



Bruxelles, den 12. september 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

**Interinstitutionel sag:
2021/0106(COD)**

UDTALELSE FRA DEN JURIDISKE TJENESTE¹

fra:	Den Juridiske Tjeneste
Vedr.:	Forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens – Hensigtsmæssigheden af artikel 114 og 16 i TEUF som retsgrundlag for så vidt angår bestemmelserne vedrørende retshåndhævende og judicielle myndigheder

I. INDLEDNING

1. Den foreslåede forordning fastsætter harmoniserede regler for omsætning og ibrugtagning af systemer med kunstig intelligens ("AI-systemer") i Unionen ("den foreslåede forordning")².

¹ Dette dokument indeholder juridisk rådgivning, der er beskyttet i henhold til artikel 4, stk. 2, i Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter, og som Rådet for Den Europæiske Union ikke har gjort offentligt tilgængelig. Rådet forbeholder sig alle sine rettigheder i tilfælde af uautoriseret offentliggørelse.

² Dok. 8115/21.

2. På mødet i Gruppen vedrørende Telekommunikation og Informationssamfundet den 7. april 2022 tog Rådets Juridiske Tjeneste stilling til spørgsmålet om hensigtsmæssigheden af det dobbelte retsgrundlag (artikel 16 og 114 i TEUF) for den foreslåede forordning om systemer med kunstig intelligens ("AI-systemer"). Redegørelserne bekræftede, at artikel 16 og 114 i TEUF er det korrekte retsgrundlag for forslaget, og at det ikke er hensigtsmæssigt at anvende artikel 87, stk. 2, i TEUF i stedet for artikel 114 i TEUF. Efter anmodning fra gruppen er det indlæg, som repræsentanten for Rådets Juridiske Tjeneste gav på dette møde, i denne udtalelse formuleret skriftligt og yderligere uddybet.
3. AI-systemer defineres i artikel 3, nr. 1), i den foreslåede forordning. Generelt svarer de til bestemte typer software. Den foreslåede forordning finder anvendelse på både udbydere, der bringer AI-systemer i omsætning, og udbydere, der ibrugtager AI-systemer. Endvidere finder den foreslåede forordning også anvendelse på brugerne. En udbyder kan være en fysisk eller juridisk person eller en offentlig myndighed eller et organ, der udvikler eller får udviklet et AI-system med henblik på at bringe det i omsætning eller ibrugtage det under eget navn eller varemærke. En bruger kan være enhver fysisk eller juridisk person, offentlig myndighed eller ethvert agentur eller andet organ, der anvender et AI-system under sin myndighed.

4. I henhold til definitionerne i artikel 3 kan retshåndhævende og judicielle myndigheder betragtes som enten udbydere og/eller brugere af et AI-system. AI-systemer, hvis tilsigtede formål som defineret af udbyderen er retshåndhævelse eller anvendelse inden for retspleje, klassificeres som højrisikosystemer i bilag III. De er som sådan underlagt væsentlige krav (risikostyring, prøvning, datastyring, teknisk dokumentation, gennemsigtighed, menneskeligt tilsyn, nøjagtighed, robusthed og cybersikkerhed) og forpligtelser (såsom kvalitetsstyringssystemer, teknisk dokumentation, overensstemmelsesvurdering, korrigerende foranstaltninger, oplysningspligt samt forpligtelser for importører og distributører) samt standarder og overensstemmelsesvurdering. Disse harmoniserede regler er inspireret af dem, der gælder for produktsikkerhed i direktiv 2006/42/EF (maskiner)³ og forordning (EU) 2017/745 (medicinsk udstyr)⁴.
5. For så vidt angår AI-systemer, der indebærer anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse, er de omfattet af kategorien af forbudte AI-systemer. Der gælder dog undtagelser fra dette forbud mod anvendelse af AI-systemer. Det er således op til medlemsstaterne at afgøre, hvorvidt de vil tillade anvendelsen af sådanne systemer eller ej. I tilfælde af at de tillades, omfattes de af detaljerede restriktioner og sikkerhedsforanstaltninger for at begrænse deres anvendelse til det strengt nødvendige og for at beskytte den grundlæggende ret til beskyttelse af personoplysninger. Disse restriktioner og sikkerhedsforanstaltninger er fastsat i den foreslåede forordning på grundlag af artikel 16 i traktaten om Den Europæiske Unions funktionsmåde ("TEUF") og skal suppleres af national ret. Artikel 5, stk. 1, litra d), og artikel 5, stk. 2, 3 og 4, i den foreslåede forordning udgør *lex specialis* i forhold til direktiv (EU) 2016/680 (retshåndhævelsesdirektivet), som blev vedtaget på grundlag af artikel 16, stk. 2, i TEUF.

³ Europa-Parlamentets og Rådets direktiv 2006/42/EF af 17. maj 2006 om maskiner og om ændring af direktiv 95/16/EF (EUT L 157 af 9.6.2006, s. 24).

⁴ Europa-Parlamentets og Rådets forordning (EU) 2017/745 af 5. april 2017 om medicinsk udstyr, om ændring af direktiv 2001/83/EF, forordning (EF) nr. 178/2002 og forordning (EF) nr. 1223/2009 og om ophævelse af Rådets direktiv 90/385/EØF og 93/42/EØF (EUT L 117 af 5.5.2017, s. 1).

