktion, granska hur mottagarna och/eller slutanvändarna avser att använda produkten eller tjänsten, baserat på slutanvändningsintyg.

b) Bekanta sig med situationen på den berörda destinationen för produkterna, särskilt vad gäller det allmänna tillståndet för mänskliga rättigheter, eftersom detta är en viktig indikator på risken för allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt i samband med exporten.

c) Granska risken för att produkten eller tjänsten kommer att avledas till en annan obehörig slutanvändare, baserat på varningsflaggor i enlighet med nedanstående.

Varningsflaggor:

a) Slutanvändaren har en uppenbar relation till en utländsk regering som tidigare har utövat internt förtryck och/eller kränkningar av mänskliga rättigheter och internationell humanitär rätt.

b) Slutanvändaren är strukturellt sett en del av de väpnade styrkorna eller en annan grupp som tidigare varit involverad i en väpnad konflikt som inbegriper interna förtryckåtgärder och/eller allvarliga kränkningar av mänskliga rättigheterna och internationell humanitär rätt.

c) Slutanvändaren har i tidigare exporterat cyberövervakningsprodukter till länder där användningen av sådana produkter har gett upphov till interna förtryckåtgärder och/eller allvarliga kränkningar av mänskliga rättigheter och internationell humanitär rätt.

3.4 Använda iakttagelserna från due diligence för att utarbeta planer för att förhindra och mildra potentiella framtida negativa effekter

Exportörerna bör, baserat på sina due diligence-iakttagelser avbryta aktiviteter som orsakar eller bidrar till negativa effekter kopplade till mänskliga rättigheter, samt utarbeta och genomföra en korrigerande åtgärdsplan. Åtgärderna kan omfatta följande:

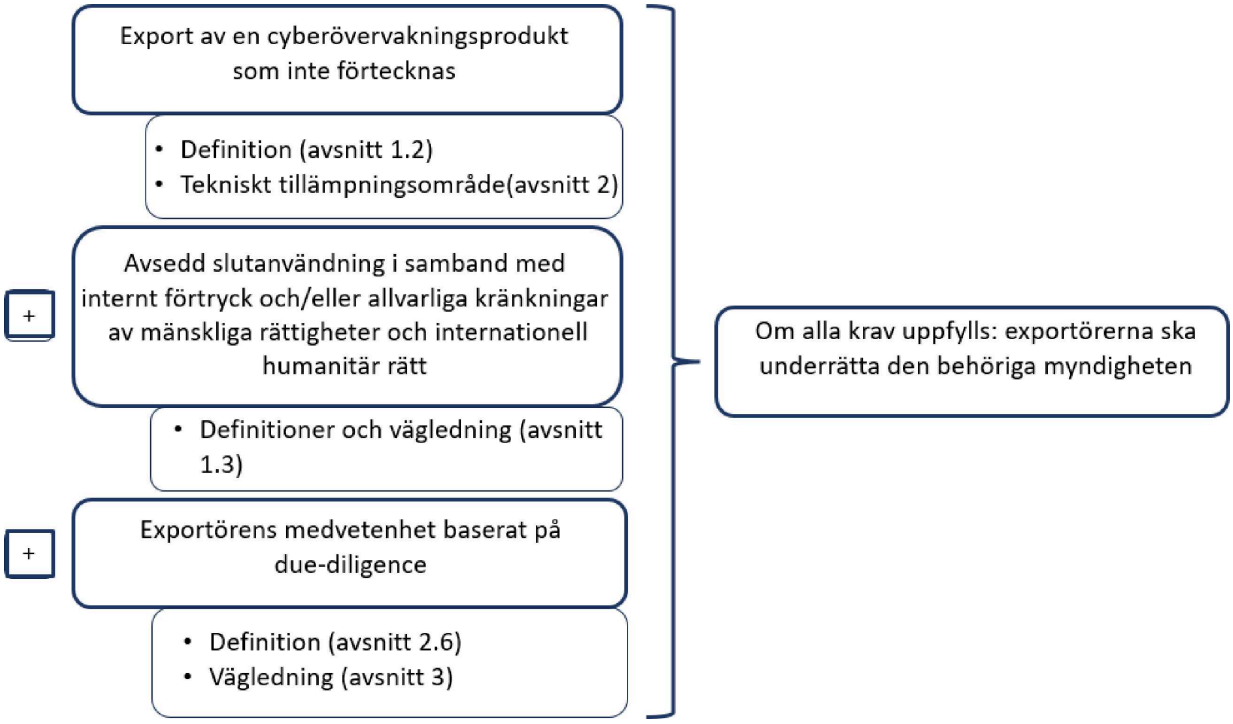
a) Uppdatera företagets policyer och tillhandahålla vägledning för hur man undviker och åtgärdar de negativa effekterna i framtiden och säkerställer genomförandet av dem.

