Regeringens proposition 2025/26:150

Polisens användning av AI för ansiktsigenkänning i realtid

Prop. 2025/26:150

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 3 mars 2026

Lotta Edholm

Gunnar Strömmer
(Justitiedepartementet)

Propositionens huvudsakliga innehåll

Allvarlig våldsbrottslighet, framför allt skjutningar och sprängningar inom den kriminella miljön, är ett svårt samhällsproblem. För att vända utvecklingen men också för att komma till rätta med annan allvarlig brottslighet måste polisen ha effektiva och ändamålsenliga verktyg. Regeringen föreslår därför en ny lag som ska ge polisen möjlighet att använda AI-system för ansiktsigenkänning i realtid för att bekämpa brott.

Den nya lagen innebär att polisen ska få använda AI-tekniken om det är absolut nödvändigt för att lokalisera eller identifiera en viss person

- som misstänks vara utsatt för människorov, människohandel eller människoexploatering eller som är försvunnen och misstänks vara utsatt för brott,
- om det finns en överhängande risk för att personen kommer att begå ett allvarligt brott som innebär fara för annans liv eller fysiska säkerhet,
- som skäligen kan misstänkas ha begått ett visst allvarligt brott för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet, eller
- som dömts för ett sådant allvarligt brott, i syfte att verkställa den straffrättsliga påföljden.

Användningen av tekniken ska vara proportionerlig och det ska krävas ett tillstånd från åklagare eller domstol. I brådskande fall ska användning dock få påbörjas utan tillstånd och då ska en ansökan om tillstånd göras inom 24 timmar.

Den nya lagen och övriga lagändringar föreslås träda i kraft den 1 juli 2026.

Innehållsförteckning

1 Förslag till riksdagsbeslut 5

2 Lagtext 6
2.1 Förslag till lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål 6
2.2 Förslag till lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål 10
2.3 Förslag till lag om ändring i lagen (1957:668) om utlämning för brott 11
2.4 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål 12
2.5 Förslag till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder 15
2.6 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400) 16
2.7 Förslag till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder 20
2.8 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder 21
2.9 Förslag till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket 24

3 Ärendet och dess beredning 25

4 AI-förordningen ger utrymme för att använda AI-system för ansiktsigenkänning i realtid 26
4.1 Kort om AI-förordningen 26
4.2 Förordningen innehåller förbud mot att använda AI-system för ansiktsigenkänning i realtid … 26
4.3 … men det är möjligt att föreskriva om undantag 27

5 Utgångspunkter vid användning av AI-system för ansiktsigenkänning i realtid 28
5.1 Inledning 28
5.2 Grundläggande fri- och rättigheter behöver beaktas 28
5.3 Relevant dataskyddsreglering 29
5.4 Regleringen av kamerabevakning 31

6 Polisen ska ges möjlighet att använda AI-system för ansiktsigenkänning i realtid 32
6.1 En ny lag om polisens användning av AI för ansiktsigenkänning i realtid 32
6.2 Lagens tillämpningsområde 37

7 Förutsättningar för att använda AI-system för ansiktsigenkänning i realtid ... 43
7.1 AI-system för ansiktsigenkänning i realtid ska få användas för vissa syften ... 43
7.2 Användningen måste vara proportionerlig ... 59
8 Det ska krävas tillstånd ... 60
9 Tillståndsprövningen ... 67
9.1 Förfarandet i domstol ... 67
9.2 Handläggningen ska ske skyndsamt ... 71
9.3 Beslutets innehåll ... 72
9.4 Ett beslut om tillstånd får verkställas omedelbart ... 76
9.5 Det ska finnas en skyldighet att omedelbart upphäva ett beslut om tillstånd ... 77
10 En möjlighet att påbörja användning utan tillstånd ... 78
11 Konsekvensbedömning och registrering i EU-databas ... 82
12 Det ska finnas ett krav på underrättelse till enskild ... 86
13 Användningen ska anmälas ... 90
14 Behovet av följdändringar ... 91
14.1 Det krävs ändringar i offentlighets- och sekretesslagen ... 91
14.2 AI-system för ansiktsigenkänning i realtid ska få användas inom det internationella straffrättsliga samarbetet ... 96
14.3 Det behöver inte göras någon ändring i befintlig dataskyddsreglering eller i kamerabevakningslagen ... 101
15 Förslagens förenlighet med grundläggande fri- och rättigheter ... 105
15.1 Inledning ... 105
15.2 Förslagen är förenliga med grundläggande fri- och rättigheter ... 106
16 Ikraftträdande- och övergångsbestämmelser ... 116
17 Konsekvenser av förslagen ... 117
17.1 Konsekvenser för det brottsbekämpande arbetet och för enskilda ... 117
17.2 Konsekvenser för det allmänna ... 119
17.3 Övriga konsekvenser ... 123
18 Författningskommentar ... 124
18.1 Förslaget till lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ... 124
18.2 Förslaget till lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ... 136
18.3 Förslaget till lag om ändring i lagen (1957:668) om utlämning för brott ... 137
18.4 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål ... 137

18.5 Förslaget till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder 140
18.6 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400) 141
18.7 Förslaget till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder 144
18.8 Förslaget till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder 145
18.9 Förslaget till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket 148
Bilaga 1 AI-förordningen 149
Bilaga 2 Sammanfattning av promemorian Polisens användning av AI för ansiktsigenkänning i realtid (Ds 2025:7) 293
Bilaga 3 Promemorians lagförslag 294
Bilaga 4 Förteckning över remissinstanserna 313
Bilaga 5 Lagrådsremissens lagförslag 314
Bilaga 6 Lagrådets yttrande 332
Utdrag ur protokoll vid regeringssammanträde den 3 mars 2026. 343

1 Förslag till riksdagsbeslut

Regeringens förslag:

1. Riksdagen antar regeringens förslag till lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.
2. Riksdagen antar regeringens förslag till lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.
3. Riksdagen antar regeringens förslag till lag om ändring i lagen (1957:668) om utlämning för brott.
4. Riksdagen antar regeringens förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål.
5. Riksdagen antar regeringens förslag till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.
6. Riksdagen antar regeringens förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).
7. Riksdagen antar regeringens förslag till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder.
8. Riksdagen antar regeringens förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder.
9. Riksdagen antar regeringens förslag till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket.

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

Härigenom föreskrivs följande.

Lagens tillämpningsområde

1 § Lagen gäller för Polismyndighetens och Säkerhetspolisens användning av system för artificiell intelligens för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid på allmän plats (AI-system för ansiktsigenkänning i realtid) i verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177).

2 § Med AI-system för ansiktsigenkänning i realtid avses i lagen sådana AI-system som omfattas av artikel 3.42 i Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens), här benämnd AI-förordningen.

Inför användning av ett AI-system

3 § Innan ett AI-system för ansiktsigenkänning i realtid används för första gången ska Polismyndigheten och Säkerhetspolisen göra en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen.

Användning av AI-system

4 § AI-system för ansiktsigenkänning i realtid får användas om det är absolut nödvändigt för att lokalisera eller identifiera en viss person

1. som misstänks vara utsatt för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken, eller för människoexploatering enligt 4 kap. 1 b § brottsbalken om exploateringen avser sexuella tjänster,
2. som är försvunnen och misstänks vara utsatt för brott,
3. om det finns en överhängande risk för att personen kommer att begå ett allvarligt brott som innebär fara för annans liv eller fysiska säkerhet,
4. som skäligen kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet, eller

5. som dömts för ett sådant brott som avses i 4, i syfte att verkställa den straffrättsliga påföljden.

5 § AI-system för ansiktsigenkänning i realtid får användas endast om skälen för användningen uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Tillståndsprövningen hos åklagare

6 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd prövas av åklagare på ansökan av Polismyndigheten eller Säkerhetspolisen.

Tillståndsprövningen i domstol

7 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att utreda eller lagföra brott prövas av rätten på ansökan av åklagare.

Ansökan prövas av den domstol som anges i 19 kap. rättegångsbalken.

8 § Förfarandet i domstolen är skriftligt.

På förfarandet tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i denna lag. Det som föreskrivs om offentliga ombud i 27 kap. 28 § rättegångsbalken ska dock inte tillämpas.

Skyndsam handläggning

9 § En ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska prövas skyndsamt.

Beslut

10 § I ett beslut att tillåta användning av AI-system för ansiktsigenkänning i realtid ska det anges

1. vilken person som tillståndet avser,
2. för vilket syfte användningen ska ske,
3. under vilken tid och i vilket eller vilka områden tillståndet gäller, och
4. skälen för beslutet.

Tiden för tillståndet får inte bestämmas längre än vad som är absolut nödvändigt och får inte överstiga en månad från dagen för beslutet. Området eller områdena som tillståndet avser får inte vara större än vad som är absolut nödvändigt.

11 § Ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid får verkställas omedelbart.

Omedelbart upphörande

12 § Om det inte längre finns skäl för ett tillstånd att använda AI-system för ansiktsigenkänning i realtid ska åklagare omedelbart upphäva beslutet. Polismyndigheten eller Säkerhetspolisen ska omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

Tillfällig användning utan tillstånd

13 § Om det är fara i dröjsmål, får Polismyndigheten eller Säkerhetspolisen påbörja användning av AI-system för ansiktsigenkänning i realtid utan tillstånd.

Den myndighet som har påbörjat användning enligt första stycket ska dokumentera den samt skälen för att användningen påbörjades utan tillstånd.

14 § Om användning har påbörjats utan tillstånd ska en ansökan om tillstånd enligt 6 eller 7 § göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades.

15 § Om användning har påbörjats utan tillstånd och det inte längre finns skäl för användningen, ska den myndighet som har påbörjat användningen eller, i fall som avses i 7 §, åklagare omedelbart besluta om att användningen ska upphöra.

Om användningen upphör innan tillståndsfrågan har prövats, ska den som får ansöka om tillstånd i stället göra en anmälan till åklagare eller, i fall som avses i 7 §, rätten, som ska pröva om det har funnits skäl för användningen.

16 § Om en ansökan om tillstånd avslås ska användning som har påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas. Uppgifterna från användningen ska också raderas om, i fall som avses i 15 § andra stycket, åklagaren eller rätten har funnit att det har saknats skäl för användningen.

Underrättelse till enskild

17 § Den som har identifierats eller lokaliserats genom en åtgärd enligt denna lag som gäller en brottsutredning eller lagföring ska underrättas om åtgärden. Underrättelsen ska lämnas så snart det kan ske utan men för det syfte som åtgärden vidtogs för.

Om uppgifterna omfattas av sekretess enligt 15 kap. 1 eller 2 §, 18 kap. 1, 2 eller 3 § eller 35 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400) ska en underrättelse skjutas upp till dess att sekretess inte längre gäller.

En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna. En underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse eller om identiteten på den som ska underrättas är okänd. Detsamma ska gälla om den personen som underrättelsen avser har avlidit.

18 § Om det på grund av sekretess eller risk för men för syftet som åtgärden vidtogs för inte har kunnat lämnas någon underrättelse inom ett år och sex månader från det att åtgärden avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller och om det kan ske utan men för syftet som åtgärden vidtogs för.

Denna lag träder i kraft den 1 juli 2026.

2.2 Förslag till lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

Härigenom föreskrivs att 3 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska ha följande lydelse.

Lydelse enligt lagförslag 2.1	*Föreslagen lydelse*
3 §	
Innan ett AI-system för ansiktsigenkänning i realtid används för första gången ska Polismyndigheten och Säkerhetspolisen göra en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen.	Innan ett AI-system för ansiktsigenkänning i realtid används för första gången ska Polismyndigheten och Säkerhetspolisen göra en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen *och registrera systemet enligt artikel 49 i förordningen. Ett sådant system får dock användas utan registrering om användningen inte kan avvakta. I sådana fall ska en registrering ske så snart det är möjligt.*

Denna lag träder i kraft den dag som regeringen bestämmer.

2.3 Förslag till lag om ändring i lagen (1957:668) om utlämning för brott

Härigenom föreskrivs att det i lagen (1957:668) om utlämning för brott ska införas en ny paragraf, 16 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	16 a § *För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 7 § andra stycket.*

Denna lag träder i kraft den 1 juli 2026.

2.4 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om lagen (2000:562) om internationell rättslig hjälp i brottmål

dels att 1 kap. 2 § och 2 kap. 1 och 2 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 4 kap. 28 i och 28 j §§, och närmast före 4 kap. 28 i § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[1]	
Rättslig hjälp enligt denna lag omfattar följande åtgärder:	
1. förhör i samband med förundersökning i brottmål,	
2. bevisupptagning vid domstol,	
3. telefonförhör,	
4. förhör genom videokonferens,	
5. kvarstad, beslag, penningbeslag samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken,	
6. föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken,	
7. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	
8. hemlig kameraövervakning,	
9. hemlig rumsavlyssning,	
10. hemlig dataavläsning,	
11. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning,	
12. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,	
13. överförande av frihetsberövade för förhör m.m., *och*	13. överförande av frihetsberövade för förhör m.m.,
14. rättsmedicinsk undersökning av en avliden person.	14. rättsmedicinsk undersökning av en avliden person, *och*
	15. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

Vad som i denna lag sägs om beslag gäller även för penningbeslag.

Lagen hindrar inte att hjälp lämnas med någon annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

[1] Senaste lydelse 2024:839.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

2 kap.

1 §[2]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10 *och* 14 ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10, 14 *och 15* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.

Rättslig hjälp som avses i 1 kap. 2 § första stycket 11–13 lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

2 §[3]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 7–10, 12 *och* 14 får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, genomsökning på distans och beslag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 7–10, 12, 14 *och 15* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, genomsökning på distans och beslag.

4 kap.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

28 i §

En ansökan om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid som avser någon som befinner sig i Sverige handläggs av

[2] Senaste lydelse 2021:239.
[3] Senaste lydelse 2022:321.

åklagare. Ansökan får endast avse användning enligt 4 § 1–4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd. Om det är fara i dröjsmål, får användningen påbörjas utan tillstånd. I sådana fall tillämpas bestämmelserna i 13–16 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

Om användningen påbörjas utan tillstånd ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

I fråga om underrättelse till en enskild enligt 17 och 18 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 4 kap. 25 § tredje stycket denna lag tillämpas.

28 j §

Om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska avse någon som befinner sig i en annan stat och den andra staten kräver att ansökan först ska prövas av domstol i Sverige, får rätten på begäran av svensk åklagare besluta att tillåta användningen.

Underrättelse enligt 17 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska inte lämnas.

Denna lag träder i kraft den 1 juli 2026.

2.5 Förslag till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder

Härigenom föreskrivs att det i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder ska införas en ny paragraf, 4 kap. 3 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	3 a §
	För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 7 § andra stycket.

Denna lag träder i kraft den 1 juli 2026.

2.6 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 18 kap. 1 och 19 §§ och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
1 §[1]	
Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.	Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. *Motsvarande sekretess gäller för uppgift som hänför sig till angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till

1. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde, eller

2. annan verksamhet än sådan som avses i 1 eller i första stycket som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

19 §[2]

Den tystnadsplikt som följer av 5–7, 8, 8 b, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att med-	Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att med-

[1] Senaste lydelse 2024:328.
[2] Senaste lydelse 2025:1508.

dela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare *eller* inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	dela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *eller uppgift om användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

35 kap.

1 §[3]

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,
3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),

[3] Senaste lydelse 2024:788.

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag, *eller*

10. utredning om självständigt förverkande.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Föreslagen lydelse

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

10. utredning om självständigt förverkande, *eller*

11. angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

Sekretessen enligt första stycket 2 *och 11* gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

2.7 Förslag till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder

Härigenom föreskrivs att det i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder ska införas en ny paragraf, 3 kap. 3 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	3 a §
	För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 7 § andra stycket.

Denna lag träder i kraft den 1 juli 2026.

2.8 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder

dels att 1 kap. 4 §, 2 kap. 1 och 5 §§ och 3 kap. 4 § ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 2 kap. 19 c och 19 d §§ och 3 kap. 37 c §, och närmast före 2 kap. 19 c § och 3 kap. 37 c § nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
4 §[1]	
En utredningsåtgärd enligt denna lag ska avse eller motsvara	
1. förhör under förundersökning,	
2. bevisupptagning vid domstol,	
3. förhör genom ljudöverföring eller ljud- och bildöverföring,	
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, en åtgärd enligt 27 kap. 15 § eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § samma balk,	
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning,	
7. tillfälligt överförande av en frihetsberövad person,	
8. rättsmedicinsk undersökning av en avliden person,	
9. kontrollerad leverans,	
10. bistånd i en brottsutredning med användning av en skyddsidentitet,	
11. inhämtande av bevis som finns hos en myndighet, *eller*	11. inhämtande av bevis som finns hos en myndighet,
	12. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid, eller
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.	*13.* andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.
2 kap.	
1 §	
En utredningsorder får utfärdas av åklagare för en utredningsåtgärd som avses i 1 kap. 4 § 1 och 3–*12*.	En utredningsorder får utfärdas av åklagare för en utredningsåtgärd som avses i 1 kap. 4 § 1 och 3–*13*.

[1] Senaste lydelse 2021:241.

5 §[2]

Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser

1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,

2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning, *eller*

3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.

2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning,	2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning,
3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m., *eller*	3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m., *eller*
	4. användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken eller 17 § lagen (2020:62) om hemlig dataavläsning utfärda en utredningsorder för en åtgärd som anges i första stycket 1 eller 2. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, genomsökning på distans, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket, 10 d § andra stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller det som föreskrivs i rättegångsbalken eller annan författning för den åtgärd som avses.

	<u>Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid</u>
	19 c §
	En utredningsorder för användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid i en annan medlemsstat får endast avse en åtgärd enligt 4 § 1–4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

[2] Senaste lydelse 2023:539.

	19 d § *Om en utredningsorder har utfärdats för användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska åklagare, om det inte längre finns skäl för ett tillstånd att använda systemet, omedelbart upphäva beslutet. Polismyndigheten eller Säkerhetspolisen ska omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.*
3 kap. 4 §	
En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10 *eller* 11 får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda.	En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10, 11 *eller 12* får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda.
	Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid
	37 c § *I fråga om underrättelse till en enskild enligt 17 och 18 §§ lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 36 § andra stycket tillämpas.*

Denna lag träder i kraft den 1 juli 2026.

2.9 Förslag till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket

Härigenom föreskrivs att det i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket ska införas en ny paragraf, 3 kap. 6 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	6 a §
	I frågor om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid tillämpas bestämmelserna i 4 kap. 3 a § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.

Denna lag träder i kraft den 1 juli 2026.

3 Ärendet och dess beredning

I november 2023 gavs en utredare i uppdrag att förbättra förutsättningarna för polisen att använda kamerabevakning i sin verksamhet. Uppdraget bestod bl.a. i att utreda polisens möjligheter att använda sig av teknik för automatisk ansiktsigenkänning. Innan uppdraget skulle redovisas antogs Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens), här benämnd AI-förordningen. AI-förordningen trädde i kraft den 1 augusti 2024 och finns i *bilaga 1*. Förordningen innehåller ett förbud mot att använda AI-system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål (här benämnt AI-system för ansiktsigenkänning i realtid om inget annat anges).

I promemorian Förbättrade möjligheter för polisen att använda kamerabevakning (Ds 2024:11) föreslogs att AI-förordningens möjlighet till undantag från förbudet ska utnyttjas. Av promemorian framgår dock att förslaget behöver kompletteras i flera avseenden. Promemorians övriga förslag har lett till lagstiftning, se propositionen Kamerabevakning i brottsbekämpning och annan offentlig verksamhet – utökade möjligheter och ett enklare förfarande (prop. 2024/25:93).

I promemorian Polisens användning av AI för ansiktsigenkänning i realtid (Ds 2025:7) lämnas förslag på en ny lag som möjliggör för Polismyndigheten och Säkerhetspolisen att använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid på allmän plats. En sammanfattning av promemorian finns i *bilaga 2*. Promemorians lagförslag finns i *bilaga 3*. Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissyttrandena finns tillgängliga på regeringens webbplats (www.regeringen.se) och i lagstiftningsärendet (Ju2025/00676). I denna proposition behandlas de lagförslag som lämnas i Ds 2025:7.

En särskild utredare har haft i uppdrag att se över behovet i övrigt av nationella anpassningar till följd av AI-förordningen. Det uppdraget redovisades den 6 oktober 2025 i betänkandet Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation (SOU 2025:101). Betänkandet har remitterats.

Lagrådet

Regeringen beslutade den 27 november 2025 att inhämta Lagrådets yttrande över de lagförslag som finns i *bilaga 5*. Lagrådets yttrande finns i *bilaga 6*. Regeringen följer delvis Lagrådets synpunkter och förslag som behandlas i avsnitt 6.1, 7.1, 8, 10, 11 och 14.2 och i författningskommentaren. I förhållande till lagrådsremissen har ikraftträdandet av förslagen flyttats fram. Förslaget om senare ikraftträdande är författningstekniskt och även i övrigt av sådan beskaffenhet att Lagrådets hörande skulle sakna betydelse. Regeringen har därför inte inhämtat Lagrådets yttrande över det förslaget. I förhållande till lagrådsremissens lagförslag görs dessutom vissa språkliga och redaktionella ändringar.

4 AI-förordningen ger utrymme för att använda AI-system för ansiktsigenkänning i realtid

4.1 Kort om AI-förordningen

Syftet med AI-förordningen är att skapa harmoniserade regler för artificiell intelligens (AI) inom EU genom att säkerställa en hög skyddsnivå för hälsa, säkerhet och grundläggande rättigheter. På så sätt främjas de positiva aspekterna av AI samtidigt som fri rörlighet av AI-system på den inre marknaden säkerställs.

Genom ett riskbaserat angreppssätt syftar AI-förordningen till att skapa en strukturerad uppdelning mellan olika typer av AI-system och dess användning där vissa är förbjudna och andra tillåtna men med restriktioner och krav i form av bl.a. registrering hos ansvarig myndighet. Ett AI-system definieras enligt AI-förordningen som ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras (artikel 3.1).

AI-förordningen är direkt tillämplig i alla EU-medlemsstater. AI-förordningen gäller alltså som lag i Sverige och ska som utgångspunkt tillämpas direkt av svenska myndigheter utan att bestämmelserna återges i nationella föreskrifter.

4.2 Förordningen innehåller förbud mot att använda AI-system för ansiktsigenkänning i realtid …

AI-system som har en negativ påverkan på säkerhet eller grundläggande rättigheter anses enligt AI-förordningen utgöra högrisksystem och omfattas av särskilda bestämmelser och begränsningar. Av artikel 5 framgår att vissa användningsområden utgör en oacceptabel risk. Det är fråga om system som anses utgöra ett hot mot människor och inom dessa områden är AI-system förbjudna. Enligt artikel 5.1 h i AI-förordningen är det förbjudet att använda AI-system för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål. Förbudet trädde i kraft den 2 februari 2025.

AI-system för biometrisk fjärridentifiering i realtid definieras som ett system för biometrisk fjärridentifiering där infångning av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål och omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående (artikel 3.42). Realtidssystem involverar direktupptagningar eller näst intill direktupptagningar av material, såsom videoupptagningar, genererade med kamera eller annan

utrustning med liknande funktion. AI-system för biometrisk fjärridentifiering i efterhand baseras däremot på redan insamlade biometriska uppgifter och jämförelsen och identifieringen sker med en betydande fördröjning. Det handlar om bilder eller videoupptagningar som har genererats genom t.ex. övervakningskameror före användningen av AI-systemet (skäl 17). En sökning mot ett register som sker med en bild som är hämtad ur ett redan insamlat material från en kamerabevakning anses därmed inte utgöra biometrisk fjärridentifiering i realtid, även om sökningen sker med ett AI-system.

4.3 … men det är möjligt att föreskriva om undantag

En medlemsstat får i sin nationella rätt föreskriva en möjlighet att helt eller delvis tillåta användning av AI-system för ansiktsigenkänning i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål.

Brottsbekämpning definieras i förordningen som verksamhet som genomförs av brottsbekämpande myndigheter eller på deras vägnar för att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 3.46). Med allmänt tillgängliga platser avses varje offentlig- eller privatägd fysisk plats som är tillgänglig för ett obestämt antal fysiska personer, utan hänsyn till om vissa villkor eller omständigheter för tillträde kan gälla, och oberoende av eventuella kapacitetsbegränsningar (artikel 3.44).

En medlemsstat får tillåta användningen inom de gränser och på de villkor som anges i artikel 5.1 h–5.7 i AI-förordningen. För varje sådan användning krävs enligt artikel 5.3 som utgångspunkt ett förhandstillstånd. Medlemsstaten ska i sin nationella rätt fastställa de nödvändiga närmare reglerna för begäran om, utfärdande och utövande av samt tillsyn över och rapportering om de tillstånd som avses i artikel 5.3. Det ska också anges för vilka av de syften som förtecknas i artikel 5.1 h, inbegripet för vilka av de brott som avses i punkten (iii), de behöriga myndigheterna kan få tillstånd att använda dessa system för brottsbekämpande ändamål (artikel 5.5).

Enligt artikel 5.1 h får användning av AI-system för ansiktsigenkänning i realtid tillåtas endast i den mån sådan användning är absolut nödvändig för något av följande syften. (i) Målinriktad sökning efter specifika offer för människorov, människohandel eller sexuellt utnyttjande av människor, samt sökning efter försvunna personer. (ii) Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ett verkligt och aktuellt eller verkligt och förutsebart hot om en terroristattack. (iii) Lokalisering eller identifiering av en person som misstänks ha begått ett brott, i syfte att genomföra en brottsutredning, lagföring eller ett verkställande av en straffrättslig påföljd för brott som avses i bilaga II och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år.

5 Utgångspunkter vid användning av AI-system för ansiktsigenkänning i realtid

5.1 Inledning

Användning av AI-system för ansiktsigenkänning i realtid innebär en biometrisk behandling av material från exempelvis en kamera. Behandlingen generar ett resultat som innebär att den person som söks kan lokaliseras eller identifieras. För att systemet ska kunna hitta den person som avses bearbetas uppgifter om en potentiellt stor mängd människor. Det är nödvändigt att användningen av tekniken är förenlig med enskildas grundläggande fri- och rättigheter. Sådana bestämmelser finns i regeringsformen och i vissa internationella rättsakter som Sverige är bunden av. Eftersom bearbetningen innebär en personuppgiftsbehandling måste tekniken också användas på ett sätt som är förenligt med den dataskyddsreglering som finns på området som bl.a. syftar till att värna om enskildas personliga integritet. Tekniken förutsätter i princip användning av kameror, vilket innebär att bevakningen, utöver den dataskyddsrättsliga regleringen, behöver förhålla sig till bestämmelserna i kamerabevakningslagen (2018:1200) eller regleringen om hemlig kameraövervakning i rättegångsbalken eller lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen).

5.2 Grundläggande fri- och rättigheter behöver beaktas

Var och en är gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § andra stycket regeringsformen). Rättigheten får begränsas bara genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och får inte sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ regeringsformen).

Enligt artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rätten till skydd för privat- och familjeliv omfattar bl.a. skydd mot övervakning i olika former. Offentliga myndigheter får inte inskränka denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt bl.a. med hänsyn till statens säkerhet och den allmänna säkerheten, till förebyggande av oordning och brott eller till skydd för andra personers fri- och rättigheter.

Artikel 8 i Europakonventionen ger inte bara upphov till negativa förpliktelser för det allmänna att avhålla sig från omotiverade inskränkningar i enskildas rättigheter, utan även positiva skyldigheter att se till att enskilda tillförsäkras skydd för sina rättigheter gentemot andra enskilda. Det inne-

bär t.ex. att staten i vissa fall kan vara skyldig att införa straffrättslig reglering för att skydda enskilda mot intrång i deras rättigheter från andra enskilda. Det innebär även att staten i sådana fall behöver säkerställa att brott kan utredas effektivt.

En bestämmelse om rätt till respekt för bl.a. privatliv finns också i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga). Stadgan innehåller även ett förbud mot diskriminering på grund av bl.a. kön och etniskt ursprung (artikel 21). Varje begränsning i utövandet av de fri- och rättigheter som erkänns i EU:s rättighetsstadga måste vara föreskriven i lag och förenlig med innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter (artikel 52.1). EU:s rättighetsstadga riktar sig till medlemsstaterna när de tillämpar unionsrätten (artikel 51.1). Det innebär att rättigheterna i stadgan måste iakttas vid tillämpningen av nationell lagstiftning som genomför EU-rätt och nationell lagstiftning som omfattas av unionens tillämpningsområde (EU-domstolens dom den 26 februari 2013 i målet Åkerberg Fransson, C-617/10, punkt 21).

Förenta nationernas konvention om barnets rättigheter (barnkonventionen) innehåller bestämmelser om barns rätt till privatliv. Av artikel 16 följer att inget barn får utsättas för godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv. Vidare framgår av artikel 3 att vid alla åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa. Sedan den 1 januari 2020 gäller barnkonventionen som svensk lag (se lagen [2018:1197] om Förenta nationernas konvention om barnets rättigheter). All lagstiftning som rör barn ska utformas i överensstämmelse med barnkonventionens bestämmelser (prop. 2017/18:186 s. 93).

Rätten till skydd för privatliv finns även i artikel 17 i FN:s internationella konvention om medborgerliga och politiska rättigheter (ICCPR). Av artikeln framgår att ingen får utsättas för godtyckligt eller olagligt ingripande med avseende på privatliv, familj, hem eller korrespondens och inte heller för olagliga angrepp på sin heder eller sitt anseende. Vidare framgår att var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.

5.3 Relevant dataskyddsreglering

När personuppgifter behandlas inom brottsbekämpningen ska Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (dataskyddsdirektivet) tillämpas. Dataskyddsdirektivet har huvudsakligen genomförts i svensk rätt genom brottsdatalagen (2018:1177).

I brottsdatalagens andra kapitel finns bestämmelser om grundläggande krav på personuppgiftsbehandling som direkt svarar mot de bestämmelser som finns i dataskyddsdirektivet. I 2 kap. 1 § anges de tillåtna rättsliga grunderna för att behandla personuppgifter. Enligt första stycket får personuppgifter behandlas om det är nödvändigt för att en behörig myndighet ska kunna utföra sin uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Bestämmelsen ger den yttre ramen för när det är tillåtet att behandla personuppgifter enligt lagen. Personuppgifter får bara behandlas om det är nödvändigt för att fullgöra en sådan uppgift. I 2 kap. 3 § anges att personuppgifter bara får behandlas för särskilda, uttryckligen angivna och berättigade ändamål. Ändamålen med behandlingen måste bestämmas redan när personuppgifter behandlas första gången, eftersom det är i för-hållande till ändamålen som det ska prövas om personuppgifterna som behandlas är adekvata och relevanta för ändamålet med behandlingen och hur många personuppgifter som behöver behandlas. Ändamålet får inte vara så vagt eller omfattande att en prövning blir omöjlig i praktiken. Att ändamålet ska vara berättigat innebär att det måste finnas en koppling till de rättsliga grunderna.

Bestämmelser om behandling av känsliga personuppgifter finns i 2 kap. 11–14 §§. I 11 § första stycket slås fast att personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som rör hälsa, sexualliv eller sexuell läggning inte får behandlas. Av andra stycket framgår att personuppgifter som behandlas dock får kompletteras med sådana känsliga personuppgifter, när det är absolut nödvändigt för ändamålet med behandlingen. Av 12 § framgår att biometriska och genetiska uppgifter endast får behandlas om det är särskilt föreskrivet och absolut nödvändigt för ändamålet med behandlingen.

Brottsdatalagen innehåller också bestämmelser om den personuppgiftsansvariges skyldigheter och säkerheten för personuppgifter. Vidare innehåller brottsdatalagen bestämmelser om enskildas rättigheter. Det handlar bl.a. om den personuppgiftsansvariges och dataskyddsombudets kontaktuppgifter samt information om kategorier av ändamål för behandlingen, rätten att begära information, rättelse eller radering och möjligheten att lämna in klagomål till tillsynsmyndigheten (Integritetsskyddsmyndigheten). Lagen innehåller också bestämmelser om tillsyn och skadestånd.

Utöver brottsdatalagen finns särskilda registerförfattningar med specialbestämmelser för myndigheter som behandlar personuppgifter på brottsdatalagens område. Dessa författningar tar hänsyn till de särskilda behov som dessa myndigheter har av att kunna behandla personuppgifter för att utföra sina arbetsuppgifter. För Polismyndighetens, och i begränsade fall även Säkerhetspolisens, behandling av personuppgifter på brottsdatalagens område gäller lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag).

Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet i dess brottsbekämpande och lagförande verksamhet omfattas inte av brottsdatalagen. För sådan behandling gäller i stället lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter. Regleringen av

dessa delar av Säkerhetspolisens personuppgiftsbehandling har varit föremål för en översyn som nyligen redovisades i betänkandet Säkerhetspolisens behandling av personuppgifter (SOU 2025:49). Betänkandet bereds för närvarande i Regeringskansliet.

5.4 Regleringen av kamerabevakning

Användning av AI-system för ansiktsigenkänning i realtid innebär en biometrisk behandling av material som samlas in med stöd av kamerabevakningslagen eller regleringen om hemlig kameraövervakning. Kamerabevakningslagens syfte är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda människor mot otillbörligt intrång i den personliga integriteten vid sådan bevakning. Lagen gäller för sådan kamerabevakning som bedrivs öppet utan att döljas för dem som bevakas (5 §).

Sedan den 1 april 2025 gäller särskilda bestämmelser i kamerabevakningslagen för kamerabevakning som en myndighet bedriver i verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen eller lagen om Säkerhetspolisens behandling av personuppgifter. I sådan verksamhet får kamerabevakning bedrivas av en myndighet om bevakningen är nödvändig för ett syfte som anges i de lagarna. Dessutom ska en dokumenterad intresseavvägning göras. Det innebär att kamerabevakning endast får bedrivas om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad.

Vid bedömningen av intresset av kamerabevakning ska det särskilt beaktas om bevakningen behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott på bl.a. en brottsutsatt plats, platser där det av särskild anledning finns risk för angrepp på någons liv, hälsa eller trygghet eller på egendom eller det med hänsyn till omständigheterna finns risk för allvarlig eller omfattande brottslighet. Det ska också särskilt beaktas om bevakningen behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott och bevakningen sker på en plats som med hänsyn till omständigheterna har strategisk betydelse för att motverka allvarlig brottslighet eller brott som har samband med sådan brottslighet.

Vid bedömningen av den enskildes intresse av att inte bli bevakad ska det särskilt beaktas hur bevakningen ska utföras, om teknik som ökar risken för integritetsintrång som exempelvis ansiktsigenkänning ska användas. Vid bedömningen ska hänsyn också tas till om teknik som främjar skyddet av den enskildes personliga integritet ska användas, och vilket område som ska bevakas.

Det krävs att myndigheterna gör intresseavvägningen innan bevakningen påbörjas. En ny bedömning ska göras och dokumenteras innan myndigheten ändrar bevakningen på ett betydande sätt som ökar risken för intrång i enskildas personliga integritet och om förhållandena på den plats som bevakas ändras på ett betydande sätt som minskar intresset av bevakningen eller ökar risken för intrång i enskildas personliga integritet. Det finns undantag som innebär att en intresseavvägning inte behöver göras eller dokumenteras.

Vad gäller hemlig kameraövervakning får sådan som utgångspunkt endast bedrivas med stöd av ett förhandstillstånd av en domstol. I vissa brådskande fall kan kameraövervakningen ske utan ett tillstånd men då sker alltid en domstolsprövning i efterhand (se 27 kap. 21 och 21 a §§ rättegångsbalken samt 6 och 6 a §§ preventivlagen). Hemlig kameraövervakning får endast ske om det är av synnerlig vikt och proportionerligt. Tiden för övervakningen får inte överstiga vad som är nödvändigt (se 27 kap. 20 b och 21 §§ rättegångsbalken samt 3 och 7 §§ preventivlagen).

6 Polisen ska ges möjlighet att använda AI-system för ansiktsigenkänning i realtid

6.1 En ny lag om polisens användning av AI för ansiktsigenkänning i realtid

Regeringens förslag

Det ska införas en ny lag som reglerar under vilka förutsättningar polisen i sin brottsbekämpande verksamhet får använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid. Lagen ska benämnas lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

Promemorians förslag

Förslaget i promemorian stämmer överens med regeringens.

Remissinstanserna

En majoritet av remissinstanserna tillstyrker förslaget eller invänder inte mot det, bl.a. *Barnombudsmannen*, *Brottsförebyggande rådet*, *Ekobrottsmyndigheten*, *Eskilstuna tingsrätt*, *Förvaltningsrätten i Jönköping*, *Hovrätten över Skåne och Blekinge*, *Kammarrätten i Göteborg*, *Kustbevakningen*, *Malmö tingsrätt*, *Polismyndigheten*, *Svea hovrätt*, *Säkerhetspolisen*, *Tullverket* och *Åklagarmyndigheten*.

Civil Rights Defenders avstyrker förslaget och menar att behovet av tekniken inte är tillräckligt välmotiverat för att berättiga en sådan långtgående inskränkning av den personliga integriteten och rättssäkerheten. *Institutet för mänskliga rättigheter* lyfter att det finns bristande evidens i forskningen kring kamerabevakningens effekter i brottsbekämpningen. Enligt *Stockholms tingsrätt* är det oklart vilka konkreta positiva följder användningen av tekniken skulle få för polisens arbete.

Centrum för rättvisa varken tillstyrker eller avstyrker förslaget om att polisen ska ges möjlighet att använda tekniken. Organisationen uppfattar att förslaget inte innebär nya möjligheter för polisen att inhämta eller

bereda sig tillgång till nya uppgifter och anser att detta med fördel skulle kunna förtydligas i den nya lagen.

Integritetsskyddsmyndigheten anser att användningen av ordet ansiktsigenkänning i lagens namn är missvisande eftersom användningen av tekniken även omfattar andra former av biometrisk fjärridentifiering.

Skälen för regeringens förslag

Det finns behov av effektiva verktyg i brottsbekämpningen

Allvarlig våldsbrottslighet, framför allt skjutningar och sprängningar inom den kriminella miljön, är ett svårt samhällsproblem. Den ökade tillgången på illegala vapen och explosiva varor i samhället tillsammans med den ökade benägenheten inom kriminella miljöer att använda dessa gör att våldet utgör ett mycket allvarligt hot. Det har blivit vanligare med dödligt våld utomhus och på allmänna platser. Inte sällan är det automatvapen som används. Det har vid flera tillfällen de senaste åren inträffat att våld kopplat till konflikter i den kriminella miljön drabbar personer utan koppling till konflikten. Utöver våldsbrottslighet är andra allvarliga brott vanligt förekommande i den kriminella miljön, däribland narkotikabrott. Narkotikahandeln utgör en betydande inkomstkälla för de kriminella nätverken och våld och konflikter i de kriminella miljöerna är ofta narkotikarelaterade. Det kan t.ex. vara fråga om uppgörelser om vem som ska hantera narkotikamarknaden i ett visst område. Den allvarliga brottsligheten är ofta organiserad. Den blir också alltmer gränsöverskridande.

Lagrådet menar att det tydligt bör motiveras varför det är nödvändigt med ytterligare verktyg, såsom användningen av AI i realtid i annan och större utsträckning än att bekämpa organiserad brottslighet och brott i kriminella miljöer. Även om stort fokus de senaste åren legat på att bekämpa den allvarliga brottslighet som utövas av kriminella nätverk och deras möjliggörare kan regeringen konstatera att också annan brottslighet än den organiserade fortsätter att innebära allvarliga utmaningar. Exempelvis är förekomsten av våld mot kvinnor och barn oacceptabelt hög. Även annan allvarlig brottslighet, som grova vålds- och sexualbrott, gränsöverskridande brottslighet som människohandel samt organiserade stöld- och bedrägeribrott i stor skala, medför otrygghet och betydande skada för enskilda, företag och samhället i stort. Otryggheten har de senaste åren hållit sig fast på höga nivåer och särskilt oroande är otryggheten bland kvinnor samt i utsatta områden. Även oron för brottsligheten har under senare år legat på höga nivåer och begränsar hur människor lever sina liv. Sammantaget är brottsligheten ett samhällsproblem med stor påverkan på såväl enskilda som Sverige som land. Riskerna som brottsligheten ger upphov till är uppenbara och utgör ett allvarligt hot mot det demokratiska samhället. Staten har ett ansvar för att upprätthålla rättstryggheten för enskilda. I det ansvaret ligger att säkerställa att det finns en väl fungerande brottsbekämpning. För att kunna vända den brottsutveckling som skett måste de brottsbekämpande myndigheterna ha effektiva och ändamålsenliga verktyg i sitt arbete med att bekämpa brott. Detta är även en viktig del i att kunna stå rustade mot terrorism och våldsbejakande extremism. Mot den bakgrunden konstaterar

regeringen att det finns behov av ytterligare åtgärder för att bekämpa den allvarliga brottsligheten.

Möjligheten att använda AI-system för ansiktsigenkänning i realtid är ett effektivt verktyg i brottsbekämpningen

Möjligheten att identifiera personer med hjälp av biometri har utvecklats mycket snabbt på senare tid. Det gäller inte minst teknik för avancerad ansiktsigenkänning och annan biometrisk fjärridentifiering med hjälp av AI. Tekniken innebär möjligheter till nya, effektiva verktyg för bl.a. brottsbekämpande myndigheter att utföra sitt uppdrag och kan bidra till en bättre och mindre resurskrävande brottsbekämpning.

Den användning av AI-system för ansiktsigenkänning och annan biometrisk fjärridentifiering i realtid som får tillåtas enligt AI-förordningen innebär att material som samlas in och behandlas med stöd av annan lagstiftning, exempelvis brottsdatalagen, i realtid bearbetas och granskas för att lokalisera eller identifiera en eller flera på förhand utpekade personer för vissa syften. AI-systemet bearbetar materialet och genererar ett resultat utifrån den data som systemet har försetts med, exempelvis en bild på en eller flera personer som är av intresse för de brottsbekämpande myndigheterna. Tekniken förutsätter i princip användning av kameror som exempelvis omfattas av kamerabevakningslagen eller regleringen om hemlig kameraövervakning i rättegångsbalken.

I anledning av synpunkten från *Stockholms tingsrätt* om vilka följder teknikanvändningen skulle få för polisens arbete vill regeringen framhålla att användning av tekniken skulle innebära att polisen ges bättre möjligheter att analysera stora mängder bildmaterial och filtrera på ansikten. Det som normalt skulle ta flera dagar eller veckor att analysera kan med hjälp av AI-tekniken ske på några sekunder, vilket skulle frigöra resurser och göra utredningsunderlagen mer träffsäkra (jfr Statskontorets rapport Myndigheterna och AI, s. 27). Det skulle också ge polisen förutsättningar att agera snabbare, vilket kan vara helt avgörande när det handlar om att förhindra planerad brottslighet, hitta en gärningsman på flykt eller säkra bevis i en pågående förundersökning. Det är fråga om en mycket effektiv metod att behandla material.

Som *Centrum för rättvisa* framhåller är det inte så att användningen innebär insamling av någon ny information. I stället handlar det om att ett AI-system bearbetar ett kameramaterial och genererar ett resultat utifrån den data som systemet har försetts med. Materialet är redan tillgängligt för polisen även utan användning av tekniken. Som *Säkerhetspolisen* påpekar har inhämtningsåtgärden som ligger till grund för insamlingen av uppgifter i det skedet redan bedömts vara förenlig med annan tillämplig reglering, exempelvis kamerabevakningslagen, vars syfte är bl.a. att säkerställa den enskildes integritet. Användningen av tekniken innebär alltså en bearbetning av material som redan är tillgängligt för polisen. Ur ett integritetsperspektiv kan det därmed inte, som *Civil Rights Defenders* menar, likställas med sådana hemliga tvångsmedel som ger polisen möjlighet att i hemlighet samla in material. Användningen av tekniken är närmast att likna vid en polisiär utredningsmetod. Som föreslås nedan kommer den nya lagen endast reglera polisens möjlighet att använda AI-tekniken och inte ge stöd för någon inhämtning av eller annan tillgång till nya uppgifter.

Enligt regeringens uppfattning finns inte något behov av att i lagen ytterligare förtydliga detta förhållande.

Polisen ska tillåtas att använda AI-system för ansiktsigenkänning i realtid

Det finns ett tydligt behov för polisen att kunna använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid bl.a. i förundersökningar avseende grovt narkotikabrott, olaga frihetsberövande, mord eller människorov där det exempelvis finns en referensbild på en känd eller okänd misstänkt gärningsperson. Det finns även ett behov av att kunna använda tekniken i ärenden om försvunna personer som misstänks ha utsatts för brott och ärenden som avser personer som är misstänkta eller dömda för brott som håller sig undan lagföring eller straffverkställighet. De senare ärendena rör framför allt personer som har anhållits eller häktats i sin frånvaro under en pågående brottsutredning eller som har dömts för brott till en frihetsberövande påföljd men som inte har inställt sig till eller avvikit från verkställighet av straffet. När material från kameror granskas i efterhand finns det en risk för att uppgifterna inte längre är användbara (exempelvis då gärningspersonen har hunnit försvinna eller ett hot redan har förverkligats).

Civil Rights Defenders anser att det krävs mycket tungt vägande skäl för att motivera användning av tekniken med hänsyn till de risker som övervakningen innebär för personlig integritet och rättssäkerhet. Enligt organisationen visar studier kring kamerabevakning i socioekonomiskt utsatta områden att kameror sällan bidrar till ökad upplevd trygghet utan andra insatser som t.ex. ökad polisiär närvaro eller trygghetsvandringar har en större påverkan på känslan av trygghet. Även *Institutet för mänskliga rättigheter* lyfter att det finns bristande evidens i forskningen kring kamerabevakningens effekter på brottsbekämpningen.

I anledning av dessa synpunkter vill regeringen framhålla att förslaget inte syftar till att kamerabevakningen och därmed övervakningen av människor i vårt samhälle ska öka utan att polisen ska ges möjlighet att i särskilt utpekade fall använda en ny effektiv teknik för behandling av material som även annars är tillgängligt för polisen för att förhindra och utreda allvarlig brottslighet. Enligt regeringen har alla rätt att tryggt vistas i det offentliga rummet utan att utsättas för brott. En sådan trygghet kan uppnås bl.a. genom att engagera medborgarna och bygga lokala samhällen som präglas av omsorg och tillit. Effekterna av det sociala brottsförebyggande arbetet ska inte underskattas. Regeringen arbetar aktivt med att bl.a. skapa goda förutsättningar för och utveckla det brottsförebyggande arbetet i skolan, öka möjligheten till en aktiv och meningsfull fritid i gemenskap med andra och se till att barn och unga i utsatthet och deras familjer tidigt får stöd och hjälp innan problematiken har eskalerat. Detta arbete bedrivs för att förebygga all sorts brottslighet men ett särskilt fokus riktas mot att bryta rekryteringar till de kriminella gängen, att förhindra att barn och unga involveras i kriminalitet och att få personer som begår brott att upphöra med det. Trots dessa ansträngningar kommer brott att begås och polisen behöver då vara rustad att kunna lösa sin uppgift framöver. För att motverka de omfattande utmaningar med kriminalitet och otrygghet som finns i Sverige behöver det

brottsförebyggande arbetet därför kombineras med moderna polisiära arbetsmetoder för brottsbekämpning.

Lagrådet invänder inte mot att det införs en möjlighet att i brottsbekämpningen använda AI-system för ansiktsigenkänning i realtid men anför på ett mer allmänt plan att det finns anledning att anlägga ett mer restriktivt perspektiv på användningen av en sådan möjlighet än vad lagrådsremissens förslag ger uttryck för.

Som redovisas nedan förväntas användningen av tekniken få effekt och göra stor nytta i polisens arbete med att bekämpa brott. Detta bedöms bidra till att tryggheten i samhället ökar. Det måste dock beaktas att användning av tekniken för brottsbekämpande ändamål på allmän plats innebär rättighetsinskränkningar för en potentiellt stor mängd människor på ett relativt påtagligt sätt. Eftersom användningen av AI i realtid kan innebära intrång i människors personliga integritet bör tekniken redan av den anledningen inte användas i större utsträckning än nödvändigt och endast för syften som är godtagbara i ett demokratiskt samhälle. Som *Åklagarmyndigheten* framhåller har lagstiftaren bedömt att den enskildes intresse av att ”inte synas” får stå tillbaka genom reglerna om kamerabevakning för angelägna samhällsintressen. I balansgången mellan en effektiv brottsbekämpning och skyddet för den personliga integriteten måste beaktas hur den aktuella brottsligheten ser ut i samhället. Organiserad brottslighet utgör allvarliga hot mot enskilda, men också mot samhället i stort. Detta innebär att ett större ingrepp i den personliga integriteten kan vara befogat till förmån för att ge de brottsbekämpande myndigheterna effektiva verktyg att genomföra sina uppdrag. Som framgår av avsnitt 15.2 (förslagens förenlighet med grundläggande fri- och rättigheter) bedöms den föreslagna regleringen utgöra en rimlig avvägning mellan behovet av effektiva verktyg i brottsbekämpningen och den enskildes rätt till skydd för sin personliga integritet och sitt privatliv. Det är därför motiverat att i möjligaste mån ge polisen förutsättningar att använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål på allmän plats inom de ramar som AI-förordningen sätter upp och med beaktande av de behov som polisen har.

Det kan i sammanhanget noteras att AI-förordningens undantag som tillåter användningen av AI-system i realtid för brottsbekämpande ändamål har utformats just med beaktande av behovet av att säkerställa respekten för enskildas mänskliga rättigheter.

Det krävs lagreglering för att polisen ska tillåtas använda AI-system för ansiktsigenkänning i realtid

För att polisen ska kunna använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål på allmän plats måste användningen vara förenlig med AI-förordningen (se artikel 5.1 h). Ett sådant regelverk behöver också omgärdas av rättssäkerhetsgarantier och kontrollmekanismer som säkerställer att användning av tekniken är rättssäker och att intrången i den personliga integriteten inte blir större än vad som kan godtas enligt regeringsformen, Europakonventionen, EU:s rättighetsstadga, barnkonventionen och ICCPR. I propositionen görs i samband med förslagen i följande avsnitt en

bedömning av deras förenlighet med enskildas fri- och rättigheter. Eftersom en bedömning även måste göras i förhållande till det föreslagna regelverket som helhet, med förutsättningar och skyddsåtgärder, och med beaktande även av de skyddsåtgärder som kan finnas i t.ex. den dataskyddsrättsliga reglering som blir tillämplig på behandlingen av personuppgifter görs en samlad bedömning av hur förslagen förhåller sig till enskildas grundläggande fri- och rättigheter i avsnitt 15.2.

Det kan konstateras att en reglering som tillåter polisen att använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål är av sådant slag att de grundläggande delarna måste finnas i lag. Det finns i dag ingen specifik reglering i svensk rätt om att använda AI-system för ansiktsigenkänning i brottsbekämpningen. I brottsdatalagen och polisens brottsdatalag regleras polisens möjlighet att behandla biometriska uppgifter. De bestämmelserna är dock allmänt hållna och tar sikte på polisens behandling av biometriska uppgifter i stort. Polisens användning av tekniken behöver omgärdas av en relativt detaljerad reglering för att vara förenlig med AI-förordningen. Det framstår mot den bakgrunden som lämpligt att det införs en ny lag som reglerar under vilka förutsättningar polisen får använda tekniken i sin brottsbekämpande verksamhet. I promemorian föreslås att den nya lagen ges namnet AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. *Integritetsskyddsmyndigheten* anser att användningen av uttrycket ansiktsigenkänning i den nya lagens namn är missvisande eftersom användningen av tekniken även omfattar andra former av biometrisk fjärridentifiering. Rubriken till en ny författning bör som utgångspunkt vara kort. Rubriken behöver inte heller vara uttömmande. Ansiktsigenkänning är också den fjärridentifiering som framför allt är i fokus och den som är mest integritetskänslig. Regeringen anser därför att lagen bör ges det namn som föreslås i promemorian.

6.2 Lagens tillämpningsområde

Regeringens förslag

Den nya lagen ska gälla Polismyndighetens användning av AI-system för ansiktsigenkänning i realtid på allmän plats för brottsbekämpande ändamål. Även Säkerhetspolisens användning ska omfattas av lagen men inte när den rör nationell säkerhet.

Med AI-system för ansiktsigenkänning i realtid ska i lagen avses sådana system för biometrisk fjärridentifiering i realtid som omfattas av AI-förordningen.

Promemorians förslag

Förslaget i promemorian stämmer i huvudsak överens med regeringens. I promemorian föreslås att det införs en definition av uttrycket AI-system, i stället för en definition av AI-system för ansiktsigenkänning i realtid.

Remissinstanserna

Åklagarmyndigheten tillstyrker förslaget att den nya lagen ska gälla för de två polismyndigheterna, med undantag för Säkerhetspolisens användning för nationell säkerhet. *Säkerhetspolisen* instämmer i promemorians slutsats att all Säkerhetspolisens användning av AI-system för ansiktsigenkänning i realtid för nationell säkerhet ligger utanför AI-förordningens tillämpningsområde. *Tullverket* anser att tekniken skulle vara till stor hjälp för myndigheten i dess brottsbekämpande uppdrag och att den föreslagna lagen bör vara tillämplig för alla myndigheter med brottsbekämpande befogenheter.

Integritetsskyddsmyndigheten föreslår att det begrepp som används i AI-förordningen – biometrisk fjärridentifiering – också bör användas i den svenska lagen. *Lunds universitet* är tveksamt till att inkludera ”annan biometrisk fjärridentifiering” i lagen och förespråkar i stället att enbart ”ansiktsigenkänning” används. Universitetet för också fram att om den nya lagen även gäller andra former av biometrisk fjärridentifiering än ansiktsigenkänning bör detta framgå direkt av lagen. *Journalistförbundet* och *Tidningsutgivarna* anser att AI-förordningens definition av AI-system är bred. Att tillämpa den definitionen på det sätt som föreslås i promemorian gör, enligt förbundet, att lagen får ett för stort tillämpningsområde. Enligt Journalistförbundet bör det vidare införas ett uttryckligt förbud mot att använda vissa typer av AI-system för ansiktsigenkänning i realtid om systemen registrerar känsliga uppgifter. Lunds universitet för fram att det finns fler begrepp än AI-system som ska ges samma innebörd som termer i AI-förordningen. Universitetet föreslår därför att det i stället bör föreskrivas att uttryck som används i lagen har, om annat inte sägs, samma innebörd som motsvarande uttryck i förordningen.

Justitiekanslern anser att en avgränsning till offentlig plats möjligen skulle medföra en lämpligare balans visavi integritetsintresset jämfört med allmän plats. *Åklagarmyndigheten* anser att det finns anledning att ge klara besked kring vad som omfattas av begreppet allmän plats i förhållande till gränsövergångar.

Skälen för regeringens förslag

Lagen ska gälla polisens användning av AI-system för ansiktsigenkänning i realtid

Den nya lagen bör först och främst gälla när Polismyndigheten använder AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål. Det finns inte förutsättningar att i detta lagstiftningsärende närmare överväga *Tullverkets* synpunkt om att lagen bör gälla generellt för myndigheter med brottsbekämpande befogenheter. För närmare resonemang om Säkerhetspolisens användning av tekniken, se nedan.

Den nya lagen bör gälla användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål. Med detta avses sådan teknik som i AI-förordningen definieras som AI-system för biometrisk fjärridentifiering i realtid. Definitionen av ett AI-system för biometrisk fjärridentifiering är enligt

förordningen ett AI-system vars syfte är att identifiera fysiska personer utan deras aktiva medverkan, vanligtvis på distans, genom jämförelse av en persons biometriska uppgifter med de biometriska uppgifterna i en referensdatabas (artikel 3.41). Det rör sig i första hand om ansiktsigenkänning men kan även vara andra former av biometrisk igenkänning, t.ex. genom rörelsemönster eller röst. För att det ska vara fråga om ett realtidssystem ska infångning av biometriska uppgifter, jämförelse och identifiering ske utan betydande dröjsmål. Det omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående (artikel 3.42).

I promemorian görs bedömningen att begreppet AI-system i den nya lagen bör ges samma innebörd som i AI-förordningen och att definitionen bör framgå av lagen. Enligt artikel 3.1 är ett AI-system ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras. *Journalistförbundet* och *Tidningsutgivarna* anser att förordningens definition av begreppet AI-system är bred, vilket gör att den föreslagna lagen får ett brett tillämpningsområde. Enligt Journalistförbundet vore det mer ändamålsenligt att utgå från det behov som polisen har av att använda AI-teknik och ta fram en definition som tydligt beskriver vilken teknik som avses. Tekniken utvecklas emellertid snabbt och för att lagstiftningen ska följa med utvecklingen behöver regleringen så långt som möjligt vara teknikneutral. Regeringen anser därför att det inte finns skäl att begränsa förslaget till viss specifik AI-teknik.

Lunds universitet är tveksamt till att användningen ska få avse både ansiktsigenkänning och annan biometrisk fjärridentifiering. Universitetet anser inte att begreppet annan biometrisk användning är tillräckligt preciserat och förespråkar i stället att enbart ansiktsigenkänning omfattas av lagens tillämpningsområde. Regeringen konstaterar att den teknik som främst kommer att användas är ansiktsigenkänning men det kan även vara aktuellt för polisen att använda andra former av biometrisk igenkänning. Enligt regeringen finns därför inte anledning att begränsa regleringen till enbart ansiktsigenkänning. *Integritetsskyddsmyndigheten* anser att användningen av uttrycket ansiktsigenkänning i definitionen av AI-system för ansiktsigenkänning i realtid är missvisande eftersom användningen av tekniken även omfattar andra former av biometrisk fjärridentifiering. Myndigheten föreslår att definitionen ändras så att det begrepp som används i AI-förordningen – biometrisk fjärridentifiering – också används i lagen. I likhet med vad regeringen anför i avsnitt 6.1 om lagens namn är det tillräckligt att beskriva det system och den användning som lagen reglerar med begreppet ansiktsigenkänning. Det är en avvägning som får göras mellan intresset av precision och lättillgänglighet. Att begreppet ansiktsigenkänning i lagen omfattar även annan biometrisk fjärridentifiering bör framgå inledningsvis i lagen. Enligt regeringens uppfattning är denna skrivning tydlig och det kan med en sådan skrivning inte råda någon tvekan om att lagen även gäller andra former av biometrisk fjärridentifiering än ansiktsigenkänning. Regeringen ställer sig därför

bakom förslaget i promemorian men tydliggör i lagtexten att AI är en förkortning av artificiell intelligens.

Definitionen av AI-system för ansiktsigenkänning i realtid avgör tillämpningsområdet för lagen. Det är därför särskilt viktigt att begreppet har samma betydelse som i AI-förordningen. Regeringen anser därför att det i lagen bör införas en definition av AI-system för ansiktsigenkänning i realtid som hänvisar till förordningens definition. Med ett sådant system ska i lagen avses sådana AI-system som omfattas av artikel 3.42 i AI-förordningen. Sådana system är alltid AI-system enligt artikel 3.1 och därför behövs inte, så som föreslås i promemorian, någon definition av uttrycket AI-system. *Lunds universitet* för fram att begreppet AI-system inte är den enda termen som ska ges samma innebörd som i AI-förordningen. Universitetet föreslår att det därför bör anges att uttryck som används i lagen har samma innebörd som motsvarande uttryck i förordningen. Regeringen bedömer att det inte finns behov av att införa en bestämmelse som uttryckligen reglerar detta.

Enligt *Journalistförbundet* bör det införas ett uttryckligt förbud mot att använda AI-system för ansiktsigenkänning i realtid om systemen registrerar känsliga uppgifter som exempelvis politisk åsikt, etnicitet eller deltagande i demonstrationer. AI-system för ansiktsigenkänning i realtid får endast användas inom de gränser och villkor som anges i förordningen. Användningen handlar i praktiken om att identifiera eller lokalisera personer med hjälp av bildmaterial som inhämtas med stöd av andra regelverk. AI-förordningen, och därmed även den nya lagen, ger inte utrymme för att använda tekniken för att registrera sådana känsliga uppgifter som Journalistförbundet lyfter. Något behov att införa ett förbud för sådan registrering finns därför inte.

Det är fråga om en verksamhet vars personuppgiftsbehandling omfattas av regleringen i brottsdatalagen (se 1 kap. 2 §). För att tydliggöra lagens tillämpningsområde bör det anges att lagen endast är tillämplig på sådan verksamhet vars personuppgiftsbehandling regleras i brottsdatalagen.

I promemorian föreslås att lagen ska omfatta polisens användning av tekniken på allmän plats. I AI-förordningen används begreppet allmänt tillgängliga platser (se artikel 5.1 h). Det begreppet omfattar varje offentlig- eller privatägd fysisk plats som är tillgänglig för ett obestämt antal fysiska personer, utan hänsyn till om vissa villkor eller omständigheter för tillträde kan gälla, och oberoende av eventuella kapacitetsbegränsningar (se artikel 3.44). Innebörden av allmänt tillgängliga platser överensstämmer i stort med allmän plats i den mening som det används i svensk rätt, bl.a. brottsbalken, se prop. 2011/12:109 s. 41 och författningskommentaren om den närmare innebörden. I AI-förordningen anges att gränskontrollområden inte utgör en allmänt tillgänglig plats (skäl 19 i AI-förordningen). I anledning av *Åklagarmyndighetens* önskemål om klargörande i detta avseende finns det anledning att peka på vad som anges i de riktlinjer som kommissionen har gett ut om att vissa platser kan ha dubbel funktion. Exempelvis betraktas en flygplats i allmänhet som en allmänt tillgänglig plats när det gäller dess gemensamma områden, men det område som är avsett för gränskontroll (där tulltjänstemän är placerade och pass- eller id-kontroller utförs) är undantagna från tillämpningsområdet (punkten 317).

Det finns ett tydligt behov för polisen att kunna använda tekniken på allmän plats och AI-förordningen ger utrymme för det. Regeringen delar därför inte *Justitiekanslerns* synpunkt om att ett mer begränsat begrepp bör användas. Allmän plats är dessutom ett begrepp som är vanligt förekommande i svensk rätt. Regeringen föreslår därför att allmän plats används i lagen.

Användning av tekniken för annan verksamhet än polisens brottsbekämpning eller på plats som inte är allmän faller utanför lagens tillämpningsområde. I vilken mån sådan användning är tillåten får avgöras utifrån det dataskyddsrättsliga regelverket samt övriga bestämmelser i AI-förordningen.

Hänvisningar till EU-rättsakter kan göras antingen statiska eller dynamiska. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse medan en dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. Den nya lagen innehåller vissa materiella hänvisningar till AI-förordningen. För att säkerställa att framtida ändringar i AI-förordningen kan få omedelbart genomslag bör sådana hänvisningar i lagen vara dynamiska.

I det följande används AI-system för ansiktsigenkänning i realtid som benämning på AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål på allmän plats.

Säkerhetspolisens användning av tekniken

Säkerhetspolisen har bl.a. i uppdrag att förebygga, förhindra, upptäcka, utreda och beivra brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott (3 § polislagen [1984:387]). I samband med genomförandet av EU:s dataskyddsreform och det samtidiga införandet av lagen om Säkerhetspolisens behandling av personuppgifter konstaterades att Säkerhetspolisens verksamhet i allt väsentligt ligger utanför dataskyddsdirektivets och brottsdatalagens tillämpningsområde eftersom den rör nationell säkerhet (se prop. 2017/18:232 s. 103 och prop. 2018/19:163 s. 48). Använder Säkerhetspolisen AI-system i sådan verksamhet görs detta alltså för nationell säkerhet.

I artikel 4.2 i fördraget om Europeiska unionen anges bl.a. att den nationella säkerheten också i fortsättningen ska vara varje medlemsstats eget ansvar. I artikel 2.3 i AI-förordningen anges att förordningen inte är tillämplig på områden som inte omfattas av unionsrättens tillämpningsområde och ska under alla omständigheter inte påverka medlemsstaternas befogenheter när det gäller nationell säkerhet. Det anges även att förordningen inte är tillämplig på AI-system om och i den mån de släpps ut på marknaden, tas i bruk eller används med eller utan ändring uteslutande för ändamål som rör nationell säkerhet. Det står alltså klart att Säkerhetspolisens användning av AI-system som enbart är avsedda och används för nationell säkerhet inte omfattas av AI-förordningen.

Av skäl 24 till AI-förordningen framgår att även AI-system som tagits fram för andra ändamål eller som används också för sådana ändamål inte omfattas av förordningen när de används för ändamål som rör nationell säkerhet. I skälet anges att om ett AI-system som utvecklas, släpps ut på marknaden, tas i bruk eller används för ändamål som rör nationell säkerhet

också används för andra ändamål så omfattas ett sådant system av förordningen för den som använder AI-systemet för det andra ändamålet.

Att ett AI-system släpps ut på marknaden eller tas i bruk för både ändamål som rör nationell säkerhet och andra ändamål påverkar inte möjligheten för den som bedriver verksamhet inom nationell säkerhet att använda system för nationell säkerhet utan att tillämpa förordningen.

Inte heller att ett AI-system släpps ut på marknaden för civila eller brottsbekämpande ändamål och sedan används med eller utan ändringar för ändamål som rör nationell säkerhet gör enligt skälet att den senare användningen omfattas av förordningen.

Sammantaget innebär detta att all Säkerhetspolisens användning av AI-system för nationell säkerhet faller utanför AI-förordningens tillämpningsområde, även om det är så att myndigheten delar eller använder andra aktörers systemlösningar. Eftersom det är syftet som avgör om användningen av ett AI-system omfattas av AI-förordningens förbud gäller det anförda även om det är en annan aktör som står för det faktiska utförandet, så länge användningen sker för Säkerhetspolisens räkning. AI-förordningens förbud mot användning av AI-system för ansiktsigenkänning i realtid gäller alltså inte användning för nationell säkerhet. För Säkerhetspolisens verksamhet som rör nationell säkerhet finns därmed inte något behov av undantag från förordningens förbud och inte någon anledning att låta lagen gälla även verksamhet utanför brottsdatalagens tillämpningsområde. I vilken utsträckning Säkerhetspolisen kan använda sig av AI-system för ansiktsigenkänning i realtid för nationell säkerhet får i stället avgöras utifrån den reglering som gäller för myndighetens personuppgiftsbehandling och kamerabevakningslagen.

Det kan i sammanhanget noteras att inte heller AI-konventionen gäller för Säkerhetspolisens verksamhet som rör nationell säkerhet (se artikel 3.2 i konventionen).

Säkerhetspolisen kan emellertid även, om än i begränsad utsträckning, bedriva brottsbekämpande verksamhet som inte rör nationell säkerhet. Detta gäller åtminstone i de fall som regleras i 13 § förordningen (2022:1719) med instruktion för Säkerhetspolisen och 27 § förordningen (2022:1718) med instruktion för Polismyndigheten. Enligt dessa bestämmelser kan Säkerhetspolisen i vissa fall bistå vid polisverksamhet som leds av Polismyndigheten och i enskilda fall kan Polismyndigheten lämna över en förundersökning eller annan liknande uppgift i den brottsbekämpande verksamheten till Säkerhetspolisen för fortsatt handläggning. När Säkerhetspolisen behandlar personuppgifter i sådan verksamhet gäller regleringen i brottsdatalagen. Det kan inte uteslutas att Säkerhetspolisen någon gång i ett sådant ärende skulle ha behov av att använda AI-system för ansiktsigenkänning i realtid. Det bör därför av den inledande bestämmelsen framgå att lagen även omfattar Säkerhetspolisen i den verksamheten.

7 Förutsättningar för att använda AI-system för ansiktsigenkänning i realtid

7.1 AI-system för ansiktsigenkänning i realtid ska få användas för vissa syften

Regeringens förslag

AI-system för ansiktsigenkänning i realtid ska få användas om det är absolut nödvändigt för att lokalisera eller identifiera en viss person

1. som misstänks vara utsatt för människorov, människohandel eller för människoexploatering om den avser sexuella tjänster,
2. som är försvunnen och misstänks vara utsatt för brott,
3. om det finns en överhängande risk för att personen kommer att begå ett allvarligt brott som innebär fara för annans liv eller fysiska säkerhet,
4. som skäligen kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet, eller
5. som dömts för ett sådant brott som avses i 4, i syfte att verkställa den straffrättsliga påföljden.

Promemorians förslag

Förslaget i promemorian stämmer delvis överens med regeringens. I promemorian uppställs delvis andra rekvisit för att AI-system för ansiktsigenkänning i realtid ska få användas, bl.a. att det ska vara av synnerlig vikt för att lokalisera eller identifiera en person, att det ska finnas en påtaglig risk för att en person kommer att begå ett brott som inte uttryckligen begränsas till allvarligt brott och att det kan misstänkas att en person har begått ett brott. Promemorian innehåller inte någon begränsning till människoexploatering om exploateringen avser sexuella tjänster. Promemorian innehåller inget krav på att det ska röra sig om fysisk säkerhet. Även i övrigt är promemorians förslag något annorlunda utformat.

Remissinstanserna

De flesta remissinstanser invänder inte mot förslaget. Flera remissinstanser är dock kritiska till det. Det handlar framför allt om den närmare utformningen och valet av rekvisit för att ange när användningen kan tillåtas. *Institutet för mänskliga rättigheter* och *Sveriges advokatsamfund* avstyrker förslaget och anför att utformningen avviker från AI-förordningen vilket leder till en osäkerhet i tillämpning och praxis. *Säkerhets- och integritetsskyddsnämnden* (från och med den 1 mars 2026 byter myndigheten namn till Myndigheten för säkerhet och integritetsskydd och det nya namnet används härefter) saknar mer

grundliga och övertygande resonemang om proportionalitet avseende behovet av användningen av tekniken för föreslagna syften ställt mot de risker för den personliga integriteten och privatlivet som åtgärderna kan innebära för de personer som berörs av dem.

Ett antal remissinstanser, bl.a. *Eskilstuna tingsrätt*, *Institutet för mänskliga rättigheter*, *Journalistförbundet*, *Centrum för rättvisa* och *Civil Rights Defenders* anser att uttrycket synnerlig vikt i förslaget inte är jämförbart med vad som anges i artikel 5.1 h om att tekniken bara får användas om det är absolut nödvändigt.

Myndigheten för säkerhet och integritetsskydd anser att det bör övervägas om det i bestämmelsen som möjliggör att tekniken används i syfte att lokalisera och identifiera försvunna personer som misstänks ha utsatts för brott ska införas ett kvalifikationskrav på de brott som kan aktualiseras. Bland andra *Svea hovrätt* ställer sig tveksamma till att tekniken ska få användas för att lokalisera potentiella offer för människoexploatering. *Lunds universitet* anser att den nya lagen även bör omfatta försvunna personer som inte misstänks ha utsatts för brott. Universitetet för även fram att vissa uttryck i artikel 5.1 h som ”specifikt” offer för, ”ett specifikt, betydande och överhängande hot” inte framgår tydligt av förslaget. Enligt universitetet bör kravet på specificitet framgå direkt av lagen. Svea hovrätt och Sveriges advokatsamfund för fram liknande synpunkter.

Flera remissinstanser, däribland *Hovrätten över Skåne och Blekinge*, *Malmö tingsrätt*, *Eskilstuna tingsrätt*, *Integritetsskyddsmyndigheten*, *Myndigheten för säkerhet och integritetsskydd*, *Lunds universitet*, *Sveriges advokatsamfund* och *Sveriges Domareförbund*, ifrågasätter uttrycket ”påtaglig risk” i promemorians lagtextförslag som gäller användning för att förhindra brott och för fram att förslaget går utöver vad som är tillåtet enligt förordningen. *Journalistförbundet* anser att det är en brist att det av förslaget inte framgår vilka brott mot människors liv och säkerhet som avses. *Domstolsverket* efterfrågar en uttrycklig begränsning kring hotets allvarsgrad som motsvarar AI-förordningens krav att hotet ska vara ”betydande”. Verket efterfrågar vidare krav på att det ska röra sig om brott med viss allvarsgrad. Hovrätten över Skåne och Blekinge anser att ordalydelsen i författningsförslaget ger intryck av att även omfatta mindre allvarliga brott mot människors liv eller säkerhet. Enligt hovrätten stämmer det inte överens med kravet i AI-förordningen. *Justitiekanslern* för fram liknande synpunkter.

Tullverket anser att det behövs ett förtydligande av om möjligheten att använda tekniken utanför ramarna för en förundersökning gäller för samtliga undantag i förslaget. Motsvarande synpunkter förs fram av *Sveriges advokatsamfund*.

Integritetsskyddsmyndigheten, *Centrum för rättvisa* och *Myndigheten för säkerhet och integritetsskydd* anser att förslaget om att tekniken får användas i syfte att utreda brott redan vid misstankegraden ”kan misstänkas” är lägre än vad som krävs enligt AI-förordningen, medan *Svea hovrätt* är av motsatt uppfattning. Hovrätten menar dock att systematiska skäl kan tala för att samma misstankegrad som används för hemliga tvångsmedel ”skäligen kan misstänkas” bör gälla även för användning av AI-system för ansiktsigenkänning i realtid.

Flera remissinstanser, däribland *Eskilstuna tingsrätt*, *Justitiekanslern* och *Åklagarmyndigheten*, invänder mot att det i regleringen hänvisas till bilaga II till AI-förordningen och anser att de svenska brott som motsvarar brotten i bilagan i stället bör anges i lagen. Justitiekanslern för också fram att kravet på att det för brottet ska vara föreskrivet fängelse i fyra år eller mer inte synes motsvara AI-förordningens lydelse som snarare indikerar ett föreskrivet minimistraff om fängelse i fyra år. *Tullverket* anser att förslaget i denna del är otydligt och anser att bestämmelsen bör utformas så att det i stället anges att tekniken får användas för utredning av ”brott för vilket fängelse i fyra år eller mer ingår i straffskalan”. Enligt *Polismyndigheten* finns det skäl att överväga att i lagtexten ange att även de osjälvständiga brottsformerna omfattas av möjligheten att använda tekniken för att utreda och lagföra brott.

Myndigheten för säkerhet och integritetsskydd ifrågasätter om den föreslagna bestämmelsen som möjliggör användning av tekniken i syfte att verkställa en straffrättslig påföljd bör vara så pass vidsträckt.

Skälen för regeringens förslag

Tekniken ska få användas om det är absolut nödvändigt för att lokalisera eller identifiera en person för vissa specifika syften

I avsnitt 6.1 föreslås att polisen ska få använda AI-system för ansiktsigenkänning i realtid. Av artikel 5 i AI-förordningen följer att tekniken får användas för vissa angivna syften och att medlemsstaterna i sin nationella rätt ska fastställa för vilka av dessa syften och inom vilka gränser tekniken får användas. Det behöver därför i den nya lagen anges under vilka förutsättningar som användningen ska få ske i Sverige. Som *Lagrådet* understryker behöver förutsättningarna för att använda tekniken utformas med tydlighet och precision för att motverka ett överutnyttjande av den.

Av artikel 5.1 h i AI-förordningen framgår att medlemsstaterna får föreskriva att AI-system för ansiktsigenkänning i realtid får användas för följande syften.

(i) Målinriktad sökning efter specifika offer för människorov, människohandel eller sexuellt utnyttjande av människor, samt sökning efter försvunna personer.

(ii) Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ett verkligt och aktuellt eller verkligt och förutsebart hot om en terroristattack.

(iii) Lokalisering eller identifiering av en person som misstänks ha begått ett brott, i syfte att genomföra en brottsutredning, lagföring eller ett verkställande av en straffrättslig påföljd för brott som avses i bilaga II och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år.

De brott som finns upptagna i bilaga II är bl.a. olaglig handel med vapen, ammunition, sprängämnen, narkotika och psykotropa ämnen, organiserad stöld eller väpnat rån, mord, grov misshandel, människohandel, olaga frihetsberövande och våldtäkt. Det kan konstateras att de brott som omfattas av förordningens undantag är allvarliga brott som kan motivera ett större ingrepp i den personliga integriteten.

Enligt artikel 5.2 i AI-förordningen får tekniken endast användas för att bekräfta identiteten på den person som särskilt avses. Vad detta innebär är

vid en läsning av artikeln för sig inte helt tydligt. Vid en jämförelse mellan artikeln och artikel 5.1 h står det emellertid klart att användningen som får tillåtas avser mer än bara ett fastslående av vilken identitet – dvs. namn, personnummer och liknande – en viss person har. Artikel 5.1 h punkten (iii) föreskriver att tekniken får användas för att lokalisera eller identifiera en person. Skulle artikel 5.2 förstås så snävt att det enbart handlar om användning för att fastslå en persons identitet skulle det innebära att användning för lokalisering, dvs. för att upptäcka var en person befinner sig, inte är tillåten och punkten (iii) i den delen sakna betydelse. Det skulle även innebära att en sökning efter en försvunnen person vars identitet är känd inte skulle få ske i syfte att lokalisera (och eventuellt rädda) denne. Det kan inte vara avsikten med bestämmelsen. I stället måste den förstås så att användningen måste vara begränsad till att lokalisera eller identifiera den person som avses. För att det inte ska råda några tvivel om hur tekniken får användas föreslås därför att det i lagtexten framgår att tekniken får användas för att lokalisera eller identifiera den person som särskilt avses med respektive punkt. *Lunds universitet* för fram att vissa uttryck i artikel 5.1 h som ”specifikt offer för…” inte framgår tydligt av förslaget. Exempelvis kan skrivningen om lokalisering och identifiering av ”en person som kan vara offer för” mycket väl, enligt universitetets mening, tolkas som en bestämmelse som avser en obestämd krets av personer som kan vara sådana offer. Enligt universitetet bör kravet på specificitet framgå direkt av lagen. Även bl.a. *Svea hovrätt* lyfter att AI-förordningen uppställer krav på att användningen ska avse en särskilt utpekad person. Regeringen delar den uppfattningen. Att det inte får röra sig om en obegränsad krets personer utan en eller flera specifika personer bör tydliggöras ytterligare i lagtexten.

Enligt artikel 5.1 h får användning av AI-system för ansiktsigenkänning i realtid endast ske om det är ”absolut nödvändigt” för något av de syften som anges i bestämmelsen. Bestämmelsen ger uttryck för att det krävs ingående bedömningar av om användningen verkligen är nödvändig. Begreppet ”absolut nödvändigt” är ett begrepp som i svensk lagstiftning framför allt används för personuppgiftsbehandling. I brottsdatalagen, som huvudsakligen genomförde dataskyddsdirektivet i svensk rätt, framgår att polisen får behandla biometriska uppgifter, förutsatt att behandlingen är absolut nödvändig för ändamålet med behandlingen (2 kap. 12 §). I promemorian konstateras att regleringen blir tillämplig på behandlingen av personuppgifter vid användning av tekniken. Mot den bakgrunden görs i promemorian bedömningen att det inte är lämpligt att låta motsvarande prövning ske av en tillståndsgivande myndighet. Det föreslås därför att begreppet ”synnerlig vikt” i stället används i den nya lagen.

Flera remissinstanser, däribland *Institutet för mänskliga rättigheter*, *Lunds universitet*, *Sveriges advokatsamfund* och *Centrum för rättvisa*, ifrågasätter att synnerlig vikt är ett lämpligt begrepp. De menar att det förhållandet att ett annat begrepp än absolut nödvändigt väljs skapar en otydlighet i lagstiftningen och det finns en risk att viss praxis kan utveckla sig grundat på tolkningen av den svenska regleringens skrivningar som skiljer sig från EU-domstolens tolkning av artikel 5.1 h. *Eskilstuna tingsrätt* och Centrum för rättvisa anser att uttrycket absolut nödvändigt i stället bör användas, och tillsammans med *Civil Rights Defenders* och

Journalistförbundet framhålls att begreppet synnerlig vikt innebär ett inte obetydligt lägre krav.

I skäl 38 till AI-förordningen anges att användningen av ansiktsigenkänning i realtid med nödvändighet involverar behandling av biometriska uppgifter och att reglerna i förordningen som baseras på artikel 16 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), bör tillämpas som *lex specialis* med avseende på de regler om behandling av biometriska uppgifter som anges i artikel 10 i dataskyddsdirektivet. De reglerar därmed sådan användning och behandling av berörda biometriska uppgifter på ett uttömmande sätt. I skäl 38 anges vidare att sådan användning därför bör vara möjlig endast i den utsträckning som den är förenlig med den ram som fastställs i förordningen, utan att myndigheter som agerar för brottsbekämpande ändamål har något utrymme att använda systemen utanför den ramen. Samtidigt är dataskyddsdirektivet tillämpligt på personuppgifter som behandlas i samband med de rättigheter och skyldigheter som fastställs i AI-förordningen (artikel 2.7 i AI-förordningen). Det innebär alltså att det även måste göras en prövning utifrån tillämplig dataskyddsreglering.

Med hänsyn till den dataskyddsaspekt som ändå ligger i prövningen (jfr skäl 38) anser regeringen att det inte finns något hinder mot att tillståndsprövande myndighet prövar frågan om tillstånd utifrån ett krav på att användningen av tekniken ska vara absolut nödvändig. Att använda samma begrepp i den nationella regleringen som i förordningen kan bidra till en tydligare koppling mellan de två regelverken och därigenom minska risken för tillämpningsproblem. Regeringen anser förvisso att begreppet synnerlig vikt i detta sammanhang i princip motsvarar begreppet absolut nödvändigt men mot ovan angivna bakgrund bör begreppet absolut nödvändigt användas. Det bör alltså i den nya lagen anges att tekniken får användas om det är absolut nödvändigt för att lokalisera eller identifiera en person. För att lyfta fram betydelsen av regeln bör den placeras tillsammans med de grundläggande bestämmelserna om för vilka syften tekniken ska få användas.

Kravet på att användningen måste vara absolut nödvändig innebär att behovet av användningen måste vara kvalificerat på något sätt för att tekniken ska få användas. Behovet ska vara kopplat till att lokalisera eller identifiera en person för något av de syften som tekniken föreslås få användas för. Genom bestämmelsen tydliggörs att tekniken ska användas med restriktivitet, vilket också *Lagrådet* understryker vikten av. Det innebär att polisen inte regelmässigt får använda den och att det måste finnas omständigheter som visar att ett ärende kan föras framåt genom att använda tekniken (jfr prop. 2017/18:232 s. 152 f.). Det ska alltså finnas skäl att räkna med att användningen av tekniken – ensam eller tillsammans med andra åtgärder – kan leda till att den som söks anträffas eller identifieras. Som utgångspunkt får tekniken endast användas när andra möjligheter att lokalisera eller identifiera den som söks har uttömts eller att sådana åtgärder skulle vara utsiktslösa eller medföra en orimligt stor arbetsinsats. Om andra åtgärder är möjliga för att lokalisera eller identifiera den som söks bör det dock ändå vara tillåtet att använda tekniken om alternativen skulle innebära att den som söks inte kan hittas eller identifieras tillräckligt skyndsamt. Se också avsnitt 7.2 där det föreslås att tekniken endast får användas om det är proportionerligt.

Tekniken ska få användas för att hitta vissa brottsoffer och försvunna personer som misstänks vara utsatta för brott

Enligt punkt (i) i artikel 5.1 h i AI-förordningen får användning av AI-system för ansiktsigenkänning i realtid tillåtas för målinriktad sökning efter specifika offer för människorov, människohandel eller sexuellt utnyttjande av människor, samt sökning efter försvunna personer.

Det får anses något oklart vilka brott som omfattas av uttrycket sexuellt utnyttjande av människor som anges i den svenska språkversionen. I den engelska versionen anges ”the targeted search for specific victims of abduction, trafficking in human beings or sexual exploitation of human beings, as well as the search for missing persons”. Till skillnad från den svenska texten tar den engelska mer tydligt sikte på när människor utnyttjas för sexuella ändamål inom ramen för människohandel. Mot den bakgrunden och med beaktande av att punkt (i) är avsedd att möjliggöra att tekniken används för att hitta personer som är försvunna på grund av att de har utsatts för ett brott bör utgångspunkten vara att enbart gärningar som innefattar ett exploaterings- eller bortförandemoment omfattas. I svensk rätt inryms människohandel som sker för sexuella ändamål i brottet människohandel. Även om den svenska versionen ger visst utrymme för att använda tekniken för andra brott som innebär sexuellt utnyttjande bör, mot bakgrund av syftet med punkten (i), sådana brott inte omfattas av den föreslagna bestämmelsen. I svensk rätt är människorov och människohandel kriminaliserat genom 4 kap. 1 och 1 a §§ brottsbalken. Brottet människorov innefattar att en person berövas sin frihet. För människohandel döms den som, i annat fall genom exempelvis olaga tvång eller vilseledande, bl.a. rekryterar eller inhyser någon annan i syfte att exploatera personen för vissa särskilda ändamål, inklusive för sexuella ändamål. Dessa brott bedöms därmed kunna omfattas av de gärningar som punkten (i) möjliggör att tekniken används för. I promemorian föreslås att även människoexploatering enligt 4 kap. 1 b § brottsbalken omfattas. *Svea hovrätt* och *Lunds universitet* menar att brottet människoexploatering inte bör ingå bland de uppräknade brotten eftersom människoexploatering är ett mindre allvarligt brott än övriga. För människoexploatering döms den som, i annat fall än som avses i 4 kap. 1 eller 1 a §, genom olaga tvång, vilseledande eller utnyttjande av någons beroendeställning, skyddslöshet eller svåra situation, exploaterar en person i tvångsarbete, arbete under uppenbart orimliga villkor eller tiggeri. Regeringen anser att människoexploatering, med fängelse fyra år i straffskalan, är ett allvarligt brott. Brottet bör därför ingå bland de uppräknade brotten. Med hänsyn till formuleringen av AI-förordningen bör tillämpningsområdet dock snävas av så att det enbart omfattar exploatering som avser sexuella tjänster.

