



Bryssel den 12 september 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

Interinstitutionellt ärende:
2021/0106(COD)

YTTRANDE FRÅN JURIDISKA AVDELNINGEN¹

från: Juridiska avdelningen

Ärende: Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens

- Lämpligheten hos de rättsliga grunderna artiklarna 114 och 16 i EUF-fördraget med avseende på bestämmelser som är tillämpliga på brottsbekämpande myndigheter och rättsliga myndigheter

I. INLEDNING

1. I förslaget till förordning fastställs harmoniserade regler för utsläppande på marknaden och ibruktagande av system med artificiell intelligens (*AI-system*) i unionen (*förslaget till förordning*)².

¹ Denna handling innehåller juridisk rådgivning som är skyddad enligt artikel 4.2 i Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar och som Europeiska unionens råd inte har gjort tillgänglig för allmänheten. Rådet kommer att hävda sina rättigheter vid otillåtet offentliggörande.

² Dok. 8115/21.

2. Vid mötet i arbetsgruppen för telekommunikation och informationssamhället den 7 april 2022 yttrade sig rådets juridiska avdelning om lämpligheten av de dubbla rättsliga grunderna (artiklarna 16 och 114 i EUF-fördraget) för förslaget till förordning om system med artificiell intelligens (AI-system). Genom förklaringarna bekräftades att artiklarna 16 och 114 i EUF-fördraget är de korrekta rättsliga grunderna för förslaget och att det inte är lämpligt att använda artikel 87.2 i EUF-fördraget i stället för artikel 114 i EUF-fördraget. På arbetsgruppens begäran återges i detta yttrande skriftligen den redogörelse juridiska avdelningens företrädare gav vid mötet, varvid den utvecklas ytterligare.
3. AI-system definieras i artikel 3.1 i förslaget till förordning. I allmänhet kan de hänföras till vissa typer av programvara. Förslaget till förordning gäller både leverantörer som släpper ut AI-system på marknaden och leverantörer som tar AI-system i bruk. Den föreslagna förordningen är också tillämplig på användare. En leverantör kan vara en fysisk eller juridisk person, en offentlig myndighet, en byrå eller ett annat organ som utvecklar eller låter utveckla ett AI-system i syfte att släppa ut det på marknaden eller ta det i bruk i eget namn eller under eget varumärke. En användare kan vara varje fysisk eller juridisk person, offentlig myndighet, byrå eller annat organ som under eget överinseende använder ett AI-system.

4. Enligt definitionerna i artikel 3 kan brottsbekämpande och rättsliga myndigheter antingen klassificeras som leverantörer och/eller användare av ett AI-system. AI-system vars avsedda ändamål, enligt leverantörens definition, är brottsbekämpning eller rättskipning, klassificeras som högrisksystem enligt bilaga III. De omfattas därför av väsentliga krav (riskhantering, provning, dataförvaltning, teknisk dokumentation, transparens, mänsklig tillsyn, noggrannhet, robusthet och cybersäkerhet) och är förenade med skyldigheter (t.ex. kvalitetsledningssystem, teknisk dokumentation, bedömning av överensstämmelse, korrigerande åtgärder, informationsskyldighet, importörers och distributörers skyldigheter) samt standarder och bedömning av överensstämmelse. Dessa harmoniserade regler bygger på dem som gäller produktsäkerhet i direktiv 2006/42/EG (maskiner)³ och förordning (EU) 2017/745 (medicintekniska produkter)⁴.
5. När det gäller AI-system som inbegriper användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål, omfattas de av kategorin förbjudna AI-system. Det finns emellertid undantag från detta förbud mot användning av AI-system. Det är upp till medlemsstaterna huruvida de vill tillåta användning av sådana system eller inte. Om systemen tillåts ska de omfattas av detaljerade begränsningar och skyddsåtgärder för att inskränka användningen till vad som är absolut nödvändigt och för att skydda den grundläggande rätten till skydd av personuppgifter. Dessa begränsningar och skyddsåtgärder föreskrivs i förslaget till förordning på grundval av artikel 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) och måste kompletteras med nationell lagstiftning. Artikel 5.1 d, 5.2, 5.3 och 5.4 i förslaget till förordning utgör *lex specialis* till direktiv (EU) 2016/680 (dataskyddsdirektivet för polis och straffrättsliga myndigheter) som antogs på grundval av artikel 16.2 i EUF-fördraget.

³ Europaparlamentets och rådets direktiv 2006/42/EG av den 17 maj 2006 om maskiner och om ändring av direktiv 95/16/EG (EUT L 157, 9.6.2006, s. 24).

⁴ Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

I enlighet med artikel 5.1 d ska målen för dessa system vara begränsade till följande:

- i) Målinriktad sökning efter specifika potentiella brottsoffer, inbegripet försvunna barn.
- ii) Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller förhindrande av en terroristattack.
- iii) Avslöjande, lokalisering, identifiering eller lagföring av en gärningsman eller misstänkt vid brott som avses i artikel 2.2 i beslutet om en europeisk arresteringsorder⁵ och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd i minst tre år, i enlighet med den medlemsstatens lagstiftning.