b) På grundval av resultaten av riskbedömningen uppdatera och stärka förvaltningssystemen för att bättre spåra information och flagga för risker innan de negativa effekterna inträffar.

c) Samla in information för att få kunskap om högnivårisker med negativa effekter i sektorn.

d) Underrätta de behöriga myndigheterna i medlemsstaterna om due diligence-iakttagelser för att underlätta informationsflödet med avseende på vissa produkter, slutanvändare och destinationer.

Krav enligt artikel 5.2 i förordning (EU) 2021/821



4. TILLÄGG

Förtecknade cyberövervakningsprodukter som kontrollerats enligt bilaga I till förordning (EU) 2021/821

— **System för avlyssning av telekommunikation (5A001.f.)**

I de flesta länder, och även medlemsstaterna, skyddas konfidentialiteten för kommunikation av lagstiftning, men dold elektronisk övervakning av kommunikation som görs av myndigheter kan vara tillåten inom en rättslig ram (s.k. laglig avlyssning). I den digitala tidsåldern har det emellertid blivit möjligt att använda avlyssningsteknik i massiv omfattning. Den libyska regimens användning av avlyssningsverktyg riktade fokus mot potentialen för användning av sådan teknik i massiv omfattning och ledde till införandet av exportkontroll för system för telekommunikationsavlyssning 2012.

Denna kontroll är tillämplig på utrustning som utformats för att extrahera innehållet i ett meddelande (röst eller data) och abonnentens unika parametrar eller andra metadata som överförs via trådlös kommunikation, samt utrustning för radiofrekvensövervakning. Denna kontroll är t.ex. tillämplig på IMSI-fångare (*International Mobile Subscriber Identity*), som avlyssnar mobiltrafik och spårar rörelserna hos mobilanvändare, och på utrustning som skapar falska wifi-hotspots som kan extrahera IMSI-nummer från en telefon, samt på vissa typer av produkter som särskilt utformats för att möjliggöra djup paketinspektion i telekommunikationssystem. Utrustning för störning av mobil telekommunikation omfattas inte av definitionen av cyberövervakningsprodukter, eftersom den inte inhämtar data.

Även om teknik för allmänna ändamål kan användas för att skapa sådana system kommer dess kapacitet för massavlyssning att bero på specifika delar och komponenter, däribland särskild programvara, avancerade eller och applikationsspecifika kretsar (t.ex. FGPA-, ASIC-kretsar osv.) som ökar antalet paket eller kommunikationssessioner som kan behandlas per sekund.

— **System för internetövervakning (5A001.j.)**

Även om mycket internetbaserad kommunikation nu normalt sett krypteras som standard kan avlyssning av trafikdata (metadata) för kommunikation – såsom ip-adresser och datautbytes frekvens och storlek – ändå användas för identifiering av kopplingar mellan personer och domännamn. Myndigheter kan använda dessa system lagligt och med rättslig tillsyn för legitima syften, t.ex. för att identifiera personer som besöker domäner associerade med brottsligt innehåll eller terrorisminnehåll. Monitorering och analys av internettrafik på grundval av etnisk, religiös, politisk eller social karakterisering kan dock leda till en omfattande mänsklig och social kartläggning av ett land för kontroll och förtryck av befolkningen, och för andra syften som identifiering av politiska oliktänkare. Vid sidan av de frågor som rör mänskliga rättigheter och internt förtryck kan dessa produkter också bidra till att stärka säkerheten och de militära förmågorna.