Enligt *Lagrådet* ligger det närmast till hands att uppfatta att artikel 5.1 h (i) syftar till att göra det möjligt att hitta personer som utsätts för brott för att kunna avvärja och stoppa pågående brott. Enligt Lagrådet är det tveksamt om bestämmelsen omfattar användning för att söka efter personer som har utsatts för brott i syfte att kunna lagföra dem som gjort sig skyldiga till brottet. Regeringen delar Lagrådets uppfattning att användningen bör begränsas till att söka efter personer som misstänks vara utsatta för brott. Det är rimligt att användningen av AI i realtid i detta avseende endast används för att hitta människor i syfte att avbryta det brott

de utsätts för. Det är inte alltid möjligt att veta om brottet alltjämt pågår förrän målsäganden lokaliserats men grunden för användningen är en misstanke om att personen utsätts för brott. Det kan i och för sig i vissa fall finnas behov av att hitta en målsägande även i ett senare skede, under förundersökning, men med hänsyn till hur ingripande användningen av AI i realtid ändå är och då restriktivitet bör prägla regleringen framstår det inte som motiverat att använda tekniken i detta syfte.

För att få använda tekniken krävs inte att personen är försvunnen på så vis att någon har anmält att personen är saknad. Det kan finnas situationer där polisen har information om att en person misstänks vara utsatt för människohandel, men ingen har anmält att personen är försvunnen. I dessa fall bör tekniken kunna användas med stöd av den föreslagna regleringen.

Vad gäller möjligheten att använda tekniken för att söka efter försvunna personer måste förordningen förstås så att det gäller de fall då försvinnandet misstänks ha sin grund i ett brott. Detta följer av att artikel 5.1 h i AI-förordningen endast gäller för brottsbekämpande ändamål. Till skillnad från det som gäller för sökning av personer som misstänks vara utsatta för brotten som nämns ovan gäller att personen måste vara försvunnen, vilket normalt bör innebära att personen har anmälts saknad. Som anförs ovan bör användningen begränsas till att söka efter personer som misstänks vara utsatta för brott.

Användning av tekniken för att lokalisera eller identifiera försvunna personer som inte misstänks vara utsatta för brott omfattas inte av artikel 5.1 h i förordningen. Den nya lagen bör därför inte, vilket *Lunds universitet* föreslår, gälla för att identifiera och lokalisera sådana. I vilken mån användningen av AI-system för ansiktsigenkänning i realtid kan användas för att söka efter personer som inte misstänks vara utsatta för brott får avgöras utifrån övriga bestämmelser i AI-förordningen och det dataskyddsrättsliga regelverket.

Varje år försvinner det ett antal personer på grund av att de misstänks vara utsatta för brott. Det handlar bl.a. om sexualbrott, barnäktenskapsbrott eller äktenskapstvång. Enligt Polismyndigheten är det i dessa fall av synnerlig vikt att kunna lokalisera de försvunna personerna så snart som möjligt. Vid exempelvis ett sexualbrott har polisen vanligen en referensbild av brottsoffret att utgå ifrån, oavsett om brottsoffrets identitet är känd eller okänd. Bilden kan finnas i en förundersökning eller ha utverkats ur kamerabevakningsmaterial. En möjlig användning av AI-system för ansiktsigenkänning i realtid i dessa ärenden förutses innebära betydligt bättre förutsättningar för polisen att hitta de försvunna personerna.

Det är viktigt att polisen ska ha så goda förutsättningar som möjligt att på ett snabbt och effektivt sätt kunna hitta, och kanske även förhindra ett pågående allvarligt brott. *Myndigheten för säkerhet och integritetsskydd* anser att det bör övervägas om det bör införas ett kvalifikationskrav på de brott som kan aktualiseras. Enligt myndigheten skulle en sådan reglering bättre svara mot polisens behov, medan den i promemorian föreslagna formuleringen innebär att tekniken skulle få användas även vid misstanke om att någon har utsatts för även ett bötesbrott. Regeringen konstaterar att de brott som anges ovan endast är exempel på sådana brott där det finns ett behov av att använda tekniken. Regeringen anser att en ordning där den tillståndsprövande myndigheten kan göra en välgrundad bedömning utifrån omständigheterna i det enskilda fallet av om det finns tillräckligt

starka skäl för en användning av tekniken är att föredra framför en brottskatalog i lag. Vid den proportionalitetsbedömning som då görs bör brottets allvar beaktas (se vidare avsnitt 7.2). Något uttryckligt kvalifikationskrav, så som Myndigheten för säkerhet och integritetsskydd föreslår, bör därför inte införas.

Att tillåta användning av AI-system för ansiktsigenkänning i realtid för detta ändamål bedöms proportionerligt i förhållande till den påverkan som den kan ha på rätten till privatliv och skyddet för den personliga integriteten (se vidare avsnitt 15.2). Mot den bakgrunden anser regeringen att polisen bör ges möjlighet att använda AI-system för ansiktsigenkänning i realtid för de syften som punkt (i) i förordningen tillåter. Det bör i den nya lagen alltså föreskrivas att AI-system för ansiktsigenkänning i realtid ska kunna användas för att lokalisera eller identifiera en person som misstänks vara utsatt för människorov eller människohandel eller för människoexploatering om den avser sexuella tjänster, eller en person som är försvunnen och som misstänks vara utsatt för brott. Det får anses vara förenligt med förordningen att tekniken får användas utan att det är klarlagt att den person som avses är utsatt för brott, eftersom det inte i alla situationer går att veta om en person är utsatt för ett brott innan personen har hittats. Det bör därför räcka att det kan misstänkas att personen utsätts för brott. En tillämpning av bestämmelsen bör inte förutsätta att en förundersökning har inletts.

Lunds universitet påpekar att bl.a. människohandel är brottslighet som många gånger innebär att offret tvingats begå brott som ett led i exploateringen. Universitetet anser att frågan om hur den data som samlats in, men inte har samband med det brott som föranlett användningen av AI-tekniken, ska få användas borde ha behandlats och ser en risk för att tekniken kan användas för att identifiera personer som begått bagatellartad brottslighet men som samtidigt är potentiella offer. Regeringen konstaterar att förslaget i denna del innebär att tekniken får användas endast för att lokalisera eller identifiera ett misstänkt brottsoffer och att användningen av tekniken inte i sig genererar någon ny form av överskottsinformation som inte redan i dag kan framkomma när polisen letar efter brottsoffer. Har t.ex. det material som AI-systemet används på tillkommit genom hemlig kameraövervakning regleras det i rättegångsbalken om hur eventuell överskottsinformation får användas. Mot den bakgrunden ser regeringen varken någon risk för kringgående av kraven för användning vid sökning efter brottsmisstänkta eller något behov av särskild reglering av eventuell överskottsinformation.

Det kan tänkas förekomma situationer där polisen genom att lokalisera en misstänkt gärningsperson, i de fall det finns en bild på denne men det saknas bilder på brottsoffret, även kan lokalisera och i förlängningen förhindra ett pågående brott. Sådana situationer skulle kunna förekomma i exempelvis ärenden om gränsöverskridande människohandel. Eftersom artikel 5.1 h (i) kräver att det ska vara fråga om en målinriktad sökning efter specifika offer ger den emellertid inte stöd för en sådan indirekt sökning av brottsoffer. Möjligheten att kunna använda tekniken i en sådan situation får i stället prövas utifrån förutsättningarna att använda tekniken på en misstänkt gärningsman enligt artikel 5.1 h (iii), se nedan.

Punkt (ii) i artikel 5.1 h i AI-förordningen möjliggör användning av AI-system för ansiktsigenkänning i realtid för att förhindra ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ett verkligt och aktuellt eller verkligt och förutsebart hot om en terroristattack.

Enligt Polismyndigheten finns det ärenden då det via underrättelse-uppslag, konkreta tips eller information inhämtad exempelvis genom preventiva tvångsmedel finns starka indikationer på att det planeras för ett sådant allvarligt brott som undantaget i punkt (ii) omfattar. I dessa ärenden finns det ibland information om var brottet kommer att ske eller mot vem hotet riktas. AI-system för ansiktsigenkänning i realtid kan då användas för att lokalisera en misstänkt gärningsperson i tid för att avvärja brottet. En annan situation kan vara att polisen har information om att en person, som befinner sig utanför Sverige, har långtgående planer på att begå ett allvarligt brott i Sverige. Om myndigheten har tillgång till en bild på personen kan realtidsidentifiering vara avgörande för att få information om när personen passerar svenska gränsen eller för att hitta personen om denne redan tagit sig in i landet och förhindra att brottet fullbordas.

Det är viktigt att polisen har tillgång till verktyg för att snabbt och effektivt kunna agera när det finns information om att mycket allvarlig brottslighet kan komma att begås. I en sådan situation kan tekniken utgöra ett kraftfullt och ibland avgörande verktyg för att kunna förhindra att brottet inträffar. Betydelsen av att förhindra allvarlig brottslighet mot fysiska personers liv eller säkerhet väger tungt och det är lämpligt och bedöms proportionerligt att polisen får använda tekniken för detta syfte i förhållande till de risker för den personliga integriteten och privatlivet som åtgärden kan innebära för de personer som berörs av den (se vidare avsnitt 15.2). Det bör därför införas en bestämmelse i den nya lagen som möjliggör för polisen att använda tekniken i sådana situationer som omfattas av artikel 5.1 h (ii).

För att användning av AI-system för ansiktsigenkänning i realtid ska få tillåtas krävs enligt punkt (ii) att det är fråga om ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ett aktuellt eller förutsebart och verkligt hot om en terroristattack. I promemorian görs bedömningen att detta innebär att det finns en påtaglig risk för att en person kommer att begå brott mot människors liv eller säkerhet. *Hovrätten över Skåne och Blekinge* påpekar att begreppet påtaglig risk inte fullt ut motsvarar AI-förordningens krav på specifikt, betydande och överhängande hot. Liknande synpunkter för även *Malmö tingsrätt*, *Eskilstuna tingsrätt*, *Lunds universitet*, *Integritetsskydds-myndigheten*, *Domstolsverket* och *Centrum för rättvisa* m.fl. fram. Av kommissionens riktlinjer framgår att ett överhängande hot mot liv eller fysisk säkerhet är ett hot som kan uppstå när som helst och som kräver att omedelbara åtgärder måste vidtas. Den beskrivningen bör jämföras med hur uttrycket påtaglig risk används i svensk rätt. I förarbetena till 1 § lagen (2024:1180) om anonyma vittnen i brottmål anges att en risk som är påtaglig ger uttryck för att risken ska vara tydlig och ligga nära till hands. Tidsmässigt behöver det inte innebära att brottsligheten förväntas de närmsta dagarna eller veckorna utan det kan röra sig om en längre period

(prop. 2024/25:20 s. 71). Riktlinjerna är visserligen inte bindande utan syftar till att ge insikter i kommissionens tolkning av förbuden i artikel 5 i AI-förordningen för att säkerställa en konsekvent, effektiv och enhetlig tillämpning av dem (punkten 4 i riktlinjerna). Vad kommissionen där ger uttryck för framstår dock som en rimlig tolkning och regeringen anser därför att begreppet påtaglig risk inte bör användas i den nya lagen.

Några remissinstanser, däribland Hovrätten över Skåne och Blekinge och Centrum för rättvisa, anser att det bör övervägas om begreppet överhängande bör användas för att närmare motsvara AI-förordningens krav. Begreppet överhängande förekommer i andra svenska författningar. Att använda samma begrepp i den nationella regleringen som i förordningen bidrar till en tydligare koppling mellan de två regelverken vilket minskar risken för tillämpningsproblem. Regeringen anser därför, i linje med remissinstanserna, att begreppet överhängande bör användas. Den närmare innebörden av begreppet bör överlämnas till rättstillämpningen och ytterst EU-domstolen att utveckla närmare praxis kring.

AI-förordningen ställer också krav på att hotet ska vara specifikt. Som *Centrum för rättvisa* påtalar innebär det en kvalificering av riskens konkretion. I kommissionens riktlinjer anges att ett specifikt hot innebär att hotet är tydligt definierat, individualiserat och konkret, i betydelsen att det inte bör vara hypotetiskt eller avse vissa faror i allmänhet. Regeringen anser, i likhet med *Integritetsskyddsmyndigheten*, att hotet eller faran bör vara konkret för att användningen ska tillåtas. Har faran i ett visst fall faktiskt varit utesluten har någon konkret fara inte förelegat. Regeringen anser dock, i motsats till *Lagrådet*, att detta inte behöver anges uttryckligen i lagen (jfr bl.a. 3 kap. 9 § brottsbalken).

Vad gäller uttrycket ”betydande…hot” i AI-förordningen påtalar *Centrum för rättvisa* att det innebär en kvalificering av riskens allvar och *Hovrätten över Skåne och Blekinge* hänvisar till kommissionens riktlinjer. Där framgår att ett betydande hot mot den fysiska säkerheten har att göra med allvarligare kroppsskador. Hovrätten anser att promemorians förslag däremot ger intryck av att omfatta även mindre allvarliga brott mot människors liv eller säkerhet. Även *Domstolsverket* och *Justitiekanslern* för fram liknande synpunkter. Regeringen delar uppfattningen att regleringen bör innehålla en kvalificering av hotets allvar. Det finns dock inte stöd i förordningen för att det måste vara fråga om brott som leder till allvarliga kroppsskador. För att bestämmelsen ska vara förenlig med AI-förordningen menar *Lagrådet* att det i lagtexten måste förtydligas att bestämmelsen är tillämplig enbart om det i det konkreta fallet finns ett betydande hot. Enligt regeringens uppfattning kan uttrycket betydande i detta sammanhang anses motsvara ett krav på att det ska handla om ett allvarligt brott. Det innebär därför inte, som Lagrådet gör gällande, ett vidare tillämpningsområde än vad förordningen medger. I enlighet med vad som föreslås i lagrådsremissen anser regeringen att det bör uppställas ett krav på att det ska röra sig om ett allvarligt brott mot människors liv eller säkerhet. Ett sådant förtydligande framstår som lämpligare än en uppräkning av vissa brott som Hovrätten över Skåne och Blekinge och *Journalistförbundet* förordar.

En precisering till allvarligt brott förekommer i flera svenska författningar. Det synsätt som framkommer i förarbetena till dessa gör sig gällande även här (se t.ex. prop. 2009/10:147 s. 14 f. och 41 f. och prop.

2024/25:12 s. 24 och 59 f.). En utgångspunkt för bedömningen av om det är fråga ett allvarligt brott är då att det rör sig om ett konkret brott med ett straffvärde motsvarande minst fängelse i sex månader. Även andra omständigheter än straffvärdet kan dock vara relevanta att beakta vid bedömningen. Exempel på brottslighet som omfattas är mord och grov misshandel.

Artikel 5.1 h (ii) i AI-förordningen avser användning av AI-tekniken i syfte att förhindra ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet. *Lagrådet* noterar att den i lagrådsremissen föreslagna lagtexten inte innehåller ett krav på ”fysisk” säkerhet. Enligt Lagrådet ger därmed den föreslagna lagtexten ett vidare tillämpningsområde för användningen av tekniken än vad som är tillåtet enligt AI-förordningen. Att använda samma begrepp i den nationella regleringen som i förordningen kan bidra till en tydligare koppling mellan de två regelverken och därigenom minska risken för tillämpningsproblem. Mot den bakgrunden delar regeringen Lagrådets uppfattning att uttrycket fysisk säkerhet bör användas i lagtexten.

Lagrådet pekar på att AI-förordningen anger att det ska finnas ett hot mot personers liv eller säkerhet och det är enligt Lagrådet då inte tillräckligt att det finns en risk att en person begår en gärning som omfattas av en brottstyp som kan innefatta angrepp på annans liv och säkerhet. Regeringen noterar i sammanhanget skäl 33 i förordningen som klargör att ett överhängande hot mot fysiska personers liv eller fysiska säkerhet kan inbegripa ett hot mot kritisk infrastruktur om en driftstörning vid eller förstörelse av sådan kritisk infrastruktur skulle leda till en omedelbar fara för en persons liv eller fysiska säkerhet, inbegripet genom allvarlig skada på tillhandahållandet av basförnödenheter till befolkningen eller på utövandet av statens kärnfunktion. Förordningen ger alltså utrymme för att tekniken får användas när det finns en risk för ett allvarligt brott som innebär fara för en enskilds liv eller fysiska säkerhet och att det är tillräckligt att brottet innebär att en sådan fara uppstår. Som *Lagrådet* uppmärksammar är samtidigt lagrådsremissens lagförslag så formulerat att vissa farebrott riskerar att falla utanför, och detta bör åtgärdas. Även brott som t.ex. allmänfarlig ödeläggelse, mordbrand och sabotage bör omfattas (jfr 4 b kap. 1 § lagen [2017:496] om internationellt polisiärt samarbete och prop. 2024/25:12 s. 59 f. där motsvarande fråga uppmärksammas). Det innebär att det går att använda tekniken för att förhindra sådana brott som ökat de senaste åren, bl.a. sprängningar i gängmiljön. Även följder av en allvarlig driftsstörning som orsakats av exempelvis sabotage av kritisk infrastruktur kan omfattas (se skäl 33 i AI-förordningen). Som *Lagrådet* påpekar räcker det med att en enda persons liv eller fysiska säkerhet är i fara för att tekniken ska få användas. Lagtexten bör tydliggöras i detta avseende.

Hovrätten över Skåne och Blekinge lyfter att förslaget i promemorian inte fullt ut nyttjar möjligheten för användning av AI-system i syfte att förhindra terroristattacker. Liknande synpunkter förs också fram av *Eskilstuna tingsrätt* och *Sveriges Domareförbund*. Regeringen konstaterar att Säkerhetspolisens användning av AI-system för nationell säkerhet inte omfattas av den föreslagna lagen (se avsnitt 6.2) och att Säkerhetspolisens möjligheter att använda tekniken vid hot om en terroristattack i stället får avgöras utifrån den reglering som gäller för myndighetens personuppgifts-

behandling (jfr prop. 2018/19:163 s. 48 f.). Detsamma gäller när Polismyndigheten har övertagit en arbetsuppgift som rör terrorbrott från Säkerhetspolisen (se 1 kap. 4 § första stycket brottsdatalagen). Det är därför inte motiverat att på det sätt som görs i förordningen införa en reglering i den nya lagen som särskilt gäller terroristbrott.

Slutligen anför *Hovrätten över Skåne och Blekinge* att användningen av tekniken enligt artikel 5.1 h (ii), till skillnad från punkterna (i) och (iii), inte förutsätter ett syfte att lokalisera eller identifiera en viss person. Som konstateras ovan bör dock artikel 5.2 i AI-förordningen förstås så att användningen måste vara begränsad till att lokalisera eller identifiera den person som avses, oavsett vilken punkt i artikel 5.1 h som är tillämplig.

Användningen bör kunna tillåtas när det finns uppgifter om ett brott, oavsett om det är under eller utanför en förundersökning.

Tekniken ska få användas för att utreda, lagföra eller verkställa straffrättslig påföljd för vissa allvarliga brott

Enligt punkt (iii) i artikel 5.1 h i AI-förordningen får användning av AI-system för ansiktsigenkänning i realtid tillåtas för att lokalisera eller identifiera en person som misstänks ha begått ett brott, i syfte att utreda, lagföra eller verkställa en straffrättslig påföljd för brott som avses i bilaga II och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år. De brott som finns upptagna i bilagan är bl.a. olaglig handel med vapen, ammunition, sprängämnen, narkotika och psykotropa ämnen, organiserad stöld, väpnat rån, mord, grov misshandel, människohandel, olaga frihetsberövande och våldtäkt.

Mot bakgrund av den omfattande grova brottslighet som finns i Sverige kan det förutses att det kan bli aktuellt för polisen att använda AI-system för ansiktsigenkänning i realtid för ett syfte som punkt (iii) tillåter i ett flertal ärenden. Genom underrättelseinformation eller annan information som inhämtats eller inkommit till polisen finns det i sådana ärenden ofta skäl att anta att en misstänkt person kommer att befinna sig i ett visst område vid en viss tidpunkt. Om den misstänkta personen befinner sig på en plats med större folksamlingar t.ex. i ett köpcentrum, under en festival, en allmän sammankomst eller offentlig tillställning kan det vara svårt att manuellt identifiera personen. Det kan i dessa situationer finnas en risk för att polisen röjer sig genom att i det öppna patrullera på platsen. I sådana fall skulle AI-system för ansiktsigenkänning i realtid kunna användas för att lokalisera och gripa personen.

Det finns också flera eftersökta personer som är misstänkta, åtalade eller dömda för allvarliga brott och som aktivt håller sig undan, där det finns indikationer på att personen gömmer sig på en specifik ort eller ska ha setts på en viss plats. Användning av AI-system för ansiktsigenkänning i realtid skulle kunna användas som komplement till polisens fysiska spaning och därmed öka möjligheten att med framgång lokalisera de eftersökta personerna.

Brottsutvecklingen i Sverige är sådan att antalet skjutningar med dödlig utgång har ökat de senaste åren. Dessa har inte sällan kopplingar till gängkriminalitet och drabbar även personer utanför den kriminella miljön. Det är viktigt att vända på denna brottsutveckling. En förutsättning för att

kunna göra det på ett framgångsrikt sätt är att polisen har tillgång till effektiva verktyg och kan agera på den information som finns i en utredning. Det är naturligt att polisen inte alltid kan finnas på plats när ett brott begås. Det finns i dag kameror på många ställen runt om i landet som polisen ofta använder sig av i sitt arbete. För att effektivisera polisens arbete ska polisens egna kameror dessutom bli fler. Polisens arbete skulle kunna effektiviseras ytterligare om kamerorna fick användas med AI-system för ansiktsigenkänning i realtid. Användning av tekniken skulle öka möjligheten att med framgång identifiera, lokalisera och gripa misstänkta eller dömda personer.

Att en person som misstänks för sådana brott som omfattas av artikel 5.1 h punkt (iii) snabbt kan lokaliseras eller identifieras är angeläget, särskilt om personen är farlig, t.ex. om han eller hon är våldsbenägen, riskerar att fortsätta att begå brott eller lämna landet och för att kunna lagföra personen. Det är vidare av grundläggande betydelse för allmänhetens förtroende för rättsväsendet att påbörjade lagföringar kan slutföras samt att utdömda påföljder verkställs. Det bedöms därför finnas ett behov för polisen att kunna använda AI-system för ansiktsigenkänning i realtid för att lokalisera eller identifiera en person som misstänks ha begått ett sådant brott som upptas i bilaga II till AI-förordningen och som kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år, i syfte att genomföra en brottsutredning eller lagföra denne. Detsamma gäller för att lokalisera eller identifiera en dömd person i syfte att verkställa straffrättslig påföljd för sådana brott. I uttrycket straffrättsliga påföljder ingår även andra påföljder än fängelse, såsom skyddstillsyn, samhällstjänst och rättspsykiatrisk vård. De brott som undantaget tillåter att tekniken används för att utreda, lagföra och verkställa straffrättslig påföljd för är sådana brott som kan motivera ett ingrepp i den personliga integriteten (se vidare avsnitt 15.2).

Det föreslås således att det införs en bestämmelse i den nya lagen som möjliggör för polisen att använda AI-system för ansiktsigenkänning i realtid för att utreda, lagföra och verkställa straffrättslig påföljd för sådana brott som artikel 5.1 h punkt (iii) tillåter.

Av punkt (iii) framgår att tekniken får användas för att lokalisera eller identifiera en person som ”misstänks” för ett sådant brott som avses i bilaga II. I svensk rätt förekommer olika grader av misstanke för användning av tvångsmedel, från den lägsta ”anledning att anta” till ”kan antas”, ”kan misstänkas”, ”skäligen misstänkt” (eller ”skäligen kan misstänkas”) och ”sannolika skäl”. Frågan är vilken grad av misstanke som ska krävas för att tekniken ska få användas. Flera remissinstanser, bl.a. *Integritetsskyddsmyndigheten*, *Myndigheten för säkerhet och integritetsskydd* och *Centrum för rättvisa* menar att den av promemorian föreslagna misstankegraden ”kan misstänkas” är lägre än vad som krävs enligt AI-förordningen för att få använda tekniken i syfte att utreda brott. Av kommissionens riktlinjer framgår att en misstänkt är en person för vilken det finns starka skäl att tro att han eller hon har begått ett straffrättsligt brott, och att tillräckliga bevis för den personens inblandning i brottet redan har samlats in. Uttrycket kan misstänkas förekommer bl.a. i 23 kap. 9 § första stycket rättegångsbalken. Den graden av misstanke krävs enligt bestämmelsen för att kunna hålla kvar någon för förhör längre än sex timmar. Samma grad av misstanke gäller för en särskild form av kroppsbesiktning,

ögonundersökning. Uttrycket kan misstänkas anses omfatta fall där det rör sig om relativt svag bevisning mot den misstänkte och regeringen delar uppfattningen att det inte kan anses motsvara AI-förordningens krav på misstanke. I stället bör uttrycket skälig misstanke användas. Det är som *Svea hovrätt* påpekar ett beviskrav som gäller för de flesta tvångsmedel och innebär ett högre krav på misstankens styrka än ”kan misstänkas”. Allmänt brukar det för ”skälig misstanke” krävas att det finns konkreta omständigheter av en viss styrka som pekar på att den misstänkte har begått den gärning som misstanken avser.

I svensk rätt räknas som brott inte bara det fullbordade brottet utan också försök, förberedelse och stämpling till brott i den utsträckning sådant ansvar för det aktuella brottet är kriminaliserat genom ett särskilt straffstadgande. Straff för försök bestäms högst till vad som gäller för fullbordat brott och får inte sättas under fängelse, om lägsta straff för det fullbordade brottet är fängelse i två år eller däröver (23 kap. 1 § brottsbalken). Straffet för förberedelse eller stämpling ska bestämmas under den högsta och får sättas under den lägsta gräns som gäller för fullbordat brott. Högre straff än fängelse i två år får bestämmas endast om fängelse i sex år eller mer kan följa på det fullbordade brottet (23 kap. 2 § brottsbalken). För vissa av de brott som omfattas av bilaga II till AI-förordningen kan det alltså i svensk rätt följa fängelse i fyra år för försök, förberedelse och stämpling. Om dessa brott är straffbelagda på försök-, förberedelse-, eller stämplingsstadiet kan de omfattas av undantaget i artikel 5.1 h (iii) och den föreslagna bestämmelsen. Som *Polismyndigheten* för fram finns det skäl att uttryckligen i lagen ange att även dessa osjälvständiga brottsformer omfattas.

När det gäller *Tullverkets* och *Sveriges advokatsamfunds* synpunkt om att det bör förtydligas när tekniken kan användas i syfte att utreda och lagföra brott kan regeringen konstatera att inte minst med hänsyn till den misstankegrad som krävs blir det aktuellt att använda tekniken för att utreda brott under en förundersökning eller för att därefter lagföra brott.

Bestämmelsen bör innebära att tekniken får användas för att lokalisera eller identifiera personer som har anhållits eller häktats i sin frånvaro under en pågående brottsutredning, som har avvikit och inte inställer sig till förhandling eller som har dömts för sådant brott som omfattas av punkt (iii) men som inte har inställt sig till eller avvikit från verkställighet av straffet.

En särskild fråga att ta ställning till är om det i regleringen bör göras en hänvisning till bilaga II i AI-förordningen där de brott som avses i artikel 5.1 h räknas upp eller om det ska väljas en konstruktion där de svenska brott som motsvarar brotten i bilagan räknas upp.

I promemorian föreslås att det ska göras en hänvisning till bilaga II. En fördel med en hänvisning till bilagan, är att regleringen inte behöver ändras om det i den svenska lagstiftningen skulle införas nya brott med fyra års fängelse i straffskalan eller om straffskalan för vissa brott höjs. *Eskilstuna tingsrätt*, som invänder mot promemorians förslag menar att en ordning där bedömningen av om ett specifikt brott omfattas av lagens tillämpningsområde ska avgöras av den tillståndsprövande myndigheten framstår som olämplig ställt mot intresset av en enhetlig och förutsebar rättstillämpning. *Justitiekanslern*, *Åklagarmyndigheten*, *Sveriges advokatsamfund* och *Journalistförbundet* för fram liknande synpunkter och menar att

hänvisningen till bilagan saknar konkretion och att det kan finnas problem med förutsebarheten.

Ett alternativ som några av dessa remissinstanser förordar är en konstruktion där de svenska brott som motsvarar brotten i bilagan anges i lagen. Eskilstuna tingsrätt och Åklagarmyndigheten kan se fördelar med att en brottskatalog är tillgänglig i de brådskande situationer där användningen kan påbörjas utan tillstånd (se avsnitt 10) för att på så sätt minimera risken för otillåten användning. *Lagrådet* menar att en hänvisning till förordningens bilaga, som dessutom är dynamisk, är mindre väl förenlig med regeringsformens föreskrifter om att betydande intrång i den personliga integriteten ska beslutas av riksdagen och anser att det tydligt och direkt av lagen bör framgå vilka svenska brott eller typer av brott som omfattas.

Vissa brott som tas upp i bilagan har givna svenska motsvarigheter, bl.a. människorov, människohandel, mord, grov misshandel, olaga frihetsberövande, kapning, våldtäkt och grovt miljöbrott. Därutöver finns ett flertal svenska brott som kan omfattas av bilagan beroende på omständigheterna i det enskilda fallet. Som exempel kan nämnas brott enligt narkotikastrafflagen (1968:64) så som grovt narkotikabrott, grovt vapenbrott enligt vapenlagen (1996:67), brott enligt lagen (2010:1011) om brandfarliga och explosiva varor, brott enligt lagen (2000:1225) om straff för smuggling såsom grov vapensmuggling, eller grov narkotikasmuggling. En förutsättning för att dessa brott ska omfattas av bilagan är att det rör sig om handel med narkotika, vapen eller explosiv vara. Andra exempel på svenska brott som kan omfattas av bilagan beroende på omständigheterna i det enskilda fallet är vissa brott enligt brottsbalken som t.ex. grov stöld eller inbrottsstöld men då under förutsättning att det rör sig om organiserad stöld. Vidare kan nämnas rån eller grovt rån om det kan bedömas som väpnat.

Det kan konstateras att det är svårt att i flera fall göra en direkt översättning till svenska brott. Det är också en utmaning att säkerställa att alla svenska brott som kan omfattas också gör det samtidigt som det är angeläget att en svensk brottskatalog inte går utöver vad AI-förordningen tillåter. I åtskilliga fall omfattar ett angivet brott i bilagan flera brott i svensk rätt men som redovisas ovan är det i vissa fall så att bilagans brott endast avser ett svenskt brott i vissa fall. Genom att i bestämmelsen hänvisa till bilagan kan den tillståndsprövande myndigheten göra en välgrundad bedömning utifrån omständigheterna i det enskilda fallet av om det aktuella brottet eller brotten omfattas av bilagan.

Av 2 kap. 6 § andra stycket regeringsformen framgår att varje medborgare är skyddad gentemot det allmänna mot betydande intrång i den personliga integriteten Denna grundlagsfästa rättighet får dock under de förutsättningar som anges i 20 § i samma kapitel begränsas genom lag. En EU-förordning kan likställas med svensk lag. Det finns inte något generellt konstitutionellt hinder mot att man i en svensk lag hänvisar till det materiella innehållet i en EU-förordning (jfr NJA 2007 s. 227). För att säkerställa en korrekt tillämpning i förhållande till vad förordningen medger bör hänvisningen vara dynamisk. Hänvisningar till brottskataloger i bilagor finns redan i dag, förutom i direkt tillämpliga EU-rättsakter, i lagen (2018:1180) om flygpassageraruppgifter i brottsbekämpningen och lagen (2022:613) om finansiell information i brottsbekämpningen (jfr

prop. 2021/22:127 s. 34 och 105 samt prop. 2017/18:234 s. 39). Det är alltså en konstruktion som redan förekommer i svensk rätt. Den nya lagen ska tillämpas av polisen, åklagare och domstol, som alla har den kompetens som krävs för att avgöra om tekniken kan användas på ett specifikt brott i det enskilda fallet. Det kan också förutses att det tas fram riktlinjer om användningen.

Sammantaget delar regeringen inte Lagrådets synpunkter i denna del utan att anser, i motsats till bl.a. Eskilstuna tingsrätt, Justitiekanslern och Åklagarmyndigheten, att en hänvisning till bilagan är en lämpligare lösning än en uppräkning i lagen av vilka brott som avses.

För att kunna använda tekniken för ändamålet att utreda, lagföra eller verkställa straffrättslig påföljd för brott som avses i bilaga II krävs enligt förordningen att det aktuella brottet kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år. *Justitiekanslern* för fram att den i promemorian föreslagna lydelsen om att det för brottet ska vara föreskrivet fängelse i fyra år eller mer inte synes motsvara AI-förordningens lydelse som snarare indikerar ett föreskrivet ”minimistraff ” om fängelse i fyra år. Regeringen delar inte den bedömningen utan anser att AI-förordningen förutsätter att brottet ska vara straffbart med fängelse med ett maximistraff på minst fyra år, vilket också är vad kommissionens riktlinjer ger uttryck för (punkten 355) , liksom den engelska språkversionen där det anges ”for a maximum period of at least four years”. I promemorian föreslås att formuleringen ”för vilket det är föreskrivet fängelse i fyra år eller mer” används. Regeringen anser, i linje med *Tullverket*, att det finns skäl att förtydliga regleringen som därför bör formuleras ”för vilket det i straffskalan ingår fängelse i fyra år eller mer”.

Enligt *Lagrådet* bör övervägas att därutöver införa ett krav på att de aktuella gärningarna ska ha ett visst minsta straffvärde. Regeringen anser inte att det är motiverat och det vore dessutom förenat med betydande svårigheter att i det ofta tidiga skede som tekniken torde komma till användning bedöma straffvärdet för en viss gärning. I stället är det tillräckligt att brottets allvar beaktas inom ramen för den proportionalitetsbedömning som ska göras (se avsnitt 7.2).

Myndigheten för säkerhet och integritetsskydd noterar att förslaget i promemorian om att tekniken även ska få användas i syfte att verkställa en straffrättslig påföljd för sådana brott som anges i bilaga II inte har begränsats till frihetsberövande påföljder. Enligt myndigheten kan det ifrågasättas om det föreslagna tillämpningsområdet för bestämmelsen bör vara så vidsträckt. Regeringen ser emellertid inte skäl att begränsa förutsättningarna för att använda tekniken för ändamålet att verkställa straffrättslig påföljd på annat sätt än vad som gäller för användning i syfte att utreda och lagföra brott, dvs. genom hänvisning till vissa brott. Det bör framhållas att den utdömda påföljden naturligtvis måste beaktas inom ramen för den proportionalitetsbedömning som alltid ska göras innan tekniken används.

Mot denna bakgrund bör det i lagen föreskrivas att tekniken får användas för att lokalisera eller identifiera en person som skäligen kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet, eller som dömts för ett sådant brott, i syfte att verkställa den straffrättsliga påföljden.

7.2 Användningen måste vara proportionerlig

Regeringens förslag

AI-system för ansiktsigenkänning i realtid ska få användas endast om skälen för användningen uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Promemorians förslag

Förslaget i promemorian stämmer överens med regeringens.

Remissinstanserna

De flest av remissinstanserna tillstyrker förslagen eller invänder inte mot det. *Lunds universitet* understryker att användningen av tekniken innebär rättighetsinskränkningar för en stor mängd människor på ett påtagligt sätt vilket är en omständighet som kontinuerligt måste beaktas i bl.a. proportionalitetsbedömningen. *Sveriges advokatsamfund* anser att den föreslagna bestämmelsen om proportionalitet inte motsvarar vad som krävs enligt AI-förordningen. *Civil Rights Defenders* anser att promemorian saknar tillräcklig vägledning kring hur proportionalitetsbedömningen ska göras.

Skälen för regeringens förslag

En grundförutsättning för all användning av AI-system för ansiktsigenkänning i realtid är enligt AI-förordningen att den måste vara proportionerlig. Detta kommer till uttryck i artikel 5.2 a och b där det framgår att användning får ske för något av de syften som avses i artikel 5.1 h endast för att bekräfta identiteten på den individ som särskilt avses och att hänsyn ska tas till arten av den situation som ger upphov till den eventuella användningen, särskilt hur allvarlig, sannolik och omfattande skadan skulle bli om systemet inte används samt konsekvenserna av användningen av systemet för alla berörda personers rättigheter och friheter, särskilt vad gäller hur allvarliga, sannolika och omfattande dessa konsekvenser är. Bestämmelsen är i linje med regleringen i 2 kap. 21 § regeringsformen som slår fast att ett intrång i den enskildes personliga integritet aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den.

Att användning av AI-system för ansiktsigenkänning i realtid ska vara proportionerlig bör komma till uttryck i en bestämmelse i den nya lagen som gäller i alla led, både inför och under användningen. Bestämmelsen utformas lämpligen på det sätt som är vanligt i svensk rätt, dvs. användning av AI-system för ansiktsigenkänning i realtid får endast ske om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse. En sådan utformning innebär att det i varje enskilt fall ska göras en bedömning av om användningen står i rimlig proportion till det önskade målet vägt mot bl.a. det intrång som användningen kan innebära för den som åtgärden

riktar sig mot (jfr prop. 2022/23:126 s. 177). Vid avvägningen behöver samtliga relevanta omständigheter, inklusive de som framgår av artikel 5.2 a och b, beaktas. *Sveriges advokatsamfund* anser att den föreslagna bestämmelsen om proportionalitet inte motsvarar vad som krävs enligt AI-förordningen. Enligt samfundet hänvisar förordningen tydligt till den EU-rättsliga proportionalitetsbedömningen som kan sammanfattas med begreppen lämplighet, nödvändighet och proportionalitet i strikt mening. Regeringen konstaterar att det, utöver den föreslagna regleringen om proportionalitet, ställs tydliga krav på i vilka syften tekniken får användas. Detta ska även framgå av beslutet (se avsnitt 9.3). Det ställs också krav på att tekniken endast får användas om det är absolut nödvändigt (se avsnitt 7.1). Tillståndet får inte heller vara mer omfattande än vad som är absolut nödvändigt (se avsnitt 9.3).

Sammantaget anser regeringen att den föreslagna regleringen i sin helhet motsvarar de krav på proportionalitetsbedömning som ställs i AI-förordningen. Se också avsnitt 7.1 där det föreslås att tekniken endast får användas om det är absolut nödvändigt.

Lunds universitet understryker att användningen av tekniken innebär rättighetsinskränkningar för en stor mängd människor på ett påtagligt sätt vilket är en omständighet som kontinuerligt måste beaktas i bl.a. proportionalitetsbedömningen. Enligt *Civil Rights Defenders* behövs vägledning kring hur proportionalitetsbedömningen ska göras. Det krävs t.ex. att det preciseras vilka intressen som ska beaktas, hur dessa ska vägas mot varandra och hur tungt varje aspekt ska väga. Regeringen anser, i linje med vad remissinstanserna framhåller, att det inom ramen för proportionalitetsbedömningen bör beaktas att åtgärden kan påverka andra än den eftersökte. Vidare bör vid bedömningen exempelvis brottets allvar, och i förekommande fall den utdömda påföljden, beaktas. Även typen av biometrisk fjärridentifiering som ska användas i det enskilda fallet, t.ex. ansikts-, röst- eller rörelseigenkänning, kan ha betydelse för proportionalitetsbedömningen. Att i förarbetena lämna en närmare vägledning för hur avvägningen mellan de olika intressena bör göras i alla de situationer av olika slag som kan uppkomma i rättstillämpningen är inte möjligt. Bedömningen av vad som utgör en proportionerlig användning av tekniken i det enskilda fallet får överlämnas till rättstillämpningen.

8 Det ska krävas tillstånd

Regeringens förslag

Åklagare ska pröva frågan om tillstånd att använda AI-system för ansiktsigenkänning i realtid för att förbygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd. Frågan ska prövas efter ansökan av Polismyndigheten eller Säkerhetspolisen.

Allmän domstol ska pröva frågan om tillstånd att använda tekniken för att utreda eller lagföra brott. Frågan ska tas upp på ansökan av åklagare.

En ansökan om ett tillstånd att använda tekniken för att utreda och lagföra brott ska prövas av den tingsrätt som är behörig enligt rättegångsbalkens regler om rättegång i brottmål. Om åtal har väckts ska ansökan prövas av den domstol där åtalet har väckts.

Promemorians förslag

Förslaget i promemorian stämmer delvis överens med regeringens. I promemorian föreslås att allmän domstol ska pröva frågan om tillstånd att använda tekniken för att verkställa straffrättslig påföljd.

Remissinstanserna

Ingen remissinstans invänder mot förslaget om att det ska krävas tillstånd för polisen att använda AI-system för ansiktsigenkänning i realtid.

Vad gäller frågan om vilken myndighet som ska besluta om tillståndet är remissutfallet blandat. *Säkerhetspolisen* anser att förslaget om att domstol ska vara tillståndsmyndighet framstår som oproportionerligt i förhållande till det intrång i den enskildes personliga integritet som det i praktiken handlar om. Enligt *Svea hovrätt* är uppdelningen mellan vilka tillstånd som ska begäras hos åklagare respektive i domstol väl avvägd. Hovrätten anser dock att det kan finnas skäl att i bestämmelserna om tillståndsmyndighet direkt hänvisa till de tillåtna syftena för användningen. *Lunds universitet* har ingen invändning mot ett delat tillståndsförfarande.

Institutet för mänskliga rättigheter, *Centrum för rättvisa* och *Civil Rights Defenders* är positiva till att domstol är tillståndsmyndighet för användning av tekniken för att utreda brott, lagföra en person eller verkställa en påföljd. Remissinstanserna anser dock att domstol bör vara tillståndsmyndighet även när det gäller användning av tekniken för att förebygga, förhindra eller upptäcka brottslig verksamhet och avstyrker därför förslaget om att åklagaren ska pröva sådana frågor om tillstånd. *Justitiekanslern* framför liknande synpunkter och menar att det från ett unionsrättsligt perspektiv framstår som osäkert att åklagare ska vara beslutsorgan. Enligt *Sveriges advokatsamfund* är domstolar mest lämpade att hantera samtliga tillståndsprövningar.

Åklagarmyndigheten och *Ekobrottsmyndigheten* ser inte skäl att dela upp beslutanderätten på åklagare och domstol, utan förordar att alla beslut om tillstånd ska prövas av åklagare. *Polismyndigheten* ansluter sig till de synpunkter som Åklagarmyndigheten lämnar. Även *Stockholms tingsrätt* anser att Åklagarmyndighetens synpunkter har fog för sig och att det därför finns skäl att överväga vilken instans som bör fatta beslut om tillstånd. Enligt tingsrätten medför ett delat tillståndsförfarande risk för gränsdragningsproblem. För att möjliggöra en sömlös användning av tekniken när grunden för tillståndet ändras bör det enligt Polismyndigheten övervägas om ett tillstånd som meddelats i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet kan gälla i avvaktan på en ny prövning av om tillstånd kan ges i syfte att utreda eller lagföra brott.

Skälen för regeringens förslag

Tillstånd ska beslutas av en rättslig myndighet eller en oberoende administrativ myndighet

För att använda AI-system för ansiktsigenkänning i realtid krävs enligt artikel 5.3 i AI-förordningen ett förhandstillstånd från en rättslig myndighet eller en oberoende administrativ myndighet vars beslut är bindande i den medlemsstat där användningen ska äga rum. Av artikeln framgår vidare att i vederbörligen motiverade brådskande situationer får användningen av ett sådant system påbörjas utan tillstånd, förutsatt att ett sådant tillstånd begärs utan onödigt dröjsmål och senast inom 24 timmar (se vidare avsnitt 10).

Regeringen delar bedömningen som görs i promemorian att det inte är ett alternativ att göra Integritetsskyddsmyndigheten eller Myndigheten för säkerhet och integritetsskydd till tillståndsmyndighet. Valet står därmed mellan domstol och åklagare.

Åklagare ska pröva frågan om tillstånd att använda tekniken för att bl.a. förebygga, förhindra eller upptäcka brottslig verksamhet

I promemorian föreslås att en ansökan om tillstånd ska prövas av domstol i vissa fall och av åklagare i andra fall. Flera remissinstanser ställer sig bakom promemorians uppdelning medan andra anser att en myndighet bör vara ensam prövningsinstans. Några menar att domstol bör väljas medan andra anser att åklagare bör väljas.

När AI-system för ansiktsigenkänning i realtid används bearbetas material från exempelvis en kamera för att kunna hitta en på förhand bestämd person. Det är närmast fråga om en polisiär utredningsmetod. När det gäller polisiära utredningsåtgärder är utgångspunkten i svensk rätt att åklagare beslutar om sådana i de fall polisen inte själv bör göra det (se t.ex. prop. 2024/25:37 s. 142 om biometrisk registerjämförelse). Från den 1 juli 2025 får t.ex. dna-baserad släktforskning användas i vissa brottsutredningar efter tillstånd av åklagaren (se samma prop. s. 160 f.). Användning av AI-system för ansiktsigenkänning i realtid aktualiserar liknande typer av skyddsintressen och inte sällan kommer det krävas att frågan om tillstånd kan avgöras snabbt. Detta talar för att i första hand välja åklagare som prövningsinstans för ansökningar om tillstånd att använda tekniken. För att detta ska vara möjligt krävs dock att åklagaren uppfyller AI-förordningens krav på att vara en rättslig myndighet.

Begreppet rättslig myndighet definieras inte i AI-förordningen men det följer av EU-rätten att en rättslig myndighet ska vara oberoende och opartisk (jfr EU-domstolens avgörande i mål C-817/19 p. 241). I promemorian föreslås att åklagare ska vara beslutsfattare när användning sker för att förebygga, förhindra och upptäcka brottslig verksamhet. Flera remissinstanser, däribland *Justitiekanslern* och *Centrum för rättvisa*, ställer sig tveksamma till om detta är förenligt med EU-rätten. Centrum för rättvisa menar att det får anses osäkert om Åklagarmyndigheten kan betraktas som en tillräckligt oberoende instans i förhållande till polisens underrättelseverksamhet för att komma i fråga som tillståndsprövningsinstans.

Svenska åklagare agerar självständigt i förhållande till den verkställande makten och ska vara objektiva. Åklagare är i en svensk och EU-rättslig

kontext att betrakta som en rättslig myndighet. Som exempel kan nämnas att Sverige angett åklagare som utfärdande rättslig myndighet både när det gäller en europeisk arresteringsorder och en europeisk utredningsorder. Regeringen har också bedömt att det är förenligt med EU-rätten att åklagare fattar beslut om hemliga tvångsmedel enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) när det sker för att förebygga, förhindra och upptäcka brottslig verksamhet (se prop. 2018/19:86 s. 74 f. och prop. 2023/24:117 s. 75 f.). *Institutet för mänskliga rättigheter* menar att en jämförelse inte kan göras med inhämtningslagen med hänsyn till de stora rättighetskränkningar som en användning av AI-system för ansiktsigenkänning i realtid innebär för den enskilde. Regeringen, som inte delar institutets uppfattning vad gäller integritetsintrånget, anser att de överväganden om beslutsordning som låg till grund för regeringens senaste bedömning är aktuella även här. Åklagaren bedriver ingen underrättelseverksamhet och har ansetts vara oberoende i förhållande till polisen när hemliga tvångsmedel används inom ramen för inhämtningslagen. Åklagare har en lagstadgad objektivitetsplikt även i de fall åklagaren fattar beslut i verksamhet utanför en förundersökning enligt 23 kap. 4 § tredje stycket rättegångsbalken, vilket innebär att såväl omständigheter som talar för som emot att en viss person är inblandad i brottslig verksamhet ska beaktas och att åklagaren inte får låta sig vägledas av andra intressen än de som åklagaren har i uppdrag att tillgodose. Även inom myndigheten är åklagare helt självständiga i sitt beslutsfattande (se prop. 2023/24:117 s. 75).

Genom att åklagare är prövningsinstans enligt inhämtningslagen har de erfarenhet av att hantera liknande ärenden i underrättelsestadiet. Åklagare har också den beredskap som krävs för att kunna fatta snabba beslut vilket är en förutsättning för att tillgodose behovet av en effektiv hantering av ärenden om tillstånd att använda AI-system för ansiktsigenkänning i realtid. Det kan i sammanhanget konstateras att underrättelseverksamhet typiskt sett är främmande för de allmänna domstolarna (se prop. 2023/24:117 s. 73 f.). Visserligen ligger beslutsfattande enligt preventivlagen på domstol men det rör hemliga tvångsmedel av en art som inte är jämförbar med den utredningsmetod som behandlas i denna proposition.

Regeringen anser mot denna bakgrund att åklagare bör pröva ansökningar om tillstånd att använda AI-system för ansiktsigenkänning i realtid i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet.

Vad gäller frågan om prövningsinstans för ansökningar om tillstånd att verkställa straffrättslig påföljd för flera remissinstanser, däribland *Åklagarmyndigheten* och *Polismyndigheten*, fram att beslut om tillstånd alltid bör prövas av åklagare. Det inkluderar tillstånd till användning i syfte att verkställa straffrättslig påföljd. I promemorian föreslås att domstol ska pröva sådana ansökningar. De skäl som anges ovan för att åklagaren ska pröva ansökningar om tillstånd för användning i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet gör sig gällande även i fråga om användning för att verkställa straffrättslig påföljd. Åklagare ansvarar inte för verkställighet av påföljd och är att anse som oberoende i förhållande till såväl Kriminalvården som ansvarar för att verkställa utdömda påföljder (förordning [2023:797] med instruktion för Kriminalvården) som Polismyndigheten som kan bistå med handräckning. Domstol fattar visserligen

sedan något år tillbaka beslut om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder. Åklagare får dock i brådskande fall fatta beslut i avvaktan på rättens prövning (5 och 6 §§ lagen [2024:326] om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder). Enligt regeringens uppfattning ger AI-förordningen utrymme för att låta åklagaren som rättslig myndighet pröva frågan om tillstånd i dessa fall och det har inte framkommit några starka skäl mot att åklagare ska ges en sådan behörighet. Sammantaget föreslår regeringen, till skillnad från förslaget i promemorian, att åklagare bör pröva även ansökningar om tillstånd att använda tekniken i syfte att verkställa straffrättslig påföljd.

Domstol ska pröva frågan om tillstånd att använda tekniken för att utreda eller lagföra brott

En enhetlig och effektiv tillståndsprövning talar för att åklagaren bör pröva även ansökningar om tillstånd att använda tekniken för att utreda eller lagföra brott. Artikel 5.3 i AI-förordningen ställer dock krav på att tillståndsprövningen ska ske efter en motiverad begäran. De brott som tekniken föreslås kunna användas för att utreda och lagföra är sådana där åklagaren i regel är förundersökningsledare. Åklagaren ansvarar då för förundersökningen i sin helhet. Som föreslås nedan ska åklagare ansöka om tillstånd i dessa fall och redan av den anledningen anser regeringen i motsats till bl.a. *Åklagarmyndigheten*, *Ekobrottsmyndigheten*, *Säkerhetspolisen* och *Polismyndigheten*, att åklagare då inte bör ges i uppgift att också besluta om tillstånd att använda tekniken i syfte att utreda eller lagföra brott.

Det har ansetts lämpligt att en domstol fattar beslut om hemliga tvångsmedel under en förundersökning (jfr prop. 2023/24:117 s. 73). Det finns i dag ett väl inarbetat system hos allmänna domstolar att handlägga ärenden där liknande integritetsaspekter behöver beaktas som vid prövningen ett tillstånd att använda AI-system för ansiktsigenkänning i realtid. Allmän domstol får därför anses ha den kompetens som krävs för att göra nödvändiga avvägningar mellan intresset av brottsbekämpning och skyddet för grundläggande fri- och rättigheter. Domstolarna har också möjlighet att ta om hand brådskande frågor, även om det inte finns någon beredskap för omedelbara beslut dygnet runt. Eftersom tekniken föreslås få användas för brottsbekämpande ändamål är det inte lämpligt att allmän förvaltningsdomstol utses till prövningsinstans. Allmän domstol bör därför pröva ansökningar om tillstånd att använda AI-system för ansiktsigenkänning i realtid i syfte att utreda och lagföra brott.

Förslagen ovan innebär ett system med två olika prövningsinstanser. Alternativet skulle vara att allmän domstol även prövar ansökningar om tillstånd att använda tekniken för att bl.a. förebygga, förhindra eller upptäcka brottslig verksamhet för att på så vis få en mer enhetlig ordning. Trots att beslutsfattande enligt preventivlagen ligger på domstol är underrättelseverksamhet emellertid typiskt sett främmande för de allmänna domstolarna (se prop. 2023/24:117 s. 73 f.). Även med beaktande av intresset av en enhetlig ordning anser regeringen att skälen för att ge åklagare rollen som tillståndsprövande myndighet när så är möjligt är så starka att en uppdelning i linje med inhämtningslagen är att föredra.

Mot bakgrund av att osjälvständiga brottsformer som försök, förberedelse och stämpling omfattas innebär en delad prövningsordning

enligt *Stockholms tingsrätt* en risk för gränsdragningsproblem, t.ex. när den misstänkte gärningspersonen bedöms ha nått förberedelsepunkten för ett brott, men ännu inte kommit att begå ett fullbordat brott. Enligt regeringens uppfattning bör det inte kunna uppstå en sådan gränsdragningsproblematik. Den föreslagna ordningen innebär att åklagare och allmän domstol ska pröva ansökningar om tillstånd för olika syften. Förenklat uttryckt prövar åklagaren när tekniken ska användas för all brottsbekämpande verksamhet inom polisen som inte direkt kan knytas till en brottsutredning medan domstol prövar användning där en förundersökning inletts. Därmed är det inte heller möjligt att utforma bestämmelserna så som *Svea hovrätt* önskar, dvs. att hänvisa till de tillåtna syftena för användningen.

Lagrådet invänder inte mot hur ansvarsfördelningen är utformad i lagen men anser att det inte är lämpligt eller en nödvändig konsekvens av förslaget att en ansökan kan prövas av både åklagaren och domstolen. Regeringen konstaterar att avsikten inte är att det ska föreligga delad behörighet i något fall. Det som framför allt avgör behörigheten är om det pågår en förundersökning (då är rätten behörig att pröva ansökan) eller inte (då är åklagaren behörig). Regeringen föreslår i avsnitt 7.1 att möjligheten att använda tekniken för att lokalisera brottsoffer begränsas till situationer där brott ska avbrytas. Men trots det kan en sådan användning komma att ske såväl före som efter en förundersökning inletts. Detta är oundvikligt och bör inte leda till problem för tillämparen.

Behörig domstol

När det gäller frågan om vilken domstol som ska vara behörig finns det skäl att jämföra med vad som gäller för hemliga tvångsmedel där det redan finns en etablerad ordning. Under förundersökning gäller reglerna i rättegångsbalken om laga domstol i brottmål. Som huvudregel är domstolen i den ort där brottet begicks behörig. Om det är lämpligt, får prövningen i stället göras där den misstänkte har sin hemvist eller mera varaktigt uppehåller sig. I vissa brådskande fall får frågor om hemliga tvångsmedel prövas även av domstol på annan ort. Vid sådana samhällsfarliga brott som anges i 27 kap. 34 § rättegångsbalken får prövningen också göras av Stockholms tingsrätt. Eftersom behovet främst uppstår vid brott inom ramen för Säkerhetspolisens verksamhet som rör nationell säkerhet, vilket faller utanför AI-förordningen, så framstår det inte som nödvändigt att ha ett sådant specialfora i detta fall. Det bedöms som lämpligt att i övrigt samma forumregler som gäller för hemliga tvångsmedel bör gälla för en ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid om syftet är att utreda brott och lagföra en person.

Ansökan om tillstånd

Tillstånd att använda AI-system för ansiktsigenkänning i realtid får endast meddelas efter en motiverad begäran (artikel 5.3 i AI-förordningen). Det bör därför tas in en bestämmelse i den nya lagen om att ett tillstånd alltid ska föregås av en ansökan.

Det bör anges i den nya lagen vilka som ska kunna ansöka om tillstånd för de olika syften som tekniken föreslås få användas för. En ansökan bör göras av den aktör inom vars ansvarsområde systemet är avsett att

användas i den specifika situationen. Polismyndighetens uppdrag är bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet. Det är vidare Polismyndigheten som kan bistå med handräckning i syfte att verkställa straffrättslig påföljd. Det bör därför vara Polismyndigheten som ansöker om tillstånd för användning av AI-system för ansiktsigenkänning i realtid när tekniken ska användas för ett sådant syfte. Även Säkerhetspolisen har i uppdrag att bl.a. förebygga, förhindra och upptäcka brottslig verksamhet. I de fåtal fall som Säkerhetspolisen bedriver sådan verksamhet vars personuppgiftsbehandling regleras i brottsdatalagen bör det ankomma på myndigheten att ansöka om tillstånd att använda tekniken.

De brott som användning av AI-system för ansiktsigenkänning i realtid föreslås kunna användas för att utreda är sådana där åklagare vanligen är förundersökningsledare. Åklagare väcker även åtal. Det innebär att det bör vara åklagare som ska ansöka om tillstånd att använda tekniken för dessa syften. Åklagaren måste vara väl insatt i de ärenden som han eller hon ansvarar för, vad det finns för behov av utredningsåtgärder och hur tillgänglig teknik kan användas. Eftersom det är polisen som tillhandahåller tekniken och har kunskap om exempelvis var det finns kameror som är utrustade med nödvändig teknik eller om en referensbild går att använda på ett meningsfullt sätt bör åklagaren som utgångspunkt samråda med polisen inför en ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid.

En ny ansökan ska krävas om grunden för tillståndet ändras

Den föreslagna ordningen innebär att åklagare och allmän domstol ska pröva ansökningar om tillstånd att använda tekniken för olika syften. Detta får till följd att exempelvis ett beslut om tillstånd som har fattats av åklagare i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet inte längre gäller om en förundersökning inleds i det specifika fallet. En ny ansökan om tillstånd behöver då göras och prövas av domstol. Det bör i allmänhet inte vara några problem att fastställa när en person ska lokaliseras eller identifieras för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda ett redan begånget brott inom ramen för en förundersökning. För att möjliggöra en sömlös användning av tekniken när grunden för tillståndet ändras bör det enligt *Polismyndigheten* övervägas om ett tillstånd som meddelats i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet kan gälla i avvaktan på en ny prövning av om tillstånd kan ges i syfte att utreda eller lagföra brott. Enligt regeringens uppfattning ger inte AI-förordningen utrymme för en sådan lösning då det som utgångspunkt krävs förhandstillstånd för ”varje användning” (artikel 5.3 i AI-förordningen). Om det uppstår en situation då behovet av att fortsätta använda tekniken för att identifiera en person kvarstår även efter att en förundersökning har inletts finns möjlighet att fortsätta användningen av tekniken enligt regleringen om tillfällig användning. Det bedöms därmed inte behövas någon särskild regel om detta.

9 Tillståndsprövningen

9.1 Förfarandet i domstol

Regeringens förslag

Förfarandet i domstol ska vara skriftligt och följa reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i den nya lagen. Bestämmelserna om offentligt ombud ska inte tillämpas.

Promemorians förslag

Förslaget i promemorian stämmer överens med regeringens.

Remissinstanserna

De flesta remissinstanser har inte någon invändning mot förslaget i promemorian. *Lunds universitet* konstaterar att det inte föreslås att föreskrifterna om offentligt ombud ska gälla och vill se ytterligare överväganden om hur allmänhetens intresse tillgodoses vid det skriftliga förfarandet. *Eskilstuna tingsrätt* anser att det finns starka skäl att överväga tydligare förfaranderegler vid domstolens prövning. *Myndigheten för säkerhet och integritetsskydd* för fram liknande synpunkter. *Justitiekanslern* efterfrågar övertygande skäl till att offentliga ombud inte ska utses vid domstolens handläggning av ärenden om tillstånd. *Sveriges advokatsamfund* anser att frånvaro av offentliga ombud i praktiken innebär att den enskilde inte har rätt till ett kontradiktoriskt förfarande. Avsaknaden av ett sådant innebär stor risk att komma i konflikt med bestämmelserna om rättvis rättegång i bl.a. Europakonventionen. Advokatsamfundet avstyrker därför förslaget i den delen. *Civil Rights Defenders* föreslår att det i tillståndsprövningen hålls ett sammanträde och, utses ett offentligt ombud samt att besluten ska vara överklagbara för båda parter. Även Sveriges advokatsamfund anser att åklagarens beslut ska kunna överklagas. *Journalistförbundet* och *Tidningsutgivarna* ifrågasätter förslaget om att det inte ska utses offentligt ombud, och anser vidare att det bör införas en bestämmelse om avlyssningsförbud som motsvarar det i 27 kap. 22 § rättegångsbalken. Enligt *Stockholms tingsrätt* behövs vissa klargöranden vad gäller domstolens handläggning av ärenden enligt den nya lagen.

Skälen för regeringens förslag

Som konstateras i promemorian behövs inte några särskilda förfaranderegler för åklagarens handläggning av ärenden om tillstånd.

I avsnitt 8 föreslås att allmän domstol ska pröva ansökningar om tillstånd att använda AI-system för ansiktsigenkänning i realtid för att utreda brott och lagföra en person. Frågan är vilka regler som bör gälla för domstolens handläggning av sådana ärenden. AI-förordningen innehåller inte

några bestämmelser om hur det närmare tillståndsförfarandet ska gå till. Det saknas krav på att förfarandet ska vara muntligt och att det ska utses ett ombud. Det överlämnas i stället åt de berörda medlemsstaterna att i sin nationella rätt fastställa nödvändiga regler för handläggningen av ansökningar om tillstånd (jfr artikel 5.5 i AI-förordningen).

För tillstånd om åtgärder i en förundersökning gäller rättegångsbalkens regler. Mot den bakgrunden är det lämpligt att ta avstamp i dessa regler.

Användning av AI-system för ansiktsigenkänning i realtid innebär att material som samlats in med stöd av exempelvis en kamera bearbetas. Materialet är alltså redan tillgängligt för polisen. Det är således en skillnad mot när hemliga tvångsmedel i form av exempelvis hemlig kameraövervakning och hemlig rumsavlyssning används där det insamlade materialet inte är tillgängligt för polisen utan ett tillstånd om att använda tvångsmedlet. I dessa ärenden utses ett offentligt ombud och hålls ett sammanträde. Däremot utses inte något ombud eller hålls något sammanträde i ärenden om hemlig övervakning av elektronisk kommunikation (27 kap. 28 § rättegångsbalken).

Justitiekanslern anser att promemorian saknar övertygande skäl för att offentliga ombud inte ska utses vid domstolens handläggning av ärenden om tillstånd att använda AI-system för ansiktsigenkänning i realtid. Med hänsyn till det stora integritetsingrepp som sker genom användningen av tekniken anser Justitiekanslern att skälen för det ställningstagandet bör utvecklas. *Civil Rights Defenders*, *Lunds universitet*, *Journalistförbundet* och *Tidningsutgivarna* för fram liknande synpunkter. *Sveriges advokatsamfund* anser att avsaknaden av offentligt ombud och rätt till förhandling i praktiken innebär att den enskilde inte har rätt till ett kontradiktoriskt förfarande. Frånvaron av ett sådant förfarande innebär stor risk att komma i konflikt med rätten till en rättvis rättegång enligt artikel 6 i Europakonventionen och artikel 47 i EU:s rättighetsstadga.

Offentliga ombud är ett institut som används vid prövningen av vissa hemliga tvångsmedel. Användningen av AI-system i realtid för ansiktsigenkänning är inte ett sådant tvångsmedel utan en polisiär utredningsmetod som innebär bearbetning av redan tillgängligt material. Polisiära utredningsmetoder prövas normalt inte av domstol (jfr prop. 2024/25:37 s. 160 f.). Ett system med offentligt ombud innebär visserligen att prövningen får en kontradiktorisk karaktär (se prop. 2008/09:201 s. 70) och fyller en funktion som rättssäkerhetsgaranti. Av tidigare förarbetsuttalanden framgår emellertid att ombuden har sin främsta betydelse vid vissa särskilt integritetskänsliga tvångsmedel som t.ex. hemlig kameraövervakning (se prop. 2013/14:237 s. 120). Ett offentligt ombud kan motsätta sig bifall till en tvångsmedelsansökan och vid bifall överklaga beslutet. Ett överklagande ska ske när ombudet anser att ett beslut inte är förenligt med lag eller att rätten har gjort en felaktig bedömning i fråga om hänsynen till ett motstående intresse. Vid hemlig rumsavlyssning och hemlig kameraövervakning finns det utrymme för stora variationer i integritetsintrånget. Det kan bero på t.ex. hur platsen för tvångsmedlet väljs och avgränsas, på vilken kameravinkel som används eller på att villkor ställs för när avlyssning eller övervakning får ske. Vid hemlig avlyssning av elektronisk kommunikation kan integritetsintrånget bero bl.a. på vilka personer som finns i den misstänktes hushåll och innehållet i de samtal som de kan förväntas föra. Offentliga ombud har däremot inte

ansetts motiverat i ärenden om hemlig övervakning av elektronisk kommunikation eftersom sådan övervakning inte ger någon information om innehållet i den kommunikation som övervakas och att integritetsintrånget typiskt sett är avsevärt mindre när detta tvångsmedel används. Det finns därför mera sällan utrymme för att ifrågasätta eller diskutera utformningen av ett sådant tillstånd (se nämnda prop. s. 120 f).

Det nu redovisade resonemanget kan appliceras även på användning av AI-system för ansiktsigenkänning i realtid. Skäl mot att införa ett system med offentliga ombud när det gäller användning av AI-system för ansiktsigenkänning i realtid är att det integritetsintrång som användningen av tekniken kan medföra är mindre jämfört med hemliga tvångsmedel. Därtill kommer att sådana frågor som offentliga ombud särskilt bevakar mer sällan torde aktualiseras vid användning av tekniken eftersom användningen inte ger någon information om exempelvis innehållet i ett samtal. En särskild utredare har fått i uppdrag att bl.a. göra en översyn av systemet med offentliga ombud (dir. 2025:12). I direktivet anges att de offentliga ombuden är en central del av det system med rättssäkerhetsgarantier som omger bl.a. den hemliga tvångsmedelsanvändningen. I direktivet anges vidare att det med dagens reglering är svårt att rekrytera tillräckligt många ombud med den efterfrågade kompetensen och den tillgänglighet som krävs. Systemet med offentliga ombud anses därför behöva ses över. I linje med vad som anges i direktiven anser regeringen att det finns ett värde i att de offentliga ombudens medverkan i ärenden i domstol koncentreras till ärenden där behoven och funktionen av detta har visat sig vara starka.

Ett snabbt beslutsfattande kan normalt sett vara viktigt i ärenden om tillstånd att använda AI-system för ansiktsigenkänning i realtid för att ändamålet med användningen inte ska gå förlorat. Det bedöms därför finnas ett behov av en mindre formbunden handläggning i domstol. Med hänsyn till de högt ställda krav som föreslås i den nya lagen om hur och när AI-system för ansiktsigenkänning i realtid får användas begränsas integritetsintrånget för samtliga som påverkas av användningen. Regelverket omgärdas dessutom av rättssäkerhetsgarantier, bl.a. genom tillståndsförfarandet, som säkerställer att intrånget i den personliga integriteten inte blir större än vad som kan godtas enligt regeringsformen, Europakonventionen, barnkonventionen och EU:s rättighetsstadga. Även den tillsyn som bl.a. kommer bedrivas av Integritetsskyddsmyndigheten utgör en viktig rättssäkerhetsgaranti.

Sammantaget delar regeringen promemorians bedömning att det inte bör införas ett krav på medverkan av offentliga ombud vid domstolens handläggning av ärenden om tillstånd att använda AI-system för ansiktsigenkänning i realtid. En följd av detta är att handläggningen också kan vara skriftlig. En motsvarande ordning gäller vid handläggning av ärenden om hemlig övervakning av elektronisk kommunikation.

Vad gäller övriga förfaranderegler bedöms det i promemorian lämpligt att rättegångsbalkens regler om handläggning vid domstol av frågor om tvångsmedel i brottmål ska gälla för förfarandet, om inte något annat sägs i den föreslagna lagen. Det innebär bl.a. att reglerna om rättens sammansättning och om överklagande ska tillämpas. *Eskilstuna tingsrätt* för fram att då det är fråga om tillstånd till en uppgiftsbehandling som innebär ett intrång i den personliga integriteten finns starka skäl att överväga mer tydliga bestämmelser kring förfarandet vid domstolens prövning. *Myndig-*

heten för säkerhet och integritetsskydd noterar att rättegångsbalkens regler om handläggning vid domstol av frågor om hemliga tvångsmedel i viss mån skiljer sig åt. Enligt myndigheten medför detta oklarheter om vilka regler som ska tillämpas på nu aktuellt förfarande och myndigheten efterfrågar därför att förfaranderegleрna förtydligas. Regeringen delar inte remissinstansernas synpunkter vad gäller oklar reglering utan anser att den är tydlig samtidigt som flexibiliteten i den inte går förlorad. Den föreslagna lagen innehåller ett antal förfaranderegler och därutöver hänvisas till rättegångsbalkens regler om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor. Det motsvarar vad som gäller enligt exempelvis preventivlagen. Regeringen anser att lagtexten i denna del bör utformas i enlighet med promemorians förslag.

AI-förordningen uppställer inga krav på att ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska kunna överklagas. Ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid som fattas av åklagaren bör inte alls kunna överklagas. Detta överensstämmer med vad som gäller enligt bl.a. inhämtningslagen och motiveras av att huvudregeln är att åklagarbeslut inte är överklagbara. Det har inte framkommit skäl att, så som *Sveriges advokatsamfund* önskar, avvika från den ordningen. *Lunds universitet* vill gärna se en uttrycklig bestämmelse om att åklagarens beslut inte kan överklagas. Någon sådan uttrycklig bestämmelse finns inte i regleringen om hemliga tvångsmedel. Regeringen ser därför inte skäl att införa en sådan i den nya lagen.

När åklagaren ansöker om ett tillstånd hos domstolen är denne part i ärendet. Som part bör åklagaren ha möjlighet att överklaga ett beslut som helt eller delvis går honom eller henne emot. Ett tungt vägande skäl för det är att det möjliggör att en rättspraxis kan växa fram, vilket är väsentligt inte minst då det är fråga om användning av ny teknik. *Civil Rights Defenders* anser att det är en betydande rättssäkerhetsbrist om beslut om tillstånd till användning av AI-system för ansiktsigenkänning i realtid inte alltid är överklagbara. Civil Rights Defenders menar att en person som utsätts för felaktig, oproportionerlig eller annars rättsstridig övervakning inte har någon faktisk möjlighet att tillvarata sina rättigheter. Regeringen kan konstatera att regleringen av användningen av AI-tekniken omgärdas av rättssäkerhetsgarantier. Som exempel kan nämnas tillståndsprövningen som är en viktig rättssäkerhetsgaranti för den enskilde och innebär att en oberoende aktör kommer att bedöma om förutsättningarna för att använda tekniken är uppfyllda och om det är proportionerligt att använda tekniken, se vidare avsnitt 7.2. En annan är att tillsynsmyndigheten ges goda förutsättningar att utöva en effektiv och kvalificerad tillsyn. Dessutom innehåller brottsdatalagen bestämmelser om information till enskild (se vidare avsnitt 12). Mot den bakgrunden anser regeringen att det inte finns något angeläget behov av att införa en sådan överklagandemöjlighet som Civil Rights Defenders efterfrågar.

För överklagandet bör reglerna i rättegångsbalken om överklagande av frågor om tvångsmedel i brottmål gälla, om inte något annat sägs i den föreslagna lagen.

Journalistförbundet och *Tidningsutgivarna* anser att det bör införas en bestämmelse om avlyssningsförbud som motsvarar det i 27 kap. 22 § rättegångsbalken. Användning av AI-system för ansiktsigenkänning i

realtid innebär bearbetning av material som är tillgängligt för polisen genom annan reglering, t.ex. kamerabevakningslagen eller regleringen om hemlig kameraövervakning i rättegångsbalken. De regler som gäller för användningen av materialet, exempelvis avlyssningsförbud, blir därmed tillämpliga även när den aktuella AI-tekniken används och detta är därför inte något som behöver regleras i den nya lagen.

Stockholms tingsrätt ställer slutligen frågan om huruvida ärenden enligt den nya lagen ska hanteras på samma sätt som hemliga tvångsmedel, dvs. med separat diarium skilt från det ordinarie målhanteringssystemet Regeringen konstaterar att det är en fråga som kan behandlas på lägre nivå än lag, jfr 3 § offentlighets- och sekretessförordningen (2009:641).

9.2 Handläggningen ska ske skyndsamt

Regeringens förslag

En ansökan om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid ska prövas skyndsamt.

Promemorians förslag

Förslaget i promemorian stämmer överens med regeringens.

Remissinstanserna

Ingen remissinstans invänder mot förslaget.

Skälen för regeringens förslag

För att AI-system för ansiktsigenkänning i realtid ska kunna användas på ett ändamålsenligt sätt är det viktigt att reglerna om hur tillståndsfrågor ska handläggas är förenliga med polisens behov. De situationer som det förutses att polisen kan komma att använda tekniken för är i de flesta fall sådana som kräver att en ansökan om ett tillstånd att använda tekniken snabbt kan prövas för att syftet med användningen inte ska riskera att gå förlorat. Det bör därför i den nya lagen föreskrivas att en ansökan om ett tillstånd ska handläggas skyndsamt.

Hur snabbt en ansökan ska hanteras får avgöras utifrån förutsättningarna i det enskilda fallet. När en ansökan om ett tillstånd görs efter att användningen redan har påbörjats bör den hanteras med särskild skyndsamhet. En ansökan om ett tillstånd till användning för en period som ligger längre fram i tiden är av naturliga skäl inte lika brådskande att pröva som när det gäller en period i närtid. Som föreslås i avsnitt 8 ska prövningen av ansökningar om tillstånd delas upp mellan åklagare och domstol. Med hänsyn till formerna för beslutsfattandet är det naturligt att en ansökan kan handläggas snabbare om det är åklagaren som ska pröva den än om det är domstolen. Mot bakgrund av den beredskap som domstolarna har i dag och det förfarande som föreslås gälla för handläggningen i domstol bör emellertid även ansökningar om tillstånd som ska prövas av domstolen kunna hanteras på kort tid.

9.3 Beslutets innehåll

Regeringens förslag

I ett beslut att tillåta användning av AI-system för ansiktsigenkänning i realtid ska det anges

1. vilken person som tillståndet avser,
2. för vilket syfte användningen ska ske,
3. under vilken tid och i vilka områden tillståndet gäller, och
4. skälen för beslutet.

Tiden för tillståndet får inte bestämmas längre än vad som är absolut nödvändigt och får inte överstiga en månad från dagen för beslutet. Området eller områdena som tillståndet avser får inte vara större än vad som är absolut nödvändigt.

Promemorians förslag

Förslaget i promemorian stämmer delvis överens med regeringens. I promemorian föreslås att tillståndets giltighet i tid och plats ska bestämmas utifrån vad som är nödvändigt.

Remissinstanserna

En majoritet av remissinstanserna har inga invändningar mot förslaget. *Svea hovrätt* efterfrågar exempel på vad som behöver anges i ett beslut om identiteten på den eftersökte är okänd. *Integritetsskyddsmyndigheten* anser att det i tillståndet behöver fastställas vilken typ av biometrisk fjärridentifiering som tillståndet avser. Myndigheten anser vidare att lagförslaget bör omformuleras så att ett krav på ”strikt” nödvändighet gäller för såväl begränsningen i tid och rum som vilka personer som omfattas. Även *Myndigheten för säkerhet och integritetsskydd* framhåller att promemorians förslag inte överensstämmer med AI-förordningen där det framgår att tillståndet ska begränsas till vad som är ”strikt nödvändigt” när det gäller bl.a. tidsperiod. Enligt *Civil Rights Defenders* är det otillräckligt att tillståndet gäller en månad i taget. Organisationen menar att utan en faktisk bortre tidsgräns riskerar användningen av AI-system för ansiktsigenkänning i realtid glida över i löpande och generell kartläggning. *Eskilstuna tingsrätt* menar att det behövs en reglering om vad en ansökan om tillstånd ska innehålla. Enligt *Journalistförbundet* bör ett beslut om tillstånd innehålla en motivering till varför beslutet är nödvändigt och proportionerligt.

Skälen för regeringens förslag

Enligt artikel 5.3 i AI-förordningen ska behöriga myndigheter bevilja ett tillstånd att använda AI-system för ansiktsigenkänning i realtid endast om behörig myndighet, på grundval av objektiva bevis eller tydliga indikationer som lagts fram för den, har förvissat sig om att användningen av det berörda systemet är nödvändig och proportionell för att uppnå ett av de syften som undantaget tillåter att tekniken används för, i enlighet med vad som anges i begäran och, i synnerhet, förblir begränsad till vad

som är strikt nödvändigt när det gäller tidsperioden samt det geografiska tillämpningsområdet och de personer som omfattas. I beslutsfattandet ska den behöriga myndigheten beakta vad som framgår av artikel 5.2 a och b. Av dessa artiklar följer att all användning av tekniken måste vara proportionerlig. För att säkerställa att användningen inte går utöver vad som är strikt nödvändigt och att beslutet överensstämmer med aktuell ansökan om tillstånd bör åklagarens och domstolens beslut innehålla vissa uppgifter. Den nya lagen föreslås därför innehålla en bestämmelse som reglerar vad ett beslut ska innehålla. Bestämmelsen bör utformas på så sätt att det i ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska anges vilken person som tillståndet avser, för vilket syfte som användningen ska ske, under vilken tid och i vilket eller vilka områden tillståndet gäller och skälen för beslutet. Eftersom den person som användningen avser kan vara okänd bör det inte uppställas krav på att det i beslutet anges identiteten på personen. Det måste dock på något sätt framgå vilken person som avses eftersom en förutsättning för att få använda tekniken enligt AI-förordningens undantag är att användningen sker för att lokalisera eller identifiera en på förhand utpekad person. Detta kan exempelvis ske genom att det i beslutet hänvisas till den person som är misstänkt i visst angivet ärende eller på liknande sätt. Om identiteten är känd bör det alltid anges i beslutet. Vad gäller den geografiska omfattningen kan det tänkas bli aktuellt att i ett beslut tillåta att tekniken används för fler än ett område. Det kan exempelvis finnas ett behov av att använda tekniken vid flera gränsövergångar om den person som avses misstänks vara på väg att lämna eller resa in i landet. Bestämmelsen bör därför utformas så att det i beslutet ska anges i vilket eller vilka områden tillståndet gäller.

Som anges ovan bör även krävas att det i beslutet anges för vilket syfte AI-system för ansiktsigenkänning i realtid får användas eftersom AI-förordningens undantag endast tillåter att tekniken används för vissa specifika syften. Om användningen avser verkställighet av straffrättslig påföljd bör det anges vilken eller vilka domar som legat till grund för åtgärden. Domstolen eller åklagaren bör i beslutet även redogöra för skälen för sitt beslut. För att allmänhetens tilltro till myndigheternas och domstolarnas kompetens och objektivitet ska kunna upprätthållas krävs att myndigheter och domstolar kan visa att beslut har en relevant rättslig grund och är väl underbyggda. Att skälen redovisas är en förutsättning för att det också ska gå att kontrollera att inte ovidkommande hänsyn har tagits vid beslutsfattandet. I motsats till *Journalistförbundet* anser regeringen dock inte att det finns skäl att särskilt reglera att ett beslut om tillstånd ska innehålla en motivering till varför beslutet är nödvändigt och proportionerligt. Någon sådan reglering finns inte heller när det gäller hemliga tvångsmedel.

Integritetsskyddsmyndigheten för fram att typen av biometrisk fjärridentifiering, t.ex. ansikts-, röst eller rörelseigenkänning har betydelse för nödvändighets- och proportionalitetsbedömningen. Myndigheten anser därför att det bör fastställas i tillståndet vilken typ av biometrisk fjärridentifiering som tillståndet avser. Regeringen konstaterar att den tillståndsprövande myndigheten måste förvissa sig om att användningen av det aktuella AI-systemet är nödvändig och proportionell för att uppnå ett av de syften som den nya lagen tillåter att tekniken används för. Vid denna bedömning skulle typen av biometrisk fjärridentifiering kunna ha betydelse i vissa fall.

Som utgångspunkt lär det dock sällan vara möjligt att på förhand veta att endast en viss typ av fjärridentifiering behöver användas, t.ex. när det handlar om att lokalisera och därefter följa en misstänkt person. Att differentiera mellan olika typer av fjärridentifiering skulle dessutom framför allt skapa förutsättningar att i något större utsträckning tillåta annan användning än ansiktsigenkänning. Regeringen anser under alla omständigheter att det inte är nödvändigt att införa en regel i lagen om att beslutet ska innehålla uppgift om vilken eller vilka typer av fjärridentifiering som får användas.

En grundförutsättning för all användning av AI-system för ansiktsigenkänning i realtid är att den är proportionerlig (se vidare avsnitt 7.2). Som framgår ovan ställer AI-förordningen även krav på att tillståndets giltighet ska förbli begränsad till vad som är ”strikt” nödvändigt när det gäller tidsperioden, det geografiska tillämpningsområdet och de personer som omfattas. Integritetsskyddsmyndigheten för fram att villkoret i förslaget i promemorian avseende tillståndets giltighet i tid och rum och den personkrets som träffas behöver skärpas så att det överensstämmer med kraven i AI-förordningen. I förslaget i promemorian framgår inte att nödvändighetsbedömningen ska vara kvalificerad och det saknas krav på nödvändighet när det gäller de personer som ska omfattas. Som föreslås i avsnitt 7.1 ska det i lag uttryckligen anges att tekniken endast får användas om det är absolut nödvändigt. I det ligger att man inte får leta efter personer eller i områden eller under en tid som inte omfattas av det nödvändighetskravet. Det finns därför inget behov av att införa någon ytterligare begränsning av personkretsen. Det finns däremot anledning att förtydliga vad som ligger i nödvändighetskravet i förhållande till tid och rum, inte minst för att säkerställa att detta anges i tillståndet. Regeringen delar därför Integritetsskyddsmyndighetens och *Myndigheten för säkerhet och integritetsskydds* uppfattning att nödvändighetskravet vad gäller tid och rum bör skärpas. I den svenska språkversionen ställs krav på att användningen ska begränsas till vad som är ”strikt” nödvändigt (artikel 5.3 i AI-förordningen). Uttrycket strikt nödvändigt förekommer inte i svensk rätt. I den engelska versionen av AI-förordningen anges ”strictly necessary” i både 5.1 h och 5.3 i betydelsen absolut nödvändigt. Motsvarande begrepp bör användas här i syfte att nå begreppsmässig överensstämmelse även i den svenska ordningen. Det bör alltså framgå direkt av lagen att ett beslut om tillstånd inte får vara mer omfattande när det gäller tid och område än vad som är absolut nödvändigt för att uppnå det avsedda syftet med användningen. Ett sådant krav knyter också an till den föreslagna bestämmelsen om att en förutsättning för att använda tekniken är att den är proportionerlig (se avsnitt 7.2). Vad som är absolut nödvändigt får avgöras utifrån omständigheterna i det enskilda fallet. Omfattningen av tiden och det geografiska området kommer skilja sig åt i olika situationer. Det kan i ärenden om exempelvis människohandel tänkas bli aktuellt att använda tekniken på flertalet gränsövergångar och över en längre tid medan det i ärenden om en försvunnen person kan handla om en mer kortvarig användning i det direkta närområdet. I ärenden om hot om brott kan det finnas signaler om på vilken plats och under vilken tidsperiod hotet ska förverkligas. Ett tillstånd kan då tänkas omfatta den platsen och tidsperioden. I andra fall kan ett hot om brott bedömas som överhängande men det saknas tydliga uppgifter om tidpunkt eller plats. Det innebär att en ansökan kan

komma att omfatta en längre tidsperiod och ett större geografiskt område, kanske till och med avse hela landet under förutsättning att det är proportionerligt i det enskilda fallet. I bedömningen bör vägas in hur allvarligt och överhängande hotet är.

I promemorian föreslås att tiden som tillståndet gäller inte ska överstiga en månad från dagen för beslutet. Om behovet kvarstår efter denna tid måste enligt promemorian en ny ansökan om tillstånd göras. *Civil Rights Defenders* anför att ett tillstånd som gäller en månad i taget är otillräckligt och menar att användning utan en faktisk bortre tidsgräns riskerar att glida över i en form av löpande och generell kartläggning. Det kan finnas ett fortsatt behov av att använda tekniken under längre tid än en månad. Det finns då inget som hindrar att ansöka om ett nytt tillstånd. För att undvika glapp kan en sådan ansökan givetvis göras innan tiden för ett gällande tillstånd har löpt ut. Vad gäller frågan om en bortre tidsgräns för tillståndet bör framhållas att varje ny ansökan blir föremål för en ny tillståndsprövning av åklagare eller domstol. Som framgår ovan innebär en sådan prövning att det bl.a. ska göras överväganden om huruvida användningen är absolut nödvändigt och om den är proportionerlig. Mot den bakgrunden delar inte regeringen Civil Rights Defenders synpunkt.