Enligt artikel 5.3 ska brottsbekämpande myndigheters användning av sådan teknik kräva förhandstillstånd från en rättslig eller administrativ myndighet. I vederbörligen motiverade brådskande situationer får dock användningen av systemet påbörjas utan tillstånd och tillståndet får då begäras under eller efter användningen.

Enligt artikel 5.4 får en medlemsstat besluta att tillåta användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpningsändamål och fastställa de nödvändiga detaljerade reglerna för begäran om, utfärdande av och utövande av förhandstillstånd samt relaterade brott.

6. Den rättsliga grunden för förslaget till förordning är artiklarna 16 i EUF-fördraget (skydd av personuppgifter) och 114 i EUF-fördraget (den inre marknadens funktion). Därmed aktualiseras frågan huruvida dessa rättsliga grunder är lämpliga i förhållande till de harmoniserade regler som är tillämpliga på AI-system som tillhandahålls eller används av brottsbekämpande och rättsliga myndigheter.

⁵ Rådets rambeslut 2002/584/RIF av den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (EGT L 190, 18.7.2002, s. 1).

7. Föreliggande yttrande fokuserar först på huruvida artikel 114 i EUF-fördraget är lämplig rättslig grund i det särskilda sammanhang med brottsbekämpande myndigheter som nämns i flera bestämmelser i förslaget till förordning, dvs. när det gäller system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser och AI-system med hög risk som avses i punkt 6 i bilaga III. I yttrandet behandlas därför frågan om huruvida artikel 87.2 i EUF-fördraget (polissamarbete) skulle vara en lämpligare rättslig grund för att täcka brottsbekämpande myndigheters tillhandahållande och användning av AI-system i stället för artikel 114 i EUF-fördraget (avsnitt II). På motsvarande sätt kan slutsatsen i denna not tillämpas på de rättsliga myndigheter som avses i bilaga III när det gäller AI-system med hög risk.
8. I denna not behandlas även frågan om huruvida artikel 16 i EUF-fördraget är lämplig som kompletterande rättslig grund och tillämpningen av protokollen 21 och 22 i samband med brottsbekämpande myndigheters användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser (avsnitt III).

II. LÄMPLIGHETEN AV ARTIKEL 114 I EUF-FÖRDRAGET SOM LÄMPLIG RÄTTSLIG GRUND

9. Enligt väletablerad rättspraxis är den rättsliga grunden för en unionsakt inte avhängig av en institutions uppfattning om det eftersträvade syftet, utan den måste fastställas i enlighet med objektiva kriterier som kan bli föremål för domstolsprövning, däribland särskilt åtgärdens syfte och innehåll. Om bedömningen av en åtgärd visar att den har två syften eller två beståndsdelar, och om ett av dessa syften eller en av dessa beståndsdelar kan identifieras som det – eller den – huvudsakliga eller dominerande, medan det – eller den – andra endast är av underordnad betydelse, ska åtgärden ha en enda rättslig grund, nämligen den som krävs med hänsyn till det huvudsakliga eller dominerande syftet eller den huvudsakliga eller dominerande beståndsdelan. Endast om det fastställs att akten samtidigt har flera mål, vilka är oskiljaktigt förbundna med varandra, utan att det ena är sekundärt och indirekt i förhållande till det andra, får en sådan akt i undantagsfall antas med stöd av de däremot svarande olika rättsliga grunderna, under förutsättning att dessa rättsliga grunder inte föreskriver förfaranden som är oförenliga med varandra. Det bör också noteras att artikel 114.1 första meningen i EUF-fördraget tydligt anger att artikelns bestämmelser ska tillämpas ”[o]m inte annat föreskrivs i fördragen”. I enlighet med detta är tillämpning av artikel 114 i EUF-fördraget endast berättigad om ingen mer specifik bestämmelse kan användas som rättslig grund för antagandet av åtgärden i fråga⁶. En mer specifik bestämmelse som kan användas som rättslig grund för antagandet av åtgärden i fråga ska användas, när det finns en sådan i fördraget⁷.

⁶ Juridiska avdelningens yttrande av den 17 maj 2016, 9007/16, punkt 6.

⁷ Domstolens dom av den 29 april 2004, kommissionen/rådet, C-338/01, ECLI:EU:C:2004:253, punkt 60.

