Säkerhetspolisen

REMISSVAR

Datum: 2026-04-20
Diarienummer: 2026-3955-2

Mottagare:
Finansdepartementet
103 33 Stockholm
Referens: Fi2026/00350

Remissvar Europeiska kommissionens förslag till förordning om digitala nät KOM(2026)16

Säkerhetspolisen har tagit del av förslagen i EU-kommissionens förslag till förordning om digitala nät KOM(2026)16 (DNA-förordningen).

Sammanfattningsvis anser Säkerhetspolisen att det nuvarande förslaget inte tar hänsyn till att frågor om nationell säkerhet ligger inom varje medlemsstats ansvar och därmed utanför EU:s kompetens. Om förslaget går igenom i sin nuvarande form skulle Säkerhetspolisens och andra svenska myndigheters möjligheter att vidta åtgärder för att skydda Sveriges säkerhet kraftigt begränsas. Dessutom finns det risk för att verkställandet av hemliga tvångsmedel försvåras för brottsbekämpande myndigheter.

Resiliens (artiklarna 4-8)

I DNA-förordningen föreslås flera nya bestämmelser som syftar till att skapa resiliens mot påfrestningar orsakade av olika typer av störningar. Säkerhetspolisen bedömer att dessa artiklar ligger nära flera andra EU-rättsliga instrument som tagits fram senaste åren, exempelvis NIS 2-direktivet[1] eller som är under framtagning, EU-kommissionens förslag om en ny cybersäkerhetsförordning (CSA 2).[2] Det är oklart hur dessa regelverk förhåller sig till varandra och hur nationell lagstiftning på samma område kommer påverkas av DNA-förordningen. Ytterligare reglering medför att det sammantagna regelverket kan bli svårt att tillämpa.

Utöver det anger artikel 7.2 att det ska samlas in omfattande information om allmänna elektroniska kommunikationsnät i syfte att förbereda beredskapsplanering på EU-nivå. Säkerhetspolisen bedömer att sådan informationsinsamling rör nationell kritisk infrastruktur, och det framstår som potentiellt olämpligt att samla in och lagra sådan känslig information på det sätt som föreslås. Sådan information kan vara säkerhetsskyddsklassificerad. Sverige och andra medlemsstater bör kunna vägra lämna sådan information med hänvisning till artikel 346 (1a) föredraget om Europeiska unionens funktionssätt.

Tillstånd för allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster (artiklarna 9-11)

Idag är den som tillhandahåller allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster i Sverige skyldig att förhålla sig till en rad olika nationella regleringar som syftar till att beakta olika säkerhetsaspekter när det gäller elektronisk kommunikation. Det gäller exempelvis lagen (2022:482) om elektronisk kommunikation (LEK), säkerhetsskyddslagen (2018:585), cybersäkerhetslagen (2025:1506) och PTS föreskrifter och allmänna

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen.
[2] EU-kommissionens förslag till förordning om cybersäkerhet KOM(2026)11, innehållande förslag till förändring i förordning (EU) 2019/881 om Europeiska unionens cybersäkerhetsbyrå och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (CSA), samt riktade ändringar i NIS 2-direktivet.

råd (2022:11) om säkerhet i nät och tjänster. Det framstår dock som oklart hur den process kring ”single market authorisation and passporting” som beskrivs i artiklarna 9-11 förhåller sig till dessa regelverk, framförallt de regler som avser att skydda Sveriges säkerhet.

Artikel 9.1 anger att friheten att erbjuda elektroniska kommunikationsnätverk och kommunikationstjänster endast är begränsade av kraven i DNA-förordningen. Medlemsstater får bara begränsa rätten att erbjuda allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster på grund av ”public policy, public security or public health”. Nationell säkerhet räknas inte upp, vilket i avsaknad av närmare motivering i preambeln kan tolkas som att det inte kommer vara möjligt att begränsa en aktör från att erbjuda allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster med hänvisning till nationell säkerhet. Säkerhetspolisen motsätter sig en sådan ordning.