Sammantaget bör tiden för tillståndet inte överstiga en månad från dagen för beslutet och det bör inte finnas någon yttersta tidsgräns. En sådan reglering överensstämmer med den som gäller för hemliga tvångsmedel och innebär att en prövning av behovet att använda tekniken sker regelbundet (se bl.a. 27 kap. 21 § rättegångsbalken och 4 § inhämtningslagen). Åklagarens eller domstolens bedömning bör kunna bli att ett tillstånd meddelas helt i enlighet med en ansökan eller att tillståndet omfattar ett mindre geografiskt område eller en kortare tidsperiod än vad ansökan avser.

I promemorian görs bedömningen att det inte finns skäl att i lagen reglera vad en ansökan ska innehålla, men att det följer indirekt av den nu föreslagna bestämmelsen att en ansökan om ett tillstånd måste innehålla viss information. *Eskilstuna tingsrätt* är av annan uppfattning. Enligt tingsrätten bör det krävas att den som ansöker även uppger omständigheterna som behövs för att tingsrätten ska kunna göra bl.a. den proportionalitetsbedömning som AI-förordningen kräver. Tingsrätten menar att det gör sig särskilt gällande i och med att förslaget innebär en skriftlig handläggning i tingsrätten där möjligheten att ställa frågor är väsentligt mindre. AI-förordningen uppställer inte något krav på att det ska regleras vad en ansökan ska innehålla. Regeringen anser, i linje med promemorians bedömning, att det genom den föreslagna regleringen om beslutets innehåll är tydligt även vad en ansökan behöver innehålla för uppgifter för att kunna bifallas. Det ligger i den sökandes intresse att förse den tillståndsprövande myndigheten med de uppgifter som behövs för att myndigheten ska kunna göra den bedömning som den föreslagna lagen kräver. Regeringen delar därför inte de farhågor som tingsrätten lyfter. I sammanhanget kan nämnas att regleringen av ärenden om hemlig övervakning av elektronisk kommunikation, som också har skriftlig handläggning, saknar en sådan bestämmelse som tingsrätten efterfrågar. Tingsrätten för också fram att det i promemorian föreslås att en proportionalitetsbedömning i vissa fall inte behöver göras och att det därför behöver ställas mycket höga krav på ansökans innehåll för att den ska kunna beviljas. Regeringen vill understryka att det varken i

promemorian eller i denna proposition föreslås att en proportionalitetsbedömning i vissa fall inte behöver göras. En proportionalitetsbedömning ska alltid göras, även i de fall polisen får påbörja användningen av tekniken utan ett tillstånd, se vidare avsnitt 7.2.

Sammantaget anser regeringen att det inte finns skäl att i lagen också reglera vad en ansökan ska innehålla.

9.4 Ett beslut om tillstånd får verkställas omedelbart

Regeringens förslag

Ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska få verkställas omedelbart.

Promemorians förslag

Förslaget i promemorian stämmer överens med regeringens.

Remissinstanserna

Ingen remissinstans invänder mot förslaget.

Skälen för regeringens förslag

För att reglerna om ett snabbt förfarande ska få genomslag i praktiken och tekniken ska kunna användas ändamålsenligt bör ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid inte behöva få laga kraft innan polisen kan verkställa beslutet. Om ett beslut om tillstånd inte börjar gälla omedelbart finns det en risk för att ändamålet med användningen förfaller. Exempelvis skulle det kunna tänkas att det brott som tekniken är avsedd att användas för att förhindra redan har genomförts eller att ett brottsoffer har förts till en annan plats. Regleringen blir framför allt viktig i de situationer där behovet av att använda tekniken ligger i närtid. Det bör därför införas en bestämmelse i den nya lagen om att ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid får verkställas omedelbart.

Bestämmelsen får endast relevans för beslut om tillstånd till användning som ska ske i en brottsutredning eller för lagföring eftersom det föreslås att ett beslut om tillstånd att använda tekniken i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att möjliggöra verkställighet av straffrättsliga påföljder inte ska gå att överklaga. Sådana beslut gäller därmed omedelbart även utan en särskild reglering.

9.5 Det ska finnas en skyldighet att omedelbart upphäva ett beslut om tillstånd

Regeringens förslag

Om det inte längre finns skäl för ett tillstånd att använda AI-system för ansiktsigenkänning i realtid, ska åklagare omedelbart upphäva beslutet. Polismyndigheten eller Säkerhetspolisen ska omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

Promemorians förslag

Förslaget i promemorian stämmer i huvudsak överens med regeringens. I promemorian föreslås att den som har ansökt om tillståndet omedelbart ska upphäva det. Promemorian innehåller inget förslag om att Polismyndigheten eller Säkerhetspolisen ska underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

Remissinstanserna

Ingen remissinstans invänder mot förslaget.

Skälen för regeringens förslag

Av den föreslagna allmänna bestämmelsen om proportionalitet får anses följa att den som beviljats ett tillstånd att använda AI-system för ansiktsigenkänning i realtid inte får använda tekniken när det inte längre finns behov av det. Det innebär exempelvis att även om ett tillstånd gäller för en lång tidsperiod ska användningen upphöra så fort behovet av den har upphört. Utöver att användningen upphör är det viktigt att beslutet om tillstånd i en sådan situation upphävs. Det bör därför i den nya lagen tas in en bestämmelse om att det när det inte längre finns skäl för ett tillstånd att använda tekniken ska beslutet omedelbart upphävas. I promemorian föreslås att den som har ansökt om tillståndet, dvs. Polismyndigheten, Säkerhetspolisen eller åklagaren ska upphäva det. Regeringen anser dock att åklagaren har bäst förutsättningar att bedöma om det inte längre finns skäl för att använda tekniken på det sätt som tillståndet medger. Det kan i många fall vara Polismyndigheten eller Säkerhetspolisen som först får den information som leder till att det inte längre finns skäl att använda tekniken. Därför bör det införas en skyldighet för dessa myndigheter att omedelbart underrätta åklagaren om sådana omständigheter. Det är viktigt att åtgärden kan ske så snabbt som möjligt för att säkerställa att tekniken inte kan fortsätta att användas när förutsättningar för det inte föreligger.

10 En möjlighet att påbörja användning utan tillstånd

Regeringens förslag

Om det är fara i dröjsmål, ska Polismyndigheten eller Säkerhetspolisen få påbörja användning av AI-system för ansiktsigenkänning i realtid utan tillstånd.

Den myndighet som har påbörjat användningen utan ett tillstånd ska dokumentera den samt skälen för att användningen påbörjades utan tillstånd.

Om användningen har påbörjats utan tillstånd ska en ansökan om tillstånd göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades.

Om användningen har påbörjats utan tillstånd och det inte längre finns skäl för användningen ska den myndighet som har påbörjat användningen eller åklagare omedelbart besluta om att användningen ska upphöra.

Om användningen upphör innan tillståndsfrågan har prövats, ska den som får ansöka om tillstånd i stället göra en anmälan till åklagare eller rätten som ska pröva om det har funnits skäl för användningen.

Om en ansökan om tillstånd avslås ska användning som har påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas. Uppgifter från användningen ska också raderas om åklagaren eller rätten efter anmälan har funnit att det har saknats skäl för användningen.

Promemorians förslag

Förslaget i promemorian stämmer i huvudsak överens med regeringens. I promemorian lämnas inte något förslag om en dokumentationsskyldighet. I promemorian lämnas inte heller något förslag om att den som får ansöka om tillstånd i vissa fall ska anmäla användningen till åklagaren eller rätten eller att uppgifterna från användningen ska raderas också om åklagaren eller rätten funnit att det har saknats skäl för användningen.

Remissinstanserna

De flesta remissinstanser har ingen invändning mot förslaget. *Åklagarmyndigheten* anser att det finns ett uppenbart behov av att kunna påbörja användningen av AI-system för ansiktsigenkänning i realtid utan ett tillstånd. Däremot framstår det, enligt myndigheten, som främmande att en åklagare som leder en förundersökning skulle ge direktiv till polisen om att med stöd av regeln om fara i dröjsmål inleda en användning av tekniken. Enligt *Myndigheten för säkerhet och integritetsskydd* är det av central betydelse att det finns dokumentation om användningen av metoden i syfte att stärka möjligheten till efterkontroll och tillsyn över om förutsättningarna för att påbörja användningen utan tillstånd förelegat. Myndigheten menar vidare att det finns skäl att överväga om det inte vore lämpligt med ett uttryckligt krav i författning på att endast vissa angivna

tjänstemän ska ha rätt att fatta beslut om användning utan tillstånd. *Journalistförbundet* och *Tidningsutgivarna* avstyrker förslaget. Eftersom det endast är resultatet av behandlingen som ska raderas bör det, enligt *Justitiekanslern*, övervägas om inte en begränsning – likt bestämmelsen i 27 kap. 21 a § tredje stycket rättegångsbalken – bör införas.

Skälen för regeringens förslag

Utgångspunkten för användning av AI-system för ansiktsigenkänning i realtid är enligt AI-förordningen att användningen ska föregås av ett förhandstillstånd. Enligt artikel 5.3 i förordningen får dock användning av tekniken påbörjas utan tillstånd i vederbörligen motiverade brådskande situationer, förutsatt att ett sådant begärs utan oskäligt dröjsmål och senast inom 24 timmar. Om ett tillstånd nekas ska användningen stoppas med omedelbar verkan och alla uppgifter samt resultat och utdata som rör denna användning förstöras och raderas. Med vederbörligen motiverade brådskande situationer avses situationer då behovet av att använda det ifrågavarande systemet är sådant att det i praktiken är objektivt omöjligt att erhålla ett tillstånd innan användningen av AI-systemet inleds. I sådana brådskande situationer bör användningen av AI-systemet begränsas till det absoluta minimum som är nödvändigt (skäl 35 i AI-förordningen).

Det finns situationer där polisen kan behöva påbörja användning av tekniken utan ett förhandstillstånd. Det kan exempelvis handla om en situation där polisen får information om att ett allvarligt brott har inträffat och man snabbt behöver lokalisera gärningspersonen för att kunna gripa denne eller förhindra att ytterligare brott begås. En annan situation kan vara att en våldsbenägen person har avvikit från häkte eller anstalt eller att det finns en påtaglig risk för att en eftersökt person är på väg att lämna landet. Det kan även vara fråga om en situation där polisen med kort varsel får kännedom om att ett möte ska äga rum där bl.a. en eftersökt person som misstänks ha begått allvarliga brott ska närvara.

Det finns alltså ett konkret behov av att kunna utnyttja tekniken i brådskande situationer och artikel 5.3 i AI-förordningen möjliggör nationell lagstiftning som tillåter att användning påbörjas utan tillstånd i vissa sådana. Regeringen instämmer därför – även med beaktande av vad *Journalistförbundet* och *Tidningsutgivarna* framför – i promemorians bedömning att det bör införas en sådan möjlighet.

I AI-förordningen används begreppet vederbörligen motiverade brådskande situationer. Uttrycket är ovanligt i svensk författning. Ett uttryck som är vanligt förekommande och som bedöms ha samma innebörd som AI-förordningens begrepp är fara i dröjsmål (jfr 27 kap. 19 c § rättegångsbalken). Eftersom det är polisen som kommer inneha tekniken och därmed vara verkställande myndighet bör det framgå av bestämmelsen att det är polisen som får påbörja användningen. I promemorian anges att en åklagare bör kunna ge polisen direktiv om att påbörja användningen utan tillstånd för de syften som det ankommer på åklagaren att ansöka om tillstånd för, om den bedömer att det är fara i dröjsmål. Som *Åklagarmyndigheten* framhåller framstår det emellertid som främmande att en åklagare som leder en förundersökning skulle ge direktiv till polisen om att med stöd av regeln om fara i dröjsmål inleda en användning av tekniken. De befintliga regler som finns av motsvarande slag (se exempelvis 27 kap.

4 §, 28 kap. 5 och 10 d §§ rättegångsbalken) innebär alla – även inom ramen för en åklagarledd förundersökning – att befogenheten att agera vid fara i dröjsmål ligger hos polisen. Som Åklagarmyndigheten framför ankommer det i stället på polisen att rimligt fort underställa frågan åklagares prövning. Regeringen anser att denna ordning lämpligen även bör gälla här, och detta gäller oavsett om beslut om tillstånd ska fattas av åklagare eller av domstol.

Möjligheten att påbörja användning av tekniken utan tillstånd bör kunna nyttjas i situationer där ändamålet med användningen riskerar att gå förlorat om ett tillstånd skulle avvaktas. Ju mer angeläget det är att påträffa den aktuella personen, t.ex. då personen bedöms vara farlig för allmänheten och det finns en risk att personen begår fler brott eller då det finns en risk att personen lämnar landet, desto större bör utrymmet vara för att få påbörja användning av tekniken utan tillstånd (jfr. prop. 2023/24:108 s. 55).

Enligt AI-förordningen får användning utan tillstånd påbörjas förutsatt att ett tillstånd begärs utan oskäligt dröjsmål och senast inom 24 timmar (artikel 5.3). En sådan regel bör därför framgå av den nya lagen. Tillståndsförfarandet bör då vara detsamma som föreslås i avsnitt 8. Det innebär att om syftet med användningen är att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd ska frågan prövas av åklagare på ansökan av Polismyndigheten eller Säkerhetspolisen. Sker användningen i syfte att utreda eller lagföra brott ska frågan prövas av rätten på ansökan av åklagare.

I de situationer där det har gjorts en inledande bedömning att det funnits förutsättningar att påbörja användningen utan tillstånd men där det inte längre finns förutsättningar att fortsätta användningen är det viktigt att den omedelbart upphör. Detta bör förvisso följa av den föreslagna allmänna bestämmelsen om proportionalitet, se avsnitt 7.2. För att tydliggöra detta bör det dock i den nya lagen tas med en bestämmelse om att den myndighet som har påbörjat användningen omedelbart ska besluta om att användningen ska upphöra. Det innebär att polisen kan avbryta användning som sker för alla de syften som användning föreslås tillåtas för, se avsnitt 7.1. Även åklagaren bör ha möjlighet att besluta om upphörande i de fall användning sker i syfte att utreda eller lagföra brott.

Användningen bör alltid efterföljas av en prövning av åklagare eller domstol. Det är viktigt med en prövning eftersom följden av att tekniken har börjat användas utan tillstånd när det inte funnits skäl för det är att uppgifterna som användningen resulterat i ska raderas. En efterföljande prövning bör ske såväl när fortsatt användning inte längre fyller någon funktion, därför att syftet redan har uppnåtts (den försvunna personen har t.ex. redan återfunnits), som när den verkställande myndigheten har kommit fram till att ansiktsigenkänning inte är någon meningsfull åtgärd i det aktuella fallet. *Lagrådet* anser att denna ordning inte på ett tillräckligt tydligt sätt framgår i lagrådsremissens lagförslag. Lagrådet pekar här på att om det görs en ansökan till en allmän domstol om tillstånd till en åtgärd som redan är vidtagen så torde domstolen som utgångspunkt betrakta den väckta frågan som överspelad och behandla ansökan som förfallen. Som konstateras ovan är avsikten att det alltid bör ske en prövning. För att säkerställa det bör paragrafen justeras i linje med vad Lagrådet föreslår.

Den som är skyldig att ansöka om tillstånd bör ansvara för att anmäla

användningen. Det innebär att om användningen sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd bör polisen anmäla beslutet till åklagare som har att pröva det. Om syftet är att utreda brott eller lagföra en person bör polisen anmäla det till åklagaren, som har att anmäla beslutet till rätten som prövar. Den som anmäler bör i likhet med vad som gäller för en ansökan om tillstånd förse prövningsinstansen med de uppgifter som behövs för att en välgrundad prövning ska kunna göras. Det är upp till rättstillämpningen att i det enskilda fallet avgöra vilka uppgifter som behövs.

Om åklagaren eller rätten avslår ansökan bör användning som påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas. . Det bör framgå i den nya lagen.

Även i de fall åklagaren eller rätten vid en prövning efter att användningen upphört finner att det saknats skäl för användningen bör uppgifter från användningen raderas. För att tydliggöra detta bör lagtexten, i linje med vad *Lagrådet* föreslår, justeras i förhållande till lagrådsremissens lagtextförslag. Uppgifter som ska raderas omfattar indata som erhållits direkt av ett AI-system i samband med användningen av systemet samt resultat och utdata från användningen. Det bör inte omfatta indata som lagligen förvärvats i enlighet med annan unionsrätt eller nationell rätt (skäl 35 i AI-förordningen). Detta bedöms innebära att det är resultatet av behandlingen av kameramaterialet som AI-systemet utför som ska raderas och inte materialet som sådant, under förutsättning att detta samlats in med stöd av exempelvis aktuell dataskyddsreglering. Eftersom det endast är resultatet av behandlingen som ska raderas bör det, enligt *Justitiekanslern*, övervägas om inte en begränsning – likt bestämmelsen i 27 kap. 21 a § tredje stycket rättegångsbalken – bör införas. Av den bestämmelsen följer att om rätten finner att det saknats skäl för en viss åtgärd får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som omfattats av åtgärden, eller för någon annan som uppgifterna avser. En sådan bestämmelse i den nu föreslagna lagen skulle emellertid bli mer långtgående, eftersom den skulle förbjuda användning av uppgifter (t.ex. kameramaterial) som polisen inte inhämtat utan enbart behandlat med stöd av lagen. Med hänsyn till detta och då det i enlighet med förordningens krav föreslås regler om radering av uppgifter anser regeringen inte att det finns behov av en sådan bestämmelse som Justitiekanslern efterfrågar.

Myndigheten för säkerhet och integritetsskydd anser att det finns skäl att överväga om det inte vore lämpligt med ett uttryckligt krav i författning på att endast vissa angivna tjänstemän ska ha rätt att fatta beslut om användning utan tillstånd. Polisen får enligt 8 § polisförordningen (2014:1104) delegera beslutanderätt och arbetsuppgifter som innebär att grundlagsskyddade fri- och rättigheter kan komma att inskränkas endast till särskilt kvalificerade beslutsfattare som har den utbildning, kompetens och erfarenhet som krävs. Polisen får alltså reglera vilka befattningshavare som kan fatta de aktuella besluten, utan att ett sådant krav behöver regleras på lag- eller förordningsnivå. Regleringen i polisförordningen är inte så allmänt hållen att den helt överlämnar till myndigheten att själv avgöra på vilken nivå beslut ska fattas. En eventuell granskning av Justitieombudsmannen eller Justitiekanslern av ett beslut om användning av tekniken kan omfatta även nivån för beslutsfattandet. Det saknas därför skäl att reglera beslutsbefogenheten närmare.

Som *Myndigheten för säkerhet och integritetsskydd* påpekar är det av central betydelse att det finns dokumentation om användning som sker utan tillstånd. Det behövs för att stärka möjligheten till efterhandskontroll och tillsyn över om förutsättningarna för att påbörja användningen av tekniken utan ett tillstånd förelegat. Det bör därför införas en bestämmelse om att den myndighet som har påbörjat användning utan tillstånd ska dokumentera det och ange skälen för att användningen påbörjades utan tillstånd. Av skälen bör exempelvis framgå varför det i praktiken inte är möjligt att erhålla ett tillstånd innan användningen av AI-systemet inleds (jfr skäl 35). För att tillsynsmyndigheten ska få kännedom om användningen avser regeringen att i förordning införa en skyldighet för den myndighet som påbörjar användning utan tillstånd att anmäla detta till Integritetsskyddsmyndigheten (se vidare avsnitt 13). *Lagrådet* noterar att förslaget inte innehåller något uttryckligt krav på dokumentation av den användning som sker efter tillstånd av åklagare eller domstol. I avsnitt 9.3 föreslås att det i ett beslut om tillstånd ska anges vilken person som tillståndet avser, för vilket syfte användning ska ske, under vilken tid och i vilket eller vilka områden tillståndet gäller och skälen för beslutet. En jämförelse kan göras med bl.a. inhämtningslagen. Av 8 § i den lagen framgår att beslut och åtgärder som rör inhämtning av uppgifter enligt lagen ska dokumenteras. Av förarbetena till regleringen framgår att det kan handla om uppgifter om tillståndet, såsom när det beviljats och om det har ändrats eller upphävts. Det kan också handla om datum och tidpunkt för verkställigheten samt vilken adress, kommunikationsutrustning eller geografiskt område som verkställigheten har avsett eller skett på (prop. 2023/24:117 s. 205). De uppgifter som ska dokumenteras i ett beslut om användningen av AI-tekniken motsvarar i huvudsak vad som normalt dokumenteras inom ramen för exempelvis inhämtning av uppgifter enligt inhämtningslagen. Mot den bakgrunden anser regeringen att en sådan dokumentationsskyldighet som Lagrådet efterfrågar inte är nödvändig.

11 Konsekvensbedömning och registrering i EU-databas

Regeringens förslag

Innan ett AI-system för ansiktsigenkänning i realtid används för första gången ska Polismyndigheten och Säkerhetspolisen göra en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen.

Från och med den dag som regeringen bestämmer krävs också att tekniken ska få användas först efter att Polismyndigheten och Säkerhetspolisen har registrerat AI-systemet i EU-databasen enligt artikel 49 i förordningen. Ett sådant system får dock användas utan registrering om användningen inte kan avvakta. I sådana fall ska en registrering ske så snart det är möjligt.

Promemorians förslag

Förslaget i promemorian stämmer i huvudsak överens med regeringens. I promemorian föreslås att en konsekvensbedömning enligt artikel 27 i sin helhet ska göras först efter att artikeln börjar tillämpas.

Remissinstanserna

De flesta remissinstanser har ingen invändning mot förslaget. *Lunds universitet* anser att förslaget är förenligt med AI-förordningen. *Civil Rights Defenders* anser att det behöver säkerställas insyn i den konsekvensbedömning som ska upprättas av myndigheterna. *Institutet för mänskliga rättigheter* föreslår att det införs ett krav på att tillståndsmyndigheten ska pröva om den sökande myndigheten har gjort en konsekvensbedömning.

Skälen för regeringens förslag

Av artikel 5.2 andra stycket i AI-förordningen framgår att användning av AI-system för ansiktsigenkänning i realtid endast får tillåtas om den brottsbekämpande myndigheten har slutfört en konsekvensbedömning avseende grundläggande rättigheter enligt artikel 27 i förordningen. Mot den bakgrunden bör det i den nya lagen framgå att tekniken endast får användas om en konsekvensbedömning har slutförts. I artikel 27 fastställs de krav rörande konsekvensbedömningar avseende grundläggande rättigheter som är tillämpliga på AI-system med hög risk. Skyldigheten att genomföra konsekvensbedömningar avseende grundläggande rättigheter enligt artikel 5.2 i AI-förordningen åläggs tillhandahållarna av systemet för ansiktsigenkänning i realtid. Regeringen konstaterar att varje myndighet som använder systemet, dvs. både Polismyndigheten och Säkerhetspolisen, behöver göra en egen konsekvensbedömning enligt artikel 27 i AI-förordningen innan den första användningen. Som *Lagrådet* anför bör detta tydliggöras i lagtexten. Det finns dock anledning att formulera den i närmare anslutning till AI-förordningens systematik än vad Lagrådet ger uttryck för.

I promemorian görs bedömningen att det inte bör ankomma på den tillståndsprövande myndigheten att kontrollera att en konsekvensbedömning är gjord när en ansökan om tillstånd kommer in till myndigheten. *Institutet för mänskliga rättigheter* föreslår att ett krav på sådan kontroll införs eftersom detta krävs för att tillståndsmyndigheten ska kunna göra en effektiv prövning av användningen i enlighet med AI-förordningen. Artikel 27.3 i AI-förordningen innehåller krav på att tillhandahållaren ska underrätta marknadskontrollmyndigheten om resultatet av konsekvensbedömningen (se vidare avsnitt 13 om marknadskontrollmyndighetens uppgift). Däremot uppställs inget krav på att den tillståndsprövande myndigheten ska ta del av konsekvensbedömningen. Av kommissionens riktlinjer om förbjudna användningsområden för AI (punkten 377) framgår att konsekvensbedömningen avseende grundläggande rättigheter bör utföras på en abstrakt nivå innan AI-systemet tas i bruk för första gången. Det anges vidare att särskilda kontextberoende överväganden som avgör inverkan av användningen i varje enskilt fall där ett system för biometrisk fjärridentifiering i realtid används bör beskrivas i närmare detalj i den

enskilda begäran om tillstånd från en rättslig myndighet eller annan oberoende administrativ myndighet för varje användning av systemet för biometrisk fjärridentifiering. Mot den bakgrunden anser regeringen att det inte finns skäl att införa ett sådant krav som Institutet för mänskliga rättigheter efterfrågar.

Vid konsekvensbedömningen ska beaktas vilken inverkan på grundläggande rättigheter som användningen av tekniken kan ge upphov till. Av artikel 27.1 i AI-förordningen framgår att bedömningen ska bestå av en beskrivning av tillhandahållarens processer där AI-systemet kommer att användas i linje med dess avsedda ändamål (a), en beskrivning av den tidsperiod inom vilken och den frekvens med vilken AI-systemet är avsett att användas (b), de kategorier av fysiska personer och grupper som sannolikt kommer att påverkas av användningen av systemet i det specifika sammanhanget (c), de specifika risker för skada som sannolikt kommer att påverka de kategorier av fysiska personer eller grupper av personer som har identifierats enligt led c, med beaktande av den information som leverantören har tillhandahållit enligt artikel 13 (d), en beskrivning av genomförandet av åtgärder för mänsklig kontroll, i enlighet med bruksanvisningen (e) och de åtgärder som ska vidtas om dessa risker förverkligas, inbegripet arrangemangen för intern styrning och klagomålsmekanismer (f).

En konsekvensbedömning avseende grundläggande rättigheter ersätter inte den konsekvensbedömning avseende dataskydd som personuppgiftsansvariga i vissa fall måste utföra. Enligt 3 kap. 7 § brottsdatalagen ska den personuppgiftsansvarige bedöma konsekvenserna för skyddet av personuppgifter innan en ny typ av behandling påbörjas som kan antas medföra särskild risk för intrång i den registrerades personliga integritet, något som regelmässigt kan förväntas vara fallet då AI-system för ansiktsigenkänning i realtid ska börja användas. I sådana fall kan, enligt artikel 27.4 i AI-förordningen, vissa av kraven i artikel 27.1 uppfyllas genom den konsekvensbedömningen. Det kan också noteras att om konsekvensbedömningen visar att det finns särskild risk för intrång i de registrerades personliga integritet, eller om typen av personuppgiftsbehandling innebär särskild risk för intrång, ska den personuppgiftsansvarige enligt 3 kap. 7 § andra stycket brottsdatalagen samråda med tillsynsmyndigheten i god tid innan behandlingen påbörjas.

Civil Rights Defenders framhåller att transparens är en grundläggande rättssäkerhetsgaranti vid användning av AI-system för ansiktsigenkänning i realtid. Enligt organisationen finns det starka skäl att säkerställa offentlig insyn i konsekvensbedömningarna, särskilt för att se till att Sverige inte kränker mänskliga rättigheter. Om en konsekvensbedömning begärs ut får en prövning göras utifrån reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen (2009:400).

Av artikel 27.3 i AI-förordningen framgår att marknadskontrollmyndigheten ska underrättas om resultatet av konsekvensbedömningen, vilket inbegriper att lämna in ett formulär grundat på en sådan mall som avses i artikel 27.5 i förordningen.

I avsnitt 16 föreslås att bestämmelserna om undantag från förbudet att använda AI-system för ansiktsigenkänning i realtid ska träda i kraft den 1 juli 2026. Artikel 27 i AI-förordningen börjar dock tillämpas först den 2 augusti 2026 (artikel 113 i AI-förordningen). Det innebär att den mall

som nämns ovan inte kommer att vara tillgänglig när de föreslagna bestämmelserna träder i kraft. Det kan dock inte ha varit avsikten att undantaget i AI-förordningen inte ska kunna utnyttjas på grund av att en sådan mall inte finns att tillgå. Mot den bakgrunden föreslås i promemorian att kravet i den nya lagen bör utformas på så sätt att en konsekvensbedömning ska göras utifrån vad som föreskrivs i artikel 27.1–27.4 i AI-förordningen, men då alltså med undantag för kravet i artikel 27.3 att lämna in en sådan mall som avses i artikel 27.5. I promemorian föreslås vidare att när artikel 27 i förordningen börjar tillämpas bör det införas en ändring i den nya lagen som anger att användning av tekniken endast får påbörjas om en konsekvensbedömning såsom föreskrivs i artikel 27 i sin helhet har slutförts. Enligt regeringen kan tillhandahållaren av tekniken, dvs. polisen, uppfylla de krav som ställs på tillhandahållaren i artikel 27 utan att det finns en särskild mall. Uppfattningen ligger i linje med kommissionens riktlinjer om förbjudna användningsområden för AI där det framgår att under den period då förbuden i artikel 5 i AI-förordningen blir tillämpliga men bestämmelserna om AI-system med hög risk ännu inte är tillämpliga bör de krav för konsekvensbedömningar avseende grundläggande rättigheter som anges i artikel 27 i AI-förordningen tillämpas av tillhandahållare av tekniken (punkten 371). Mot den bakgrunden anser regeringen att det inte finns behov av en sådan uppdelning av artikel 27 som föreslås i promemorian. Regleringen bör därför utformas så att tekniken ska få användas först efter att polisen har gjort en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordning. Någon ändring i den nya lagen såvitt avser konsekvensbedömningen behövs därför inte.

För att få använda tekniken krävs enligt artikel 5.2 i AI-förordningen också att AI-systemet har registrerats i EU-databasen enligt artikel 49 i förordningen. Det är i samband med att systemet släpps ut på marknaden eller tas i bruk som leverantören ska registrera det (artikel 49.1 i AI-förordningen). Det innebär att det endast behöver göras en registrering per system. EU-databasen ska innehålla viss information om AI-system med hög risk och databasen ska införas och upprätthållas av kommissionen i samarbete med medlemsstaterna (se artikel 71 i AI-förordningen). I egenskap av tillhandahållare av AI-systemet bör polisen lämpligen registrera systemet i EU-databasen. Som framgår ovan behövs endast en registrering per system. Av artikel 5.2. andra stycket i förordningen följer att tekniken får användas utan att systemet har registrerats i EU-databasen i vederbörligen motiverade brådskande fall, förutsatt att registreringen slutförs utan oskäligt dröjsmål.

Artikel 49 i AI-förordningen, som innehåller krav på hur registreringen ska gå till, ska inte börja tillämpas förrän den 2 augusti 2026 vilket innebär att EU-databasen inte kommer att vara öppen för registrering innan det datumet. Avsikten kan dock inte ha varit att undantaget i AI-förordningen inte ska kunna utnyttjas på grund av att EU-databasen öppnas först vid ett senare tillfälle. Den nya lagen bör därför inte innehålla något krav på registrering. I samband med att artikel 49 i förordningen börjar tillämpas bör det införas en ändring i den nya lagen som anger ett krav på registrering i EU-databasen, med möjlighet till undantag i brådskande situationer. I AI-förordningen används begreppet vederbörligen motiverade brådskande situationer. I promemorian föreslås att uttrycket

fara i dröjsmål bör användas. Regeringen anser i stället att uttrycket ”inte kan avvakta” bör användas. Det uttrycket bedöms ha samma innebörd som AI-förordningens begrepp. Om en registrering innebär att ändamålet med tillståndet riskerar att gå förlorat bör det vara fråga om en användning som inte kan avvakta. Om användning av tekniken påbörjats utan att AI-systemet har registrerats i EU-databasen krävs enligt förordningen att en registrering görs utan oskäligt dröjsmål. Regeringen anser att uttrycket ”så snart som möjligt” bör användas i stället för uttrycket ”utan onödigt dröjsmål” som föreslås i promemorian. Att en registrering ska ske så snart som möjligt innebär att den som är skyldig att ansöka om ett tillstånd ska göra det skyndsamt. Som angetts ovan är det polisen som ska säkerställa att AI-systemet registreras i EU-databasen. Den tillståndsprövande myndigheten behöver inte kontrollera att det görs. Detta gäller även i det fall då en registrering sker i efterhand på grund av fara i dröjsmål.

I EU har lyfts frågan om att senarelägga dag för ikraftträdande av vissa delar i AI-förordningen som gäller AI-system med hög risk. Det innebär att det i detta skede råder viss osäkerhet kring när artikel 49 ska börja tillämpas. I avsnitt 16 föreslås därför att ändringen i den nya lagen ska träda i kraft den dag som regeringen bestämmer.

12 Det ska finnas ett krav på underrättelse till enskild

Regeringens förslag

Den som har identifierats eller lokaliserats genom en åtgärd enligt den nya lagen som gäller en brottsutredning eller lagföring ska underrättas om åtgärden. Underrättelsen ska lämnas så snart det kan ske utan men för det syfte som åtgärden vidtogs för. I vissa situationer ska en underrättelse kunna skjutas upp på grund av sekretess.

Promemorians förslag

Förslaget i promemorian stämmer i huvudsak överens med regeringens. I promemorian föreslås att även de som inte lokaliseras eller identifieras ska underrättas. I promemorian föreslås vidare att en enskild ska underrättas om åtgärden skett inom ramen för verkställighet av påföljd.

Remissinstanserna

Den övervägande majoriteten har inte någon invändning mot förslaget. *Civil Rights Defenders* avstyrker förslaget i promemorian om att den som har varit föremål för ett beslut enligt lagen endast ska underrättas i vissa situationer. Med hänsyn till det stora integritetsingrepp som sker genom användningen av AI-system för ansiktsigenkänning i realtid anser *Justitiekanslern* att det bör övervägas en skyldighet att underrätta enskild även när tekniken har använts för att förebygga, förhindra och upptäcka

brottslig verksamhet. *Åklagarmyndigheten* avstyrker förslaget i promemorian om att enskild ska underrättas.

Skälen för regeringens förslag

Det kommer alltid finnas en bestämd, om än inte alltid identifierad, person som eftersöks inom ramen för ett ärende om användning av AI-system för ansiktsigenkänning i realtid, vilken kommer att få sina personuppgifter behandlade. Därutöver kan andra personer komma att beröras genom att deras personuppgifter behandlas när de passerar en kamera med AI-system för ansiktsigenkänning i realtid. Frågan är om en underrättelse bör ske efter att ett sådant AI-system har använts och i sådana fall vem som bör underrättas. En underrättelse kan ha betydelse för den enskildes möjlighet att få personuppgiftsbehandlingen prövad. Mot den bakgrunden kan det hävdas att samtliga som passerar en kamera med sådant AI-system bör få en underrättelse om användningen. I motsatt riktning talar dock det förhållandet att det i praktiken vore ogenomförbart att identifiera alla som passerar en kamera och därefter söka upp dem för att underrättas. Det skulle också innebära ett integritetsintrång i sig. Någon motsvararande ordning finns inte vid underrättelse av användning av hemliga tvångsmedel där även andra än den som tvångsmedlet avser kan komma att t.ex. avlyssnas eller kameraövervakas. Det bör därför inte införas en generell underrättelseskyldighet när tekniken har använts.

Frågan är då om det bör införas en skyldighet att underrätta den person som eftersöks. Som anges ovan kan en underrättelse ha betydelse för att få personuppgiftsbehandlingen prövad. En skyldighet att lämna en underrättelse skulle även kunna ha en återhållande verkan och bidra till att prövningen inför en ansökan om den aktuella åtgärden görs på ett än mer noggrant sätt (jfr prop. 2023/24:108 s. 72 f.). Mot den bakgrunden föreslås i promemorian att det i den nya lagen bör regleras att det ska lämnas en underrättelse om att tekniken har använts till den person som eftersökts.

Åklagarmyndigheten anser att en sådan resurskrävande underrättelseskyldighet inte är motiverad. Som skäl för det anför Åklagarmyndigheten att användningen av tekniken inte går att jämföra med hemliga tvångsmedel. De starka integritetssynpunkter som regelmässigt föreligger vid användning av hemliga tvångsmedel har inte samma tyngd här. Andra remissinstanser, som *Justitiekanslern* och *Civil Rights Defenders*, anser däremot att en underrättelseskyldighet är viktig med hänsyn till det integritetsingrepp som sker genom användning av tekniken.

Regeringen anser att integritetsingreppet vid användning av tekniken inte kan jämföras med hemliga tvångsmedel. Den nya lagen ger nämligen inte utrymme för annat än att lokalisera eller identifiera en person utifrån uppgifter som polisen redan har tillgång till. Integritetsintrånget får därigenom anses mer begränsat. Användningen av tekniken kan dock vara känslig och behöver därför omgärdas av skyddsregler som exempelvis en tillståndsprövning. Underrättelseskyldigheten är en annan sådan skyddsregel. Genom underrättelsen ges den enskilde, som inte är involverad i tillståndsprocessen, möjlighet att bedöma det integritetsintrång som har skett och reagera om han eller hon anser att åtgärden har varit felaktig. En underrättelseskyldighet kan bidra till att stärka rättssäkerheten i förfarandet, förbättra tillsynen och skapa legitimitet till och förtroende för den

nya utredningsmetoden. Mot den bakgrunden anser regeringen, till skillnad från Åklagarmyndigheten, att det bör införas en underrättelseskyldighet när tekniken har använts i en brottsutredning eller för lagföring. I promemorian föreslås att en enskild också ska underrättas om åtgärden skett inom ramen för verkställighet av påföljd. Regeringen anser emellertid att skyddsintresset inte motiverar att en underrättelse sker i den situationen. En sådan skyldighet bör därför inte införas.

Av naturliga skäl kan en underrättelse inte ske med den som är okänd. I promemorian föreslås att alla andra som har varit föremål för en åtgärd enligt den nya lagen ska underrättas om det. Det innebär att även personer som inte lokaliseras ska underrättas. Enligt regeringens bedömning kommer det i praktiken att vara svårt att underrätta de personer som inte lokaliseras eftersom det saknas uppgifter om var de befinner sig. Om användningen av tekniken inte leder till någon träff blir dessutom integritetsintrånget mindre. Det framstår inte som motiverat att Åklagarmyndighetens resurser ska läggas på en sådan uppgift. Mot den bakgrunden bör underrättelseskyldigheten begränsas till de som är identifierade eller som har lokaliserats.

Justitiekanslern anser att det bör övervägas en skyldighet att underrätta enskild även när tekniken har använts i underrättelseverksamhet. *Civil Rights Defenders* för fram liknande synpunkter. I likhet med vad som gäller i inhämtningslagen anser regeringen dock att en underrättelse inte bör ske i sådana fall. Sådan verksamhet bedrivs med ett framåtblickande perspektiv och har en övergripande karaktär. En underrättelseskyldighet skulle då riskera att motverka huvudsyftet med verksamheten. En sådan bestämmelse skulle även behöva förses med en lång rad undantag och det skulle i många fall kunna ta lång tid innan en underrättelse skulle kunna lämnas.

Den enskilde bör underrättas så snart det kan ske utan men för syftet som åtgärden vidtogs för. Detta motsvarar vad som gäller enligt rättegångsbalken i fråga om underrättelse vid hemliga tvångsmedel. Av den regleringen följer även att om uppgifterna omfattas av sekretess enligt 15 kap. 1 eller 2 §, 18 kap. 1, 2 eller 3 § eller 35 kap. 1 eller 2 § offentlighets- och sekretesslagen ska en underrättelse skjutas upp till dess att sekretess inte längre gäller. Kravet på att en underrättelse ska lämnas gäller inte heller till den som redan har fått del av eller tillgång till uppgifterna, om en underrättelse med hänsyn till omständigheterna uppenbart är utan betydelse eller om den person som underrättelsen avser har avlidit. Det föreslås att samma ordning ska gälla för underrättelse om användning av AI-system för ansiktsigenkänning i realtid. Det bör därför tas med bestämmelser om detta i lagen. En skillnad mot när hemliga tvångsmedel används enligt rättegångsbalken är dock att när AI-system för ansiktsigenkänning i realtid används kommer identiteten på den som omfattas av användningen inte alltid vara känd på annat sätt än genom en bild. En underrättelse är då omöjlig att lämna. Det bör därför även tas in en bestämmelse i lagen om att en underrättelse inte ska ske om identiteten på den som är föremål för ett beslut om tillstånd är okänd.

Frågan om underrättelse bör prövas slutligt om underrättelse inte har kunnat ske inom ett år och sex månader från det att användningen av tekniken avslutades. Tiden bör räknas från den tidpunkt då användningen slutfördes. Det bör gälla oavsett vilken tidsperiod som framgår av det

beslutade tillståndet. En sådan reglering om när frågan om underrättelse bör prövas slutligt motsvarar den som gäller för hemliga tvångsmedel enligt rättegångsbalken. För att minimera risken för att en slutlig prövning, på grund av sekretess eller risk för men för syftet som åtgärden vidtogs för, kommer till stånd väldigt sent eller inte alls bedöms det viktigt med en yttersta tidpunkt för att pröva frågan (jfr prop. 2023/24:108 s. 74).

Genom underrättelsen kan den enskilde få sin rätt tillgodosedd bl.a. genom de möjligheter som finns att begära rättelse, radering eller begränsning av behandling av personuppgifterna enligt 4 kap. 9 och 10 §§ brottsdatalagen. Den enskilde kan genom den regleringen förvisso inte få ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid prövat men däremot kan en prövning av personuppgiftsbehandlingen komma till stånd. Den enskilde kommer även kunna överklaga ett beslut från en myndighet att inte vidta rättelse eller att radera en uppgift och han eller hon kan begära ersättning för skada eller kränkning som orsakats av behandling av personuppgifter i strid med lagen (7 kap. 1 och 2 §§ brottsdatalagen). Den enskildes rätt till prövning tillgodoses också på andra sätt än genom underrättelse. AI-förordningen ställer krav på att all användning av tekniken ska anmälas till den berörda nationella marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten. Som framgår av avsnitt 13 avser regeringen att utse Integritetsskyddsmyndigheten till marknadskontrollmyndighet i fråga om användning av tekniken. Integritetsskyddsmyndigheten är också nationell dataskyddsmyndighet. Myndigheten kommer således att få anmälan även i den egenskapen. Att anmäla all användning utgör ett betydelsefullt verktyg för att Integritetsskyddsmyndigheten ska kunna granska att reglerna om den personuppgiftsbehandling som sker inom ramen för användning av tekniken följs.

Vad en underrättelse ska innehålla och vem som ska fullgöra underrättelseskyldigheten bör regleras på förordningsnivå.

Civil Rights Defenders anför att enskilda borde kunna informeras om användningen av tekniken genom skyltning på plats och hänvisar till bestämmelser i dataskyddsdirektivet om den registrerades rätt till information. Organisationen anför vidare att en digital tjänst för underrättelse annars hade kunnat användas. Artikel 26.11 i AI-förordningen innehåller en upplysning om att när det gäller AI-system med hög risk som används för brottsbekämpande ändamål ska artikel 13 i brottsdatadirektivet tillämpas. Regleringen i 4 kap. 1 § brottsdatalagen genomför artikel 13.1. I paragrafen anges vilken allmän information som på den personuppgiftsansvariges eget initiativ ska göras tillgänglig för den registrerade. Informationen, som riktar sig till allmänheten eller en obestämd, större krets av registrerade, kan göras tillgänglig t.ex. på den behöriga myndighetens webbplats (prop. 2017/18:232 s. 465). I 4 kap. 2 § brottsdatalagen, som genomför artikel 13.2, anges vilken information som ska lämnas till den registrerade i ett enskilt fall för att han eller hon ska kunna ta till vara sina rättigheter. Sådana fall som avses i bestämmelsen kan t.ex. vara att den registrerade riskerar att lida rättsförlust om han eller hon inte får del av informationen eller att det av annat skäl är viktigt för honom eller henne att känna till behandlingen för att kunna ta till vara sina rättigheter. Ett annat exempel kan vara att känsliga personuppgifter har behandlats i strid med 2 kap. 11 §. Bestämmelserna i 4 kap. 5 § brottsdatalagen, som genomför artikel 13.3, gör det dock möjlighet att införa

undantag från den personuppgiftsansvariges informationsskyldighet. Regleringen innebär att den personuppgiftsansvarige får begränsa eller utelämna informationen bl.a. till skydd för intresset av att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder eller upprätthålla allmän ordning och säkerhet. Det är främst sekretess och tystnadsplikt enligt offentlighets- och sekretesslagen som avses men även andra författningar kan innehålla bestämmelser som gör paragrafen tillämplig (prop. 2017/18:232 s. 468 f). I sammanhanget kan nämnas den ändring i offentlighets- och sekretesslagen som föreslås i avsnitt 14.1.

Sammantaget anser regeringen att den befintliga dataskyddsrättsliga regleringen om information som den personuppgiftsansvarige ska lämna på eget initiativ, t.ex. på myndighetens webbplats, är tillräcklig och det finns inte skäl att såsom Civil Rights Defenders förespråkar föreslå en utökad informationsskyldighet.

13 Användningen ska anmälas

Regeringens bedömning

Integritetsskyddsmyndigheten bör utses till marknadskontrollmyndighet i fråga om användning av AI-system för ansiktsigenkänning i realtid.

Det bör i förordning föreskrivas att all användning av AI-system för ansiktsigenkänning i realtid enligt den nya lagen ska anmälas till Integritetsskyddsmyndigheten.

Promemorians förslag

Förslaget i promemorian stämmer överens med regeringens bedömning.

Remissinstanserna

Ingen remissinstans invänder mot förslaget. *Integritetsskyddsmyndigheten* tillstyrker förslaget i promemorian om att myndigheten får uppdrag som marknadskontrollmyndighet.

Skälen för regeringens bedömning

AI-förordningen uppställer ett krav på att varje användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål på allmänt tillgängliga platser ska anmälas till den berörda nationella marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten, som årligen ska rapportera till kommissionen om användningen (artikel 5.4 och 5.6). Det ankommer på varje medlemsstat att utse vilken myndighet som ska vara marknadskontrollmyndighet för användning av sådana AI-system. Av artikel 74.8 följer att marknadskontrollmyndigheten bör vara den behöriga tillsynsmyndigheten för dataskydd enligt EU:s dataskyddsförordning eller dataskyddsdirektivet, eller någon annan myndighet som

har utsetts enligt de villkor som fastställs i artiklarna 41–44 i dataskyddsdirektivet.

I betänkandet Anpassningar till AI-förordningen – säker användning, effektiv kontroll och stöd för innovation (SOU 2025:101) föreslås att Integritetsskyddsmyndigheten ska utses till marknadskontrollmyndighet med ansvar bl.a. för AI-system som används inom biometri och system för biometrisk fjärridentifiering och att myndigheten därmed skulle vara den berörda myndigheten enligt artikel 5.4 och 5.6. I betänkandet föreslås vidare att regleringen av ansvaret för marknadskontroll ska ske i en förordning med kompletterande bestämmelser till AI-förordningen. Betänkandets förslag har skickats ut på remiss till den 23 februari 2026.

Integritetsskyddsmyndigheten är tillsynsmyndighet enligt både EU:s dataskyddsförordning och dataskyddsdirektivet och har samlad kompetens om behandling av personuppgifter på området för brottsbekämpning. Myndigheten har även kunskap om kamerabevakning och olika typer av teknik som används för kamerabevakning inom ramen för sitt uppdrag som tillsynsmyndighet enligt kamerabevakningslagen (se 2 och 2 a §§ förordningen [2007:975] med instruktion för Integritetsskyddsmyndigheten). Mot denna bakgrund bedömer regeringen att Integritetsskyddsmyndigheten bör utses till marknadskontrollmyndighet i fråga om användning av AI-system för ansiktsigenkänning i realtid enligt AI-förordningen, vilket alltså överensstämmer med betänkandets förslag. Detta bör regleras på förordningsnivå.

Som framgår ovan ska en anmälan om användning av AI-system för ansiktsigenkänning i realtid även göras till den nationella dataskyddsmyndigheten. Integritetsskyddsmyndigheten är nationell dataskyddsmyndighet. Myndigheten kommer således att få anmälan även i den egenskapen.

I förordning bör regleras att användning av AI-system för ansiktsigenkänning i realtid enligt den nya lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska anmälas till Integritetsskyddsmyndigheten. Enligt AI-förordningen behöver anmälan innehålla vissa uppgifter. Regeringen avser i enlighet med detta att på förordningsnivå även reglera vilka uppgifter en anmälan ska innehålla, inklusive uppgift om att användning av tekniken i förkommande fall har påbörjats utan tillstånd.

14 Behovet av följdändringar

14.1 Det krävs ändringar i offentlighets- och sekretesslagen

Regeringens förslag

Sekretess ska gälla för uppgift som hänför sig till angelägenhet som avser användning av AI-system för ansiktsigenkänning i realtid om det

kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Sekretess ska även gälla om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men.

Tystnadsplikten ska ha företräde framför rätten att meddela och offentliggöra uppgifter som hänför sig till användning av AI-system för ansiktsigenkänning i realtid.

Promemorians förslag

Förslaget i promemorian stämmer överens med regeringens.

Remissinstanserna

Den stora majoriteten av remissinstanserna har ingen invändning mot förslaget. *Journalistförbundet* och *Tidningsutgivarna* avstyrker promemorians förslag om ett omvänt skaderekvisit och föreslår i stället ett rakt skaderekvisit som möjliggör insyn. De avstyrker också promemorians förslag om att begränsa meddelarfriheten.

Skälen för regeringens förslag

Sekretess för uppgifter som avser användning av AI-system för ansiktsigenkänning i realtid

I ärenden enligt den nya lagen kommer det finnas uppgifter som, om de blir offentliga, kan äventyra syftet med användningen av AI-tekniken. Förutom uppgifter i förhållande till enskilda personer kan det också handla om uppgifter som skulle kunna äventyra pågående brottsutredningar. Det kan komma att finnas känsliga uppgifter om enskilda personer och i vilket geografiskt område personerna kan befinna sig. Med stöd av dessa uppgifter kan det gå att kartlägga en persons rörelsemönster och uppgifterna är därför mycket skyddsvärda ur integritetssynpunkt. Polis, åklagare och domstol kommer alltså hantera uppgifter inom ramen för ett ärende som behöver skyddas. Den sekretess som gäller hos myndigheterna för uppgifter som hänför sig till förundersökning i brottmål och verksamhet hos polisen för att förebygga, förhindra eller upptäcka brottslig verksamhet finns i 18 kap. 1 och 2 §§ samt 35 kap. offentlighets- och sekretesslagen. I den nya lagen föreslås att tekniken ska få användas för att söka efter personer som misstänks ha blivit utsatta för brott, förhindra allvarliga brott och lokalisera eller identifiera en person som misstänks ha begått vissa allvarliga brott i syfte att utreda eller lagföra brottet eller verkställa straffrättslig påföljd för brottet. Användning av tekniken utgör inget hemligt tvångsmedel utan är närmast en polisiär utredningsmetod. När användning av tekniken sker i syfte att förebygga, förhindra och upptäcka brottslig verksamhet bedöms uppgifter i ärendet omfattas av den befintliga sekretessregleringen i 18 kap. 2 § offentlighets- och sekretesslagen. Likaså bedöms uppgifter i ärenden som rör användning av tekniken för att utreda ett brott kunna omfattas av den befintliga sekretessregleringen i 18 kap. 1 § offentlighets- och sekretesslagen. Uppgifter i ett ärende som rör användning av tekniken för att söka efter personer för lagföring bedöms i

vissa fall kunna omfattas av den befintliga regleringen i den mån uppgifterna har generell betydelse för spaning och brottsutredning (jfr. RÅ 1989 ref. 56). För att ändamålet med användningen inte ska gå förlorat är det dock viktigt att samtliga uppgifter i ett ärende om användning av tekniken för lagföring omfattas av sekretess.

Vad gäller uppgifter i ärenden som rör användning av tekniken för att söka efter personer som misstänks ha blivit utsatta för brott eller för att verkställa straffrättslig påföljd för ett brott bedöms dessa inte alltid omfattas av sekretess enligt befintlig sekretessreglering. Den befintliga sekretessregleringen anses därmed inte ge ett tillräckligt starkt skydd för uppgifter i samtliga ärenden enligt den nya lagen. Frågan är då om det med anledning av detta finns behov av att införa en ny reglering i offentlighets- och sekretesslagen.

Rätten att ta del av allmänna handlingar får begränsas endast om det krävs med hänsyn till bl.a. intresset av att förebygga eller beivra brott eller skyddet för enskildas personliga eller ekonomiska förhållanden (2 kap. 2 § tryckfrihetsförordningen). Utgångspunkten är att offentlighet och inskränkningar i offentlighetsprincipen måste vara motiverade. För att en ny sekretessbestämmelse ska införas krävs det därför att intresset av sekretess väger tyngre än intresset av insyn. En grundläggande utgångspunkt är att den offentliga verksamheten angår alla medborgare och att den därför ska ske under allmän insyn. Myndigheternas verksamhet ska så långt som möjligt bedrivas i öppna former då detta bl.a. bidrar till att främja allmänhetens förtroende för myndigheterna. Även om användning av AI-system för ansiktsigenkänning i realtid inte utgör ett hemligt tvångsmedel gör sig samma skyddsintressen gällande i ärenden om användning av tekniken som när hemliga tvångsmedel används. Det är därför av vikt att uppgifter om användningen är sekretessreglerade hos berörda myndigheter. Ett ärende om användning av tekniken motiveras av allmänna intressen i form av att hitta brottsoffer, förhindra andra allvarliga brott samt utreda, lagföra och verkställa straffrättslig påföljd för vissa brott. Det finns ett starkt allmänt intresse av att kunna skydda uppgifter i sådana ärenden. Det finns även ett starkt enskilt skyddsintresse när det gäller de uppgifter om enskildas förhållanden som kan finnas i ett ärende. Vid en avvägning mellan sekretessintresset och intresset av insyn i myndigheternas verksamhet görs bedömningen att det är motiverat att införa regler om sekretess till skydd för allmänna och enskilda intressen.

Det är av avgörande betydelse att ärenden om användning av AI-system för ansiktsigenkänning i realtid omgärdas av sekretess hos berörda myndigheter för att tekniken ska kunna användas effektivt. I detta avseende saknar det betydelse för vilket syfte som användningen sker. Det finns därmed ett behov av en sekretessreglering som träffar uppgifter i alla ärenden enligt den nya lagen. Ärendena kommer i huvudsak att följa samma regler som vid användning av hemlig övervakning av elektronisk kommunikation. Eftersom skyddsintressena är desamma är det lämpligt och ändamålsenligt att samma sekretess och terminologi även ska gälla för sekretess vid användning av AI-system för ansiktsigenkänning i realtid enligt den nya lagen. Det bör därmed införas en ändring i 18 kap. 1 § offentlighets- och sekretesslagen.

Det föreslås att sekretess ska gälla för uppgift som hänför sig till angelägenhet som avser användning av tekniken enligt den nya lagen, om

det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. I likhet med vad som gäller för användning av hemliga tvångsmedel i brottmål gäller sekretess med ett rakt skaderekvisit, vilket innebär en presumtion för offentlighet. Eftersom sekretess gäller för uppgift som hänför sig till angelägenhet som avser användning av tekniken enligt den nya lagen följer sekretessen med uppgiften när den lämnas vidare till en annan myndighet. Ett exempel på när uppgifter inte längre bör omfattas av sekretess är när den person som avses att lokaliseras eller identifieras har hittats, om uppgifterna inte har generell betydelse för brottsspaning och brottsutredning.

För uppgift i en allmän handling gäller sekretessen enligt 18 kap. 1 § offentlighets- och sekretesslagen i högst fyrtio år (se 18 kap. 1 § tredje stycket offentlighets- och sekretesslagen).

När användning av tekniken sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet kommer uppgifter, enligt den föreslagna ändringen, omfattas av sekretess både enligt 18 kap. 1 och 2 §§ offentlighets- och sekretesslagen. Vid konkurrens mellan flera olika tillämpliga sekretessbestämmelser är det den bestämmelsen som ger det starkaste skyddet för uppgiften som får fälla utslaget (jfr 7 kap. 3 § offentlighets- och sekretesslagen och prop. 1979/80:2 Del A s. 70). När tekniken används i syfte att förebygga, förhindra och upptäcka brottslig verksamhet bör en prövning om uppgifter kan offentliggöras därför göras med stöd av 18 kap. 2 § offentlighets- och sekretesslagen. Detta innebär att uppgifterna omfattas av sekretess om det inte står klart att uppgifterna kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas.

I ett ärende enligt den nya lagen kan känsliga uppgifter om en enskilds personliga förhållanden förekomma varför behovet av skydd är detsamma för enskilda oavsett för vilket syfte tekniken har använts. I promemorian föreslås därför att det bör införas en ändring i 35 kap. 1 § offentlighets- och sekretesslagen. Sekretess bör gälla om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i angelägenhet som avser användning av AI-system för ansiktsigenkänning i realtid. Sekretess skulle därmed gälla för sådana uppgifter med ett omvänt skaderekvisit, vilket innebär en presumtion för sekretess. *Journalistförbundet* och *Tidningsutgivarna* avstyrker att förslaget ska ha ett omvänt skaderekvisit. Journalistförbundets erfarenhet av omvända skaderekvisit är att de i praktiken tillämpas som absolut sekretess. Som framgår ovan föreligger ett behov av sekretess för sådana uppgifter som är aktuella. Dessutom följer sekretessens styrka det som normalt gäller hos myndigheterna för uppgifter som hänför sig till verksamhet hos polisen för att förebygga, förhindra eller upptäcka brottslig verksamhet och vad gäller skydd för enskilda. Regeringen anser därför att en sådan bestämmelse, med omvänt skaderekvisit, som föreslås i promemorian bör införas.

Av 35 kap. 1 § andra stycket offentlighets- och sekretesslagen följer att om uppgifterna förekommer i angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder gäller hos domstolar ett rakt skaderekvisit, dvs.

det råder en presumtion för att uppgifterna är offentliga. Enligt regeringen bör samma sekretess gälla för uppgifter som förekommer i angelägenhet som avser användning av AI-system för ansiktsigenkänning i realtid. En sådan ändring bör därför införas.

För uppgift i en allmän handling gäller sekretessen enligt 35 kap. 1 § offentlighets- och sekretesslagen i högst sjuttio år (se 35 kap 1 § fjärde stycket offentlighets- och sekretesslagen).

Utifrån det sekretessbehov som finns bör sekretessbestämmelserna placeras i anslutning till nuvarande bestämmelser som avser sekretess vid förundersökningar m.m., dvs. genom ett tillägg till 18 kap. 1 § första stycket och 35 kap. 1 § första och andra stycket offentlighets- och sekretesslagen.

Tystnadsplikten ska ha företräde framför rätten att meddela och offentliggöra uppgifter

Av 3 kap. 1 § offentlighets- och sekretesslagen följer att sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt. Sekretess innebär alltså både en handlingssekretess och en tystnadsplikt.

Den rätt att meddela och offentliggöra uppgifter som följer av 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen har som huvudregel företräde framför tystnadsplikten. Det kan alltså vara tillåtet att t.ex. muntligen lämna en uppgift till en journalist eller att själv publicera uppgiften, men det är aldrig tillåtet att med stöd av rätten att meddela och offentliggöra uppgiften lämna den allmänna handling där den sekretessbelagda uppgiften framgår till t.ex. en journalist. I ett antal fall har emellertid även bestämmelser om tystnadsplikt företräde framför rätten att meddela och offentliggöra uppgifter. Enligt 18 kap. 19 § andra stycket offentlighets- och sekretesslagen inskränker tystnadsplikten enligt bl.a. 18 kap. 1 § rätten att meddela och offentliggöra uppgift om angelägenhet som avser användning av tvångsmedel i brottsmål, som exempelvis hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning. Sådana uppgifter är delvis jämförbara med nu aktuella uppgifter.

Uppgifter om användning av AI-system för ansiktsigenkänning i realtid är mycket känsliga och röjande av sådana uppgifter skulle kunna leda till stor skada. Det kan bl.a. medföra att en gärningsperson som begått ett allvarligt brott inte kan lokaliseras eller att ett hot om skada mot människors liv och säkerhet realiseras. Även med beaktande av den restriktivitet som ska gälla vid inskränkningar av rätten att meddela och offentliggöra uppgifter är det, i motsats till vad *Journalistförbundet* och *Tidningsutgivarna* anser, motiverat att låta sekretessen begränsa meddelarfriheten. För att meddelarfriheten inte ska gälla krävs en justering i 18 kap. 19 § andra stycket offentlighets- och sekretesslagen.

Den föreslagna placeringen innebär att sekretessen kommer att gälla i annan verksamhet än sådan som avses i 18 kap. 1 och 2 §§ hos en myndighet för att biträda exempelvis en åklagarmyndighet, Polismyndigheten eller Säkerhetspolisen med att förebygga, uppdaga, utreda eller beivra brott (18 kap. 3 § offentlighets- och sekretesslagen). Ett av syftena med sekretess till skydd för brottsutredande verksamhet är att uppgifterna ska

skyddas oavsett var de finns. Uppgifter i sådan verksamhet har samma skyddsbehov oavsett hos vilken myndighet uppgifterna förekommer. Säkerhetspolisen kan exempelvis i vissa fall bistå vid polisverksamhet som leds av Polismyndigheten och i enskilda fall kan Polismyndigheten lämna över en förundersökning eller annan liknande uppgift i den brottsbekämpande verksamheten till Säkerhetspolisen för fortsatt handläggning (13 § förordningen med instruktion för Säkerhetspolisen och 27 § förordningen med instruktion för Polismyndigheten).

14.2 AI-system för ansiktsigenkänning i realtid ska få användas inom det internationella straffrättsliga samarbetet

Regeringens förslag

AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska få användas för att lokalisera en person som är anhållen eller häktad i ett ärende om överlämnande eller utlämning i syfte att verkställa frihetsberövandet. Tekniken ska också få användas inom ramen för det internationella straffrättsliga samarbetet för bevisinhämtning.

Promemorians förslag

Förslaget i promemorian stämmer i huvudsak överens med regeringens. I promemorian föreslås att åklagaren själv ska kunna besluta om användning av AI-system för ansiktsigenkänning i realtid om det är fara i dröjsmål och att användningen ska kunna ske även enligt bestämmelserna i den nya lagen som avser lokalisering eller identifiering av en dömd person.

Remissinstanserna

Åklagarmyndigheten anser att det saknas skäl att införa särskilda regler om användning av AI-system för ansiktsigenkänning i realtid i lagarna som reglerar överlämnande och utlämning. Övriga remissinstanser har ingen invändning eller yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Överlämnande och utlämning

Brottsligheten blir alltmer gränsöverskridande. Detta gäller inte minst den organiserade brottsligheten. Det förekommer att kriminella gömmer sig både i Sverige och i andra länder, i synnerhet inom Schengenområdet. Det är därför viktigt att svensk polis kan få hjälp av andra länders myndigheter att lokalisera personer som gömmer sig utanför Sveriges gränser, och att svensk polis effektivt kan söka efter personer i Sverige som eftersöks av polisen i andra länder.

AI-system för ansiktsigenkänning i realtid är en mycket effektiv metod för att hitta en person och det föreslås nu att svensk polis ska få använda

tekniken i syfte att lagföra eller verkställa en straffrättslig påföljd för vissa allvarliga brott. Det bör vara möjligt att använda samma utredningsåtgärd inom ramen för det internationella straffrättsliga samarbetet i syfte att hitta en eftersökt person när det gäller ett ärende om överlämnande enligt lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder, lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder eller lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket. Detsamma bör gälla när det är fråga om ett ärende enligt lagen (1957:668) om utlämning för brott.

Det kan inledningsvis konstateras att det i nyss nämnda lagar i princip inte görs någon skillnad på om överlämnande eller utlämning begärs på grund av lagföring eller straffverkställighet. I lagarna finns särskilda bestämmelser om tvångsmedel rörande anhållande och häktning vid utlämning eller överlämnande på grund av lagföring eller straffverkställighet. I situationer som inte omfattas av de särskilda reglerna om tvångsmedel i dessa lagar tillämpas rättegångsbalkens regler om förundersökning. Bland annat anges i 4 kap. 3 § andra stycket lagen om överlämnande från Sverige enligt en europeisk arresteringsorder att bestämmelserna om förundersökning i brottmål ska tillämpas vid utredningen av om det finns förutsättningar för överlämnande från Sverige, om inte annat anges i lagen. Det kan exempelvis handla om utredningsåtgärder för att verkställa ett beslut om anhållande eller häktning vid överlämnande för lagföring eller straffverkställighet och som fattats med stöd av de särskilda bestämmelserna i lagen. Då kan det bli aktuellt att t.ex. använda hemliga tvångsmedel enligt 27 kap. rättegångsbalken eller vidta en husrannsakan enligt 28 kap. rättegångsbalken för att leta efter den eftersökte (se hänvisning i 23 kap. 16 § rättegångsbalken till bestämmelserna om tvångsmedel i 24–28 kap. rättegångsbalken). I propositionen Bättre möjligheter att verkställa frihetsberövanden (prop. 2023/24:108) konstaterade regeringen att även 27 kap. 19 c § rättegångsbalken skulle kunna tillämpas på motsvarande sätt för att lokalisera den som anhållits eller häktats i ett ärende om överlämnande eller utlämning utan ytterligare författningsändringar (s. 45 f).

AI-system för ansiktsigenkänning i realtid bör också kunna tillämpas för att lokalisera någon som anhållits eller häktats i ett överlämnande- eller utlämningsärende i syfte att verkställa frihetsberövandet eftersom anhållandet eller häktningen avser en person som eftersöks i Sverige på grund av brottsmisstankar eller domar i andra länder. Användningen kommer således att tillämpas inom ramen för utredningen av om det finns förutsättningar för överlämnande eller utlämnande från Sverige och bör därför endast, till skillnad från vad som föreslås i promemorian, ske i enlighet med regleringen i 4 § 4 i den nya lagen. Detta ska dock bara kunna ske om den gärning som ligger till grund för begäran om utlämning eller överlämnande motsvaras av ett brott som omfattas av lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. *Lagrådet* påpekar att det inte framgår om beslut att använda tekniken ska fattas av rätten eller av åklagare. Regeringen konstaterar att beslut fattas av rätten vilket följer av att användningen endast kan ske i enlighet med den föreslagna 4 § 4 i den nya lagen. Det bör även förtydligas i författningskommentaren.

I promemorian föreslås att lagarna om överlämnande och utlämning kompletteras med regler som uttryckligen gör den nu aktuella tekniken tillgänglig i det internationella straffrättsliga samarbetet. *Åklagarmyndigheten* hänvisar till vissa uttalanden i propositionen Bättre möjligheter att verkställa frihetsberövanden och menar att de ska uppfattas så att – i den mån dessa lagar inte anger annat – de nationella verktygen alltid är tillgängliga för att leta efter den som eftersöks. I konsekvens med det anser Åklagarmyndigheten att det inte finns skäl att införa särskilda regler i dessa lagar om användning av AI-system för ansiktsigenkänning i realtid. Som beskrivs ovan innehåller lagarna om överlämnande och utlämning en uttrycklig reglering om att bestämmelserna om förundersökning i brottsmål ska tillämpas vid utredningen om inte annat anges i lagen. De nya bestämmelserna om användning av AI-system för ansiktsigenkänning i realtid avser inte särskilt den situationen att en person som anhållits eller häktats ska lokaliseras för att verkställa frihetsberövandet. Vidare är användningen av AI-system för ansiktsigenkänning i realtid närmast en polisiär utredningsmetod som är ny och placeras i en särskild ny lag. Regeringen anser därför, till skillnad från Åklagarmyndigheten, att det behövs en uttrycklig reglering i lagarna om överlämnande och utlämning för att den nu aktuella tekniken ska kunna tillämpas för att lokalisera någon som anhållits eller häktats i ett överlämnande- eller utlämningsärende.

Sammantaget bör det därför införas en reglering i nämnda lagar som möjliggör användning av AI-system för ansiktsigenkänning i realtid för att lokalisera någon som anhållits eller häktats i ett ärende om överlämnande eller utlämning i syfte att verkställa frihetsberövandet. Användningen bör ske enligt de förutsättningar som anges i den nya lagen och de föreskrifter som har meddelats i anslutning till lagen med undantag för bestämmelserna om forum som ska följa av ovan angivna lagar.

Bevisinhämtning

Bevisinhämtning i en annan stat eller i Sverige under en pågående brottsutredning eller en rättegång i brottmål är många gånger av stor betydelse, bl.a. vid utredning av grov organiserad brottslighet. Det bör därför vara möjligt att på samma sätt som i en svensk förundersökning eller rättegång använda AI-system för ansiktsigenkänning i realtid inom ramen för det internationella straffrättsliga samarbetet för bevisinhämtning enligt lagen (2017:1000) om en europeisk utredningsorder och lagen (2000:562) om internationell rättslig hjälp i brottmål. Det bör därför införas bestämmelser i nämnda lagar som möjliggör användning av AI-system för ansiktsigenkänning i realtid för bevisinhämtning.

Användning av AI-system för ansiktsigenkänning i realtid finns inte med i förteckningen över vilka åtgärder som rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål omfattar. Ett tillägg behöver därför göras i förteckningen.

På motsvarande sätt som gäller för hemliga tvångsmedel bör därför rättslig hjälp med användning av AI-system för ansiktsigenkänning i realtid lämnas under de förutsättningar som gäller för åtgärden i en svensk förundersökning (2 kap. 1 § första stycket lagen om internationell rättslig hjälp i brottmål). Det bör dessutom ställas upp ett krav på dubbel straffbarhet, dvs. den gärning som avses i den utländska brottsutredningen ska

vara straffbar i Sverige (2 kap. 2 § lagen om internationell rättslig hjälp i brottmål). Detta innebär att förutsättningarna i den föreslagna lagen om användning av AI-system för ansiktsigenkänning i realtid ska vara uppfyllda för att rättslig hjälp ska få lämnas.

Det bör dessutom framgå av lagen att rättslig hjälp endast får lämnas för de åtgärder som enligt lagen om AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål avser bevisinhämtning. En sådan bestämmelse bör införas i lagens fjärde kapitel om särskilda bestämmelser om olika former av rättslig hjälp.

Som anges ovan finns skäl att i så stor utsträckning som möjligt låta de gällande bestämmelserna om rättslig hjälp i Sverige med hemliga tvångsmedel bilda utgångspunkt vid utformningen av reglerna om användning av AI-system för ansiktsigenkänning i realtid. I enlighet med detta bör en ansökan om användning av AI-system för ansiktsigenkänning i realtid för någon som befinner sig i Sverige handläggas av åklagare. Samma skyndsamhetskrav som finns beträffande åklagarens prövning och överlämnande till rätten som gäller för de hemliga tvångsmedlen bör också gälla. Det bör därför föreskrivas att åklagaren genast ska pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd. Det bör även i lagen om internationell rättslig hjälp i brottmål föreskrivas en möjlighet att påbörja användning av AI-system för ansiktsigenkänning i realtid innan rätten fattat beslut. I lagrådsremissens lagtextförslag anges att vissa bestämmelser i lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål som gäller användning utan tillstånd är tillämpliga. *Lagrådet* påpekar att det inte är tydligt vem som beslutar om sådan användning och inte heller om regleringen i den nya lagen som gäller radering av uppgifter ska tillämpas. Regeringen konstaterar att det är polisen som får påbörja användning utan tillstånd. Det följer av att det i lagtexten finns en hänvisning till en bestämmelse i den nya lagen. Det bör tydliggöras att om användning påbörjas utan tillstånd får återredovisning till det ansökande landet inte ske förrän domstol fattat beslut att tillåta åtgärden. Det bör också tydliggöras i lagtexten att regleringen om radering är tillämplig i nu aktuella fall.

När det gäller underrättelse till enskilda bör samma ordning gälla vid rättslig hjälp med användning av AI-system för ansiktsigenkänning i realtid som gäller vid rättslig hjälp med hemliga tvångsmedel enligt lagen om internationell rättslig hjälp i brottmål. Det kan enklast åstadkommas genom en direkt hänvisning till vad som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 § tredje stycket. Eftersom användning av tekniken inte är ett hemligt tvångsmedel bör det dock inte ankomma på åklagaren att informera Myndigheten för säkerhet och integritetsskydd om en underrättelse inte har lämnats.

Enligt lagen om internationell rättslig hjälp i brottmål får åklagare ansöka om rättslig hjälp med användning av hemliga tvångsmedel av någon som befinner sig i en annan stat. Vidare anges att om den anmodade staten kräver att åklagarens ansökan först ska prövas av domstol i Sverige får en svensk domstol, på åklagarens begäran, pröva frågan om att tillåta hemliga tvångsmedel. Motsvarande bör gälla för rättslig hjälp med användning av AI-system för ansiktsigenkänning i realtid. Någon

underrättelse till enskilda behöver dock inte lämnas eftersom den andra staten vidtar åtgärden.

För att omfattas av lagen om en europeisk utredningsorder bör användning av AI-system för ansiktsigenkänning i realtid tas in i förteckningen i 1 kap. 4 § lagen om en europeisk utredningsorder, vilken definierar vilka utredningsåtgärder som en europeisk utredningsorder ska avse eller motsvara. Som en följd av att åtgärden tas in som en utredningsåtgärd i lagen behövs vissa följdändringar.

Även om användning av AI-system för ansiktsigenkänning i realtid är närmast en polisiär utredningsmetod tillämpas en tillståndsprövning likt den för hemliga tvångsmedel. En ordning där det krävs domstolsprövning innan en utredningsorder kan utfärdas (2 kap. 5 § första stycket 2) bör därför även gälla för denna utredningsmetod. För hemliga tvångsmedel finns det en möjlighet för åklagaren att i avvaktan på domstolens beslut fatta ett interimistiskt beslut om en utredningsåtgärd (2 kap. 5 § andra stycket). Någon sådan möjlighet finns inte för åklagaren när det gäller användning av AI-system för ansiktsigenkänning i realtid enligt den nya lagen. Därför bör det inte heller, till skillnad från vad som föreslås i promemorian, vara möjligt för åklagaren att fatta ett sådant beslut inom ramen för en europeisk utredningsorder.

För vissa utredningsåtgärder finns särskilda bestämmelser i lagen om en europeisk utredningsorder beträffande vad som gäller för åtgärden när den ska eller har utfärdats i Sverige (2 kap. 9–19 b §§). En europeisk utredningsorder kan endast vidtas i syfte att inhämta bevis, varför det bör framgå av en särskild bestämmelse att en utredningsorder endast får utfärdas för de åtgärder som enligt lagen om AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål avser bevisinhämtning. För hemliga tvångsmedel finns även särskilda bestämmelser om att rätten eller åklagaren omedelbart ska häva ett beslut om det inte finns skäl för det. Enligt den föreslagna lagen om AI-system för ansiktsigenkänning ska en åtgärd omedelbart hävas om det inte längre finns skäl för den. Att åklagare omedelbart ska häva ett beslut om det inte längre finns skäl för det bör gälla även vid utfärdande av en utredningsorder och en sådan bestämmelse bör införas.

I 3 kap. lagen om en europeisk utredningsorder finns bestämmelser som erkännande och verkställighet i Sverige av en europeisk utredningsorder. För utredningsåtgärder som innebär en kontinuerlig bevisinhämtning i realtid och under en viss tidsperiod får det uppställas krav på att en sådan åtgärd får vägras om verkställigheten av den berörda utredningsåtgärden inte skulle vara tillåten i ett liknande inhemskt ärende enligt artikel 28 i Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området. Ett sådant krav har uppställts för hemlig kameraövervakning och hemlig rumsavlyssning och bör även tillämpas för en utredningsorder som avser användning av AI-system för ansiktsigenkänning i realtid. Det innebär att förutsättningarna i den föreslagna lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska vara uppfyllda för att en utredningsorder som avser användning av AI-system för ansiktsigenkänning i realtid ska få erkännas och verkställas i Sverige. En hänvisning till den aktuella utredningsåtgärden ska därför införas i 3 kap. 4 §.

Även när det gäller erkännande och verkställande i Sverige av en europeisk utredningsorder från en annan medlemsstat bör domstolsprövning föregå utredningsordern eftersom det är ett krav i motsvarande situation i Sverige. Vid hemliga tvångsmedel får åklagaren i avvaktan på domstolens beslut, under de förutsättningar som gäller enligt rättegångsbalken, besluta att erkänna och verkställa en utredningsorder rörande hemliga tvångsmedel (3 kap. 10 §). Någon sådan möjlighet har inte åklagaren vid användning av AI-system för ansiktsigenkänning i realtid enligt den nya lagen. Åklagaren bör därför inte heller, till skillnad från vad som föreslås i promemorian, ha en sådan möjlighet vid erkännande och verkställighet av en utredningsorder.

I den föreslagna lagen om användning av AI-system för ansiktsigenkänning föreslås att den som har varit föremål för ett beslut om sådan användning som gäller en brottsutredning eller lagföring ska underrättas om åtgärden. Detta bör gälla även när tekniken används inom ramen för en utredningsorder. I likhet med vad som gäller för hemliga tvångsmedel bör de bestämmelser som reglerar underrättelse i lagen om en europeisk utredningsorder gälla i stället för de som föreslås i den nya lagen och föreskrifter som har meddelats i anslutning till lagen. Eftersom användning av tekniken inte är ett hemligt tvångsmedel bör det dock inte ankomma på åklagaren att informera Myndigheten för säkerhet och integritetsskydd om en underrättelse inte har lämnats.

14.3 Det behöver inte göras någon ändring i befintlig dataskyddsreglering eller i kamerabevakningslagen

Regeringens bedömning

Det behövs inte någon ytterligare reglering för den personuppgiftsbehandling som lagförslagen ger upphov till. Det krävs inte heller några ändringar i kamerabevakningslagen.

Promemorians bedömning

Bedömningen i promemorian stämmer överens med regeringens.

Remissinstanserna

Den stora majoriteten av remissinstanserna har ingen invändning mot förslaget. *Försvarsmakten* har inte några synpunkter på förslaget men vill påtala vikten av hög informationssäkerhet vid såväl kamerabevakning som användning av AI-system. *Diskrimineringsombudsmannen* noterar att behovet av eventuella anpassningar i svensk rätt i förhållande till flera bestämmelser i AI-förordningen som t.ex. AI med hög risk och hur utdata får användas inte har behandlats i promemorian. *Integritetsskyddsmyndigheten* föreslår att det i lagförslaget förs in ett undantag från sökförbudet avseende känsliga personuppgifter i

brottsdatalagen. *Myndigheten för säkerhet och integritetsskydd* för fram liknande synpunkter.

Skälen för regeringens bedömning

Det finns rättslig grund för personuppgiftsbehandlingen

Brottsdatalagen innehåller övergripande och grundläggande bestämmelser om polisens behandling av personuppgifter. Enligt lagen, som genomför dataskyddsdirektivet, får Polismyndigheten och Säkerhetspolisen i sin brottsbekämpande verksamhet, som inte avser nationell säkerhet, bl.a. behandla personuppgifter för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder (1 kap. 2 och 4 §§ brottsdatalagen). En mer detaljerad reglering finns i polisens brottsdatalag, som gäller för polisens personuppgiftsbehandling som sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa uppbörd eller upprätthålla allmän ordning och säkerhet. Enligt lagen får polisen behandla personuppgifter om det är nödvändigt bl.a. för att kunna förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott (2 kap. 1 § polisens brottsdatalag).

När ett AI-system för ansiktsigenkänning i realtid används sker en behandling av personuppgifter. Den form av personuppgifter som det är fråga om är biometriska uppgifter och dessa hör till kategorin känsliga personuppgifter. Behandlingen av personuppgifter som kommer att ske inom ramen för användning av tekniken kan innebära vissa risker för den personliga integriteten. Riskerna består bl.a. i att det finns en större möjlighet att kartlägga var en viss person befinner sig. En annan risk är att personuppgiftsbehandlingen i vissa fall kan omfatta ett större antal personer. Förslagen i denna proposition är dock sådana att det ställs höga krav för att använda AI-system för biometrisk fjärridentiering i realtid. Exempelvis får användning endast ske om det är absolut nödvändigt för att lokalisera eller identifiera en person och då för vissa bestämda syften. I ett beslut om tillstånd till användning får tiden inte bestämmas längre än vad som är absolut nödvändigt och området eller områdena får inte vara mer omfattande än vad som är absolut nödvändigt. I föregående avsnitt konstateras att uppgifter i ett ärende om användning av tekniken, beroende på i vilken verksamhet det sker inom, omfattas av sekretess och i de fall de inte bedöms göra det föreslås nya bestämmelser om sekretess. Sekretessregleringen minskar risken för att uppgifterna ska få spridning som kan få negativ påverkan på den personliga integriteten. Sammantaget minskar dessa bestämmelser risken för onödigt intrång i den personliga integriteten.

Polisen får behandla biometriska uppgifter endast om det är särskilt föreskrivet och det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 12 § brottsdatalagen). En sådan särskild föreskrift finns i 2 kap. 4 § polisens brottsdatalag. Den ger stöd för polisen att behandla biometriska uppgifter om det görs för ett syfte som anges i lagen (se 2 kap. 1 § polisens brottsdatalag). Det innebär att det finns rättsligt stöd för polisen att inom ramen för användning av AI-system för ansiktsigenkänning i realtid behandla biometriska uppgifter om det sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott.

Polisens brottsdatalag gäller inte för behandling av personuppgifter som sker inom ramen för verkställighet av straffrättslig påföljd. Frågan är då om lagen bör utvidgas till att omfatta även sådan personuppgiftsbehandling. Det skulle få vissa följder, bl.a. skulle reglerna om gemensamt tillgängliga uppgifter bli tillämpliga för sådan behandling. Vilka effekter det skulle få kan inte överblickas inom ramen för denna proposition. Det är dock nödvändigt att det finns rättsligt stöd för polisen att kunna behandla biometriska uppgifter för samtliga syften som AI-system för ansiktsigenkänning i realtid föreslås få användas för. I avsnitt 7.1 föreslås en uttrycklig bestämmelse som ger polisen rätt att använda AI-system för ansiktsigenkänning i realtid i syfte att verkställa straffrättslig påföljd. Den föreslagna bestämmelsen bedöms utgöra en sådan särskild föreskrift som möjliggör för polisen att behandla biometriska uppgifter när tekniken används för att verkställa straffrättslig påföljd.

Polisens brottsdatalag innehåller ett flertal bestämmelser som minskar integritetsriskerna och dessa är tillämpliga även vid behandling av personuppgifter när AI-system för ansiktsigenkänning i realtid används. Som exempel kan nämnas bestämmelser om begränsningar vad gäller direktåtkomst (2 kap. 12 §), bestämmelser om s.k. gemensamt tillgängliga uppgifter (3 kap.) och bestämmelser om längsta tid som personuppgifter får behandlas (4 kap). Med anledning av det som *Försvarsmakten* för fram om vikten av informationssäkerhet vill regeringen betona att det följer av brottsdatalagen att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas, särskilt mot obehörig eller otillåten behandling och mot förlust, förstöring eller annan oavsiktlig skada (3 kap. 8 § brottsdatalagen).

Det ska också framhållas att den personuppgiftsansvarige, här ofta Polismyndigheten, alltid är skyldig att se till att tillgången till personuppgifter begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter (3 kap. 6 § brottsdatalagen). Därutöver ska när myndigheten tilldelar behörighet för åtkomst till personuppgifter särskilt beaktas behovet av uppgifterna, utbildning och erfarenhet (3 kap. 5 § brottsdataförordningen [2018:1202]). Myndigheten ska även ha rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter (3 kap. 6 § samma förordning). Vidare ska den personuppgiftsansvarige säkerställa att det i automatiserade behandlingssystem förs loggar över personuppgiftsbehandling i den utsträckning det är särskilt föreskrivet (3 kap. 5 § brottsdatalagen). Med logg avses en behandlingshistorik som sparas viss tid. Det är en teknisk funktion som ska fungera automatiskt och som inte ska gå att ändra eller påverka på annat sätt (se Lindberg, brottsdatalagen, 3 kap. 5 §, Karnov 2025-11-17 [JUNO]). Skyldigheten att föra loggar preciseras i 3 kap. 4 § brottsdataförordningen. Denna reglering motverkar otillbörliga intrång i de registrerades rättigheter.

Diskrimineringsombudsmannen noterar att behovet av eventuella anpassningar i svensk rätt i förhållande till flera bestämmelser i AI-förordningen som t.ex. AI med hög risk och hur utdata får användas inte har behandlats i promemorian. Regeringen kan konstatera att det sker en behandling av personuppgifter när ett AI-system för ansiktsigenkänning i realtid används. Som framgår ovan finns regler om personuppgiftsbehandlingen i framför allt polisens brottsdatalag. Regleringen gäller också

behandlingen av utdata. Frågan om utdata hanteras vidare i avsnitt 10 där det föreslås att om ett tillstånd nekas ska användningen stoppas med omedelbar verkan och alla uppgifter samt resultat och utdata som rör denna användning förstöras och raderas. Dessutom föreskriver AI-förordningen, som är direkt tillämplig, att beslut som har negativa rättsliga följder för en person inte får fattas enbart på grundval av utdata från AI-system för ansiktsigenkänning i realtid (artikel 5.3), se avsnitt 15.2. När det gäller behovet av anpassningar i svensk rätt i förhållande till andra bestämmelser i AI-förordningen, t.ex. om AI med hög risk, behandlas dessa i betänkandet Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation (SOU 2025:101) som för närvarande bereds i Regeringskansliet.