A. SYFTET MED DEN FÖRESLAGNA FÖRORDNINGEN

10. Genom den föreslagna förordningen harmoniseras utsläppandet på marknaden, ibruktagandet och användningen av en viss typ av programvara (AI-system). Det faktum att offentliga myndigheter och privata aktörer kan vara leverantörer eller användare av sådana AI-system är inte i sig oförenligt med den rättsliga grunden i artikel 114 i EUF-fördraget⁸.
11. Den omständigheten att brottsbekämpande myndigheter eller de som agerar på deras vägnar kan vara leverantörer eller användare av sådana AI-system är dessutom inte tillräckligt för att motivera att artikel 87 i EUF-fördraget används som rättslig grund. Syftet med och innehållet i den föreslagna förordningen måste analyseras för att avgöra om detta är nödvändigt.
12. Den föreslagna förordningen syftar i allmänhet, liksom när det gäller system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser och AI-system med hög risk, till att säkerställa en konsekvent och hög skyddsnivå i hela unionen och samtidigt förhindra att avvikelser hindrar den fria rörligheten för AI-system och relaterade produkter och tjänster på den inre marknaden. I den föreslagna förordningen fastställs enhetliga skyldigheter för operatörerna. Förordningen garanterar också ett enhetligt skydd för tvingande hänsyn till allmänintresset och personers rättigheter på hela den inre marknaden (skäl 2). För att uppnå detta syfte innehåller den föreslagna förordningen bestämmelser som reglerar utsläppandet på marknaden och ibruktagandet av vissa AI-system, för att på så sätt säkerställa en fungerande inre marknad och göra det möjligt för dessa system att omfattas av principen om fri rörlighet för varor och tjänster (skäl 5). På det hela taget syftar förslaget till att inrätta AI med inbyggd tillförlitlighet, som är allmänt tillämplig, med en fullständig uppsättning regler för utveckling, marknadsföring och användning av AI-drivna produkter, tjänster och system. Med tanke på att AI redan ingår i ett stort antal tjänster och produkter och kommer att fortsätta att göra det i framtiden följer förslaget en inre marknadslogik genom att fastställa en ”produktsäkerhetsram” som bygger på fyra riskkategorier. Det inför krav på marknadstillträde och certifiering av AI-system med hög risk genom ett obligatoriskt CE-märkningsförfarande.

⁸ Se yttrandet från rådets juridiska avdelning (ST 11395/14, punkterna 39–41) och prejudikat såsom direktiv (EU) 2016/2102 samt direktiven 2014/24/EU, 2014/25/EU och 2014/23/EU.

13. Inget av de mål som anges i förslaget till förordning avser säkerställande av mål som rör den allmänna säkerheten. Målen för den allmänna säkerheten ska visserligen indirekt uppnås genom harmoniseringen av de brottsbekämpande myndigheternas utsläppande på marknaden/ibruktagande/användning av AI-system, men domstolen⁹ har, vid tolkningen av artikel 87.2 i EUF-fördraget mot bakgrund av artikel 67 i EUF-fördraget, slagit fast att en unionsrättsakt, med beaktande av dess syfte och innehåll, för att grundas på den förstnämnda artikeln måste vara direkt förbunden med de mål som anges i artikel 67 i EUF-fördraget (dvs. i detta fall förebyggande av brottslighet och polissamarbete). När det gäller den föreslagna förordningen är detta uteslutet, eftersom de enda harmoniserade reglerna för brottsbekämpande myndigheters användning av sådana system är antingen 1) produktsäkerhetsregler som tillämpas enhetligt på alla leverantörer och användare med avseende på utsläppande på marknaden/ibruktagande eller användning av AI-system eller 2) regler om skydd av personuppgifter för vilka artikel 16 i EUF-fördraget lade till som rättslig grund (se del III nedan).
14. I ett annat mål¹⁰ var syftet med ändringen av skjutvapendirektivet visserligen att säkerställa en högre nivå av allmän säkerhet i förhållande till terroristhotet och andra former av brottslighet, men domstolen slog fast att harmoniseringen av olika säkerhetsaspekter beträffande varor är en väsentlig åtgärd för att säkerställa att den inre marknaden fungerar väl, eftersom skillnader i lagstiftningen på detta område kan ge upphov till handelshinder¹¹.

⁹ Domstolens dom av den 6 maj 2014, Europeiska kommissionen/Europaparlamentet och Europeiska unionens råd, C43/12, ECLI:EU:C:2014:298.

¹⁰ Domstolens dom av den 3 december 2019, Republiken Tjeckien/Europaparlamentet, C482/17, ECLI:EU:C:2019:1035.

¹¹ Ibid., skäl 57: *”Det som är utmärkande för skjutvapen är, tvärt emot vad Republiken Polen har hävdat, att de utgör en fara inte bara för användarna utan även för den breda allmänheten, vilket domstolen redan har påpekat i punkt 54 i dom av den 23 januari 2018, Buhagiar m.fl. (C- 267/16, EU:C:2018:26). Det framstår därmed som oundgängligt att ta hänsyn till den allmänna säkerheten, såsom anges i femte skälet i direktiv 91/477, i samband med antagandet av bestämmelser om förvärv och innehav av sådana varor”*. Se även domstolens dom av den 23 januari 2018, Albert Buhagiar m.fl./Minister for Justice, C-267/16, EU:C:2018:26, punkt 54: *” Härvidlag är det viktigt att påpeka att med beaktande av den säkerhetsrisk som skjutvapen utgör för människor, kan fri rörlighet för sådana vapen endast uppnås genom en strikt reglering av villkoren för att överföra dem mellan medlemsstaterna, däribland principen om att de berörda medlemsstaterna ska utfärda föregående tillstånd att överföra sådana varor”*.