Kontrollen enligt 5A001.j är tillämplig på internetkontrollsystem som använder ett IP-nät av carrier-klass (t.ex. ett nationellt IP-stamnät) för att analys, extraktion och indexering av överfört metadatainnehåll (tal, video, meddelanden, bilagor) baserat på ”hårda selektorer” och kartlägger människors kontaktnät. Detta är produkter som utför ”dold övervakning” eftersom de berörda personerna inte är medvetna om avlyssningen av kommunikationen. Kontrollerna inriktas däremot inte på system där en användares eller abonnents handling eller en interaktion med en användare eller abonnent förekommer, och de är inte tillämpliga på sociala nätverk eller kommersiella sökmotorer. Kontrollerna är också tillämpliga på system som behandlar data som kommer från en internetleverantörs stomnät, men inte på sociala nätverk eller kommersiella sökmotorer som behandlar data som lämnas av användarna.

— **”Intrångsprogram” (4A005, 4D004 och tillhörande kontroller enligt 4E001.a. och 4E001.c.)**

Intrångsprogram gör det möjligt för operatören att i hemlighet få fjärråtkomst till en elektronisk enhet, såsom en smarttelefon, en bärbar dator, en server eller en enhet med sakernas internet, för att erhålla data som lagrats på enheten, avlyssna via en kamera eller mikrofon som är inbyggd i eller ansluten till enheten och använda enheten som en språngbräda för att utföra attacker på utrustning som enheten ansluter sig till eller mot användarens kontakter (”hackande via tredje parts enhet”). Även om det finns legitima användningsområden ([8]) för intrångsprogram, t.ex. ”programvara för fjärråtkomst” som används av it-avdelningar för fjärrstöd, innebär övervakningens hemliga karaktär, och omfattningen av den information som det är möjligt att inhämta, en hög risk för kränkningar av rätten till integritet och dataskydd och detta kan allvarligt undergräva yttrandefriheten.

([8]) För tydlighetens skull, förtecknade cyberövervakningsprodukter som kontrolleras enligt bilaga I till förordningen om dubbla användningsområden skulle behöva ett tillstånd för att kunna exporteras till tredjeländer, oavsett om användningen av produkten är legitim.

Kontrollen enligt 4A005 et al innefattar såväl programvara som system, utrustning och komponenter samt tillhörande teknik, som är särskilt konstruerad eller modifierad för att generera, styra och kontrollera, eller leverera ”intrångsprogram”, men är inte tillämplig på själva ”intrångsprogrammet”, enligt definitionen i bilaga I till förordningen. Dessa cyberverktyg kontrolleras med hänsyn till de potentiella störningar och skador de kan orsaka om de används och det utförs framgångsrikt, men kontrollerna är inte avsedda att påverka t.ex. cybersäkerhetsforskares eller branschens verksamhet, eftersom de behöver utbyta information om intrångsprogam för att kunna utveckla lösningar för sina produkter så att sådana är på plats innan en sårbarhet släpps ut till allmänheten.