Integritetsskyddsmyndigheten föreslår att det inför ett undantag från förbudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter i 2 kap. 14 § brottsdatalagen. Som stöd för att det behövs en sådan reglering hänvisar myndigheten till uttalanden i propositionen Biometri i brottsbekämpningen (prop. 2024/25:37 s. 145 f.). Även *Myndigheten för säkerhet och integritetsskydd* efterfrågar resonemang och bedömning kring frågan om användningen av tekniken medför sådan behandling av biometriska uppgifter som aktualiserar ett behov av undantag från sökförbudet. Vid införandet av polisens brottsdatalag konstaterades att behandling av biometriska uppgifter i ett ansiktsigenkänningsprogram inte kan anses motsvara en sökning i syfte att få fram ett visst urval av personer, utan måste ses som en sådan normal behandling av biometriska uppgifter som är tillåten om den är absolut nödvändig för ändamålet med behandlingen (prop. 2017/18:269 s. 156). I den proposition som Integritetsskyddsmyndigheten hänvisar till angav regeringen dock att det behövs ett undantag från sökförbudet för att möjliggöra biometriska jämförelser i Migrationsverkets register över fingeravtryck och fotografier. Till skillnad från det lagförslaget innebär det nu aktuella förslaget om användning av AI-system för ansiktsigenkänning i realtid emellertid inte att det sker någon sökning i ett register. Den typ av behandling som är aktuell måste i stället ses som en sådan normal behandling av biometriska uppgifter som avses i prop. 2017/18:269 och som är tillåten om den är absolut nödvändig för ändamålet med behandlingen. Det finns därför inte något behov av ett sådant undantag från sökförbudet som Integritetsskyddsmyndigheten föreslår.

Polisen har ett stort behov av att använda AI-system för ansiktsigenkänning i realtid för att effektivt kunna bekämpa brott. Med hänsyn till de skyddsåtgärder som finns i dataskyddsregleringen bedöms behandlingen av biometriska uppgifter som användning av tekniken ger upphov till inte medföra en oproportionerlig börda för de personer som berörs av den i förhållande till det eftersträvade målet att bekämpa och lagföra allvarliga brott och verkställa straffrättsliga påföljder för sådana brott.

Mot denna bakgrund bedöms de författningsförslag som lämnas i denna proposition inte kräva några ändringar i polisens brottsdatalag eller annan dataskyddsreglering.

För att kunna använda AI-system för ansiktsigenkänning i realtid krävs att det exempelvis finns en kamera uppsatt på den eller de platser som tekniken ska användas. För varaktig eller regelbundet upprepad personbevakning gäller kamerabevakningslagen. Lagen är till stora delar ett komplement till de allmänna reglerna om behandling av personuppgifter. Syftet med kamerabevakningslagen är att tillgodose behovet av kamerabevakning för berättigade ändamål och att skydda människor mot otillbörligt intrång i den personliga integriteten vid sådan bevakning. Ändringar i kamerabevakningslagen har nyligen genomförts, se propositionen Kamerabevakning i brottsbekämpning och annan offentlig verksamhet – utökade möjligheter och ett enklare förfarande (prop. 2024/25:93). Förslagen trädde i kraft under våren 2025. Enligt förslagen får polisen bedriva kamerabevakning om det är nödvändigt för de ändamål som anges i brottsdatalagen eller Säkerhetspolisens brottsdatalag. Innan kamerabevakningen påbörjas ska polisen göra en dokumenterad intresseavvägning. Kamerabevakning får endast bedrivas om intresset av bevakningen väger tyngre än den enskildes intresse av att inte bli bevakad. Vid bedömningen ska det särskilt beaktas bl.a. hur bevakningen ska utföras, om teknik som ökar risken för integritetsintrång som exempelvis AI-system för ansiktsigenkänning i realtid ska användas. En intresseavvägning ska även göras innan bevakningen ändras på ett betydande sätt som ökar risken för intrång i den enskildes personliga integritet. Polisen kan alltså innan en kamera sätts upp beakta om viss teknik kan komma att användas på kameran. Om polisen i sin intresseavvägning har beaktat detta bör det inte krävas någon ny intresseavvägning innan polisen kan använda tekniken. Om tekniken däremot ska användas på en befintlig kamera som satts upp utan att det i intresseavvägningen har beaktats att tekniken kan komma att användas ska polisen göra en ny intresseavvägning. I de fall som polisen har möjlighet att bedriva kamerabevakning utan att det krävs att en intresseavvägning görs bör det inte finnas några hinder mot att polisen använder tekniken.

Mot denna bakgrund bedöms de förslag som lämnas i denna proposition inte föranleda något behov av ändringar i kamerabevakningslagen.

15 Förslagens förenlighet med grundläggande fri- och rättigheter

15.1 Inledning

Staten har en skyldighet att skydda mot obefogade intrång i enskildas grundläggande fri- och rättigheter. Detta gäller intrång som görs av offentliga aktörer men även intrång som sker av andra enskilda. När en enskild utsätts för brott behöver staten se till att brottet utreds. En förutsättning för att kunna upprätthålla rättstryggheten för enskilda är att det finns en välfungerande och effektiv brottsbekämpning. Detta innebär

exempelvis att de brottsbekämpande myndigheterna behöver ha tillgång till effektiva utredningsverktyg. Staten har dock en skyldighet att säkerställa att de verktyg som de brottsbekämpande myndigheterna har tillgång till används på ett sätt som är förenligt med grundläggande fri- och rättigheter. Om de brottsbekämpande myndigheterna ska ges nya verktyg som kan innebära intrång i grundläggande fri- och rättigheter behöver därför noggranna avvägningar göras utifrån behovet av en effektiv brottsbekämpning och proportionalitet samt nödvändighet. I detta avsnitt görs en analys av om de förslag som lämnas i denna proposition är förenliga med enskildas grundläggande fri- och rättigheter.

15.2 Förslagen är förenliga med grundläggande fri- och rättigheter

Regeringens bedömning

Den föreslagna regleringen utgör en rimlig avvägning mellan behovet av effektiva verktyg i brottsbekämpningen och den enskildes rätt till skydd för sin personliga integritet och sitt privatliv.

Promemorians bedömning

Bedömningen i promemorian stämmer överens med regeringens.

Remissinstanserna

De flesta av remissinstanserna har ingen invändning mot promemorians bedömning. *Riksdagens ombudsmän* (JO) anser att de förslag som lämnas i promemorian synes innefatta godtagbara rättssäkerhetsgarantier för de personer som blir föremål för beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid. Enligt JO behöver dock risken för att enskilda kan komma att avstå från att utöva grundlagsstadgade rättigheter, som exempelvis mötesfriheten, belysas ytterligare. Enligt *Integritetsskyddsmyndigheten* bör det övervägas om inte förbudet i AI-förordningen om att inget beslut som har negativa rättsliga följder för en person får fattas enbart på grundval av utdata från system för biometrisk fjärridentifiering ska tas in i den svenska lagen i förtydligande syfte. *Säkerhets- och integritetsskyddsmyndigheten* för fram motsvarande synpunkter. *Diskrimineringsombudsmannen* instämmer i och för sig i behovet av att ge polisen utökade verktyg för att bekämpa den organiserade brottsligheten men anser att det är av yttersta vikt att analysera de risker som är inbyggda i AI-system i sig och vid användning av sådana system. Enligt ombudsmannen gäller det särskilt i förhållande till skyddet för mänskliga rättigheter och förbudet mot diskriminering, för att säkerställa att de verktyg som föreslås är proportionerliga till det eftersträvade ändamålet. Även *Institutet för mänskliga rättigheter* lyfter problem avseende diskriminering.

Justitiekanslern anser att förslaget framstår som generöst såvitt avser förutsättningarna för att använda tekniken i fråga. Justitiekanslern påpekar

att det med hänsyn till riskerna för att tekniken i framtiden kan användas för andra ändamål finns anledning att anlägga ett betydligt mer restriktivt perspektiv än förslaget ger uttryck för. *Institutet för mänskliga rättigheter* betonar risken för ändamålsglidning som kan leda till att användningsområdet för kamerabevakning utökas och behoven av ansiktsigenkänning kan komma att utvidgas.

Lunds universitet understryker att en användning av tekniken innebär rättighetsinskränkningar för en stor mängd människor på ett påtagligt sätt vilket är en omständighet som kontinuerligt måste beaktas i bl.a. regleringen av tekniken. Enligt universitetet är avvägningen som görs i promemorian obalanserad och beaktar inte att systemet kan skada grundläggande rättigheter som exempelvis mötesfriheten och yttrandefriheten. Enligt *Institutet för mänskliga rättigheter* får förslagen konsekvenser inte bara för den personliga integriteten och rätten till privat- och familjeliv, utan även för rättigheter såsom yttrandefriheten samt mötes- och demonstrationsfriheten. *Civil Rights Defenders* för fram liknande synpunkter och anför även att ansiktsigenkänningssystem tenderar att vara mindre träffsäkra för personer med mörkare hudtoner samt för kvinnor. Organisationen för även fram en oro för att polisen kommer att behöva samarbeta med privata aktörer vid utveckling och inköp av AI-system, vilket begränsar insynen för bl.a. allmänheten.

Justitiekanslern konstaterar att det den senaste tiden har pågått flera parallella lagstiftningsprojekt som berör utökningar av statens möjligheter att använda olika typer av hemliga tvångsmedel i förhållande till enskilda. Enligt Justitiekanslern innebär denna lagstiftningsteknik stora svårigheter att bedöma de enskilda förslagens proportionalitet eftersom en sådan bedömning delvis är beroende av övriga förslag på området. *Institutet för mänskliga rättigheter* för fram motsvarande synpunkter.

Skälen för regeringens bedömning

En avvägning mellan behov och integritetsintrång

Vid användning av AI-system för ansiktsigenkänning i realtid måste vissa grundläggande fri- och rättigheter beaktas, bl.a. skyddet för den personliga integriteten och rätten till privatliv samt enskildas rättssäkerhet. Som *Lunds universitet* påtalar innebär användningen av tekniken rättighetsinskränkningar för en stor mängd människor vilket givetvis är en omständighet som måste beaktas i regleringen av tekniken och i proportionalitetsbedömningen. I bedömningen måste t.ex. vägas in att användningen kan få konsekvenser för mötesfriheten vilket också framgår av skäl 32 till AI-förordningen där det anges att användningen indirekt kan avskräcka från utövande av mötesfrihet. I avsnitt 5.2 redogörs närmare för det skydd som finns för den personliga integriteten och rätten till privatliv i regeringsformen, Europakonventionen, EU:s rättighetsstadga, barnkonventionen och ICCPR. Begränsningar i nämnda fri- och rättigheter får endast ske genom lag och för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Det krävs också att begränsningen är nödvändig och proportionerlig (2 kap. 21 § regeringsformen, artikel 52 i EU:s rättighetsstadga och artikel 8.2 i Europakonventionen). Vid en sådan bedömning måste en avvägning göras mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan

grundläggande fri- och rättigheter. En noggrann bedömning ska göras av behovet av åtgärden, åtgärdens förväntade effektivitet och nytta samt vilka integritetsintrång som åtgärden kan förväntas medföra. Användning av den föreslagna åtgärden måste motsvaras av ett faktiskt behov, vilket ska vägas mot vikten av att värna rättssäkerhet och personlig integritet (se t.ex. SOU 2007:22 del 1 s. 176 f.).

Polisens behov och förväntad effekt

I avsnitt 6.1 och 7.1 redogörs närmare för Polismyndighetens behov av att kunna använda AI-system för ansiktsigenkänning i realtid i olika situationer och hur tekniken skulle förbättra polisens arbete. Det bedöms stå klart att det finns ett konkret behov som kan motivera sådana begränsningar i skyddet för den personliga integriteten och rätten till privatliv som användning av tekniken utgör. De ändamål som polisen vill kunna använda tekniken för är legitima i ett demokratiskt samhälle och är sådana som omfattas av AI-förordningens undantag. Det är fråga om att förhindra och bekämpa viss allvarlig brottslighet men även att lagföra och verkställa straffrättslig påföljd för sådan brottslighet och att söka efter vissa brottsoffer. Användning av tekniken utgör en polisiär utredningsmetod där AI-systemet bearbetar exempelvis ett kameramaterial och genererar ett resultat utifrån den data som systemet har försetts med, exempelvis en bild på en eller flera personer som är av intresse för de brottsbekämpande myndigheterna. Det rör sig alltså i första hand om ansiktsigenkänning men kan även vara andra former av biometrisk igenkänning, t.ex. genom rörelsemönster eller röst. Det är fråga om en mycket effektiv behandling av material som även annars är tillgängligt för de brottsbekämpande myndigheterna. Polismyndigheten har framfört att det kan vara avgörande att tekniken får användas för att kunna förhindra hot mot människors liv och säkerhet eftersom tekniken ökar förutsättningarna för att kunna lokalisera den misstänkta personen innan hotet kan förverkligas. Tekniken innebär även bättre förutsättningar för att hitta, och kanske även rädda, offer för viss brottslighet och utreda och lagföra sådana brott som undantaget i AI-förordningen tillåter samt verkställa straffrättslig påföljd för sådana brott, eftersom polisen, genom tekniken, på ett bättre sätt kan hantera den information som ofta finns i dessa ärenden. Genom att använda tekniken kan polisens arbete utföras av färre tjänstemän än vid manuell granskning vilket dels ökar kvaliteten på analysarbetet, dels minimerar spridning av uppgifterna och på så sätt även integritetsintrånget.

Sammantaget förväntas användningen av tekniken få effekt och göra stor nytta för polisens arbete. Det förslag som lämnas i propositionen innebär att det i en ny lag regleras att polisen, för vissa specifikt angivna syften, får använda tekniken. Det blir på detta sätt tydligt för vilka ändamål som användningen får ske.

Användningen måste vara proportionerlig och nödvändig

När ett AI-system för ansiktsigenkänning i realtid används behandlas biometriska uppgifter om alla personer som passerar den aktuella kameran som tekniken används på. Det innebär att även personer som varken misstänks eller är dömda för brott kommer att påverkas av användningen

på ett sätt som innebär ett intrång i deras fri- och rättigheter. Det står klart att behandlingen i flera fall kommer att beröra många personer och att det rör sig om en integritetskänslig behandling av personuppgifter. I sammanhanget bör dock påpekas att tekniken ska appliceras på uppgifter som samlas in på annan grund. Inhämtningsåtgärden som ligger till grund för insamlingen av uppgifter har alltså redan bedömts vara förenlig med annan tillämplig reglering, exempelvis kamerabevakningslagen, vars syfte är bl.a. att säkerställa den enskildes integritet vid kamerabevakning.

Justitiekanslern anser att förslaget i promemorian framstår som generöst såvitt avser förutsättningarna för att använda tekniken i fråga. Regeringen bedömer i avsnitt 7.1, att promemorians förslag inte fullt ut motsvarar de krav som ställs i AI-förordningen. Regeringen har därför justerat flera av förslagen i syfte att uppnå en reglering som stämmer överens med AI-förordningens bestämmelser men med beaktande av polisens behov.

Justitiekanslern ger uttryck för att det finns risk för att tekniken i framtiden kan användas för andra ändamål. Även *Institutet för mänskliga rättigheter* betonar risken för ändamålsglidning som kan leda till att användningsområdet för kamerabevakning ska tendera att utökas allt eftersom det används och att behoven av ansiktsigenkänning kan komma att utvidgas. Som framgår ovan ger AI-förordningen ett begränsat utrymme för att använda AI-system för ansiktsigenkänning i realtid. I denna proposition föreslås tydliga regler för användningen som håller sig inom det utrymme som AI-förordningen tillåter. Regeringen delar därför inte remissinstansernas farhågor om framtida ändamålsglidning.

Den senaste tiden har det pågått flera parallella lagstiftningsprojekt som berör utökningar av statens möjligheter att använda olika typer av hemliga tvångsmedel i förhållande till enskilda. Enligt Justitiekanslern innebär denna lagstiftningsteknik stora svårigheter att bedöma de enskilda förslagens proportionalitet eftersom en sådan bedömning delvis är beroende av övriga förslag på området. Regeringen har nyligen tillsatt en utredning för att göra en rättslig och systematisk översyn av reglerna om hemliga och preventiva tvångsmedel i syfte att åstadkomma en mer effektiv och tydlig reglering (dir. 2025:12) men konstaterar samtidigt att användning av AI-system för ansiktsigenkänning i realtid inte är ett hemligt tvångsmedel..

Institutet för mänskliga rättigheter anser att det är viktigt att se de sammanlagda konsekvenserna av bl.a. tidigare antagna lagförslag om kamerabevakning och biometriregister. Användning av AI-system för ansiktsigenkänning i realtid förutsätter i princip användning av kameror, vilket innebär att användningen kan behöva förhålla sig till bestämmelserna i kamerabevakningslagen. Vid kamerabevakning ska det göras en intresseavvägning. Det innebär att kamerabevakning endast får ske om intresset av sådan bevakning väger tyngre än den enskildes intresse av att inte bli bevakad. Vid bedömningen av den enskildes intresse av att inte bli bevakad ska det särskilt beaktas hur bevakningen ska utföras, om teknik som ökar risken för integritetsintrång som exempelvis ansiktsigenkänning ska användas. Det innebär alltså, i linje med vad Institutet lyfter, att det görs en samlad bedömning av konsekvenserna till följd av kamerabevakning och användning av AI-tekniken.

Enligt den föreslagna lagen får tekniken endast användas om skälen för användningen uppväger det intrång eller men i övrigt som åtgärden

innebär för den som åtgärden riktas mot eller för något annat motstående intresse, se avsnitt 7.2. Det framgår därmed att det måste vara proportionerligt att använda tekniken i det enskilda fallet, vilket också följer av AI-förordningen. När det inte längre finns stöd för användningen ska den omedelbart upphöra (se avsnitt 9.5). Ett ytterligare krav är att tekniken endast får användas om det är absolut nödvändigt för ändamålet (se avsnitt 7.1). Det innebär att tekniken endast får användas när det finns ett påtagligt behov av det och det inte finns några andra effektiva åtgärder att tillgå som är mindre ingripande för de berörda. En viktig begränsning som följer av AI-förordningen är att användningen alltid ska avse en på förhand utpekad person. Tekniken kommer därmed inte kunna användas för allmän bevakning. Det föreslås vidare att tillstånd endast får meddelas i den geografiska och tidsmässiga omfattning som är absolut nödvändig. Detta innebär att omfattningen av tillståndet alltid ska stå i rimlig proportion till ändamålet (se avsnitt 9.3). AI-förordningen föreskriver även att beslut som har negativa rättsliga följder för en person inte får fattas enbart på grundval av utdata från AI-system för ansiktsigenkänning i realtid (artikel 5.3). *Integritetsskyddsmyndigheten* och *Myndigheten för säkerhet och integritetsskydd* anser att det förbudet bör tas in i den nya lagen i förtydligande syfte. Förbudet är direkt tillämpligt och regeringen anser därför att det inte också bör återges i den nationella regleringen.

Rättssäkerhetsgarantier

AI-förordningen uppställer ett krav på att användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål på allmänt tillgängliga platser ska föregås av ett tillstånd från en rättslig myndighet eller en oberoende administrativ myndighet. Enligt den nya lagen kommer därmed att användning som utgångspunkt endast får ske efter att en åklagare eller domstol har meddelat ett tillstånd till användningen (se avsnitt 8). I vissa brådskande situationer får tekniken börja användas utan tillstånd, men en prövning av användningen kommer då alltid att ske av åklagare eller domstol kort därpå. Om rätten eller åklagaren anser att det inte funnits förutsättningar att påbörja användningen ska den omedelbart upphöra och uppgifterna från användningen raderas (se avsnitt 10). Tillståndsprövningen utgör en viktig rättssäkerhetsgaranti för den enskilde och innebär att en oberoende aktör alltid kommer bedöma om förutsättningarna för att använda tekniken är uppfyllda och om det är proportionerligt att använda tekniken i det specifika fallet. För att ett tillsynsorgan ska kunna utföra en kontroll av handläggningen och användning av tekniken föreslås att åklagarens och rättens beslut om tillstånd ska innehålla uppgifter om skälen för beslutet, tid och plats för tillståndet samt vilken person som avses, även om det inte alltid kommer finnas en känd identitet på personen (se avsnitt 9.3.)

Eftersom användning av tekniken innebär att personuppgifter behandlas krävs att användningen, utöver att ha stöd i den nu föreslagna regleringen, även sker på ett sätt som är förenligt med brottsdatalagen och polisens brottsdatalag. Regleringen om personuppgiftsbehandling utgör ett omfattande skydd för den enskildes personliga integritet och innebär bl.a. att vissa skyddsåtgärder måste vidtas och att personuppgifter måste behandlas på ett sådant sätt att risken för diskriminering och felaktig

identifiering minimeras, se avsnitt 5.2. Rätten till integritet och skydd av personuppgifter måste garanteras under AI-systemets hela livscykel. De åtgärder som leverantörer vidtar för att säkerställa efterlevnaden av principerna om uppgiftsminimering och inbyggt dataskydd och dataskydd som standard kan omfatta inte bara anonymisering och kryptering, utan även användning av teknik som gör det möjligt att föra in algoritmer i data och möjliggöra träning av AI-system utan överföring mellan parter eller kopiering av rådata eller strukturerade data i sig, utan att det påverkar tillämpningen av de krav på dataförvaltning som föreskrivs i AI-förordningen (skäl 69 i AI-förordningen). Genom AI-förordningens krav på att användning av tekniken ska anmälas till den nationella dataskyddsmyndigheten och en marknadskontrollmyndighet – som föreslås bli Integritetsskyddsmyndigheten – möjliggörs en mer effektiv kontroll över tillämpningen av reglerna om användningen. Därmed kan Integritetsskyddsmyndigheten på ett bättre sätt uppfylla sitt uppdrag som tillsynsmyndighet över personuppgiftsbehandlingen. Den enskilde kommer även kunna initiera en prövning av personuppgiftsbehandlingen med stöd av dataskyddsregleringen eftersom det föreslås att den som blir föremål för ett beslut enligt den nya lagen i vissa situationer ska underrättas om åtgärden, se avsnitt 12.

Utöver detta kan Justitieombudsmannen och Justitiekanslern inom ramen för sin respektive tillsyn, uttala sig i frågor om användningen av tekniken. När tekniken används för att lokalisera eller identifiera en person som misstänks för brott skyddas denne även av de regler som gäller vid förundersökning och ytterst genom det högt ställda beviskrav som gäller vid en domstolsprövning i brottmål. Utöver den nationella tillsynen ska medlemsstaterna årligen förse kommissionen med rapporter om användningen (artikel 5.6).

Övriga krav enligt AI-förordningen och annan lagstiftning

Utöver AI-förordningens reglering som gäller undantaget om användning av AI-system för ansiktsigenkänning i realtid uppställs i förordningen ett antal andra krav på AI-system för biometrisk fjärridentifiering. Sådana system utgör högrisksystem och omfattas därmed av flera skyddskrav som måste uppfyllas, däribland krav på riskhanteringssystem och dokumentation (se bl.a. artikel 9 och 49). Medlemsstaterna ska även inrätta regulatoriska sandlådor där AI-system kan testas och tränas utifrån relevant data (artikel 57). På det sättet kan risken för felaktiga resultat och resultat som är diskriminerande minimeras.

Civil Rights Defenders anser att det är ett problem att polisen i stor utsträckning kommer att behöva samarbeta med privata aktörer vid utveckling och inköp av AI-system. Organisationen menar att detta innebär att kontrollen över hur systemen utformas, tränas etc. delvis ligger hos företag, vilket begränsar insynen för både myndigheten själv och för allmänheten. Polisens eventuella samarbete med privata aktörer vid utveckling och inköp är en fråga för myndigheten – som vid all utveckling och inköp av teknik – och fråntar inte polisen ansvaret att säkerställa att systemen uppfyller samtliga krav. Genom kravet på inrättande av regulatoriska sandlådor tillhandahåller AI-förordningen ett effektivt verktyg för detta. AI-förordningen definierar en regulatorisk sandlåda för AI som en

kontrollerad ram som har inrättats av en behörig myndighet och som erbjuder leverantörer eller potentiella leverantörer av AI-system möjlighet att utveckla, träna, validera och testa, när så är lämpligt under verkliga förhållanden, ett innovativt AI-system. Medlemsstaterna ska säkerställa att deras behöriga myndigheter inrättar minst en regulatorisk sandlåda för AI på nationell nivå. De behöriga myndigheterna ska tillhandahålla vägledning, tillsyn och stöd inom den regulatoriska sandlådan för AI i syfte att identifiera risker, särskilt när det gäller bl.a. grundläggande rättigheter (artikel 57.6).

I sammanhanget bör det även beaktas att det, för att kunna använda tekniken, krävs att det finns en kamera på den plats som aktualiseras. När en kamera som satts upp i enlighet med kamerabevakningslagen har bedömningen gjorts att bevakningen väger tyngre än den enskildes intresse av att inte bli bevakad. Vid den bedömningen ska bl.a. beaktas om teknik som ökar risken för integritetsintrång, såsom AI-system för ansiktsigenkänning i realtid, ska användas. Detta innebär, i dessa fall, att skyddet för den enskildes personliga integritet har beaktats redan när kameran sattes upp.

Den föreslagna regleringen är förenlig med grundläggande fri- och rättigheter

Användning av AI-system för ansiktsigenkänning i realtid innebär att biometriska uppgifter avseende en i många fall omfattande personkrets granskas av ett AI-system, dessutom utan samtycke från de berörda. Det förslag som lämnas i propositionen om att polisen ska få använda tekniken innebär alltså en begränsning av skyddet mot intrång i den personliga integriteten och privatlivet. Sådana begränsningar får enligt regeringsformen göras genom lag, men endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får inte sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ regeringsformen). Förslagen i propositionen innebär att begränsningen görs genom lag och ändamålen – dvs. att söka efter vissa brottsoffer, förhindra terrorbrott och annan allvarlig brottslighet mot människors liv eller säkerhet samt utreda, lagföra och verkställa straffrättslig påföljd för vissa allvarliga brott – är godtagbara i ett demokratiskt samhälle. Tekniken får endast användas när det är absolut nödvändigt för ändamålet och användningen ska även vara proportionerlig. Det föreslås även att möjligheten att använda tekniken ska omgärdas av rättssäkerhetsgarantier i form av krav på tillstånd och underrättelse till enskilda. Därutöver kan polisens användning av tekniken falla under olika aktörers tillsyn. Begränsningen av skyddet för den enskildes personliga integritet och rätt till privatliv bedöms därmed inte gå utöver vad som är nödvändigt med hänsyn till ändamålen och sträcker sig inte så långt att den utgör ett hot mot den fria åsiktsbildningen. Sammantaget bedömer regeringen att förslagen innebär en begränsning som är motiverad utifrån 2 kap. 20 och 21 §§ regeringsformen.

Rätten till respekt för privatlivet enligt Europakonventionen får inskränkas med stöd av lag om det i ett demokratiskt samhälle är nödvändigt med hänsyn till den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd eller till förebyggande av

oordning eller brott, till skydd för hälsa eller moral eller för andra personers fri- och rättigheter (artikel 8.2). Mot bakgrund av att polisen föreslås få använda tekniken enbart för vissa begränsade ändamål och med särskild restriktivitet bedöms det förslag som lämnas i denna proposition vara förenligt med Europakonventionen.

För att begränsa skyddet för privatlivet enligt EU:s rättighetsstadga krävs att begränsningen är föreskriven i lag och förenlig med det väsentliga innehållet i rättigheten. En begränsning får, med beaktande av proportionalitetsprincipen, endast göras om den är nödvändig och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter (artikel 52.1). Det är av allmänt samhällsintresse att polisen på ett effektivt sätt kan söka efter brottsoffer och förhindra, utreda och lagföra allvarliga brott samt verkställa straffrättslig påföljd för sådana brott. Som redogjorts för i avsnitt 6.1 och 7.1 ökar förutsättningarna för detta om polisen tillåts använda AI-system för ansiktsigenkänning i realtid. Den inskränkning som förslagen innebär av rätten till respekt för privatliv enligt EU:s rättighetsstadga är därför nödvändig. Eftersom förslagen dessutom får anses vara proportionerliga är de förenliga med stadgans bestämmelse om rätt till respekt för privatlivet.

Diskrimineringsombudsmannen, som i och för sig instämmer i behovet av att ge polisen utökade verktyg för att bekämpa den organiserade brottsligheten, anför att man i olika sammanhang identifierat att användningen av AI-system kan leda till systematisk diskriminering. Som framgår av remissynpunkter på förslagen i promemorian Förbättrade möjligheter för polisen att använda kamerabevakning (Ds 2024:11) medför användningen av tekniken problem kopplat till bias och diskriminering. Mot den bakgrunden finner Diskrimineringsombudsmannen det anmärkningsvärt att promemorian som ligger till grund för nu aktuella förslag saknar analys av de risker för diskriminering, kopplat till exempelvis personers etniska tillhörighet, som nu aktuella förslag kan innebära. Enligt ombudsmannen utgör det en väsentlig brist. Enligt *Civil Rights Defenders* tenderar ansiktsigenkänningssystem att vara mindre träffsäkra för personer med mörkare hudtoner samt för kvinnor. Även *Institutet för mänskliga rättigheter* lyfter att det finns risk för diskriminering. Regeringen bedömer, i linje med vad som anges i kommissionens riktlinjer om förbjudna användningsområden för AI, att rätten till icke-diskriminering (artikel 21 i stadgan) kan påverkas om AI-systemet har inbäddade biaser såsom könsrelaterade eller etniska som leder till felaktig identifiering av en misstänkt eller gärningsperson. En liknande bedömning förs fram i Statskontorets rapport Myndigheterna och AI – En studie om möjligheter och risker med att använda AI i statsförvaltningen. I rapporten anges också att om AI används som stöd i beslutsfattande och förutsatt att algoritmerna är rätt utformade kan risken minska för att beslut påverkas av att handläggare, medvetet eller omedvetet diskriminerar utifrån diskrimineringsgrunder som kön, etnisk tillhörighet eller ålder (s. 30).

Som framgår av artikel 5.3 i AI-förordningen får inget beslut som har negativa rättsföljder för en person fattas enbart på grundval av utdata från systemet för ansiktsigenkänning i realtid. Förordningen ger alltså inte utrymme för annat än att tekniken får användas som stöd i polisens verksamhet. Ett stöd som kan leda till bl.a. effektivare utredningar och att fler

brott kan klaras upp (jfr Statskontorets rapport Myndigheterna och AI, s. 27). För att motverka att AI-systemet har inbäddade bias är det viktigt att polisen gör noggranna tester av sina AI-satsningar innan de införs i verksamheten. Som framgår ovan utgör regulatoriska sandlådor en sådan miljö där AI-system kan testas och tränas utifrån relevant data (artikel 57 i AI-förordningen). På det sättet kan risken för felaktiga resultat och resultat som är diskriminerande minimeras. I linje med vad Statskontoret lyfter i sin rapport är det också viktigt att polisen gör regelbundna uppföljningar även efter att de har börjat använda tekniken, för att säkerställa att det blivit som det var tänkt. Det är vidare viktigt att polisen genomför systematiska utvärderingar för att bedöma om satsningarna har lett till förväntade effektiviseringar och ökad rättssäkerhet (jfr Statskontorets rapport Myndigheterna och AI, s. 57). Som Diskrimineringsombudsmannen påtalar kommer delar i AI-förordningen, bl.a. bestämmelserna om regulatoriska sandlådor börja tillämpas en tid efter att nu aktuella förslag ska träda i kraft. Som framgår av avsnitt 11 ska det även genomföras en konsekvensbedömning som omfattar grundläggande rättigheter. Enligt kommissionens riktlinjer bör konsekvensbedömningen avseende grundläggande rättigheter beskriva systemets prestanda och noggrannhetsnivå på grundval av den tekniska dokumentationen och, och i förekommande fall, de träningsdata som tekniken testades och utvecklades på för att förhindra biaser och diskriminering (punkten 377). Även om reglering i AI-förordningen som gäller konsekvensbedömning blir tillämplig först i augusti 2026 ska de krav för konsekvensbedömningar avseende grundläggande rättigheter som anges i artikel 27 i AI-förordningen tillämpas av tillhandahållare av AI-system för ansiktsigenkänning i realtid från det att den nya lagen träder i kraft (se avsnitt 11 och 16). Därigenom kommer en bedömning av de risker som Diskrimineringsombudsmannen påpekar att behöva ske redan från början.

Mot den bakgrunden bedömer regeringen att risken för diskriminering begränsas så långt det är möjligt. I sammanhanget kan påpekas att användning av AI-system för ansiktsigenkänning i realtid, använt på rätt sätt, rentav kan minska risken för diskriminering eftersom AI har förutsättningar att vara helt objektiv. För att åstadkomma detta är det angeläget att de system som används utarbetas och tillämpas på ett korrekt och objektiv sätt. Förslagen är därför förenliga med stadgans skydd mot diskriminering.

Diskrimineringsombudsmannen efterfrågar även att diskrimineringslagen (2008:567) utvidgas på så sätt att all offentlig verksamhet, inklusive Polismyndighetens och andra rättsvårdande myndigheters verksamhet, fullt ut omfattas av lagens förbud mot diskriminering. Regeringen kan konstatera att ett sådant förslag återfinns i betänkandet Ett utökat skydd mot diskriminering (SOU 2021:94). Betänkandet bereds inom Regeringskansliet och frågan övervägs därför inte närmare i detta lagstiftningsärende.

Barnkonventionen innehåller bl.a. bestämmelser om barns rätt till respekt för privatlivet (artikel 16). Av barnkonventionen framgår också att vid alla åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa (artikel 3). De förslag som lämnas innebär att AI-system för ansiktsigenkänning i realtid kommer kunna användas för att lokalisera eller identifiera barn och unga och innebär, på samma sätt som för vuxna, begränsningar i rätten till privatliv. Samtidigt innebär förslagen att polisen

får verkningsfulla verktyg att hitta barn som kan vara offer för exempelvis människohandel eller sexualbrott eller för att förhindra allvarliga brott, eller utreda, lagföra och verkställa straffrättslig påföljd för sådana brott. Förslagen medför att barn och unga exempelvis kan skyddas från att utnyttjas och dras in i brottslighet och att de kan få nödvändig vård och behandling. Att tekniken kan användas är också angeläget för barns säkerhet, trygghet och tilltro till rättsväsendet och vuxenvärlden, inte minst i de fall där ett barn är ett brottsoffer. Mot den bakgrunden bedöms förslagen vara förenliga med barnkonventionen, däribland principen om barnets bästa. Dessutom finns det inom ramen för den proportionalitetsbedömning som ska göras vid varje enskilt beslut även utrymme för att ta hänsyn till vad som är bäst för barnet.

Artikel 17 i ICCPR innehåller bl.a. skydd mot godtyckliga eller olagliga ingrepp i den enskildes privatliv. Eftersom det föreslås att polisens användning av AI-system för ansiktsigenkänning i realtid ska regleras i lag bedöms förslagen vara förenliga med artikel 17 i ICCPR.

I skäl 32 till AI-förordningen anges att användning av AI-system för ansiktsigenkänning i realtid kan skapa en känsla av konstant övervakning och indirekt avskräcka från utövande av mötesfriheten. Som följer av skälen och som *Institutet för mänskliga rättigheter*, *Riksdagens ombudsmän* och *Civil Rights Defenders* påtalar kan användning av tekniken medföra en risk att enskilda, med vetskap om att kameror som kan användas för ansiktsigenkänning sitter uppe, censurerar sig själva genom att exempelvis avstå från att delta i en demonstration eller göra sin röst hörd. *Lunds universitet* för också fram att användningen av tekniken innebär rättighetsinskränkningar för en stor mängd människor och att det måste vägas in att förslaget inte bara får konsekvenser för den personliga integriteten utan för befolkningen i övrigt som utsätts för övervakning. Enligt universitet kan det minska utövandet av exempelvis mötesfriheten. Regeringen konstaterar att tekniken endast kommer att få användas för begränsade och noga angivna syften och på ett sådant sätt att det inte kan bli fråga om allmän bevakning. Förslagen kommer alltså inte att rent faktiskt hindra enskilda från att utöva sina fri- och rättigheter som exempelvis mötesfriheten. Mot den bakgrunden bedömer regeringen att risken för självcensur är begränsad. Även om risken är begränsad måste den tas på stort allvar. Det behöver därför finnas robusta skyddsmekanismer som kan kompensera för en sådan risk. En sådan är kravet på tillståndsprövning. En annan är genom de krav som ställs i AI-förordningen och som ger tillsynsmyndigheten goda förutsättningar att utföra en effektiv och kvalificerad tillsyn över tillämpningen av reglerna om användningen. Trots dessa skyddsmekanismer finns en risk, om än liten, för att opinionsfriheterna påverkas negativt. Regeringen bedömer dock att den är motiverad av det mycket angelägna intresset av att bekämpa brottslig verksamhet.

AI-konventionen innehåller inget särskilt förbud mot användning av AI-system för ansiktsigenkänning i realtid. Konventionen har undertecknats av kommissionen. Undertecknandet uttrycker EU:s avsikt att bli part i konventionen. Kommissionens bedömning är att ramkonventionen är förenlig med unionsrätten och AI-förordningens bestämmelser samt att konventionen genomförs genom AI-förordningen. Förslagen i propositionen bedöms därmed även vara förenliga med AI-konventionen.

16 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag

Den nya lagen och följdändringar i andra författningar ska träda i kraft den 1 juli 2026. Ändringen i den nya lagen ska träda i kraft den dag som regeringen bestämmer.

Regeringens bedömning

Det finns inte behov av övergångsbestämmelser.

Promemorians förslag och bedömning

Förslaget och bedömningen i promemorian stämmer delvis överens med regeringens. I promemorian föreslås att den nya lagen och följdändringar i andra författningar ska träda i kraft den 1 januari 2026. I promemorian föreslås vidare att ändringen i den nya lagen ska träda i kraft den 2 augusti 2026.

Remissinstanserna

Ingen remissinstans invänder mot förslaget eller bedömningen i promemorian.

Skälen för regeringens förslag och bedömning

Förbudet mot att använda AI-system för ansiktsigenkänning i realtid i artikel 5.1 h i AI-förordningen började tillämpas den 2 februari 2025 (artikel 113 i AI-förordningen). Med hänsyn till att det är angeläget att införa bestämmelser som möjliggör undantag från förbudet bör den nya lagen och föreslagna följdändringar i andra författningar träda i kraft så snart som möjligt. Det bedöms kunna ske den 1 juli 2026.

I avsnitt 11 föreslås en ändring i den nya lagen till följd av att artikel 49 i AI-förordningen börjar tillämpas vid en senare tidpunkt än artikel 5.1 h. Som framgår av avsnitt 11 råder viss osäkerhet kring när artikeln ska börja tillämpas. Ändringen bör därför träda i kraft den dag som regeringen bestämmer.

Det bedöms inte finnas något behov av övergångsbestämmelser till den nya regleringen.

17 Konsekvenser av förslagen

17.1 Konsekvenser för det brottsbekämpande arbetet och för enskilda

Regeringens bedömning

Förslagen innebär en ökad risk för intrång i skyddet för privatliv och den personliga integriteten men bidrar samtidigt till att förbättra möjligheterna för Polismyndigheten och Säkerhetspolisen att söka efter brottsoffer, förebygga, förhindra, upptäcka, utreda och lagföra allvarliga brott och för att verkställa straffrättslig påföljd för sådana brott. Därmed innebär förslagen en ökad rättstrygghet för enskilda. Förslagen ger sammantaget uttryck för en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sitt privatliv och sin personliga integritet.

Förslagen är förenliga med principen om barnets bästa.

Promemorians bedömning

Bedömningen i promemorian stämmer överens med regeringens.

Remissinstanserna

De flesta remissinstanser tillstyrker bedömningen eller invänder inte mot den. Enligt *Åklagarmyndigheten* framgår det inte helt klart av promemorian att tekniken är tillåten även då målpersonen är ett barn som är misstänkt för brott. Några remissinstanser, däribland *Integritetsskyddsmyndigheten*, *Myndigheten för säkerhet och integritetsskydd* och *Centrum för rättvisa*, anser att den föreslagna lagen bör tidsbegränsas.

Skälen för regeringens bedömning

Konsekvenser för det brottsbekämpande arbetet

Förslagen innebär att polisen får tillgång till ett ändamålsenligt och effektivt verktyg som kan användas för att förbättra polisens möjligheter att söka efter brottsoffer, förebygga, förhindra, upptäcka, utreda och lagföra allvarlig brottslighet samt för att verkställa straffrättsliga påföljder för sådan brottslighet. Ett exempel på en situation där tekniken kan användas är i ett ärende där polisen via underrättelseuppslag fått starka indikationer på att det planeras för ett allvarligt brott. I sådana ärenden finns det ibland information om var brottet kommer att ske eller mot vem hotet riktas. AI-system för ansiktsigenkänning i realtid kan då användas för att lokalisera en misstänkt gärningsperson i tid för att avvärja brottet. Det kan också handla om att polisen har information om en försvunnen person som misstänks vara utsatt för brott och som behöver hittas snabbt eller ärenden som avser personer som är misstänkta eller dömda för brott som håller sig undan lagföring eller straffverkställighet. De senare ärendena rör framför allt personer som har anhållits eller häktats i sin frånvaro under en

pågående brottsutredning eller som har dömts för brott till en frihetsberövande påföljd men som inte har inställt sig till eller avvikit från verkställighet av straffet. Förslagen innebär att AI-systemet granskar ett kameramaterial och lokaliserar eller identifierar en på förhand utpekad person i stället för att det görs av en fysisk person. Det innebär att polisens arbete kan effektiviseras. Den brottsutveckling som skett i Sverige är allvarlig och det har under de senaste åren skett en ökning av det dödliga skjutvapenvåldet i samhället. Det sagda ställer högre krav på att polisen måste arbeta på ett delvis annat sätt än tidigare och det finns därför ett stort behov av att polisens verktyg anpassas till den utvecklingen. Förslagen har utformats med hänsyn till dessa behov. En närmare redogörelse för behoven och den förväntade effektiviteten finns i avsnitt 6.1 och 7.1.

Möjligheten att använda AI-system för ansiktsigenkänning i realtid för att förebygga, förhindra eller upptäcka allvarlig brottslighet förväntas leda till att färre brott begås. Att AI-system för ansiktsigenkänning i realtid ska kunna användas för att utreda begångna brott förväntas bidra till att fler brott lagförs. Om fler personer lagförs för brott och döms till en frihetsberövande påföljd, kan det också leda till minskad brottslighet. Detsamma får antas gälla om fler personer verkställer straffrättslig påföljd. Möjligheten att använda tekniken för att hitta personer som misstänks vara utsatta för brott förväntas leda till att fler brottsoffer i vissa fall kan räddas.

Konsekvenser för enskilda

Enskilda tillförsäkras skydd mot godtyckliga ingrepp i sitt privatliv och sin personliga integritet från statens sida genom bl.a. 2 kap. 6 § regeringsformen, artikel 8 i Europakonventionen och artikel 7 i EU:s rättighetsstadga. En inskränkning av rätten till skydd för privatlivet och den personliga integriteten får bara ske i enlighet med vissa särskilt angivna förutsättningar (2 kap. 20 och 21 §§ regeringsformen, artikel 8.2 i Europakonventionen och artikel 52.1 i EU:s rättighetsstadga, se även avsnitt 5.2 och 15.2).

De förslag som lämnas om att polisen ska få använda AI-system för ansiktsigenkänning i realtid innebär en begränsning av skyddet mot intrång i den personliga integriteten och privatlivet, se avsnitt 15.2. Som framgår där bedöms förslagen vara förenliga med regeringsformen, Europakonventionen och EU:s rättighetsstadga. Även om användningen innebär ökade integritetsrisker för enskilda innehåller den föreslagna regleringen samtidigt rättssäkerhetsgarantier som syftar till att begränsa integritetsintrånget och gör det möjligt att utöva en effektiv tillsyn. Som anges ovan bedöms förslagen leda till minskad brottslighet vilket innebär ett förstärkt skydd för enskildas personliga integritet och bidra till ökad trygghet för enskilda.

Några remissinstanser, däribland *Centrum för rättvisa* och *Myndigheten för säkerhet och integritetsskydd*, anser att förslaget bör tidsbegränsas för att dess effektivitet och påverkan på enskildas rättigheter ska kunna utvärderas innan den görs permanent. Regeringen anser att det inte finns skäl att göra lagen tidsbegränsad. Det finns däremot skäl att följa upp lagens effekt på bl.a. den personliga integriteten efter att den varit i kraft en tid. En uppföljning bör ske, antingen genom en utredning eller ett myndighetsuppdrag. Vid uppföljningen bör användningen av tekniken ur

ett integritetsperspektiv och den praktiska tillämpningen analyseras. Det krävs ett tillräckligt omfattande underlag för att en robust och välgrundad uppföljning av den nya regleringen ska kunna genomföras. Uppföljningen bör därför inledas ca tre år efter ikraftträdandet.

Sammantaget innebär förslagen som lämnas i propositionen en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sitt privatliv och sin personliga integritet.

Konsekvenser för barn och unga

Barnkonventionen gäller som svensk lag. I artikel 3 i konventionen slås fast att vid alla åtgärder som rör barn ska i första hand beaktas vad som bedöms vara barnets bästa, vare sig de vidtas av offentliga eller privata sociala välfärdsinstitutioner, domstolar, administrativa myndigheter eller lagstiftande organ.

Enligt *Åklagarmyndigheten* framgår det inte helt klart av promemorian att tekniken är tillåten även då målpersonen är ett barn som är misstänkt för brott. I anledning av synpunkten kan regeringen konstatera att AI-förordningen inte innehåller något förbud mot att tillåta sådan användning och att någon sådan begränsning inte heller föreslås i den nya lagen. De förslag som lämnas kommer därmed på samma sätt som för vuxna att innebära ökade risker för intrång i barns privatliv och personliga integritet. Som framgår av avsnitt 15.2 vägs dessa risker dock upp av de angelägna ändamålen att polisen har verkningsfulla möjligheter att bl.a. hitta barn som kan vara offer för allvarliga brott, att skydda barn från att utnyttjas och dras in i brottslighet samt att lagföra brott och verkställa straffrättsliga påföljder. Förslagen bedöms på samma sätt som för vuxna leda till minskad brottslighet bland barn och mot barn. Att det kan ske är angeläget för barns säkerhet, trygghet och tilltro till rättsväsendet och vuxenvärlden, inte minst i de fall där ett barn är brottsoffer. Förslagen bedöms innebära bättre förutsättningar att upptäcka och stötta barn och unga som riskerar att begå eller begår grova brott, ofta i miljöer kopplade till organiserad brottslighet, så att de exempelvis får nödvändig vård och behandling. Som framgår av avsnitt 15.2 innebär förslagen en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och barn och ungas rätt till skydd för sitt privatliv och sin personliga integritet. Förslagen är därmed också förenliga med barnkonventionen.

17.2 Konsekvenser för det allmänna

Regeringens bedömning

Förslagen bedöms leda till ökade kostnader för Integritetsskyddsmyndigheten. I budgetpropositionen för 2026 föreslås att myndigheten tillförs medel fr.o.m. 2027 för att finansiera dessa kostnader. Förslagen bedöms leda till något ökade kostnader för Sveriges Domstolar. Kostnadsökningarna bedöms dock inte vara större än att de kan hanteras inom befintlig ekonomisk ram. I övrigt bedöms de kostnadsökningar som förslagen kan medföra för staten enbart vara marginella och bedöms kunna hanteras inom befintliga ekonomiska ramar.

Promemorians bedömning

Bedömningen i promemorian stämmer i huvudsak överens med regeringens. I promemorian görs ingen bedömning av behovet av finansiering.

Remissinstanserna

Domstolsverket för fram att förslaget bedöms innebära kostnadsökningar som är så stora att de inte kan hanteras inom givna anslagsramar. *Integritetsskyddsmyndigheten* bedömer att det finns ett behov av anslagsökning. *Polismyndigheten* anser, till skillnad från bedömningen i promemorian, att förslaget kommer att innebära ökade kostnader för myndigheten. *Åklagarmyndigheten* framhåller att förslagen innebär helt nya arbetsuppgifter för åklagare och att det finns behov av it-stöd för ärendehandläggningen vilket behöver beaktas vid bedömningen av kostnaderna för myndigheten. *Region Stockholm* anser att det bör förtydligas om polisen kommer kunna använda andra aktörers kameror för att använda AI-system för ansiktsigenkänning i realtid eller om det krävs att myndigheten själv äger utrustningen. *Stockholms tingsrätt* för fram liknande synpunkter.

Skälen för regeringens bedömning och förslag

Konsekvenser för Polismyndigheten och Säkerhetspolisen

Förslagen medför inte någon skyldighet för Polismyndigheten eller Säkerhetspolisen att använda AI-system för ansiktsigenkänning i realtid, men öppnar för möjligheten att använda tekniken i den utsträckning AI-förordningen medger. Polismyndigheten bedriver kamerabevakning på ett antal offentliga platser i landet med olika kameralösningar. I nuläget finns det inga kameror som är utrustade med AI-system för ansiktsigenkänning i realtid. För att använda tekniken krävs att Polismyndigheten utvecklar nya tekniska lösningar och att befintliga kameror som tekniken inte kan användas på byts ut. Eftersom det är fråga om en ny teknik och en ny reglering har Polismyndigheten uppskattat att antalet ansökningar om tillstånd under en uppbyggnadsfas om ett år kommer uppgå till knappt 100. För att förslagen ska få genomslag i brottsbekämpningen krävs att fler kameror förses med tekniken. Polismyndigheten gör gällande att detta kommer att ske stegvis. Det innebär att antalet ansökningar om tillstånd att använda AI-system för ansiktsigenkänning i realtid kommer att öka i takt med att kamerorna utrustas med tekniken. Det är dock mycket svårt att uppskatta antalet ansökningar eftersom det bl.a. rör sig om en ny ärendetyp. Vid en grov uppskattning bedöms, bl.a. utifrån uppskattningar som gjort av Polismyndigheten, antalet ansökningar om tillstånd, efter något år uppgå till cirka 500 per år och efter några år till cirka 1 000 per år. Uppskattningen avser både ansökningar som ska prövas av åklagare och av domstol.

Att utrusta kamerorna med AI-system för ansiktsigenkänning i realtid kommer, särskilt under uppbyggnadsfasen, att leda till kostnader för Polismyndigheten. I promemorian görs bedömningen att användningen av tekniken samtidigt kan innebära en minskad arbetsbörda på såväl kort som lång sikt för myndigheten eftersom tekniken nämligen kan ersätta den granskning som annars måste ske av en fysisk person vilket kan leda till lägre kostnader. *Polismyndigheten* delar inte den bedömningen utan menar

att eftersom syftet är att i realtid kunna identifiera eftersökta personer krävs personal som omedelbart kan ta emot och agera på informationen. Det kommer också krävas att en fysisk person granskar bildmaterialet för att bedöma resultatet som AI-systemet genererat. Regeringen ifrågasätter inte att myndigheten behöver personal som utför dessa uppgifter men bedömer ändå att tekniken som på ett effektivt sätt kan selektera material i vart fall inte kan förväntas leda till en ökad arbetsbörda. Sammantaget med att förslagen inte medför någon skyldighet att utrusta kamerorna med tekniken innebär det att de kostnadsökningar som förslagen kan medföra kan finansieras inom befintlig anslagsram.

Säkerhetspolisens verksamhet ligger i allt väsentligt utanför AI-förordningens tillämpningsområde eftersom den rör nationell säkerhet. Med hänsyn till att förslagen endast i begränsad mån kommer att beröra Säkerhetspolisen bedöms de inte leda till annat än marginella kostnader för myndigheten.

Region Stockholm anser att det bör förtydligas om polisen kommer kunna använda andra aktörers kameror för att använda AI-system för ansiktsigenkänning i realtid eller om det krävs att myndigheten själv äger utrustningen. Detta mot bakgrund av Polismyndighetens pågående initiativ gällande att ta del av andra aktörers videoströmmar genom den s.k. SOT-lösningen (”säker oberoende transmission”). Även *Stockholms tingsrätt* efterfrågar liknande klargöranden. Regeringen konstaterar att förslagen inte hindrar att andra aktörers kameror används. I vilken omfattning det är tekniskt och rättsligt möjligt för polisen att ta del av material från sådana kameror i realtid är emellertid inte något som hanteras inom ramen för detta ärende, utan är i första hand en fråga för polisen och de aktörer som äger relevanta kamerasystem som exempelvis kommuner och regioner. Förslagen i denna proposition medför oavsett i sig inga kostnader för vare sig polisen eller övriga aktörer.

Konsekvenser för Åklagarmyndigheten

Förslagen innebär att Åklagarmyndigheten kommer vara både prövningsinstans och sökande myndighet för ansökningar om tillstånd att använda AI-system för ansiktsigenkänning i realtid. Det kan förutses att merparten av ansökningarna kommer att avse sådan användning av tekniken som inte ska prövas av åklagare utan av domstol, men Åklagarmyndigheten kommer även att ha vissa kostnader i egenskap av sökande myndighet i de ärendena. Baserat på detta och på Polismyndighetens uppskattning av antal ansökningar om tillstånd görs i promemorian bedömningen att förslagen endast kommer ha ringa påverkan på Åklagarmyndighetens kostnader. *Åklagarmyndigheten* framhåller emellertid att förslagen innebär helt nya arbetsuppgifter för åklagare. Det kommer också att finnas ett stort behov av it-stöd för ärendehandläggning. Vid bedömningen behöver man enligt myndigheten således beakta de kostnader som följer med att utveckla och etablera ett sådant stöd. Regeringen invänder inte mot de ytterligare behov som Åklagarmyndigheten för fram. Regeringen bedömer dock att de kostnadsökningar som förslagen kan medföra sammantaget ändå kan finansieras inom myndighetens befintliga anslagsram.

Konsekvenser för de allmänna domstolarna

Förslagen innebär att en ny ärendetyp kommer att tillföras allmän domstol. Som framgår ovan bedöms antalet ansökningar om tillstånd att använda AI-system för realtidsidentifiering, efter något respektive några år, uppgå till grovt beräknat cirka 500 respektive 1 000 per år. Huvuddelen av ansökningarna kommer att prövas av allmän domstol vilka därigenom sammantaget bedöms få fler ärenden än Åklagarmyndigheten i anledning av förslagen. Detta kommer att leda till kostnader för verksamheten bl.a. för ärendehandläggning. I promemorian görs en jämförelse med styckkostnaden för domstolsärenden inklusive ärenden om utsökning och det anges att även om det är mycket svårt att göra någon säker prognos om antalet ärenden bedöms förslagen innebära kostnadsökningar år 2027 med cirka 2,65 miljoner kronor och därefter med cirka 5,3 miljoner kronor årligen. Under uppbyggnadsfasen bedöms kostnaderna dock som marginella. *Domstolsverket* finner inte skäl att uppskatta kostnaden till andra belopp än de nämnda och anser att Sveriges Domstolar bör tillföras medel i enlighet med den beräkningen. Regeringen bedömer dock att de kostnadsökningar som förslaget kommer att medföra kan finansieras inom befintlig anslagsram.

Konsekvenser för Integritetsskyddsmyndigheten

Som framgår av avsnitt 13 avser regeringen att utse Integritetsskyddsmyndigheten till marknadskontrollmyndighet i fråga om användning av AI-system för ansiktsigenkänning i realtid. I det uppdraget ingår bl.a. att ta emot och registrera anmälningar om användningen av AI-system för ansiktsigenkänning i realtid och att upprätta årliga rapporter till kommissionen om sådan användning. Myndigheten kommer även i egenskap av nationell dataskyddsmyndighet få tillkommande arbetsuppgifter genom att bl.a. utöva tillsyn och ta emot klagomål avseende personuppgiftsbehandling knuten till användning av tekniken. Integritetsskyddsmyndigheten bedömer, utifrån Polismyndighetens uppskattning av antalet ansökningar, att de tillkommande arbetsuppgifterna kräver en krypterad e-tjänst. Det krävs också personalresurser för att bl.a. sammanställa årliga rapporter, samt för underhåll och drift av systemet. Sammantaget bedömer Integritetsskyddsmyndigheten att förslagen innebär kostnadsökningar efter uppbyggnadsfasen på något år med 3 miljoner kronor årligen. Under uppbyggnadsfasen bedöms dock kostnaderna som begränsade. *Integritetsskyddsmyndigheten* för i sitt remissvar fram att myndigheten har behov av anslagsökning som motsvarar dessa kostnadsökningar. Regeringen har i budgetpropositionen för 2026 (prop. 2025/26:1 utg.omr. 1 avsnitt 10.11.3) föreslagit att myndigheten ska tillskjutas 3 miljoner kronor i ökade anslag fr.o.m. år 2027 för att finansiera nämnda kostnadsökningar.

Konsekvenser för Myndigheten för säkerhet och integritetsskydd

Myndigheten för säkerhet och integritetsskydd kommer att utöva tillsyn över den personuppgiftsbehandling som utförs av Polismyndigheten och Säkerhetspolisen vid användning av AI-system för ansiktsigenkänning i realtid. Förslagen innebär således att omfattningen av myndighetens tillsynsuppdrag kommer att öka något. De eventuella kostnadsökningar som det kan leda till bedöms dock vara marginella.

17.3 Övriga konsekvenser

Regeringens bedömning

Förslagen bedöms kunna bidra till att uppnå det jämställdhetspolitiska målet att kvinnor och män ska ha samma makt att forma samhället och sina egna liv. De bedöms även kunna förbättra förutsättningarna för Sveriges internationella straffstraffrättsliga samarbeten.

I övrigt bedöms inte förslagen leda till några konsekvenser.

Promemorians bedömning

Bedömningen i promemorian stämmer överens med regeringens.

Remissinstanserna

Ingen remissinstans invänder mot bedömningen.

Skälen för regeringens bedömning

Samtliga förslag är könsneutrala. Även med bestämmelser som gäller lika för alla kan olika grupper påverkas av dem i olika utsträckning. Enligt kriminalstatistiken misstänks och lagförs fler män än kvinnor för allvarlig brottslighet. Det är därför högst sannolikt att fler män än kvinnor kommer att beröras av de nya reglerna.

Förslagen bedöms bidra till en ökad trygghet i samhället eftersom fler brott bl.a. kommer att förebyggas, förhindras och upptäckas. Kvinnor uttrycker i större utsträckning än män otrygghet enligt de nationella trygghetsundersökningar som Brottsförebyggande rådet, Brå, årligen genomför. Det innebär att förslagen kan bidra till att uppnå det jämställdhetspolitiska målet att kvinnor och män ska ha samma makt att forma samhället och sina egna liv.

Det föreslås att det, på samma sätt som i en svensk förundersökning, rättegång eller vid verkställighet av påföljder enligt svenska domar, ska vara möjligt att använda AI-system för ansiktsigenkänning i realtid inom ramen för det internationella straffrättsliga samarbetet. Det bedöms innebära att förutsättningarna för Sveriges internationella straffrättsliga samarbeten förbättras.

Förslagen bedöms inte medföra några konsekvenser för miljön, det kommunala självstyret eller sysselsättningen.

Förslagen bedöms inte heller medföra några konsekvenser för små företags förutsättningar. Människor som vistas i ett område som ett tillstånd till användning av AI-system för ansiktsigenkänning i realtid avser kommer inte att ha kännedom om användningen. Någon påverkan på benägenheten att vistas i ett visst område bör förslagen därför inte ha. Mot den bakgrunden bedöms förslagen inte påverka företag som verkar inom ett sådant område.

18 Författningskommentar

18.1 Förslaget till lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

Lagens tillämpningsområde

1 § Lagen gäller för Polismyndighetens och Säkerhetspolisens användning av system för artificiell intelligens för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid på allmän plats (AI-system för ansiktsigenkänning i realtid) i verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177).

Paragrafen anger lagens tillämpningsområde. Övervägandena finns i avsnitt 6.1 och 6.2.

Lagens regler om användning av AI-system för biometrisk fjärridentifiering i realtid utgör ett undantag från AI-förordningens förbud mot sådan användning, i enlighet med artikel 5.1 h–5.7 i förordningen.

Av paragrafen framgår att lagen reglerar Polismyndighetens och Säkerhetspolisens användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål på allmän plats samt att lagen endast gäller i verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen. Med brottsbekämpande ändamål avses polisens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Att lagen endast är tillämplig på sådan verksamhet vars personuppgiftsbehandling regleras i brottsdatalagen innebär att lagen inte gäller i Säkerhetspolisens verksamhet som rör nationell säkerhet eller när Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen (se 1 kap. 4 § första stycket brottsdatalagen). Begreppet allmän plats har samma innebörd som i brottsbalken (se t.ex. 16 kap. 11 §). Med allmän plats avses varje plats, inom- eller utomhus, som är upplåten för eller regelbundet besöks av allmänheten, såsom gator, torg, parker, väntsalar, tunnelbanestationer eller järnvägsstationer. Om allmänheten har tillträde endast under vissa tider, är platsen allmän under denna tid men inte i övrigt. Även tåg, båtar, hotell, restauranger, butiker, teatrar, kyrkogårdar, biografer, idrottsområden och liknande utgör allmänna platser i den mån och under den tid allmänheten har tillträde till dem. När tekniken används för verksamhet och på platser som faller utanför lagens tillämpningsområde får en bedömning av användningen i stället göras utifrån det dataskyddsrättsliga regelverket samt övriga bestämmelser i AI-förordningen, när dessa trätt i kraft. Som framgår av paragrafen används i lagen genomgående begreppet AI-system för ansiktsigenkänning, som då inkluderar användning av system för annan biometrisk fjärridentifiering, exempelvis igenkänning genom rörelsemönster eller röst.

2 § Med AI-system för ansiktsigenkänning i realtid avses i lagen sådana AI-system som omfattas av artikel 3.42 i Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens), här benämnd AI-förordningen.

I paragrafen definieras begreppet AI-system för ansiktsigenkänning i realtid. Övervägandena finns i avsnitt 6.2.

Av paragrafen framgår att begreppet AI-system för ansiktsigenkänning i realtid ska ges samma innebörd som artikel 3.42 i AI-förordningen. Det innebär att begreppet i lagen definieras som ett system för biometrisk fjärridentifiering där infångning, dvs. upptagning, av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål. Det omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående (jfr artikel 3.41 i AI-förordningen). Det rör sig i första hand om ansiktsigenkänning men kan även vara andra former av biometrisk igenkänning, se kommentaren till 1 §.

Hänvisningen till AI-förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

Inför användning av ett AI-system

3 § Innan ett AI-system för ansiktsigenkänning i realtid används för första gången ska Polismyndigheten och Säkerhetspolisen göra en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen.

I paragrafen regleras en skyldighet för Polismyndigheten och Säkerhetspolisen att göra en konsekvensbedömning innan ett AI-system för ansiktsigenkänning i realtid får börja användas. Övervägandena finns i avsnitt 11.

Paragrafen innebär att varje myndighet som använder systemet, dvs. både Polismyndigheten och Säkerhetspolisen måste göra en konsekvensbedömning enligt artikel 27 i AI-förordningen innan den första användningen av ett AI-system för ansiktsigenkänning i realtid. Det är alltså en åtgärd som måste vidtas innan den första användningen av ett system och inte inför varje användning. Polisen kan vid en fortsatt användning alltså förlita sig på en tidigare genomförd konsekvensbedömning av systemet. Om något av de element som anges i artikel 27.1 har ändrats eller inte längre är aktuellt ska polisen vidta nödvändiga åtgärder för att uppdatera informationen (se artikel 27.2 i AI-förordningen). I en konsekvensbedömning ska beaktas vilken inverkan på grundläggande rättigheter som användningen av tekniken kan ge upphov till. Detta gäller både när tekniken används efter att ett tillstånd har meddelats och i en brådskande situation innan ett tillstånd har sökts.

Enligt artikel 27.1 i AI-förordningen ska konsekvensbedömningen bl.a. innehålla en beskrivning av användningen av den biometriska fjärridentifieringen och tillhandahållarens processer för användningen, jämte det avsedda ändamålet. Av artikel 3.4 framgår att med tillhandahållare avses bl.a. en fysisk eller juridisk person eller offentlig myndighet som under

eget överinseende använder ett AI-system, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet. Av artikel 27.1 följer vidare att konsekvensbedömningen ska innehålla exempelvis användningsperiod och användningsfrekvens, de kategorier av personer och grupper som berörs av systemet och de särskilda risker för att de påverkade personerna ska åsamkas skada samt riskbegränsande åtgärder. Den aktuella konsekvensbedömningen ersätter inte den konsekvensbedömning avseende dataskydd som personuppgiftsansvariga måste utföra. Innan en ny typ av personuppgiftsbehandling påbörjas som kan antas medföra särskild risk för intrång i den registrerades personliga integritet ska den personuppgiftsansvarige enligt 3 kap. 7 § brottsdatalagen (2018:1177) bedöma konsekvenserna för skyddet av personuppgifter. Användning av AI-system för ansiktsigenkänning i realtid kan regelmässigt förväntas utgöra en sådan behandling. Om en konsekvensbedömning har gjorts enligt brottsdatalagen kan vissa av kraven i artikel 27.1 i AI-förordningen uppfyllas genom den (se artikel 27.4).

Av artikel 27.3 i AI-förordningen framgår att när konsekvensbedömningen är utförd ska marknadskontrollmyndigheten underrättas om resultatet av bedömningen. Enligt artikeln kan undantag göras från underrättelseskyldigheten i sådana situationer som avses i artikel 46.1. Det är fråga om exceptionella skäl som bl.a. rör allmän säkerhet eller skydd av människors liv och hälsa. I artikel 27.3 anges att tillhandahållaren, dvs. polisen, ska fylla i en sådan mall som avses i artikel 27.5. Den behöver dock inte fyllas i förrän artikel 27 börjar tillämpas.

Den myndighet som ska pröva en ansökan om tillstånd att använda tekniken (se 6 och 7 §§) behöver inte kontrollera att förutsättningarna enligt bestämmelsen är uppfyllda när en ansökan om tillstånd kommer in till myndigheten.

Hänvisningen till AI-förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

Användning av AI-system

4 § AI-system för ansiktsigenkänning i realtid får användas om det är absolut nödvändigt för att lokalisera eller identifiera en viss person

1. som misstänks vara utsatt för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken, eller för människoexploatering enligt 4 kap. 1 b § brottsbalken om exploateringen avser sexuella tjänster,
2. som är försvunnen och misstänks vara utsatt för brott,
3. om det finns en överhängande risk för att personen kommer att begå ett allvarligt brott som innebär fara för annans liv eller fysiska säkerhet,
4. som skäligen kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet, eller
5. som dömts för ett sådant brott som avses i 4, i syfte att verkställa den straffrättsliga påföljden.

Paragrafen, som utformas delvis enligt *Lagrådets* förslag, reglerar i vilka syften AI-system för ansiktsigenkänning i realtid får användas. Övervägandena finns i avsnitt 7.1.

För att få använda ett AI-system för ansiktsigenkänning i realtid krävs tillstånd (se 6 och 7 §§). Tillstånd kan endast ges för användning i de fem olika fall som paragrafen reglerar.

För att få använda tekniken måste det finnas en specifik person som ska lokaliseras eller identifieras. Det krävs inte att identiteten på personen är känd men det behöver finnas vissa uppgifter som visar vem användningen ska avse, t.ex. en bild på personen. Det är alltså inte tillåtet att använda tekniken för att allmänt leta efter personer som uppträder misstänkt. Att tekniken används för att lokalisera en person innefattar inte bara att hitta personen utan också att därefter följa personen i syfte att se var han eller hon tar vägen. Kravet på absolut nödvändigt innebär att behovet av användningen behöver vara kvalificerat. Det innebär att tekniken endast får användas med restriktivitet och att polisen inte regelmässigt får använda den. Det måste finnas omständigheter som visar att ett ärende kan föras framåt genom att använda tekniken. Uttrycket absolut nödvändigt ska tolkas restriktivt och behovet av åtgärden måste prövas noga i den enskilda fallet (jfr prop. 2017/18:232 s. 447). Som utgångspunkt får tekniken endast användas när andra möjligheter att lokalisera eller identifiera den som söks har uttömts eller sådana åtgärder skulle vara utsiktslösa eller medföra en orimligt stor arbetsinsats. Om andra åtgärder är möjliga för att lokalisera eller identifiera den som söks är det dock ändå tillåtet att använda tekniken om alternativen skulle innebära att den som söks inte kan hittas eller identifieras tillräckligt skyndsamt. Det innebär att polisen inte regelmässigt får använda den och det måste finnas omständigheter som visar att ett ärende kan föras framåt genom att använda tekniken. Det ska alltså finnas skäl att räkna med att användningen av tekniken – ensam eller tillsammans med andra åtgärder – kan leda till att den som söks anträffas eller identifieras.

Enligt *punkt 1* får tekniken användas för att hitta en viss person som misstänks vara utsatt för brott. Tekniken får användas i en situation då en person misstänks vara utsatt för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken. Tekniken får också användas när en person misstänks vara utsatt för människoexploatering enligt 4 kap. 1 b § brottsbalken om den avser sexuella tjänster. Hänvisningen innebär att användning får ske om exploateringen i arbete eller tiggeri avser sexuella tjänster. Det krävs inte att personen har anmälts saknad utan bestämmelsen träffar också situationer där polisen har information om att en person misstänks vara utsatt för exempelvis människohandel.

Enligt *punkt 2*får tekniken användas för att söka efter en person som är försvunnen och misstänks vara utsatt för brott. Det ställs inte något krav på att det ska vara fråga om ett visst brott. Användningen måste dock vara proportionerlig vilket innebär att hänsyn måste tas till brottets allvar, se kommentaren till 5 §. I vilken mån användning av AI-system för ansiktsigenkänning i realtid kan användas för att söka efter försvunna personer som inte misstänks vara utsatta för brott får avgöras utifrån det dataskyddsrättsliga regelverket samt övriga bestämmelser i AI-förordningen. För att bestämmelsen ska kunna tillämpas krävs inte att en förundersökning har inletts.

Enligt *punkt 3* får tekniken användas om det finns en överhängande risk för att en person kommer att begå ett allvarligt brott som innebär fara för annans liv eller fysiska säkerhet. Den risk det ska vara fråga om består i

en viss sannolikt för att brottet kommer att begås och att det kan inträffa nära i tiden. Det krävs dock inte att brottet är omedelbart förestående (jfr 13 § om möjligheten att använda AI-system för ansiktsigenkänning i realtid utan tillstånd när det föreligger fara i dröjsmål). Det ska finnas konkreta omständigheter som tyder på att det finns en risk för att en person kommer att begå ett brott. Det ställs vidare krav på att det ska vara fråga om ett allvarligt brott som innebär fara för annans liv eller fysiska säkerhet. Exempel på sådan brottslighet är mord, dråp, misshandel av allvarligare slag, , rån, grövre fall av olaga tvång och våldtäkt och andra allvarliga sexualbrott. Även brott som typiskt sett riktar sig mot en mer obestämd krets av människor kan omfattas, såsom mordbrand och allmänfarlig ödeläggelse. Likaså omfattas medhjälp och anstiftan samt försök och andra osjälvständiga brottsformer. En utgångspunkt för bedömningen av om det är fråga om ett allvarligt brott är att det rör sig om ett konkret brott med ett straffvärde motsvarande fängelse i minst sex månader. Även andra omständigheter än straffvärdet kan dock vara relevanta vid bedömningen. Användning enligt punkten kan ske oavsett om det är i eller utanför en förundersökning.

Enligt *punkt 4* får tekniken användas för att lokalisera eller identifiera en person som skäligen kan misstänkas ha begått vissa brott för vilka det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet. Det kan exempelvis handla om att i ett inledande skede i en förundersökning hitta personer som skäligen kan misstänkas för ett sådant brott, eller i ett senare skede hitta en misstänkt person som har anhållits eller häktats i sin frånvaro under en pågående brottsutredning eller som har avvikit och inte inställer sig till en domstolsförhandling. För skälig misstanke krävs det i regel att det finns konkreta omständigheter av en viss styrka som pekar på att just den misstänkte har begått den gärning som misstanken avser. Vad som närmare krävs får bedömas från fall till fall. AI-tekniken får användas för brott som avses i bilaga II till AI-förordningen. Brott som upptas i den bilagan är bl.a. mord, grov misshandel, människohandel, våldtäkt, olaglig handel med narkotika samt olaglig handel med vapen och sprängämnen. En bedömning får göras av om de brott som anges i bilagan har en motsvarighet i svensk rätt och vilka brott det i så fall handlar om. Det krävs också att det i straffskalan för brottet måste ingå fängelse i fyra år eller mer. Bedömningen är alltså hänförlig till straffskalan för ett brott och inte till straffvärdet Kravet innebär enligt svensk rätt att brott i flera fall måste bedömas som grova för att de ska omfattas av lagens tillämpningsområde även om de i och för sig omfattas av bilagan. AI-tekniken kan användas för försök, förberedelse eller stämpling till sådana brott som anges i bilagan, om det enligt svensk rätt kan följa fängelse i fyra år eller mer för det aktuella brottet. Hänsyn ska alltså tas till vilket straff som är möjligt i förhållande till bestämmelserna om försök, förberedelse och stämpling till brott enligt 23 kap. brottsbalken. Användning av AI-tekniken enligt punkten kan ske om det är i en förundersökning men också för att utreda brott som begåtts av någon innan han eller hon fyllt 15 år (jfr 31 § lagen [1964:167] med särskilda bestämmelser om unga lagöverträdare). Användning enligt punkten kan också ske under den fortsatta lagföringen. Hänvisningen till AI-förord-

ningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

Enligt *punkt 5* får AI-tekniken användas i syfte att verkställa en straffrättslig påföljd för sådana brott som anges i bilaga II till AI-förordningen. Det kan exempelvis handla om att hitta personer som inte har inställt sig till eller avvikit från verkställighet av ett straff. I uttrycket straffrättsliga påföljder ingår även andra påföljder än fängelse, såsom skyddstillsyn, samhällstjänst och rättspsykiatrisk vård. Vilken påföljd som är aktuell ska beaktas vid den proportionalitetsbedömning som ska göras (se 5 §).

5 § AI-system för ansiktsigenkänning i realtid får användas endast om skälen för användningen uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Paragrafen anger att AI-system för realtidsidentifiering endast får användas om åtgärden är proportionerlig. Övervägandena finns i avsnitt 7.2.

Bestämmelsen innebär att det i varje enskilt fall måste göras en bedömning om användningen i fråga om arten av den situation som ger upphov till användningen, särskilt hur allvarlig, sannolik och omfattande skadan skulle bli om tekniken inte används står i rimlig proportion till konsekvenserna av att tekniken används för berörda personers rättigheter och friheter, särskilt vad gäller hur allvarliga, sannolika och omfattande dessa konsekvenser är (jfr artikel 5.2 a och b i AI-förordningen). Vid bedömningen ska t.ex. beaktas det aktuella brottets allvar, eventuellt utdömd påföljd, vilken typ av biometrisk fjärridentifiering som avses, hur många personer som påverkas av användningen och om målpersonen är ett barn. Att användningen ska vara proportionerlig gäller i alla led, både inför och under användning. I situationer där integritetsintrånget under användningen blir oproportionerligt stort måste användningen avbrytas, trots att åtgärden fortfarande kan ha betydelse för t.ex. en brottsutredning. Det kan antingen bero på att nyttan är låg eller integritetsintrånget särskilt högt eller en kombination av båda. Att användningen ska vara proportionerlig får också betydelse för hur ett tillstånd ska utformas och vilka villkor som ska förenas med det (se 10 §).

Tillståndsprövningen hos åklagare

6 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd prövas av åklagare på ansökan av Polismyndigheten eller Säkerhetspolisen.

Paragrafen reglerar vem som ska ansöka om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd och vem som ska pröva ansökan. Övervägandena finns i avsnitt 8.

I paragrafen anges att om AI-system för ansiktsigenkänning i realtid ska användas för att förebygga, förhindra eller upptäcka brottslig verksamhet ska ansökan om tillstånd prövas av åklagare. Begreppen har samma innebörd som i den dataskyddsrättsliga regleringen. Bestämmelsen gäller alltså när tekniken ska användas för all egentlig brottsbekämpande verksamhet inom polisen som inte direkt kan knytas till en brottsutredning

(jfr prop. 2009/10:85 s. 100 och prop. 2017/18:232 s. 93). Därutöver gäller bestämmelsen när tekniken ska användas i syfte att verkställa straffrättslig påföljd. Paragrafen innebär att åklagare kan pröva frågor enligt 4 § 1–3 och 5. Ett beslut som fattas av åklagaren är inte överklagbart. Det är den myndighet som är ansvarig för frågan, dvs. Polismyndigheten eller Säkerhetspolisen, som kan ansöka om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid.

Tillståndsprövningen i domstol

7 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att utreda eller lagföra brott prövas av rätten på ansökan av åklagare.

Ansökan prövas av den domstol som anges i 19 kap. rättegångsbalken.

Paragrafen reglerar vem som ska ansöka om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid om syftet är att utreda brott eller lagföra en person och vem som ska pröva ansökan. Övervägandena finns i avsnitt 8.

Av *första stycket* framgår att rätten ska pröva en ansökan om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid i syfte att utreda eller lagföra brott. Både brottsoffer och gärningsmän kan bli föremål för användning i ett sådant fall. Paragrafen innebär att domstol kan pröva frågor enligt 4 § 1–4 men inte 5. Det ankommer på åklagare att ansöka om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för de syften som nämns i paragrafen. Detta får till följd att exempelvis ett beslut om tillstånd som har fattats av åklagare i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet enligt 6 § inte längre kan utgöra grund för användningen om en förundersökning inleds i det specifika fallet. En ny ansökan om tillstånd för användning i syfte att utreda brott behöver då göras och prövas av domstolen.

Av *andra stycket* följer vilken domstol som är behörig att pröva ansökan. Den forumregel som anges i bestämmelsen motsvarar befintliga forumregler som gäller vid en ansökan om hemliga tvångsmedel i en förundersökning enligt rättegångsbalken. Enligt regleringen ska en ansökan om att använda tekniken i syfte att utreda och lagföra brott prövas av den domstol som anges i 19 kap. rättegångsbalken. Som huvudregel är således behörig domstol tingsrätten i den ort där brottet begicks. Om det är lämpligt får prövningen i stället göras där den misstänkte har hemvist eller mera varaktigt uppehåller sig. I vissa brådskande fall får frågan även prövas av en tingsrätt på annan ort.

8 § Förfarandet i domstolen är skriftligt.

På förfarandet tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i denna lag. Det som föreskrivs om offentliga ombud i 27 kap. 28 § rättegångsbalken ska dock inte tillämpas.

I paragrafen regleras formen för domstolens handläggning av ärenden om tillstånd att använda AI-system för ansiktsigenkänning i realtid. Övervägandena finns i avsnitt 9.1.

Enligt 7 § ska rätten pröva en ansökan om ett tillstånd att använda tekniken för att utreda eller lagföra brott.

Av *första stycket* framgår att förfarandet i domstol ska vara skriftligt. Det innebär att tillståndsärendet avgörs utan sammanträde.

Enligt *andra stycket* är rättegångsbalkens regler om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor tillämpliga på ärenden enligt den nya lagen, om inte något annat anges i lagen. Det innebär bl.a. att reglerna i rättegångsbalken om rättens sammansättning och om överklagande ska tillämpas. Av paragrafen framgår att reglerna om offentligt ombud i balken inte ska tillämpas i ärenden om tillstånd att använda AI-system för ansiktsigenkänning i realtid. I egenskap av part i ett ärende hos domstolen om tillstånd att använda tekniken har åklagare rätt att överklaga, om beslutet går honom eller henne emot.

Skyndsam handläggning

9 § En ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska prövas skyndsamt.

Paragrafen reglerar inom vilken tid en ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska prövas. Övervägandena finns i avsnitt 9.2.

I paragrafen anges att en ansökan om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid ska prövas skyndsamt. Hur snabbt en ansökan ska hanteras får avgöras i det enskilda fallet utifrån de förutsättningar som gäller. Kravet på skyndsamhet gäller för både åklagarens och tingsrättens tillståndsprövning, liksom i överrätt om tingsrättens beslut överklagas.

Beslut

10 § I ett beslut att tillåta användning av AI-system för ansiktsigenkänning i realtid ska det anges

1. vilken person som tillståndet avser,
2. för vilket syfte användningen ska ske,
3. under vilken tid och i vilket eller vilka områden tillståndet gäller, och
4. skälen för beslutet.

Tiden för tillståndet får inte bestämmas längre än vad som är absolut nödvändigt och får inte överstiga en månad från dagen för beslutet. Området eller områdena som tillståndet avser får inte vara större än vad som är absolut nödvändigt.

Paragrafen reglerar vad ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska innehålla. Övervägandena finns i avsnitt 9.3.

Första stycket innehåller en uppräkning av vilka uppgifter som ska finnas i ett tillstånd. Enligt *punkt 1* ska det anges i beslutet vilken person som tillståndet avser. Eftersom personens identitet kan vara okänd krävs inte att det i beslutet anges identiteten på personen. Det måste dock på något sätt framgå vilken person som avses eftersom det är en förutsättning enligt 4 § att användningen sker för att lokalisera eller identifiera en på förhand utpekad person. Om identiteten är känd ska den anges i beslutet.

Av *punkt 2* framgår att det ska anges i beslutet för vilket syfte användningen ska ske. Om användningen avser verkställighet av

straffrättslig påföljd ska det anges vilken eller vilka domar som legat till grund för åtgärden.

Enligt *punkt 3* ska den tidsmässiga och geografiska omfattningen på tillståndet anges i beslutet. Vad gäller den geografiska omfattningen kan det bli aktuellt att i ett beslut tillåta att tekniken används för mer än ett område. Det kan exempelvis finnas ett behov av att använda tekniken vid flera gränsövergångar om den person som avses misstänks vara på väg att lämna eller resa in i landet (se andra stycket).

Enligt *punkt 4* ska skälen för beslutet anges.

Enligt *andra stycket* får tillståndet inte vara mer omfattande än vad som är absolut nödvändigt när det gäller tidsperioden och det geografiska området eller områdena. Absolut nödvändigt har samma innebörd som i 4 §, se kommentaren till den paragrafen. Vad som är absolut nödvändigt får avgöras utifrån omständigheterna i det enskilda fallet. Tiden för tillståndet får dock aldrig överstiga en månad från dagen för beslutet. Det geografiska tillämpningsområdet kan påverkas av vilka uppgifter som finns om var personen i fråga befinner sig. Om det t.ex. saknas närmare uppgifter om var personen kan befinna sig kan tillståndet behöva omfatta ett större geografiskt område jämfört med om det finns tydliga indikationer på var personen kan uppehålla sig. Den geografiska omfattningen kan vidare behöva anpassas för att möjliggöra för polisen att följa efter en person.

Åklagarens eller rättens beslut kan bli att ett tillstånd meddelas helt i enlighet med en ansökan eller att tillståndet begränsas till att omfatta ett mindre geografiskt område eller en kortare tidsperiod än vad ansökan avser. Det finns inget hinder mot att ansöka om ett nytt tillstånd innan tiden för ett tillstånd har löpt ut. Den nya ansökan blir då föremål för en ny prövning av åklagaren eller rätten.

Av paragrafen följer indirekt att en ansökan om ett tillstånd att använda tekniken behöver innehålla viss information.

11 § Ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid får verkställas omedelbart.

I paragrafen finns en bestämmelse om omedelbar verkställighet. Övervägandena finns i avsnitt 9.4.

Av paragrafen framgår att ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid får verkställas omedelbart. Paragrafen gäller både åklagarens och rättens beslut.

Omedelbart upphörande

12 § Om det inte längre finns skäl för ett tillstånd att använda AI-system för ansiktsigenkänning i realtid ska åklagare omedelbart upphäva beslutet. Polismyndigheten eller Säkerhetspolisen ska omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

Paragrafen anger en skyldighet för åklagaren att omedelbart upphäva ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid när det inte längre finns skäl för det. Övervägandena finns i avsnitt 9.5.

Paragrafen ger uttryck för att tekniken inte får användas när behovet har upphört. Det innebär exempelvis att även om ett tillstånd gäller för en lång tidsperiod ska användningen upphöra så fort det inte längre finns skäl för den. Det är åklagaren som ska säkerställa att beslutet omedelbart hävs. Polismyndigheten eller Säkerhetspolisen är skyldig att omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

Tillfällig användning utan tillstånd

13 § Om det är fara i dröjsmål, får Polismyndigheten eller Säkerhetspolisen påbörja användning av AI-system för ansiktsigenkänning i realtid utan tillstånd.

Den myndighet som har påbörjat användning enligt första stycket ska dokumentera den samt skälen för att användningen påbörjades utan tillstånd.

Paragrafen innebär en möjlighet för Polismyndigheten eller Säkerhetspolisen att använda AI-system för ansiktsigenkänning i realtid utan tillstånd i vissa brådskande situationer. Övervägandena finns i avsnitt 10.

Enligt *första stycket* får Polismyndigheten eller Säkerhetspolisen påbörja användningen av AI-system för ansiktsigenkänning i realtid utan ett tillstånd om det är fara i dröjsmål. Det är alltså fråga om situationer där ändamålet med användningen riskerar att gå förlorat om ett tillstånd skulle avvaktas. Ju mer angeläget det är att påträffa den aktuella personen, t.ex. då personen bedöms vara farlig för allmänheten och det finns en risk att personen begår fler brott eller då det finns en risk att personen lämnar landet, desto större är utrymmet att få påbörja användning av tekniken utan tillstånd (jfr prop. 2023/24:108 s. 55). Det är Polismyndigheten eller Säkerhetspolisen som innehar tekniken och det är dessa verkställande myndigheter som själva får besluta att påbörja användningen. I de fall det ankommer på åklagaren att ansöka om tillstånd, se 14 §, ska polisen rimligt fort underställa frågan åklagarens prövning.