I overensstemmelse med artikel 5, stk. 1, litra d), er formålet med disse systemer begrænset til:

- i) målrettet eftersøgning af specifikke potentielle ofre for kriminalitet, herunder forsvundne børn
- ii) forebyggelse af en specifik, væsentlig og overhængende trussel mod fysiske personers liv eller fysiske sikkerhed eller om et terrorangreb
- iii) afsløring, lokalisering, identifikation eller retsforfølgning af en gerningsmand, der har begået, eller af en person, der mistænkes for at have begået, en strafbar handling, der er omhandlet i artikel 2, stk. 2, i afgørelsen om en europæisk arrestordre⁵, og som i den pågældende medlemsstat kan straffes med frihedsstraf eller en anden frihedsberøvende foranstaltning af en maksimal varighed på mindst tre år som fastsat i denne medlemsstats lovgivning.

I henhold til artikel 5, stk. 3, skal retshåndhævende myndigheders anvendelse af sådanne teknologier være betinget af en forudgående tilladelse fra en judiciel eller administrativ myndighed. I behørigt begrundede hastetilfælde kan anvendelsen af systemet dog påbegyndes uden tilladelse, og der kan anmodes om tilladelse under eller efter anvendelsen.

I henhold til artikel 5, stk. 4, kan en medlemsstat beslutte at tillade anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse og fastsætte de nødvendige detaljerede regler for anmodning, udstedelse og benyttelse af den forudgående tilladelse samt de relaterede strafbare handlinger.

6. Den foreslåede forordnings retsgrundlag er artikel 16 i TEUF (beskyttelse af personoplysninger) og artikel 114 i TEUF (det indre markeds funktion). Spørgsmålet er derfor, hvorvidt disse retsgrundlag er hensigtsmæssige i forhold til de harmoniserede regler, der gælder for de AI-systemer, som udbydes eller anvendes af retshåndhævende og judicielle myndigheder.

⁵ Rådets rammeafgørelse 2002/584/RIA af 13. juni 2002 om den europæiske arrestordre og om procedurerne for overgivelse mellem medlemsstaterne (EFT L 190 af 18.7.2002, s. 1).

7. Denne udtalelse fokuserer først og fremmest på hensigtsmæssigheden af retsgrundlaget i artikel 114 i TEUF, navnlig i forbindelse med retshåndhævende myndigheder, som nævnes i flere bestemmelser i den foreslåede forordning, bl.a. i forbindelse med systemer til biometrisk fjernidentifikation i realtid på offentlige steder og højrisiko-AI-systemer som omhandlet i bilag III, punkt 6. Den behandler derfor spørgsmålet om, hvorvidt artikel 87, stk. 2, i TEUF (politisamarbejde) ville være et mere hensigtsmæssigt retsgrundlag til at dække de retshåndhævende myndigheders udbud og anvendelse af AI-systemer i stedet for artikel 114 i TEUF (afsnit II). Tilsvarende kan konklusionen i denne note anvendes på de judicielle myndigheder, der nævnes i bilag III, vedrørende højrisiko-AI-systemer.
8. Denne note omhandler også hensigtsmæssigheden af artikel 16 i TEUF som supplerende retsgrundlag og anvendelsen af protokol 21 og 22 i forbindelse med retshåndhævende myndigheders anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder (afsnit III).

II. HENSIGTSMÆSSIGHEDEN AF ARTIKEL 114 I TEUF SOM RETSGRUNDLAG

9. Ifølge fast retspraksis afhænger retsgrundlaget for en EU-retsakt ikke af institutionens egen opfattelse med hensyn til det formål, der forfølges, men skal fastlægges efter objektive kriterier, som gør det muligt at foretage en domstolskontrol, herunder navnlig retsaktens formål og indhold. Hvis en gennemgang af en retsakt viser, at den har et dobbelt formål, eller at den består af to led, og det ene af disse kan bestemmes som det primære eller fremherskende, mens det andet kun er sekundært, skal retsakten have et enkelt retsgrundlag, nemlig det, der kræves af det primære formål eller led. Det gælder kun undtagelsesvis, at hvis det godtgøres, at der med retsakten samtidig forfølges flere formål, der er uløseligt forbundne, uden at et af disse formål er sekundært og indirekte i forhold til det andet, kan en sådan retsakt dog baseres på de dertil svarende forskellige retsgrundlag, medmindre disse retsgrundlag foreskriver procedurer, der er uforenelige med hinanden. Det skal også bemærkes, at det i artikel 114, stk. 1, første punktum, i TEUF slås fast, at artiklens bestemmelser finder anvendelse, "[m]edmindre andet er bestemt i traktaterne". Dermed er anvendelsen af artikel 114 i TEUF kun berettiget, hvis ingen anden mere specifik bestemmelse kan udgøre hjemmel for vedtagelse af den omhandlede retsakt⁶. Når der i traktaten forefindes en mere specifik bestemmelse, som kan udgøre hjemmel for den omhandlede retsakt, skal retsakten have hjemmel i denne bestemmelse⁷.

⁶ Udtalelse fra Rådets Juridiske Tjeneste af 17. maj 2016, 9007/16, punkt 6.