EU-kommissionens förslag innebär också att den nationella kompetenta myndigheten endast får ställa upp de villkor som räknas upp i artikel 9.4. Uppräkningen i artikel 9.4 är enligt Säkerhetspolisens bedömning ofullständig och innehåller flera oklarheter. Det framstår därför som oklart vilken rådighet svenska myndigheter kommer ha över de villkor som får ställas upp. Dessutom är det ett EU-organ som får mandat att utfärda riktlinjer för hur dessa villkor ska tillämpas, enligt artikel 11.1, vilket innebär ett betydligt minskat inflytande för svenska myndigheter i dessa frågor.

Som ett exempel innehåller artikel 9.4 (d) regelefterlevnadskrav kring cybersäkerhet, och CSA 2 nämns. CSA 2 innehåller vissa undantag för nationell säkerhet men är fortfarande under framtagande. Det framstår som oklart för Säkerhetspolisen hur regelefterlevnadskraven kring cybersäkerhet i artikel 9.4 (d) förhåller sig till nationell lagstiftning på samma område, samt hur detta förhåller sig till andra EU-rättsliga instrument inom cybersäkerhetsområdet, exempelvis NIS 2-direktivet. Området cybersäkerhet och informationssäkerhet är komplext, och det framstår som olyckligt att DNA-förordningen endast räknar upp vissa delar av regelverket som täcker detta område. DNA-förordningen innehåller dessutom inte några undantag för nationell säkerhet trots att de instrument som hänvisas till har sådana undantag. Eftersom det endast är de villkor som räknas upp i DNA-förordningen som får ställas enligt artikel 9.1 framstår det som att delar av nu gällande svensk lagstiftning kring cybersäkerhet och informationssäkerhet möjligtvis inte kommer kunna tillämpas vad gäller allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Liknande problematik gäller för vilka villkor som kan ställas upp för radiospektrumtillstånd och användningen av hemliga tvångsmedel, se vidare under dessa rubriker.

Enligt artikel 11.4 är det den nationella kompetenta myndigheten i den medlemsstat där tillståndet erhållits som ska vidta åtgärder (”penalties”) gentemot en aktör som bryter mot tillståndsvillkoren. Sannolikt kommer ”single market authorisation and passporting” innebära att flertalet aktörer väljer att söka tillstånd i en viss medlemsstat och verka i en annan, så kallad ”forumshopping”. Det får konsekvenser för de praktiska möjligheterna att utöva en effektiv tillsyn. Det finns en risk att svenska tillsynsmyndigheter kommer ha små möjligheter att verkställa åtgärder gentemot aktörer som bryter mot tillståndsvillkoren. Vidare ska EU-kommissionen ha mandat att via genomförandeakter harmonisera tillämpningen av DNA-förordningen enligt artikel 186, om det föreligger hinder för den inre marknaden. Det innebär att EU-kommissionen tillskriver sig själva möjligheten att styra över hur detaljerna i villkoren ska utformas. Även om artikel 11.4 anger att en nationell myndighet kan vidta åtgärder i enlighet med sin nationella lagstiftning är det oklart hur detta förhåller sig till att DNA-förordningen styr vilka villkor som kan ställas, enligt artikel 9.1.

Ett undantag till artikel 11.4 utgörs av artikel 11.5, där den nationella kompetenta myndigheten kan bötfälla aktörer om den nationella kompetenta myndigheten drar slutsatsen att ett brott mot tillståndsvillkoren kan ha en allvarlig negativ inverkan på nationell säkerhet inom det egna territoriet. Den nationella kompetenta myndigheten ska också, om det är lämpligt, konsultera med relevanta myndigheter i den medlemsstat där den aktuella aktören har fått sitt tillstånd.