15. Målen för den föreslagna förordningen, inbegripet artikel 5.1 d, 5.2, 5.3 och 5.4 om användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål och de bestämmelser om AI-system med hög risk som avses i punkt 6 i bilaga III, är inte direkt förbundna med ett mål om allmän säkerhet. Tvärtom är förslaget ett svar på de viktigaste frågorna om hur AI-system påverkar hälsa, säkerhet och grundläggande rättigheter. De relevanta bestämmelserna är därför direkt kopplade till målet att säkerställa lika villkor vid utsläppande på marknaden/ibruktagande eller användning av AI-system på den inre marknaden, samtidigt som användarnas hälsa, säkerhet och grundläggande rättigheter skyddas.
16. Mot ovanstående bakgrund är huvudsyftet med den föreslagna förordningen att förbättra den inre marknadens funktion i den mening som avses i artikel 114 i EUF-fördraget. De mål som avses i artikel 67 i EUF-fördraget har endast en indirekt koppling till detta huvudmål.

B. INNEHÅLLET I FÖRSLAGET TILL FÖRORDNING

17. Förslaget till förordning innehåller i huvudsak bestämmelser om vad som krävs för att släppa ut en viss produkt (en AI-programvara) på marknaden (eller ta den i bruk) för att säkerställa att den är säker och respekterar de grundläggande rättigheterna. Det innehåller en fullständig uppsättning regler för utveckling, marknadsföring och användning av AI-drivna produkter, tjänster och system. Den föreslagna förordningen ålägger inte brottsbekämpande myndigheter att använda ett AI-system som lagligen släpps ut på marknaden, och den reglerar inte heller direkt hur brottsbekämpande myndigheter bör använda ett sådant AI-system. I stället avgränsas tydligt situationer där den avsedda användningen betraktas som förenad med hög risk helt enkelt på grund av att ett AI-system kommer att användas av brottsbekämpande eller rättsliga myndigheter.

18. Artikel 29 i förslaget till förordning innehåller i och för sig regler om villkoren för användning av AI-system med hög risk, men bestämmelsen är inte sektorsspecifik, den har ett begränsat tillämpningsområde (främst med avseende på produktens bruksanvisningar) och är ouplösligt förbunden med de skyldigheter som åläggs utvecklare av AI-system enligt den föreslagna förordningen. Bestämmelsen ger också medlemsstaterna ett visst spelrum för att kunna fastställa ytterligare regler för användningen av sådana AI-system med hög risk. När det gäller system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser som används för brottsbekämpande ändamål (artikel 5) reglerar den föreslagna förordningen delvis användningen av sådana system ur ett dataskyddsperspektiv på grundval av artikel 16 i EUF-fördraget (se del III nedan).
19. Dessutom är det bara medlemsstaterna som kan besluta att föreskriva möjligheten att helt eller delvis tillåta användning av sådana system för biometrisk fjärridentifiering i realtid. De särskilda villkoren för sådan användning ska stadfästas i nationell lagstiftning, men måste respektera de allmänna kriterier och skyddsåtgärder som fastställs i förordningen: rättsligt eller administrativt förhandstillstånd, begäran om, utfärdande av och utövande av förhandstillstånd samt fastställande av de brott som sådana system får användas för.

20. AI-system är en särskild typ av programvara. De harmoniserade regler som gäller för utsläppande på marknaden eller ibruktagande/användning av AI-system utgör således produktsäkerhetsliknande harmoniserade regler. De tillämpas på ett enhetligt sätt utan åtskillnad mellan offentliga och privata användare. Enligt de tillämpliga skälen i förslaget till förordning bör därför en hög enhetlig skyddsnivå säkerställas i hela unionen. Samtidigt bör skillnader som hindrar den fria rörligheten för AI-system och relaterade produkter och tjänster på den inre marknaden förebyggas. Detta kan uppnås genom fastställande av enhetliga skyldigheter för operatörerna och garantier för ett enhetligt skydd för tvingande hänsyn till allmänintresset och personers rättigheter på hela den inre marknaden enligt artikel 114 i EUF-fördraget¹².
21. Förslaget till förordning innehåller flera hänvisningar till brottsbekämpning, gränskontrollförvaltning samt rättskipning i bilaga III om AI-system med hög risk (punkterna 6, 7 respektive 8). Utöver andra högrisksystem med avseende på de produktsäkerhetsrisker som avses i artikel 6.1 innefattar dessa en detaljerad och uttömmande uppräknings som motsvarar artikel 6.2. Enligt artikel 6.1 ska vissa AI-system per definition betraktas som högrisksystem på grund av deras förväntade allvarlighetsgrad och höga risker för de grundläggande rättigheterna, hälsan och säkerheten. Andra system som anses vara högrisksystem och som förtecknas i bilaga III omfattar utbildning, förvaltning av kritisk infrastruktur, sysselsättning, biometrisk identifiering och kategorisering samt tillgång till viktiga offentliga och privata tjänster.