⁷ Dom af 29. april 2004, *Kommissionen mod Rådet*, C-338/01, EU:C:2004:253, præmis 60.

A. FORMÅLET MED DEN FORESLÅEDE FORORDNING

10. Den foreslåede forordning harmoniserer omsætningen, ibrugtagningen og anvendelsen af en bestemt type software (AI-systemer). Det forhold, at offentlige myndigheder og private operatører kan være udbydere eller brugere af sådanne AI-systemer, er ikke i sig selv uforeneligt med retsgrundlaget i artikel 114 i TEUF⁸.
11. Desuden er det forhold, at retshåndhævende myndigheder eller dem, der handler på deres vegne, kan være blandt udbyderne eller brugerne af sådanne AI-systemer, ikke tilstrækkeligt til at begrunde anvendelsen af retsgrundlaget i artikel 87 i TEUF. Den foreslåede forordnings formål og indhold skal analyseres for at kunne afgøre, hvorvidt dette er nødvendigt.
12. Den foreslåede forordning har generelt til formål, herunder med hensyn til systemer til biometrisk fjernidentifikation i realtid på offentlige steder og højrisiko-AI-systemer, at sikre et konsekvent og højt beskyttelsesniveau i hele Unionen og samtidig forhindre, at forskelle hæmmer den frie bevægelighed for AI-systemer og relaterede varer og tjenesteydelser på det indre marked. Forordningen fastsætter ensartede forpligtelser for operatører og garanterer en ensartet beskyttelse af tvingende almene hensyn og personers rettigheder i hele det indre marked (betragtning 2). Nærmere bestemt fastsætter den foreslåede forordning regler for omsætning og ibrugtagning af visse AI-systemer for at sikre et velfungerende indre marked og give disse systemer mulighed for at drage fordel af princippet om fri bevægelighed for varer og tjenesteydelser (betragtning 5). Overordnet set søger forslaget at etablere en pålidelig kunstig intelligens gennem design, der gælder over hele linjen, med et komplet sæt regler for udvikling, omsætning og anvendelse af AI-baserede produkter, tjenester og systemer. Eftersom kunstig intelligens allerede indgår i et stort antal tjenester og produkter og fortsat vil gøre det i fremtiden, følger forslaget det indre markeds logik med fastlæggelsen af en "produktsikkerhedsramme", der bygger på fire risikokategorier. Forslaget indfører krav til markedsadgang for og certificering af højrisiko-AI-systemer gennem en obligatorisk CE-mærkningsprocedure.

⁸ Jf. Udtalelse fra Rådets Juridiske Tjeneste (ST 11395/14, punkt 39-41) og præcedens såsom direktiv (EU) 2016/2102 samt direktiv 2014/24/EU, 2014/25/EU og 2014/23/EU.

13. Ingen af de erklærede mål i den foreslåede forordning vedrører sikring af målene for den offentlige sikkerhed. Selv om målene for den offentlige sikkerhed indirekte skal nås gennem harmoniseringen af de retshåndhævende myndigheders omsætning/ibrugtagning/anvendelse af AI-systemer, har Domstolen⁹ med fortolkningen af artikel 87, stk. 2, i TEUF på baggrund af artikel 67 i TEUF fastslået, at for at en EU-retsakt, henset til dens formål og indhold, kan være baseret på førstnævnte artikel, skal den være direkte forbundet med de formål, der er fastsat i artikel 67 i TEUF (dvs. i dette tilfælde forebyggelse af kriminalitet og politisamarbejde). Dette er udelukket i tilfældet med den foreslåede forordning, da de eneste harmoniserede regler for de retshåndhævende myndigheders anvendelse af sådanne systemer enten er 1) produktsikkerhedsregler, der finder ensartet anvendelse på alle udbydere og brugere i forbindelse med omsætning/ibrugtagning eller anvendelse af AI-systemer, eller 2) regler om beskyttelse af personoplysninger, for hvilke retsgrundlaget i artikel 16 i TEUF blev tilføjet (jf. del III nedenfor).
14. Selv om formålet med ændringen af direktivet om våben i en anden sag¹⁰ var at sikre et højere niveau af offentlig sikkerhed i forbindelse med terrortruslen og andre former for kriminalitet, fastslog Domstolen, at harmoniseringen af aspekter vedrørende sikre varebevægelser er et af de væsentligste elementer med henblik på at sikre et velfungerende indre marked, idet forskellige lovgivninger på dette område kan skabe hindringer for samhandelen¹¹.

⁹ Dom af 6. maj 2014, *Europa-Kommissionen mod Europa-Parlamentet og Rådet for Den Europæiske Union*, C-43/12, EU:C:2014:298.

¹⁰ Dom af 3. december 2019, *Den Tjekkiske Republik mod Europa-Parlamentet*, C-482/17, EU:C:2019:1035.