När ett sådant förfarande som beskrivs i artikel 11.5 inleds har dock sannolikt skada för Sveriges säkerhet redan inträffat. En reglering som innebär att en svensk myndighet, eventuellt efter konsultation med myndigheter i en annan medlemsstat, endast kan bötfälla en aktör efter att avtalsbrott inträffat innebär i praktiken att det inte finns effektiva verktyg för att skydda Sveriges säkerhet. Enligt Säkerhetspolisen måste svenska myndigheter ha en möjlighet att på förhand vidta åtgärder eller ställa upp villkor, exempelvis genom svensk lagstiftning eller på andra sätt, för att skydda Sveriges säkerhet. Ett sådant mandat kan inte överlämnas till EU-kommissionen, EU-organ eller tillsynsmyndigheter i andra medlemsstater.

Radiospektrumtillstånd (artiklarna 13-35)

Enligt nuvarande ordning har Post och telestyrelsen (PTS) möjlighet att villkora tillstånd för att använda radiosändare med krav som är av betydelse för Sveriges säkerhet, enligt 3 kap. 12 § första stycket 9 LEK. Så har också skett, se framförallt Kammarrätten i Stockholms dom 2022-06-22, mål nr. 5222-21, 5223-21 där PTS efter samråd med Säkerhetspolisen och Försvarsmakten villkorade tillstånd att använda radiosändare i frekvensbanden, bland annat med att komponenter från vissa leverantörer inte fick användas samt vissa tekniskt inriktade villkor. Vidare ska PTS enligt nuvarande ordning endast bevilja tillstånd att använda radiosändare om det kan antas att radioanvändningen inte kommer att orsaka skada för Sveriges säkerhet, enligt 3 kap. 6 § första stycket 7 LEK.

Regelverket infördes under våren år 2020 och grundar sig i att regeringen menade att det måste finnas förutsättningar för staten att ingripa vid hot om IT-angrepp eller annan antagonistisk verksamhet som har betydelse för Sveriges säkerhet när den digitala infrastrukturen byggs ut. Digitaliseringen för med sig risker och hot av delvis okänd karaktär som innebär stora säkerhetsutmaningar som kan vara mycket komplexa. Hot är svårare att upptäcka, risker mer svårbedömda och beroenden svårare att överblicka. I detta sammanhang konstaterade regeringen att den EU-rättsliga regleringen inte hindrar att åtgärder vidtas för att skydda nationell säkerhet, med hänvisning till artikel 4.2 i fördraget om Europeiska unionen där det bland annat anges att den nationella säkerheten också i fortsättningen ska vara varje medlemsstats nationella ansvar.[3]

Så som Säkerhetspolisen förstår innehåller inte EU-kommissionens förslag några möjligheter för nationella myndigheter i medlemsstaterna att ingripa mot aktörer eller ställa villkor till skydd för medlemsstatens nationella säkerhet när det gäller tilldelning av radiospektrumtillstånd. Det finns en möjlighet att undanta vissa rättigheter att använda radiospektrum från delad användning om det är nödvändigt för bland annat nationell säkerhet enligt artikel 15.1 (c), men det finns inga regler kring att neka eller villkora en aktörs ansökan om användning av radiospektrum med hänvisning till nationell säkerhet.

Det innebär att PTS exempelvis inte längre skulle kunna ställa upp villkor för att förbjuda användningen av komponenter från vissa utpekade leverantörer på grund av att sådan användning kan utgöra ett hot mot Sveriges säkerhet, så som skedde i ovan nämnda dom. Det är även oklart i

[3] Se prop. 2019/20:15 s. 17 ff.

vilken mån PTS kan ställa upp mer tekniskt inriktade villkor. Säkerhetspolisen bedömer därför att EU-kommissionens förslag innebär att det inte längre kommer vara möjligt för svenska myndigheter att villkora tillståndsprocesser kring radiospektrumtillstånd för att skydda Sveriges säkerhet. Det innebär också att det inte alls verkar vara möjligt inom EU att villkora tillstånd för radiospektrumtillstånd med hänsyn till EU:s inre säkerhet.