Av *andra stycket* framgår att den myndighet som har påbörjat användning, dvs. Polismyndigheten eller Säkerhetspolisen, ska dokumentera den och ange skälen för att användningen påbörjades. Av dokumentationen ska exempelvis framgå varför ett tillstånd inte har kunnat avvaktas.

14 § Om användning har påbörjats utan tillstånd ska en ansökan om tillstånd enligt 6 eller 7 § göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades.

Paragrafen reglerar förfarandet när Polismyndigheten eller Säkerhetspolisen har påbörjat användningen av AI-system för ansiktsigenkänning i realtid utan tillstånd. Övervägandena finns i avsnitt 10.

Av paragrafen framgår att om användning av AI-system för ansiktsigenkänning i realtid har påbörjats utan tillstånd ska en ansökan om tillstånd enligt 6 eller 7 § göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades. Om användningen sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd ska Polismyndigheten eller Säkerhetspolisen ansöka om tillstånd hos åklagaren. Om syftet är att utreda brott

eller lagföra en person måste Polismyndigheten eller Säkerhetspolisen rimligt fort underställa frågan åklagarens prövning, som har att ansöka till rätten.

15 § Om användning har påbörjats utan tillstånd och det inte längre finns skäl för användningen, ska den myndighet som har påbörjat användningen eller, i fall som avses i 7 §, åklagare omedelbart besluta om att användningen ska upphöra.

Om användningen upphör innan tillståndsfrågan har prövats, ska den som får ansöka om tillstånd i stället göra en anmälan till åklagare eller, i fall som avses i 7 §, rätten, som ska pröva om det har funnits skäl för användningen.

Paragrafen, som utformas delvis enligt *Lagrådets* förslag, reglerar förfarandet när Polismyndigheten eller Säkerhetspolisen påbörjat användning av AI-system för ansiktsigenkänning i realtid utan tillstånd och det inte längre finns skäl för användningen. Övervägandena finns i avsnitt 10.

Av *första stycket* framgår att om användningen av AI-system för ansiktsigenkänning i realtid har påbörjats utan tillstånd och det inte längre finns skäl för användningen, ska den myndighet som har påbörjat användningen eller, i fall som avses i 7 §, åklagare omedelbart besluta om att användningen ska upphöra. Det innebär att polisen kan avbryta användning som sker för alla de syften som räknas upp i 4 §. Regleringen innebär också att åklagare kan besluta om upphörande i de fall användning sker i syfte att utreda eller lagföra brott. Om användning sker för dessa syften kan alltså en åklagare som bedömer att det saknas rättsliga förutsättningar för att ansöka om tillstånd besluta om att användningen ska upphöra.

I *andra stycket* anges att om användningen upphör innan tillståndsfrågan har prövats, ska den som får ansöka om tillstånd i stället göra en anmälan till åklagare eller, i fall som avses i 7 §, rätten, som ska pröva om det har funnits skäl för användningen. Regleringen får till följd att användning som sker utan tillstånd alltid kommer att underställas åklagares eller rättens prövning. I de fall användning sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd är det polisen som ska anmäla till åklagaren som ska pröva om det har funnits skäl för användningen medan det i fall där användning sker för att utreda eller lagföra brott är åklagare som ska anmäla till rätten som ska pröva. Den som anmäler ska i likhet med vad som gäller för en ansökan om tillstånd förse prövningsinstansen med de uppgifter som behövs för att en välgrundad prövning ska kunna göras. Exempelvis kan skälen till varför användningen har upphört redovisas. Det är dock ytterst upp till rättstillämpningen att i det enskilda fallet avgöra vilka uppgifter som behövs.

Följden av en situation där användning av tekniken har påbörjats utan tillstånd när det inte funnits förutsättningar för det är att uppgifterna som användningen resulterat i ska raderas, se kommentaren till 16 §.

16 § Om en ansökan om tillstånd avslås ska användning som har påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas. Uppgifterna från användningen ska också raderas om, i fall som avses i 15 § andra stycket, åklagaren eller rätten har funnit att det har saknats skäl för användningen.

Paragrafen, som utformas i huvudsak enligt *Lagrådets* förslag, reglerar en skyldighet att i vissa situationer upphöra med användningen och radera uppgifter. Övervägandena finns i avsnitt 8 och 10.

Av paragrafen framgår att om en ansökan om ett tillstånd att använda AI-system för ansiktsigenkänning i realtid avslås när användningen redan har påbörjats, ska användningen omedelbart upphöra och uppgifter från den raderas. Av paragrafen framgår vidare att uppgifter från användningen också ska raderas i de fall, efter en anmälan, åklagaren eller rätten har funnit att det har saknats skäl för användningen. Det som ska raderas är resultatet av behandlingen av kameramaterialet som AI-systemet utför och inte materialet som sådant. Det kan förekomma situationer när användning av tekniken påbörjas och avslutas inom 24 timmar på grund av att den person som avses snabbt kan lokaliseras eller identifieras. I en sådan situation ankommer det ändå på den som enligt lagen är den som ska ansöka om ett tillstånd att anmäla användningen till åklagare eller, i fall som avses i 7 §, rätten, som ska pröva om det har funnits skäl för användningen

Underrättelse till enskild

17 § Den som har identifierats eller lokaliserats genom en åtgärd enligt denna lag som gäller en brottsutredning eller lagföring ska underrättas om åtgärden. Underrättelsen ska lämnas så snart det kan ske utan men för det syfte som åtgärden vidtogs för.

Om uppgifterna omfattas av sekretess enligt 15 kap. 1 eller 2 §, 18 kap. 1, 2 eller 3 § eller 35 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400) ska en underrättelse skjutas upp till dess att sekretess inte längre gäller.

En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna. En underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse eller om identiteten på den som ska underrättas är okänd. Detsamma ska gälla om den personen som underrättelsen avser har avlidit.

Paragrafen innehåller bestämmelser om underrättelse till enskild. Övervägandena finns i avsnitt 12.

Av *första stycket* framgår att en eftersökt person som har identifierats eller lokaliserats genom en åtgärd enligt lagen i syfte att utreda eller lagföra brott ska underrättas om åtgärden. En underrättelse behöver alltså inte ske om användningen varit resultatlös. En underrättelse ska som utgångspunkt lämnas så snart det kan ske utan men för det syfte som åtgärden vidtogs för.

I *andra stycket* anges de situationer då en underrättelse till enskild enligt första stycket kan skjutas upp på grund av sekretess. Det kan t.ex. handla om att en underrättelse i det aktuella ärendet skulle röja åtgärder av betydelse för utredningen eller andra utredningar.

En underrättelse enligt *tredje stycket* behöver inte lämnas till den som redan har fått del av eller tillgång till samtliga de uppgifter som ska ingå i en underrättelse. Det är inte heller nödvändigt att lämna någon underrättelse om det med hänsyn till omständigheterna är uppenbart att en underrättelse är utan betydelse eller om identiteten på den som ska underrättas är okänd. Detsamma ska gälla om den personen som underrättelsen avser har avlidit.

18 § Om det på grund av sekretess eller risk för men för syftet som åtgärden vidtogs för inte har kunnat lämnas någon underrättelse inom ett år och sex månader från det att åtgärden avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller och om det kan ske utan men för syftet som åtgärden vidtogs för.

Paragrafen anger situationer då det inte har kunnat lämnas någon underrättelse. Övervägandena finns i avsnitt 12.

Bestämmelsen innebär att en prövning måste göras om en underrättelse ska lämnas till den enskilde när fristen på ett och ett halvt år löper ut. Om det vid den tidpunkten fortfarande gäller sekretess för de uppgifter som ska ingå i underrättelsen eller om uppgifterna inte kan lämnas utan men för syftet som åtgärden vidtogs för ska någon underrättelse inte lämnas. Även om fristen har löpt ut får underrättelse ske.

18.2 Förslaget till lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

3 § Innan ett AI-system för ansiktsigenkänning i realtid används för första gången ska Polismyndigheten och Säkerhetspolisen göra en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen *och registrera systemet enligt artikel 49 i förordningen. Ett sådant system får dock användas utan registrering om användningen inte kan avvakta. I sådana fall ska en registrering ske så snart det är möjligt.*

I paragrafen regleras vad som behöver göras innan ett AI-system för ansiktsigenkänning i realtid får användas för första gången. Övervägandena finns i avsnitt 11.

Ändringen i paragrafen innebär att det för att kunna börja använda tekniken krävs att AI-systemet har registrerats i EU-databasen enligt artikel 49 i AI-förordningen. Det är alltså en åtgärd som måste vidtas innan den första användningen av ett system och inte inför varje användning. EU-databasen ska innehålla viss information om AI-system med hög risk och databasen ska införas och upprätthållas av kommissionen i samarbete med medlemsstaterna (se artikel 71 i AI-förordningen). Artikel 49 innehåller krav på hur registreringen ska gå till. I paragrafen ges en möjligt att göra undantag från kravet på registrering i databasen när användningen inte kan avvakta. Det kan exempelvis vara fallet om en registrering innebär att ändamålet med användningen riskerar att gå förlorat. En registrering ska i dessa situationer göras så snart det är möjligt.

Det är Polismyndighetens och Säkerhetspolisens ansvar att registrera AI-systemet i EU-databasen, även i det fall då en registrering sker i efterhand om användningen inte har kunnat avvakta. Den tillståndsprövande myndigheten behöver inte kontrollera att förutsättningarna enligt bestämmelsen är uppfyllda när en ansökan om tillstånd kommer in till myndigheten.

Hänvisningen till AI-förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

18.3 Förslaget till lag om ändring i lagen (1957:668) om utlämning för brott

16 a § *För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 7 § andra stycket.*

Paragrafen, som är ny, innehåller bestämmelser om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid (AI-system för ansiktsigenkänning i realtid) för att lokalisera någon som är anhållen eller häktad i ett ärende om utlämning i syfte att verkställa frihetsberövandet. Övervägandena finns i avsnitt 14.2.

AI-system för ansiktsigenkänning i realtid ska kunna användas för att lokalisera någon som anhållits eller häktats med anledning av ett ärende enligt lagen i syfte att verkställa ett frihetsberövande. Detta innebär att tekniken får användas för att hitta personer som har anhållits eller häktats i sin frånvaro under en pågående utredning om utlämning för lagföring eller straffverkställighet. Andra ledet i paragrafen handlar om under vilka förutsättningar användningen får ske. Användning får endast ske i den utsträckning som anges i 4 § 4 lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. De krav som där uppställs i fråga om bl.a. avgränsningen till viss brottslighet får då prövas av rätten mot den gärning som ligger till grund för begäran om utlämning. Vid användning av tekniken tillämpas dessutom övriga bestämmelser, t.ex. tillståndsprövning, omedelbart upphörande och underrättelser, i den lagen, med undantag för bestämmelserna om forum som ska följa av lagen om utlämning för brott.

18.4 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

1 kap.

2 § Rättslig hjälp enligt denna lag omfattar följande åtgärder:

1. förhör i samband med förundersökning i brottmål,
2. bevisupptagning vid domstol,
3. telefonförhör,
4. förhör genom videokonferens,
5. kvarstad, beslag, penningbeslag samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken,
6. föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken,

7. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
8. hemlig kameraövervakning,
9. hemlig rumsavlyssning,
10. hemlig dataavläsning,
11. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning,
12. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,
13. överförande av frihetsberövade för förhör m.m.,
14. rättsmedicinsk undersökning av en avliden person, *och*
15. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

Vad som i denna lag sägs om beslag gäller även för penningbeslag.

Lagen hindrar inte att hjälp lämnas med någon annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

Paragrafen innehåller en uppräkning av vilka åtgärder som omfattas av rättslig hjälp. Övervägandena finns i avsnitt 14.2.

I *första stycket* läggs användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål till i uppräkningen av åtgärder som omfattas av rättslig hjälp.

2 kap.

1 § Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10, 14 *och 15* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.

Rättslig hjälp som avses i 1 kap. 2 § första stycket 11–13 lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

I paragrafen regleras vad som krävs för att sådan rättslig hjälp som räknas upp i 1 kap. 2 § ska kunna lämnas. Övervägandena finns i avsnitt 14.2.

Ändringen i *första stycket* innebär att rättslig hjälp i form av användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål kan lämnas under de förutsättningar som gäller för en motsvarande åtgärd enligt den lagen. Härtill gäller de särskilda bestämmelserna i 4 kap. 28 i och 28 j §§.

2 § Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 7–10, 12, 14 *och 15* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, genomsökning på distans och beslag.

I paragrafen regleras när dubbel straffbarhet uppställs som krav för att rättslig hjälp ska få lämnas. Övervägandena finns i avsnitt 14.2.

Ändringen innebär att rättslig hjälp i form av användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål får lämnas endast om kravet på dubbel straffbarhet är uppfyllt.

4 kap.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

28 i § *En ansökan om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid som avser någon som befinner sig i Sverige handläggs av åklagare. Ansökan får endast avse användning enligt 4 § 1–4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd. Om det är fara i dröjsmål, får användningen påbörjas utan tillstånd. I sådana fall tillämpas bestämmelserna i 13–16 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Om användningen påbörjas utan tillstånd ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

I fråga om underrättelse till en enskild enligt 17 och 18 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 4 kap. 25 § tredje stycket denna lag tillämpas.

Paragrafen, som är ny har utformats i huvudsak enligt *Lagrådets* förslag, innehåller bestämmelser om vilka åtgärder enligt lagen om AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål som rättslig hjälp kan lämnas för och om handläggningen av en ansökan om detta. Övervägandena finns i avsnitt 14.2.

Enligt *första stycket* ska en ansökan handläggas av åklagare. Denne ska pröva om förutsättningarna för användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid (AI-system för ansiktsigenkänning i realtid) enligt denna lag och lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål är uppfyllda. Om så är fallet, ska åklagaren ansöka om rättens tillstånd till åtgärden. Om det är fara i dröjsmål får användningen påbörjas under de förutsättningar som anges i 13–16 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Det innebär bl.a. att det är Polismyndigheten eller Säkerhetspolisen som får påbörja användningen utan tillstånd. Ansökan om tillstånd ska då göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades. Att det i många fall kan vara brådskande understryks av kravet att åklagarens prövning ska ske genast. Rättslig hjälp får lämnas för sådan användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid som anges i 4 § 1–4 i lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Det handlar om användning för att lokalisera eller identifiera en person som misstänks offer för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken, eller för människo-

exploatering enlig 4 kap. 1 b § brottsbalken om exploateringen avser sexuella tjänster (punkten 1) eller som är försvunnen och som misstänks vara utsatt för brott (punkten 2), om det finns en överhängande risk för att personen kommer att begå ett allvarligt brott som innebär fara för någon annans liv eller fysiska säkerhet (punkten 3), eller som skäligen kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet (punkten 4).

I *andra stycket* finns en bestämmelse om återredovisning enligt 2 kap. 17 §. Av bestämmelsen följer att återredovisning inte får ske om rätten – i motsats till åklagaren – inte anser att det har funnits grund för användning av AI-system för ansiktsigenkänning i realtid.

Av *tredje stycket* framgår att bestämmelserna i denna lag om underrättelse till enskild ska tillämpas i stället för 17 och 18 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Genom hänvisningen till 25 § tredje stycket blir flera av rättegångsbalkens regler tillämpliga vid underrättelsen. Vissa undantag görs dock från regleringen i rättegångsbalken. Det gäller bl.a. vid vilken tidpunkt en underrättelse ska ske och när en underrättelse kan underlåtas.

28 j § *Om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska avse någon som befinner sig i en annan stat och den andra staten kräver att ansökan först ska prövas av domstol i Sverige, får rätten på begäran av svensk åklagare besluta att tillåta användningen.*

Underrättelse enligt 17 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska inte lämnas.

I paragrafen, som är ny, finns en bestämmelse om rättens tillstånd till användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål för att lokalisera någon som finns i utlandet. Det är åklagaren som gör en sådan ansökan men om den anmodade staten kräver ett svenskt domstolsbeslut får rätten på begäran av svensk åklagare besluta att tillåta användningen. Eftersom användningen ska verkställas utomlands ska den statens verkställighetsregler tillämpas. Övervägandena finns i avsnitt 14.2.

18.5 Förslaget till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder

4 kap.

3 a § *För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 7 § andra stycket.*

Paragrafen, som är ny, innehåller bestämmelser om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid (AI-system för ansiktsigenkänning i realtid) för att lokalisera någon som är anhållen eller häktad enligt lagen. Övervägandena finns i avsnitt 14.2.

Användning av AI-system för ansiktsigenkänning i realtid ska kunna tillämpas för att lokalisera någon som anhållits eller häktats enligt lagen i syfte att verkställa frihetsberövandet. Detta innebär att tekniken får användas för att hitta personer som har anhållits eller häktats i sin frånvaro under en pågående utredning om överlämnande för lagföring eller straffverkställighet. De krav som uppställs i fråga om bl.a. avgränsningen till viss brottslighet enligt 4 § 4 lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål får då prövas av rätten mot den gärning som ligger till grund för arresteringsordern. Vid användning av tekniken tillämpas dessutom övriga bestämmelser, om t.ex. tillståndsprövning, omedelbart upphörande och underrättelser, i den lagen med undantag för bestämmelserna om forum som ska följa av lagen om överlämnande från Sverige enligt en europeisk arresteringsorder.

18.6 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

18 kap.

1 § Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. *Motsvarande sekretess gäller för uppgift som hänför sig till angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till

1. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde, eller

2. annan verksamhet än sådan som avses i 1 eller i första stycket som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Paragrafen reglerar sekretess för uppgift som hänför sig till bl.a. förundersökning i brottmål. Övervägandena finns i avsnitt 14.1.

Ändringen i *första stycket* innebär att sekretess gäller för uppgift som hänför sig till angelägenhet som avser användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om

uppgiften röjs. Sekretessen gäller med ett rakt skaderekvisit, vilket innebär en presumtion för offentlighet. Eftersom sekretessen gäller för uppgift som hänför sig till angelägenhet som avser användning av tekniken enligt den nya lagen följer sekretessen med uppgiften när den lämnas vidare till en annan myndighet. Sekretess för uppgift gäller därmed oavsett hos vilken myndighet som uppgiften finns.

Ändringen innebär även att sekretessen kommer att gälla i annan verksamhet än sådan som avses i 1 och 2 §§ hos en myndighet för att biträda exempelvis en åklagarmyndighet, Polismyndigheten eller Säkerhetspolisen med att förebygga, uppdaga, utreda eller beivra brott (3 § offentlighets- och sekretesslagen). När användningen av AI-system för ansiktsigenkänning i realtid sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet gäller sekretess enligt 2 §.

19 § Den tystnadsplikt som följer av 5–7, 8, 8 b, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *eller uppgift om användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

I paragrafen regleras vilka tystnadsplikter enligt 18 kap. offentlighets- och sekretesslagen som har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 14.1.

Ändringen i *andra stycket* innebär att den sekretess som enligt 1 § gäller för uppgifter som hänför sig till angelägenhet som avser användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

35 kap.

1 § Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde

eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,
3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),
4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,
5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,
6. register som förs enligt lagen (1998:621) om misstankeregister,
7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,
8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,
9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,
10. utredning om självständigt förverkande, *eller*
11. *angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Sekretessen enligt första stycket 2 *och 11* gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Paragrafen reglerar sekretess till skydd för uppgift om en enskilds personliga och ekonomiska förhållanden om uppgiften förekommer i en verksamhet som bl.a. syftar till att förebygga eller utreda brott. Övervägandena finns i avsnitt 14.1.

En ny punkt införs i *första stycket* som reglerar sekretess för uppgift som förekommer i angelägenhet som avser användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Ändringen innebär att sekretess gäller för uppgift som förekommer i angelägenhet som avser användning av AI-system för ansiktsigenkänning i realtid enligt nya lagen, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men. Sekretessen gäller därmed med ett omvänt skaderekvisit, vilket innebär en presumtion för sekretess. Eftersom sekretessen gäller för en uppgift som hänför sig till angelägenhet som avser användning av tekniken enligt den nya lagen följer sekretessen

med uppgiften när den lämnas vidare till en annan myndighet. Sekretess för en uppgift gäller därmed oavsett hos vilken myndighet som uppgiften finns.

Ändringen i *andra stycket* innebär att för uppgift som förekommer i angelägenhet som avser användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid för brottsbekämpande ändamål enligt nya lagen gäller sekretess hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Sekretessen gäller då alltså med ett rakt skaderekvisit, vilket innebär en presumtion för offentlighet.

18.7 Förslaget till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder

3 kap.

3 a § *För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 7 § andra stycket.*

Paragrafen, som är ny, innehåller bestämmelser om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid (AI-system för ansiktsigenkänning i realtid) för att lokalisera någon som är anhållen eller häktad. Övervägandena finns i avsnitt 14.2.

Användning av AI-system för ansiktsigenkänning i realtid ska kunna tillämpas för att lokalisera någon som anhållits eller häktats enligt lagen i syfte att verkställa frihetsberövandet. Detta innebär att tekniken får användas för att hitta personer som har anhållits eller häktats i sin frånvaro under en pågående utredning om överlämnande för lagföring eller straffverkställighet. De krav som uppställs i fråga om bl.a. avgränsningen till viss brottslighet enligt 4 § 4 lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål får då prövas av rätten mot den gärning som ligger till grund för arresteringsordern. Vid användning av tekniken tillämpas dessutom övriga bestämmelser, om t.ex. tillståndsprövning, omedelbart upphörande och underrättelser i den lagen med undantag för bestämmelserna om forum som ska följa av lagen om överlämnande från Sverige enligt en nordisk arresteringsorder.

18.8 Förslaget till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

1 kap.

4 § En utredningsåtgärd enligt denna lag ska avse eller motsvara

1. förhör under förundersökning,
2. bevisupptagning vid domstol,
3. förhör genom ljudöverföring eller ljud- och bildöverföring,
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, en åtgärd enligt 27 kap. 15 § eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § samma balk,
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning,
7. tillfälligt överförande av en frihetsberövad person,
8. rättsmedicinsk undersökning av en avliden person,
9. kontrollerad leverans,
10. bistånd i en brottsutredning med användning av en skyddsidentitet,
11. inhämtande av bevis som finns hos en myndighet,
12. *användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid, eller*
13. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.

Paragrafen innehåller en uppräkning av de utredningsåtgärder som en europeisk utredningsorder ska avse eller motsvara. Övervägandena finns i avsnitt 14.2.

I paragrafen införs en ny punkt som anger att en utredningsåtgärd enligt lagen ska avse eller motsvara användning av AI-system eller annan biometrisk fjärridentifiering i realtid enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

2 kap.

1 § En utredningsorder får utfärdas av åklagare för en utredningsåtgärd som avses i 1 kap. 4 § 1 och 3–*13*.

I paragrafen anges vilka utredningsåtgärder en utredningsorder kan omfatta i de fall en svensk åklagare utfärdar ordern. Övervägandena finns i avsnitt 13.2.

En punkt läggs till i hänvisningen i paragrafen. Ändringen innebär att en åklagare får utfärda en utredningsorder som omfattar användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

5 § Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser

1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,
2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning,

3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m., *eller*

4. användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken eller 17 § lagen (2020:62) om hemlig dataavläsning utfärda en utredningsorder för en åtgärd som anges i första stycket 1 eller 2. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, genomsökning på distans, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket, 10 d § andra stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller det som föreskrivs i rättegångsbalken eller annan författning för den åtgärd som avses.

Paragrafen innehåller bestämmelser om domstolens prövning av vissa utredningsåtgärder. Övervägandena finns i avsnitt 14.2.

I *första stycket* läggs användning av AI-system enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål till bland de utredningsåtgärder som kräver domstolsprövning innan åklagaren får utfärda en utredningsorder. Samma villkor gäller för domstolens prövning som vid den prövning som görs om åtgärden hade kunnat vidtas i Sverige.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

19 c § *En utredningsorder för användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid i en annan medlemsstat får endast avse en åtgärd enligt 4 § 1–4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

I paragrafen, som är ny, anges vilka åtgärder enligt lagen om AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål som en utredningsorder kan utfärdas för i Sverige. Övervägandena finns i avsnitt 14.2.

Enligt paragrafen får en utredningsorder utfärdas för åtgärder som anges i 4 § 1–4 lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Det handlar om användning för att lokalisera eller identifiera en person som misstänks vara utsatt för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken, eller för människoexploateringen enligt 4 kap. 1 b § brottsbalken om exploateringen avser sexuella tjänster (punkten 1), eller som är försvunnen och misstänks vara utsatt för brott (punkten 2), om det finns en överhängande risk för att personen kommer att begå ett allvarligt brott som innebär fara mot någon annans liv eller fysiska säkerhet (punkten 3), eller som skäligen kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet (punkten 4).

19 d § *Om en utredningsorder har utfärdats för användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska åklagare, om det inte längre finns skäl för ett tillstånd att använda systemet, omedelbart upphäva beslutet. Polismyndigheten eller Säkerhetspolisen ska omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.*

I paragrafen, som är ny, anges en skyldighet för åklagare att omedelbart upphäva ett beslut om tillstånd att använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid när det inte längre finns skäl för det. Övervägandena finns i avsnitt 14.2.

Paragrafen ska tillämpas när en utredningsorder har utfärdats för användning av AI-system i en annan medlemsstat. Paragrafen ger uttryck för att AI-system inte får användas när behovet har upphört. Det innebär exempelvis att även om ett tillstånd gäller för en lång tidsperiod ska användningen upphöra så fort det inte längre finns skäl för den. Det är åklagaren som ska säkerställa att beslutet omedelbart hävs. Polismyndigheten eller Säkerhetspolisen är skyldig att omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas. Paragrafen motsvarar regleringen om omedelbart upphörande av användningen i 12 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

3 kap.

4 § En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10, 11 *eller 12* får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda.

Paragrafen innehåller ett generellt krav på dubbel straffbarhet för de åtgärder som räknas upp. Övervägandena finns i avsnitt 14.2.

Ändringen i paragrafen innebär att för att kunna erkänna och verkställa en utredningsorder från en annan stat för användande av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid krävs att den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och att övriga förutsättningar enligt lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål och föreskrifter som har meddelats i anslutning till lagen är uppfyllda. Det innebär bl.a. att det även måste vara fråga om ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

37 c § *I fråga om underrättelse till en enskild enligt 17 och 18 §§ lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 36 § andra stycket tillämpas.*

Paragrafen, som är ny, innehåller bestämmelser om underrättelse till en enskild som varit föremål för ett beslut om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid. Övervägandena finns i avsnitt 14.2.

Genom hänvisningen till 36 § andra stycket blir flera av rättegångsbalkens regler tillämpliga vid underrättelsen. Vissa undantag görs dock från regleringen i rättegångsbalken. Det gäller bl.a. vid vilken tidpunkt en underrättelse ska ske och när en underrättelse kan underlåtas.

18.9 Förslaget till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket

3 kap.

6 a § *I frågor om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid tillämpas bestämmelserna i 4 kap. 3 a § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.*

Paragrafen, som är ny, innebär att vid användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska 4 kap. 3 a § i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder tillämpas. Övervägandena finns i avsnitt 14.2.

Hänvisningen till 4 kap. 3 a § lagen om överlämnande från Sverige enligt en europeisk arresteringsorder innebär att användningen av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid får användas för att hitta personer som har anhållits eller häktats i sin frånvaro under en pågående utredning om överlämnande för lagföring eller straffverkställighet. I övrigt hänvisas till kommentaren till nämnda paragraf.

Europeiska unionens officiella tidning

SV
L-serien

2024/1689

12.7.2024

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2024/1689

av den 13 juni 2024

om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artiklarna 16 och 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

med beaktande av Europeiska centralbankens yttrande ([2]),

med beaktande av Regionkommitténs yttrande ([3]),

i enlighet med det ordinarie lagstiftningsförfarandet ([4]),

och av följande skäl:

(1) Syftet med denna förordning är att förbättra den inre marknadens funktion genom att fastställa en enhetlig rättslig ram för i synnerhet utveckling, utsläppande på marknaden, ibruktagande och användning av system för artificiell intelligens (AI-system) i unionen i enlighet med unionens värden, främja användningen av människocentrerad och tillförlitlig artificiell intelligens (AI) och samtidigt säkerställa en hög skyddsnivå för hälsa, säkerhet och grundläggande rättigheter såsom fastställs i Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*), inbegripet demokrati, rättsstatens principer och miljöskydd, skydda mot skadliga effekter av AI-system i unionen, och stödja innovation. Denna förordning säkerställer fri rörlighet över gränserna för AI-baserade varor och tjänster, och förhindrar således att medlemsstaterna inför begränsningar av utvecklingen, saluföringen och användningen av AI- system, om sådana inte uttryckligen tillåts enligt denna förordning.

(2) Denna förordning bör tillämpas i enlighet med unionens värden, som fastställs i stadgan, och underlätta skyddet av fysiska personer, företag, demokratin, rättsstatens principer och miljöskyddet, och samtidigt främja innovation och sysselsättning och göra unionen ledande när det gäller användningen av tillförlitlig AI.

(3) AI-system kan enkelt utnyttjas inom ett stort antal olika ekonomiska sektorer och i många delar av samhället, inklusive över gränser, och kan enkelt cirkulera i hela unionen. Vissa medlemsstater har redan undersökt antagandet av nationella regler för att säkerställa att AI är tillförlitligt och säkert samt utvecklas och används i enlighet med skyldigheter som rör grundläggande rättigheter. Skiljaktiga nationella regler kan leda till fragmentering av den inre marknaden och minska rättssäkerheten för operatörer som utvecklar, importerar eller använder AI-system. En enhetlig och hög skyddsnivå bör därför säkerställas i hela unionen för att tillförlitlig AI ska uppnås, medan skillnader som hindrar den fria rörligheten för samt innovation inom och användning och spridning av AI-system och relaterade produkter och tjänster på den inre marknaden bör förhindras genom fastställande av enhetliga

([1]) EUT C 517, 22.12.2021, s. 56.
([2]) EUT C 115, 11.3.2022, s. 5.
([3]) EUT C 97, 28.2.2022, s. 60.
([4]) Europaparlamentets ståndpunkt av den 13 mars 2024 (ännu inte offentliggjord i EUT) och rådets beslut av den 21 maj 2024.

skyldigheter för operatörer och garanterande av ett enhetligt skydd för tvingande hänsyn till allmänintresset och personers rättigheter på hela den inre marknaden på grundval av artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget). I den utsträckning som denna förordning omfattar särskilda regler för skydd av individer när det gäller behandling av personuppgifter avseende begränsning av användningen av AI-system för biometrisk fjärridentifiering för brottsbekämpande ändamål, av användningen av AI-system för riskbedömningar av fysiska personer för brottsbekämpande ändamål och av användningen av AI-system för biometrisk kategorisering för brottsbekämpande ändamål, är det, när det gäller dessa särskilda regler, lämpligt att grunda denna förordning på artikel 16 i EUF-fördraget. Mot bakgrund av dessa särskilda regler och användningen av artikel 16 i EUF-fördraget är det lämpligt att samråda med Europeiska dataskyddsstyrelsen.

(4) AI ingår i en teknikfamilj under snabb utveckling som bidrar till en mängd ekonomiska, miljömässiga och samhälleliga vinster över hela spektrumet av näringslivssektorer och samhällsverksamheter. Genom att förbättra förutsägelserna, optimera verksamheter och resurstilldelning och individanpassa de digitala lösningar som är tillgängliga för enskilda och organisationer kan användningen av AI ge företag viktiga konkurrensfördelar och stödja socialt och miljömässigt fördelaktiga utfall, exempelvis inom hälso- och sjukvård, jordbruk, livsmedelssäkerhet, utbildning, media, sport, kultur, infrastrukturförvaltning, energi, transport och logistik, offentliga tjänster, säkerhet, rättsväsende, resurs- och energieffektivitet. Miljöövervakning, bevarande och återställande av biologisk mångfald och ekosystem samt begränsning av och anpassning till klimatförändringar.

(5) Samtidigt kan AI, beroende på omständigheterna kring den specifika tillämpningen, användningen och den tekniska utvecklingsnivån, ge upphov till risker och skada allmänna intressen och grundläggande rättigheter som skyddas av unionsrätten. Dessa skador kan vara materiella eller immateriella, inbegripet fysiska, psykologiska, samhälleliga eller ekonomiska skador.

(6) Med tanke på den stora inverkan som AI kan ha på samhället, och behovet av att bygga upp förtroende, är det mycket viktigt att AI och dess regelverk utvecklas i enlighet med unionens värden såsom de fastställs i artikel 2 i fördraget om Europeiska unionen (EU-fördraget), de grundläggande rättigheter och friheter som fastställs i fördragen och, enligt artikel 6 i EU-fördraget, stadgan. En förutsättning är att AI bör vara en människocentrerad teknik. Den bör fungera som ett verktyg för människor, med slutmålet att öka människors välbefinnande.

(7) För att säkerställa en konsekvent och hög skyddsnivå för allmänintressen på områdena hälsa, säkerhet och grundläggande rättigheter bör gemensamma regler fastställas för AI-system med hög risk. Dessa regler bör vara förenliga med stadgan, icke-diskriminerande och i linje med unionens internationella handelsåtaganden. De bör också ta hänsyn till den europeiska förklaringen om digitala rättigheter och principer för det digitala decenniet och de etiska riktlinjerna för tillförlitlig AI från högnivåexpertgruppen för artificiell intelligens (AI-expertgruppen).

(8) Därmed behövs en rättslig ram för unionen som fastställer harmoniserade regler för AI för att främja utvecklingen, användningen och spridningen av AI på den inre marknaden, varigenom samtidigt en hög skyddsnivå uppnås för allmänintressen, såsom hälsa, säkerhet och skydd av grundläggande rättigheter, inbegripet demokrati, rättsstatens principer och miljöskydd, såsom erkänns och skyddas enligt unionsrätten. För att uppnå detta syfte bör det fastställas regler som reglerar utsläppandet på marknaden, ibruktagandet och användningen 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. Dessa regler bör vara tydliga och robusta när det gäller att skydda grundläggande rättigheter, stödja nya innovativa lösningar, möjliggöra ett europeiskt ekosystem av offentliga och privata aktörer som skapar AI-system i linje med unionens värden och ta tillvara den digitala omställningens potential i hela unionen. Genom fastställandet av dessa regler, och åtgärder till stöd för innovation med särskild inriktning på små och medelstora företag, inbegripet uppstartsföretag, stöder denna förordning unionens mål att främja den europeiska människocentrerade AI-strategin och att bli världsledande inom utvecklingen av säker, tillförlitlig och etisk AI, såsom fastställts av Europeiska rådet ([5]), och den säkerställer skyddet av etiska principer, vilket särskilt har begärts av Europaparlamentet ([6]).

([5]) Europeiska rådet, extra möte i Europeiska rådet (den 1 och 2 oktober 2020) – Slutsatser, EUCO 13/20, 2020, s. 6.
([6]) Europaparlamentets resolution av den 20 oktober 2020 med rekommendationer till kommissionen om en ram för etiska aspekter av artificiell intelligens, robotteknik och tillhörande teknik (2020/2012(INL)).

(9) Harmoniserade regler som är tillämpliga på utsläppande på marknaden, ibruktagande och användning av AI-system med hög risk bör fastställas i enlighet med Europaparlamentets och rådets förordning (EG) nr 765/2008 ([7]), Europaparlamentets och rådets beslut nr 768/2008/EG ([8]) och Europaparlamentets och rådets förordning (EU) 2019/1020 ([9]) (*den nya lagstiftningsramen*). De harmoniserade regler som fastställs i den här förordningen bör gälla i alla sektorer och bör, i linje med den nya lagstiftningsramen, inte påverka befintlig unionsrätt, särskilt om dataskydd, konsumentskydd, grundläggande rättigheter, sysselsättning och skydd för arbetstagare, samt produktsäkerhet, vilken den här förordningen kompletterar. Alla rättigheter och rättsmedel som föreskrivs genom sådan unionsrätt för konsumenter, och andra personer som AI-system kan ha en negativ inverkan på, inbegripet när det gäller ersättning för eventuella skador enligt rådets direktiv 85/374/EEG ([10]), förblir som en följd av detta opåverkade och fullt tillämpliga. Vidare bör den här förordningen, när det gäller anställning och skydd för arbetstagare, därför inte påverka unionsrätten om socialpolitik och nationell arbetsrätt, i överensstämmelse med unionsrätten, om anställnings- och arbetsvillkor, inbegripet hälsa och säkerhet på arbetsplatsen och förhållandet mellan arbetsgivare och arbetstagare. Den här förordningen bör inte heller påverka utövandet av grundläggande rättigheter som erkänns i medlemsstaterna och på unionsnivå, inbegripet rätten eller friheten att strejka eller att vidta annan åtgärd som ingår i medlemsstaternas respektive arbetsmarknadsmodell, eller rätten att förhandla om, ingå och tillämpa kollektivavtal eller vidta kollektiva åtgärder i enlighet med nationell rätt. Den här förordningen bör inte påverka de bestämmelser som syftar till att förbättra arbetsvillkoren för plattformsarbete som fastställs i ett direktiv från Europaparlamentet och rådet om bättre arbetsvillkor för plattformsarbete. Dessutom syftar den här förordningen till att stärka effektiviteten hos sådana befintliga rättigheter och rättsmedel genom att särskilda krav och skyldigheter fastställs, bland annat när det gäller transparens, teknisk dokumentation och loggning avseende AI-system. Vidare bör de skyldigheter som åläggs olika operatörer som ingår i AI-värdekedjan enligt den här förordningen tillämpas utan att det påverkar nationell rätt i överensstämmelse med unionsrätten, med verkan att användningen av vissa AI-system begränsas när sådan rätt inte omfattas av den här förordningen eller eftersträvar andra legitima mål av allmänt intresse än dem som eftersträvas genom den här förordningen. Till exempel bör nationell arbetsrätt och nationell rätt om skydd av minderåriga, dvs. personer under 18 år, med beaktande av allmän kommentar nr 25 (2021) till FN:s barnkonvention om barns rättigheter i den digitala miljön, i den mån de inte är specifika för AI-system och eftersträvar andra legitima mål av allmänt intresse, inte påverkas av den här förordningen.

(10) Den grundläggande rätten till skydd av personuppgifter garanteras särskilt genom Europaparlamentets och rådets förordningar (EU) 2016/679 ([11]) och (EU) 2018/1725 ([12]) samt Europaparlamentets och rådets direktiv (EU) 2016/680 ([13]). Europaparlamentets och rådets direktiv 2002/58/EG ([14]) skyddar dessutom privatlivet och konfidentialitet vid kommunikation, bland annat genom att villkor föreskrivs för all lagring av personuppgifter och icke-personuppgifter i, och för åtkomst från, terminalutrustning. De unionsrättsakterna ger grunden för en hållbar och ansvarsfull databehandling, även i de fall då dataset innehåller en blandning av personuppgifter och icke-personuppgifter. Den här förordningen syftar inte till att påverka tillämpningen av befintlig unionsrätt om behandling av personuppgifter, inbegripet uppgifter och befogenheter för de oberoende tillsynsmyndigheter som är behöriga att övervaka efterlevnaden av dessa instrument. Den påverkar inte heller de skyldigheter som leverantörer och tillhandahållare av AI-system har i sin roll som personuppgiftsansvariga eller personuppgiftsbiträden enligt unionsrätten eller nationell rätt om skydd av personuppgifter, i den mån utformningen, utvecklingen eller användningen av AI-system inbegriper behandling av personuppgifter. Det är också lämpligt att klargöra att

([7]) Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och upphävande av förordning (EEG) nr 339/93 (EUT L 218, 13.8.2008, s. 30).

([8]) Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG (EUT L 218, 13.8.2008, s. 82).

([9]) Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 (EUT L 169, 25.6.2019, s. 1).

([10]) Rådets direktiv 85/374/EEG av den 25 juli 1985 om tillnärmning av medlemsstaternas lagar och andra författningar om skadeståndsansvar för produkter med säkerhetsbrister (EGT L 210, 7.8.1985, s. 29).

([11]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([12]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([13]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

([14]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (Direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

registrerade fortsätter att åtnjuta alla de rättigheter och garantier som de tillerkänns genom sådan unionsrätt, inbegripet de rättigheter som rör uteslutande automatiserat individuellt beslutsfattande, inbegripet profilering. Harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av AI-system som inrättas enligt den här förordningen bör underlätta ett effektivt genomförande och göra det möjligt för de registrerade att utöva sina rättigheter och andra rättsmedel som garanteras enligt unionsrätten om skydd av personuppgifter och av andra grundläggande rättigheter.

(11) Denna förordning bör inte påverka tillämpningen av bestämmelserna om ansvar för leverantörer av förmedlingstjänster i Europaparlamentets och rådets förordning (EU) 2022/2065 ([15]).

(12) Begreppet *AI-system* i denna förordning bör vara tydligt definierat och nära anpassat till det arbete som utförs av internationella organisationer som arbetar med AI för att säkerställa rättssäkerhet, underlätta internationell konvergens och bred acceptans, och samtidigt ge flexibilitet för att hantera den snabba tekniska utvecklingen på detta område. Dessutom bör definitionen baseras på centrala egenskaper hos AI-system som skiljer det från enklare traditionella programvarusystem eller programmeringsmetoder och inte omfatta system som bygger på de regler som fastställs endast av fysiska personer för att automatiskt utföra operationer. En viktig egenskap hos AI-system är deras förmåga att dra slutsatser. Denna slutsatsförmåga avser processen att erhålla utdata, såsom förutsägelser, innehåll, rekommendationer eller beslut, som kan påverka fysiska och virtuella miljöer och AI-systemens förmåga att härleda modeller eller algoritmer, eller både och, från indata eller data. De tekniker som gör inferens möjlig när ett AI-system byggs upp inbegriper metoder för maskininlärning för inlärning genom data om hur vissa mål uppnås, och logik- och kunskapsbaserade strategier som drar slutsatser av kodad kunskap om eller symbolisk representation av den uppgift som ska lösas. Ett AI-systems kapacitet att dra slutsatser går utöver grundläggande databehandling genom att möjliggöra inlärning, resonemang eller modellering. Termen *maskinbaserad* avser det faktum att AI-system körs på maskiner. Hänvisningen till uttryckliga eller underförstådda mål understryker att AI-system kan fungera enligt uttryckliga definierade mål eller underförstådda mål. AI-systemets mål kan skilja sig från AI-systemets avsedda ändamål i ett specifikt sammanhang. Vid tillämpningen av denna förordning bör miljöer förstås som de sammanhang där AI-systemen är i drift, medan utdata som genereras av AI-systemet återspeglar olika funktioner som utförs av AI-system och inbegriper förutsägelser, innehåll, rekommendationer eller beslut. AI-system är utformade för att fungera med varierande grad av autonomi, vilket innebär att de är oberoende av mänsklig kontroll i viss mån och har förmåga att fungera utan mänskligt ingripande. Den anpassningsförmåga som ett AI-system kan uppvisa när det införts avser förmågan till självlärande, vilket gör det möjligt för systemet att förändras under sin användning. AI-system kan användas fristående eller som komponent i en produkt, oavsett om systemet är fysiskt integrerat i produkten (inbyggt) eller tjänar produktens funktioner utan att vara integrerat i produkten (icke-inbyggt).

(13) Begreppet *tillhandahållare*, som det hänvisas till i denna förordning, bör tolkas som varje fysisk eller juridisk person, inbegripet en offentlig myndighet, offentlig byrå eller ett annat organ, som under eget överinseende använder ett AI-system, med undantag för om AI-systemet används under personlig icke-yrkesmässig verksamhet. Beroende på typen av AI-system kan användningen av systemet påverka andra personer än tillhandahållaren.

(14) Begreppet *biometriska uppgifter* som används i denna förordning bör tolkas mot bakgrund av begreppet biometriska uppgifter enligt definitionen i artikel 4.14 i förordning (EU) 2016/679, artikel 3.18 i förordning (EU) 2018/1725 och artikel 3.13 i direktiv (EU) 2016/680. Biometriska uppgifter kan ge möjlighet till autentisering, identifiering och kategorisering av fysiska personer och igenkänning av fysiska personers känslor.

(15) Begreppet *biometrisk identifiering*, som det hänvisas till i denna förordning, bör definieras som automatiserad igenkänning av fysiska, fysiologiska och beteendemässiga mänskliga särdrag såsom ansikte, ögonrörelser, kroppsform, röst, prosodi, gång, hållning, hjärtfrekvens, blodtryck, lukt eller tangenttryckningskarakteristik för att fastställa en enskild persons identitet genom att jämföra denna individs biometriska uppgifter med lagrade biometriska uppgifter tillhörande individer i en referensdatabas, oavsett om individen har givit sitt medgivande eller inte. Detta utesluter AI-system som är avsedda att användas för biometrisk verifiering, vilket inbegriper autentisering, vars enda syfte är att bekräfta att en specifik fysisk person är den person som denne utger sig för att vara och att bekräfta identiteten på en fysisk person med det enda syftet att få åtkomst till en tjänst, låsa upp en enhet eller ha säker tillgång till lokaler.

([15]) Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

(16) Begreppet *biometrisk kategorisering*, som det hänvisas till i denna förordning, bör definieras som att fysiska personer hänförs till särskilda kategorier på grundval av deras biometriska uppgifter. Sådana särskilda kategorier kan avse aspekter som kön, ålder, hårfärg, ögonfärg, tatueringar, beteende- eller personlighetsdrag, språk, religion, tillhörighet till nationell minoritet, sexuell läggning eller politisk åskådning. Detta omfattar inte system för biometrisk kategorisering som har en ren extrafunktion som är oupplösligt kopplad till en annan kommersiell tjänst, vilket innebär att funktionen av objektiva tekniska skäl inte kan användas utan den huvudsakliga tjänsten, och integreringen av denna funktion är inte ett sätt att kringgå tillämpligheten av reglerna i denna förordning. Filter som kategoriserar ansikts- eller kroppsegenskaper som används på marknadsplatser online kan till exempel utgöra en sådan extrafunktion, eftersom de kan användas endast i förhållande till den huvudsakliga tjänsten, som är att sälja en produkt genom att göra det möjligt för konsumenten att i förväg se produkten på sig själv och hjälpa konsumenten att fatta ett köpbeslut. Filter som används på sociala nätverkstjänster online och som kategoriserar ansikts- eller kroppsfunktioner för att göra det möjligt för användare att lägga till eller ändra bilder eller videor kan också betraktas som extrafunktioner, eftersom ett sådant filter inte kan användas utan den huvudsakliga tjänsten hos de sociala nätverkstjänsterna som utgörs av delning av innehåll online.

(17) Begreppet *system för biometrisk fjärridentifiering*, som det hänvisas till i denna förordning, bör definieras utifrån funktion, som ett AI-system avsett för identifiering av fysiska personer utan deras aktiva medverkan, vanligtvis på distans, genom jämförelse mellan en persons biometriska uppgifter och biometriska uppgifter i en referensdatabas, oavsett den specifika teknik, process eller typ av biometriska uppgifter som används. Sådana system för biometrisk fjärridentifiering används vanligtvis för att samtidigt uppfatta flera personer eller deras beteende för att avsevärt underlätta identifieringen av fysiska personer utan deras aktiva medverkan. Detta utesluter AI-system som är avsedda att användas för biometrisk verifiering, vilket inbegriper autentisering, vars enda syfte är att bekräfta att en specifik fysisk person är den person som denne utger sig för att vara, och system som används för att bekräfta identiteten på en fysisk person med det enda syftet att få åtkomst till en tjänst, låsa upp en enhet eller ha säker tillgång till lokaler. Detta uteslutande motiveras av att sådana system sannolikt har mindre inverkan på fysiska personers grundläggande rättigheter än de system för biometrisk fjärridentifiering som kan användas för behandling av biometriska uppgifter om ett stort antal personer utan deras aktiva medverkan. När det gäller system i *realtid* sker insamlingen av biometriska uppgifter, jämförelsen och identifieringen omedelbart, näst intill omedelbart eller under alla omständigheter utan betydande dröjsmål. I detta avseende bör det inte finnas något utrymme för att kringgå denna förordnings regler om användning i *realtid* av de berörda AI-systemen genom att medge mindre fördröjningar. Realtidssystem involverar *direktupptagningar* eller *näst intill direktupptagningar* av material, såsom videoupptagningar, genererade med kamera eller annan utrustning med liknande funktion. *Efterhandssystem* baseras däremot på redan insamlade biometriska uppgifter och jämförelsen och identifieringen sker med en betydande fördröjning. Detta involverar sådant material som bilder eller videoupptagningar som genereras genom övervakningskameror (CCTV) eller privat utrustning och som har genererats före användningen av systemet avseende de berörda fysiska personerna.

(18) Begreppet *system för känsloigenkänning*, som det hänvisas till i denna förordning, bör definieras som ett AI-system vars syfte är att identifiera eller uttyda fysiska personers känslor eller avsikter på grundval av deras biometriska uppgifter. Begreppet avser känslor eller avsikter som lycka, sorg, ilska, överraskning, avsky, förlägenhet, sinnesrörelse, skam, förakt, nöjdhet och förnöjelse. Det omfattar inte fysiska tillstånd, såsom smärta eller trötthet, inbegripet till exempel system som används för att upptäcka trötthetstillståndet hos yrkespiloter eller yrkeschaufförer i syfte att förebygga olyckor. Detta omfattar inte heller enbart upptäckt av lätt skönjbara uttryck, gester eller rörelser, såvida de inte används för att identifiera eller dra slutsatser om känslor. De uttrycken kan vara grundläggande ansiktsuttryck såsom en sur min eller ett leende, eller gester som rörelser av händer, armar eller huvud, eller egenskaper hos en persons röst, till exempel höjd röst eller viskningar.

(19) I denna förordning bör begreppet *allmänt tillgänglig plats* förstås som varje fysisk plats som är tillgänglig för ett obestämt antal fysiska personer och oberoende av om platsen i fråga är privatägd eller offentligägd, oberoende av den verksamhet för vilken platsen får användas, såsom handel, till exempel för affärer, restauranger, kaféer, för tjänster, till exempel banker, yrkesverksamhet, besöksnäring, för idrott, till exempel simbassänger, gym, arenor, för transport, till exempel buss-, tunnelbane- och järnvägsstationer, flygplatser, transportmedel, för underhållning, till exempel biografer, teatrar, museer, konsert- och konferenslokaler, eller för fritidsändamål eller annat, till exempel allmänna vägar och torg, parker, skogar, lekplatser. En plats bör även klassificeras som allmänt tillgänglig om tillträdet, oavsett potentiella kapacitets- eller säkerhetsbegränsningar, omfattas av vissa på förhand fastställda villkor som kan uppfyllas av ett obestämt antal personer, såsom köp av en biljett, förhandsregistrering eller en viss ålder. Däremot bör en plats inte anses vara allmänt tillgänglig om åtkomsten är begränsad till specifika och definierade fysiska personer antingen genom unionsrätt eller nationell rätt med direkt anknytning till allmän säkerhet eller säkerhet eller genom att den person som har relevant befogenhet avseende platsen tydligt uttrycker sin vilja. Den

faktiska möjligheten till tillträde, till exempel en olåst dörr, en öppen grind i ett stängsel, innebär inte att platsen är allmänt tillgänglig om det finns indikationer eller omständigheter som tyder på motsatsen, till exempel skyltar som förbjuder eller begränsar tillträde. Företags- och fabrikslokaler samt kontor och arbetsplatser till vilka avsikten är att endast berörda anställda och tjänsteleverantörer ska ha tillträde är platser som inte är allmänt tillgängliga. Allmänt tillgängliga platser bör inte omfatta fängelser eller gränskontrollområden. Vissa andra områden kan bestå av både områden som är allmänt tillgängliga och områden som inte är allmänt tillgängliga, såsom en korridor i ett privat bostadshus som krävs för tillträde till en läkarmottagning eller en flygplats. Onlineplatser omfattas inte eftersom de inte är fysiska platser. Det bör dock avgöras från fall till fall om en viss plats är tillgänglig för allmänheten, med beaktande av den individuella situationens särdrag.

(20) För att dra största möjliga nytta av AI-system och samtidigt skydda grundläggande rättigheter, hälsa och säkerhet och möjliggöra demokratisk kontroll bör AI-kunnighet förse leverantörer, tillhandahållare och berörda personer med de begrepp som krävs för att fatta välgrundade beslut om AI-system. Dessa begrepp kan variera med avseende på det relevanta sammanhanget och kan inbegripa förståelse av den korrekta tillämpningen av tekniska delar under AI-systemets utvecklingsfas, de åtgärder som ska tillämpas under dess användning, lämpliga sätt att tolka AI-systemets utdata och, när det gäller berörda personer, den kunskap som krävs för att förstå hur beslut som fattas med hjälp av AI kommer att påverka dem. I samband med tillämpningen av denna förordning bör AI-kunnighet ge alla relevanta aktörer i AI-värdekedjan de insikter som krävs för att säkerställa lämplig efterlevnad och korrekt efterlevnadskontroll. Dessutom kan ett brett genomförande av åtgärder för AI-kunnighet och införandet av lämpliga uppföljningsåtgärder bidra till att förbättra arbetsvillkoren och i slutändan upprätthålla konsolideringen av och innovationsbanan för tillförlitlig AI i unionen. Den europeiska styrelsen för artificiell intelligens (*styrelsen*) bör stödja kommissionen för att främja AI-kunnighet, allmänhetens medvetenhet om och förståelse av fördelar, risker, skyddsåtgärder, rättigheter och skyldigheter i samband med användningen av AI-system. I samarbete med berörda parter bör kommissionen och medlemsstaterna underlätta utarbetandet av frivilliga uppförandekoder för att öka AI-kunnigheten hos personer som arbetar med utveckling, drift och användning av AI.

(21) För att säkerställa lika villkor och ett effektivt skydd av individers rättigheter och friheter i hela unionen bör de regler som fastställs genom denna förordning tillämpas på leverantörer av AI-system på ett icke-diskriminerande sätt, oavsett om de är etablerade i unionen eller i ett tredjeland, och på tillhandahållare av AI-system som är etablerade i unionen.

(22) Mot bakgrund av deras digitala natur bör vissa AI-system omfattas av denna förordning även om de inte släpps ut på marknaden, tas i bruk eller används i unionen. Detta är exempelvis fallet om en operatör som är etablerad i unionen lägger ut vissa tjänster på entreprenad hos en operatör som är etablerad i ett tredjeland i fråga om en aktivitet som ska utföras av ett AI-system som skulle klassificeras som AI-system med hög risk. Under dessa omständigheter kan det AI-system som används i ett tredjeland av operatören behandla data som på lagligt sätt samlats in och överförts från unionen och förse den avtalsslutande operatören i unionen med utdata från detta AI-system som är resultatet av denna behandling, utan att det berörda AI-systemet släpps ut på marknaden, tas i bruk eller används i unionen. För att förhindra att denna förordning kringgås och säkerställa ett effektivt skydd av fysiska personer som befinner sig i unionen, bör denna förordning också tillämpas på leverantörer och tillhandahållare av AI-system som är etablerade i tredjeländer, i den utsträckning som de utdata som produceras av dessa AI-system är avsedda att användas i unionen. För att ta hänsyn till befintliga arrangemang och särskilda behov av framtida samarbete med utländska partner med vilka information och bevis utbyts, bör denna förordning dock inte tillämpas på offentliga myndigheter i ett tredjeland eller internationella organisationer som agerar inom ramen för samarbete eller internationella avtal som ingåtts på unionsnivå eller nationell nivå och som avser brottsbekämpande och rättsligt samarbete med unionen eller medlemsstaterna, förutsatt att det tredjeland eller den internationella organisation som berörs erbjuder tillräckliga skyddsåtgärder vad avser skyddet av enskildas grundläggande rättigheter och friheter. I relevanta fall kan detta omfatta verksamhet som bedrivs av enheter som av tredjeländerna fått i uppdrag att utföra särskilda uppgifter till stöd för sådant brottsbekämpande och rättsligt samarbete. Sådana ramar för samarbete eller avtal har fastställts bilateralt mellan medlemsstater och tredjeländer eller mellan Europeiska unionen, Europol och andra unionsbyråer och tredjeländer och internationella organisationer. De myndigheter som är behöriga att utöva tillsyn över brottsbekämpande och rättsliga myndigheter enligt denna förordning bör bedöma huruvida dessa ramar för samarbete eller internationella avtal innehåller lämpliga skyddsåtgärder med avseende på skyddet av enskildas

grundläggande rättigheter och friheter. Mottagande nationella myndigheter och unionsinstitutioner, unionsbyråer och unionsorgan som använder sådana utdata i unionen förblir ansvariga för att säkerställa att användningen av dessa är förenlig med unionsrätten. När dessa internationella avtal ses över eller när nya ingås i framtiden bör de avtalsslutande parterna göra sitt yttersta för att anpassa dessa avtal till kraven i denna förordning.

(23) Denna förordning bör också tillämpas på unionens institutioner, organ och byråer när de agerar som leverantör eller tillhandahållare av ett AI-system.

(24) Om och i den mån AI-system släpps ut på marknaden, tas i bruk eller används med eller utan ändringar av sådana system för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet, bör dessa undantas från denna förordnings tillämpningsområde, oberoende av vilken typ av enhet som bedriver denna verksamhet, till exempel huruvida det är en offentlig eller privat enhet. När det gäller militära ändamål och försvarsändamål motiveras ett sådant undantagande både av artikel 4.2 i EU-fördraget och av särdragen i medlemsstaternas och unionens gemensamma försvarspolitik som omfattas av kapitel 2 i avdelning V i EU-fördraget och som omfattas av folkrätten, som därför är den lämpligaste rättsliga ramen för reglering av AI-system i samband med användning av dödligt våld och andra AI-system inom ramen för militär verksamhet och försvarsverksamhet. När det gäller ändamål som rör nationell säkerhet motiveras undantagandet både av att nationell säkerhet helt och hållet faller under medlemsstaternas ansvarsområde i enlighet med artikel 4.2 i EU-fördraget och av den särskilda karaktär och de operativa behov som verksamheten avseende nationell säkerhet har samt av de särskilda nationella regler som är tillämpliga på denna verksamhet. Om ett AI-system som utvecklas, släpps ut på marknaden, tas i bruk eller används för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet tillfälligt eller permanent används för andra ändamål, till exempel civila eller humanitära ändamål, eller ändamål som rör brottsbekämpning eller allmän säkerhet, skulle ett sådant system ändå omfattas av denna förordning. I så fall bör den enhet som använder AI-systemet för andra ändamål än militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet säkerställa att AI-systemet överensstämmer med denna förordning, såvida inte systemet redan är förenligt med denna förordning. AI-system som släpps ut på marknaden eller tas i bruk för ett ändamål som är undantaget, dvs. militärt eller som rör försvar eller nationell säkerhet, och ett eller flera icke-undantagna ändamål, såsom civila ändamål eller brottsbekämpning, omfattas av denna förordning, och leverantörer av dessa system bör säkerställa efterlevnad av denna förordning. I dessa fall bör det faktum att ett AI-system kan omfattas av denna förordning inte påverka möjligheten för enheter som bedriver verksamhet inom nationell säkerhet, försvarsverksamhet och militär verksamhet, oavsett vilken typ av enhet som bedriver denna verksamhet, att använda AI-system för nationell säkerhet, militära ändamål och försvarsändamål, vars användning är undantagen från denna förordnings tillämpningsområde. Ett AI-system som släpps ut på marknaden för civila eller brottsbekämpande ändamål och som används med eller utan ändringar för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet bör inte omfattas av denna förordning, oavsett vilken typ av enhet som bedriver denna verksamhet.

(25) Denna förordning bör stödja innovation, respektera forskningens frihet och inte underminera forsknings- och utvecklingsverksamhet. Det är därför nödvändigt att från dess tillämpningsområde undanta AI-system och AI-modeller som särskilt utvecklats och tagits i bruk enbart för vetenskaplig forskning och utveckling. Det är dessutom nödvändigt att säkerställa att denna förordning inte på annat sätt påverkar vetenskaplig forsknings- och utvecklingsverksamhet avseende AI-system eller AI-modeller innan dessa släpps ut på marknaden eller tas i bruk. Inte heller när det gäller produktorienterad forsknings-, testnings- och utvecklingsverksamhet avseende AI-system eller AI-modeller bör bestämmelserna i denna förordning tillämpas innan dessa system och modeller tas i bruk eller släpps ut på marknaden. Detta undantagande påverkar inte skyldigheten att följa denna förordning om ett AI-system som faller inom tillämpningsområdet för denna förordning släpps ut på marknaden eller tas i bruk till följd av sådan forsknings- och utvecklingsverksamhet eller tillämpningen av bestämmelser om regulatoriska sandlådor för AI och testning under verkliga förhållanden. Utan att det påverkar tillämpningen av undantagandet av AI-system som särskilt utvecklats och tagits i bruk enbart för vetenskaplig forskning och utveckling bör andra AI-system som kan användas för att genomföra forsknings- och utvecklingsverksamhet även fortsättningsvis omfattas av bestämmelserna i denna förordning. All forsknings- och utvecklingsverksamhet bör under alla omständigheter genomföras i enlighet med erkända etiska och yrkesmässiga standarder för vetenskaplig forskning och bör bedrivas i enlighet med tillämplig unionsrätt.

(26) För att införa en proportionell och effektiv uppsättning bindande regler för AI-system bör en tydligt definierad riskbaserad metod användas. Denna metod bör innebära att dessa reglers art och innehåll anpassas till intensiteten och omfattningen av de risker som AI-systemen kan generera. Det är därför nödvändigt att förbjuda vissa oacceptabla AI-användningsområden, fastställa vissa krav för AI-system med hög risk och skyldigheter för berörda operatörer samt fastställa transparensskyldigheter för vissa AI-system.

(27) Den riskbaserade metoden utgör grunden för en proportionell och effektiv uppsättning bindande regler, men det är viktigt att påminna om de etiska riktlinjer för tillförlitlig AI från 2019 som utarbetats av den oberoende AI-expertgruppen, som utsetts av kommissionen. I dessa riktlinjer utarbetade AI-expertgruppen sju icke-bindande etiska principer för AI som bör bidra till att säkerställa att AI är tillförlitlig och etiskt sund. De sju principerna omfattar mänskligt agentskap och mänsklig tillsyn, teknisk robusthet och säkerhet, integritet och dataförvaltning, transparens, mångfald, icke-diskriminering och rättvisa, samhällets och miljöns välbefinnande samt ansvarsskyldighet. Utan att det påverkar de rättsligt bindande kraven i denna förordning och annan tillämplig unionsrätt bidrar dessa riktlinjer till utformningen av konsekvent, tillförlitlig och människocentrerad AI, i linje med stadgan och de värden som unionen bygger på. Enligt AI-expertgruppens riktlinjer innebär mänskligt agentskap och mänsklig tillsyn att AI-system utvecklas och används som ett verktyg som tjänar människor, respekterar mänsklig värdighet och personlig självständighet och ska fungera så att de på ett lämpligt sätt kan kontrolleras och övervakas av människor. Teknisk robusthet och säkerhet innebär att AI-system ska utvecklas och användas på ett sätt som möjliggör robusthet i händelse av problem och resiliens mot försök att ändra AI-systemets användning eller prestanda för att möjliggöra olaglig användning från tredje parters sida, och minimerar oavsiktlig skada. Integritet och dataförvaltning innebär att AI-system utvecklas och används i enlighet med integritets- och dataskyddsregler, samtidigt som data som uppfyller höga standarder i fråga om kvalitet och integritet behandlas. Transparens innebär att AI-system utvecklas och används på ett sätt som möjliggör lämplig spårbarhet och förklarbarhet, samtidigt som människor informeras om att de kommunicerar eller interagerar med ett AI-system och att tillhandahållare vederbörligen informeras om AI-systemets kapacitet och begränsningar samt att personer som påverkas informeras om sina rättigheter. Mångfald, icke-diskriminering och rättvisa innebär att AI-system utvecklas och används på ett sätt som inkluderar olika aktörer och främjar lika tillgång, jämställdhet och kulturell mångfald, samtidigt som diskriminerande effekter och oskäliga biaser, som är förbjudna enligt unionsrätten eller nationell rätt undviks. Samhällets och miljöns välbefinnande innebär att AI-system utvecklas och används på ett hållbart och miljövänligt sätt samt för att gynna alla människor, samtidigt som de långsiktiga effekterna för individen, samhället och demokratin övervakas och bedöms. Tillämpningen av dessa principer bör, när så är möjligt, omsättas i utformningen och användningen av AI-modeller. De bör under alla omständigheter ligga till grund för utarbetandet av uppförandekoder inom ramen för denna förordning. Alla berörda parter, inbegripet industrin, den akademiska världen, det civila samhället och standardiseringsorganisationer, uppmanas att på lämpligt sätt beakta de etiska principerna för utveckling av frivillig bästa praxis och standarder.

(28) Vid sidan av de många nyttiga användningsområdena för AI kan den också missbrukas och tillhandahålla nya och kraftfulla verktyg för manipulation, utnyttjande och social kontroll. Sådana användningsområden är särskilt skadliga och kränkande och bör förbjudas eftersom de strider mot unionens värden och respekten för människans värdighet, frihet, jämlikhet, demokrati och rättsstatens principer samt grundläggande rättigheter som fastställs i stadgan, inbegripet rätten till icke-diskriminering, dataskydd och personlig integritet samt barnets rättigheter.

(29) AI-baserad manipulativ teknik kan användas för att övertyga personer att ägna sig åt oönskat beteende, eller för att vilseleda dem genom att driva dem till beslut på ett sätt som undergräver och försämrar deras autonomi, beslutsfattande och fria val. Utsläppandet på marknaden, ibruktagandet eller användningen av vissa AI-system med målet eller följden att det mänskliga beteendet väsentligt påverkas och som sannolikt kan medföra betydande skador, i synnerhet med tillräckligt betydande negativa konsekvenser för den fysiska eller psykiska hälsan eller ekonomiska intressen, är särskilt farliga och bör därför förbjudas. Sådana AI-system utnyttjar subliminala komponenter såsom ljud-, bild- och videostimuli som människor inte kan uppfatta, eftersom dessa stimuli ligger utanför människans uppfattningsförmåga, eller annan manipulativ eller vilseledande teknik som undergräver eller försämrar människors autonomi, beslutsfattande eller fria val på sätt där människor inte är medvetna om denna teknik, eller om de är medvetna om den, fortfarande kan vilseledas eller inte kan kontrollera eller stå emot den. Detta kan underlättas av till exempel maskin–hjärna-gränssnitt eller virtuell verklighet eftersom det möjliggör en högre grad av kontroll av vilka stimuli som personer utsätts för, i den mån som de väsentligt kan påverka deras beteende på ett betydande skadligt sätt. Dessutom kan AI-system också på annat sätt utnyttja sårbarheterna hos en person eller en viss grupp av personer på grund av ålder, funktionsnedsättning i den mening som avses i Europaparlamentets och rådets direktiv (EU) 2019/882 ([16]) eller en specifik social eller ekonomisk situation som sannolikt kommer att göra dessa personer mer sårbara för utnyttjande, såsom personer som lever i extrem fattigdom, etniska minoriteter eller religiösa minoriteter. Sådana AI-system kan släppas ut på marknaden, tas i bruk eller användas med målet eller verkan att väsentligt påverka en persons beteende och på ett sätt som orsakar eller med rimlig sannolikhet kommer att orsaka betydande skada för den personen eller en annan person eller grupper av personer, inbegripet skador som kan

([16]) Europaparlamentets och rådets direktiv (EU) 2019/882 av den 17 april 2019 om tillgänglighetskrav för produkter och tjänster (EUT L 151, 7.6.2019, s. 70).

ackumuleras över tid, och bör därför förbjudas. Det är kanske inte möjligt att anta att det finns en avsikt att påverka beteendet, om påverkan beror på faktorer utanför AI-systemet som ligger utanför leverantörens eller tillhandahållarens kontroll, dvs. faktorer som kanske inte är rimligen förutsebara och därför inte kan begränsas av leverantören eller tillhandahållaren av AI-systemet. I alla händelser är det inte nödvändigt att leverantören eller tillhandahållaren har för avsikt att orsaka den betydande skadan, förutsatt att sådan skada beror på de manipulativa eller utnyttjande AI-baserade användningsområdena. Förbuden mot sådana AI-användningsområden kompletterar bestämmelserna i Europaparlamentets och rådets direktiv 2005/29/EG ([17]), särskilt att otillbörliga affärsmetoder som leder till ekonomisk eller finansiell skada för konsumenter är förbjudna under alla omständigheter, oavsett om de har införts genom AI-system eller på annat sätt. Förbuden mot manipulativa och utnyttjande användningsområden i denna förordning bör inte påverka lagliga användningsområden i samband med medicinsk behandling, såsom psykologisk behandling av en psykisk sjukdom eller fysisk rehabilitering, när denna användning sker i enlighet med tillämplig lag och tillämpliga medicinska normer, till exempel de enskilda personernas eller deras ombuds uttryckliga samtycke. Dessutom bör vanliga och legitima affärsmetoder, till exempel på reklamområdet, som är förenliga med tillämplig rätt inte i sig anses utgöra skadliga manipulativa AI-baserade metoder.

(30) System för biometrisk kategorisering som baseras på fysiska personers biometriska uppgifter, såsom en enskild persons ansikte eller fingeravtryck, för att härleda eller dra slutsatser om en persons politiska åsikter, medlemskap i fackförening, religiösa eller filosofiska övertygelse, ras, sexualliv eller sexuella läggning bör förbjudas. Detta förbud omfattar inte laglig märkning, filtrering eller kategorisering av biometriska dataset som förvärvats i enlighet med unionsrätten eller nationell rätt på grundval av biometriska uppgifter, såsom sortering av bilder enligt hår- eller ögonfärg, som till exempel kan användas inom brottsbekämpning.

(31) AI-system som tillhandahåller offentliga eller privata aktörers sociala poängsättning av fysiska personer kan medföra diskriminering och uteslutning av vissa grupper. De kan strida mot rätten till värdighet och icke-diskriminering och värdena jämlikhet och rättvisa. Sådana AI-system utvärderar eller klassificerar fysiska personer eller grupper av sådana på grundval av flera datapunkter relaterade till deras sociala beteende i olika sammanhang eller kända, uttydda eller förutsedda personliga egenskaper eller personlighetsegenskaper under vissa tidsperioder. Den sociala poängsättning som erhålls från sådana AI-system kan leda till negativ eller ogynnsam behandling av fysiska personer eller hela grupper av fysiska personer i sociala sammanhang som saknar koppling till det sammanhang där berörda data ursprungligen genererades eller samlades in, eller till en negativ behandling som är oproportionerlig eller omotiverad i förhållande till hur allvarligt deras sociala beteende är. AI-system som medför sådana oacceptabla poängsättningsmetoder och som leder till sådana negativa eller ogynnsamma resultat bör därför förbjudas. Detta förbud bör inte påverka lagliga metoder för bedömning av fysiska personer som utförs för ett specifikt ändamål i enlighet med unionsrätten och nationell rätt.

(32) Användningen av system för biometrisk fjärridentifiering i *realtid* av fysiska personer på allmänt tillgängliga platser för brottsbekämpande ändamål inkräktar särskilt på de berörda personernas rättigheter och friheter, i och med att denna användning kan påverka privatlivet för en stor del av befolkningen, kan skapa en känsla av konstant övervakning och indirekt avskräcka från utövande av mötesfrihet och andra grundläggande rättigheter. Tekniska brister i AI-system som är avsedda för biometrisk fjärridentifiering av fysiska personer kan leda till biaser i resultat och medföra diskriminerande effekter. Sådana eventuella biaser i resultat och diskriminerande effekter är särskilt relevanta när det gäller ålder, etnicitet, ras, kön eller funktionsnedsättning. De omedelbara effekterna och de begränsade möjligheterna till ytterligare kontroll eller korrigering när det gäller användningen av sådana system som fungerar i realtid innebär ökade risker för rättigheterna och friheterna för berörda personer i samband med, eller som påverkas av, brottsbekämpande verksamhet.

(33) Användningen av sådana system för brottsbekämpning bör därför vara förbjuden, utom i de snävt definierade situationer som anges i den uttömmande förteckningen, i de fall då användningen är strikt nödvändig för att uppnå ett väsentligt allmänintresse vars betydelse är större än riskerna. Dessa situationer inbegriper sökandet efter vissa brottsoffer, inklusive försvunna personer, vissa hot mot fysiska personers liv eller fysiska säkerhet eller hot om en terroristattack, och lokalisering eller identifiering av gärningsmän till eller misstänkta för brott som förtecknas i en bilaga till denna förordning, om dessa brott i den berörda medlemsstaten kan leda till fängelse eller annan

([17]) Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (*direktiv om otillbörliga affärsmetoder*) (EUT L 149, 11.6.2005, s. 22).

frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år och i enlighet med fastställda brottsrekvisit för dessa brott i den medlemsstatens nationella rätt. En sådan tröskel för påföljden fängelse eller annan frihetsberövande åtgärd i enlighet med nationell rätt bidrar till att säkerställa att brottet är allvarligt nog för att potentiellt motivera användningen av system för biometrisk fjärridentifiering i *realtid*. Vidare grundas förteckningen över brott i en bilaga till denna förordning på de 32 brott som förtecknas i rådets rambeslut 2002/584/RIF ([18]), med beaktande av att vissa av dessa brott i praktiken sannolikt kommer att vara mer relevanta än andra, i och med att det kommer att variera mycket hur nödvändig och proportionell användningen av biometrisk fjärridentifiering i *realtid* kan förutses vara för det praktiska arbetet med lokalisering eller identifiering av gärningsmän eller misstänkta när det gäller brott som anges i förteckningen, och med beaktande av de sannolika skillnaderna vad gäller allvarlighetsgrad, sannolikhet och omfattning på skadan eller de möjliga negativa konsekvenserna. Ett överhängande hot mot en persons liv eller fysiska säkerhet kan också vara följden av en allvarlig driftsstörning vid kritisk infrastruktur enligt definitionen i artikel 2.4 i Europaparlamentets och rådets direktiv (EU) 2022/2557 ([19]), om en driftsstörning vid eller förstörelse av sådan kritisk infrastruktur skulle leda till en omedelbar fara för en persons liv eller fysiska säkerhet, inbegripet genom allvarlig skada på tillhandahållandet av basförnödenheter till befolkningen eller på utövandet av statens kärnfunktion. Dessutom bör denna förordning bevara möjligheten för brottsbekämpande myndigheter, gränskontrollmyndigheter, immigrations- eller asylmyndigheter att utföra identitetskontroller i närvaro av den berörda personen i enlighet med villkoren i unionsrätten och nationell rätt för sådana kontroller. I synnerhet bör brottsbekämpande myndigheter, gränskontrollmyndigheter, migrationsmyndigheter eller asylmyndigheter kunna använda informationssystem, i enlighet med unionsrätten eller nationell rätt, för att identifiera personer som under en identitetskontroll antingen vägrar att identifieras eller inte kan ange eller bevisa sin identitet, utan att det enligt denna förordning krävs förhandstillstånd. Detta kan till exempel röra sig om en person som är inblandad i ett brott, är ovillig eller på grund av en olycka eller ett medicinskt tillstånd är oförmögen att uppge sin identitet för brottsbekämpande myndigheter.

(34) För att säkerställa att dessa system används på ett ansvarsfullt och proportionellt sätt är det också viktigt att fastställa att hänsyn bör tas till vissa faktorer i var och en av de snävt definierade situationerna i den uttömmande förteckningen, i synnerhet vad gäller arten av den situation som ger upphov till begäran och användningens konsekvenser för alla berörda personers rättigheter och friheter samt de skyddsåtgärder och villkor som föreskrivs i samband med användningen. Användningen av system för biometrisk fjärridentifiering i *realtid* på allmänt tillgänglig plats för brottsbekämpande ändamål bör utnyttjas endast för att bekräfta identiteten på den individ som särskilt avses och bör begränsas till vad som är strikt nödvändigt vad gäller tidsperiod samt det geografiska tillämpningsområdet och de personer som omfattas, med särskild hänsyn till bevis eller indikationer vad gäller hoten, offren eller gärningsmännen. Användningen av systemet för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats bör tillåtas endast om den relevanta brottsbekämpande myndigheten har slutfört en konsekvensbedömning avseende grundläggande rättigheter och, om inte annat föreskrivs i denna förordning, har registrerat systemet i den databas som föreskrivs i denna förordning. Referensdatabasen över personer bör vara ändamålsenlig för varje användningsfall i var och en av de situationer som anges ovan.

(35) Varje användning av system för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser för brottsbekämpande ändamål bör vara föremål för ett uttryckligt och specifikt tillstånd som lämnas av en rättslig myndighet eller en oberoende administrativ myndighet i en medlemsstat vars beslut är bindande. Dessa tillstånd bör i princip erhållas innan AI-systemet används för att identifiera en eller flera personer. Undantag från denna regel bör tillåtas av hänsyn till vederbörligen motiverade brådskande situationer, dvs. situationer då behovet av att använda de ifrågavarande systemen är sådant att det i praktiken är objektivt omöjligt att erhålla ett tillstånd innan användningen av AI-systemet inleds. I sådana brådskande situationer bör användningen av AI-systemet begränsas till det absoluta minimum som är nödvändigt och bör omfattas av lämpliga skyddsmekanismer och villkor som fastställs i nationell rätt och som specificeras av den berörda brottsbekämpande myndigheten i samband med varje enskilt fall av brådskande användning. Dessutom bör den brottsbekämpande myndigheten i sådana situationer begära ett sådant tillstånd samtidigt som den anger skälen till att den inte har kunnat begära det tidigare, utan oskäligt dröjsmål och senast inom 24 timmar. Om ett sådant tillstånd nekas bör användningen av system för biometrisk identifiering i realtid som är kopplade till det tillståndet stoppas med omedelbar verkan och alla uppgifter som rör sådan användning bör förstöras och raderas. Sådana data omfattar indata som erhållits direkt av ett AI-system i samband

([18]) 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).

([19]) Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (EUT L 333, 27.12.2022, s. 164).

med användningen av ett sådant system samt resultat och utdata från den användning som är kopplad till det tillståndet. Det bör inte omfatta indata som lagligen förvärvats i enlighet med annan unionsrätt eller nationell rätt. Under inga omständigheter bör beslut som har negativa rättsliga följder för en person fattas enbart på grundval av utdata från systemet för biometrisk fjärridentifiering.

(36) För att kunna utföra sina uppgifter i enlighet med kraven i denna förordning och i nationella regler bör den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten underrättas om varje användning av systemet för biometrisk identifiering i realtid. Marknadskontrollmyndigheterna och de nationella dataskyddsmyndigheter som har underrättats bör lämna in en årlig rapport till kommissionen om användningen av system för biometrisk identifiering i realtid.

(37) Det är också lämpligt att, inom den uttömmande ram som fastställs genom denna förordning, föreskriva att en sådan användning på en medlemsstats territorium i enlighet med denna förordning endast bör vara möjlig i de fall och i den utsträckning som den berörda medlemsstaten har beslutat att uttryckligen föreskriva möjligheten att tillåta sådan användning i sina närmare bestämmelser i nationell rätt. Enligt denna förordning behåller alltså medlemsstaterna sin frihet att inte alls föreskriva någon sådan möjlighet eller att endast föreskriva en sådan möjlighet med avseende på några av de syften som kan motivera användning som tillåten enligt denna förordning. Sådana nationella bestämmelser bör anmälas till kommissionen senast 30 dagar efter det att de har antagits.

(38) Användningen av system för biometrisk fjärridentifiering i realtid av fysiska personer på allmänt tillgängliga platser för brottsbekämpande ändamål involverar med nödvändighet behandling av biometriska uppgifter. Reglerna i denna förordning som med vissa undantag förbjuder sådan användning, och som baseras på artikel 16 i EUF-fördraget, bör tillämpas som *lex specialis* med avseende på de regler om behandling av biometriska uppgifter som anges i artikel 10 i direktiv (EU) 2016/680, och reglerar därmed sådan användning och behandling av berörda biometriska uppgifter på ett uttömmande sätt. Därför bör sådan användning och behandling vara möjlig endast i den utsträckning som den är förenlig med den ram som fastställs i denna förordning, utan att de behöriga myndigheterna har något utrymme, då de agerar för brottsbekämpande ändamål, att utanför den ramen använda sådana system och behandla sådana data i samband med detta av de skäl som förtecknas i artikel 10 i direktiv (EU) 2016/680. I det sammanhanget är denna förordning inte avsedd att tillhandahålla en rättslig grund för behandling av personuppgifter enligt artikel 8 i direktiv (EU) 2016/680. Användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för andra ändamål än brottsbekämpning, inbegripet av behöriga myndigheter, bör inte omfattas av den särskilda ram för sådan användning för brottsbekämpande ändamål som fastställs i denna förordning. Sådan användning för andra ändamål än brottsbekämpning bör därför inte omfattas av kravet på tillstånd enligt denna förordning och de tillämpliga närmare bestämmelser i nationell rätt som kan ge verkan åt det tillståndet.

(39) Användning av biometriska uppgifter och andra personuppgifter i samband med användningen av AI-system för biometrisk identifiering som inte sker i samband med användning av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för brottsbekämpande ändamål som regleras av denna förordning bör även fortsättningsvis uppfylla alla krav som följer av artikel 10 i direktiv (EU) 2016/680. För andra ändamål än brottsbekämpning förbjuds enligt artikel 9.1 i förordning (EU) 2016/679 och artikel 10.1 i förordning (EU) 2018/1725 behandling av biometriska uppgifter med förbehåll för begränsade undantag enligt de artiklarna. Med tillämpning av artikel 9.1 i förordning (EU) 2016/679 har användningen av biometrisk fjärridentifiering för andra ändamål än brottsbekämpning redan förbjudits av nationella dataskyddsmyndigheter.

(40) I enlighet med artikel 6a i protokoll nr 21 om Förenade kungarikets och Irlands ställning med avseende på området med frihet, säkerhet och rättvisa, fogat till EU-fördraget och EUF-fördraget, är Irland inte bundet av reglerna i artikel 5.1 första stycket g i den mån den är tillämplig på system för biometrisk kategorisering inom polissamarbete och straffrättsligt samarbete, artikel 5.1 första stycket d i den mån den är tillämplig på användning av AI-system som omfattas av den bestämmelsen, artikel 5.1 första stycket h samt artiklarna 5.2–5.6 och 26.10 i denna förordning som antagits på grundval av artikel 16 i EUF-fördraget och som avser medlemsstaternas behandling av personuppgifter när de bedriver verksamhet som omfattas av avdelning V kapitel 4 eller 5 i tredje delen av EUF-fördraget i det fall då Irland inte är bundet av bestämmelserna om formerna för straffrättsligt samarbete eller polissamarbete inom ramen för vilka de bestämmelser måste iakttas som fastställs på grundval av artikel 16 i EUF-fördraget.

(41) I enlighet med artiklarna 2 och 2a i protokoll nr 22 om Danmarks ställning, fogat till EU-fördraget och EUF-fördraget, är Danmark inte bundet av reglerna i artikel 5.1 första stycket g i den mån den är tillämplig på användning av system för biometrisk kategorisering inom polissamarbete och straffrättsligt samarbete, artikel 5.1 första stycket d i den mån den är tillämplig på användning av AI-system som omfattas av den bestämmelsen, artikel 5.1 första stycket h samt artiklarna 5.2–5.6 och 26.10 i denna förordning som antagits på grundval av

artikel 16 i EUF-fördraget, eller tillämpningen av dessa, som avser medlemsstaternas behandling av personuppgifter när dessa utövar verksamhet som omfattas av tillämpningsområdet för avdelning V kapitel 4 eller 5 i tredje delen av EUF-fördraget.

(42) I enlighet med presumtionen för oskuld bör fysiska personer i unionen alltid bedömas utifrån sitt faktiska beteende. Fysiska personer bör aldrig bedömas på grundval av genom AI förutsett beteende enbart grundat på deras profilering, personlighetsdrag eller egenskaper, såsom nationalitet, födelseort, bostadsort, antal barn, skuldsättning eller typ av bil, utan rimlig misstanke om att personen är inblandad i en brottslig verksamhet på grundval av objektiva, kontrollerbara fakta och utan mänsklig bedömning av detta. Därför bör riskbedömningar som genomförs med avseende på fysiska personer för att bedöma sannolikheten för att de begår brott eller för att förutsäga förekomsten av ett faktiskt eller potentiellt brott enbart på grundval av deras profilering eller en bedömning av deras personlighetsdrag och egenskaper förbjudas. I vilket fall som helst avser eller berör förbudet inte riskanalyser som inte baseras på profilering av enskilda personer eller på enskilda personers personlighetsdrag och egenskaper, såsom AI-system som använder riskanalyser för att bedöma sannolikheten för ekonomiska bedrägerier från företags sida på grundval av misstänkta transaktioner eller riskanalysverktyg för förutsägelser om sannolikheten för tullmyndigheters lokalisering av narkotika eller olagliga varor, till exempel på grundval av kända smugglingsvägar.

(43) Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användningen av AI-system som skapar eller utvidgar databaser för ansiktsigenkänning genom oriktad skrapning av ansiktsbilder från internet eller övervakningskameror bör förbjudas, eftersom metoden ökar känslan av att det förekommer massövervakning och kan leda till grova kränkningar av grundläggande rättigheter, inbegripet rätten till integritet.