¹¹ Ibid. præmis 57: "*Da det særlige kendetegn ved skydevåben i modsætning til det af Republikken Polen hævdede ikke kun er deres sikkerhedsudfordringer for brugerne, men også for den brede offentlighed, således som Domstolen allerede har bemærket i præmis 54 i dom af 23. januar 2018, Buhagiar m.fl. (C-267/16, EU:C:2018:26), anses beskyttelsen af den offentlige sikkerhed, som anført i femte betragtning til direktiv 91/477, for nødvendig inden for rammerne af en lovgivning om erhvervelse og besiddelse af disse varer*". Jf. også dom af 23. januar 2018, *Albert Buhagiar m.fl. mod Minister for Justice*, C-267/16, EU:C:2018:26, præmis 54: "*I denne henseende skal det bemærkes, at den frie bevægelighed for skydevåben, henset til den sikkerhedsrisiko for mennesker, som disse udgør, kun har kunnet opnås ved hjælp af en streng regulering af betingelserne for overførsel heraf mellem medlemsstaterne, hvilke bl.a. omfatter princippet om forudgående tilladelse udstedt af de medlemsstater, som berøres af overførslen af sådanne varer*".

15. Formålene med den foreslåede forordning, herunder artikel 5, stk. 1, litra d), og artikel 5, stk. 2, 3 og 4, om anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse og de bestemmelser vedrørende højrisiko-AI-systemer, der er omhandlet i bilag III, punkt 6, er ikke direkte knyttet til et mål for den offentlige sikkerhed. Tværtimod imødekommer forslaget de vigtigste betænkeligheder med hensyn til, hvordan AI-systemer påvirker sundhed, sikkerhed og grundlæggende rettigheder. De relevante bestemmelser er derfor direkte knyttet til målet om at sikre lige vilkår i forbindelse med omsætning/ibrugtagning eller anvendelse af AI-systemer på det indre marked, samtidig med at brugernes sundhed, sikkerhed og grundlæggende rettigheder beskyttes.
16. I lyset af ovenstående er hovedformålet med den foreslåede forordning at forbedre det indre markeds funktion som omhandlet i artikel 114 i TEUF, og de mål, der er omhandlet i artikel 67 i TEUF, er kun indirekte og accessorisk knyttet til dette hovedformål.

B. DEN FORESLÅEDE FORORDNINGS INDHOLD

17. Den foreslåede forordning indeholder primært regler om, hvad der er nødvendigt for at bringe et specifikt produkt (en AI-software) i omsætning (eller for at tage det i brug) for at sikre, at det er sikkert og respekterer de grundlæggende rettigheder. Den indeholder et komplet sæt regler for udvikling, omsætning og anvendelse af AI-drevne produkter, tjenester og systemer. Den foreslåede forordning forpligter ikke de retshåndhævende myndigheder til at anvende et AI-system, der lovligt bringes i omsætning, og regulerer heller ikke direkte, hvordan de retshåndhævende myndigheder bør anvende et sådant AI-system. Den afgrænser i stedet tydeligt de situationer, hvor den tilsigtede anvendelse anses for at udgøre en høj risiko, netop fordi et AI-system vil blive anvendt af retshåndhævende eller judicielle myndigheder.

18. I øvrigt indeholder artikel 29 i den foreslåede forordning regler for betingelserne for anvendelse af højrisiko-AI-systemer, men en sådan bestemmelse er ikke sektorspecifik, har et begrænset anvendelsesområde (hovedsagelig vedrørende produktets brugsanvisning) og er uløseligt forbundet med de forpligtelser, der påhviler udviklere af AI-systemer i henhold til den foreslåede forordning. Artiklen giver også medlemsstaterne et vist spillerum til at fastsætte yderligere regler for anvendelsen af sådanne højrisiko-AI-systemer. Med hensyn til systemer til biometrisk fjernidentifikation i realtid på offentlige steder, der anvendes med henblik på retshåndhævelse (artikel 5), regulerer den foreslåede forordning delvis anvendelsen af sådanne systemer ud fra et databeskyttelsesperspektiv på grundlag af artikel 16 i TEUF (jf. del III nedenfor).
19. Desuden er det kun medlemsstaterne, der kan beslutte at give mulighed for helt eller delvist at tillade anvendelse af sådanne systemer til biometrisk fjernidentifikation i realtid. De specifikke betingelser for en sådan anvendelse skal fortsat fastsættes i national ret, men skal overholde de generelle kriterier og sikkerhedsforanstaltninger, der er fastsat i forordningen: forudgående retlig eller administrativ tilladelse, anmodning, udstedelse og benyttelse af den forudgående tilladelse samt angivelse af de strafbare handlinger, i forbindelse med hvilke sådanne systemer kan anvendes.

20. AI-systemer er en bestemt type software. De harmoniserede regler, der gælder for omsætning eller ibrugtagning/anvendelse af AI-systemer, er således produktsikkerhedslignende harmoniserede regler. De anvendes på en ensartet måde uden at skelne mellem offentlige og private brugere. I henhold til de relevante betragtninger i den foreslåede forordning bør der derfor sikres et ensartet og højt beskyttelsesniveau i hele Unionen. Samtidig bør forskelle, der hæmmer den frie bevægelighed for AI-systemer og relaterede varer og tjenesteydelser på det indre marked, forhindres. Det ville kunne opnås ved at fastsætte ensartede forpligtelser for operatører og garantere en ensartet beskyttelse af tvingende almene hensyn og personers rettigheder i hele det indre marked på grundlag af artikel 114 i TEUF¹².
21. Den foreslåede forordning indeholder flere henvisninger til retshåndhævelse, grænsekontrol og retspleje i bilag III om højrisiko-AI-systemer (henholdsvis punkt 6, 7 og 8). Disse omfatter en detaljeret og udtømmende opregning, der svarer til artikel 6, stk. 2, ud over andre højrisikosystemer i forbindelse med produktsikkerhedsrisici, jf. artikel 6, stk. 1. I henhold til artikel 6, stk. 1, skal nogle AI-systemer således pr. definition betragtes som højrisikosystemer på grund af deres forventede alvorlighed og høje risici for de grundlæggende rettigheder, sundheden og sikkerheden. Andre systemer, der betragtes som højrisikosystemer, og som er opført i bilag III, omfatter uddannelse, forvaltning af kritisk infrastruktur, beskæftigelse, biometrisk identifikation og kategorisering samt adgang til væsentlige offentlige og private tjenester.