Det finns också oklarheter kring hur dessa regler förhåller sig till krav och behov kring radiospektrumanvändning som finns inom Försvarsmakten, Försvarets radioanstalt, Nato, Säkerhetspolisen, Polismyndigheten och det civila försvaret, exempelvis att vissa aktörer idag inte omfattas av kravet på tillstånd att använda radiosändare enligt 3 kap. 3 § LEK. Framförallt kravet på att tillåta användning av radiofrekvenser som sådana aktörer för tillfället inte använder (”use it or share it”) enligt artikel 15.2 skulle kunna innebära svårigheter.

Tillstånd för satellitbaserad kommunikation (artiklarna 36-45)

Den process för tillstånd för satellitbaserad kommunikation som föreslås innehåller inte några relevanta regler som tar hänsyn till eventuella säkerhetshot som kan härröra från aktörer verksamma inom satellitbaserad kommunikation. Eftersom hela processen för tillståndsgivning kommer föras på EU-nivå frånhänder sig nationella myndigheter i praktiken inflytande över vilka aktörer som kommer ges satellittillstånd, om tillstånd söks i EU eller i flera medlemsstater. En sådan förflyttning skulle innebära att EU-kommissionen inom satellitkommunikation i praktiken får mandat att fatta beslut som kan röra medlemsstaternas nationella säkerhet.

Det framstår som problematiskt att det inte anges några regler kring möjligheten att neka aktörer tillstånd med hänvisning till medlemsstaternas nationella säkerhet, eller EU:s säkerhet. EU-kommissionen ger sig själva mandat att ta fram genomförandeakter där villkoren för tillstånd ytterligare kan utvecklas. Det framgår inte om sådana genomförandeakter ger mandat till EU-kommissionen att ställa upp villkor för att helt neka vissa aktörer att delta i tillståndsprocesser på grund av att aktören anses utgöra ett säkerhetshot. Mandat att besluta om sådana villkor i en genomförandeakt bör enligt Säkerhetspolisen i sådana fall hänvisas till i förordningen som ligger till grund för genomförandeakten. Vid en liknande situation som den ovan nämnda domen i Kammarrätten i Stockholm, men som gällde en aktör inom satellitbaserad kommunikation, skulle det som Säkerhetspolisen förstår inte finnas några möjligheter att ställa upp villkor för att utesluta vissa aktörer, med hänvisning till att deras inträde på den europeiska satellitkommunikations-marknaden skulle kunna innebära ett hot mot medlemsstaternas och/eller EU:s säkerhet.

Utöver det uppkommer praktiska problem kring hur EU-kommissionen ska kunna bedöma vilka aktörer som utgör säkerhetshot. Sådan information finns i normalfallet hos underrättelse- och säkerhetstjänster. Det finns ingen process eller informationsdelning, och det föreslås inte heller någon, där EU-kommissionen kan få ta del av de bedömningar som europeiska underrättelse- och säkerhetstjänster gör kring specifika aktörer verksamma inom satellitkommunikation, motsvararande det samrådsförfarande som finns mellan PTS, Säkerhetspolisen och Försvarsmakten. Att etablera en sådan informationsdelningsprocess från nationella underrättelse- och säkerhetstjänster till EU-kommissionen skulle innebära betydande svårigheter på flera sätt.

Sammanfattningsvis bedömer Säkerhetspolisen att EU-kommissionens förslag i denna del innebär att svenska myndigheters möjlighet att påverka vilka satellitoperatörer som tillåts vara verksamma i Sverige kommer vara i princip obefintlig. Det innebär att svenska myndigheter kommer ha små möjligheter att vidta åtgärder eller ställa upp villkor, exempelvis genom svensk lagstiftning eller på andra sätt, för att skydda Sveriges säkerhet. Så som Säkerhetspolisen förstår DNA-förordningen

verkar inte heller EU-kommissionen ha möjlighet att neka aktörer med hänvisning till eventuella säkerhetshot. EU-kommissionen och underliggande organ kommer dessutom inte ha de praktiska förutsättningarna att göra bedömningar kring vilka aktörer som kan utgöra säkerhetshot.