— **Programvara för övervakning av kommunikation (5D001.e.)**

Denna programvara är utformad för bemyndigade brottsbekämpande myndigheters monitorering och analys av data som inhämtas via riktade avlyssningsåtgärder som begärs från en leverantör av kommunikationstjänster. Den möjliggör sökningar baserat på ”hårda selektorer” i kommunikationsinnehåll eller metadata, med användning av ett gränssnitt för laglig avlyssning, och kartläggning av kontaktnät eller spårning av rörelser för de berörda individerna. Programvaran är avsedd för ”dold övervakning” eftersom den använder data som inhämtats genom avlyssning av kommunikation utan de berörda personernas vetskap. Den ”analyserar” också data som inhämtas via ”telekommunikationssystem”. Programvaran är installerad hos myndigheten (t.ex. rättsväsendets övervakningsanläggning) och kontrollen avser inte kontrollsystem för laglig avlyssning (*lawful interception, LI*) (t.ex. LI-förvaltningssystem och mediationsutrustning) som är kommersiellt utvecklade och installerade i kommunikationstjänsteleverantörens lokaler (t.ex. integrerade i kommunikationsnätet) och som tjänsteleverantören driver och underhåller. Såsom klargörs i kontrolltexten är kontroller inte tillämpliga på ”programvara” som är speciellt utformad eller modifierad för rent kommersiella ändamål, såsom fakturering, nätverkets servicekvalitet (QoS), upplevelsekvalitet (QoE), mediationsutrustning eller mobil betalning eller bankändamål.

— **Produkter som används för att utföra kryptoanalys (5A004.a.)**

Denna kontroll är tillämplig på produkter som konstruerats för att övervinna kryptografiska mekanismer för att utvinna konfidentiella variabler eller känsliga data, inklusive klartext, lösenord eller kryptografiska nycklar. Kryptografi används för att skydda informationens konfidentialitet vid överföring och i vila. Kryptoanalys används föra att övervinna denna konfidentialitet, och tekniken ”möjliggör” därför dold övervakning genom monitorering, extraktion, inhämtning eller analys av data från informations- och telekommunikationssystem.

— **Forensiska verktyg/utredningsverktyg (5A004.b., 5D002.a.3.b. och 5D002.c.3.b.)**

Forensiska verktyg/utredningsverktyg är utformade för att extrahera rådata från en enhet (t.ex. databehandling eller kommunikation) utan att dessa data manipuleras eller förvanskas och så att de kan användas för rättsliga ändamål, t.ex. i en brottsutredning eller i domstol. Dessa produkter tar sig förbi ”autentisering” eller auktorisationskontroller i enheten så att rådata kan extraheras från den. De används av myndigheter och brottsbekämpande organ och även av militära styrkor för extraktion och analys av data från beslagtagen utrustning. De kan ha legitima användningsområden, men kan också missbrukas och utgör därmed en risk för känsliga eller kommersiella uppgifter.

Forensiska verktyg/utredningsverktyg som inte är ”särskilt” konstruerade för dold övervakning faller inte under definitionen av cyberövervakningsprodukter i artikel 2.20. Forensiska verktyg/utredningsverktyg som endast extraherar användardata eller där data är oskyddade på enheten täcks inte av kontrolltexten i 5A004.b. et al. Samtidigt är kontrollerna inte tillämpliga på tillverkarens produktions- eller testutrustning, systemadministratörsverktyg eller produkter uteslutande till för den kommersiella återförsäljningssektorn som t.ex. upplåsningsprodukter för mobiltelefoner. Mot bakgrund av de många olika typerna av teknik avgörs därför tillämpningen av kontroller av en bedömning från fall till fall av varje enskild produkt.

Observera slutligen att det finns andra övervakningsrelaterade produkter som förtecknas i bilaga I till förordningen vilka inte bör anses falla under definitionen av cyberövervakningsprodukter, såsom utrustning för störning av mobil telekommunikation (5A001.f.) som konstruerats för att skada eller störa kommunikation eller system, intrångsprogram som modifierar ett system (4D004) och laserutrustning för akustisk detektion (6A005.g.) som inhämtar audiodata med laser eller möjliggör avlyssning av samtal på distans (ibland benämnd ”lasermikrofon”). En användning av förtecknade obemannade luftfartyg (UAV) för övervakningsändamål skulle inte heller innebära att dessa produkter omfattas av definitionen av cyberövervakningsprodukter.