¹² Der er derfor behov for en EU-retlig ramme, der fastsætter harmoniserede regler for kunstig intelligens, for at fremme udviklingen, anvendelsen og udbredelsen af kunstig intelligens på det indre marked, som samtidig opfylder et højt beskyttelsesniveau for offentlige interesser, såsom sundhed og sikkerhed og beskyttelse af grundlæggende rettigheder, som anerkendt og beskyttet i EU-retten. For at nå dette mål bør der fastsættes regler for omsætning og ibrugtagning af visse AI-systemer for at sikre et velfungerende indre marked og give disse systemer mulighed for at drage fordel af princippet om fri bevægelighed for varer og tjenesteydelser (jf. betragtning 2 og 5 i forslaget).

22. Sådanne regler om højrisiko-AI-systemer fastsætter imidlertid ikke, om de retshåndhævende og judicielle myndigheder (eller myndighederne på de andre identificerede områder) bør eller ikke bør anvende disse systemer. Den foreslåede forordning vil kun indirekte have indvirkning på den faktiske udvikling af AI-systemer, der kan anvendes af retshåndhævende myndigheder, og på de AI-systemer, der anvendes i øjeblikket og i fremtiden. Reglerne henviser således til AI-systemer, der er "*beregnet til at blive anvendt*" af sådanne myndigheder (jf. f.eks. artikel 3, nr. 12), artikel 8, stk. 2, og bilag III). Konsekvensen af at opføre et bestemt AI-system som et højrisikosystem er, at der skal anvendes et særligt sæt regler om risikostyring, datastyring og tekniske specifikationer. Brugere af sådanne højrisiko-AI-systemer skal overholde brugsanvisningen, opbevare logfiler og foretage konsekvensanalyser vedrørende databeskyttelse.
23. Desuden kan der i EU-retten eller national ret fastsættes andre brugerforpligtelser end dem, der vedrører brugsanvisningen, og uden at det berører brugerens mulighed for selv at tilrettelægge sine egne ressourcer og aktiviteter med henblik på at gennemføre de af udbyderen angivne foranstaltninger til menneskeligt tilsyn (artikel 29, stk. 2, i den foreslåede forordning). I disse regler fastsættes der yderligere garantier for grundlæggende rettigheder for højrisiko-AI-systemer.

24. På baggrund af ovenstående bør det understreges, at den foreslåede forordning ikke indeholder regler, der har til formål at tillade eller forhindre, at et højrisiko-AI-system, der bringes i omsætning, anvendes af de retshåndhævende myndigheder. Ifølge de foreslåede regler vil der blive anbragt en særskilt mærkning (højrisiko) på et AI-system, der udvikles eller anvendes af de retshåndhævende myndigheder som følge af dets tilsigtede anvendelse. Denne anvendelse vil blive reguleret af national ret, og de retshåndhævende myndigheder vil i et vist omfang selv træffe afgørelse herom. I den foreslåede forordning fastsættes der faktisk minimumsbetingelser for anvendelse af højrisiko-AI-systemer i artikel 29 (begrænset til brugsanvisninger), herunder dem, der er opført i punkt 6, 7 og 8 i bilag III, som vil blive suppleret af national ret. Der bør derfor i overensstemmelse med Domstolens retspraksis skelnes mellem på den ene side det tilsigtede formål med den foreslåede forordning, som ikke er at regulere de retshåndhævende myndigheders anvendelse af AI-systemer, og på den anden side de virkninger, som den indirekte kan have¹³, og som er irrelevant for analysen af retsgrundlagets hensigtsmæssighed.
25. Punkt 6, 7 og 8 (henholdsvis retshåndhævelse, migration og retspleje) er ikke fremherskende blandt højrisiko-AI-systemer. I henhold til den foreslåede forordning er et højrisiko-AI-system således ikke nødvendigvis et system, der er opført i bilag III. De fleste højrisikosystemer er faktisk dem, der er anført generelt i artikel 6, stk. 1, litra a) og b), i den foreslåede forordning (i forbindelse med produktsikkerhed). Andre højrisiko-AI-systemer er opført i bilag III, der indeholder punkt 1 (biometrisk identifikation), 2 (kritisk infrastruktur), 3 (uddannelse og erhvervsuddannelse) og 4 (beskæftigelse, forvaltning af arbejdstagere og adgang til selvstændig virksomhed), som vedrører andre områder end retlige og indre anliggender ("RIA"). Alle brugere af sådanne højrisiko-AI-systemer er omfattet af en ensartet ordning, der ikke er fastsat ud fra deres specifikke status (f.eks. om de er en økonomisk operatør eller en offentlig myndighed), men med henblik på beskyttelse af sundhed, sikkerhed og grundlæggende rettigheder.