(44) Det råder allvarlig oro över den vetenskapliga grunden för AI-system som syftar till att identifiera eller uttyda känslor, särskilt som uttryck för känslor varierar avsevärt mellan olika kulturer och situationer och till och med hos en och samma individ. Några av de största bristerna i sådana system är begränsad tillförlitlighet, brist på specificitet och begränsad generaliserbarhet. AI-system som identifierar eller uttyder fysiska personers känslor eller avsikter på grundval av deras biometriska uppgifter kan därför leda till diskriminerande resultat och kan inkräkta på de berörda personernas rättigheter och friheter. Med tanke på maktobalansen i fråga om arbete eller utbildning, i kombination med dessa systems inkräktande karaktär, kan sådana system leda till skadlig eller ogynnsam behandling av vissa fysiska personer eller hela grupper av fysiska personer. Därför bör utsläppande på marknaden, ibruktagande eller användning av AI-system som är avsedda att användas för att upptäcka känslomässiga förhållanden hos enskilda personer i situationer som rör arbetsplats och utbildning förbjudas. Förbudet bör inte omfatta AI-system som släpps ut på marknaden uteslutande av medicinska skäl eller säkerhetsskäl, såsom system som är avsedda för terapeutisk användning.

(45) Metoder som är förbjudna enligt unionsrätten, inbegripet dataskyddslagstiftning, lagstiftning om icke-diskriminering, konsumentskyddslagstiftning och konkurrensrätt, bör inte påverkas av denna förordning.

(46) AI-system med hög risk bör endast släppas ut på unionsmarknaden eller tas i bruk om de uppfyller vissa obligatoriska krav. Dessa krav bör säkerställa att AI-system med hög risk vilka finns tillgängliga i unionen eller vars utdata på annat sätt används i unionen inte utgör någon oacceptabel risk för viktiga allmänna intressen för unionen som erkänns och skyddas av unionsrätten. Baserat på den nya lagstiftningsramen, som klargörs i kommissionens meddelande 2022 års *blåbok* om genomförandet av EU:s produktbestämmelser ([20]), är den allmänna regeln att mer än en rättsakt inom unionens harmoniseringslagstiftning, exempelvis Europaparlamentets och rådets förordningar (EU) 2017/745 ([21]) och (EU) 2017/746 ([22]) eller Europaparlamentets och rådets direktiv 2006/42/EG ([23]), kan äga tillämpning med avseende på en produkt, eftersom tillhandahållandet eller ibruktagandet endast kan ske när produkten överensstämmer med all tillämplig unionsharmoniseringslagstiftning. För att säkerställa samstämmighet

([20]) EUT C 247, 29.6.2022, s. 1.
([21]) 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).
([22]) Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för *in vitro*-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).
([23]) 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).

och undvika onödig administrativ börda eller onödiga kostnader bör leverantörer av en produkt som innehåller ett eller flera AI-system med hög risk som omfattas av kraven i den här förordningen och i unionens harmoniseringslagstiftning som förtecknas i en bilaga till den här förordningen ha flexibilitet när det gäller operativa beslut om hur det ska säkerställas att en produkt som innehåller ett eller flera AI-system uppfyller alla tillämpliga krav i unionens harmoniseringslagstiftning på ett optimalt sätt. AI-system som identifieras som AI-system med hög risk bör begränsas till sådana som har en betydande skadlig inverkan på hälsa, säkerhet och grundläggande rättigheter för personer i unionen och denna avgränsning bör minimera de potentiella begränsningarna av den internationella handeln.

(47) AI-system kan ha negativa effekter för människors hälsa och säkerhet, i synnerhet när sådana system fungerar som säkerhetskomponenter i produkter. I enlighet med syftena för unionens harmoniseringslagstiftning, som är att främja den fria rörligheten för produkter på den inre marknaden och säkerställa att endast säkra produkter som uppfyller kraven släpps ut på marknaden, är det viktigt att de säkerhetsrisker som kan genereras av produkten som helhet på grund av dess digitala komponenter, inklusive AI-system, förhindras och begränsas. Robotar som blir allt mer autonoma, oavsett om det är i samband med tillverkning eller personlig assistans och vård, bör också kunna arbeta säkert och utföra sina funktioner i komplexa miljöer. Inom vårdsektorn, där liv och hälsa i särskilt hög grad kan påverkas, bör de allt mer sofistikerade diagnossystemen och systemen som stöder mänskliga beslut vara tillförlitliga och noggranna.

(48) Omfattningen av de negativa effekter som AI-systemet har på de grundläggande rättigheter som skyddas av stadgan har särskilt stor betydelse när ett AI-system klassificeras som AI-system med hög risk. Dessa rättigheter innefattar rätten till människans värdighet, respekt för privatlivet och familjelivet, skydd av personuppgifter, yttrandefrihet och informationsfrihet, mötesfrihet och organisationsfrihet, rätten till icke-diskriminering, rätten till utbildning, konsumentskydd, arbetstagares rättigheter, rättigheter för personer med funktionsnedsättning, jämställdhet, immateriella rättigheter, rätten till ett effektivt rättsmedel och till en opartisk domstol, rätten till försvar och presumtionen för oskuld och rätten till god förvaltning. Vid sidan av dessa rättigheter är det viktigt att lyfta fram den omständigheten att barn har särskilda rättigheter i enlighet med artikel 24 i stadgan och Förenta nationernas konvention om barnets rättigheter, som vidareutvecklas i allmän kommentar nr 25 till FN:s barnkonvention vad gäller den digitala miljön, som båda kräver att barns utsatthet beaktas och att de ges ett sådant skydd och sådan omsorg som krävs för deras välbefinnande. Även den grundläggande rättigheten till en hög nivå av miljöskydd, som också ingår i stadgan och genomförs i unionspolitik, bör beaktas vid bedömningen av allvarlighetsgraden i den skada som ett AI-system kan orsaka, inbegripet vad gäller människors hälsa och säkerhet.

(49) När det gäller AI-system med hög risk som är säkerhetskomponenter i produkter eller system, eller som i sig själva utgör produkter eller system som omfattas av Europaparlamentets och rådets förordning (EG) nr 300/2008 ([24]), Europaparlamentets och rådets förordning (EU) nr 167/2013 ([25]), Europaparlamentets och rådets förordning (EU) nr 168/2013 ([26]), Europaparlamentets och rådets direktiv 2014/90/EU ([27]), Europaparlamentets och rådets direktiv (EU) 2016/797 ([28]), Europaparlamentets och rådets förordning (EU) 2018/858 ([29]), Europaparlamentets och rådets

([24]) Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

([25]) Europaparlamentets och rådets förordning (EU) nr 167/2013 av den 5 februari 2013 om godkännande och marknadstillsyn av jordbruks- och skogsbruksfordon (EUT L 60, 2.3.2013, s. 1).

([26]) Europaparlamentets och rådets förordning (EU) nr 168/2013 av den 15 januari 2013 om godkännande av och marknadstillsyn för två- och trehjuliga fordon och fyrhjulingar (EUT L 60, 2.3.2013, s. 52).

([27]) Europaparlamentets och rådets direktiv 2014/90/EU av den 23 juli 2014 om marin utrustning och om upphävande av rådets direktiv 96/98/EG (EUT L 257, 28.8.2014, s. 146).

([28]) Europaparlamentets och rådets direktiv (EU) 2016/797 av den 11 maj 2016 om driftskompatibiliteten hos järnvägssystemet inom Europeiska unionen (EUT L 138, 26.5.2016, s. 44).

([29]) Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG (EUT L 151, 14.6.2018, s. 1).

förordning (EU) 2018/1139 ([30]) och Europaparlamentets och rådets förordning (EU) 2019/2144 ([31]), är det lämpligt att ändra de akterna för att säkerställa att kommissionen, på grundval av de tekniska och regleringsmässiga särdragen för varje sektor och utan att inkräkta på befintliga mekanismer för styrelseformer, för kontroll av överensstämmelse och för kontroll av efterlevnad och myndigheter som inrättats inom ramen för dessa, beaktar de obligatoriska krav för AI-system med hög risk som fastställs i den här förordningen när de antar relevanta delegerade akter eller genomförandeakter på grundval av de akterna.

(50) När det gäller AI-system som är säkerhetskomponenter i produkter, eller som i sig själva utgör produkter, vilka omfattas av viss unionsharmoniseringslagstiftning som förtecknas i en bilaga till denna förordning, är det lämpligt att klassificera dessa som AI-system med hög risk enligt denna förordning om den berörda produkten genomgår förfarandet för bedömning av överensstämmelse hos ett tredjepartsorgan för bedömning av överensstämmelse enligt relevant unionsharmoniseringslagstiftning. Det handlar närmare bestämt om sådana produkter som maskiner, leksaker, hissar, utrustning och skyddssystem avsedda för användning i potentiellt explosionsfarliga omgivningar, radioutrustning, tryckutrustning, utrustning för fritidsfartyg, linbaneanläggningar, anordningar för förbränning av gasformiga bränslen, medicintekniska produkter, medicintekniska produkter för *in vitro*-diagnostik, fordon och luftfart.

(51) En klassificering av ett AI-system som AI-system med hög risk enligt denna förordning bör inte nödvändigtvis innebära att den produkt vars säkerhetskomponent utgörs av AI-systemet, eller AI-systemet i sig självt som produkt, anses utgöra ett system med hög risk enligt de kriterier som fastställs i den relevanta unionsharmoniseringslagstiftning som är tillämplig på produkten. Detta gäller i synnerhet för förordningarna (EU) 2017/745 och (EU) 2017/746, i vilka tredjepartsbedömning av överensstämmelse föreskrivs för produkter med medelhög risk och hög risk.

(52) När det gäller fristående AI-system, det vill säga andra AI-system med hög risk än sådana som utgör säkerhetskomponenter i produkter, eller som i sig själva utgör produkter, är det lämpligt att klassificera dem som AI-system med hög risk om de mot bakgrund av sitt avsedda ändamål utgör en hög risk för skada på personers hälsa och säkerhet eller grundläggande rättigheter, med beaktande både den möjliga skadans allvarlighetsgrad och sannolikheten för att den ska uppstå, och de används på ett antal specifikt fördefinierade områden som anges i denna förordning. Identifieringen av sådana system baseras på samma metoder och kriterier som även är avsedda att användas för framtida ändringar av förteckningen över AI-system med hög risk som kommissionen bör ges befogenhet att anta genom delegerade akter, för att ta hänsyn till den snabba tekniska utvecklingen samt potentiella förändringar i användningen av AI-system.

(53) Det är också viktigt att klargöra att det kan finnas särskilda fall där AI-system som det hänvisas till inom fördefinierade områden som anges i denna förordning inte leder till en betydande risk för skada för de rättsliga intressen som skyddas inom dessa områden, eftersom de inte väsentligt påverkar beslutsfattandet eller inte skadar dessa intressen väsentligt. Vid tillämpningen av denna förordning bör ett AI-system som inte väsentligt påverkar resultatet av beslutsfattande förstås som ett AI-system som inte påverkar innehållet, och därmed resultatet, av beslutsfattande, oavsett om det är mänskligt eller automatiserat. Ett AI-system som inte väsentligt påverkar resultatet av beslutsfattande kan omfatta situationer där ett eller flera av nedanstående villkor är uppfyllda. Det första sådana villkoret bör vara att AI-systemet är avsett att utföra en snäv processuell uppgift, såsom ett AI-system som omvandlar ostrukturerade data till strukturerade data, ett AI-system som klassificerar inkommande handlingar i kategorier eller ett AI-system som används för att upptäcka dubbletter bland ett stort antal applikationer. Dessa uppgifter är av så snäv och begränsad art att de endast medför begränsade risker som inte ökar genom användning av ett AI-system i ett sammanhang som förtecknas som användning med hög risk i en bilaga till denna förordning.

([30]) Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91, (EUT L 212, 22.8.2018, s. 1).

([31]) Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter, om ändring av Europaparlamentets och rådets förordning (EU) 2018/858 och om upphävande av Europaparlamentets och rådets förordningar (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 samt kommissionens förordningar (EG) nr 631/2009, (EU) nr 406/2010, (EU) nr 672/2010, (EU) nr 1003/2010, (EU) nr 1005/2010, (EU) nr 1008/2010, (EU) nr 1009/2010, (EU) nr 19/2011, (EU) nr 109/2011, (EU) nr 458/2011, (EU) nr 65/2012, (EU) nr 130/2012, (EU) nr 347/2012, (EU) nr 351/2012, (EU) nr 1230/2012 och (EU) 2015/166 (EUT L 325, 16.12.2019, s. 1).

Det andra villkoret bör vara att den uppgift som utförs av AI-systemet är avsedd att förbättra resultatet av tidigare slutförd mänsklig verksamhet som kan vara relevant för den användning med hög risk som förtecknas i en bilaga till denna förordning. Med tanke på dessa egenskaper tillhandahåller AI-systemet endast ett extra skikt till mänsklig verksamhet och innebär följaktligen lägre risk. Detta villkor skulle till exempel tillämpas på AI-system som är avsedda att förbättra det språk som används i tidigare utarbetade dokument, till exempel när det gäller yrkesmässig ton eller akademisk språkstil eller genom att anpassa texten till ett visst varumärkesbudskap. Det tredje villkoret bör vara att AI-systemet är avsett att upptäcka beslutsmönster eller avvikelser från tidigare beslutsmönster. Risken skulle minska eftersom användningen av AI-systemet följer en tidigare slutförd mänsklig bedömning som den inte avser ersätta eller påverka utan ordentlig mänsklig granskning. Sådana AI-system omfattar till exempel system som, med tanke på en viss lärares betygsättningsmönster, kan användas för att i efterhand kontrollera om läraren har avvikit från betygsättningsmönstret för att på så sätt uppmärksamma potentiella inkonsekvenser eller avvikelser. Det fjärde villkoret bör vara att AI-systemet är avsett att utföra en uppgift som endast är förberedande för en bedömning som är relevant för de AI-system som förtecknas i en bilaga till denna förordning, så att den möjliga effekten av systemets utdata blir mycket låg när det gäller att utgöra en risk för den bedömning som ska följa. Detta villkor omfattar bland annat smarta lösningar för ärendehandläggning som omfattar olika funktioner såsom indexering, sökning, text- och talbehandling eller länkning av data till andra datakällor, eller AI-system som används för översättning av ursprungliga dokument. Under alla omständigheter bör AI-system som används i användningsfall med hög risk som förtecknas i en bilaga till denna förordning anses utgöra en betydande risk för skada på hälsa, säkerhet eller grundläggande rättigheter om AI-systemet innebär profilering i den mening som avses i artikel 4.4 i förordning (EU) 2016/679 eller artikel 3.4 i direktiv (EU) 2016/680 eller artikel 3.5 i förordning (EU) 2018/1725. För att säkerställa spårbarhet och transparens bör en leverantör som anser att ett AI-system inte är ett AI-system med hög risk på grundval av de villkor som avses ovan upprätta dokumentation om bedömningen innan systemet släpps ut på marknaden eller tas i bruk och bör på begäran tillhandahålla den dokumentationen till de nationella behöriga myndigheterna. En sådan leverantör bör vara skyldig att registrera AI-systemet i den EU-databas som inrättas enligt den här förordningen. I syfte att ge ytterligare vägledning för det praktiska genomförandet av de villkor enligt vilka AI-system som förtecknas i en bilaga till denna förordning undantagsvis inte är förenade med hög risk bör kommissionen, efter samråd med styrelsen, tillhandahålla riktlinjer som specificerar detta praktiska genomförande, kompletterat med en omfattande förteckning över praktiska exempel på fall av användning av AI-system som medför hög risk och fall av användning som inte medför hög risk.

(54) Eftersom biometriska uppgifter utgör en särskild kategori av personuppgifter är det lämpligt att klassificera flera kritiska användningsfall av biometriska system som användningsfall med hög risk, i den mån användningen av dem är tillåten enligt relevant unionsrätt och nationell rätt. Tekniska brister i AI-system som är avsedda för biometrisk fjärridentifiering av fysiska personer kan leda till biaser i resultat och medföra diskriminerande effekter. Risken för sådana biaser i resultat och diskriminerande effekter är särskilt relevant när det gäller ålder, etnicitet, ras, kön eller funktionsnedsättning. System för biometrisk fjärridentifiering bör därför klassificeras som system med hög risk med tanke på de risker de medför. En sådan klassificering utesluter AI-system som är avsedda att användas för biometrisk verifiering, inbegripet autentisering, vars enda syfte är att bekräfta att en specifik fysisk person är den som vederbörande utger sig för att vara och för att bekräfta identiteten på en fysisk person med det enda syftet att få åtkomst till en tjänst, låsa upp en enhet eller ha säker tillgång till lokaler. Dessutom bör AI-system som är avsedda att användas för biometrisk kategorisering enligt känsliga attribut eller egenskaper som skyddas enligt artikel 9.1 i förordning (EU) 2016/679 på grundval av biometriska uppgifter, i den mån dessa inte är förbjudna enligt den här förordningen, och system för känsloigenkänning som inte är förbjudna enligt den här förordningen, klassificeras som AI-system med hög risk. Biometriska system som är avsedda att användas enbart för att möjliggöra cybersäkerhet och åtgärder för skydd av personuppgifter bör inte betraktas som AI-system med hög risk.

(55) När det gäller förvaltning och drift av kritisk infrastruktur är det lämpligt att som AI-system med hög risk klassificera AI-system avsedda att användas som säkerhetskomponenter i förvaltningen och driften av kritisk digital infrastruktur enligt förteckningen i punkt 8 i bilagan till direktiv (EU) 2022/2557, vägtrafik och tillhandahållandet av vatten, gas, uppvärmning och el, eftersom funktionsavbrott eller funktionsstörning i sådana system kan medföra risk för personers liv och hälsa i stor skala och leda till märkbara störningar av det normala bedrivandet av social och ekonomisk verksamhet. Säkerhetskomponenter i kritisk infrastruktur, inbegripet kritisk digital infrastruktur, är system som används för att direkt skydda kritisk infrastrukturs fysiska integritet eller människors hälsa och säkerhet och egendom, men som inte är nödvändiga för att systemet ska fungera. Funktionsavbrott eller funktionsstörning

i sådana komponenter kan direkt leda till risker för den kritiska infrastrukturens fysiska integritet och därmed till risker för människors hälsa och säkerhet och egendom. Komponenter som är avsedda att användas enbart för cybersäkerhetsändamål bör inte betraktas som säkerhetskomponenter. Exempel på säkerhetskomponenter i sådan kritisk infrastruktur kan omfatta system för övervakning av vattentryck eller styrsystem för brandlarm vid centrum för molntjänster.

(56) Införandet av AI-system inom utbildning är viktigt för att främja digital utbildning av hög kvalitet och göra det möjligt för alla studerande och lärare att förvärva och dela de digitala färdigheter och kompetenser som krävs, inbegripet mediekunnighet, och kritiskt tänkande, för att aktivt delta i ekonomin, samhället och i demokratiska processer. AI-system som används för yrkesutbildning eller annan utbildning, i synnerhet när det gäller fastställandet av personers tillgång till eller antagning till institutioner för yrkesutbildning eller annan utbildning eller program på alla nivåer, för utvärdering av personers läranderesultat, för bedömning av en persons lämpliga utbildningsnivå och för väsentlig påverkan av den utbildningsnivå som personer kommer att få eller kommer kunna få tillgång till, eller för övervakning och upptäckt av förbjudet beteende bland studerande under provtillfällen, bör klassificeras som AI-system med hög risk eftersom de kan avgöra en persons utbildningsväg och yrkeskarriär och därmed påverka en persons försörjningsmöjligheter. När sådana system utformas och används på otillbörligt sätt kan de vara särskilt inkräktande och kan innebära en kränkning av rätten till utbildning liksom rätten att inte utsättas för diskriminering eller för en fortsättning på historiska diskrimineringsmönster mot till exempel kvinnor, vissa åldersgrupper, personer med funktionsnedsättning eller personer av vissa etniska ursprung eller av viss sexuell läggning.

(57) AI-system som används för anställning, arbetsledning och tillgång till egenföretagande, i synnerhet när det gäller rekrytering eller urval av personer, för beslutsfattande som påverkar villkoren för arbetsrelaterad befordran, eller uppsägning av arbetsrelaterade avtalsförhållanden, för fördelning av uppgifter på grundval av individuellt beteende eller personlighetsdrag och egenskaper och för övervakning eller utvärdering av personer i arbetsrelaterade avtalsförhållanden, bör också klassificeras som AI-system med hög risk, eftersom dessa system märkbart kan påverka framtida karriärutsikter och försörjning för dessa personer samt arbetstagares rättigheter. Relevanta arbetsrelaterade avtalsförhållanden bör på ett meningsfullt sätt innefatta arbetstagare och personer som tillhandahåller tjänster via plattformar enligt kommissionens arbetsprogram för 2021. Under hela rekryteringsförfarandet och vid utvärdering, befordran eller bibehållande av personer i arbetsrelaterade avtalsförhållanden, kan sådana system reproducera historiska mönster av diskriminering, exempelvis mot kvinnor, vissa åldersgrupper, personer med funktionsnedsättning eller mot personer på grund av ras, etniskt ursprung eller sexuell läggning. AI-system som används för att övervaka sådana personers prestation och beteende kan också undergräva deras grundläggande rätt till dataskydd och personlig integritet.

(58) Ett annat område där användningen av AI-system förtjänar särskild vaksamhet är när det gäller tillgång till och åtnjutande av vissa väsentliga privata och offentliga tjänster och förmåner som är nödvändiga för att människor fullt ut ska kunna delta i samhället eller förbättra sin levnadsstandard. I synnerhet är fysiska personer som ansöker om eller får viktiga offentliga bidragsförmåner och tjänster från offentliga myndigheter, nämligen hälso- och sjukvårdstjänster, sociala trygghetsförmåner, sociala tjänster som tillhandahåller skydd i fall som moderskap, sjukdom, arbetsolyckor, vårdbehov eller ålderdom och arbetslöshet samt socialbidrag och bostadsbidrag, vanligtvis beroende av dessa förmåner och tjänster och befinner sig i en utsatt situation i förhållande till de ansvariga myndigheterna. Om AI-system används för att avgöra om sådana förmåner och tjänster ska beviljas, vägras, minskas, upphävas eller återkallas av myndigheterna, inbegripet huruvida mottagarna är legitimt berättigade till sådana förmåner eller tjänster, kan dessa system ha en betydande inverkan på personers försörjning och kan inkräkta på deras grundläggande rättigheter, såsom rätten till socialt skydd, icke-diskriminering, mänsklig värdighet eller ett effektivt rättsmedel och bör där klassificeras som AI-system med hög risk. Denna förordning bör dock inte hämma utvecklingen och användningen av innovativa metoder inom offentlig förvaltning, som kan gagnas av en bredare användning av säkra AI-system som uppfyller kraven, förutsatt att dessa system inte medför hög risk för juridiska och fysiska personer. Dessutom bör AI-system som används för att utvärdera fysiska personers kreditbetyg eller kreditvärdighet klassificeras som AI-system med hög risk, eftersom de avgör de berörda personernas tillgång till ekonomiska resurser eller väsentliga tjänster som bostad, el och telekommunikationstjänster. AI-system som används för dessa ändamål kan medföra diskriminering av personer eller grupper och kan reproducera sådana historiska diskrimineringsmönster som det som baseras på rasmässigt eller etniskt ursprung, kön, funktionsnedsättning, ålder eller sexuell läggning, eller skapa nya former av diskriminerande effekter. AI-system som föreskrivs i unionsrätten i syfte att upptäcka bedrägerier i samband med tillhandahållande av finansiella tjänster och för tillsynsändamål för att beräkna kreditinstituts och försäkringsföretags kapitalkrav bör dock inte betraktas som AI-system med hög risk enligt denna förordning. Vidare kan AI-system som är avsedda att användas för riskbedömning och prissättning när

det gäller fysiska personer av sjuk- och livförsäkring också ha en betydande inverkan på människors försörjningsmöjligheter och kan, om de inte utformas, utvecklas och används på rätt sätt, inkräkta på deras grundläggande rättigheter och leda till allvarliga konsekvenser för människors liv och hälsa, inbegripet ekonomisk utestängning och diskriminering. Slutligen bör även AI-system som används för att utvärdera och klassificera nödsamtal från fysiska personer eller för att sända ut eller fastställa prioriteringsordning för utsändning av larmtjänster, inbegripet av polis, brandkår och sjukvård, samt av patientsorteringssystem för akutsjukvård klassificeras som AI-system med hög risk, eftersom dessa system fattar beslut i situationer som är mycket kritiska för personers liv, hälsa och egendom.

(59) Med tanke på brottsbekämpande myndigheters roll och ansvar kännetecknas deras åtgärder, när de omfattar vissa typer av användning av AI-system, av en betydande grad av maktobalans och kan leda till övervakning, gripande eller frihetsberövande av en fysisk person, liksom annan negativ inverkan på grundläggande rättigheter som garanteras i stadgan. AI-system kan – i synnerhet om de inte tränats med data av hög kvalitet, inte uppfyller lämpliga krav i fråga om prestanda, riktighet eller robusthet, eller inte har utformats och testats tillräckligt innan de släpps ut på marknaden eller på annat sätt tas i bruk – peka ut människor på ett diskriminerande eller på ett annat oriktigt eller orättvist sätt. Dessutom kan utövandet av viktiga processuella grundläggande rättigheter, såsom rätten till ett effektivt rättsmedel och till en opartisk domstol samt rätten till försvar och presumtionen för oskuld, hämmas, i synnerhet i de fall då AI-systemen inte är tillräckligt transparenta, förklarade och dokumenterade. Det är därför lämpligt att, i den mån deras användning är tillåten enligt relevant unionsrätt och nationell rätt, som AI-system med hög risk klassificera ett antal AI-system som är avsedda att användas i brottsbekämpningssammanhang där det är särskilt viktigt med riktighet, tillförlitlighet och transparens för att undvika negativa effekter, upprätthålla allmänhetens förtroende och säkerställa ansvarsskyldighet och effektiv rättslig prövning. Mot bakgrund av åtgärdernas art och relaterade risker bör dessa AI-system med hög risk i synnerhet inbegripa AI-system avsedda att användas av brottsbekämpande myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer till stöd för brottsbekämpande myndigheter vid bedömning av risken för att en fysisk person ska falla offer för brott, som lögndetektorer och liknande verktyg, för utvärdering av bevisens tillförlitlighet i samband med utredning eller lagföring av brott, och, i den mån det inte är förbjudet enligt denna förordning, för bedömning av risken för att en fysisk person begår brott eller återfaller i brott inte enbart på grundval av profilering av fysiska personer eller en bedömning av personlighetsdrag och egenskaper eller tidigare brottsligt beteende hos fysiska personer eller grupper, för profilering i samband med upptäckt, utredning eller lagföring av brott. AI-system som är specifikt avsedda att användas av skattemyndigheter och tullmyndigheter för administrativa förfaranden samt av finansunderrättelseenheter som utför administrativa uppgifter för analys av information enligt unionsrätt på området penningtvätt bör inte klassificeras som AI-system med hög risk som används av brottsbekämpande myndigheter i syfte att förebygga, förhindra, upptäcka, utreda eller lagföra brott. Användningen av AI-verktyg av brottsbekämpande myndigheter och andra relevanta myndigheter bör inte bli en faktor som bidrar till ojämlikhet, sociala klyftor eller utestängning. Den inverkan som användningen av AI-verktyg har på misstänktas rätt till försvar bör inte ignoreras, särskilt svårigheten att få meningsfull information om hur dessa system fungerar och den därav följande svårigheten att överklaga resultaten i domstol, särskilt för fysiska personer som är under utredning.

(60) AI-system som används i samband med migration, asyl och gränskontrollförvaltning påverkar människor som ofta är i en särskilt utsatt situation och som är beroende av resultatet av de behöriga offentliga myndigheternas åtgärder. Det är därmed särskilt viktigt att de AI-system som används i dessa sammanhang är tillförlitliga, icke-diskriminerande och transparenta, för att garantera iakttagandet av de påverkade personernas grundläggande rättigheter, särskilt deras rätt till fri rörlighet, icke-diskriminering, skydd av privatliv och personuppgifter, internationellt skydd och god förvaltning. I den mån deras användning är tillåten enligt relevant unionsrätt och nationell rätt är det därför lämpligt att som AI-system med hög risk klassificera AI-system som är avsedda att användas som lögndetektorer eller liknande verktyg av behöriga offentliga myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer som anförtrotts uppgifter på områdena migration, asyl och gränskontrollförvaltning, för bedömning av vissa risker som fysiska personer som reser in till en medlemsstats territorium eller som ansöker om visering eller asyl medför, för att bistå behöriga offentliga myndigheter i granskningen, inbegripet den relaterade bedömningen av bevisens tillförlitlighet, av ansökningar om asyl, visering och uppehållstillstånd och därmed förbundna klagomål med avseende på syftet att fastställa om den ansökande fysiska personen uppfyller kraven för denna status, i syfte att upptäcka, känna igen eller identifiera fysiska personer i samband med migration, asyl och gränskontrollförvaltning, med undantag för kontroll av resehandlingar. AI-system på området migration, asyl och gränskontrollförvaltning vilka omfattas av denna förordning bör uppfylla de relevanta förfarandemässiga krav som fastställs i Europaparlamentets och rådets förordning (EG) nr 810/2009 ([32]),

([32]) Europaparlamentets och rådets förordning (EG) nr 810/2009 av den 13 juli 2009 om införande av en gemenskapskodex om viseringar (viseringskodex) (EUT L 243, 15.9.2009, s. 1).

Europaparlamentets och rådets direktiv 2013/32/EU ([33]) och annan relevant unionsrätt. AI-system som används i samband med migration, asyl och gränskontrollförvaltning bör under inga omständigheter användas av medlemsstater eller unionens institutioner, organeller byråer som ett medel för att kringgå sina internationella skyldigheter enligt FN-konventionen om flyktingars rättsliga ställning, som undertecknades i Genève den 28 juli 1951 i dess ändrade lydelse genom protokollet av den 31 januari 1967. De bör inte heller användas för att på något sätt bryta mot principen om *non-refoulement* eller neka säkra och effektiva lagliga vägar in på unionens territorium, inbegripet rätten till internationellt skydd.

(61) Vissa AI-system som är avsedda för rättsskipning och demokratiska processer bör klassificeras som AI-system med hög risk, mot bakgrund av deras potentiellt betydande inverkan på demokrati, rättsstatens principer, individuella friheter och rätten till ett effektivt rättsmedel och till en opartisk domstol. För att motverka riskerna för potentiella biaser, felaktigheter och bristande insyn är det i synnerhet lämpligt att som AI-system med hög risk klassificera sådana AI-system som är avsedda att användas av en rättslig myndighet eller på dess vägnar för att hjälpa de rättsliga myndigheterna att efterforska och tolka fakta och lagstiftning och att tillämpa denna lagstiftning på en konkret uppsättning fakta. AI-system som är avsedda att användas av organ för alternativ tvistlösning för dessa ändamål bör också anses vara förenade med hög risk när resultaten av förfarandena för alternativ tvistlösning har rättsverkan för parterna. Användningen av AI-verktyg kan stödja domarnas beslutanderätt eller rättsväsendets oberoende men bör inte ersätta det: det slutliga beslutsfattandet måste förbli en människodriven verksamhet. Klassificeringen av AI-system som AI-system med hög risk bör dock inte omfatta AI-system som är avsedda för rent administrativa stödfunktioner som inte påverkar den faktiska rättskipningen i enskilda fall, exempelvis anonymisering eller pseudonymisering av rättsliga beslut, handlingar eller data, kommunikation mellan anställda, administrativa uppgifter.

(62) Utan att det påverkar de regler som föreskrivs i Europaparlamentets och rådets förordning (EU) 2024/900 ([34]) och för att hantera riskerna för otillbörlig extern inblandning i rösträtten enligt artikel 39 i stadgan och negativa följder för demokrati och rättsstatens principer bör AI-system som är avsedda att användas för att påverka resultatet av ett val eller en folkomröstning eller fysiska personers röstbeteende vid val eller folkomröstningar klassificeras som AI-system med hög risk, med undantag för AI-system vars utdata fysiska personer inte är direkt exponerade för, såsom verktyg som används för att organisera, optimera och strukturera politiska kampanjer ur administrativ och logistisk synvinkel.

(63) Det faktum att ett AI-system klassificerats som ett AI-system med hög risk enligt denna förordning bör inte tolkas som att användningen av det systemet är laglig enligt andra unionsrättsliga akter eller enligt nationell rätt som är förenlig med unionsrätten, exempelvis vad gäller skydd av personuppgifter, användning av lögndetektorer och liknande verktyg eller andra system för att läsa av fysiska personers känslomässiga tillstånd. All sådan användning bör även fortsättningsvis endast ske i enlighet med de tillämpliga krav som följer av stadgan eller av tillämpliga rättsakter i unionens sekundärrätt och nationell rätt. Denna förordning bör inte tolkas som att den omfattar en rättslig grund för behandling av personuppgifter, inbegripet särskilda kategorier av personuppgifter, i förekommande fall, såvida inte annat uttryckligen föreskrivs i denna förordning.

(64) För att begränsa riskerna med AI-system med hög risk som släpps ut på marknaden eller tas i bruk och för att säkerställa hög tillförlitlighet bör vissa obligatoriska krav gälla för AI-system med hög risk, med beaktande av AI-systemets avsedda ändamål och det sammanhang i vilket det används samt enligt det riskhanteringssystem som ska upprättas av leverantören. De åtgärder som antas av leverantörerna för att uppfylla de obligatoriska kraven i denna förordning bör ta hänsyn till den allmänt erkända senaste utvecklingen när det gäller AI och vara proportionella och effektiva för att uppnå målen i denna förordning. På grundval av den nya lagstiftningsramen, som klargörs i kommissionens meddelande 2022 års *blåbok* om genomförandet av EU:s produktbestämmelser, är den allmänna regeln att mer än en rättsakt inom unionens harmoniseringslagstiftning kan vara tillämplig på en produkt, eftersom tillhandahållandet eller ibruktagandet endast kan ske först när produkten överensstämmer med alla tillämpliga delar av unionens harmoniseringslagstiftning. Riskerna med AI-system som omfattas av kraven i denna förordning rör andra aspekter än unionens befintliga harmoniseringslagstiftning, och därför skulle kraven i denna förordning komplettera det befintliga innehållet i unionens harmoniseringslagstiftning. Maskiner eller medicintekniska produkter som innehåller ett AI-system kan till exempel utgöra risker som inte hanteras genom de grundläggande hälso- och säkerhetskrav som fastställs i berörd unionsharmoniseringslagstiftning, eftersom denna

([33]) Europaparlamentets och rådets direktiv 2013/32/EU av den 26 juni 2013 om gemensamma förfaranden för att bevilja och återkalla internationellt skydd (EUT L 180, 29.6.2013, s. 60).

([34]) Europaparlamentets och rådets direktiv (EU) 2024/900 av den 13 mars 2024 om transparens och inriktning när det gäller politisk reklam (EUT L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

sektorsspecifika lagstiftning inte behandlar risker som är specifika för AI-system. Det krävs därför att de olika lagstiftningsakterna tillämpas samtidigt och komplementärt. För att säkerställa samstämmighet och undvika en onödig administrativ börda eller onödiga kostnader bör leverantörer av en produkt som innehåller ett eller flera AI-system med hög risk som omfattas av kraven i denna förordning eller i unionens harmoniseringslagstiftning som bygger på den nya lagstiftningsramen och som förtecknas i en bilaga till denna förordning ha flexibilitet när det gäller operativa beslut om hur det på bästa sätt ska säkerställas att en produkt som innehåller ett eller flera AI-system uppfyller alla tillämpliga krav i unionens harmoniseringslagstiftning på ett optimalt sätt. Denna flexibilitet kan till exempel innebära att leverantören beslutar att integrera en del av de nödvändiga testnings- och rapporteringsprocesser, den information och den dokumentation som krävs enligt denna förordning i dokumentation och förfaranden som redan finns och som krävs enligt befintlig unionsharmoniseringslagstiftning som bygger på den nya lagstiftningsramen och som förtecknas i en bilaga till denna förordning. Detta bör dock inte på något sätt undergräva leverantörens skyldighet att uppfylla alla tillämpliga krav.

(65) Riskhanteringssystemet bör bestå av en kontinuerlig iterativ process som planeras och löper under hela livscykeln för ett AI-system med hög risk. Den processen bör syfta till att identifiera och begränsa de relevanta riskerna med AI-system för hälsa, säkerhet och grundläggande rättigheter. Riskhanteringssystemet bör regelbundet ses över och uppdateras för att säkerställa dess fortsatta effektivitet samt motivet för och dokumentationen av alla viktiga beslut och åtgärder som vidtas i enlighet med denna förordning. Denna process bör säkerställa att leverantören identifierar risker eller negativa effekter och genomför begränsningsåtgärder för de kända och rimligen förutsebara riskerna med AI-system för hälsa, säkerhet och grundläggande rättigheter mot bakgrund av deras avsedda ändamål och rimligen förutsebar felaktig användning, inbegripet de möjliga risker som uppstår till följd av interaktionen mellan AI-systemet och den miljö där det är i drift. Riskhanteringssystemet bör välja de lämpligaste riskhanteringsåtgärderna mot bakgrund av den senaste utvecklingen inom AI. Vid identifieringen av de lämpligaste riskhanteringsåtgärderna bör leverantören dokumentera och förklara de val som gjorts och, när så är relevant, involvera experter och externa berörda parter. Vid identifieringen av den rimligen förutsebara felaktiga användningen av AI-system med hög risk bör leverantören inkludera användningar av AI-system som, även om de inte direkt täcks av det avsedda ändamålet och anges i bruksanvisningen, ändå rimligen kan förväntas bli resultatet av ett lätt förutsägbart mänskligt beteende i samband med det specifika AI-systemets särskilda egenskaper och användning. Varje känd eller förutsebar omständighet med anknytning till användningen av AI-systemet med hög risk i enlighet med dess avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning som kan leda till risker för hälsa och säkerhet eller grundläggande rättigheter bör ingå i den bruksanvisning som leverantören tillhandahåller. Syftet med detta är att säkerställa att tillhandahållaren är medveten om och tar hänsyn till dessa när AI-systemet med hög risk används. Identifiering och genomförande av riskbegränsningsåtgärder för förutsebar felaktig användning enligt denna förordning bör inte kräva särskild ytterligare träning för AI-systemet med hög risk från leverantörens sida för att hantera förutsebar felaktig användning. Leverantörerna uppmanas dock att överväga sådana ytterligare träningsåtgärder för att begränsa rimligen förutsebar felaktig användning om de är nödvändiga och lämpliga.

(66) Kraven bör tillämpas på AI-system med hög risk när det gäller riskhantering, kvaliteten på och relevansen av använda dataset, teknisk dokumentation och loggning, transparens och information till tillhandahållare, mänsklig kontroll samt robusthet, riktighet och cybersäkerhet. Dessa krav är nödvändiga för att på ett effektivt sätt begränsa riskerna för hälsa, säkerhet och grundläggande rättigheter. Eftersom inga andra åtgärder som är mindre handelsbegränsande finns rimligen tillgängliga så utgör dessa krav inte omotiverade begränsningar av handeln.

(67) Data av hög kvalitet och tillgång till data av hög kvalitet spelar en avgörande roll när det gäller att tillhandahålla struktur och att säkerställa många AI-systems prestanda, i synnerhet vid användning av teknik som förutsätter träning av modeller för att säkerställa att AI-system med hög risk fungerar säkert och på avsett sätt och inte blir en källa till diskriminering som är förbjuden enligt unionsrätten. Högkvalitativa dataset för träning, validering och testning förutsätter genomförande av lämpliga metoder för dataförvaltning och datahantering. Dataset för träning, validering och testning, inbegripet märkningarna, bör vara relevanta, tillräckligt representativa och i största möjliga utsträckning fria från fel och fullständiga med tanke på systemets avsedda ändamål. För att underlätta efterlevnaden av unionens dataskyddslagstiftning, såsom förordning (EU) 2016/679, bör dataförvaltnings- och datahanteringsmetoderna när det gäller personuppgifter inbegripa transparens om det ursprungliga syftet med uppgiftsinsamlingen. Dataseten bör också ha lämpliga statistiska egenskaper, även när det gäller de personer eller grupper av personer i fråga om vilka AI-systemet med hög risk är avsett att användas, med särskild uppmärksamhet på att begränsa eventuella biaser i dataseten som sannolikt påverkar människors hälsa och säkerhet, inverkar negativt på grundläggande rättigheter eller leder till diskriminering som är förbjuden enligt unionsrätten, särskilt när utdata

påverkar indata för framtida operationer (återföring). Biaser kan exempelvis vara inneboende i underliggande dataset, särskilt när historiska data används eller genereras när systemen tillämpas i verkliga sammanhang. De resultat som AI-system ger kan påverkas av sådana inneboende biaser som tenderar att gradvis öka och därigenom vidmakthålla och förstärka befintliga diskriminering, särskilt för personer som tillhör vissa sårbara grupper, inbegripet rasgrupper eller etniska grupper. Kravet på att dataseten i största möjliga utsträckning ska vara fullständiga och fria från fel bör inte påverka användningen av integritetsbevarande teknik i samband med utveckling och testning av AI-system. I synnerhet bör dataset, i den mån som krävs för deras avsedda ändamål, beakta funktioner, särdrag eller element som är specifika för den särskilda geografiska, kontextuella, beteendemässiga eller funktionsmässiga situation där AI-systemet är avsett att användas. De krav som rör dataförvaltning kan uppfyllas genom att tredje parter anlitas som erbjuder certifierade tjänster för uppfyllelse av kraven, inbegripet kontroll av dataförvaltning, datasetens integritet och metoder för träning, validering och testning av data, i den mån överensstämmelse med uppgiftskraven i denna förordning säkerställs.

(68) För utvecklingen och bedömningen av AI-system med hög risk bör vissa aktörer, såsom leverantörer, anmälda organ och andra berörda enheter – exempelvis europeiska digitala innovationsknutpunkter, test- och experimentfaciliteter och forskare – kunna få åtkomst till och använda dataset av hög kvalitet inom sina respektive verksamhetsområden som är relaterade till denna förordning. Gemensamma europeiska dataområden som inrättas av kommissionen och främjande av datadelning mellan företag och med offentlig förvaltning i allmänhetens intresse kommer att vara avgörande för tillhandahållandet av förtroendefull, ansvarsskyldig och icke-diskriminerande åtkomst till högkvalitativa data för träning, validering och testning av AI-system. På exempelvis hälsoområdet kommer det europeiska hälsodataområdet att främja icke-diskriminerande åtkomst till hälsodata och träning av AI-algoritmer på dessa dataset, på ett sätt som bevarar den personliga integriteten och är säkert, snabbt, transparent och tillförlitligt och med lämpliga institutionella styrelseformer. Berörda behöriga myndigheter, även sektorsbaserade sådana, som tillhandahåller eller stöder åtkomst till data får också stödja tillhandahållandet av högkvalitativa data för träning, validering och testning av AI-system.

(69) Rätten till integritet och skydd av personuppgifter måste garanteras under AI-systemets hela livscykel. I detta avseende är principerna om uppgiftsminimering och inbyggt dataskydd och dataskydd som standard, i enlighet med unionens dataskyddslagstiftning, tillämpliga när personuppgifter behandlas. De åtgärder som leverantörer vidtar för att säkerställa efterlevnaden av dessa principer kan omfatta inte bara anonymisering och kryptering, utan även användning av teknik som gör det möjligt att föra in algoritmer i data och möjliggöra träning av AI-system utan överföring mellan parter eller kopiering av rådata eller strukturerade data i sig, utan att det påverkar tillämpningen av de krav på dataförvaltning som föreskrivs i denna förordning.

(70) För att skydda andras rätt att slippa diskriminering som kan följa av bias i AI-system bör leverantörerna undantagsvis, i den utsträckning det är absolut nödvändigt för att säkerställa upptäckt och korrigering av bias i samband med AI-systemen med hög risk, med förbehåll för lämpliga skyddsåtgärder för fysiska personers grundläggande rättigheter och friheter och enligt tillämpningen av alla tillämpliga villkor som fastställs i denna förordning och i förordningarna (EU) 2016/679, (EU) 2018/1725 och (EU) nr 2016/680, kunna behandla även särskilda kategorier av personuppgifter, av hänsyn till ett viktigt allmänt intresse i den mening som avses i artikel 9.2 g i förordning (EU) 2016/679 och artikel 10.2 g i förordning (EU) 2018/1725.

(71) Det är mycket viktigt att ha begriplig information om hur AI-system med hög risk har utvecklats och hur de presterar under hela sin livstid, för att möjliggöra att dessa system är spårbara, kontrollera att kraven enligt denna förordning uppfylls samt kunna utföra övervakning av deras drift och övervakning efter utsläppande på marknaden. Detta förutsätter arkivering och tillgång till teknisk dokumentation som innehåller den information som krävs för att bedöma om AI-systemet uppfyller de berörda kraven och underlätta övervakning efter utsläppande på marknaden. Denna information bör innefatta systemets allmänna egenskaper, kapacitet och begränsningar samt algoritmer, data, de förfaranden som används för träning, testning och validering samt dokumentation av relevanta riskhanteringssystem och ha utformats i tydlig och begriplig form. Den tekniska dokumentationen bör vara lämpligt uppdaterad under hela AI-systemets livstid. AI-system med hög risk bör dessutom tekniskt möjliggöra automatisk registrering av händelser genom loggar under systemets livstid.

(72) För att ta itu med farhågor som hör samman med den bristande insynen och komplexiteten i vissa AI-system och göra det lättare för tillhandahållare att fullgöra sina skyldigheter enligt denna förordning bör transparens krävas för AI-system med hög risk innan de släpps ut på marknaden eller tas i bruk. AI-system med hög risk bör utformas på ett sätt som gör det möjligt för tillhandahållare att förstå hur AI-systemet fungerar, utvärdera dess funktionalitet och förstå dess styrkor och begränsningar. AI-system med hög risk bör åtföljas av lämplig information i form av bruksanvisningar. Sådan information bör omfatta AI-systemets egenskaper, kapacitet och prestandabegränsningar. Dessa skulle omfatta information om eventuella kända och förutsebara omständigheter som har samband med användningen av AI-systemet med hög risk, inbegripet tillhandahållares åtgärder som kan påverka systemets beteende och prestanda, under vilka AI-systemet kan leda till risker för hälsa, säkerhet och grundläggande rättigheter, om de förändringar som på förhand har fastställts och bedömts för överensstämmelse av leverantören och om relevanta åtgärder för mänsklig kontroll, inbegripet åtgärderna för att underlätta tillhandahållarnas tolkning av AI-systemets utdata. Transparens, inklusive åtföljande bruksanvisningar bör hjälpa tillhandahållare att använda systemet och stödja deras välgrundade beslutsfattande. Tillhandahållare bör bland annat ha bättre förutsättningar att göra rätt val av vilket system de avser att använda mot bakgrund av de skyldigheter som gäller för dem, få kunskap om avsedd och utesluten användning samt använda AI-systemet korrekt och när så är lämpligt. För att förbättra läsbarheten och tillgängligheten för den information som ingår i bruksanvisningen bör, när så är lämpligt, belysande exempel om exempelvis begränsningar och om avsedd och utesluten användning av AI-systemet inkluderas. Leverantörer bör säkerställa att all dokumentation, inbegripet bruksanvisningen, innehåller meningsfull, heltäckande, tillgänglig och begriplig information, med beaktande av de behov och den förmodade kunskap som de tillhandahållare som man riktar sig till har. Bruksanvisningen bör tillhandahållas på ett språk som lätt kan förstås av de tillhandahållare som man riktar sig till, i enlighet med vad som fastställs av den berörda medlemsstaten.

(73) AI-system med hög risk bör utformas och utvecklas på ett sådant sätt att fysiska personer kan övervaka deras funktionssätt, säkerställa att de används som avsett och att deras effekter hanteras under systemets livscykel. För det ändamålet bör lämpliga åtgärder för mänsklig kontroll identifieras av leverantören av systemet innan detta släpps ut på marknaden eller tas i bruk. Sådana åtgärder bör i synnerhet, när så är lämpligt, garantera att systemet är föremål för inbyggda operativa begränsningar som inte kan åsidosättas av systemet självt och som lyder den mänskliga operatören, och att de fysiska personer som anförtros uppgiften att utöva mänsklig kontroll har den kompetens, utbildning och auktoritet som de behöver för att utföra sina uppgifter. Det är också viktigt, beroende på vad som är lämpligt, att säkerställa att AI-system med hög risk innehåller mekanismer för att vägleda och informera den fysiska person som anförtros uppgiften att utöva mänsklig kontroll när det gäller att fatta välgrundade beslut om, när och hur ett ingripande ska ske för att undvika negativa konsekvenser eller risker eller stoppa systemet om det inte fungerar som avsett. Med tanke på de betydande konsekvenserna för personer vid vissa biometriska identifieringssystems felaktiga träffar är det lämpligt att föreskriva ett förstärkt krav på mänsklig kontroll för dessa system så att tillhandahållaren inte kan vidta åtgärder eller fatta beslut på grundval av den identifiering som systemet ger upphov till såvida inte detta har verifierats och bekräftats separat av minst två fysiska personer. Dessa personer kan komma från en eller flera enheter och inbegripa den person som driver eller använder systemet. Detta krav bör inte medföra onödiga bördor eller förseningar och det kan vara tillräckligt att de olika personernas separata kontroller automatiskt registreras i de loggar som genereras av systemet. Med tanke på särdragen inom brottsbekämpning, migration, gränskontroll och asyl bör detta krav inte tillämpas i fall där tillämpningen av detta krav enligt unionsrätten eller nationell rätt betraktas som oproportionerlig.

(74) AI-system med hög risk bör fungera konsekvent under hela sin livscykel och uppnå en lämplig nivå av riktighet, robusthet och cybersäkerhet mot bakgrund av sitt avsedda ändamål och i enlighet med den allmänt erkända senaste utvecklingen. Kommissionen och relevanta organisationer och berörda parter uppmanas att ta vederbörlig hänsyn till riskbegränsning och AI-systemets negativa konsekvenser. Den förväntade graden av prestandamått bör anges i den medföljande bruksanvisningen. Leverantörer uppmanas att förmedla denna information till tillhandahållare på ett tydligt och lättbegripligt sätt, utan missförstånd eller vilseledande uttalanden. Unionsrätten om legal metrologi, inbegripet Europaparlamentets och rådets direktiv 2014/31/EU ([35]) och 2014/32/EU ([36]), syftar till att säkerställa mätningarnas noggrannhet och att bidra till öppenhet och rättvisa i handelstransaktioner. I detta sammanhang bör kommissionen, i samarbete med relevanta berörda parter och organisationer, såsom metrologi- och riktmärkningsmyndigheter, vid behov uppmuntra utvecklingen av riktmärken och mätmetoder för AI-system. Därvid bör kommissionen följa och samarbeta med internationella partner som arbetar med metrologi och relevanta mätindikatorer som rör AI.

([35]) Europaparlamentets och rådets direktiv 2014/31/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av icke-automatiska vågar (EUT L 96, 29.3.2014, s. 107).

([36]) Europaparlamentets och rådets direktiv 2014/32/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av mätinstrument (EUT L 96, 29.3.2014, s. 149).

(75) Teknisk robusthet är ett nyckelkrav för AI-system med hög risk. De bör vara resilienta mot skadligt eller på annat sätt oönskat beteende som kan bero på begränsningar inom de system eller den miljö där systemen fungerar (t.ex. felaktigheter, funktionsfel, inkonsekvenser, oväntade situationer). Därför bör tekniska och organisatoriska åtgärder vidtas för att säkerställa robustheten i AI-system med hög risk, till exempel genom att utforma och utveckla lämpliga tekniska lösningar för att förebygga eller minimera skadligt eller på annat sätt oönskat beteende. Dessa tekniska lösningar kan till exempel omfatta mekanismer som gör det möjligt för systemet att på ett säkert sätt avbryta sin drift (felsäkra planer) vid vissa avvikelser eller när driften sker utanför vissa på förhand fastställda gränser. Bristande skydd mot dessa risker kan leda till säkerhetskonsekvenser eller inverka negativt på grundläggande rättigheter, exempelvis på grund av felaktiga beslut eller felaktigheter eller bias i den utdata som genereras av AI-systemet.

(76) Cybersäkerhet har avgörande betydelse för att säkerställa att AI-system är resilienta mot försök att ändra deras användning, beteende eller prestanda eller att undergräva deras säkerhetsegenskaper genom tredje parter med avsikt att vålla skada som utnyttjar systemets svagheter. Cyberattacker mot AI-system kan riktas mot AI-specifika tillgångar, såsom träningsdataset (t.ex. dataförgiftning) eller tränade modeller (t.ex. antagonistiska attacker eller medlemskapsinferens), eller utnyttja sårbarheter i AI-systemets digitala tillgångar eller i den underliggande IKT-infrastrukturen. För att säkerställa en cybersäkerhetsnivå som är anpassad till riskerna bör lämpliga åtgärder såsom säkerhetskontroller därför vidtas av leverantörerna av AI-system med hög risk, även med beaktande av den underliggande IKT-infrastrukturen när så är lämpligt.

(77) Utan att det påverkar de krav avseende robusthet och riktighet som fastställs i denna förordning kan AI-system med hög risk som omfattas av tillämpningsområdet för en förordning från Europaparlamentet och rådet om övergripande cybersäkerhetskrav för produkter med digitala element i enlighet med den förordningen visa överensstämmelse med cybersäkerhetskraven i den här förordningen genom att uppfylla de grundläggande cybersäkerhetskrav som anges i den förordningen. Om AI-system med hög risk uppfyller de grundläggande kraven i en förordning från Europaparlamentet och rådet om övergripande cybersäkerhetskrav för produkter med digitala element, bör de anses uppfylla de cybersäkerhetskrav som fastställs i den här förordningen, i den mån uppfyllandet av dessa krav visas i den EU-försäkran om överensstämmelse eller delar av den som utfärdats enligt den förordningen. I detta syfte bör den bedömning av cybersäkerhetsrisker som är förknippade med en produkt med digitala element som klassificeras som AI-system med hög risk enligt den här förordningen och som utförs enligt en förordning från Europaparlamentet och rådet om övergripande cybersäkerhetskrav för produkter med digitala element, beakta risker för ett AI-systems cyberresiliens när det gäller obehöriga tredje parters försök att ändra dess användning, beteende eller prestanda, inbegripet AI-specifika sårbarheter såsom dataförgiftning eller antagonistiska attacker, samt, i relevanta fall, risker för grundläggande rättigheter i enlighet med kraven i den här förordningen.

(78) Det förfarande för bedömning av överensstämmelse som föreskrivs i denna förordning bör tillämpas på de grundläggande cybersäkerhetskraven för en produkt med digitala element som omfattas av en förordning från Europaparlamentet och rådet om övergripande cybersäkerhetskrav för produkter med digitala element och som klassificeras som ett AI-system med hög risk enligt den här förordningen. Denna regel bör dock inte leda till att den nödvändiga assuransnivån sänks för kritiska produkter med digitala element som omfattas av en förordning från Europaparlamentet och rådet om övergripande cybersäkerhetskrav för produkter med digitala element. Genom undantag från denna regel omfattas därför också AI-system med hög risk som omfattas av den här förordningen och som också kategoriseras som viktiga eller kritiska produkter med digitala element enligt en förordning från Europaparlamentet och rådet om övergripande cybersäkerhetskrav för produkter med digitala element, och på vilka förfarandet för bedömning av överensstämmelse baserat på intern kontroll enligt en bilaga till den här förordningen är tillämpligt, av bestämmelserna om bedömning av överensstämmelse i en förordning från Europaparlamentet och rådet om övergripande cybersäkerhetskrav för produkter med digitala element i den mån som de grundläggande cybersäkerhetskraven i den förordningen berörs. Om så är fallet bör de respektive bestämmelserna om bedömning av överensstämmelse på grundval av intern kontroll i en bilaga till den här förordningen gälla för alla andra aspekter som omfattas av den här förordningen. Med utgångspunkt i Enisas kunskap och expertis om den cybersäkerhetspolicy och de uppgifter som tilldelats Enisa enligt Europaparlamentets och rådets förordning (EU) 2019/881 ([37]) bör kommissionen samarbeta med Enisa i frågor som rör cybersäkerhet i AI-system.

([37]) Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

(79) Det är lämpligt att en specifik fysisk eller juridisk person, definierad som leverantören, tar ansvaret för utsläppande på marknaden eller ibruktagandet av ett AI-system med hög risk, oavsett om denna fysiska eller juridiska person är den person som utformat eller utvecklat systemet.

(80) Som signatärer av FN:s konvention om rättigheter för personer med funktionsnedsättning är unionen och alla medlemsstater rättsligt förpliktigade att skydda personer med funktionsnedsättning från diskriminering och främja deras jämlikhet, att säkerställa att personer med funktionsnedsättning på lika villkor som andra har tillgång till informations- och kommunikationsteknik och informations- och kommunikationssystem samt att säkerställa att integriteten hos personer med funktionsnedsättning respekteras. Med tanke på den ökande betydelsen och användningen av AI-system bör tillämpningen av universella konstruktionsprinciper för all ny teknik och alla nya tjänster säkerställa fullständig och jämlik tillgång för alla som potentiellt påverkas av eller använder AI-teknik, inbegripet personer med funktionsnedsättning, på ett sätt som tar full hänsyn till deras inneboende värdighet och mångfald. Det är därför viktigt att leverantörer säkerställer full överensstämmelse med tillgänglighetskrav, inbegripet Europaparlamentets och rådets direktiv (EU) 2016/2102 ([38]) och direktiv (EU) 2019/882. Leverantörer bör säkerställa att dessa krav uppfylls genom utformning. Därför bör de nödvändiga åtgärderna i så stor utsträckning som möjligt integreras i utformningen av AI-systemet med hög risk.

(81) Leverantören bör inrätta ett sunt kvalitetsstyrningssystem, säkerställa att det föreskrivna förfarandet för bedömning av överensstämmelse genomförs, utarbeta den relevanta dokumentationen och inrätta ett robust system för övervakning efter utsläppande på marknaden. Leverantörer av AI-system med hög risk som omfattas av skyldigheter avseende kvalitetsstyrningssystem enligt relevant sektorsspecifik unionsrätt bör ha möjlighet att inkludera delarna av det kvalitetsstyrningssystem som föreskrivs i denna förordning som en del av befintliga kvalitetsstyrningssystem som föreskrivs i denna andra sektorsspecifika unionsrätt. Komplementariteten mellan denna förordning och befintlig sektorsspecifik unionsrätt bör också beaktas i framtida standardiseringsverksamhet eller vägledning som antas av kommissionen. Offentliga myndigheter som för egen användning tar i bruk AI-system med hög risk kan anta och genomföra reglerna för kvalitetsstyrningssystem som en del av det kvalitetsstyrningssystem som införs på nationell eller regional nivå, beroende på vad som är lämpligt, med beaktande av sektorns särdrag och den berörda offentliga myndighetens kompetensområde och organisation.

(82) För att möjliggöra kontroll av efterlevnaden av denna förordning och skapa lika villkor för operatörer, och med beaktande av de olika formerna för att tillhandahålla digitala produkter, är det viktigt att säkerställa att en person som är etablerad i unionen under alla omständigheter kan förse myndigheterna med all nödvändig information om AI-systemens överensstämmelse. Innan leverantörer etablerade i tredjeländer tillhandahåller sina AI-system i unionen bör de genom skriftlig fullmakt utse ett ombud som är etablerat i unionen. Detta ombud har en central roll för att säkerställa att de AI-system med hög risk som släpps ut på marknaden eller tas i bruk av de leverantörer som inte är etablerade i unionen uppfyller kraven och för att fungera som leverantörernas kontaktperson etablerad i unionen.

(83) Mot bakgrund av karaktären hos och komplexiteten i värdekedjan för AI-system och i linje med den nya lagstiftningsramen är det viktigt att säkerställa rättssäkerhet och underlätta efterlevnaden av denna förordning. Det är därför nödvändigt att klargöra rollen och de särskilda skyldigheterna för berörda operatörer längs den värdekedjan, såsom importörer och distributörer som kan bidra till utvecklingen av AI-system. I vissa situationer kan dessa operatörer agera i mer än en roll samtidigt och bör därför kumulativt fullgöra alla relevanta skyldigheter med anknytning till dessa roller. En operatör kan till exempel samtidigt agera som distributör och importör.

(84) För att säkerställa rättssäkerhet är det nödvändigt att klargöra att under vissa särskilda villkor bör varje distributör, importör, tillhandahållare eller annan tredje part betraktas som leverantör av ett AI-system med hög risk och därför åta sig alla relevanta skyldigheter. Detta skulle vara fallet om den parten sätter sitt namn eller varumärke på ett AI-system med hög risk som redan släppts ut på marknaden eller tagits i bruk, utan att det påverkar avtalsarrangemang som föreskriver att skyldigheterna tilldelas på annat sätt. Detta skulle även vara fallet om den parten gör en väsentlig ändring av ett AI-system med hög risk som redan släppts ut på marknaden eller redan tagits i bruk på ett sätt som innebär att det förblir ett AI-system med hög risk i enlighet med denna förordning, eller om den ändrar det avsedda ändamålet med ett AI-system, inbegripet ett AI-system för allmänna ändamål, som inte har klassificerats som system med hög risk och som redan släppts ut på marknaden eller tagits i bruk, på ett sätt som innebär att AI-systemet blir ett AI-system med hög risk i enlighet med denna förordning. Dessa bestämmelser bör tillämpas utan att det påverkar tillämpningen av mer specifika bestämmelser som fastställs i vissa delar av unionens harmoniseringslagstiftning som bygger på den nya lagstiftningsramen, med vilken denna förordning bör tillämpas

([38]) Europaparlamentets och rådets direktiv (EU) 2016/2102 av den 26 oktober 2016 om tillgänglighet avseende offentliga myndigheters webbplatser och mobila applikationer (EUT L 327, 2.12.2016, s. 1).

gemensamt. Till exempel bör artikel 16.2 i förordning (EU) 2017/745, där det fastställs att vissa ändringar inte bör anses vara en ändring av en produkt som kan påverka dess överensstämmelse med de tillämpliga kraven, fortsätta att tillämpas på AI-system med hög risk som är medicintekniska produkter i den mening som avses i den förordningen.

(85) AI-system för allmänna ändamål kan själva användas som AI-system med hög risk eller kan vara komponenter i andra AI-system med hög risk. Därför bör leverantörerna av sådana system, på grund av systemens särskilda karaktär och för att säkerställa en rättvis ansvarsfördelning längs AI-värdekedjan, oavsett om systemen som sådana kan användas som AI-system med hög risk av andra leverantörer eller som komponenter i AI-system med hög risk och utom i de fall annat föreskrivs i denna förordning, ha ett nära samarbete med leverantörerna av de berörda AI-systemen med hög risk för att göra det möjligt för dem att uppfylla de relevanta skyldigheterna enligt denna förordning och rätta sig efter de behöriga myndigheter som inrättats enligt denna förordning.

(86) Om den leverantör som ursprungligen släppte ut AI-systemet på marknaden eller tog det i bruk, i enlighet med de villkor som fastställs i denna förordning, inte längre bör anses vara leverantör vid tillämpning av denna förordning, och om denna leverantör inte uttryckligen har uteslutit omvandlingen av AI-systemet till ett AI-system med hög risk, bör den förstnämnda leverantören detta till trots ha ett nära samarbete och tillgängliggöra den nödvändiga informationen och tillhandahålla den rimligen förväntade tekniska åtkomsten och annat stöd som krävs för att fullgöra de skyldigheter som fastställs i denna förordning, särskilt när det gäller efterlevnaden av bedömningen av överensstämmelse för AI-system med hög risk.

(87) Om ett AI-system med hög risk som ingår som säkerhetskomponent i en produkt som omfattas av unionens harmoniseringslagstiftning som bygger på den nya lagstiftningsramen inte släpps ut på marknaden och inte heller tas i bruk fristående från produkten, bör den produkttillverkare som definieras i den lagstiftningen fullgöra de leverantörsskyldigheter som fastställs i denna förordning och i synnerhet säkerställa att det AI-system som ingår i slutprodukten uppfyller kraven i denna förordning.

(88) Längs AI-värdekedjan tillhandahåller flera parter ofta AI-system, verktyg och tjänster, men även komponenter eller processer som leverantören integrerar i AI-systemet för olika ändamål som bland annat omfattar träning, omträning, testning och utvärdering av modeller samt integrering i programvara eller andra aspekter av modellutveckling. Dessa parter har en viktig roll i värdekedjan gentemot leverantören av AI-systemet med hög risk i vilken deras AI-system, verktyg, tjänster, komponenter eller processer är integrerade, och bör genom skriftligt avtal tillhandahålla denna leverantör nödvändig information, kapacitet, teknisk åtkomst och annat stöd baserat på den allmänt erkända senaste utvecklingen, för att göra det möjligt för leverantören att fullt ut uppfylla de skyldigheter som fastställs i denna förordning, utan att äventyra sina egna immateriella rättigheter eller företagshemligheter.

(89) Tredje parter som för allmänheten tillgängliggör andra verktyg, tjänster, processer eller AI-komponenter än AI-modeller för allmänna ändamål bör inte åläggas att uppfylla krav som är inriktade på ansvarsområdena längs AI-värdekedjan, särskilt gentemot den leverantör som har använt eller integrerat dem, när dessa verktyg, tjänster, processer eller AI-komponenter görs tillgängliga med en kostnadsfri licens med öppen källkod. Utvecklare av kostnadsfria verktyg, tjänster eller processer med öppen källkod, eller andra AI-modeller än AI-modeller för allmänna ändamål, bör uppmuntras att tillämpa allmänt vedertagen dokumentationspraxis, såsom modellkort och datablad, som ett sätt att påskynda informationsutbytet längs AI-värdekedjan, vilket gör det möjligt att främja tillförlitliga AI-system i unionen.

(90) Kommissionen kan utveckla och rekommendera frivilliga standardavtalsvillkor mellan leverantörer av AI-system med hög risk och tredje parter som tillhandahåller verktyg, tjänster, komponenter eller processer som används eller är integrerade i AI-system med hög risk för att underlätta samarbetet längs värdekedjan. Vid utarbetandet av frivilliga standardavtalsvillkor bör kommissionen också ta hänsyn till eventuella avtalskrav som är tillämpliga inom specifika sektorer eller affärsförhållanden.

(91) Mot bakgrund av AI-systemens natur och de risker för säkerhet och grundläggande rättigheter som kan vara förknippade med användningen av dem, inbegripet när det gäller behovet av att säkerställa en korrekt övervakning av ett AI-systems prestanda under verkliga förhållanden, är det lämpligt att fastställa särskilda ansvarsområden för tillhandahållare. Tillhandahållare bör i synnerhet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de använder AI-system med hög risk i enlighet med bruksanvisningarna, och vissa andra skyldigheter bör föreskrivas när det gäller övervakning av AI-systemens funktionssätt och i fråga om loggning, på lämpligt sätt.

Tillhandahållare bör dessutom säkerställa att de personer som anförtros uppgiften att implementera bruksanvisningarna och mänsklig kontroll enligt denna förordning har den kompetens som krävs, särskilt en lämplig nivå av AI-kunnighet, utbildning och befogenhet för att korrekt fullgöra dessa uppgifter. Dessa skyldigheter bör inte påverka andra skyldigheter för tillhandahållare i samband med AI-system med hög risk enligt unionsrätten eller nationell rätt.

(92) Denna förordning påverkar inte arbetsgivares skyldigheter att informera eller att informera och samråda med arbetstagare eller deras företrädare enligt unionsrätten eller nationell rätt och praxis, inbegripet Europaparlamentets och rådets direktiv 2002/14/EG ([39]), avseende beslut att ta i bruk eller använda AI-system. Det måste fortfarande säkerställas att arbetstagarna och deras företrädare informeras om det planerade införandet av AI-system med hög risk på arbetsplatsen om villkoren för dessa informations- eller informations- och samrådsskyldigheter i andra rättsliga instrument inte är uppfyllda. Denna rätt till information är dessutom kompletterande och nödvändig för att skydda de grundläggande rättigheter som ligger till grund för denna förordning. Därför bör ett informationskrav för detta fastställas i denna förordning utan att det påverkar arbetstagares befintliga rättigheter.

(93) Risker med anknytning till AI-system kan ha att göra med hur systemen utformas, men de kan även härröra från hur dessa AI-system används. Tillhandahållare av AI-system med hög risk spelar därför en avgörande roll när det gäller att säkerställa att grundläggande rättigheter skyddas, och kompletterar leverantörens skyldigheter vid utvecklingen av AI-systemet. Tillhandahållare har bäst förutsättningar att förstå hur AI-system med hög risk kommer att användas i praktiken och kan därför fastställa potentiella risker som inte har förutsetts under utvecklingsfasen, tack vare mer exakt kunskap om sammanhanget för användningen och de personer eller grupper av personer som sannolikt kommer att påverkas, däribland sårbara grupper. Tillhandahållare av AI-system med hög risk som förtecknas i en bilaga till denna förordning spelar också en avgörande roll när det gäller att informera fysiska personer och bör när de fattar beslut eller hjälper till att fatta beslut som rör fysiska personer i förekommande fall informera de fysiska personerna om att de är föremål för användning av AI-systemet med hög risk. Denna information bör omfatta det avsedda ändamålet och typen av beslut som det fattar. Tillhandahållaren bör också informera fysiska personer om deras rätt till en förklaring enligt denna förordning. När det gäller AI-system med hög risk som används för brottsbekämpande ändamål bör denna skyldighet genomföras i enlighet med artikel 13 i direktiv (EU) 2016/680.

(94) All behandling av biometriska uppgifter som ingår i användningen av AI-system för biometrisk identifiering för brottsbekämpning måste vara förenlig med artikel 10 i direktiv (EU) 2016/680, som medger sådan behandling endast när det är absolut nödvändigt, med förbehåll för lämpliga skyddsåtgärder för den registrerades rättigheter och friheter, och när detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt. När sådan användning är tillåten måste den också respektera de principer som fastställs i artikel 4.1 i direktiv (EU) 2016/680, inbegripet laglighet, rättvisa och öppenhet, ändamålsbegränsning, korrekthet och lagringsbegränsning.

(95) Utan att det påverkar tillämplig unionsrätt, särskilt förordning (EU) 2016/679 och direktiv (EU) 2016/680, bör användningen av system för biometrisk fjärridentifiering i efterhand omfattas av skyddsåtgärder, med tanke på den inkräktande karaktären hos system för biometrisk fjärridentifiering i efterhand. System för biometrisk fjärridentifiering i efterhand bör alltid användas på ett sätt som är proportionellt, legitimt och strikt nödvändigt, och därmed målinriktat, när det gäller de personer som ska identifieras, plats och tidsmässig omfattning samt baserat på ett slutet dataset av lagligen förvärvade videoupptagningar. Under alla omständigheter bör system för biometrisk fjärridentifiering i efterhand inte användas inom ramen för brottsbekämpning för att leda till urskillningslös övervakning. Villkoren för biometrisk fjärridentifiering i efterhand bör under inga omständigheter utgöra en grund för att kringgå villkoren för förbudet och de strikta undantagen för biometrisk fjärridentifiering i realtid.

(96) För att effektivt säkerställa att grundläggande rättigheter skyddas bör tillhandahållare av AI-system med hög risk som är offentligrättsliga organ, eller privata enheter som tillhandahåller offentliga tjänster och tillhandahållare av vissa AI-system med hög risk som förtecknas i en bilaga till denna förordning, såsom bank- eller försäkringsenheter, genomföra en konsekvensbedömning avseende grundläggande rättigheter innan systemen tas i bruk. Tjänster som är viktiga för enskilda personer och som är av offentlig karaktär kan också tillhandahållas av privata enheter. Privata enheter som tillhandahåller offentliga tjänster är kopplade till uppgifter av allmänt intresse, såsom inom utbildning, hälso- och sjukvård, sociala tjänster, bostäder och rättsskipning. Syftet med konsekvensbedömningen avseende grundläggande rättigheter är att tillhandahållaren ska identifiera de specifika riskerna för rättigheterna för enskilda personer eller grupper av enskilda personer som sannolikt kommer att beröras och identifiera åtgärder som ska

([39]) Europaparlamentets och rådets direktiv 2002/14/EG av den 11 mars 2002 om inrättande av en allmän ram för information till och samråd med arbetstagare i Europeiska gemenskapen (EGT L 80, 23.3.2002, s. 29).

vidtas om dessa risker förverkligas. Konsekvensbedömningen bör göras innan AI-systemet med hög risk införs och bör uppdateras när tillhandahållaren anser att någon av de relevanta faktorerna har förändrats. Konsekvensbedömningen bör identifiera tillhandahållarens relevanta processer där AI-systemet med hög risk kommer att användas i linje med dess avsedda ändamål, och bör innehålla en beskrivning av den tidsperiod under vilken och den frekvens med vilken systemet är avsett att användas samt av specifika kategorier av fysiska personer och grupper som sannolikt kommer att påverkas i det specifika användningssammanhanget. Bedömningen bör också omfatta identifiering av särskilda risker för skada som sannolikt kommer att påverka dessa personers eller gruppers grundläggande rättigheter. Vid utförandet av denna bedömning bör tillhandahållaren beakta information som är relevant för en korrekt konsekvensbedömning, inbegripet men inte begränsat till den information som tillhandahålls av leverantören av AI-systemet med hög risk i bruksanvisningen. Mot bakgrund av de risker som identifierats bör tillhandahållare fastställa vilka åtgärder som ska vidtas om dessa risker förverkligas, inbegripet till exempel styrningsformer i det specifika användningssammanhanget, såsom arrangemang för mänsklig kontroll i enlighet med bruksanvisningen eller klagomålshanteringsförfaranden och prövningsförfaranden, eftersom de kan vara avgörande för att bidra till att begränsa riskerna för grundläggande rättigheter i konkreta användningsfall. Efter att ha utfört denna konsekvensbedömning bör tillhandahållaren underrätta den berörda marknadskontrollmyndigheten. För att samla in relevant information som är nödvändig för att utföra konsekvensbedömningen kan tillhandahållare av AI-system med hög risk, särskilt när AI-system används i den offentliga sektorn, involvera relevanta berörda parter, inbegripet företrädare för grupper av personer som sannolikt kommer att påverkas av AI-systemet, oberoende experter och organisationer i det civila samhället i genomförandet av sådana konsekvensbedömningar och utformningen av åtgärder som ska vidtas om riskerna förverkligas. Europeiska byrån för artificiell intelligens (AI-byrån) bör utarbeta en mall för ett frågeformulär för att underlätta efterlevnad och minska den administrativa bördan för tillhandahållare.

(97) För att skapa rättssäkerhet bör begreppet AI-modeller för allmänna ändamål definieras tydligt och särskiljas från begreppet AI-system. Definitionen bör baseras på de viktigaste funktionella egenskaperna hos en AI-modell för allmänna ändamål, generaliteten och förmågan att på ett kompetent sätt utföra ett stort antal olika uppgifter. Dessa modeller tränas vanligtvis med stora mängder data genom olika metoder, såsom självövervakad inlärning, oövervakad inlärning eller återkopplingsinlärning. AI-modeller för allmänna ändamål får släppas ut på marknaden på olika sätt, bland annat genom bibliotek, gränssnitt för applikationsprogrammering, som direkt nedladdning eller som fysisk kopia. Dessa modeller kan ändras ytterligare eller finjusteras till nya modeller. Även om AI-modeller är väsentliga komponenter i AI-system utgör de inte AI-system i sig. AI-modeller kräver tillägg av ytterligare komponenter, till exempel ett användargränssnitt, för att bli AI-system. AI-modeller är vanligtvis integrerade i och utgör en del av AI-system. I denna förordning fastställs särskilda regler för AI-modeller för allmänna ändamål och för AI-modeller för allmänna ändamål som medför systemrisker, vilka bör gälla även när dessa modeller är integrerade eller ingår i ett AI-system. Det bör förstås att skyldigheterna för leverantörer av AI-modeller för allmänna ändamål bör gälla när AI-modellerna för allmänna ändamål släpps ut på marknaden. När leverantören av en AI-modell för allmänna ändamål integrerar en egen modell i sitt eget AI-system som tillhandahålls på marknaden eller tas i bruk, bör den modellen anses ha släppts ut på marknaden, och skyldigheterna i denna förordning för modeller bör därför fortsätta att gälla utöver skyldigheterna för AI-system. De skyldigheter som föreskrivs för modeller bör under alla omständigheter inte gälla när en egen modell används för rent interna processer som inte är väsentliga för att tillhandahålla en produkt eller tjänst till tredje parter och fysiska personers rättigheter inte påverkas. Med tanke på att de har potentiellt betydande negativa effekter bör AI-modeller för allmänna ändamål med systemrisk alltid omfattas av de relevanta skyldigheterna enligt denna förordning. Definitionen bör inte omfatta AI-modeller som används innan de släpps ut på marknaden enbart för forsknings-, utvecklings- och prototypverksamhet. Detta påverkar inte skyldigheten att följa denna förordning när en modell släpps ut på marknaden efter sådan verksamhet.

(98) En modells generalitet kan, bland annat, också bestämmas av ett antal parametrar, men modeller med minst en miljard parametrar som tränats med en stor mängd data med hjälp av självövervakning i stor skala bör anses uppvisa betydande generalitet och på ett kompetent sätt utföra ett brett spektrum av olika uppgifter.

(99) Stora generativa AI-modeller är ett typiskt exempel på en AI-modell för allmänna ändamål, eftersom de möjliggör flexibel generering av innehåll, exempelvis i form av text, ljud, bilder eller video, som lätt kan rymma ett brett spektrum av olika uppgifter.

(100) När en AI-modell för allmänna ändamål integreras i eller ingår i ett AI-system bör detta system anses vara ett AI-system för allmänna ändamål när systemet, på grund av denna integrering, har förmåga att tjäna en rad olika ändamål. Ett AI-system för allmänna ändamål kan användas direkt eller integreras i andra AI-system.

(101) Leverantörer av AI-modeller för allmänna ändamål har en särskild roll och ett särskilt ansvar i AI-värdekedjan, eftersom de modeller som de tillhandahåller kan utgöra grunden för en rad system i efterföljande led, som ofta tillhandahålls av leverantörer i efterföljande led, vilka behöver ha god kunskap om modellerna och deras kapacitet, både för att möjliggöra integrering av sådana modeller i sina produkter och för att fullgöra sina skyldigheter enligt denna eller andra förordningar. Därför bör proportionella transparensåtgärder föreskrivas, inbegripet utarbetande och uppdatering av dokumentation och tillhandahållande av information om AI-modellen för allmänna ändamål för dess användning av leverantörer i efterföljande led. Den tekniska dokumentationen bör utarbetas och hållas uppdaterad av leverantören av AI-modellen för allmänna ändamål så att den på begäran kan tillhandahållas AI-byrån och de nationella behöriga myndigheterna. Den minimiuppsättning element som ska ingå i sådan dokumentation bör anges i särskilda bilagor till denna förordning. Kommissionen bör ges befogenhet att ändra dessa bilagor genom delegerade akter mot bakgrund av ny teknisk utveckling.

(102) Programvara och data, inbegripet modeller, som släpps ut med en kostnadsfri licens med öppen källkod som gör det möjligt att dela dem öppet och där användarna fritt kan få tillgång till, använda, modifiera och omdistribuera dem eller ändrade versioner av dem, kan bidra till forskning och innovation på marknaden och ge betydande tillväxtmöjligheter för unionens ekonomi. AI-modeller för allmänna ändamål som släpps ut med kostnadsfria licenser med öppen källkod bör övervägas för att säkerställa en hög grad av transparens och öppenhet om modellernas parametrar, inbegripet vikter, information om modellarkitekturen samt information om modellanvändning görs allmänt tillgängliga. Licensen bör betraktas som kostnadsfri licens med öppen källkod även när den gör det möjligt för användare att köra, kopiera, distribuera, studera, ändra och förbättra programvara och data, inbegripet modeller under förutsättning att den ursprungliga leverantören av modellen krediteras och att identiska eller jämförbara distributionsvillkor respekteras.

(103) Kostnadsfria AI-komponenter med öppen källkod omfattar programvara och data, inbegripet modeller och AI-modeller för allmänna ändamål, verktyg, tjänster eller processer i ett AI-system. Kostnadsfria AI-komponenter med öppen källkod kan tillhandahållas genom olika kanaler, inbegripet utveckling av dem i öppna databaser. Vid tillämpningen av denna förordning bör AI-komponenter som tillhandahålls mot en kostnad eller på annat sätt monetariseras, inbegripet genom tillhandahållande av tekniskt stöd eller andra tjänster, inbegripet genom en programvaruplattform, som rör AI-komponenten, eller användning av personuppgifter av andra skäl än uteslutande för att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet, med undantag för transaktioner mellan mikroföretag, inte omfattas av de undantag som föreskrivs för kostnadsfria AI-komponenter med öppen källkod. Det faktum att AI-komponenter tillhandahålls via öppna databaser bör inte i sig utgöra en monetarisering.

(104) Leverantörer av AI-modeller för allmänna ändamål som släpps ut med en kostnadsfri licens med öppen källkod och vars parametrar, inbegripet vikter, information om modellarkitekturen och information om modellanvändning, görs allmänt tillgängliga bör omfattas av undantag från de transparensrelaterade krav som gäller för AI-modeller för allmänna ändamål, såvida de inte kan anses utgöra en systemrisk, i vilket fall den omständigheten att modellen är transparent och åtföljs av en licens med öppen källkod inte bör anses vara ett tillräckligt skäl för att utesluta efterlevnad av skyldigheterna enligt denna förordning. Med tanke på att utsläppandet av AI-modeller för allmänna ändamål med en kostnadsfri licens med öppen källkod inte nödvändigtvis avslöjar väsentlig information om det dataset som används för träning eller finjustering av modellen och om hur efterlevnaden av upphovsrätten därmed säkerställdes, bör det undantag som föreskrivs för AI-modeller för allmänna ändamål från efterlevnad av transparensrelaterade krav under alla omständigheter inte avse skyldigheten att utarbeta en sammanfattning av det innehåll som används för modellträning och skyldigheten att införa en policy för efterlevnad av unionens upphovsrättsliga lagstiftning, särskilt för att identifiera och efterleva förbehållet för rättigheter enligt artikel 4.3 i Europaparlamentets och rådets direktiv (EU) 2019/790 ([40]).

(105) AI-modeller för allmänna ändamål, särskilt stora generativa AI-modeller, som kan generera text, bilder och annat innehåll, erbjuder unika innovationsmöjligheter men utgör även utmaningar för konstnärer, författare och andra upphovsmän och för det sätt på vilket deras kreativa innehåll skapas, distribueras, används och konsumeras. Utvecklingen och träningen av sådana modeller kräver tillgång till stora mängder text, bilder, videor och andra data. Text- och datautvinningstekniker kan användas i stor utsträckning i detta sammanhang för hämtning och analys av sådant innehåll, som kan vara skyddat av upphovsrätt och närstående rättigheter. All användning av upphovsrättsligt skyddat innehåll kräver tillstånd från den berörda rättsinnehavaren, såvida inte relevanta upphovsrättsliga undantag och inskränkningar tillämpas. Genom direktiv (EU) 2019/790 infördes undantag och inskränkningar som tillåter mångfaldigande av och utdrag ur verk eller andra alster, för text- och datautvinningsändamål, på vissa villkor. Enligt

([40]) Europaparlamentets och rådets direktiv (EU) 2019/790 av den 17 april 2019 om upphovsrätt och närstående rättigheter på den digitala inre marknaden och om ändring av direktiven 96/9/EG och 2001/29/EG (EUT L 130, 17.5.2019, s. 92).

dessa regler får rättsinnehavare välja att rättigheterna till deras verk eller andra alster ska förbehållas dem för att förhindra text- och datautvinning, såvida detta inte sker för forskningsändamål. Om undantaget har förbehållits uttryckligen på lämpligt sätt måste leverantörer av AI-modeller för allmänna ändamål erhålla ett tillstånd från rättsinnehavarna om de vill utföra text- och datautvinning från sådana verk.

(106) Leverantörer som släpper ut AI-modeller för allmänna ändamål på unionsmarknaden bör säkerställa efterlevnad av de relevanta skyldigheterna i denna förordning. För detta ändamål bör leverantörer av AI-modeller för allmänna ändamål införa en policy för efterlevnad av unionsrätten om upphovsrätt och närstående rättigheter, särskilt för att identifiera och efterleva förbehåll om rättigheter som uttryckts av rättsinnehavare enligt artikel 4.3 i direktiv (EU) 2019/790. Alla leverantörer som släpper ut en AI-modell för allmänna ändamål på unionsmarknaden bör uppfylla denna skyldighet, oavsett i vilken jurisdiktion de upphovsrättsligt relevanta handlingar som ligger till grund för träningen av dessa AI-modeller för allmänna ändamål äger rum. Detta är nödvändigt för att säkerställa lika villkor för leverantörer av AI-modeller för allmänna ändamål, så att ingen leverantör får en konkurrensfördel på unionsmarknaden genom att tillämpa lägre upphovsrättsstandarder än de som tillhandahålls i unionen.