¹² Därmed behövs en rättslig ram för unionen som omfattar harmoniserade regler för artificiell intelligens, för att främja utvecklingen, användningen och spridningen av artificiell intelligens på den inre marknaden, och som samtidigt uppnår en hög skyddsnivå för allmänintressen, såsom hälsa, säkerhet och skydd av grundläggande rättigheter, som erkänns och är skyddade enligt unionsrätten. För att uppnå detta syfte bör det fastställas bestämmelser som reglerar utsläppandet på marknaden och ibruktagandet av vissa AI-system, för att på så sätt säkerställa en väl fungerande inre marknad och göra det möjligt för dessa system att omfattas av principen om fri rörlighet för varor och tjänster (se skälen 2 och 5 i förslaget).

22. Sådana bestämmelser om AI-system med hög risk reglerar dock inte frågan om huruvida brottsbekämpande och rättsliga myndigheter (eller myndigheter på andra identifierade områden) bör använda sig av sådana system eller inte. Den föreslagna förordningen får endast indirekt inverkan på den faktiska utvecklingen av AI-system som kan användas av brottsbekämpande myndigheter och på de AI-system som används för närvarande och i framtiden. Reglerna hänvisar således till AI-system som är ”*avsedda att användas*” av sådana myndigheter (se t.ex. artiklarna 3.12, 8.2 och bilaga III). Om ett visst system förtecknas som AI-system med hög risk kommer det att omfattas av en särskild uppsättning regler för riskhantering, dataförvaltning och tekniska specifikationer. Användare av sådana AI-system med hög risk måste följa bruksanvisningen, föra loggar och utföra konsekvensbedömningar avseende dataskydd.
23. Dessutom får andra användarskyldigheter än de som rör bruksanvisningen fastställas i unionslagstiftning eller nationell lagstiftning och utan att det påverkar användarens handlingsutrymme när det gäller att organisera sina egna resurser och aktiviteter i syfte att genomföra de åtgärder för mänsklig tillsyn som leverantören anger (artikel 29.2 i förslaget till förordning). I dessa regler fastställs ytterligare skyddsåtgärder för grundläggande rättigheter för AI-system med hög risk.

24. Mot bakgrund av ovanstående bör det betonas att den föreslagna förordningen inte innehåller några regler som syftar till att tillåta eller förhindra att ett AI-system med hög risk som släpps ut på marknaden används av brottsbekämpande myndigheter. Genom de föreslagna reglerna kommer en särskild märkning (hög risk) att tillämpas på ett AI-system som utvecklas eller används av brottsbekämpande myndigheter till följd av dess avsedda användning. Denna användning skulle regleras i nationell lagstiftning och i viss mån beslutas av de brottsbekämpande myndigheterna själva. I förslaget till förordning fastställs minimivillkor för användning i artikel 29 (avser endast bruksanvisningar) för AI-system med hög risk, inbegripet de som förtecknas i punkterna 6, 7 och 8 i bilaga III, som kommer att kompletteras av nationell lagstiftning. Därför bör en åtskillnad göras, i linje med domstolens rättspraxis, mellan å ena sidan det avsedda syftet med den föreslagna förordningen, som inte är att reglera de brottsbekämpande myndigheternas användning av AI-system, och, å andra sidan, de effekter som det indirekt kan ge upphov till¹³ och som saknar relevans för analysen av den rättsliga grundens lämplighet.
25. Punkterna 6, 7 och 8 som avser brottsbekämpning, migration respektive rättskipning är inte dominerande bland AI-system med hög risk. Enligt den föreslagna förordningen är ett AI-system med hög risk inte nödvändigtvis ett system som förtecknas i bilaga III. De flesta högrisksystem är i själva verket de som förtecknas allmänt i artikel 6.1 a och b i förslaget till förordning (i samband med produktsäkerhet). Andra AI-system med hög risk förtecknas i bilaga III som innehåller punkterna 1 (biometrisk identifiering), 2 (kritisk infrastruktur), 3 (utbildning och yrkesutbildning) och 4 (sysselsättning, arbetsledning och tillgång till egenföretagande) som rör andra områden än rättsliga och inrikes frågor ("RIF"). Alla användare av sådana AI-system med hög risk omfattas av ett enhetligt system som inrättats med tanke på deras specifika status (t.ex. om de är en ekonomisk aktör eller en offentlig myndighet), men ur perspektivet skydd av hälsa, säkerhet och grundläggande rättigheter.