¹³ Jf. Domstolens dom af 21. juni 2018, *Republikken Polen mod Europa-Parlamentet, Rådet for Den Europæiske Union*, C-5/16, EU:C:2018:483, præmis 63-68, og Domstolens dom af 22. juni 2022, *Leistritz AG mod LH*, C-534/20, EU:C:2022:495, præmis 28.

26. Den foreslåede forordning indeholder således harmoniserede regler for omsætning, ibrugtagning og anvendelse af AI-systemer, uanset om de anvendes af private operatører eller offentlige myndigheder, herunder tillige¹⁴ retshåndhævende og judicielle myndigheder.
27. Bortset fra anvendelsen af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse, som er underlagt særlige regler om behandling af personoplysninger (jf. del III nedenfor), indeholder den foreslåede forordning ingen harmoniserede regler for anvendelsen af højrisiko-AI-systemer. Som anført i punkt 18 og 19 ovenfor vedrører henvisningen til anvendelsen af højrisiko-AI-systemer i det væsentlige produktets brugsanvisning (artikel 29) og er knyttet til de forpligtelser, der påhviler udviklere. Som anført i punkt 22 skal afgørelsen om, hvorvidt de retshåndhævende eller judicielle myndigheder kan anvende et højrisiko-AI-system, der lovligt bringes i omsætning i henhold til den foreslåede forordning, træffes i henhold til national ret og af de nationale myndigheder.
28. Artikel 87, stk. 2, i TEUF, navnlig litra a), er derfor ikke et hensigtsmæssigt retsgrundlag for den foreslåede forordning. Reglerne i forslaget hverken fremmer eller hindrer indsamling, opbevaring, behandling, analyse og udveksling af relevante oplysninger. Når sådanne aktiviteter udføres af retshåndhævende myndigheder, vil det helt enkelt være nødvendigt at overholde en række ikkespecifikke, harmoniserede betingelser for at beskytte brugernes rettigheder. Ligeledes omfatter de erklærede mål i den foreslåede forordning ikke udvikling af fælles efterforskningsteknikker. De foreslåede krav vedrørende anvendelse af højrisiko-AI-systemer er ikke specifikke for RIA-området, og de vedrører ikke politisamarbejde i snæver forstand som defineret i TEUF.

¹⁴ Jf. Domstolens udtalelse om *Istanbulkonventionen*, A-1/19, EU:C:2021:198, navnlig præmis 298 og 301.

29. Med hensyn til bestemmelserne i artikel 5, stk. 4, i den foreslåede forordning kan en medlemsstat stadig beslutte at tillade anvendelse af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse. Når det er tilfældet, har medlemsstaten pligt til at fastsætte de nødvendige detaljerede regler for anmodning, udstedelse og benyttelse af den forudgående tilladelse samt de relaterede strafbare handlinger, for hvilke anvendelse er tilladt med henblik på efterforskning eller retsforfølgning ¹⁵. På grundlag af resultatet af drøftelserne i Rådet vil disse foreslåede regler ikke medføre, at de respektive nationale myndigheder tildeles nye beføjelser. I stedet indskrænkes anvendelsen af eksisterende eller mulige fremtidige mekanismer med henblik på at sikre beskyttelsen af retten til privatlivets fred og personoplysninger.
30. På baggrund af ovenstående er artikel 114 i TEUF det eneste hensigtsmæssige retsgrundlag for harmoniserede regler for højrisiko-AI-systemer, herunder dem, der anvendes af retshåndhævende og judicielle myndigheder, og ethvert RIA-retsgrundlag i tredje del, afsnit V, i TEUF, såsom artikel 87 i TEUF med hensyn til disse harmoniserede regler, er hverken berettiget eller hensigtsmæssigt.

¹⁵ Det er værd at bemærke, at forslagets artikel 5, stk. 4, har visse karakteristika, der svarer til dem i artikel 15, stk. 1, i e-databeskyttelsesdirektiv 2002/58. Den giver navnlig medlemsstaterne mulighed for at fravige visse forbud, der er fastsat i EU-retten. I lyset af fast retspraksis vil de nationale bestemmelser, der har til hensigt at fravige disse forbud, nødvendigvis være omfattet af EU-rettens anvendelsesområde, hvilket igen vil udløse anvendelsen af chartret i den henseende.