(107) För att öka transparensen när det gäller de data som används i förträning och träning av AI-modeller för allmänna ändamål, inbegripet text och data som skyddas av upphovsrätt, är det lämpligt att leverantörer av sådana modeller utarbetar en tillräckligt detaljerad sammanfattning av det innehåll som används för att träna AI-modellen för allmänna ändamål och gör denna allmänt tillgänglig. Samtidigt som vederbörlig hänsyn tas till behovet av att skydda företagshemligheter och konfidentiell affärsinformation bör denna sammanfattning ha en allmän omfattning med avseende på tillämpningsområde i stället för att vara tekniskt detaljerad, så att det blir det lättare för parter med legitima intressen, inbegripet upphovsrättsinnehavare, att utöva och hävda sina rättigheter enligt unionsrätten, till exempel genom att förteckna de viktigaste datauppsättningarna eller dataseten som ingick i träningen av modellen, såsom stora privata eller offentliga databaser eller dataarkiv, och genom att tillhandahålla en beskrivande förklaring om andra datakällor som använts. Det är lämpligt att AI-byrån tillhandahåller en mall för sammanfattningen, som bör vara enkel och effektiv och göra det möjligt för leverantören att tillhandahålla den sammanfattning som krävs i beskrivande form.

(108) När det gäller de skyldigheter som åläggs leverantörer av AI-modeller för allmänna ändamål att införa en policy för efterlevnad av unionens upphovsrättslagstiftning och göra en sammanfattning av det innehåll som används för träningen allmänt tillgänglig, bör AI-byrån övervaka huruvida leverantören har uppfyllt dessa skyldigheter utan att kontrollera eller gå vidare till en bedömning verk för verk av träningsdata när det gäller efterlevnaden av upphovsrätten. Denna förordning påverkar inte kontrollen av efterlevnaden av upphovsrättsliga bestämmelser enligt unionsrätten.

(109) Efterlevnaden av de skyldigheter som är tillämpliga på leverantörer av AI-modeller för allmänna ändamål bör stå i proportion till typen av modelleverantör, vilket utesluter behovet av efterlevnad för personer som utvecklar eller använder modeller för icke-yrkesmässiga ändamål eller vetenskapliga forskningsändamål, vilka dock bör uppmuntras att frivilligt uppfylla dessa krav. Utan att det påverkar tillämpningen av unionens upphovsrättslagstiftning bör fullgörandet av dessa skyldigheter ta vederbörlig hänsyn till leverantörens storlek och möjliggöra förenklade efterlevnadsmetoder för små och medelstora företag, inbegripet uppstartsföretag, som inte bör innebära en alltför stor kostnad och inte avskräcka från användningen av sådana modeller. Vid ändring eller finjustering av en modell bör skyldigheterna för leverantörer av AI-modeller för allmänna ändamål begränsas till den ändringen eller finjusteringen, till exempel genom att komplettera den redan befintliga tekniska dokumentationen med information om ändringarna, inbegripet nya träningsdatakällor, som ett sätt att uppfylla de skyldigheter avseende värdekedjan som föreskrivs i denna förordning.

(110) AI-modeller för allmänna ändamål kan medföra systemrisker som omfattar, men inte är begränsade till, faktiska eller rimligen förutsebara negativa effekter i samband med allvarliga olyckor, störningar i kritiska sektorer och allvarliga konsekvenser för folkhälsan och säkerheten, alla faktiska eller rimligen förutsebara negativa effekter på demokratiska processer, allmän och ekonomisk säkerhet, och spridning av olagligt, falskt eller diskriminerande innehåll. Det bör antas att systemrisker ökar med modellkapacitet och modellräckvidd, kan uppstå under modellens hela livscykel och påverkas av förhållanden med felaktig användning, modellens tillförlitlighet, rättvisa och säkerhet, dess grad av autonomi, tillgång till verktyg, nya eller kombinerade metoder, strategier för utsläppande och distribution, potentialen att avlägsna skyddsmekanismer och andra faktorer. I synnerhet har internationella strategier hittills identifierat behovet av att ägna uppmärksamhet åt risker till följd av potentiellt avsiktlig felaktig användning eller oavsiktliga kontrollproblem i samband med anpassning till mänsklig avsikt, kemiska, biologiska, radiologiska och nukleära risker, såsom de sätt på vilka inträdeshindren kan minskas, inbegripet för utveckling, konstruktion, förvärv

eller användning av vapen, offensiv cyberkapacitet, såsom de sätt på vilka upptäckt, utnyttjande eller operativ användning av sårbarheter kan möjliggöras, effekterna av interaktion och verktygsanvändning, inklusive till exempel kapaciteten att styra fysiska system och störa kritisk infrastruktur, risker med modeller för framställning av kopior av dem själva eller *självreplikering* eller träning av andra modeller, de sätt på vilka modeller kan ge upphov till skadlig bias och diskriminering med risker för enskilda personer, grupper eller samhällen, underlättandet av desinformation eller skada på integritet med hot mot demokratiska värden och mänskliga rättigheter, och risk för att en viss händelse kan leda till en kedjereaktion med betydande negativa effekter som kan påverka upp till en hel stad, en hel domäns verksamhet eller ett helt lokalsamhälle.

(111) En metod bör fastställas för klassificering av AI-modeller för allmänna ändamål som AI-modeller för allmänna ändamål med systemrisker. Eftersom systemrisker härrör från särskilt hög kapacitet bör en AI-modell för allmänna ändamål anses medföra systemrisker om den har kapacitet med hög påverkansgrad, utvärderad på grundval av lämpliga tekniska verktyg och metoder, eller har betydande inverkan på den inre marknaden på grund av sin räckvidd. Med kapacitet med hög påverkansgrad i AI-modeller för allmänna ändamål avses kapacitet som motsvarar eller överstiger den kapacitet som registrerats i de mest avancerade AI-modellerna för allmänna ändamål. Hela spektrumet av kapacitet i en modell kan förstås bättre efter det att den släppts ut på marknaden eller när tillhandahållare interagerar med modellen. Enligt den senaste utvecklingen vid tidpunkten för denna förordnings ikraftträdande är den sammanlagda beräkningsmängd som används för träning av AI-modellen för allmänna ändamål, mätt i flyttalsberäkningar, en av de relevanta approximationerna för modellkapacitet. Den sammanlagda beräkningsmängd som används för träning inkluderar den beräkning som används för de verksamheter och metoder som är avsedda att förbättra modellens kapacitet före införandet, såsom förträning, generering av syntetiska data och finjustering. Därför bör ett inledande tröskelvärde för flyttalsberäkningar fastställas som, om det uppfylls av en AI-modell för allmänna ändamål, leder till en presumtion om att modellen är en AI-modell för allmänna ändamål med systemrisker. Detta tröskelvärde bör justeras med tiden för att återspegla tekniska och industriella förändringar, såsom algoritmiska förbättringar eller ökad hårdvarueffektivitet, och bör kompletteras med riktmärken och indikatorer för modellkapacitet. För att ta fram underlag för detta bör AI-byrån samarbeta med forskarsamhället, industrin, det civila samhället och andra experter. Tröskelvärden, liksom verktyg och riktmärken för bedömning av kapacitet med hög påverkansgrad, bör vara kraftfulla prediktorer för generalitet, dess kapacitet och tillhörande systemrisk hos AI-modeller för allmänna ändamål, och kan ta hänsyn till hur modellen kommer att släppas ut på marknaden eller hur många användare den kan påverka. För att komplettera detta system bör kommissionen ha möjlighet att fatta enskilda beslut om att utse en AI-modell för allmänna ändamål till en AI-modell för allmänna ändamål med systemrisk, om det konstateras att en sådan modell har en kapacitet eller en inverkan som är likvärdig med den som blir resultatet med det fastställda tröskelvärdet. Det beslutet bör fattas på grundval av en övergripande bedömning av de kriterier för utseende av en AI-modell för allmänna ändamål med systemrisk som förtecknas i en bilaga till denna förordning, såsom kvaliteten på eller storleken på träningsdatasetet, antalet företags- och slutanvändare, dess metoder för in- och utdata, dess grad av autonomi och skalbarhet, eller de verktyg som det har tillgång till. På motiverad begäran av en leverantör vars modell har betecknats som en AI-modell för allmänna ändamål med systemrisk bör kommissionen beakta begäran och kan besluta att ompröva huruvida AI-modellen för allmänna ändamål fortfarande kan anses medföra systemrisker.

(112) En metod bör fastställas för klassificeringen av AI-modeller för allmänna ändamål som AI-modeller för allmänna ändamål med systemrisker. En AI-modell för allmänna ändamål som uppfyller det tillämpliga tröskelvärdet för kapacitet med hög påverkansgrad bör antas vara en AI-modell för allmänna ändamål med systemrisk. Leverantören bör underrätta AI-byrån senast två veckor efter det att kraven har uppfyllts eller det blir känt att en AI-modell för allmänna ändamål kommer att uppfylla de krav som leder till presumtionen. Detta är särskilt relevant när det gäller tröskelvärdet för flyttalsberäkningar, eftersom träning av AI-modeller för allmänna ändamål kräver betydande planering, vilket inbegriper förhandstilldelning av beräkningskraftsresurser, och därför kan leverantörer av AI-modeller för allmänna ändamål veta om deras modell skulle uppfylla tröskelvärdet innan träningen avslutas. I samband med denna underrättelse bör leverantören kunna visa att en AI-modell för allmänna ändamål på grund av sina särskilda egenskaper undantagsvis inte medför några systemrisker och att den därför inte bör klassificeras som en AI-modell för allmänna ändamål med systemrisker. Denna information är värdefull för att AI-byrån ska kunna förutse utsläppandet på marknaden av AI-modeller för allmänna ändamål med systemrisker, och leverantörerna kan börja samarbeta med AI-byrån i ett tidigt skede. Den informationen är särskilt viktig när det gäller AI-modeller för

allmänna ändamål som planeras att släppas ut med öppen källkod, med tanke på att de åtgärder som krävs för att säkerställa efterlevnaden av skyldigheterna enligt denna förordning kan vara svårare att genomföra efter att modellen med öppen källkod har släppts ut.

(113) Om kommissionen får kännedom om att en AI-modell för allmänna ändamål uppfyller kraven för att klassificeras som en AI-modell för allmänna ändamål med systemrisk, som antingen inte tidigare varit känd eller som den berörda leverantören inte har underrättat kommissionen om, bör kommissionen ges befogenhet att beteckna den som sådan. Ett system med kvalificerade varningar bör säkerställa att den vetenskapliga panelen uppmärksammar AI-byrån på AI-modeller för allmänna ändamål som eventuellt bör klassificeras som AI-modeller för allmänna ändamål med systemrisk, utöver AI-byråns övervakningsverksamhet.

(114) Utöver de skyldigheter som föreskrivs för leverantörer av AI-modeller för allmänna ändamål bör leverantörer av AI-modeller för allmänna ändamål som medför systemrisker omfattas av skyldigheter som syftar till att identifiera och begränsa dessa risker och säkerställa en lämplig nivå av cybersäkerhetsskydd, oavsett om den tillhandahålls som en fristående modell eller inbyggd i ett AI-system eller en produkt. För att uppnå dessa mål bör det genom denna förordning krävas att leverantörer utför nödvändiga utvärderingar av modeller, särskilt innan de släpps ut på marknaden för första gången, vilket bör inbegripa att genomföra och dokumentera antagonistiska tester av modeller, även när så är lämpligt genom intern eller oberoende extern testning. Dessutom bör leverantörer av AI-modeller för allmänna ändamål med systemrisker kontinuerligt bedöma och begränsa systemriskerna, bland annat genom att införa riskhanteringspolicyer, såsom processer för ansvarsskyldighet och styrning, genomföra övervakning efter utsläppande på marknaden, vidta lämpliga åtgärder längs hela modellens livscykel och samarbeta med relevanta aktörer längs AI-värdekedjan.

(115) Leverantörer av AI-modeller för allmänna ändamål med systemrisker bör bedöma och begränsa eventuella systemrisker. Om utvecklingen eller användningen av modellen, trots insatser för att identifiera och förebygga risker i samband med en AI-modell för allmänna ändamål som kan medföra systemrisker, orsakar en allvarlig incident, bör leverantören av AI-modellen för allmänna ändamål utan oskäligt dröjsmål bevaka incidenten och rapportera all relevant information och möjliga korrigerande åtgärder till kommissionen och de nationella behöriga myndigheterna. Dessutom bör leverantörer säkerställa en lämplig nivå av cybersäkerhetsskydd för modellen och dess fysiska infrastruktur, om så är lämpligt, under modellens hela livscykel. Cybersäkerhetsskydd som avser systemrisker i samband med skadlig användning eller attacker bör ta vederbörlig hänsyn till oavsiktligt modelläckage, otillåtet utsläppande, kringgående av säkerhetsåtgärder och försvar mot cyberattacker, obehörig åtkomst eller modellstöld. Detta skydd kan underlättas genom att modellvikter, algoritmer, servrar och dataset säkras, exempelvis genom operativa säkerhetsåtgärder för informationssäkerhet, särskilda cybersäkerhetspolicyer, lämpliga tekniska och etablerade lösningar samt kontroller av cyberåtkomst och fysisk åtkomst som är lämpliga för de relevanta omständigheterna och riskerna i samband med detta.

(116) AI-byrån bör uppmuntra och underlätta utarbetandet, översynen och anpassningen av förfarandekoder, med beaktande av internationella strategier. Alla leverantörer av AI-modeller för allmänna ändamål kan bjudas in att delta. För att säkerställa att förfarandekoderna återspeglar den senaste utvecklingen och tar vederbörlig hänsyn till en rad olika perspektiv bör AI-byrån samarbeta med relevanta nationella behöriga myndigheter och kan, när så är lämpligt, samråda med det civila samhällets organisationer och andra relevanta intressenter och experter, inbegripet den vetenskapliga panelen, för att utarbeta sådana koder. Förfarandekoder bör omfatta skyldigheter för leverantörer av AI-modeller för allmänna ändamål och AI-modeller för allmänna ändamål som medför systemrisker. När det gäller systemrisker bör förfarandekoder dessutom bidra till att fastställa en risktaxonomi för systemriskernas typ och art på unionsnivå, inbegripet källorna till dem. Förfarandekoder bör också inriktas på särskilda riskbedömnings- och riskbegränsningsåtgärder.

(117) Förfarandekoderna bör utgöra ett centralt verktyg för korrekt fullgörande av de skyldigheter som föreskrivs i denna förordning för leverantörer av AI-modeller för allmänna ändamål. Leverantörerna bör kunna förlita sig på förfarandekoder för att visa att skyldigheterna fullgörs. Genom genomförandeakter kan kommissionen besluta att godkänna en förfarandekod och ge den en allmän giltighet inom unionen, eller alternativt att tillhandahålla gemensamma regler för genomförandet av de relevanta skyldigheterna, om en förfarandekod vid den tidpunkt då denna förordning blir tillämplig inte kan färdigställas eller inte anses vara lämplig av AI-byrån. När en harmoniserad

standard har offentliggjorts och bedömts vara lämplig för att täcka AI-byråns relevanta skyldigheter bör efterlevnad av en europeisk harmoniserad standard ge leverantörer presumtion om överensstämmelse. Leverantörer av AI-modeller för allmänna ändamål bör dessutom kunna påvisa efterlevnad med hjälp av alternativa lämpliga sätt, om förfarandekoder eller harmoniserade standarder inte finns tillgängliga, eller om de väljer att inte förlita sig på dessa.

(118) Denna förordning reglerar AI-system och AI-modeller genom att införa vissa krav och skyldigheter för relevanta marknadsaktörer som släpper ut dem på marknaden, tar dem i bruk eller använder dem i unionen, och kompletterar därigenom skyldigheterna för leverantörer av förmedlingstjänster som bygger in sådana system eller modeller i sina tjänster som regleras genom förordning (EU) 2022/2065. I den mån sådana system eller modeller är inbyggda i utsedda mycket stora onlineplattformar eller mycket stora onlinesökmotorer omfattas de av den riskhanteringsram som föreskrivs i förordning (EU) 2022/2065. Följaktligen bör motsvarande skyldigheter i den här förordningen förutsättas vara uppfyllda, såvida inte betydande systemrisker som inte omfattas av förordning (EU) 2022/2065 uppstår och identifieras i sådana modeller. Inom denna ram är leverantörer av mycket stora onlineplattformar och mycket stora onlinesökmotorer skyldiga att bedöma potentiella systemrisker som härrör från utformningen, funktionen och användningen av deras tjänster, inbegripet hur utformningen av algoritmiska system som används i tjänsten kan bidra till sådana risker, samt systemrisker som härrör från potentiell felaktig användning. Dessa leverantörer är också skyldiga att vidta lämpliga riskbegränsningsåtgärder med respekt för grundläggande rättigheter.

(119) Med tanke på den snabba innovationstakten och den tekniska utvecklingen av digitala tjänster som omfattas av olika unionsrättsliga instrument, särskilt med tanke på mottagarnas användning och uppfattning, kan de AI-system som omfattas av denna förordning tillhandahållas som förmedlingstjänster eller delar av sådana i den mening som avses i förordning (EU) 2022/2065, som bör tolkas på ett teknikneutralt sätt. AI-system kan till exempel användas för att tillhandahålla onlinesökmotorer, särskilt i den mån ett AI-system såsom en onlinechatbot gör sökningar på, i princip, alla webbplatser, sedan införlivar resultaten i sin befintliga kunskap och använder den uppdaterade kunskapen för att generera ett enda resultat som kombinerar olika informationskällor.

(120) Dessutom är de skyldigheter som åläggs leverantörer och tillhandahållare av vissa AI-system i denna förordning för att det ska vara möjligt att upptäcka och visa att utdata från dessa system genereras eller manipuleras artificiellt särskilt relevanta för att underlätta ett effektivt genomförande av förordning (EU) 2022/2065. Detta gäller särskilt i fråga om skyldigheterna för leverantörer av mycket stora onlineplattformar eller mycket stora onlinesökmotorer att identifiera och begränsa systemrisker som kan uppstå till följd av spridning av innehåll som genererats eller manipulerats artificiellt, särskilt risken för faktiska eller förutsebara negativa effekter på demokratiska processer, samhällsdebatten och valprocesser, inbegripet genom desinformation.

(121) Standardisering bör ha en nyckelroll för att förse leverantörer med tekniska lösningar för att säkerställa efterlevnaden av denna förordning i linje med den senaste utvecklingen, för att främja innovation samt konkurrenskraft och tillväxt på den inre marknaden. Överenstämmelse med harmoniserade standarder enligt definitionen i artikel 2.1 c i Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([41]), som normalt förväntas återspegla den senaste utvecklingen, bör vara ett sätt för leverantörer att visa att de uppfyller kraven i den här förordningen. En balanserad representation av intressen som involverar alla berörda parter i utarbetandet av standarder, särskilt små och medelstora företag, konsumentorganisationer samt miljö- och arbetstagarintressenter i enlighet med artiklarna 5 och 6 i förordning (EU) nr 1025/2012, bör därför uppmuntras. För att underlätta efterlevnaden bör begäranden om standardisering utfärdas av kommissionen utan oskäligt dröjsmål. När kommissionen utarbetar en begäran om standardisering bör den samråda med det rådgivande forumet och styrelsen för att samla in relevant expertis. I avsaknad av relevanta hänvisningar till harmoniserade standarder bör kommissionen dock, genom genomförandeakter och efter samråd med det rådgivande forumet, kunna fastställa gemensamma specifikationer för vissa krav enligt den här förordningen. Den gemensamma specifikationen bör vara en exceptionell reservlösning för att underlätta leverantörens skyldighet att uppfylla kraven i den här förordningen, när begäran om standardisering inte har godtagits av någon av de europeiska standardiseringsorganisationerna eller när de relevanta harmoniserade standarderna inte i tillräcklig utsträckning behandlar frågor om grundläggande rättigheter, eller när de harmoniserade standarderna inte överensstämmer med begäran, eller när antagandet av en lämplig harmoniserad

([41]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

standard försenas. Om en sådan försening av antagandet av en harmoniserad standard beror på den tekniska komplexiteten hos den standarden bör kommissionen beakta detta innan den överväger att fastställa gemensamma specifikationer. Vid utarbetandet av gemensamma specifikationer uppmanas kommissionen att samarbeta med internationella partner och internationella standardiseringsorgan.

(122) Utan att det påverkar användningen av harmoniserade standarder och gemensamma specifikationer är det lämpligt att leverantörer av ett AI-system med hög risk som har tränats och testats på data som återspeglar den specifika geografiska, beteendemässiga, kontextuella eller funktionella situation där AI-systemet är avsett att användas, förutsätts följa den relevanta åtgärd som föreskrivs enligt kravet på dataförvaltning i denna förordning. Utan att det påverkar de krav avseende robusthet och riktighet som fastställs i denna förordning, i enlighet med artikel 54.3 i förordning (EU) 2019/881, bör AI-system med hög risk som har certifierats eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en cybersäkerhetsordning i enlig den förordningen och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning* förutsättas uppfylla cybersäkerhetskravet i den här förordningen i den mån cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar därav omfattar cybersäkerhetskravet i den här förordningen. Detta påverkar inte cybersäkerhetsordningens frivilliga karaktär.

(123) För att säkerställa en hög nivå av tillförlitlighet för AI-system med hög risk bör sådana system vara föremål för en bedömning av överensstämmelse innan de släpps ut på marknaden eller tas i bruk.

(124) För att minimera bördan för operatörer och förhindra allt eventuellt dubbelarbete är det, för AI-system med hög risk som är relaterade till produkter som omfattas av befintlig unionsharmoniseringslagstiftning som bygger på den nya lagstiftningsramen, lämpligt att bedöma dessa AI-systems uppfyllande av kraven i denna förordning inom ramen för den bedömning av överensstämmelse som redan föreskrivs i den lagstiftningen. Tillämpligheten för kraven i denna förordning bör därmed inte påverka den specifika logiken, metoden eller allmänna strukturen för bedömningen av överensstämmelse enligt relevant unionsharmoniseringslagstiftning.

(125) Med tanke på komplexiteten hos AI-system med hög risk och de risker som är förknippade med dem är det viktigt att utveckla ett lämpligt förfarande för bedömning av överensstämmelse för AI-system med hög risk som involverar anmälda organ, så kallad tredjepartsbedömning av överensstämmelse. Mot bakgrund av den nuvarande erfarenheten hos professionella certifieringsorgan före utsläppandet på marknaden på området produktsäkerhet och de olika typer av risker som är involverade är det dock lämpligt att, åtminstone i den inledande fasen av denna förordnings tillämpning, begränsa tillämpningsområdet för tredjepartsbedömning av överensstämmelse när det gäller andra AI-system med hög risk än dem som är relaterade till produkter. Därför bör bedömningen av överensstämmelse för sådana system som en allmän regel utföras av leverantören på eget ansvar, med det enda undantaget för AI-system som är avsedda att användas för biometri.

(126) För genomförandet av tredjepartsbedömningar av överensstämmelse när så krävs, bör anmälda organ anmälas enligt denna förordning av de nationella behöriga myndigheterna, under förutsättning att de uppfyller ett antal krav, i synnerhet vad gäller oberoende, kompetens, avsaknad av intressekonflikter samt lämpliga krav för cybersäkerhet. De nationella behöriga myndigheterna bör skicka anmälan av dessa organ till kommissionen och de övriga medlemsstaterna med hjälp av det elektroniska anmälningsverktyg som utvecklats och förvaltas av kommissionen enligt artikel R23 i bilaga I till beslut nr 768/2008/EG.

(127) I linje med unionens åtaganden enligt Världshandelsorganisationens avtal om tekniska handelshinder är det lämpligt att underlätta ömsesidigt erkännande av resultat av bedömningar av överensstämmelse som tagits fram av behöriga organ för bedömning av överensstämmelse som är oberoende av det territorium där de är etablerade, förutsatt att dessa organ för bedömning av överensstämmelse som inrättats enligt ett tredjelands rätt uppfyller de tillämpliga kraven i denna förordning och att unionen har ingått ett avtal om detta. I detta sammanhang bör kommissionen aktivt undersöka möjliga internationella instrument för detta ändamål och särskilt sträva efter att ingå avtal om ömsesidigt erkännande med tredjeländer.

(128) Vid varje ändring som kan påverka efterlevnaden av denna förordning för ett AI-system med hög risk (t.ex. en ändring av operativsystem eller programvaruarkitektur) eller vid ändring av systemets avsedda ändamål är det lämpligt att AI-systemet, i linje med det vedertagna begreppet väsentlig ändring som avser produkter som regleras genom unionens harmoniseringslagstiftning, anses vara ett nytt AI-system som bör genomgå en ny bedömning av överensstämmelse. Ändringar av algoritmen och prestandan i AI-system som fortsätter sin *inlärning* efter att de släppts ut på marknaden eller tagits i bruk, dvs. automatiskt anpassar hur funktionerna utförs, bör dock inte utgöra väsentliga ändringar, förutsatt att dessa ändringar på förhand har fastställts av leverantören och bedömts vid tidpunkten för bedömning av överensstämmelse.

(129) AI-system med hög risk bör vara försedda med en CE-märkning som visar att de överensstämmer med denna förordning, så att de kan omfattas av den fria rörligheten på den inre marknaden. För AI-system med hög risk som är inbyggda i en produkt bör en fysisk CE-märkning anbringas, och den kan kompletteras med en digital CE-märkning. För AI-system med hög risk som endast tillhandahålls digitalt bör en digital CE-märkning användas. Medlemsstaterna bör inte sätta upp omotiverade hinder för utsläppandet på marknaden eller ibruktagandet av AI-system med hög risk som uppfyller kraven i denna förordning och är försedda med en CE-märkning.

(130) Under vissa omständigheter kan en snabb tillgång till innovativ teknik vara avgörande för människors hälsa och säkerhet, miljöskyddet och klimatförändringarna och för samhället som helhet. Det är därför lämpligt att marknadskontrollmyndigheterna, när det föreligger exceptionella skäl som rör allmän säkerhet eller skydd av fysiska personers liv och hälsa, miljöskydd och skydd av viktiga industriella och infrastrukturella tillgångar, har möjlighet att tillåta utsläppandet på marknaden eller ibruktagandet av AI-system som inte har genomgått en bedömning av överensstämmelse. I vederbörligen motiverade situationer enligt denna förordning kan brottsbekämpande myndigheter eller civilskyddsmyndigheter ta ett specifikt AI-system med hög risk i bruk utan marknadskontrollmyndighetens tillstånd, förutsatt att ett sådant tillstånd begärs under eller efter användningen utan oskäligt dröjsmål.

(131) För att underlätta kommissionens och medlemsstaternas arbete på AI-området och öka transparensen gentemot allmänheten, bör leverantörer av andra AI-system med hög risk än dem som är relaterade till produkter som faller inom tillämpningsområdet för relevant befintlig unionsharmoniseringslagstiftning, samt leverantörer som anser att ett AI-system som förtecknas under användningsfall med hög risk i en bilaga till denna förordning inte är ett AI-system med hög risk på grundval av ett undantag, åläggas att registrera sig själva och information om sina AI-system i en EU-databas som ska upprättas och förvaltas av kommissionen. Innan ett AI-system som förtecknas under användningsfall med hög risk i en bilaga till denna förordning används bör tillhandahållare av AI-system med hög risk som är offentliga myndigheter, byråer eller organ registrera sig i en sådan databas och välja det system som de avser att använda. Andra tillhandahållare bör ha rätt att göra detta frivilligt. Denna del av EU-databasen bör vara kostnadsfritt åtkomlig för allmänheten, och det bör vara lätt att navigera i informationen, som bör vara begriplig och maskinläsbar. EU-databasen bör också vara användarvänlig, till exempel genom att sökfunktioner, inbegripet genom nyckelord, tillhandahålls som gör det möjligt för allmänheten att hitta relevant information som ska lämnas in vid registreringen av AI-system med hög risk och om det användningsfall av AI-system med hög risk som anges i en bilaga till denna förordning som AI-systemen med hög risk motsvarar. Alla väsentliga ändringar av AI-system med hög risk bör också registreras i EU-databasen. För AI-system med hög risk på området brottsbekämpning, migration, asyl och gränskontrollförvaltning bör registreringsskyldigheterna uppfyllas i en säker icke-offentlig del av EU-databasen. Åtkomsten till den säkra icke-offentliga delen bör strikt begränsas till kommissionen och till marknadskontrollmyndigheterna när det gäller deras nationella del av databasen. AI-system med hög risk på området kritisk infrastruktur bör endast registreras på nationell nivå. Kommissionen bör vara personuppgiftsansvarig för EU-databasen i enlighet med förordning (EU) 2018/1725. För att säkerställa att EU-databasen är fullt funktionell när den börjar utnyttjas, bör förfarandet för inrättandet av databasen innefatta funktionsspecifikationer som utvecklas av kommissionen samt en oberoende revisionsrapport. Kommissionen bör ta hänsyn till cybersäkerhetsrisker när den utför sina uppgifter som personuppgiftsansvarig i EU-databasen. För att allmänheten ska få så stor tillgång till och kunna använda EU-databasen så mycket som möjligt bör EU-databasen, och den information som tillgängliggörs genom den, uppfylla kraven i direktiv (EU) 2019/882.

(132) Vissa AI-system avsedda för att interagera med fysiska personer eller generera innehåll kan utgöra särskilda risker för identitetsmissbruk eller vilseledning oavsett om de kategoriseras som AI-system med hög risk eller inte. Under vissa omständigheter bör därför användningen av dessa system omfattas av särskilda transparensskyldigheter utan att det påverkar kraven eller skyldigheterna för AI-system med hög risk och omfattas av riktade undantag för att ta hänsyn till brottsbekämpningens särskilda behov. I synnerhet bör fysiska personer underrättas om att de interagerar med ett AI-system, såvida detta inte är uppenbart för en fysisk person som är normalt informerad och skäligen uppmärksam och medveten med beaktande av omständigheterna kring och sammanhanget för användningen. Vid genomförandet av den skyldigheten bör det som kännetecknar fysiska personer som tillhör sårbara grupper på grund av ålder eller funktionsnedsättning beaktas i den mån AI-systemet även är avsett att interagera med dessa grupper. Dessutom bör fysiska personer underrättas när de utsätts för AI-system som genom att behandla deras biometriska uppgifter kan identifiera eller härleda dessa personers känslor eller avsikter eller hänföra dem till särskilda kategorier. Sådana särskilda kategorier kan avse aspekter som kön, ålder, hårfärg, ögonfärg, tatueringar, personlighetsdrag, etniskt ursprung, personliga preferenser och intressen. Sådan information och sådana underrättelser bör tillhandahållas i format som är tillgängliga för personer med funktionsnedsättning.

(133) En rad olika AI-system kan generera stora mängder syntetiskt innehåll som blir allt svårare för människor att skilja från mänskligt genererat och autentiskt innehåll. Dessa systems breda tillgänglighet och ökande kapacitet har en betydande inverkan på integriteten och förtroendet för informationsekosystemet, vilket medför nya risker för felaktig information och manipulering i stor skala, bedrägeri, identitetsmissbruk och vilseledande av konsumenter. Mot bakgrund av denna inverkan, den snabba tekniska takten och behovet av nya metoder och tekniker för att spåra ursprunget till information är det lämpligt att kräva att leverantörer av dessa system integrerar tekniska lösningar som möjliggör märkning i maskinläsbart format och upptäckt av att utdata har genererats eller manipulerats av ett AI-system och inte av en människa. Sådana tekniker och metoder bör vara tillräckligt tillförlitliga, driftskompatibla, effektiva och robusta i den mån det är tekniskt möjligt, med beaktande av tillgänglig teknik eller en kombination av sådana tekniker, såsom vattenmärken, metadataidentifiering, krypteringsmetoder för att bevisa innehållets härkomst och äkthet, loggningsmetoder, fingeravtryck eller annan teknik, beroende på vad som är lämpligt. När denna skyldighet fullgörs bör leverantörer även beakta särdragen och begränsningarna hos olika typer av innehåll, och den relevanta tekniska utvecklingen och marknadsutvecklingen på området, såsom detta återspeglas i den allmänt erkända senaste utvecklingen. Sådana tekniker och metoder kan genomföras på AI-systemnivå eller AI-modellnivå, inbegripet i fråga om AI-modeller för allmänna ändamål som genererar innehåll, för att därigenom underlätta fullgörandet av denna skyldighet av AI-systemets leverantör i efterföljande led. För att förbli proportionell är det lämpligt att föreskriva att denna märkningsskyldighet inte bör omfatta AI-system som i första hand utför en hjälpfunktion för vanlig redigering eller AI-system som inte väsentligt ändrar de indata som tillhandahålls av tillhandahållaren eller deras semantik.

(134) Med hänsyn till de tekniska lösningar som används av leverantörerna av AI-systemet bör tillhandahållare som använder ett AI-system för att generera eller manipulera bilder eller ljud- eller videoinnehåll som på ett märkbart sätt liknar befintliga personer, föremål, platser, enheter eller händelser, och som för en person felaktigt kan framstå som autentiska eller sanningsenliga (*deepfake*), även på ett tydligt och urskiljbart sätt upplysa om att innehållet har skapats artificiellt eller manipulerats genom märkning av de utdata som producerats med AI i enlighet med det och upplysa om dess artificiella ursprung. Fullgörandet av denna transparensskyldighet bör inte tolkas som att användningen av AI-systemet eller dess utdata hindrar rätten till yttrandefrihet och konstens och vetenskapens frihet, som garanteras i stadgan, särskilt när innehållet ingår i ett uppenbart kreativt, satiriskt, konstnärligt, skönlitterärt eller liknande verk eller program, med förbehåll för lämpliga garantier för tredje parters rättigheter och friheter. I dessa fall är den transparensskyldighet för deepfake som fastställs i denna förordning begränsad till en upplysning om förekomsten av sådant genererat eller manipulerat innehåll på ett lämpligt sätt som inte hindrar visningen eller åtnjutandet av verket, inbegripet dess normala utnyttjande och användning, samtidigt som verkets nytta och kvalitet upprätthålls. Det är också lämpligt att föreskriva en liknande upplysningsskyldighet när det gäller AI-genererad eller AI-manipulerad text i den mån den offentliggörs i syfte att informera allmänheten om frågor av allmänt intresse, såvida inte det AI-genererade innehållet har genomgått en process för mänsklig granskning eller redaktionell kontroll och en fysisk eller juridisk person har redaktionellt ansvar för offentliggörandet av innehållet.

(135) Utan att det påverkar transparensskyldigheternas obligatoriska karaktär och fullständiga tillämplighet kan kommissionen också uppmuntra och underlätta utarbetandet av förfarandekoder på unionsnivå för att underlätta ett effektivt genomförande av skyldigheterna avseende upptäckt och märkning av artificiellt genererat eller manipulerat innehåll, bland annat för att stödja praktiska arrangemang för att, när så är lämpligt, göra mekanismerna för upptäckt tillgängliga och underlätta samarbetet med andra aktörer längs värdekedjan, sprida innehåll eller kontrollera dess autenticitet och ursprung för att göra det möjligt för allmänheten att på ett effektivt sätt urskilja AI-genererat innehåll.

(136) Dessutom är de skyldigheter som åläggs leverantörer och tillhandahållare av vissa AI-system i denna förordning för att det ska vara möjligt att upptäcka och visa att utdata från dessa system är artificiellt genererade eller manipulerade vara särskilt relevanta för att underlätta ett effektivt genomförande av förordning (EU) 2022/2065. Detta gäller särskilt i fråga om skyldigheterna för leverantörer av mycket stora onlineplattformar eller mycket stora onlinesökmotorer att identifiera och begränsa systemrisker som kan uppstå till följd av spridning av innehåll som genererats eller manipulerats artificiellt, särskilt risken för faktiska eller förutsebara negativa effekter på demokratiska processer, samhällsdebatten och valprocesser, inbegripet genom desinformation. Kravet på märkning av innehåll som genereras av AI-system enligt den här förordningen påverkar inte skyldigheten i artikel 16.6 i förordning (EU) 2022/2065 för leverantörer av värdtjänster att behandla anmälningar om olagligt innehåll som mottagits enligt artikel 16.1 i den förordningen och bör inte påverka bedömningen och beslutet om det specifika innehållets olaglighet. Denna bedömning bör göras endast med hänsyn till de regler som reglerar innehållets lagenlighet.

(137) Fullgörandet av transparensskyldigheterna för AI-system som omfattas av denna förordning bör inte tolkas som att användningen av AI-systemet eller dess utdata är laglig enligt denna förordning eller annan unionsrätt och nationell rätt i medlemsstaterna och bör inte påverka andra transparensskyldigheter för tillhandahållare av AI-system som fastställs i unionsrätten eller nationell rätt.

(138) AI är en teknikfamilj i snabb utveckling som kräver tillsyn och ett säkert och kontrollerat område för experiment, med säkerställande av ansvarsfull innovation och integrering av ändamålsenliga skydds- och riskbegränsningsåtgärder. För att säkerställa en rättslig ram som främjar innovation och är framtidssäkrad och resilient mot störningar, bör medlemsstaterna säkerställa att deras nationella behöriga myndigheter inrättar åtminstone en regulatorisk sandlåda för AI på nationell nivå, för att underlätta utveckling och testning av innovativa AI-system under strikt tillsyn innan dessa system släpps ut på marknaden eller på annat sätt tas i bruk. Medlemsstaterna kan också fullgöra denna skyldighet genom att delta i redan befintliga regulatoriska sandlådor eller gemensamt inrätta en sandlåda med en eller flera medlemsstaters behöriga myndigheter, i den mån detta deltagande ger de deltagande medlemsstaterna likvärdig nationell täckning. Regulatoriska sandlådor för AI kan inrättas i fysisk eller digital form eller i hybridform och kan rymma både fysiska och digitala produkter. Inrättandet av myndigheter bör också säkerställa att de regulatoriska sandlådorna för AI har tillräckliga resurser för sin funktion, inbegripet ekonomiska och mänskliga resurser.

(139) Målen med dessa regulatoriska sandlådor för AI bör vara att främja AI-innovation genom inrättande av en kontrollerad experiment- och testmiljö vid utveckling och under fasen före utsläppandet på marknaden, med sikte på att säkerställa att de innovativa AI-systemen är förenliga med denna förordning och annan relevant unionsrätt och nationell rätt. Dessutom bör regulatoriska sandlådor för AI syfta till att öka rättssäkerheten för innovatörer och förbättra de behöriga myndigheternas tillsyn och förståelse av möjligheterna, de nya riskerna och effekterna av AI-användning, att underlätta regulatoriskt lärande för myndigheter och företag, även med tanke på framtida anpassningar av den rättsliga ramen, att stödja samarbete och utbyte av bästa praxis med de myndigheter som deltar i regulatoriska sandlådan för AI och att påskynda tillträdet till marknader, bland annat genom att undanröja hinder för små och medelstora företag, inbegripet uppstartsföretag. Regulatoriska sandlådor för AI bör vara tillgängliga i bred omfattning i hela unionen, och särskild uppmärksamhet bör ägnas åt deras tillgänglighet för små och medelstora företag, inbegripet uppstartsföretag. Deltagandet i den regulatoriska sandlådan för AI bör inriktas på problem som skapar rättsosäkerhet för leverantörer och potentiella leverantörer när de ska vara innovativa, experimentera med AI i unionen och bidra till evidensbaserat regulatoriskt lärande. Tillsynen av AI-systemen i den regulatoriska sandlådan för AI bör därför omfatta deras utveckling, träning, testning och validering innan systemen släpps ut på marknaden eller tas i bruk, samt begreppet och förekomsten av väsentlig ändring som kan kräva ett nytt förfarande för bedömning av överensstämmelse. Alla betydande risker som upptäcks under utvecklingen och testningen av sådana AI-system bör leda till omedelbar riskbegränsning och, om detta inte är möjligt, leda till att utvecklings- och testningsprocessen tillfälligt avbryts. När så är lämpligt bör nationella behöriga myndigheter som inrättar regulatoriska sandlådor för AI samarbeta med andra relevanta myndigheter, inbegripet dem som övervakar skyddet av grundläggande rättigheter, och de skulle kunna tillåta deltagande av andra aktörer inom AI-ekosystemet, såsom nationella eller europeiska standardiseringsorganisationer, anmälda organ, test- och experimentfaciliteter, forsknings- och experimentlaboratorier, europeiska digitala innovationsknutpunkter och relevanta organisationer för berörda parter och för det civila samhället. För att säkerställa ett enhetligt genomförande i hela unionen och stordriftsfördelar är det lämpligt att fastställa gemensamma regler för införandet av regulatoriska sandlådor för AI och en samarbetsram för de berörda myndigheter som deltar i tillsynen över sådana sandlådor. Regulatoriska sandlådor för AI som inrättas enligt denna förordning bör inte påverka annan rätt som tillåter inrättande av andra sandlådor som syftar till att säkerställa överensstämmelse med annan rätt än denna förordning. När så är lämpligt bör relevanta behöriga myndigheter som ansvarar för dessa andra regulatoriska sandlådor överväga fördelarna med att använda dessa sandlådor även i syfte att säkerställa AI-systemens överensstämmelse med denna förordning. Efter överenskommelse mellan de nationella behöriga myndigheterna och deltagarna i den regulatoriska sandlådan för AI kan testning under verkliga förhållanden också genomföras och övervakas inom ramen för den regulatoriska sandlådan för AI.

(140) Denna förordning bör erbjuda den rättsliga grunden för att leverantörer och potentiella leverantörer i den regulatoriska sandlådan för AI använder personuppgifter som samlats in för andra ändamål för att utveckla vissa AI-system i allmänhetens intresse inom regulatoriska sandlådor för AI, endast på de angivna villkoren, i enlighet med artiklarna 6.4 och 9.2 g i förordning (EU) 2016/679 och artiklarna 5, 6 och 10 i förordning (EU) 2018/1725, och utan att det påverkar tillämpningen av artiklarna 4.2 och 10 i direktiv (EU) 2016/680. Alla andra skyldigheter för personuppgiftsansvariga och de registrerades rättigheter enligt förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680 förblir tillämpliga. I synnerhet bör den här förordningen inte utgöra en rättslig grund i den mening som avses i artikel 22.2 b i förordning (EU) 2016/679 och artikel 24.2 b i förordning (EU) 2018/1725.

Leverantörer och potentiella leverantörer i den regulatoriska sandlådan för AI bör säkerställa ändamålsenliga skyddsåtgärder och samarbeta med de behöriga myndigheterna, vilket omfattar att följa deras vägledning och agera snabbt och i god tro för att på lämpligt sätt begränsa eventuella identifierade väsentliga risker för säkerhet, hälsa och grundläggande rättigheter som kan uppstå i samband med utvecklings-, testnings- och experimentverksamhet i den sandlådan.

(141) För att påskynda utvecklingen och utsläppandet på marknaden av de AI-system med hög risk som förtecknas i en bilaga till denna förordning är det viktigt att leverantörer eller potentiella leverantörer av sådana system också kan dra nytta av en särskild ordning för testning av dessa system under verkliga förhållanden, utan att delta i en regulatorisk sandlåda för AI. I sådana fall bör det, med beaktande av de möjliga konsekvenserna av sådan testning för enskilda personer, dock säkerställas att lämpliga och tillräckliga garantier och villkor införs genom denna förordning för leverantörer eller potentiella leverantörer. Sådana garantier bör bland annat inbegripa en begäran om informerat samtycke från fysiska personer att delta i testning under verkliga förhållanden, med undantag för brottsbekämpning om inhämtandet av informerat samtycke skulle hindra AI-systemet från att testas. Försökspersonernas samtycke till att delta i sådan testning enligt denna förordning skiljer sig från och påverkar inte de registrerades samtycke till behandling av deras personuppgifter enligt relevant dataskyddslagstiftning. Det är också viktigt att minimera riskerna och göra det möjligt för behöriga myndigheter att utöva tillsyn, och därför kräva att potentiella leverantörer har en plan för testning under verkliga förhållanden som lämnas in till den behöriga marknadskontrollmyndigheten och att de registrerar testningen i särskilda delar av EU-databasen med vissa begränsade undantag, samt att fastställa begränsningar för den period under vilken testningen kan utföras och kräva ytterligare skyddsåtgärder för personer som tillhör vissa sårbara grupper, liksom ett skriftligt avtal som definierar rollerna och ansvarsområdena för potentiella leverantörer och tillhandahållare samt formerna för en effektiv tillsyn av personal med lämplig kompetens som deltar i testningen under verkliga förhållanden. Det är dessutom lämpligt att överväga ytterligare skyddsåtgärder för att säkerställa att AI-systemets förutsägelser, rekommendationer eller beslut effektivt kan upphävas och ignoreras och att personuppgifter skyddas och raderas när försökspersonerna har dragit tillbaka sitt samtycke till att delta i testningen, utan att det påverkar deras rättigheter som registrerade enligt unionens dataskyddslagstiftning. När det gäller överföring av uppgifter är det också lämpligt att förutse att uppgifter som samlats in och behandlats för testning under verkliga förhållanden bör överföras till tredjeländer endast om lämpliga och tillämpliga skyddsåtgärder enligt unionsrätten vidtas, särskilt i enlighet med grunderna för överföring av personuppgifter enligt unionsrätten om dataskydd, medan det i fråga om icke-personuppgifter införs lämpliga skyddsåtgärder i enlighet med unionsrätten, såsom Europaparlamentets och rådets förordningar (EU) 2022/868 ([42]) och (EU) 2023/2854 ([43]).

(142) För att säkerställa att AI leder till socialt och miljömässigt fördelaktiga utfall uppmuntras medlemsstaterna att stödja och främja forskning och utveckling av AI-lösningar till stöd för socialt och miljömässigt fördelaktiga utfall, såsom AI-baserade lösningar för att öka tillgängligheten för personer med funktionsnedsättning, ta itu med socioekonomiska ojämlikheter eller uppnå miljömål, genom att anslå tillräckliga resurser, inbegripet offentlig finansiering och unionsfinansiering, och, när så är lämpligt och förutsatt att behörighets- och urvalskriterierna är uppfyllda, genom att särskilt beakta projekt som eftersträvar sådana mål. Projekten bör grunda sig på principen om interdisciplinärt samarbete mellan AI-utvecklare, experter på ojämlikhet och icke-diskriminering, tillgänglighet, konsument- och miljörättigheter samt digitala rättigheter, och akademiker.

(143) För att främja och skydda innovation är det viktigt att särskild hänsyn tas till intressena hos små och medelstora företag, inbegripet uppstartsföretag, som är leverantörer eller tillhandahållare av AI-system. För det ändamålet bör medlemsstaterna ta fram initiativ som riktar sig till dessa operatörer, bland annat vad gäller medvetandehöjande och information. Medlemsstaterna bör ge små och medelstora företag, inbegripet uppstartsföretag, som har ett säte eller en filial i unionen prioriterad tillgång till de regulatoriska sandlådorna för AI, förutsatt att de uppfyller behörighetskraven och urvalskriterierna och utan att andra leverantörer och potentiella leverantörer hindras från att få tillgång till sandlådorna, förutsatt att samma krav och kriterier är uppfyllda. Medlemsstaterna bör använda befintliga kanaler och, när så är lämpligt, inrätta nya särskilda kanaler för kommunikation med små och medelstora företag, inbegripet uppstartsföretag, tillhandahållare, andra innovatörer och, i förekommande fall, lokala offentliga myndigheter i syfte att stödja små och medelstora företag under deras utveckling genom att ge vägledning och svara på frågor om genomförandet av denna förordning. Där så är lämpligt bör dessa kanaler samarbeta för att skapa synergier och säkerställa homogenitet i sin vägledning till små och medelstora företag, inbegripet uppstartsföretag, och tillhandahållare. Medlemsstaterna bör dessutom underlätta små och medelstora företags och andra berörda parters deltagande i processerna för standardiseringsutveckling. De särskilda intressena och behoven hos

([42]) Europaparlamentets och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten) (EUT L 152, 3.6.2022, s. 1).

([43]) Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) (EUT L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

leverantörer som är små och medelstora företag, inbegripet uppstartsföretag, bör också beaktas när anmälda organ fastställer avgifterna för bedömning av överensstämmelse. Kommissionen bör regelbundet bedöma kostnaderna för certifiering och efterlevnad för små och medelstora företag, inbegripet uppstartsföretag, genom transparenta samråd, och samarbeta med medlemsstaterna för att sänka sådana kostnader. Till exempel kan kostnaderna för översättning av obligatorisk dokumentation och kommunikation med myndigheter utgöra betydande kostnader för leverantörer och andra operatörer, i synnerhet mer småskaliga sådana. Medlemsstaterna bör eventuellt säkerställa att ett av de språk som fastställs och godtas av dem för relevant dokumentation från leverantörer och för kommunikation med operatörer är ett språk som i huvudsak förstås av största möjliga antal tillhandahållare i gränsöverskridande situationer. För att tillgodose de särskilda behoven hos små och medelstora företag, inbegripet uppstartsföretag, bör kommissionen på styrelsens begäran tillhandahålla standardiserade mallar för de områden som omfattas av denna förordning. Kommissionen bör dessutom komplettera medlemsstaternas insatser genom att tillhandahålla en enda informationsplattform med information om denna förordning som är lätt att använda för alla leverantörer och tillhandahållare, genom att anordna lämpliga kommunikationskampanjer i syfte att öka medvetenheten om de skyldigheter som följer av denna förordning och genom att utvärdera och främja konvergens av bästa praxis i förfaranden för offentlig upphandling när det gäller AI-system. Medelstora företag som fram till nyligen betraktades som små företag i den mening som avses i bilagan till kommissionens rekommendation 2003/361/EG ([44]) bör ha tillgång till dessa stödåtgärder, eftersom dessa nya medelstora företag ibland saknar de rättsliga resurser och den utbildning som krävs för att säkerställa en korrekt förståelse och efterlevnad av denna förordning.

(144) För att främja och skydda innovation bör plattformen för efterfrågestyrd AI samt alla relevanta unionsfinansieringsprogram och unionsprojekt, såsom programmet för ett digitalt Europa och Horisont Europa, som genomförs av kommissionen och medlemsstaterna på unionsnivå eller nationell nivå i förekommande fall bidra till att målen i denna förordning uppnås.

(145) För att minimera risker för genomförandet som följer av bristande kunskap och expertis på marknaden, och för att främja leverantörernas, särskilt små och medelstora företags, inbegripet uppstartsföretags, och de anmälda organens uppfyllande av sina skyldigheter enligt denna förordning, bör plattformen för efterfrågestyrd AI, de europeiska digitala innovationsknutpunkterna och de test- och experimentfaciliteter som inrättas av kommissionen och medlemsstaterna på unionsnivå eller nationell nivå bidra till genomförandet av denna förordning. Inom sina respektive uppdrag och kompetensområden kan plattformen för efterfrågestyrd AI, de europeiska digitala innovationsknutpunkterna och test- och experimentfaciliteterna i synnerhet tillhandahålla tekniskt och vetenskapligt stöd till leverantörer och anmälda organ.

(146) Med tanke på vissa operatörers mycket begränsade storlek och för att säkerställa proportionalitet när det gäller innovationskostnader, bör dessutom mikroföretag tillåtas att fullgöra en av de mest kostsamma skyldigheterna, nämligen inrättandet av ett kvalitetsstyrningssystem, på ett förenklat sätt som skulle minska den administrativa bördan och kostnaderna för dessa företag utan att skyddsnivån och behovet av efterlevnad av kraven för AI-system med hög risk påverkas. Kommissionen bör utarbeta riktlinjer för att specificera de delar av kvalitetsstyrningssystemet som mikroföretag bör fullgöra på detta förenklade sätt.

(147) Det är lämpligt att kommissionen i möjligaste mån underlättar tillgången till test- och experimentfaciliteter för organ, grupper eller laboratorier som inrättats eller ackrediterats enligt relevant unionsharmoniseringslagstiftning och som utför uppgifter inom ramen för bedömning av överensstämmelse för produkter eller utrustning som omfattas av den unionsharmoniseringslagstiftningen. Detta gäller i synnerhet för expertpaneler, expertlaboratorier och referenslaboratorier på området medicintekniska produkter enligt förordningarna (EU) 2017/745 och (EU) 2017/746.

(148) Denna förordning bör fastställa en styrningsram som gör det möjligt såväl att samordna och stödja tillämpningen av denna förordning på nationell nivå som att bygga upp kapacitet på unionsnivå och involvera berörda parter på AI-området. Ett effektivt genomförande och en effektiv kontroll av efterlevnaden av denna förordning kräver en styrningsram som gör det möjligt att samordna och bygga upp central expertis på unionsnivå. AI-byrån inrättades genom ett kommissionsbeslut ([45]) och har som uppdrag att utveckla unionens expertis och kapacitet på AI-området och att bidra till genomförandet av unionsrätten om AI. Medlemsstaterna bör underlätta AI-byråns uppgifter med målet att stödja utvecklingen av unionens expertis och kapacitet på unionsnivå och stärka den digitala inre marknadens funktion. Det bör dessutom inrättas en styrelse bestående av företrädare för medlemsstaterna, en vetenskaplig panel för att involvera forskarsamhället och ett rådgivande forum för att genom synpunkter från berörda parter bidra till genomförandet av denna förordning, på unionsnivå och nationell nivå. Utvecklingen av

([44]) Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).
([45]) Kommissionens beslut av den 24 januari 2024 om inrättande av Europeiska byrån för artificiell intelligens C(2024) 390.

unionens expertis och kapacitet bör också inbegripa användning av befintliga resurser och befintlig expertis, särskilt genom synergier med strukturer som byggts upp i samband med efterlevnaden av annan rätt på unionsnivå och synergier med därmed sammanhängande initiativ på unionsnivå, såsom det gemensamma företaget EuroHPC och test- och experimentfaciliteter för AI inom ramen för programmet för ett digitalt Europa.

(149) För att främja ett smidigt, effektivt och harmoniserat genomförande av denna förordning bör en styrelse inrättas. Styrelsen bör återspegla AI-ekosystemets olika intressen och bestå av företrädare för medlemsstaterna. Styrelsen bör ansvara för ett antal rådgivande uppgifter, däribland att utfärda yttranden, rekommendationer, råd eller bidra till vägledning om frågor som rör genomförandet av denna förordning, inbegripet när det gäller frågor som rör kontroll av efterlevnad, tekniska specifikationer eller befintliga standarder avseende kraven i denna förordning och råd till kommissionen, medlemsstaterna och deras nationella behöriga myndigheter om specifika frågor som rör AI. För att ge medlemsstaterna viss flexibilitet när de utser sina företrädare i styrelsen kan sådana företrädare utgöras av alla personer som tillhör offentliga enheter och som bör ha relevant kompetens och relevanta befogenheter för att underlätta samordningen på nationell nivå och bidra till att styrelsens uppgifter fullgörs. Styrelsen bör inrätta två ständiga undergrupper för att tillhandahålla en plattform för samarbete och utbyte mellan marknadskontrollmyndigheter och anmälande myndigheter i frågor som rör marknadskontroll respektive anmälda organ. Den ständiga arbetsgruppen för marknadskontroll bör fungera som grupp för administrativt samarbete (Adco-grupp) för denna förordning i den mening som avses i artikel 30 i förordning (EU) 2019/1020. I enlighet med artikel 33 i den förordningen bör kommissionen stödja verksamheten i den ständiga arbetsgruppen för marknadskontroll genom att genomföra marknadsutvärderingar eller marknadsstudier, särskilt i syfte att identifiera aspekter av den här förordningen som kräver särskild och brådskande samordning mellan marknadskontrollmyndigheter. Styrelsen får inrätta andra ständiga eller tillfälliga undergrupper när så är lämpligt i syfte att granska specifika frågor. Styrelsen bör också, när så är lämpligt, samarbeta med relevanta unionsorgan, unionsexpertgrupper och unionsnätverk som är verksamma inom ramen för relevant unionsrätt, särskilt de som är verksamma inom ramen för relevant unionsrätt om data, digitala produkter och tjänster.

(150) För att säkerställa berörda parters deltagande i genomförandet och tillämpningen av denna förordning bör ett rådgivande forum inrättas för att ge råd till och tillhandahålla teknisk expertis till styrelsen och kommissionen. För att säkerställa en varierad och balanserad representation av berörda parter i fråga om kommersiella och icke-kommersiella intressen samt, inom kategorin kommersiella intressen, med avseende på små och medelstora företag och andra företag, bör det rådgivande forumet bland annat omfatta industrin, uppstartsföretag, små och medelstora företag, den akademiska världen, det civila samhället, inbegripet arbetsmarknadens parter, samt Europeiska unionens byrå för grundläggande rättigheter, Enisa, Europeiska standardiseringskommittén (CEN), Europeiska kommittén för elektroteknisk standardisering (Cenelec) och Europeiska institutet för telekommunikationsstandarder (Etsi).

(151) För att stödja genomförandet och kontrollen av efterlevnaden av denna förordning, särskilt AI-byråns övervakningsverksamhet avseende AI-modeller för allmänna ändamål, bör en vetenskaplig panel av oberoende experter inrättas. De oberoende experter som ingår i den vetenskapliga panelen bör väljas ut på grundval av aktuell vetenskaplig eller teknisk expertis på AI-området och bör utföra sina uppgifter opartiskt och objektivt samt säkerställa att den information och de uppgifter som de erhåller vid utförandet av sina uppgifter och sin verksamhet behandlas konfidentiellt. För att göra det möjligt att stärka den nationella kapacitet som krävs för en effektiv kontroll av efterlevnaden av denna förordning bör medlemsstaterna kunna begära stöd för sin verksamhet avseende efterlevnadskontroll från poolen av experter i den vetenskapliga panelen.

(152) För att stödja en lämplig kontroll av efterlevnaden i fråga om AI-system och för att stärka medlemsstaternas kapacitet bör unionsstödstrukturer för testning av AI inrättas och göras tillgängliga för medlemsstaterna.

(153) Medlemsstaterna har en central roll i tillämpningen och kontrollen av efterlevnaden av denna förordning. I detta hänseende bör varje medlemsstat till nationella behöriga myndigheter utse minst en anmälande myndighet och minst en marknadskontrollmyndighet för att utöva tillsyn avseende tillämpningen och genomförandet av denna förordning. Medlemsstaterna kan besluta att utse valfri typ av offentlig enhet för att utföra de nationella behöriga myndigheternas uppgifter i den mening som avses i denna förordning, i enlighet med sina specifika nationella organisatoriska särdrag och behov. För att öka den organisatoriska effektiviteten från medlemsstaternas sida och inrätta en gemensam kontaktpunkt för kontakterna med allmänheten och andra motparter på medlemsstatsnivå och unionsnivå bör varje medlemsstat utse en marknadskontrollmyndighet som ska fungera som gemensam kontaktpunkt.

(154) De nationella behöriga myndigheterna bör utöva sina befogenheter på ett oberoende, objektivt och opartiskt sätt för att säkerställa principen om objektivitet i sin verksamhet och sina uppgifter och för att säkerställa tillämpningen och genomförandet av denna förordning. Personalen vid dessa myndigheter bör avhålla sig från varje handling som är oförenlig med deras uppdrag och bör omfattas av bestämmelserna om konfidentialitet enligt denna förordning.

(155) För att säkerställa att leverantörer av AI-system med hög risk kan beakta erfarenheterna från användning av AI-system med hög risk för att förbättra sina system och utformnings- och utvecklingsprocessen, eller kan vidta eventuella korrigerande åtgärder i rätt tid, bör alla leverantörer ha infört ett system för övervakning efter utsläppande på marknaden. I förekommande fall bör övervakningen efter utsläppande på marknaden omfatta en analys av interaktionen med andra AI-system, inbegripet andra enheter och programvara. Övervakningen efter utsläppande på marknaden bör inte omfatta känsliga operativa uppgifter om tillhandahållare som är brottsbekämpande myndigheter. Detta system är också viktigt för att säkerställa att eventuella risker som härrör från AI-system som fortsätter sin *inlärning* efter att de släppts ut på marknaden eller tagits i bruk kan hanteras på ett mer effektivt sätt och i rätt tid. I detta sammanhang bör leverantörer också åläggas att ha ett system för rapportering till de berörda myndigheterna av alla allvarliga incidenter som orsakas av användningen av deras AI-system, varmed avses en incident eller en funktionsstörning som leder till dödsfall eller allvarlig skada för hälsan, en allvarlig och oåterkallelig störning av förvaltningen och driften av kritisk infrastruktur, överträdelser av skyldigheter enligt unionsrätten avsedda att skydda grundläggande rättigheter eller allvarlig skada för egendom eller för miljön.

(156) För att säkerställa ändamålsenlig och effektiv kontroll av att de krav och skyldigheter som fastställs i denna förordning och som utgör en del av unionens harmoniseringslagstiftning efterlevs bör det system för marknadskontroll och överensstämmelse för produkter som inrättas genom förordning (EU) 2019/1020 gälla i sin helhet. Marknadskontrollmyndigheter som utsetts enligt den här förordningen bör ha alla de befogenheter som fastställs i den här förordningen och i förordning (EU) 2019/1020 vad gäller kontroll av efterlevnad och bör utöva sina befogenheter och utföra sina uppgifter oberoende, objektivt och opartiskt. Även om majoriteten av AI-systemen inte omfattas av särskilda krav och skyldigheter enligt den här förordningen kan marknadskontrollmyndigheterna vidta åtgärder med avseende på alla AI-system när de utgör en risk i enlighet med den här förordningen. På grund av den särskilda karaktären hos unionens institutioner, byråer och organ som omfattas av den här förordningen bör Europeiska datatillsynsmannen utses till behörig marknadskontrollmyndighet för dem. Detta bör inte påverka medlemsstaternas utseende av nationella behöriga myndigheter. Marknadskontrollen bör inte påverka förmågan hos de enheter som står under tillsyn att utföra sina uppgifter på ett oberoende sätt, när ett sådant oberoende krävs enligt unionsrätten.

(157) Denna förordning påverkar inte behörigheten, uppgifterna, befogenheterna och oberoendet för relevanta nationella offentliga myndigheter eller organ som övervakar tillämpningen av unionsrätten till skydd för grundläggande rättigheter, inbegripet jämställdhetsorgan och dataskyddsmyndigheter. När det är nödvändigt för dessa nationella offentliga myndigheters eller organs uppdrag bör de också ha tillgång till all dokumentation som skapas enligt denna förordning. Ett särskilt förfarande för skyddsåtgärder bör fastställas för att säkerställa adekvat och snabb kontroll av efterlevnaden gentemot AI-system som utgör en risk för hälsa, säkerhet och grundläggande rättigheter. Förfarandet för sådana AI-system som utgör en risk bör tillämpas på AI-system med hög risk som utgör en risk, på förbjudna system som har släppts ut på marknaden, tagits i bruk eller använts i strid med de bestämmelser om förbjudna användningsområden som fastställs i denna förordning och på AI-system som har gjorts tillgängliga i strid med de transparenskrav som fastställs i denna förordning och som utgör en risk.

(158) Unionsrätten om finansiella tjänster omfattar regler och krav för interna styrelseformer och riskhantering som är tillämpliga på reglerade finansinstitut i samband med tillhandahållandet av dessa tjänster, även när de använder AI-system. För att säkerställa en enhetlig tillämpning och kontroll av efterlevnaden av skyldigheterna enligt denna förordning och relevanta regler och krav i unionsrättsakter om finansiella tjänster, bör de myndigheter som är behöriga för tillsynen och kontrollen av efterlevnaden av dessa rättsakter, i synnerhet behöriga myndigheter enligt definitionen i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([46]) och Europaparlamentets och rådets direktiv 2008/48/EG ([47]), 2009/138/EG ([48]), 2013/36/EU ([49]), 2014/17/EU ([50]) och (EU) 2016/97 ([51]), inom ramen för

([46]) Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).

([47]) Europaparlamentets och rådets direktiv 2008/48/EG av den 23 april 2008 om konsumentkreditavtal och om upphävande av rådets direktiv 87/102/EEG (EUT L 133, 22.5.2008, s. 66).

([48]) Europaparlamentets och rådets direktiv 2009/138/EG av den 25 november 2009 om upptagande och utövande av försäkrings- och återförsäkringsverksamhet (Solvens II) (EUT L 335, 17.12.2009, s. 1).

([49]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

([50]) Europaparlamentets och rådets direktiv 2014/17/EU av den 4 februari 2014 om konsumentkreditavtal som avser bostadsfastighet och om ändring av direktiven 2008/48/EG och 2013/36/EU och förordning (EU) nr 1093/2010 (EUT L 60, 28.2.2014, s. 34).

([51]) Europaparlamentets och rådets direktiv (EU) 2016/97 av den 20 januari 2016 om försäkringsdistribution (EUT L 26, 2.2.2016, s. 19).

sina respektive befogenheter, utses till behöriga myndigheter för tillsynen över genomförandet av den här förordningen, även med avseende på marknadskontroll, när det gäller AI-system som tillhandahålls eller används av finansinstitut som är reglerade och står under tillsyn, såvida inte medlemsstaterna beslutar att utse en annan myndighet att utföra dessa marknadskontrolluppgifter. Dessa behöriga myndigheter bör ha alla befogenheter enligt den här förordningen och förordning (EU) 2019/1020 för att genomdriva kraven och skyldigheterna i den här förordningen, inbegripet befogenheter att utföra efterhandskontroll av marknaden som, när så är lämpligt, kan integreras i deras befintliga tillsynsmekanismer och tillsynsförfaranden enligt relevant unionsrätt om finansiella tjänster. Det är lämpligt att de nationella myndigheter som ansvarar för tillsynen av kreditinstitut som regleras genom direktiv 2013/36/EU och som deltar i den gemensamma tillsynsmekanism som inrättats genom rådets förordning (EU) nr 1024/2013 ([52]), när de agerar som marknadskontrollmyndigheter enligt den här förordningen, utan dröjsmål till Europeiska centralbanken rapporterar all information som identifierats i samband med deras marknadskontroll och som kan vara av potentiellt intresse för Europeiska centralbankens tillsynsuppgifter enligt den förordningen. För att ytterligare öka samstämmigheten mellan den här förordningen och de regler som är tillämpliga på kreditinstitut som regleras genom direktiv 2013/36/EU är det också lämpligt att i de befintliga skyldigheterna och förfarandena enligt direktiv 2013/36/EU integrera några av leverantörernas förfarandemässiga skyldigheter vad gäller riskhantering, övervakning av produkter som släppts ut på marknaden och dokumentation. För att undvika överlappningar bör begränsade undantag också förutses när det gäller leverantörers kvalitetsstyrningssystem och de övervakningsskyldigheter som gäller för tillhandahållare av AI-system med hög risk i den utsträckning som dessa är tillämpliga på kreditinstitut som regleras genom direktiv 2013/36/EU. Samma ordning bör tillämpas på försäkrings- och återförsäkringsföretag och försäkringsholdingbolag enligt direktiv 2009/138/EG och försäkringsförmedlare enligt direktiv (EU) 2016/97 och andra typer av finansinstitut som omfattas av krav avseende interna styrelseformer, arrangemang eller processer som inrättats enligt relevant unionsrätt om finansiella tjänster för att säkerställa samstämmighet och likabehandling inom finanssektorn.

(159) Varje marknadskontrollmyndighet för AI-system med hög risk på biometriområdet, enligt förteckningen i en bilaga till denna förordning, bör, i den mån dessa system används för brottsbekämpning, migration, asyl och gränskontrollförvaltning eller för rättskipning och demokratiska processer, ha effektiva utredningsbefogenheter och korrigerande befogenheter, inbegripet åtminstone befogenhet att få tillgång till alla personuppgifter som behandlas och till all information som krävs för att den ska kunna utföra sina uppgifter. Marknadskontrollmyndigheterna bör vara fullständigt oberoende i utövandet av sina befogenheter. Eventuella begränsningar av deras tillgång till känsliga operativa uppgifter enligt denna förordning bör inte påverka de befogenheter som de tilldelas genom direktiv (EU) 2016/680. Inget undantag när det gäller utlämnande av uppgifter till nationella dataskyddsmyndigheter enligt denna förordning bör påverka dessa myndigheters nuvarande eller framtida befogenheter utanför denna förordnings tillämpningsområde.

(160) Marknadskontrollmyndigheterna och kommissionen bör kunna föreslå gemensamma aktiviteter, inbegripet gemensamma utredningar, som ska genomföras av marknadskontrollmyndigheterna själva eller av marknadskontrollmyndigheter tillsammans med kommissionen, och som syftar till att främja överensstämmelse, identifiera bristande överensstämmelse, öka medvetenheten och ge vägledning om denna förordning med avseende på specifika kategorier av AI-system med hög risk som befinns utgöra en allvarlig risk i två eller flera medlemsstater. Gemensamma aktiviteter för att främja överensstämmelse bör genomföras i enlighet med artikel 9 i förordning (EU) 2019/1020. AI-byrån bör tillhandahålla samordningsstöd för gemensamma utredningar.

(161) Det är nödvändigt att klargöra ansvarsområdena och befogenheterna på unionsnivå och nationell nivå när det gäller AI-system som bygger på AI-modeller för allmänna ändamål. När ett AI-system bygger på en AI-modell för allmänna ändamål och modellen och systemet tillhandahålls av samma leverantör bör, i syfte att undvika överlappande

([52]) Rådets förordning (EU) nr 1024/2013 av den 15 oktober 2013 om tilldelning av särskilda uppgifter till Europeiska centralbanken i fråga om politiken för tillsyn över kreditinstitut (EUT L 287, 29.10.2013, s. 63).

befogenheter, tillsynen ske på unionsnivå genom AI-byrån, som bör ha befogenheter som marknadskontrollmyndighet i den mening som avses i förordning (EU) 2019/1020 för detta ändamål. I alla andra fall förblir de nationella marknadskontrollmyndigheterna ansvariga för tillsynen av AI-system. När det gäller AI-system för allmänna ändamål som kan användas direkt av tillhandahållare för minst ett ändamål som klassificeras som AI-system med hög risk bör marknadskontrollmyndigheterna dock samarbeta med AI-byrån för att utföra bedömningar av överensstämmelse och informera styrelsen och andra marknadskontrollmyndigheter om detta. Dessutom bör marknadskontrollmyndigheterna kunna begära bistånd från AI-byrån om marknadskontrollmyndigheten inte kan slutföra en utredning avseende ett AI-system med hög risk på grund av att den inte får tillgång till viss information om den AI-modell för allmänna ändamål som AI-systemet med hög risk bygger på. I sådana fall bör förfarandet för ömsesidig assistans i gränsöverskridande fall i kapitel VI i förordning (EU) 2019/1020 gälla i tillämpliga delar.

(162) I syfte att på bästa sätt utnyttja unionens centraliserade sakkunskap och synergier på unionsnivå bör befogenheterna avseende tillsyn och kontroll av efterlevnaden av skyldigheterna för leverantörer av AI-modeller för allmänna ändamål omfattas av kommissionens behörighet. AI-byrån bör kunna vidta alla nödvändiga åtgärder för att övervaka det effektiva genomförandet av denna förordning när det gäller AI-modeller för allmänna ändamål. Den bör kunna utreda eventuella överträdelser av reglerna för leverantörer av AI-modeller för allmänna ändamål, både på eget initiativ, baserat på resultaten av dess övervakningsverksamhet, eller på begäran av marknadskontrollmyndigheterna i enlighet med villkoren i denna förordning. I syfte att stödja en effektiv övervakning genom AI-byrån bör det föreskrivas en möjlighet för leverantörer i efterföljande led att lämna in klagomål om eventuella överträdelser av reglerna för leverantörer av AI-modeller och AI-system för allmänna ändamål.

(163) I syfte att komplettera styrningssystemen för AI-modeller för allmänna ändamål bör den vetenskapliga panelen stödja AI-byråns övervakningsverksamhet och får, i vissa fall, tillhandahålla kvalificerade varningar till AI-byrån som utlöser uppföljningar, såsom utredningar. Detta bör vara fallet om den vetenskapliga panelen har skäl att misstänka att en AI-modell för allmänna ändamål utgör en konkret och identifierbar risk på unionsnivå. Detta bör dessutom vara fallet om den vetenskapliga panelen har skäl att misstänka att en AI-modell för allmänna ändamål uppfyller kriterierna för att klassificeras som en AI-modell för allmänna ändamål med systemrisk. I syfte att förse den vetenskapliga panelen med den information som krävs för utförandet av dessa uppgifter bör det finnas en mekanism genom vilken den vetenskapliga panelen kan uppmana kommissionen att begära dokumentation eller information från en leverantör.

(164) AI-byrån bör kunna vidta nödvändiga åtgärder för att övervaka det faktiska genomförandet och efterlevnaden av de skyldigheter för leverantörer av AI-modeller för allmänna ändamål som fastställs i denna förordning. AI-byrån bör kunna utreda eventuella överträdelser i enlighet med de befogenheter som föreskrivs i denna förordning, bland annat genom att begära dokumentation och information, genom att genomföra utvärderingar och genom att kräva åtgärder från leverantörer av AI-modeller för allmänna ändamål. Vid genomförandet av utvärderingar bör AI-byrån, i syfte att utnyttja oberoende sakkunskap, kunna anlita oberoende experter som kan utföra utvärderingarna för dess räkning. Efterlevnaden av skyldigheterna bör kunna verkställas, bland annat genom begäranden om att vidta lämpliga åtgärder, inbegripet riskbegränsningsåtgärder i händelse av identifierade systemrisker samt begränsning av tillhandahållandet på marknaden, tillbakadragande eller återkallande av modellen. Som en skyddsåtgärd, när detta behövs utöver de processuella rättigheter som föreskrivs i denna förordning, bör leverantörer av AI-modeller för allmänna ändamål ha de processuella rättigheter som föreskrivs i artikel 18 i förordning (EU) 2019/1020, som bör gälla i tillämpliga delar, utan att det påverkar de mer specifika processuella rättigheter som föreskrivs i den här förordningen.

(165) Utvecklingen av andra AI-system än AI-system med hög risk i enlighet med kraven i denna förordning kan leda till en ökad användning av etisk och tillförlitlig AI i unionen. Leverantörer av AI-system som inte är AI-system med hög risk bör uppmuntras att ta fram uppförandekoder, inbegripet tillhörande styrningsmekanismer, avsedda att främja en frivillig tillämpning av vissa eller alla av de obligatoriska krav som gäller för AI-system med hög risk, anpassade med hänsyn till systemens avsedda ändamål och den lägre risk som de medför och med beaktande av tillgängliga tekniska lösningar och bästa branschpraxis, såsom modellkort och datakort. Leverantörer och, i förekommande fall, tillhandahållare av alla AI-system, med eller utan hög risk, och AI-modeller bör också uppmuntras att på frivillig grund tillämpa ytterligare krav avseende exempelvis inslagen i unionens etiska riktlinjer för tillförlitlig AI,

miljömässig hållbarhet, åtgärder för AI-kunnighet, inkluderande och diversifierad utformning och utveckling av AI-system, inbegripet uppmärksamhet för sårbara personer och tillgänglighet för personer med funktionsnedsättning, berörda parters deltagande med medverkan, i förekommande fall, av sådana berörda parter som näringslivsorganisationer och det civila samhällets organisationer, den akademiska världen, forskningsorganisationer, fackföreningar och konsumentskyddsorganisationer i utformningen och utvecklingen av AI-system samt mångfald i utvecklingsteamen, inbegripet en jämn könsfördelning. För att säkerställa att de frivilliga uppförandekoderna är effektiva bör de grunda sig på tydliga mål och centrala resultatindikatorer för att mäta uppnåendet av dessa mål. De bör också utvecklas på ett inkluderande sätt, när så är lämpligt, med deltagande av berörda parter såsom näringslivsorganisationer och det civila samhällets organisationer, den akademiska världen, forskningsorganisationer, fackföreningar och konsumentskyddsorganisationer. Kommissionen kan utveckla initiativ, även på sektorsbasis, för att minska de tekniska hindren för gränsöverskridande utbyte av data för AI-utveckling, däribland vad gäller infrastruktur för dataåtkomst samt semantisk och teknisk interoperabilitet för olika typer av data.

(166) Det är viktigt att AI-system som är relaterade till produkter som inte är AI-system med hög risk enligt denna förordning och som därmed inte måste uppfylla kraven på AI-system med hög risk ändå är säkra när de släpps ut på marknaden eller tas i bruk. För att bidra till detta mål skulle Europaparlamentets och rådets förordning (EU) 2023/988 ([53]) tillämpas som ett skyddsnät.

(167) För att säkerställa ett förtroendefullt och konstruktivt samarbete mellan behöriga myndigheter på unionsnivå och nationell nivå bör alla parter som är involverade i tillämpningen av denna förordning säkerställa konfidentiell behandling av information och data som de erhåller i utförandet av sina uppgifter, i enlighet med unionsrätten eller nationell rätt. De bör utföra sina uppgifter och bedriva sin verksamhet på ett sådant sätt att de i synnerhet skyddar immateriella rättigheter, konfidentiell affärsinformation och företagshemligheter, det effektiva genomförandet av denna förordning, allmänna och nationella säkerhetsintressen, integriteten i straffrättsliga och administrativa förfaranden samt integriteten hos säkerhetsskyddsklassificerade uppgifter.

(168) Efterlevnaden av denna förordning bör kunna verkställas genom åläggande av sanktioner och andra verkställighetsåtgärder. Medlemsstaterna bör vidta alla nödvändiga åtgärder för att säkerställa att bestämmelserna i denna förordning genomförs, bland annat genom att fastställa effektiva, proportionella och avskräckande sanktioner för åsidosättande av dem, och för att iaktta principen *ne bis in idem*. För att stärka och harmonisera de administrativa sanktionerna för överträdelser av denna förordning bör det fastställas övre gränser för fastställande av administrativa sanktionsavgifter för vissa specifika överträdelser. Vid bedömningen av storleken på sanktionsavgifterna bör medlemsstaterna i varje enskilt fall beakta alla relevanta omständigheter i den specifika situationen, med vederbörlig hänsyn särskilt till överträdelsens art, svårighetsgrad och varaktighet och dess konsekvenser samt till leverantörens storlek, särskilt om leverantören tillhör kategorin små och medelstora företag, inbegripet uppstartsföretag. Europeiska datatillsynsmannen bör ha befogenhet att ålägga böter för unionens institutioner, byråer och organ som omfattas av denna förordning.

(169) Efterlevnaden av de skyldigheter för leverantörer av AI-modeller för allmänna ändamål som införs enligt denna förordning bör kunna verkställas bland annat genom sanktionsavgifter. I detta syfte bör lämpliga nivåer på sanktionsavgifterna också fastställas för överträdelser av dessa skyldigheter, inbegripet åsidosättande av de åtgärder som kommissionen begär i enlighet med denna förordning, med förbehåll för lämpliga preskriptionstider i enlighet med proportionalitetsprincipen. Alla beslut som kommissionen fattar enligt denna förordning kan prövas av Europeiska unionens domstol i enlighet med EUF-fördraget, inbegripet domstolens obegränsade behörighet när det gäller sanktioner enligt artikel 261 i EUF-fördraget.

(170) Unionsrätten och nationell rätt föreskriver redan effektiva rättsmedel för fysiska och juridiska personer vars rättigheter och friheter påverkas negativt av användningen av AI-system. Utan att det påverkar dessa rättsmedel bör varje fysisk eller juridisk person som har skäl att anse att denna förordning har överträtts ha rätt att lämna in klagomål till den berörda marknadskontrollmyndigheten.

(171) Berörda personer bör ha rätt att få en förklaring om en tillhandahållares beslut huvudsakligen grundar sig på utdata från vissa AI-system med hög risk som omfattas av denna förordning och om det beslutet har rättslig verkan eller på liknande sätt i betydande grad påverkar dessa personer på ett sätt som de anser ha en negativ inverkan på deras hälsa,

([53]) Europaparlamentets och rådets förordning (EU) 2023/988 av den 10 maj 2023 om allmän produktsäkerhet, ändring av Europaparlamentets och rådets förordning (EU) nr 1025/2012 och Europaparlamentets och rådets direktiv (EU) 2020/1828 och om upphävande av Europaparlamentets och rådets direktiv 2001/95/EG och rådets direktiv 87/357/EEG (EUT L 135, 23.5.2023, s. 1).

säkerhet eller grundläggande rättigheter. Den förklaringen bör vara tydlig och meningsfull och bör tillhandahålla en grund på vilken de berörda personerna kan utöva sina rättigheter. Rätten att få en förklaring bör inte tillämpas på sådan användning av AI-system som enligt unionsrätten eller nationell rätt omfattas av undantag eller begränsningar och bör endast tillämpas i den mån denna rätt inte redan föreskrivs i unionsrätten.

(172) Personer som agerar som visselblåsare när det gäller överträdelser av denna förordning bör skyddas enligt unionsrätten. Europaparlamentets och rådets direktiv (EU) 2019/1937 ([54]) bör därför tillämpas på rapportering av överträdelser av denna förordning och skydd för personer som rapporterar sådana överträdelser.

(173) För att säkerställa att regelverket vid behov kan anpassas bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen när det gäller ändring av de villkor enligt vilka ett AI-system inte ska betraktas som ett AI-system med hög risk, förteckningen över AI-system med hög risk, bestämmelserna om teknisk dokumentation, innehållet i EU-försäkran om överensstämmelse, bestämmelserna om förfaranden för bedömning av överensstämmelse, bestämmelserna om fastställande av de AI-system med hög risk som omfattas av det förfarande för bedömning av överensstämmelse som baseras på en bedömning av kvalitetsstyrningssystemet och en bedömning av den tekniska dokumentationen, tröskelvärdet, riktmärkena och indikatorerna, inbegripet genom komplettering av dessa riktmärken och indikatorer, i reglerna för klassificering av AI-modeller för allmänna ändamål med systemrisk, kriterierna för utseende av AI-modeller för allmänna ändamål med systemrisk, den tekniska dokumentationen för leverantörer av AI-modeller för allmänna ändamål och transparensinformationen för leverantörer av AI-modeller för allmänna ändamål. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([55]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(174) Med tanke på den snabba tekniska utvecklingen och den tekniska expertis som krävs för en effektiv tillämpning av denna förordning bör kommissionen utvärdera och se över denna förordning senast den 2 augusti 2029 och därefter vart fjärde år samt rapportera till Europaparlamentet och rådet. Dessutom bör kommissionen, med beaktande av konsekvenserna för denna förordnings tillämpningsområde, en gång om året göra en bedömning av behovet av att ändra förteckningen över AI-system med hög risk och förteckningen över förbjudna användningsområden. Senast den 2 augusti 2028 och därefter vart fjärde år bör kommissionen dessutom utvärdera och till Europaparlamentet och rådet rapportera om behovet av att ändra förteckningen över högriskområdesrubriker i bilagan till denna förordning, de AI-system som omfattas av transparensskyldigheterna, tillsyns- och styrningssystemets effektivitet och framstegen med utvecklingen av standardiseringsprodukter för energieffektiv utveckling av AI-modeller för allmänna ändamål, inbegripet behovet av ytterligare åtgärder eller insatser. Senast den 2 augusti 2028 och därefter vart tredje år bör kommissionen slutligen utvärdera inverkan och effektiviteten hos de frivilliga uppförandekoder som syftar till att främja tillämpningen av de krav som fastställs för AI-system med hög risk när det gäller andra AI-system än AI-system med hög risk och eventuellt andra ytterligare krav för sådana AI-system.

(175) För att säkerställa enhetliga villkor för genomförandet av denna förordning, bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([56]).

(176) Eftersom målet för denna förordning, nämligen att förbättra den inre marknadens funktion och främja användningen av människocentrerad och tillförlitlig AI, samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan, inbegripet demokrati, rättsstatens principer och miljöskydd, mot de skadliga effekterna av AI-system i unionen, och att stödja innovation, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning och verkningar, kan

([54]) Europaparlamentets och rådets direktiv (EU) 2019/1937 av den 23 oktober 2019 om skydd för personer som rapporterar om överträdelser av unionsrätten (EUT L 305, 26.11.2019, s. 17).
([55]) EUT L 123, 12.5.2016, s. 1.
([56]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EU-fördraget. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

(177) För att säkerställa rättssäkerhet, säkerställa en lämplig anpassningsperiod för operatörer och undvika störningar på marknaden, bland annat genom att säkerställa kontinuitet i användningen av AI-system, bör denna förordning tillämpas på AI-system med hög risk som har släppts ut på marknaden eller tagits i bruk före det allmänna tillämpningsdatumet för denna förordning, endast om dessa system från och med den dagen genomgår betydande ändringar av sin utformning eller sitt avsedda ändamål. Det är lämpligt att klargöra att begreppet betydande ändring i detta avseende bör tolkas som att det i sak är likvärdigt med begreppet väsentlig ändring, som endast används med avseende på AI-system med hög risk enligt denna förordning. I undantagsfall och mot bakgrund av offentlig ansvarsskyldighet bör operatörer av AI-system som är komponenter i de stora it-system som inrättats genom de rättsakter som förtecknas i en bilaga till denna förordning respektive operatörer av AI-system med hög risk som är avsedda att användas av offentliga myndigheter vidta nödvändiga åtgärder för att uppfylla kraven i denna förordning senast i slutet av 2030 och senast den 2 augusti 2030.

(178) Leverantörer av AI-system med hög risk uppmuntras att på frivillig basis börja fullgöra de relevanta skyldigheterna i denna förordning redan under övergångsperioden.