¹³ Se domstolens dom av den 21 juni 2018, Republiken Polen/Europaparlamentet, Europeiska unionens råd, C-5/16, EU:C:2018:483, punkterna 63–68, och domstolens dom av den 22 juni 2022, Leistritz AG/LH, C-534/20, EU:C:2022:495, punkt 28.

26. Den föreslagna förordningen innehåller därför harmoniserade regler om utsläppande på marknaden, ibruktagande och användning av AI-system, oavsett om de används av privata aktörer eller offentliga myndigheter, inbegripet, för övrigt¹⁴, brottsbekämpande och rättsliga myndigheter.
27. Bortsett från användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål, som omfattas av särskilda regler för behandling av personuppgifter (se del III nedan), innehåller den föreslagna förordningen inga harmoniserade regler om användningen av AI-system med hög risk. Såsom förklaras i punkterna 18 och 19 ovan hänför sig hänvisningen till användningen av AI-system med hög risk i huvudsak till bruksanvisningen för produkten (artikel 29) och är kopplad till de skyldigheter som åläggs utvecklare. Beslutet om huruvida brottsbekämpande eller rättsliga myndigheter får använda ett AI-system med hög risk som lagligen släpps ut på marknaden enligt den föreslagna förordningen är, såsom påpekas i punkt 22, en fråga för nationell rätt och nationella myndigheter.
28. Därför är artikel 87.2 i EUF-fördraget, särskilt led a, inte en lämplig rättslig grund för den föreslagna förordningen. Bestämmelserna i förslaget varken främjar eller hindrar insamling, lagring, behandling, analys och utbyte av relevant information. När sådan verksamhet utförs av brottsbekämpande myndigheter måste helt enkelt ett antal icke-specifika, harmoniserade villkor respekteras för att skydda användarnas rättigheter. På samma sätt omfattar de mål som anges i förslaget till förordning inte utvecklingen av gemensamma utredningsmetoder. De föreslagna kraven för användning av AI-system med hög risk är inte specifika för RIF-området, och de rör inte polissamarbete i egentlig mening enligt definitionen i EUF-fördraget.

¹⁴ Se domstolens yttrande över Istanbulkonventionen, A-1/19, EU:C:2021:198, särskilt punkterna 298 och 301.

29. Vad beträffar artikel 5.4 i förslaget till förordning bibehåller medlemsstaterna rätten att besluta att tillåta användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål. En medlemsstat som beslutar att göra det är skyldig att fastställa de nödvändiga närmare reglerna för begäran om, utfärdande och utövande av förhandstillstånd samt för de brott som hör samman med de brott vid vilkas utredning eller lagföring användningen är tillåten¹⁵. Utifrån resultatet av diskussionerna i rådet skulle dessa föreslagna regler inte leda till att respektive nationella myndigheter skulle tilldelas nya befogenheter. I stället begränsas användningen av befintliga eller eventuella framtida mekanismer för att säkerställa skyddet av rätten till dataskydd och personlig integritet.
30. Mot bakgrund av ovanstående är artikel 114 i EUF-fördraget den enda lämpliga rättsliga grunden för harmoniserade regler om AI-system med hög risk, inbegripet sådana system som används av brottsbekämpande och rättsliga myndigheter. Med avseende på dessa harmoniserade regler är det varken motiverat eller lämpligt med någon rättslig grund för rättsliga och inrikes frågor som hämtas ur tredje delen avdelning V i EUF-fördraget, t.ex. artikel 87 i EUF-fördraget.

¹⁵ Det är värt att notera att artikel 5.4 i förslaget i vissa delar liknar artikel 15.1 i direktiv 2002/58 om elektronisk handel. I artikeln föreskrivs en möjlighet för medlemsstaterna att göra undantag från vissa förbud som fastställs i unionsrätten. Enligt fast rättspraxis faller de nationella bestämmelser som syftar till att göra undantag från dessa förbud med nödvändighet inom unionsrättens tillämpningsområde, vilket i sin tur utlöser tillämpningen av stadgan i detta avseende.