Reglering som påverkar användningen av hemliga tvångsmedel (artiklarna 9, 11 och 38)

Möjligheten för en medlemsstat att ställa upp ytterligare krav på tillhandahållare av allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster är inte begränsat till åtgärder som vidtas för att skydda den nationella säkerheten, utan den sträcker sig längre än så. Det har i tidigare EU-rättsakter uttalats att en EU-rättslig reglering på området elektronisk kommunikation inte åsidosätter medlemsstaternas möjlighet att vidta nödvändiga åtgärder för att tillåta utredning, upptäckt och lagföring av brott.[4] Denna princip behöver komma till uttryck även i DNA-förordningen. Det behöver säkerställas att det även i fortsättningen är möjligt att på området för elektronisk kommunikation ha nationell reglering inom dessa områden.

Vad gäller nationella myndigheters möjligheter att ställa krav kring verkställande av hemliga tvångsmedel, exempelvis anpassningsskyldighet och lagringsskyldighet, anges att sådana villkor får ställas enligt artikel 9.4 (e). Enligt artikel 11.1 ska dock EU-organ ha mandat att publicera riktlinjer för att säkerställa att villkor enligt artikel 9.4 tillämpas på ett koherent, icke-diskriminerande och proportionerligt sätt. Som Säkerhetspolisen förstår detta kan ett EU-organ därmed få betydande inflytande över hur villkoren kring verkställande av hemliga tvångsmedel utformas i Sverige. Det kan få omfattande konsekvenser för brottsbekämpande myndigheters praktiska arbete för att verkställa hemliga tvångsmedel. Till detta kommer problemen kring att utöva en effektiv tillsyn som nämnts ovan, på grund av utformningen av artikel 11.4.

Vad gäller satellitkommunikation går DNA-förordningen ett steg längre i regleringen av hemliga tvångsmedel. EU-kommissionen har via genomförandeakter mandat att själv utforma hur verkställigheten av hemliga tvångsmedel, inklusive datalagring, ska gå till enligt artikel 38.3 (e). Svenska myndigheter kommer därmed ha mycket små möjligheter att påverka villkoren för verkställande av hemliga tvångsmedel inom satellitkommunikation, vilket kan komma att medföra omfattande praktiska problem när ett verkställande av hemliga tvångsmedel ska genomföras.

Även om EU har kompetens att reglera vissa frågor kring verkställandet av hemliga tvångsmedel och brottsbekämpning är nationell säkerhet ofrånkomligen en aspekt av dessa områden när Säkerhetspolisen utreder brott som har bäring på Sveriges säkerhet. Aktörer kan behöva anpassa sin verksamhet till de särskilda krav som gäller för säkerhetskänslig verksamhet, vilket kan röra exempelvis hur teleoperatörer skyddar sina system, att viss personal ska placeras i säkerhetsklass och därför genomgå säkerhetsprövning, med mera. Möjligheten att ställa regulatoriska villkor på aktörer för att möta Säkerhetspolisens krav i dessa delar är avgörande för att Säkerhetspolisen ska ha praktiska möjligheter att använda hemliga tvångsmedel. Detta försämras vad gäller markbaserad elektronisk kommunikation och försvinner vad gäller satellitbaserad kommunikation.

I den utsträckning EU har kompetens att reglera frågor inom detta område finns det skäl att framhålla att det redan pågår arbete på EU-nivå som syftar till att säkerställa att brottsbekämpande myndigheter har effektiv tillgång till elektronisk information.[5] Ett av dessa initiativ anges som en

[4] Se skäl 7 i Europaparlamentets och rådets direktiv 2002/21/EG den 7 mars 2002.
[5] Se Roadmap for effective and lawful access to data for law enforcement COM(2025) 349 final, 24 juni 2025 samt det arbete som bedrivs av "High-Level Group (HLG) on access to data for effective law enforcement" inom EU, som lanserades av EU-kommissionen i juni 2023.

viktig leverans inom den europeiska strategin för inre säkerhet.[6] Det är viktigt att bevaka att de initiativ som tas i DNA-förordningen inte på något sätt motverkar eller försvårar detta arbete. I ljuset av vad som föreslås finns en risk för att det skapas parallella strukturer till de nationella myndigheternas brottsbekämpande uppdrag och samarbetskanaler. Frågor rörande dessa åtgärder bör istället lyftas ur DNA-förordningen och hanteras inom ramen för andra pågående initiativ.