III. HENSIGTSMÆSSIGHEDEN AF ARTIKEL 16 I TEUF SOM ET SUPPLERENDE RETSGRUNDLAG

31. Den foreslåede forordning medtager artikel 16 i TEUF som retsgrundlag for behandlingen af personoplysninger på retshåndhævelsesområdet, og betragtning 25 og 26 indeholder en henvisning til artikel 6a i protokol nr. 21 og artikel 2a i protokol nr. 22 om behandling af personoplysninger på området forebyggelse af kriminalitet. Artikel 16 i TEUF skal efter Kommissionens opfattelse udelukkende tjene som retsgrundlag for de bestemmelser, der indfører begrænsninger for behandlingen af biometriske personoplysninger på en supplerende måde i forhold til direktiv (EU) 2016/680 ("retshåndhævelsesdirektivet"). Artikel 5, stk. 1, litra d), er formuleret som et principielt forbud, for hvilket der gælder tre undtagelser. Konkret er anvendelsen af systemer til biometrisk fjernidentifikation i realtid på offentlige steder med henblik på retshåndhævelse forbudt, medmindre den er streng nødvendig for a) at foretage målrettede eftersøgninger af ofre for kriminalitet, b) at forebygge et nært forestående terrorangreb eller angreb på en persons fysiske integritet/liv, c) at lokalisere eller identificere eller retsforfølge en gerningsmand eller mistænkt for grov kriminalitet (med henvisning til den europæiske arrestordre). Yderligere krav i artikel 5, stk. 2, 3 og 4, knytter sig til de retshåndhævende myndigheders specifikke anvendelse af AI-systemer, navnlig en vurdering af nødvendighed og proportionalitet, en forudgående tilladelse (undtagen i nødsituationer) og en afgørelse truffet af medlemsstaterne om, hvorvidt der på nationalt plan skal gives tilladelse til specifik anvendelse af AI-værktøjer i sådanne situationer.
32. Artikel 5 er en detaljeret bestemmelse, der regulerer en specifik anvendelse af AI-værktøjer, som ikke blot har til formål at supplere Unionens eksisterende lovgivningsmæssige ramme (retshåndhævelsesdirektivet, der selv er baseret på artikel 16 i TEUF), men også kræver en national gennemførelsesramme.

33. Trods sin formulering som et forbud kan den særlige regel i artikel 5 i det væsentlige beskrives som en streng og ekstraordinær ramme for AI-instrumenters generelle overvågning i realtid af enkeltpersoner i åbne områder med henblik på at identificere dem. Forbuddet går også videre end den simple brug af kameraer til registrering og henviser til anvendelsen af AI-værktøjer til automatisk genkendelse af menneskelige træk på offentlige steder (træk som f.eks. ansigter, men også gangart, fingeraftryk, DNA, stemme, tasteanslag og andre biometriske eller adfærdsmæssige signaler). Det indebærer også samtidig optagelse og identifikation af personer ved at sammenligne/kontrollere data. Desuden skal reglen også vurderes i lyset af det forhold, at private brugeres identifikation i realtid i det offentlige rum også kan tillades (til begivenheder som f.eks. fodboldkampe).
34. Yderligere præciseringer fra Kommissionen synes at antyde, at der i øjeblikket ikke er nogen eller muligvis kun meget få medlemsstater, der har reguleret dette specifikke spørgsmål med henblik på at tillade de retshåndhævende myndigheder at anvende AI-værktøjer til afsløring i realtid af enkeltpersoner i det offentlige rum. Selv om der i praksis ikke er fremlagt konkrete beviser for, at eksisterende praksis og værktøjer bør ændres, synes det dog klart, at fremtidige efterforskningsteknikker, kriminaltekniske metoder og regler om indsamling af bevismateriale vil skulle integrere denne forbuds-/undtagelsestilgang.
35. For så vidt angår retsgrundlaget, ser det ud til, at de bestemmelser, der indfører begrænsninger for behandlingen af biometriske personoplysninger på en supplerende måde (i forhold til retshåndhævelsesdirektivet), har til formål at beskytte personoplysninger ved at fastsætte de fornødne sikkerhedsforanstaltninger. Et sådant formål er uløseligt forbundet med formålet med de bestemmelser, der er omfattet af anvendelsesområdet for artikel 114 i TEUF, uden at det ene er sekundært og indirekte i forhold til det andet. Den foreslåede forordning har til formål at fastlægge en generel ramme for AI-systemer efter en risikobaseret tilgang. I den sammenhæng kan en horisontal regulering af AI-systemer omfatte strenge sikkerhedsforanstaltninger, der gælder for dette specifikke AI-system til afsløring i realtid. Et sådant specifikt AI-system, der indeholder passende sikkerhedsforanstaltninger for beskyttelse af personoplysninger, er derfor uløseligt forbundet med det overordnede mål om at forbedre det indre markeds funktion og er ikke sekundært eller indirekte i forhold til sidstnævnte. Den foreslåede forordning bør derfor have et dobbelt retsgrundlag i overensstemmelse med relevant retspraksis (jf. punkt 9 ovenfor).