III. LÄMPLIGHETEN AV ARTIKEL 16 I EUF-FÖRDRAGET SOM KOMPLETTERANDE RÄTTSLIG GRUND

31. I förslaget till förordning ingår artikel 16 i EUF-fördraget som rättslig grund när det gäller behandling av personuppgifter på brottsbekämpningsområdet. Skälen 25 och 26 innehåller en hänvisning till artikel 6a i protokoll 21 och artikel 2a i protokoll 22 om behandling av personuppgifter på området förebyggande av brottslighet. Kommissionen anser att artikel 16 i EUF-fördraget uteslutande ska tjäna som rättslig grund för de bestämmelser som begränsar behandlingen av biometriska personuppgifter på ett sätt som kompletterar direktiv (EU) 2016/680 (*dataskyddsdirektivet för brottsbekämpning*). Artikel 5.1 c är formulerad som ett principiellt förbud, från vilket tre undantag är möjliga. Rent konkret är det förbjudet att använda system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål, såvida det inte är absolut nödvändigt för att a) utföra riktade sökningar efter potentiella brottsoffer, b) förhindra en överhängande terroristattack eller angrepp på en persons fysiska integritet/liv, c) lokalisera eller identifiera eller lagföra en gärningsman eller misstänkt för ett allvarligt brott (med åberopande av en europeisk arresteringsorder). Ytterligare krav i artikel 5.2, 5.3 och 5.4 är kopplade till brottsbekämpande myndigheters specifika användning av AI-system, t. ex. en bedömning av nödvändighet och proportionalitet, ett förhandsgodkännande (utom i nödsituationer) och ett beslut av medlemsstaterna om huruvida de ska godkänna specifik användning av AI-verktyg på nationell nivå i sådana situationer.
32. Artikel 5 är en detaljerad bestämmelse som reglerar specifik användning av AI-verktyg som inte bara syftar till att komplettera unionens befintliga rättsliga ram (*dataskyddsdirektivet för brottsbekämpning*, som i sig grundar sig på artikel 16 i EUF-fördraget), utan också kräver en nationell ram för genomförande.

33. Trots att den formulerats som ett förbud kan den särskilda bestämmelsen i artikel 5 i sak beskrivas som en strikt och exceptionell ram för AI-instrumentens allmänna realtidsövervakning av enskilda personer på allmän plats i syfte att identifiera dem. Förbudet går också utöver enkel användning av kameror för inspelning och avser användningen av AI-verktyg för automatisk igenkänning av mänskliga särdrag på allmänt tillgängliga platser (t.ex. sådana egenskaper som ansikten, men också gångstil, fingeravtryck, DNA, röst, tangentryckningar och andra biometriska eller beteendemässiga signaler). Det innebär också en samtidig insamling och identifiering av personer genom analysjämförelse/kontroll av uppgifter. Dessutom ska regeln även bedömas mot bakgrund av att identifiering i realtid av privata användare på allmän plats också kan tillåtas (för sådana evenemang som fotbollsmatcher).
34. Av kommissionens kompletterande klargöranden framgår att inga eller möjligen endast ett mycket litet antal medlemsstater för närvarande har reglerat denna specifika fråga för att göra det möjligt för brottsbekämpande myndigheter att använda AI-verktyg för avslöjande i realtid av enskilda personer på allmän plats. Det har visserligen inte lagts fram några konkreta bevis för att befintliga metoder och verktyg kommer att behöva ändras, men det framstår som uppenbart att framtida utredningstekniker, kriminaltekniska metoder och regler för insamling av bevis kommer att behöva integrera detta tillvägagångssätt med förbud/undantag.
35. När det gäller den rättsliga grunden förefaller det som om de bestämmelser som begränsar behandlingen av biometriska personuppgifter på ett kompletterande sätt (jämfört med dataskyddsdirektivet för brottsbekämpning) syftar till att skydda personuppgifter genom att fastställa lämpliga skyddsåtgärder. Ett sådant syfte är oupplösligt förbundet med syftet med de bestämmelser som omfattas av artikel 114 i EUF-fördraget, utan att det ena är sekundärt och indirekt i förhållande till det andra. Den föreslagna förordningen syftar till att fastställa en allmän ram för AI-system enligt en riskbaserad metod. I detta sammanhang kan en horisontell reglering av AI-system inbegripa strikta skyddsåtgärder som är tillämpliga på detta specifika AI-system för avslöjande i realtid. Ett sådant specifikt AI-system som innehåller lämpliga skyddsåtgärder för personuppgifter är därför oupplösligt förbundet med det övergripande målet att förbättra den inre marknadens funktion och är inte sekundärt eller indirekt i förhållande till det sistnämnda. I enlighet med relevant rättspraxis (se punkt 9 ovan) bör den föreslagna förordningen således antas med stöd av två grunder.