Övergripande kommentar kring EU och nationell säkerhet

Som regeringen konstaterat hindrar den EU-rättsliga regleringen inte att åtgärder vidtas för att skydda nationell säkerhet.[7] Det har länge uttalats att en EU-rättslig reglering på området elektronisk kommunikation inte åsidosätter medlemsstaternas möjlighet att vidta nödvändiga åtgärder för att skydda en medlemsstats väsentliga säkerhetsintressen.[8] Vid implementeringen i svensk rätt av direktivet inom detta område konstaterade också regeringen, bland annat med hänvisning till artikel 4.2 fördraget om Europeiska unionen, att medlemsstaternas åtgärder till skydd för nationell säkerhet faller utanför direktivet.[9]

Säkerhetspolisen anser att det är viktigt att under förhandlingen av DNA-förordningen bevaka att principen som kommer till uttryck i artikel 4.2 EU-fördraget – att den nationella säkerheten också i fortsättningen ska vara varje medlemsstats nationella ansvar – inte urholkas. Denna fundamentala princip måste upprätthållas. Att endast göra vissa mycket begränsade undantag för nationell säkerhet i ett fåtal artiklar och i viss reglering helt bortse från medlemsstaternas legitima säkerhetsintressen är långt ifrån tillräckligt. Mot bakgrund av det som framförts ovan anser Säkerhetspolisen att DNA-förordningen riskerar att leda till en maktförskjutning av kompetens till EU som inte är förenlig med EU-fördraget.

Dessutom beskrivs det i EU-kommissionens europeiska strategi för inre säkerhet[10] som angeläget att med kraftfulla och hållbara åtgärder stärka den inre säkerheten och möta hoten från ett förändrat säkerhetspolitiskt läge och ett föränderligt geopolitiskt landskap. Behovet uppges vara särskilt tydligt i arbetet mot olika typer av hybridaktiviteter, där framförallt brottsbekämpande men även militära kapaciteter berörs och måste samverka som en resilienskedja. Medlemsstaterna och EU behöver säkerställa att den civila och den militära hanteringen av hoten samordnas med beaktande av medlemsstaternas ansvar för nationell säkerhet. EU-kommissionen föreslog i samma strategi att potentiella säkerhetskonsekvenser ska beaktas i framtida EU-politik oavsett politikområde. Regeringen fakta-PM angående denna strategi framhöll att nya initiativ behöver respektera medlemsstaternas ansvar för nationell säkerhet, samt kompetensfördelningen mellan medlemsstaterna och kommissionen respektive mellan rådet och kommissionen.[11] Dessa perspektiv verkar inte ha tagits i beaktande under arbetet med DNA-förordningen.

Detta remissvar har beslutats av säkerhetspolischefen Charlotte von Essen. Verksjuristen Simon Rose har varit föredragande.

[6] Se pressmeddelande ”Commission presents Roadmap for effective and lawful access to data for law enforcement”, 24 juni 2025 och ProtectEU: Europeisk strategi för inre säkerhet COM(2025) 148 final, 1 april 2025.
[7] Se exempelvis prop. 2019/20:15 s. 17.
[8] Se skäl 7 i Europaparlamentets och rådets direktiv 2002/21/EG den 7 mars 2002.
[9] Prop. 2021/22:136, s. 131.
[10] ProtectEU: Europeisk strategi för inre säkerhet COM(2025) 148 final, 1 april 2025.
[11] Faktapromemoria 2024/25:FPM37, EU:s inre säkerhetsstrategi, 6 maj 2025.