36. Spørgsmålet er dog fortsat, hvilket retsgrundlag der bør anvendes til at regulere behandlingen af personoplysninger til brug for de systemer, der er omhandlet i artikel 5, stk. 1, litra c), og artikel 5, stk. 2-4, i den foreslåede forordning. Artikel 87, stk. 2, litra a), i TEUF udgør således et retsgrundlag for de retshåndhævende myndigheders foranstaltninger til forebyggelse, afsløring og efterforskning af strafbare handlinger vedrørende indsamling, opbevaring, behandling, analyse og udveksling af relevante oplysninger.
37. Som generaladvokaten anførte i sit forslag til afgørelse vedrørende PNR og Canada (A1/15), kan artikel 16 i TEUF, på den ene side, og artikel 87, stk. 2, litra a), og artikel 82, stk. 1, litra d), i TEUF, på den anden side, ikke opretholde et over- og underordningsforhold i form af "*lex generalis – lex specialis*"¹⁶. Artikel 16, stk. 2, i TEUF er den eneste bestemmelse, der fastsætter regler for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger foretaget af medlemsstaternes retshåndhævende myndigheder, når de udfører aktiviteter til forebyggelse af kriminalitet. Den omstændighed, at artikel 5 henviser til listen over grov kriminalitet i rammeafgørelsen om den europæiske arrestordre, ændrer ikke ved denne vurdering: Denne henvisning betyder ikke, at nævnte rammeafgørelse finder anvendelse som sådan¹⁷. Det er blot lovgivningsteknik at opføre en liste over grov kriminalitet, uden at det er nødvendigt at udarbejde et særskilt bilag.
38. Det forholder sig ikke desto mindre således, at reglen i artikel 5 ikke er fastsat for yderligere at afgrænse betingelserne for anvendelse af disse RIA-relaterede foranstaltninger, men for i fremtiden at sikre, at enhver anvendelse af AI-systemer til biometrisk identifikation i realtid i tilstrækkelig grad imødekommer bekymringer vedrørende grundlæggende rettigheder og primært behovet for at sikre, at biometriske data indsamles og behandles under overholdelse af retten til privatlivets fred og til personoplysninger.

I denne henseende har forordningen ikke til formål at fastlægge en ny, obligatorisk RIA-specifik procedure, men bygger snarere på afprøvede proceduremæssige midler for at sikre, at de grundlæggende rettigheder overholdes.

¹⁶ Jf. udtalelse fra generaladvokat P. Mengozzi af 8. september 2016, *Udkast til aftale mellem Canada og Den Europæiske Union*, Udtalelse 1/15, EU:C:2016:656, præmis 112-120.

¹⁷ Med hensyn til medlemsstaternes gennemførelse af denne liste over grov kriminalitet, jf. Domstolens dom af 21. juni 2022, *Ligue des droits humains ASBL mod Ministerrådet*, C-817/19, EU:C:2022:65, præmis 150-152.

39. Hvis artikel 16 i TEUF er et hensigtsmæssigt supplerende retsgrundlag, rejser dette spørgsmål om anvendelsen af artikel 6a og 2a i henholdsvis protokol nr. 21 og 22. Som anført i forslagets betragtning 25 og 26 betyder dette, at når de retshåndhævende myndigheder i Irland eller Danmark anvender systemer til biometrisk fjernidentifikation i realtid på offentlige steder til forebyggelse af kriminalitet, og i tilfælde hvor Irland eller Danmark ikke er bundet af de tilsvarende regler om politisamarbejde eller retligt samarbejde i straffesager, vil disse to medlemsstater ikke være bundet af artikel 5, stk. 1, litra d), og artikel 5, stk. 2 og 3, i den foreslåede forordning. Dette betyder ikke, at artikel 5, stk. 1, litra d), og artikel 5, stk. 2 og 3, indeholder regler om politisamarbejde såsom regler om udveksling af oplysninger mellem retshåndhævende myndigheder. Det betyder blot, at artikel 5, stk. 1, litra d), og artikel 5, stk. 2 og 3, i den foreslåede forordning i lighed med direktiv (EU) 2016/680 ("retshåndhævelsesdirektivet"), som er *lex generalis*, og som er vedtaget på grundlag af artikel 16 i TEUF, regulerer behandlingen af biometriske personoplysninger i det særlige tilfælde med systemer til biometrisk fjernidentifikation i realtid på offentlige steder til forebyggelse af kriminalitet og intet andet. Kommissionens forslag følger i denne henseende den tilgang, som EU-lovgiveren har valgt for retshåndhævelsesdirektivet, og bekræfter derfor, at det ikke er berettiget at anvende artikel 87, stk. 2, i TEUF i denne sammenhæng.
40. Tilføjelsen af artikel 16 i TEUF til artikel 114 i TEUF i dette tilfælde er begrundet i, at artikel 5, stk. 1, litra d), og artikel 5, stk. 2 og 3, er de eneste bestemmelser, der regulerer anvendelsen af et AI-system, der er blevet tilladt, og som griber ind i retten til beskyttelse af personoplysninger, som er *lex specialis* i forhold til den generelle ramme for databeskyttelse. Sådanne *lex specialis*-databeskyttelsesregler, der påvirker anvendelsen af disse følsomme AI-systemer, kan ikke betragtes som sekundære eller indirekte i forhold til retsgrundlaget for det indre marked. Tilføjelsen af artikel 16 i TEUF som retsgrundlag er derfor tilstrækkeligt begrundet i den foreslåede forordning, og anvendelsen af artikel 87, stk. 2, litra a), i TEUF er ikke hensigtsmæssig.

IV. KONKLUSION

41. På baggrund af ovenstående mener Rådets Juridiske Tjeneste, at:

- a) Anvendelsen af artikel 16 og 114 i TEUF som retsgrundlag for den foreslåede forordning er berettiget og hensigtsmæssig.
 - b) Anvendelsen af artikel 87, stk. 2, i TEUF eller et andet RIA-retsgrundlag er ikke berettiget eller hensigtsmæssig i forhold til de harmoniserede regler, der gælder for AI-systemer, som kan udbydes eller anvendes af retshåndhævende eller judicielle myndigheder.
-