36. Frågan kvarstår emellertid om vilken rättslig grund som bör användas för att reglera behandlingen av personuppgifter för användning av de system som avses i artikel 5.1 c–5.4 i förslaget till förordning. Artikel 87.2 a i EUF-fördraget utgör en rättslig grund för brottsbekämpande myndigheters åtgärder för att förebygga, avslöja och utreda brott som rör insamling, lagring, behandling, analys och utbyte av relevant information.
37. Såsom generaladvokaten har förklarat i sitt förslag till avgörande om förslaget till avtal mellan Europeiska unionen och Kanada om överföring och behandling av passageraruppgifter (A1/15), kan det emellertid inte finnas något hierarkiskt förhållande av typen ”*lex generalis–lex specialis*” mellan artikel 16 i EUF-fördraget, å ena sidan, och artikel 87.2 a och 82.1 d i EUF-fördraget, å andra sidan¹⁶. Artikel 16.2 i EUF-fördraget är den enda bestämmelse som är tillämplig på regler om skydd för enskilda personer med avseende på behandling av personuppgifter som utförs av medlemsstaternas brottsbekämpande myndigheter när dessa utövar brottsförebyggande verksamhet. Enbart det faktum att det i artikel 5 hänvisas till förteckningen över allvarliga brott i rambeslutet om en europeisk arresteringsorder ändrar inte denna bedömning: hänvisningen medför inte att själva rambeslutet är tillämpligt¹⁷. Att upprätta en förteckning över allvarliga brott utan att behöva skapa en separat bilaga är endast ett lagstiftningstekniskt grepp.
38. Regeln i artikel 5 fastställs dock inte som ett sätt att ytterligare avgränsa tillämpningsvillkoren för dessa RIF-relaterade åtgärder, utan för att säkerställa att AI-systemens användning av biometrisk identifiering i realtid i framtiden på ett adekvat sätt kan bemöta farhågorna rörande grundläggande rättigheter, i första hand behovet av att säkerställa att biometriska uppgifter samlas in och behandlas och att rätten till integritet och personuppgifter därvid respekteras.

I detta avseende syftar förordningen inte till att fastställa ett nytt, obligatoriskt RIF-specifikt förfarande, utan bygger snarare på beprövade förfaranden för att säkerställa respekten för de grundläggande rättigheterna.

¹⁶ Se generaladvokat P. Mengozzis förslag till avgörande av den 8 september 2016, om förslaget till avtal mellan Europeiska unionen och Kanada om överföring och behandling av passageraruppgifter, yttrande 1/15, EU:C:2016:656, punkterna 112–120.

¹⁷ När det gäller medlemsstaternas genomförande av denna förteckning över allvarliga brott, se domstolens dom av den 21 juni 2022, Ligue des droits humains/Conseil des ministres, C-817/19, EU:C:2022:65, punkterna 150–152.

39. Om artikel 16 i EUF-fördraget är en lämplig kompletterande rättslig grund aktualiserar detta frågor om tillämpningen av artiklarna 6a och 2a i protokoll 21 respektive 22. Såsom förklaras i skälen 25 och 26 i förslaget innebär detta att när brottsbekämpande myndigheter i Irland eller Danmark använder system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för förebyggande av brott, och om Irland eller Danmark inte är bundna av motsvarande bestämmelser om polissamarbete eller straffrättsligt samarbete, kommer dessa två medlemsstater inte att vara bundna av artikel 5.1 d, 5.2 och 5.3 i förslaget till förordning. Detta innebär inte att artikel 5.1 d, 5.2 och 5.3 innehåller bestämmelser om polissamarbete, såsom regler om informationsutbyte mellan brottsbekämpande myndigheter. Det innebär bara att artikel 5.1 d, 5.2 och 5.3 i förslaget till förordning, i likhet med direktiv (EU) 2016/680 (dataskyddsdirektivet för brottsbekämpning), som är *lex generalis* som antagits på grundval av artikel 16 i EUF-fördraget, reglerar behandlingen av biometriska personuppgifter i det särskilda sammanhang som utgörs av system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för förebyggande av brott och ingenting annat. Kommissionens förslag följer i detta avseende unionslagstiftarens tillvägagångssätt avseende dataskyddsdirektivet för brottsbekämpning och bekräftar därmed att det inte är motiverat att använda artikel 87.2 i EUF-fördraget i detta sammanhang.
40. I detta fall är det motiverat att lägga till artikel 16 i EUF-fördraget till artikel 114 i EUF-fördraget eftersom artikel 5.1 d, 5.2 och 5.3 är de enda bestämmelserna som reglerar användningen av ett AI-system som har godkänts och som inkräktar på rätten till skydd av personuppgifter, som är *lex specialis* i förhållande till den allmänna ramen för dataskydd. Dataskyddsregler av slaget *lex specialis* som påverkar användningen av dessa känsliga AI-system kan inte betraktas som sekundära eller indirekta i förhållande till den rättsliga grunden avseende den inre marknaden. Tillägget av artikel 16 i EUF-fördraget som rättslig grund är därför tillräckligt motiverat i den föreslagna förordningen och det är inte lämpligt att använda artikel 87.2 a i EUF-fördraget.

IV. SLUTSATS

41. Med hänsyn till ovanstående anser rådets juridiska avdelning följande:

- a) Det är motiverat och lämpligt att använda artiklarna 16 och 114 i EUF-fördraget som rättsliga grunder för den föreslagna förordningen.
 - b) Användningen av artikel 87.2 i EUF-fördraget eller någon annan rättslig grund på RIF-området är varken motiverad eller lämplig i förhållande till de harmoniserade regler som är tillämpliga på AI-system som kan tillhandahållas eller användas av brottsbekämpande eller rättsliga myndigheter.
-