(179) Denna förordning bör tillämpas från och med den 2 augusti 2026. Med hänsyn till den oacceptabla risk som är förknippad med användning av AI på vissa sätt bör dock förbuden och de allmänna bestämmelserna i denna förordning redan tillämpas från och med den 2 februari 2025. Även om dessa förbuds fulla verkan följer av inrättandet av styrningen och kontrollen av efterlevnaden av denna förordning, är det viktigt att föregripa tillämpningen av förbuden för att ta hänsyn till oacceptabla risker och påverka andra förfaranden, såsom civilrättsliga förfaranden. Vidare bör infrastrukturen för styrning och systemet för bedömning av överensstämmelse vara operativa före den 2 augusti 2026, varför bestämmelserna om anmälda organ och styrningsstruktur bör tillämpas från och med den 2 augusti 2025. Med tanke på den snabba takten inom tekniska framsteg och införandet av AI-modeller för allmänna ändamål bör skyldigheterna för leverantörer av AI-modeller för allmänna ändamål gälla från och med 2 augusti 2025. Förfarandekoder bör vara klara senast den 2 maj 2025 för att leverantörer ska kunna visa efterlevnad i tid. AI-byrån bör säkerställa att klassificeringsregler och klassificeringsförfaranden är aktuella mot bakgrund av teknisk utveckling. Medlemsstaterna bör också fastställa och meddela kommissionen reglerna om sanktioner, inklusive administrativa sanktionsavgifter, och säkerställa att de genomförs korrekt och effektivt senast den dag då denna förordning börjar tillämpas. Därför bör bestämmelserna om sanktioner tillämpas från och med den 2 augusti 2025.

(180) Europeiska datatillsynsmannen och Europeiska dataskyddsstyrelsen har hörts i enlighet med artikel 42.1 och 42.2 i förordning (EU) 2018/1725 och avgav sitt gemensamma yttrande den 18 juni 2021.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

1. Syftet med denna förordning är att förbättra den inre marknadens funktion och främja användningen av människocentrerad och tillförlitlig artificiell intelligens (AI), samtidigt som en hög skyddsnivå säkerställs för hälsa, säkerhet och grundläggande rättigheter som fastställs i stadgan, inbegripet demokrati, rättsstatens principer och miljöskydd, mot de skadliga effekterna av AI-system i unionen, och att stödja innovation.

2. I denna förordning fastställs

a) harmoniserade regler för utsläppande på marknaden, ibruktagande och användning av AI-system i unionen,

b) förbud mot vissa AI-användningsområden,

c) särskilda krav för AI-system med hög risk och skyldigheter för operatörer av sådana system,

d) harmoniserade transparensregler för vissa AI-system,

e) harmoniserade regler för utsläppande på marknaden av AI-modeller för allmänna ändamål,

f) regler om marknadsövervakning, marknadskontroll, styrning och kontroll av efterlevnad,

g) åtgärder till stöd för innovation med särskild inriktning på små och medelstora företag, inbegripet uppstartsföretag.

Artikel 2

Tillämpningsområde

1. Denna förordning är tillämplig på

a) leverantörer som släpper ut AI-system på marknaden eller tar sådana i bruk eller släpper ut AI-modeller för allmänna ändamål på marknaden i unionen, oavsett om dessa leverantörer är etablerade eller befinner sig i unionen eller i ett tredjeland,

b) tillhandahållare av AI-system som har sin etableringsort eller befinner sig i unionen,

c) leverantörer och tillhandahållare av AI-system som har sin etableringsort eller befinner sig i ett tredjeland, om de utdata som produceras av AI-systemet används i unionen,

d) importörer och distributörer av AI-system,

e) produkttillverkare som på marknaden släpper ut eller som tar i bruk ett AI-system tillsammans med sin produkt och i eget namn eller under eget varumärke,

f) ombud för leverantörer som inte är etablerade i unionen,

g) berörda personer som befinner sig i unionen.

2. För AI-system som klassificeras som AI-system med hög risk enligt artikel 6.1 och som är relaterade till produkter som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt B i bilaga I är endast artiklarna 6.1, 102-109 och 112 tillämpliga. Artikel 57 är endast tillämplig i den mån som kraven för AI-system med hög risk enligt denna förordning har integrerats i den unionsharmoniseringslagstiftningen.

3. Denna förordning är inte tillämplig på områden som inte omfattas av unionsrättens tillämpningsområde och ska under alla omständigheter inte påverka medlemsstaternas befogenheter när det gäller nationell säkerhet, oavsett vilken typ av enhet som av medlemsstaterna har anförtrotts uppgiften i fråga om dessa befogenheter.

Denna förordning är inte tillämplig på AI-system om och i den mån de släpps ut på marknaden, tas i bruk eller används med eller utan ändring uteslutande för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet, oavsett vilken typ av enhet som bedriver denna verksamhet.

Denna förordning är inte tillämplig på AI-system som inte släpps ut på marknaden eller tas i bruk i unionen, om utdata används i unionen uteslutande för militära ändamål, försvarsändamål eller ändamål som rör nationell säkerhet, oavsett vilken typ av enhet som bedriver denna verksamhet.

4. Denna förordning är inte tillämplig på offentliga myndigheter i ett tredjeland, eller på internationella organisationer som omfattas av denna förordnings tillämpningsområde enligt punkt 1, om dessa myndigheter eller organisationer använder AI-system inom ramen för internationellt samarbete eller internationella avtal om brottsbekämpande och rättsligt samarbete med unionen eller med en eller flera medlemsstater, förutsatt att ett sådant tredjeland eller en sådan internationell organisation erbjuder lämpliga skyddsåtgärder med avseende på skyddet av enskildas grundläggande rättigheter och friheter.

5. Denna förordning påverkar inte tillämpningen av bestämmelserna om ansvar för leverantörer av förmedlingstjänster i kapitel II i förordning (EU) 2022/2065.

6. Denna förordning är inte tillämplig på AI-system eller AI-modeller, inbegripet deras utdata, som specifikt utvecklas och tas i bruk enbart i vetenskapligt forsknings- och utvecklingssyfte.

7. Unionsrätt om skydd av personuppgifter, integritet och konfidentialitet vid kommunikation är tillämplig på personuppgifter som behandlas i samband med de rättigheter och skyldigheter som fastställs i denna förordning. Denna förordning påverkar inte förordning (EU) 2016/679 eller (EU) 2018/1725 eller direktiv 2002/58/EG eller (EU) 2016/680, utan att det påverkar tillämpningen av artiklarna 10.5 och 59 i den här förordningen.

8. Denna förordning är inte tillämplig på forsknings-, testnings- eller utvecklingsverksamhet för AI-system eller AI-modeller innan de släpps ut på marknaden eller tas i bruk. Sådan verksamhet ska bedrivas i enlighet med tillämplig unionsrätt. Testning under verkliga förhållanden omfattas inte av detta undantag.

9. Denna förordning påverkar inte tillämpningen av de regler som fastställs genom andra unionsrättsakter om konsumentskydd och produktsäkerhet.

10. Denna förordning är inte tillämplig på skyldigheter för tillhandahållare som är fysiska personer och som använder AI-system inom ramen för en rent personlig icke-yrkesmässig verksamhet.

11. Denna förordning hindrar inte unionen eller medlemsstaterna från att behålla eller införa lagar och andra författningar som är förmånligare för arbetstagare när det gäller att skydda deras rättigheter i fråga om arbetsgivares användning av AI-system, eller att uppmuntra eller tillåta tillämpning av kollektivavtal som är förmånligare för arbetstagare.

12. Denna förordning är inte tillämplig på AI-system som släpps ut med kostnadsfria licenser med öppen källkod, såvida de inte släpps ut på marknaden eller tas i bruk som ett AI-system med hög risk eller som ett AI-system som omfattas av artikel 5 eller 50.

Artikel 3

Definitioner

I denna förordning gäller följande definitioner:

1. *AI-system*: ett maskinbaserat system som är utformat för att fungera med varierande grad av autonomi och som kan uppvisa anpassningsförmåga efter införande och som, för uttryckliga eller underförstådda mål, drar slutsatser härledda från den indata det tar emot, om hur utdata såsom förutsägelser, innehåll, rekommendationer eller beslut som kan påverka fysiska eller virtuella miljöer ska genereras.

2. *risk*: kombinationen av sannolikheten för skada och denna skadas allvarlighetsgrad.

3. *leverantör*: en fysisk eller juridisk person, en offentlig myndighet, en byrå eller ett annat organ som utvecklar ett AI-system eller en AI-modell för allmänna ändamål eller som har ett AI-system eller en AI-modell för allmänna ändamål och släpper ut det eller den på marknaden eller tar AI-systemet i bruk i eget namn eller under eget varumärke, antingen mot betalning eller kostnadsfritt.

4. *tillhandahållare*: en fysisk eller juridisk person, offentlig myndighet, en byrå eller annat organ som under eget överinseende använder ett AI-system, utom när AI-systemet används inom ramen för en personlig icke-yrkesmässig verksamhet.

5. *ombud*: en fysisk eller juridisk person som befinner sig eller är etablerad i unionen och som har fått och godtagit en skriftlig fullmakt från en leverantör av ett AI-system eller av en AI-modell för allmänna ändamål för att för dennes räkning fullgöra respektive genomföra de skyldigheter och förfaranden som fastställs i denna förordning.

6. *importör*: en fysisk eller juridisk person som befinner sig eller är etablerad i unionen och som släpper ut ett AI-system på marknaden som bär namnet på eller varumärket för en fysisk eller juridisk person som är etablerad i ett tredjeland.

7. *distributör*: en annan fysisk eller juridisk person i leveranskedjan än leverantören eller importören, som tillhandahåller ett AI-system på unionsmarknaden.

8. *operatör*: en leverantör, en produkttillverkare, en tillhandahållare, ett ombud, en importör eller en distributör.

9. *utsläppande på marknaden*: den första gången ett AI-system eller en AI-modell för allmänna ändamål tillhandahålls på unionsmarknaden.

10. *tillhandahållande på marknaden*: leveransen av ett AI-system eller en AI-modell för allmänna ändamål för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, mot betalning eller kostnadsfritt.

11. *ibruktagande*: leverans av ett AI-system för första användning direkt till tillhandahållaren eller för eget bruk i unionen för dess avsedda ändamål.

12. *avsett ändamål*: den användning för vilken ett AI-system är avsett av leverantören, inbegripet det specifika användningssammanhanget och de specifika användningsvillkoren, enligt specifikationerna i de uppgifter som tillhandahålls av leverantören i bruksanvisningen, reklam- eller försäljningsmaterial och uttalanden samt i den tekniska dokumentationen.

13. *rimligen förutsebar felaktig användning*: användning av ett AI-system på ett sätt som inte överensstämmer med dess avsedda ändamål, men som kan vara resultatet av rimligen förutsebart mänskligt beteende eller interaktion med andra system, inbegripet andra AI-system.

14. *säkerhetskomponent*: en komponent som finns i en produkt eller i ett AI-system och som fyller en säkerhetsfunktion för den produkten eller det AI-systemet eller som, om den upphör att fungera eller fungerar felaktigt, medför fara för människors hälsa och säkerhet eller för egendom.

15. *bruksanvisning*: information som tillhandahålls av leverantören för att informera tillhandahållaren om, i synnerhet, ett AI-systems avsedda ändamål och korrekta användning.

16. *återkallelse av ett AI-system*: varje åtgärd som syftar till att få till stånd ett återlämnande till leverantören, ett urdrifttagande eller en avaktivering av användningen av ett AI-system som tillhandahållits för tillhandahållare.

17. *tillbakadragande av ett AI-system*: varje åtgärd som syftar till att förhindra att ett AI-system i leveranskedjan tillhandahålls på marknaden.

18. *ett AI-systems prestanda*: ett AI-systems förmåga att uppnå sitt avsedda ändamål.

19. *anmälande myndighet*: den nationella myndighet som ansvarar för inrättandet och genomförandet av de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa.

20. *bedömning av överensstämmelse*: processen att visa om kraven i kapitel III avsnitt 2 avseende ett AI-system med hög risk har uppfyllts.

21. *organ för bedömning av överensstämmelse*: organ som utför tredjepartsbedömning av överensstämmelse, inbegripet testning, certifiering och inspektion.

22. *anmält organ*: organ för bedömning av överensstämmelse som anmälts i enlighet med denna förordning och annan relevant unionsharmoniseringslagstiftning.

23. *väsentlig ändring*: en ändring av ett AI-system efter dess utsläppande på marknaden eller ibruktagande som inte förutsetts eller planerats i leverantörens ursprungliga bedömning av överensstämmelse och som leder till att AI-systemets uppfyllelse av kraven i kapitel III avsnitt 2 påverkas eller leder till en ändring av det avsedda ändamål för vilket AI-systemet har bedömts.

24. *CE-märkning*: märkning genom vilken en leverantör anger att ett AI-system överensstämmer med kraven i kapitel III avsnitt 2 och annan tillämplig unionsharmoniseringslagstiftning som föreskriver att den anbringas.

25. *system för övervakning efter utsläppande på marknaden*: all verksamhet som bedrivs av leverantörer av AI-system för att samla in och granska erfarenheter från användningen av AI-system som de släpper ut på marknaden eller tar i bruk, i syfte att fastställa ett eventuellt behov av att omedelbart vidta eventuella nödvändiga korrigerande eller förebyggande åtgärder.

26. *marknadskontrollmyndighet*: den nationella myndighet som utför aktiviteter och vidtar åtgärder enligt förordning (EU) 2019/1020.

27. *harmoniserad standard*: en harmoniserad standard enligt definitionen i artikel 2.1 c i förordning (EU) nr 1025/2012.

28. *gemensam specifikation*: en uppsättning tekniska specifikationer enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012 som ger förutsättningar för att uppfylla vissa krav som fastställts enligt den här förordningen.

29. *träningsdata*: data som används för att träna ett AI-system genom anpassning av dess inlärningsbara parametrar.

30. *valideringsdata*: data som används för att tillhandahålla en utvärdering av det tränade AI-systemet och för att stämma av dess icke-inlärningsbara parametrar och dess inlärningsprocess för att bland annat förhindra under- eller överanpassning.

31. *valideringsdataset*: ett separat dataset eller en separat del av träningsdatasetet, antingen som en fast eller variabel uppdelning.

32. *testdata*: data som används för att tillhandahålla en oberoende utvärdering av AI-systemet för att bekräfta systemets förväntade prestanda innan det släpps ut på marknaden eller tas i bruk.

33. *indata*: data som lämnas till eller anskaffas direkt av ett AI-system och som utgör den grund på vilken systemet producerar utdata.

34. *biometriska uppgifter*: personuppgifter som erhållits genom särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken, såsom ansiktsbilder eller fingeravtrycksuppgifter.

35. *biometrisk identifiering*: automatiserad igenkänning av fysiska, fysiologiska, beteendemässiga eller psykologiska mänskliga drag för att fastställa en fysisk persons identitet genom jämförelse av personens biometriska uppgifter med biometriska uppgifter om enskilda personer som lagrats i en databas.

36. *biometrisk verifiering*: automatiserad en-till-en-verifiering, inklusive autentisering, av fysiska personers identitet genom jämförelse av deras biometriska uppgifter med tidigare lämnade biometriska uppgifter.

37. *särskilda kategorier av personuppgifter*: de kategorier av personuppgifter som avses i artikel 9.1 i förordning (EU) 2016/679, artikel 10 i direktiv (EU) 2016/680 och artikel 10.1 i förordning (EU) 2018/1725.

38. *känsliga operativa uppgifter*: operativa uppgifter som rör verksamhet för att förebygga, förhindra, upptäcka, utreda eller lagföra brott och vars röjande skulle kunna äventyra straffrättsliga förfarandens integritet.

39. *system för känsloigenkänning*: ett AI-system vars syfte är att identifiera eller uttyda fysiska personers känslor eller avsikter på grundval av deras biometriska uppgifter.

40. *system för biometrisk kategorisering*: ett AI-system för hänförande av fysiska personer till särskilda kategorier på grundval av deras biometriska uppgifter, om det inte utgör en extrafunktion till en annan kommersiell tjänst och är strikt nödvändigt av objektiva tekniska skäl.

41. *system för biometrisk fjärridentifiering*: ett AI-system vars syfte är att identifiera fysiska personer utan deras aktiva medverkan, vanligtvis på distans, genom jämförelse av en persons biometriska uppgifter med de biometriska uppgifterna i en referensdatabas.

42. *system för biometrisk fjärridentifiering i realtid*: ett system för biometrisk fjärridentifiering där infångning av biometriska uppgifter, jämförelse och identifiering sker utan betydande dröjsmål, som omfattar inte bara omedelbar identifiering utan även begränsade korta fördröjningar för att undvika kringgående.

43. *system för biometrisk fjärridentifiering i efterhand*: ett annat system för biometrisk fjärridentifiering än ett system för biometrisk fjärridentifiering i realtid.

44. *allmänt tillgänglig plats*: varje offentlig- eller privatägd fysisk plats som är tillgänglig för ett obestämt antal fysiska personer, utan hänsyn till om vissa villkor eller omständigheter för tillträde kan gälla, och oberoende av eventuella kapacitetsbegränsningar.

45. *brottsbekämpande myndighet*:

a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, eller

b) ett annat organ eller en annan enhet som genom medlemsstaternas nationella rätt har anförtrotts myndighetsutövning för att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

46. *brottsbekämpning*: verksamhet som genomförs av brottsbekämpande myndigheter eller på deras vägnar för att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

47. *AI-byrån*: kommissionens funktion att bidra till genomförandet, övervakningen och tillsynen av AI-system samt AI-modeller för allmänna ändamål, och AI-styrning, enligt kommissionens beslut av den 24 januari 2024; hänvisningar i denna förordning till AI-byrån ska anses som hänvisningar till kommissionen.

48. *nationell behörig myndighet*: en anmälande myndighet eller en marknadskontrollmyndighet; när det gäller AI-system som tas i bruk eller används av unionens institutioner, byråer och organ ska hänvisningar till nationella behöriga myndigheter eller marknadskontrollmyndigheter i denna förordning anses som hänvisningar till Europeiska datatillsynsmannen.

49. *allvarlig incident*: en incident eller ett fel i ett AI-system som direkt eller indirekt orsakar något av följande:

a) Dödsfall eller allvarlig skada på en persons hälsa.

b) En allvarlig och oåterkallelig störning av förvaltningen eller driften av kritisk infrastruktur.

c) Åsidosättande av skyldigheter enligt unionsrätten avsedda att skydda grundläggande rättigheter.

d) Allvarlig skada på egendom eller på miljön.

50. *personuppgifter*: personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

51. *icke-personuppgifter*: andra uppgifter än personuppgifter enligt definitionen i artikel 4.1 i förordning (EU) 2016/679.

52. *profilering*: profilering enligt definitionen i artikel 4.4 i förordning (EU) 2016/679.

53. *plan för testning under verkliga förhållanden*: ett dokument som beskriver målen och metoden för samt den geografiska, befolkningsmässiga och tidsmässiga omfattningen, övervakningen, organisationen samt genomförandet av testning under verkliga förhållanden.

54. *sandlådeplan*: ett dokument om vilket den deltagande leverantören och den behöriga myndigheten har kommit överens och som beskriver målen, villkoren, tidsplanen, metoden och kraven för den verksamhet som ska bedrivas i sandlådan.

55. *regulatorisk sandlåda för AI*: en kontrollerad ram som inrättats av en behörig myndighet och som erbjuder leverantörer eller potentiella leverantörer av AI-system möjlighet att utveckla, träna, validera och testa, när så är lämpligt under verkliga förhållanden, ett innovativt AI-system, enligt en specifik sandlådeplan för en begränsad tid under regulatorisk tillsyn.

56. *AI-kunnighet*: kompetens, kunskap och förståelse som gör det möjligt för leverantörer, tillhandahållare och berörda personer att, med hänsyn till deras respektive rättigheter och skyldigheter i samband med denna förordning, införa AI-system på ett välgrundat sätt samt bli medvetna om möjligheterna och riskerna med AI, och den potentiella skada den kan vålla.

57. *testning under verkliga förhållanden*: tillfällig testning av ett AI-system med avseende på dess avsedda ändamål under verkliga förhållanden utanför ett laboratorium eller en på annat sätt simulerad miljö i syfte att samla in tillförlitliga och robusta data och bedöma och kontrollera AI-systemets överensstämmelse med kraven i denna förordning, som inte innebär att AI-systemet släpps ut på marknaden eller tas i bruk i den mening som avses i denna förordning förutsatt att alla villkor i artikel 57 eller 60 är uppfyllda.

58. *försöksperson*: vid testning under verkliga förhållanden en fysisk person som deltar i testning under verkliga förhållanden.

59. *informerat samtycke*: en försökspersons frivilliga, specifika, informerade och otvetydiga uttryck för sin vilja att delta i en viss testning under verkliga förhållanden, efter att ha informerats om alla aspekter av testningen som är relevanta för försökspersonens beslut att delta.

60. *deepfake*: AI-genererat eller AI-manipulerat bild-, ljud- eller videoinnehåll som liknar existerande personer, föremål, platser, enheter eller händelser och som för en person felaktigt kan framstå som autentiskt eller sanningsenligt.

61. *utbredd överträdelse*: varje handling eller underlåtenhet som strider mot unionsrätten om skydd av enskilda personers intressen och som

    a) har skadat eller sannolikt kommer att skada de kollektiva intressena för enskilda personer som är bosatta i minst två andra medlemsstater än den där

        i) handlingen eller underlåtenheten hade sitt ursprung eller ägde rum,

        ii) den berörda leverantören befinner sig eller är etablerad eller, i tillämpliga fall, dess ombud befinner sig eller är etablerat, eller

        iii) tillhandahållaren är etablerad, i de fall där överträdelsen begås av tillhandahållaren,

    b) har orsakat, orsakar eller sannolikt kommer att orsaka skada på enskilda personers kollektiva intressen och uppvisar gemensamma drag, till exempel genom att innebära bruk av samma olagliga metoder eller åsidosättande av samma intresse, samt begås av samma operatör och begås samtidigt i minst tre medlemsstater.

62. *kritisk infrastruktur*: kritisk infrastruktur enligt definitionen i artikel 2.4 i direktiv (EU) 2022/2557.

63. *AI-modell för allmänna ändamål*: en AI-modell, även när en sådan AI-modell tränas med en stor mängd data med hjälp av självövervakning i stor skala, som uppvisar betydande generalitet och på ett kompetent sätt kan utföra ett brett spektrum av distinkta uppgifter oavsett hur modellen släppts ut på marknaden och som kan integreras i en rad system eller tillämpningar i efterföljande led, utom AI-modeller som används för forsknings-, utvecklings- eller prototypverksamhet innan de släpps ut på marknaden.

64. *kapacitet med hög påverkansgrad*: kapacitet som motsvarar eller överstiger den kapacitet som registrerats i de mest avancerade AI-modellerna för allmänna ändamål.

65. *systemrisk*: en risk som är specifikt kopplad till den kapacitet för hög påverkansgrad som finns hos AI-modeller för allmänna ändamål och som påverkar unionsmarknaden i betydande grad på grund av sin räckvidd eller på grund av faktiska eller rimligen förutsebara negativa effekter på folkhälsa, säkerhet, allmän säkerhet, grundläggande rättigheter eller samhället som helhet, och som kan spridas i stor skala i hela värdekedjan.

66. *AI-system för allmänna ändamål*: ett AI-system som bygger på en AI-modell för allmänna ändamål och som har kapacitet att tjäna en rad olika ändamål, både för direkt användning och för integrering i andra AI-system.

67. *flyttalsberäkning*: varje matematisk operation eller tilldelning som inbegriper flyttal, som är en delmängd av de reella talen som typiskt representeras på datorer genom ett heltal med fast precision multiplicerad med en heltalsexponent med en fast talbas.

68. *leverantör i efterföljande led*: en leverantör av ett AI-system, inbegripet ett AI-system för allmänna ändamål, som integrerar en AI-modell, oavsett om AI-modellen levereras av dem själva och integreras vertikalt eller levereras av en annan enhet på grundval av avtalsförhållanden.

Artikel 4

AI-kunnighet

Leverantörer och tillhandahållare av AI-system ska vidta åtgärder för att i största möjliga mån säkerställa att deras personal och andra personer som för deras räkning arbetar med drift och användning av AI-system har tillräcklig AI-kunnighet, med beaktande av deras tekniska kunskaper, erfarenhet och utbildning samt det sammanhang i vilket AI-systemen ska användas, och med hänsyn till de personer eller grupper av personer på vilka AI-systemen ska användas.

KAPITEL II

FÖRBJUDNA AI-ANVÄNDNINGSOMRÅDEN

Artikel 5

Förbjudna AI-användningsområden

1. Följande AI-användningsområden ska vara förbjudna:

a) Utsläppande på marknaden, ibruktagande eller användning av ett AI-system som utnyttjar subliminala tekniker som människor inte är medvetna om eller avsiktligt manipulerande eller vilseledande tekniker som syftar eller leder till en väsentlig påverkan på en persons eller en grupp av personers beteende genom att avsevärt försämra deras förmåga att fatta ett välgrundat beslut, vilket får dem att fatta ett beslut som de annars inte skulle ha fattat, på ett sätt som orsakar eller med rimlig sannolikhet kommer att orsaka betydande skada för den personen, en annan person eller en grupp av personer.

b) Utsläppande på marknaden, ibruktagande eller användning av ett AI-system som utnyttjar en sårbarhet hos en fysisk person eller en specifik grupp av personer som härrör från ålder, funktionsnedsättning eller en specifik social eller ekonomisk situation, med målet eller verkan att väsentligt påverka beteendet hos den personen eller en person som tillhör den gruppen på ett sätt som orsakar eller med rimlig sannolikhet kommer att orsaka betydande skada för den personen eller en annan person.

c) Utsläppande på marknaden, ibruktagande eller användning av AI-system för utvärdering eller klassificering av fysiska personer eller grupper av personer under en viss tidsperiod på grundval av deras sociala beteende eller kända, uttydda eller förutsedda personliga eller personlighetsrelaterade egenskaper, med en social poängsättning som leder till det ena eller båda av följande:

   i) Skadlig eller ogynnsam behandling av vissa fysiska personer eller grupper av personer i sociala sammanhang som saknar koppling till de sammanhang i vilka berörda data ursprungligen genererades eller samlades in.

   ii) Skadlig eller ogynnsam behandling av vissa fysiska personer eller grupper av personer som är omotiverad eller oproportionerlig i förhållande till personernas sociala beteende eller till hur allvarligt beteendet är.

d) Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av ett AI-system för riskbedömningar av fysiska personer i syfte att bedöma eller förutse risken för att en fysisk person begår ett brott, uteslutande grundat på profileringen av en fysisk person eller på en bedömning av deras personlighetsdrag och egenskaper. Detta förbud är inte tillämpligt på AI-system som används för att stödja mänsklig bedömning av en persons inblandning i brottslig verksamhet, som redan grundas på objektiva och verifierbara fakta med direkt anknytning till brottslig verksamhet.

e) Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av AI-system som skapar eller utvidgar databaser för ansiktsigenkänning genom oriktad skrapning av ansiktsbilder från internet eller övervakningskameror.

f) Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av AI-system för att uttyda en fysisk persons känslor på arbetsplatsen eller vid utbildningsinstitutioner, såvida inte AI-systemets användning är avsett att införas eller släppas ut på marknaden av medicinska skäl eller säkerhetsskäl.

g) Utsläppande på marknaden, ibruktagande för detta specifika ändamål eller användning av system för biometrisk kategorisering som kategoriserar fysiska personer individuellt på grundval av deras biometriska uppgifter för att härleda eller dra slutsatser om en persons ras, politiska åsikter, medlemskap i fackförening, religiösa eller filosofiska övertygelse, sexualliv eller sexuella läggning. Detta förbud omfattar inte märkning eller filtrering av lagligen förvärvade biometriska dataset, såsom bilder, grundat på biometriska uppgifter eller kategorisering av biometriska uppgifter på området för brottsbekämpning.

h) Användning av system för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser för brottsbekämpande ändamål, om inte och endast i den mån sådan användning är absolut nödvändig för något av följande syften:

i) Målinriktad sökning efter specifika offer för människorov, människohandel eller sexuellt utnyttjande av människor, samt sökning efter försvunna personer.

ii) Förhindrande av ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet eller ett verkligt och aktuellt eller verkligt och förutsebart hot om en terroristattack.

iii) Lokalisering eller identifiering av en person som misstänks ha begått ett brott, i syfte att genomföra en brottsutredning eller lagföring för brott eller verkställande av en straffrättslig påföljd för brott som avses i bilaga II och som i den berörda medlemsstaten kan leda till fängelse eller annan frihetsberövande åtgärd under en längsta tidsperiod på minst fyra år.

Första stycket h påverkar inte artikel 9 i förordning (EU) 2016/679 vad gäller behandling av biometriska uppgifter för andra ändamål än brottsbekämpning.

2. Användningen av system för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser för brottsbekämpande ändamål för något av de syften som avses i punkt 1 första stycket h ska införas för de ändamål som anges i det ledet endast för att bekräfta identiteten på den individ som särskilt avses och ska ta hänsyn till följande faktorer:

a) Arten av den situation som ger upphov till den eventuella användningen, särskilt hur allvarlig, sannolik och omfattande skadan skulle bli om systemet inte användes.

b) Konsekvenserna av användningen av systemet för alla berörda personers rättigheter och friheter, särskilt vad gäller hur allvarliga, sannolika och omfattande dessa konsekvenser är.

Dessutom ska användningen av system för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser för brottsbekämpande ändamål för något av de syften som avses i punkt 1 första stycket h i denna artikel vara förenlig med nödvändiga och proportionella skyddsåtgärder och villkor avseende användningen i enlighet med nationell rätt som tillåter användning av dessa, särskilt vad gäller tidsmässiga och geografiska begränsningar samt personbegränsningar. Användningen av systemet för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser ska tillåtas endast om den brottsbekämpande myndigheten har slutfört en konsekvensbedömning avseende grundläggande rättigheter såsom föreskrivs i artikel 27 och har registrerat systemet i EU-databasen enligt artikel 49. I vederbörligen motiverade brådskande fall får dock användningen av sådana system påbörjas utan registrering i EU-databasen, förutsatt att denna registrering slutförs utan oskäligt dröjsmål.

3. Vid tillämpning av punkt 1 första stycket h och punkt 2 ska det för varje användning för brottsbekämpande ändamål av ett system för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser krävas ett förhandstillstånd från en rättslig myndighet eller en oberoende administrativ myndighet vars beslut är bindande i den medlemsstat där användningen ska äga rum, utfärdat på motiverad begäran och i enlighet med de närmare bestämmelser i nationell rätt som avses i punkt 5. I vederbörligen motiverade brådskande situationer får dock användningen av ett sådant system påbörjas utan tillstånd, förutsatt att ett sådant tillstånd begärs utan oskäligt dröjsmål och senast inom 24 timmar. Om ett sådant tillstånd nekas ska användningen stoppas med omedelbar verkan och alla uppgifter samt resultat och utdata som rör denna användning förstöras och raderas.

Den behöriga rättsliga myndigheten eller en oberoende administrativ myndighet vars beslut är bindande ska bevilja tillståndet endast om den, på grundval av objektiva bevis eller tydliga indikationer som lagts fram för den, har förvissat sig om att användningen av det berörda systemet för biometrisk fjärridentifiering i *realtid* är nödvändig och proportionell för att uppnå ett av de syften som anges i punkt 1 första stycket h, i enlighet med vad som anges i begäran och, i synnerhet,

förblir begränsad till vad som är strikt nödvändigt när det gäller tidsperioden samt det geografiska tillämpningsområdet och de personer som omfattas. Vid beslut om begäran ska den myndigheten beakta de faktorer som avses i punkt 2. Inget beslut som har negativa rättsliga följder för en person får fattas enbart på grundval av utdata från systemet för biometrisk fjärridentifiering i *realtid*.

4. Utan att det påverkar punkt 3 ska varje användning av ett system för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser för brottsbekämpande ändamål anmälas till den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten i enlighet med de nationella regler som avses i punkt 5. Anmälan ska åtminstone innehålla den information som specificeras enligt punkt 6 och får inte inbegripa känsliga operativa uppgifter.

5. En medlemsstat får besluta att föreskriva en möjlighet att helt eller delvis tillåta användning av system för biometrisk fjärridentifiering i *realtid* på allmänt tillgängliga platser för brottsbekämpande ändamål inom de gränser och på de villkor som anges i punkt 1 första stycket h samt punkterna 2 och 3. De berörda medlemsstaterna ska i sin nationella rätt fastställa de nödvändiga närmare reglerna för begäran om, utfärdande av och utövande av samt tillsyn över och rapportering om de tillstånd som avses i punkt 3. I dessa regler ska det också anges för vilka av de syften som förtecknas i punkt 1 första stycket h, inbegripet för vilka av de brott som avses i led h iii i den punkten, de behöriga myndigheterna kan få tillstånd att använda dessa system för brottsbekämpande ändamål. Medlemsstaterna ska till kommissionen anmäla dessa regler senast 30 dagar efter deras antagande. Medlemsstaterna får införa mer restriktiva lagar om användningen av system för biometrisk fjärridentifiering i enlighet med unionsrätten.

6. Medlemsstaternas nationella marknadskontrollmyndigheter och nationella dataskyddsmyndigheter som har underrättats om användningen av system för biometrisk fjärridentifiering i *realtid* på allmänt tillgänglig plats för brottsbekämpande ändamål enligt punkt 4 ska lämna in årliga rapporter till kommissionen om sådan användning. För detta ändamål ska kommissionen förse medlemsstaterna och de nationella marknadskontrollmyndigheterna och dataskyddsmyndigheterna med en mall som inkluderar information om antalet beslut som fattats av behöriga rättsliga myndigheter eller en oberoende administrativ myndighet vars beslut är bindande gällande ansökningar om tillstånd i enlighet med punkt 3 och resultatet av dessa.

7. Kommissionen ska offentliggöra årliga rapporter om användningen av system för biometrisk fjärridentifiering i realtid på allmänt tillgänglig plats för brottsbekämpande ändamål på grundval av aggregerade data från medlemsstaterna baserat på de årliga rapporter som avses i punkt 6. Dessa årliga rapporter får inte omfatta känsliga operativa uppgifter som rör relaterad brottsbekämpande verksamhet.

8. Denna artikel påverkar inte de förbud som är tillämpliga när ett AI-användningsområde strider mot annan unionsrätt.

KAPITEL III

AI-SYSTEM MED HÖG RISK

AVSNITT 1

Klassificering av AI-system som AI-system med hög risk

Artikel 6

Klassificeringsregler för AI-system med hög risk

1. Oavsett om ett AI-system släpps ut på marknaden eller tas i bruk oberoende av de produkter som avses i leden a och b ska detta AI-system betraktas som ett AI-system med hög risk om båda följande villkor är uppfyllda:

a) AI-systemet är avsett att användas som en säkerhetskomponent i en produkt, eller AI-systemet är i sig en produkt, som omfattas av unionens harmoniseringslagstiftning som förtecknas i bilaga I.

b) Den produkt vars säkerhetskomponent enligt led a är AI-systemet, eller själva AI-systemet som en produkt, omfattas av krav på att genomgå en tredjepartsbedömning av överensstämmelse för att den produkten ska kunna släppas ut på marknaden eller tas i bruk enligt unionens harmoniseringslagstiftning som förtecknas i bilaga I.

2. Utöver de AI-system med hög risk som avses i punkt 1 ska AI-system som avses i bilaga III också betraktas som AI-system med hög risk.

3. Genom undantag från punkt 2 ska ett AI-system som avses i bilaga III inte betraktas som ett AI-system med hög risk om det inte utgör en betydande risk för skada på fysiska personers hälsa, säkerhet eller grundläggande rättigheter, inbegripet genom att det inte materiellt påverkar resultatet av beslutsfattande.

Första stycket ska vara tillämpligt om något av följande villkor är uppfyllt:

a) AI-systemet är avsett att utföra en snäv processuell uppgift,

b) AI-systemet är avsett att förbättra resultatet av tidigare slutförd mänsklig verksamhet,

c) AI-systemet är avsett att upptäcka beslutsmönster eller avvikelser från tidigare beslutsmönster och är inte avsett att ersätta eller påverka tidigare slutförd mänsklig bedömning, utan ordentlig mänsklig granskning, eller

d) AI-systemet är avsett att utföra en förberedande uppgift för en bedömning som är relevant för de användningsfall som förtecknas i bilaga III.

Utan hinder av första stycket ska ett AI-system som avses i bilaga III alltid anses vara ett AI-system med hög risk om det utför profilering av fysiska personer.

4. En leverantör som anser att ett AI-system som avses i bilaga III inte är ett AI-system med hög risk ska upprätta dokumentation för sin bedömning innan systemet släpps ut på marknaden eller tas i bruk. Sådana leverantörer ska omfattas av de registreringsskyldigheter som föreskrivs i artikel 49.2. På begäran av nationella behöriga myndigheter ska leverantören tillhandahålla den dokumentation som legat till grund för bedömningen.

5. Efter samråd med den europeiska styrelsen för artificiell intelligens (*styrelsen*) ska kommissionen senast den 2 februari 2026 tillhandahålla riktlinjer som specificerar det praktiska genomförandet av denna artikel i överensstämmelse med artikel 96, och som innefattar en omfattande förteckning över praktiska exempel på användningsfall av AI-system som innebär hög risk och användningsfall som inte innebär hög risk.

6. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 för att ändra punkt 3 andra stycket i den här artikeln genom att lägga till nya villkor utöver dem som föreskrivs i det stycket eller genom att ändra dem, om det finns konkreta och tillförlitliga bevis på förekomst av AI-system som omfattas av tillämpningsområdet för bilaga III men som inte utgör en betydande risk för skada på fysiska personers hälsa, säkerhet eller grundläggande rättigheter.

7. Kommissionen ska anta delegerade akter i enlighet med artikel 97 för att ändra punkt 3 andra stycket i den här artikeln genom att stryka något av de villkor som föreskrivs i det stycket, om det finns konkreta och tillförlitliga bevis för att detta är nödvändigt för att upprätthålla den skyddsnivå för hälsa, säkerhet och grundläggande rättigheter som föreskrivs i denna förordning.

8. Eventuella ändringar av villkoren i punkt 3 andra stycket som antas i enlighet med punkterna 6 och 7 i denna artikel får inte sänka den allmänna skyddsnivå för hälsa, säkerhet och grundläggande rättigheter som föreskrivs i denna förordning och ska säkerställa samstämmighet med de delegerade akter som antagits enligt artikel 7.1 samt ta hänsyn till marknadsutveckling och tekniska utveckling.

Artikel 7

Ändringar av Bilaga III

1. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 med avseende på att ändra bilaga III genom att lägga till eller ändra användningsfall för AI-system med hög risk om båda följande villkor är uppfyllda:

a) AI-systemen är avsedda att användas inom något av de områden som förtecknas i bilaga III.

b) AI-systemen utgör en risk för skada på hälsa och säkerhet, eller för negativ inverkan på grundläggande rättigheter, och denna risk är likvärdig med eller större än den risk för skada eller negativ inverkan som förorsakas av de AI-system med hög risk som redan anges i bilaga III.

2. Vid bedömningen av villkoret i punkt 1 b ska kommissionen beakta följande kriterier:

a) Det avsedda ändamålet med AI-systemet.

b) I vilken utsträckning ett AI-system har använts eller sannolikt kommer att användas.

c) Typen och mängden data som behandlas och används av AI-systemet, i synnerhet huruvida särskilda kategorier av personuppgifter behandlas.

d) I vilken utsträckning AI-systemet agerar självständigt och om det är möjligt för en människa att åsidosätta ett beslut eller rekommendationer som kan leda till potentiell skada.

e) I vilken utsträckning användningen av ett AI-system redan har orsakat skada på hälsa och säkerhet, har haft negativ inverkan på grundläggande rättigheter eller har gett upphov till betydande farhågor när det gäller sannolikheten för sådan skada eller negativ inverkan, vilket till exempel framgår av rapporter eller dokumenterade anklagelser som lämnats till nationella behöriga myndigheter, eller, i förekommande fall, av andra rapporter.

f) Den potentiella omfattningen av sådan skada eller sådan negativ inverkan, särskilt i fråga om intensitet och förmåga att påverka en stor mängd personer eller att i oproportionerlig utsträckning påverka en viss grupp av personer.

g) I vilken utsträckning potentiellt skadade eller negativt påverkade personer är beroende av det resultat som producerats med ett AI-system, särskilt till följd av att det av praktiska eller juridiska skäl inte rimligen är möjligt att undantas från detta resultat.

h) I vilken utsträckning det föreligger en obalans i fråga om makt, eller potentiellt skadade eller negativt påverkade personer befinner sig i ett utsatt läge i förhållande till tillhandahållaren av ett AI-system, särskilt på grund av status, auktoritet, kunskap, ekonomiska eller sociala omständigheter eller ålder.

i) I vilken utsträckning det resultat som produceras med medverkan av ett AI-system är lätt att korrigera eller upphäva, med beaktande av tillgängliga tekniska lösningar som möjliggör dess korrigering eller upphävande, varvid resultat med en negativ påverkan på hälsa, säkerhet eller grundläggande rättigheter inte ska anses vara lätta att korrigera eller upphäva.

j) Omfattningen av och sannolikheten för nyttan med införandet av AI-systemet för enskilda personer, grupper eller samhället i stort, inbegripet eventuella förbättringar av produktsäkerheten.

k) I vilken utsträckning befintlig unionsrätt föreskriver

   i) effektiva åtgärder för rättslig prövning med hänsyn till de risker som ett AI-system medför, med undantag för skadeståndsanspråk,

   ii) effektiva åtgärder för att förebygga eller avsevärt minimera dessa risker.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 med avseende på att ändra förteckningen i bilaga III genom att låta AI-system med hög risk utgå om båda följande villkor är uppfyllda:

a) Det berörda AI-systemet medför inte längre någon betydande risk för grundläggande rättigheter, hälsa eller säkerhet, med beaktande av kriterierna i punkt 2.

b) Strykningen sänker inte den övergripande nivån på skyddet för hälsa, säkerhet och grundläggande rättigheter enligt unionsrätten.

AVSNITT 2

Krav på AI-system med hög risk

Artikel 8

Förenlighet med kraven

1. AI-system med hög risk ska uppfylla kraven i detta avsnitt, med beaktande av deras avsedda ändamål samt den allmänt erkända senaste utvecklingen inom AI och AI-relaterad teknik. Det riskhanteringssystem som avses i artikel 9 ska beaktas när förenligheten med dessa krav säkerställs.

2. Om en produkt innehåller ett AI-system som omfattas av kraven i denna förordning och kraven i unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I, ska leverantörer ansvara för att säkerställa att deras produkt uppfyller alla tillämpliga krav i tillämplig unionsharmoniseringslagstiftning. Vid säkerställandet av att AI-system med hög risk som avses i punkt 1 överensstämmer med kraven i detta avsnitt, och för att säkerställa samstämmighet, motverka dubbelarbete och minimera ytterligare bördor, ska leverantörer kunna välja att, beroende på vad som är lämpligt, integrera de nödvändiga test- och rapporteringsprocesserna, den information och den dokumentation som de tillhandahåller med avseende på sin produkt i dokumentation och förfaranden som redan finns och som krävs enligt unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I.

Artikel 9

Riskhanteringssystem

1. Ett riskhanteringssystem ska inrättas, genomföras, dokumenteras och underhållas för AI-system med hög risk.

2. Riskhanteringssystemet ska förstås som en kontinuerlig iterativ process som planeras och löper under hela livscykeln för ett AI-system med hög risk, med krav på regelbunden och systematisk översyn och uppdatering. Det ska innehålla följande steg:

a) Identifiering och analys av de kända och rimligen förutsebara risker som AI-systemet med hög risk kan medföra för hälsa, säkerhet och grundläggande rättigheter när AI-systemet med hög risk används i enlighet med sitt avsedda ändamål.

b) Uppskattning och utvärdering av de risker som kan uppstå när AI-systemet med hög risk används i enlighet med sitt avsedda ändamål och under förhållanden där det kan förekomma rimligen förutsebar felaktig användning.

c) Utvärdering av andra risker som eventuellt kan uppstå på grundval av en analys av data som samlats in från det system för övervakning efter utsläppande på marknaden som avses i artikel 72.

d) Antagande av lämpliga och riktade riskhanteringsåtgärder utformade för att hantera de risker som identifierats enligt led a.

3. De risker som avses i denna artikel ska endast avse de risker som rimligen kan begränsas eller elimineras genom utveckling eller utformning av AI-systemet med hög risk eller tillhandahållande av adekvat teknisk information.

4. I de riskhanteringsåtgärder som avses i punkt 2 d ska vederbörlig hänsyn tas till de effekter och den möjliga interaktion som följer av den kombinerade tillämpningen av kraven i detta avsnitt, i syfte att minimera riskerna mer effektivt och samtidigt uppnå en lämplig balans i genomförandet av åtgärderna för att uppfylla dessa krav.

5. De riskhanteringsåtgärder som avses i punkt 2 d ska vara sådana att relevanta kvarvarande risker förknippade med varje fara samt den totala kvarvarande risken i AI-systemen med hög risk bedöms vara acceptabla.

Vid fastställandet av de lämpligaste riskhanteringsåtgärderna ska följande säkerställas:

a) Eliminering eller minskning av risker som identifierats och utvärderats enligt punkt 2 så långt som tekniskt möjligt genom lämplig konstruktion och utveckling av AI-systemet med hög risk.

b) När det är lämpligt, genomförande av lämpliga begränsnings- och kontrollåtgärder för att hantera risker som inte kan elimineras.

c) Tillhandahållande av den information som krävs enligt artikel 13 och, i förekommande fall, utbildning för tillhandahållare.

För att eliminera eller minska risker i samband med användningen av AI-systemet med hög risk ska vederbörlig hänsyn tas till den tekniska kunskap, erfarenhet och utbildning som tillhandahållaren förväntas ha och det förmodade sammanhang i vilket systemet är avsett att användas.

6. AI-system med hög risk ska testas i syfte att identifiera de lämpligaste och bäst riktade riskhanteringsåtgärderna. Testerna ska säkerställa att AI-system med hög risk fungerar konsekvent för sitt avsedda ändamål och att de uppfyller kraven i detta avsnitt.

7. Testningsförfarandena får omfatta testning under verkliga förhållanden i enlighet med artikel 60.

8. Testning av AI-systemen med hög risk ska utföras, beroende på vad som är lämpligt, när som helst under hela utvecklingsprocessen och i alla händelser innan de släpps ut på marknaden eller tas i bruk. Testning ska utföras på grundval av i förväg definierade mått och sannolikhetsgränser som är lämpliga för det avsedda ändamålet med AI-systemet med hög risk.

9. Vid genomförandet av det riskhanteringssystem som föreskrivs i punkterna 1–7 ska leverantörer ta hänsyn till huruvida AI-systemet med hög risk, med tanke på dess avsedda ändamål, sannolikt kommer att ha en negativ påverkan på personer som är yngre än 18 år och, i förekommande fall, andra sårbara grupper.

10. För leverantörer av AI-system med hög risk som omfattas av krav avseende interna riskhanteringsprocesser enligt andra relevanta bestämmelser i unionsrätten får de aspekter som regleras i punkterna 1–9 ingå i, eller kombineras med, de riskhanteringsförfaranden som fastställs enligt den unionsrätten.

Artikel 10

Data och dataförvaltning

1. AI-system med hög risk som använder teknik som inbegriper träning av AI-modeller med data ska utvecklas på grundval av tränings-, validerings- och testdataset som uppfyller de kvalitetskriterier som avses i punkterna 2–5 när sådana dataset används.

2. Tränings-, validerings- och testdataset ska omfattas av metoder för dataförvaltning och datahantering som är lämpliga för det avsedda ändamålet med AI-systemet med hög risk. Dessa metoder ska särskilt avse

a) relevanta utformningsval,

b) datainsamlingsprocesser och uppgifternas ursprung samt, när det gäller personuppgifter, datainsamlingens ursprungliga ändamål,

c) relevanta åtgärder för datapreparering, såsom annotation, märkning, rensning, uppdatering, förädling och aggregering,

d) formulering av antaganden, särskilt när det gäller den information som berörda data förväntas beskriva och representera,

e) en bedömning av tillgängligheten, mängden och lämpligheten avseende de dataset som behövs,

f) undersökning med avseende på eventuella biaser som sannolikt kommer att påverka människors hälsa och säkerhet, inverka negativt på grundläggande rättigheter eller leda till diskriminering som är förbjuden enligt unionsrätten, särskilt när utdata påverkar indata för framtida drift,

g) lämpliga åtgärder för att upptäcka, förebygga och begränsa eventuella biaser som identifierats enligt led f,

h) identifiering av relevanta dataluckor eller brister som hindrar efterlevnad av denna förordning, och hur dessa luckor och brister kan åtgärdas.

3. Tränings-, validerings- och testdataset ska vara relevanta, tillräckligt representativa, och så långt som möjligt fria från fel och fullständiga i förhållande till det avsedda ändamålet. De ska ha lämpliga statistiska egenskaper, inbegripet, i förekommande fall, vad gäller de personer eller grupper av personer med avseende på vilka AI-systemet med hög risk är avsett att användas. Egenskaperna hos dessa dataset kan uppfyllas på nivån för enskilda dataset eller på nivån av en kombination av dessa.

4. Dataseten ska, i den mån som krävs med hänsyn till det avsedda ändamålet, beakta de egenskaper eller element som är utmärkande för just den specifika geografiska, kontextuella, beteendemässiga eller funktionsmässiga situation där AI-systemet med hög risk är avsett att användas.

5. I den utsträckning det är absolut nödvändigt för att säkerställa upptäckt och korrigering av bias i samband med AI-systemen med hög risk i enlighet med punkt 2 f och g i denna artikel får leverantörer av sådana system undantagsvis behandla särskilda kategorier av personuppgifter, med förbehåll för lämpliga skyddsåtgärder för fysiska personers grundläggande rättigheter och friheter. Utöver bestämmelserna i förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680 måste samtliga följande villkor vara uppfyllda för att sådan behandling ska kunna äga rum:

a) Upptäckt och korrigering av bias kan inte uppnås på ett effektivt sätt genom behandling av andra data, inbegripet syntetiska eller anonymiserade data.

b) De särskilda kategorierna av personuppgifter omfattas av tekniska begränsningar för vidareutnyttjande av personuppgifter samt säkerhetsåtgärder och integritetsbevarande åtgärder på en nivå som motsvarar den senaste utvecklingen, inbegripet pseudonymisering.

c) De särskilda kategorierna av personuppgifter omfattas av åtgärder för att säkerställa att de personuppgifter som behandlas är säkra, skyddade, omfattas av lämpliga skyddsåtgärder, inbegripet strikta kontroller och dokumentation av åtkomsten, för att undvika missbruk och säkerställa att endast personer som är behöriga har tillgång till dessa personuppgifter med lämpliga konfidentialitetsskyldigheter.

d) De särskilda kategorierna av personuppgifter får inte översändas, överföras eller på annat sätt göras tillgängliga för andra parter.

e) De särskilda kategorierna av personuppgifter raderas när biasen har korrigerats eller personuppgifternas lagringstid har löpt ut, beroende på vilket som inträffar först.

f) Registren över behandling enligt förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680 innehåller skälen till varför behandlingen av särskilda kategorier av personuppgifter var absolut nödvändig för att upptäcka och korrigera biaser och varför detta mål inte kunde uppnås genom behandling av andra data.

6. För utvecklingen av AI-system med hög risk som inte använder teknik som inbegriper träning av AI-modeller är punkterna 2–5 endast tillämpliga på testdataset.

Artikel 11

Teknisk dokumentation

1. Den tekniska dokumentationen för ett AI-system med hög risk ska upprättas innan systemet släpps ut på marknaden eller tas i bruk och ska hållas uppdaterad.

Den tekniska dokumentationen ska upprättas på ett sådant sätt att det visas att AI-systemet med hög risk är förenligt med kraven i detta avsnitt, och så att nationella behöriga myndigheter och anmälda organ får den information som krävs i klar och begriplig form för att bedöma om AI-systemet uppfyller dessa krav. Den ska minst innehålla de delar som anges i bilaga IV. Små och medelstora företag, inbegripet uppstartsföretag, får tillhandahålla de delar av den tekniska dokumentation som anges i bilaga IV på ett förenklat sätt. För detta ändamål ska kommissionen upprätta ett förenklat formulär för teknisk dokumentation som är inriktat på små företags och mikroföretags behov. Om ett litet eller medelstort företag, inbegripet ett uppstartsföretag, väljer att tillhandahålla den information som krävs enligt bilaga IV på ett förenklat sätt ska det använda det formulär som avses i denna punkt. Anmälda organ ska godta formuläret för bedömning av överensstämmelse.

2. Om ett AI-system med hög risk som är kopplat till en produkt, som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I, släpps ut på marknaden eller tas i bruk ska en enda teknisk uppsättning dokumentation upprättas som innehåller all den information som anges i punkt 1 samt den information som krävs enligt dessa rättsakter.

3. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 för att ändra bilaga IV när så krävs för att säkerställa att den tekniska dokumentationen, mot bakgrund av teknisk utveckling, innehåller all information som krävs för att bedöma systemets förenlighet med kraven i detta avsnitt.

Artikel 12

Loggning

1. AI-system med hög risk ska tekniskt möjliggöra automatisk registrering av händelser (loggar) under hela systemets livstid.

2. För att säkerställa en spårbarhetsnivå för funktionen hos ett AI-system med hög risk som är lämplig för systemets avsedda ändamål ska loggningskapaciteten möjliggöra registrering av händelser som är relevanta för

a) identifiering av situationer som kan resultera i att AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 eller i en väsentlig ändring,

b) underlättande av den övervakning efter utsläppande på marknaden som avses i artikel 72, och

c) övervakning av driften av AI-system med hög risk som avses i artikel 26.5.

3. För AI-system med hög risk som avses i punkt 1 a i bilaga III ska loggningsfunktionerna åtminstone tillhandahålla följande:

a) Registrering av perioden för varje användning av systemet (startdatum och starttidpunkt samt slutdatum och sluttidpunkt för varje användning).

b) Den referensdatabas mot vilken indata har kontrollerats av systemet.

c) Indata för vilka sökningen har lett till en träff.

d) Identifiering av de fysiska personer som deltar i kontrollen av resultaten enligt artikel 14.5.

Artikel 13

Transparens och tillhandahållande av information till tillhandahållare

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt att driften av dem är tillräckligt transparent för att tillhandahållare ska kunna tolka systemets utdata och använda dem på lämpligt sätt. En lämplig typ och grad av transparens ska säkerställas, i syfte att uppnå uppfyllelse av leverantörens och tillhandahållarens relevanta skyldigheter enligt avsnitt 3.

2. AI-system med hög risk ska åtföljas av en bruksanvisning i ett lämpligt digitalt eller annat format som inbegriper kortfattad, fullständig, korrekt och tydlig information som är relevant, tillgänglig och begriplig för tillhandahållare.

3. Bruksanvisningen ska minst innehålla följande information:

a) Identitet och kontaktuppgifter för leverantören och i tillämpliga fall för dennes ombud.

b) Egenskaperna, kapaciteten och prestandabegränsningarna hos AI-systemet med hög risk, inbegripet

i) dess avsedda ändamål,

ii) den nivå avseende riktighet, inbegripet mätningarna av denna, robusthet och cybersäkerhet som avses i artikel 15 mot vilken AI-systemet med hög risk har testats och validerats och som kan förväntas, samt alla kända och förutsebara omständigheter som kan påverka den förväntade riktighets-, robusthets- och cybersäkerhetsnivån,

iii) varje känd eller förutsebar omständighet, som har samband med användningen av AI-systemet med hög risk i enlighet med dess avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, som kan leda till risker för hälsa och säkerhet eller grundläggande rättigheter som avses i artikel 9.2,

iv) i tillämpliga fall, den tekniska kapaciteten och de tekniska egenskaperna hos AI-systemet med hög risk med avseende på att tillhandahålla information som är relevant för att förklara dess utdata,

v) när så är lämpligt, dess prestanda vad gäller specifika personer eller grupper av personer som omfattas av den avsedda användningen av systemet,

vi) i tillämpliga fall, specifikationer för indata, eller annan relevant information i fråga om de tränings-, valideringS- och testdataset som används, med beaktande av det avsedda ändamålet för AI-systemet med hög risk.

vii) i tillämpliga fall, information som gör det möjligt för tillhandahållare att tolka utdata från AI-systemet med hög risk och använda dem på lämpligt sätt.

c) Eventuella ändringar av AI-systemet med hög risk och dess prestanda som leverantören på förhand har fastställt vid tidpunkten för den inledande bedömningen av överensstämmelse.

d) De åtgärder för mänsklig kontroll som avses i artikel 14, inbegripet de tekniska åtgärder som införts för att underlätta tillhandahållarnas tolkning av utdata från AI-systemet med hög risk.

e) De data- och maskinvaruresurser som krävs, den förväntade livstiden för AI-systemet med hög risk och alla nödvändiga underhålls- och omsorgsåtgärder, inbegripet deras frekvens, för att säkerställa att AI-systemet fungerar korrekt, även när det gäller programvaruuppdateringar.

f) I förekommande fall, en beskrivning av de mekanismer som ingår i AI-systemet med hög risk vilka gör det möjligt för tillhandahållarna att korrekt samla in, lagra och tolka loggarna i enlighet med artikel 12.

Artikel 14

Mänsklig kontroll

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt, inbegripet med lämpliga verktyg för människa–maskin-gränssnitt, att fysiska personer på ett effektivt sätt kan utöva kontroll över dem när de används.

2. Mänsklig kontroll ska syfta till att förebygga eller minimera de risker för hälsa, säkerhet eller grundläggande rättigheter som kan uppstå när ett AI-system med hög risk används i enlighet med sitt avsedda ändamål eller under förhållanden där det kan förekomma rimligen förutsebar felaktig användning, särskilt när sådana risker kvarstår trots tillämpningen av andra krav i detta avsnitt.

3. Tillsynsåtgärderna ska stå i proportion till riskerna, graden av autonomi och användningssammanhang för AI-systemet med hög risk, och ska säkerställas genom en eller båda av följande typer av åtgärder:

a) Åtgärder som leverantören har fastställt och, när det är tekniskt möjligt, byggt in i AI-systemet med hög risk innan det släpps ut på marknaden eller tas i bruk.

b) Åtgärder som leverantörer har fastställt innan AI-systemet med hög risk släpps ut på marknaden eller tas i bruk och som är lämpliga att genomföras av tillhandahållaren.

4. Vid genomförandet av punkterna 1, 2 och 3 ska AI-systemet med hög risk tillhandahållas tillhandahållaren på ett sådant sätt att fysiska personer som fått i uppdrag att utöva mänsklig kontroll ges möjlighet, enligt vad som är lämpligt och proportionellt, att

a) korrekt förstå den relevanta kapaciteten och begränsningarna hos AI-systemet med hög risk och på vederbörligt sätt kunna övervaka dess drift, bland annat i syfte att upptäcka och ta itu med avvikelser, funktionsstörningar och oväntad prestanda,

b) förbli medvetna om den möjliga tendensen att automatiskt eller i alltför hög grad lita på de utdata som produceras av ett AI-system med hög risk (automation bias), särskilt när det gäller AI-system med hög risk som används för att tillhandahålla information eller rekommendationer för beslut som ska fattas av fysiska personer,

c) korrekt kunna tolka utdata från AI-systemet med hög risk, med beaktande av till exempel tillgängliga tolkningsverktyg och tolkningsmetoder,

d) i vissa situationer besluta att inte använda AI-systemet med hög risk eller på annat sätt bortse från, åsidosätta eller reversera de resultat som AI-systemet med hög risk genererar,

e) ingripa i driften av AI-systemet med hög risk eller stoppa systemet med en *stoppknapp* eller ett liknande förfarande som gör det möjligt för systemet att stoppas i ett säkert läge.

5. För AI-system med hög risk som avses i punkt 1 a i bilaga III ska de åtgärder som avses i punkt 3 i denna artikel dessutom vara sådana att de säkerställer att ingen åtgärd och inget beslut vidtas respektive fattas av tillhandahållaren på grundval av den identifiering som systemet resulterar i, såvida inte denna identifiering har kontrollerats och bekräftats separat av minst två fysiska personer med nödvändig kompetens, utbildning och auktoritet.

Kravet på en separat kontroll av minst två fysiska personer är inte tillämpligt på AI-system med hög risk som används inom områdena brottsbekämpning, migration, gränskontroll eller asyl, om en tillämpning av detta krav enligt unionsrätten eller nationell rätt skulle betraktas som oproportionell.

Artikel 15

Riktighet, robusthet och cybersäkerhet

1. AI-system med hög risk ska utformas och utvecklas på ett sådant sätt att de uppnår en lämplig nivå avseende riktighet, robusthet och cybersäkerhet och presterar väl i dessa avseenden under hela sin livscykel.

2. För att hantera de tekniska aspekterna av hur de lämpliga nivåer av riktighet och robusthet som anges i punkt 1 och andra relevanta prestandamått mäts ska kommissionen i samarbete med relevanta berörda parter och organisationer, såsom metrologi- och riktmärkningsmyndigheter, vid behov, uppmuntra utvecklingen av riktmärken och mätmetoder.

3. Riktighetsnivåerna och relevanta riktighetsmått för AI-system med hög risk ska anges i de medföljande bruksanvisningarna.

4. AI-system med hög risk ska vara så resilienta som möjligt mot felaktigheter, funktionsfel eller inkonsekvenser som kan uppstå inom det system eller den miljö där systemet är i drift, särskilt på grund av deras interaktion med fysiska personer eller andra system. Tekniska och organisatoriska åtgärder ska vidtas i detta avseende.

Robustheten hos AI-system med hög risk kan uppnås genom lösningar med teknisk redundans, som kan omfatta backup eller felsäkra planer.

AI-system med hög risk som fortsätter att lära sig efter det att de har släppts ut på marknaden eller tagits i bruk ska utvecklas på ett sådant sätt att risken för att eventuella biaser i utdata påverkar indata för framtida drift (återföring) elimineras eller minskas så mycket som möjligt och så att det säkerställs att sådan återföring hanteras på vederbörligt sätt med lämpliga kompenserande åtgärder.

5. AI-system med hög risk ska vara resilienta mot försök av obehöriga tredje parter att ändra deras användning, utdata eller prestanda genom att utnyttja systemets sårbarheter.

De tekniska lösningar som syftar till att säkerställa cybersäkerhet i AI-system med hög risk ska vara anpassade till de relevanta omständigheterna och riskerna.

De tekniska lösningarna för att hantera AI-specifika sårbarheter ska, när det är lämpligt, inbegripa åtgärder för att förebygga, upptäcka, reagera på, komma till rätta med och bekämpa attacker som försöker manipulera träningsdatasetet (*dataförgiftning*) eller förtränade komponenter som används i träningen (*modellförgiftning*), indata som är utformade för att få AI-modellen att göra ett misstag (*antagonistiska exempel* eller *modellkringgående*), sekretessangrepp eller modellfel.

AVSNITT 3

Skyldigheter för leverantörer och tillhandahållare av AI-system med hög risk samt andra parter

Artikel 16

Skyldigheter för leverantörer av AI-system med hög risk

Leverantörer av AI-system med hög risk ska

a) säkerställa att deras AI-system med hög risk uppfyller kraven i avsnitt 2,

b) på AI-systemet med hög risk eller, om detta inte är möjligt, på dess förpackning eller i dess åtföljande dokumentation, beroende på vad som är tillämpligt, ange sitt namn, registrerade firmanamn eller registrerade varumärke, den adress där de kan kontaktas,

c) ha ett kvalitetsstyrningssystem som uppfyller kraven i artikel 17,

d) förvara den dokumentation som avses i artikel 18,

e) spara de loggar som genereras automatiskt av deras AI-system med hög risk enligt artikel 19, när loggarna står under deras kontroll,

f) säkerställa att AI-systemet med hög risk genomgår det relevanta förfarande för bedömning av överensstämmelse som avses i artikel 43 innan det släpps ut på marknaden eller tas i bruk,

g) utarbeta en EU-försäkran om överensstämmelse i enlighet med artikel 47,

h) anbringa CE-märkningen på AI-systemet med hög risk eller, om detta inte är möjligt, på dess förpackning eller i dess åtföljande dokumentation, för att påvisa överensstämmelse med denna förordning i enlighet med artikel 48,

i) fullgöra de registreringsskyldigheter som avses i artikel 49.1,

j) vidta nödvändiga korrigerande åtgärder och tillhandahålla den information som krävs enligt artikel 20,

k) på motiverad begäran av en nationell behörig myndighet visa att AI-systemet med hög risk uppfyller kraven i avsnitt 2,

l) säkerställa att AI-systemet med hög risk uppfyller tillgänglighetskraven i enlighet med direktiven (EU) 2016/2102 och (EU) 2019/882.

Artikel 17

Kvalitetsstyrningssystem

1. Leverantörer av AI-system med hög risk ska inrätta ett kvalitetsstyrningssystem som säkerställer efterlevnad av denna förordning. Systemet ska dokumenteras på ett systematiskt och ordnat sätt i form av skriftliga riktlinjer, förfaranden och instruktioner och ska omfatta åtminstone följande aspekter:

a) En strategi för efterlevnad av regelverket, inklusive efterlevnad av förfaranden för bedömning av överensstämmelse och för hantering av ändringar av AI-systemet med hög risk.

b) Tekniker, förfaranden och systematiska åtgärder som ska användas för utformning av AI-systemet med hög risk samt för kontroll och verifikation av utformningen.

c) Tekniker, förfaranden och systematiska åtgärder som ska användas för utveckling, kvalitetskontroll och kvalitetssäkring av AI-systemet med hög risk.

d) Undersöknings-, test- och valideringsförfaranden som ska utföras före, under och efter utvecklingen av AI-systemet med hög risk och hur ofta de ska utföras.

e) Tekniska specifikationer, inbegripet standarder, som ska tillämpas och, om de relevanta harmoniserade standarderna inte tillämpas fullt ut, eller inte omfattar alla relevanta krav i avsnitt 2, de medel som ska användas för att säkerställa att AI-systemet med hög risk uppfyller dessa krav.

f) System och förfaranden för datahantering, inbegripet datafångst, datainsamling, dataanalys, datamärkning, datalagring, datafiltrering, datautvinning, dataaggregering, lagring av uppgifter och varje annan åtgärd som avser data och som utförs före och med avseende på utsläppandet på marknaden eller ibruktagandet av AI-system med hög risk.

g) Det riskhanteringssystem som avses i artikel 9.

h) Upprättande, genomförande och underhåll av ett system för övervakning efter utsläppande på marknaden i enlighet med artikel 72.

i) Förfaranden som berör rapportering av en allvarlig incident i enlighet med artikel 73.

j) Hantering av kommunikation med nationella behöriga myndigheter, andra relevanta myndigheter, inbegripet de som tillhandahåller eller stöder tillgången till uppgifter, anmälda organ, andra operatörer, kunder eller andra berörda parter.

k) System och förfaranden för arkivering av all relevant dokumentation och information.

l) Resurshantering, inbegripet åtgärder som berör försörjningstrygghet.

m) En ram för ansvarsutkrävande som fastställer ledningens och övrig personals ansvar vad gäller samtliga aspekter som anges i denna punkt.

2. Genomförandet av de aspekter som avses i punkt 1 ska stå i proportion till storleken på leverantörens organisation. Leverantörer ska i alla händelser iaktta den grad av noggrannhet och den skyddsnivå som krävs för att säkerställa att deras AI-system med hög risk står i överensstämmelse med denna förordning.

3. Leverantörer av AI-system med hög risk som omfattas av skyldigheter avseende kvalitetsstyrningssystem eller en likvärdig funktion enligt relevant sektorsspecifik unionsrätt får inkludera de aspekter som anges i punkt 1 i de kvalitetsstyrningssystem som fastställs enligt den unionsrätten.

4. För leverantörer som är finansinstitut som omfattas av krav avseende interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster ska skyldigheten att införa ett kvalitetsstyrningssystem, med undantag för punkt 1 g, h och i) i denna artikel, anses vara uppfylld genom att reglerna om interna styrelseformer, arrangemang eller processer efterlevs enligt relevant unionsrätt om finansiella tjänster. I detta syfte ska alla harmoniserade standarder som avses i artikel 40 beaktas.

Artikel 18

Bevarande av dokumentation

1. Leverantören ska under en period på 10 år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk, för de nationella behöriga myndigheternas räkning hålla tillgängligt

a) den tekniska dokumentation som avses i punkt 11,

b) den dokumentation avseende kvalitetsstyrningssystemet som det hänvisas till i artikel 17,

c) i tillämpliga fall, dokumentation om de ändringar som godkänts av anmälda organ,

d) i tillämpliga fall, de beslut och andra handlingar som utfärdats av de anmälda organen,

e) EU-försäkran om överensstämmelse enligt artikel 47.

2. Varje medlemsstat ska fastställa på vilka villkor den dokumentation som avses i punkt 1 ska hållas tillgänglig för de nationella behöriga myndigheterna under den period som anges i den punkten i de fall då en leverantör eller dennes ombud som är etablerad på dess territorium går i konkurs eller upphör med sin verksamhet före utgången av denna period.

3. Leverantörer som är finansinstitut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster ska bevara den tekniska dokumentationen som en del av den dokumentation som ska bevaras enligt relevant unionsrätt om finansiella tjänster.

Artikel 19

Automatiskt genererade loggar

1. Leverantörer av AI-system med hög risk ska spara de loggar enligt artikel 12.1 som genereras automatiskt av deras AI-system med hög risk, i den mån sådana loggar står under deras kontroll. Utan att det påverkar tillämplig unionsrätt eller nationell rätt ska loggarna sparas under en period som är lämplig för det avsedda ändamålet med AI-systemet med hög risk, dock i minst sex månader, om inte annat föreskrivs i tillämplig unionsrätt eller nationell rätt, i synnerhet unionsrätten om skydd av personuppgifter.

2. Leverantörer som är finansinstitut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster ska bevara de loggar som genereras automatiskt av deras AI-system med hög risk som en del av den dokumentation som ska bevaras enligt relevant rätt om finansiella tjänster.

Artikel 20

Korrigerande åtgärder och informationsplikt

1. Leverantörer av AI-system med hög risk som anser eller har skäl att tro att ett AI-system med hög risk som de har släppt ut på marknaden eller tagit i bruk inte överensstämmer med denna förordning ska omedelbart vidta de korrigerande åtgärder som krävs för att, beroende på vad som är lämpligt, få systemet att överensstämma med kraven, dra tillbaka det, inaktivera det eller återkalla det. De ska underrätta distributörerna av det berörda AI-systemet med hög risk och, i förekommande fall, tillhandahållarna, ombudet och importörerna om detta.

2. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 och leverantören blir medveten om denna risk, ska den omedelbart utreda orsakerna, i samarbete med den rapporterande tillhandahållaren, i tillämpliga fall, och informera de marknadskontrollmyndigheter som är behöriga för det berörda AI-systemet med hög risk och, i tillämpliga fall, det anmälda organ som utfärdat ett intyg för detta AI-system med hög risk i enlighet med artikel 44, särskilt om typen av bristande överensstämmelse och om eventuella relevanta korrigerande åtgärder som vidtagits.

Artikel 21

Samarbete med behöriga myndigheter

1. Leverantörer av AI-system med hög risk ska på motiverad begäran av en behörig myndighet förse den myndigheten med all information och dokumentation som krävs för att visa att AI-systemet med hög risk överensstämmer med kraven i avsnitt 2, på ett språk som är lätt att förstå för myndigheten och som är ett av unionsinstitutionernas officiella språk som anges av den berörda medlemsstaten.

2. På motiverad begäran av en behörig myndighet ska leverantörer också ge den begärande behöriga myndigheten, i tillämpliga fall, tillgång till de automatiskt genererade loggar för AI-systemet med hög risk som avses i artikel 12.1, i den mån sådana loggar står under deras kontroll.

3. All information som en behörig myndighet har erhållit enligt denna artikel ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

Artikel 22

Ombud för leverantörer av AI-system med hög risk

1. Innan leverantörer etablerade i tredjeländer tillhandahåller sina AI-system med hög risk på unionsmarknaden ska de genom skriftlig fullmakt utse ett ombud som är etablerat i unionen.

2. Leverantören ska göra det möjligt för sitt ombud att utföra de uppgifter som anges i fullmakten från leverantören.

3. Ombudet ska utföra de uppgifter som anges i fullmakten från leverantören. Ombudet ska på begäran lämna en kopia av fullmakten till marknadskontrollmyndigheterna på ett av unionsinstitutionernas officiella språk som anges av den behöriga myndigheten. Vid tillämpning av denna förordning ska fullmakten ge ombudet befogenhet att utföra följande uppgifter:

a) Kontrollera att den EU-försäkran om överensstämmelse som avses i artikel 47 och den tekniska dokumentation som avses i artikel 11 har upprättats och att leverantören har utfört ett lämpligt förfarande för bedömning av överensstämmelse.

b) Under en period på tio år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk hålla kontaktuppgifterna till den leverantör som utsåg ombudet, en kopia av den EU-försäkran om överensstämmelse som avses i artikel 47, den tekniska dokumentationen och, i tillämpliga fall, det intyg som utfärdats av det anmälda organet tillgängliga för de behöriga myndigheter och nationella myndigheter eller organ som avses i artikel 74.10.

c) På motiverad begäran ge en behörig myndighet all information och dokumentation, inbegripet den som avses i led b i detta stycke, som är nödvändig för att visa att ett AI-system med hög risk överensstämmer med kraven i avsnitt 2, inbegripet tillgång till de loggar enligt artikel 12.1 som automatiskt genereras av AI-systemet med hög risk, i den mån sådana loggar står under leverantörens kontroll.

d) På motiverad begäran samarbeta med behöriga myndigheter i eventuella åtgärder som dessa vidtar med avseende på AI-systemet med hög risk, i synnerhet för att minska och begränsa de risker som AI-systemet med hög risk utgör.

e) I tillämpliga fall, fullgöra de registreringsskyldigheter som avses i artikel 49.1 eller, om registreringen utförs av leverantören själv, säkerställa att den information som avses i avsnitt A punkt 3 i bilaga VIII är korrekt.

Fullmakten ska ge ombudet befogenhet att utöver eller i stället för leverantören stå till förfogande inför de behöriga myndigheterna, i alla frågor som rör efterlevnaden av denna förordning.

4. Ombudet ska säga upp fullmakten om denne anser eller har skäl att tro att leverantören agerar i strid med sina skyldigheter enligt denna förordning. I sådana fall ska det omedelbart underrätta den berörda marknadskontrollmyndigheten samt, i tillämpliga fall, det berörda anmälda organet om uppsägningen av fullmakten och skälen till detta.

Artikel 23

Importörers skyldigheter

1. Innan importörer släpper ut ett AI-system med hög risk på marknaden ska de säkerställa att systemet överensstämmer med denna förordning genom att kontrollera att

a) det tillämpliga förfarandet för bedömning av överensstämmelse enligt artikel 43 har utförts av leverantören av AI-systemet med hög risk,

b) leverantören har upprättat den tekniska dokumentationen i enlighet med artikel 11 och bilaga IV,

c) systemet är försett med erforderlig CE-märkning och åtföljs av den EU-försäkran om överensstämmelse som avses i artikel 47 och bruksanvisning,

d) leverantören har utsett ett ombud i enlighet med artikel 22.1.

2. Om en importör har tillräckliga skäl att tro att ett AI-system med hög risk inte överensstämmer med denna förordning, är förfalskat eller åtföljs av förfalskad dokumentation får den inte släppa ut systemet på marknaden förrän det har bringats i överensstämmelse med kraven. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 ska importören informera leverantören av systemet, ombudet och marknadskontrollmyndigheterna om detta.

3. Importörer ska ange sitt namn, sitt registrerade firmanamn eller sitt registrerade varumärke och en kontaktadress på AI-systemet med hög risk och på dess förpackning eller i dess åtföljande dokumentation, i tillämpliga fall.

4. Importörer ska så länge de har ansvar för ett AI-system med hög risk säkerställa att lagrings- eller transportförhållanden, i förekommande fall, inte äventyrar dess överensstämmelse med kraven i avsnitt 2.

5. Importörer ska under en period på tio år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk bevara en kopia av det intyg som utfärdats av det anmälda organet, i tillämpliga fall, av bruksanvisningen och av den EU-försäkran om överensstämmelse som avses i artikel 47.

6. Importörer ska på motiverad begäran ge berörda behöriga myndigheter all information och dokumentation som är nödvändig, inbegripet den som avses i punkt 5, för att visa att ett AI-system med hög risk överensstämmer med kraven i avsnitt 2 på ett språk som lätt kan förstås av dem. I detta syfte ska de också säkerställa att den tekniska dokumentationen kan göras tillgänglig för dessa myndigheter.

7. Importörer ska samarbeta med de berörda behöriga myndigheterna i alla åtgärder som dessa myndigheter vidtar med avseende på ett AI-system med hög risk som importörerna har släppt ut på marknaden, i synnerhet för att minska och begränsa de risker som det utgör.

Artikel 24

Distributörers skyldigheter

1. Innan distributörer tillhandahåller ett AI-system med hög risk på marknaden ska de kontrollera att det är försett med erforderlig CE-märkning, att det åtföljs av en kopia av den EU-försäkran om överensstämmelse som avses i artikel 47 och bruksanvisningen och att leverantören och importören av det systemet, beroende på vad som är tillämpligt, har uppfyllt sina respektive skyldigheter enligt artiklarna 16 b och c samt 23.3.

2. Om en distributör – på grundval av den information som denne har kännedom om – anser eller har skäl att tro att ett AI-system med hög risk inte överensstämmer med kraven i avsnitt 2, får distributören inte tillhandahålla AI-systemet med hög risk på marknaden förrän systemet har bringats i överensstämmelse med dessa krav. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 ska distributören dessutom informera leverantören eller importören av systemet, beroende på vad som är tillämpligt, om detta.

3. Distributörer ska så länge de har ansvar för ett AI-system med hög risk säkerställa att lagrings- eller transportförhållanden, i förekommande fall, inte äventyrar systemets överensstämmelse med kraven i avsnitt 2.

4. En distributör som – på grundval av den information som denne har kännedom om – anser eller har skäl att tro att ett AI-system med hög risk som denne har tillhandahållit på marknaden inte överensstämmer med kraven i avsnitt 2 ska vidta de korrigerande åtgärder som krävs för att bringa systemet i överensstämmelse med dessa krav, dra tillbaka det eller återkalla det, eller ska säkerställa att leverantören, importören eller någon berörd operatör, beroende på vad som är lämpligt, vidtar dessa korrigerande åtgärder. Om AI-systemet med hög risk utgör en risk i den mening som avses i artikel 79.1 ska distributören omedelbart informera leverantören eller importören av systemet och de myndigheter som är behöriga för det berörda AI-systemet med hög risk om detta och lämna uppgifter särskilt om den bristande överensstämmelsen och om eventuella korrigerande åtgärder som vidtagits.

5. På motiverad begäran av en berörd behörig myndighet ska distributörer av ett AI-system med hög risk förse den myndigheten med all information och dokumentation om deras åtgärder enligt punkterna 1–4 som är nödvändig för att visa att det systemet uppfyller kraven i avsnitt 2.

6. Distributörer ska samarbeta med de berörda behöriga myndigheterna i alla åtgärder som dessa myndigheter vidtar med avseende på ett AI-system med hög risk som distributörerna har gjort tillgängligt på marknaden, i synnerhet för att minska eller begränsa den risk som det utgör.

Artikel 25

Ansvar längs AI-värdekedjan

1. Varje distributör, importör, tillhandahållare eller annan tredje part ska vid tillämpningen av denna förordning anses vara en leverantör av ett AI-system med hög risk och ha de skyldigheter som leverantören har enligt artikel 16, under någon av följande omständigheter:

a) De sätter sitt namn eller varumärke på ett AI-system med hög risk som redan släppts ut på marknaden eller tagits i bruk, utan att det påverkar avtalsarrangemang som föreskriver att skyldigheterna ska fördelas på annat sätt.

b) De gör en väsentlig ändring av ett AI-system med hög risk som redan har släppts ut på marknaden eller redan har tagits i bruk på ett sådant sätt att det fortfarande är ett AI-system med hög risk enligt artikel 6.

c) De ändrar det avsedda ändamålet för ett AI-system, inklusive ett AI-system för allmänna ändamål, som inte har klassificerats som ett AI-system med hög risk och som redan har släppts ut på marknaden eller tagits i bruk på ett sådant sätt att det berörda AI-systemet blir ett AI-system med hög risk i enlighet med artikel 6.

2. Om de omständigheter som avses i punkt 1 uppstår, ska den leverantör som ursprungligen släppte ut AI-systemet på marknaden eller tog det i bruk inte längre anses vara en leverantör av det specifika AI-systemet vid tillämpningen av denna förordning. Den ursprungliga leverantören ska nära samarbeta med nya leverantörer och tillgängliggöra den nödvändiga informationen och tillhandahålla den rimligen förväntade tekniska åtkomsten och annat stöd som krävs för att fullgöra de skyldigheter som fastställs i denna förordning, särskilt när det gäller efterlevnaden av bedömningen av överensstämmelse för AI-system med hög risk. Denna punkt är inte tillämplig i fall där den ursprungliga leverantören tydligt har angett att dess AI-system inte får omvandlas till ett AI-system med hög risk och därför inte omfattas av skyldigheten att överlämna dokumentationen.

3. När det gäller AI-system med hög risk som är säkerhetskomponenter i produkter som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I, ska produkttillverkaren anses vara leverantören av AI-systemet med hög risk och omfattas av de skyldigheter som avses i artikel 16 under någon av följande omständigheter:

a) AI-systemet med hög risk släpps ut på marknaden tillsammans med produkten under produkttillverkarens namn eller varumärke.

b) AI-systemet med hög risk tas i bruk under produkttillverkarens namn eller varumärke efter det att produkten släppts ut på marknaden.

4. Leverantören av ett AI-system med hög risk och den tredje part som tillhandahåller ett AI-system, verktyg, tjänster, komponenter eller processer som används eller integreras i ett AI-system med hög risk ska genom ett skriftligt avtal ange den nödvändiga informationen, kapaciteten och tekniska åtkomsten samt det andra stödet, baserat på den allmänt erkända senaste utvecklingen, för att göra det möjligt för leverantören av AI-systemet med hög risk att fullt ut uppfylla de skyldigheter som fastställs i denna förordning. Denna punkt är inte tillämplig på tredje part som för allmänheten tillgängliggör andra verktyg, tjänster, processer eller komponenter än AI-modeller för allmänna ändamål, med en kostnadsfri licens med öppen källkod.

AI-byrån får utveckla och rekommendera frivilliga standardvillkor för avtal mellan leverantörer av AI-system med hög risk och tredje parter som tillhandahåller verktyg, tjänster, komponenter eller processer som används för eller är integrerade i AI-system med hög risk. Vid utarbetandet av dessa frivilliga standardvillkor ska AI-byrån ta hänsyn till eventuella avtalskrav som är tillämpliga inom specifika sektorer eller affärsförhållanden. De frivilliga standardvillkoren ska offentliggöras och vara tillgängliga kostnadsfritt i ett lättanvänt elektroniskt format.

5. Punkterna 2 och 3 påverkar inte behovet av att iaktta och skydda immateriella rättigheter, konfidentiell affärsinformation och företagshemligheter i enlighet med unionsrätten och nationell rätt.

Artikel 26

Skyldigheter för tillhandahållare av AI-system med hög risk

1. Tillhandahållare av AI-system med hög risk ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att de använder sådana system i enlighet med de bruksanvisningar som åtföljer systemen, enligt punkterna 3 och 6.

2. Tillhandahållare ska tilldela fysiska personer som har nödvändig kompetens, utbildning och auktoritet samt nödvändigt stöd uppgiften att utöva mänsklig kontroll.

3. De skyldigheter som fastställs i punkterna 1 och 2 påverkar inte andra skyldigheter för tillhandahållare enligt unionsrätten eller nationell rätt eller tillhandahållarens frihet att organisera sina egna resurser och sin egen verksamhet i syfte att genomföra de åtgärder för mänsklig kontroll som leverantören anger.

4. Utan att det påverkar tillämpningen av punkterna 1 och 2 ska tillhandahållaren, i den mån tillhandahållaren utövar kontroll över indata, säkerställa att indata är relevanta och tillräckligt representativa med tanke på det avsedda ändamålet med AI-systemet med hög risk.

5. Tillhandahållare ska övervaka driften av AI-systemet med hög risk på grundval av bruksanvisningen och, i förekommande fall, informera leverantörerna i enlighet med artikel 72. Om tillhandahållare har skäl att tro att användningen av AI-systemet med hög risk i enlighet med instruktionerna kan leda till att AI-systemet utgöra en risk i den mening som avses i artikel 79.1 ska de, utan oskäligt dröjsmål, informera leverantören eller distributören och den berörda marknadskontrollmyndigheten och tillfälligt avbryta användningen av det systemet. Om tillhandahållare har fastställt en allvarlig incident ska de också omedelbart informera först leverantören och sedan importören eller distributören och de berörda marknadskontrollsmyndigheterna om den incidenten. Om tillhandahållaren inte kan nå leverantören ska artikel 73 gälla i tillämpliga delar. Denna skyldighet omfattar inte känsliga operativa uppgifter om tillhandahållare av AI-system som är brottsbekämpande myndigheter.

För tillhandahållare som är finansinstitut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster ska övervakningsskyldigheten i första stycket anses vara uppfylld genom att reglerna om interna styrelseformer, arrangemang, processer och mekanismer enligt relevant unionsrätt om finansiella tjänster följs.

6. Tillhandahållare av AI-system med hög risk ska spara de loggar som genereras automatiskt av det AI-systemet med hög risk, i den mån sådana loggar står under deras kontroll, under en period som är lämplig för det avsedda ändamålet med AI-systemet med hög risk, dock i minst sex månader, om inte annat föreskrivs i tillämplig unionsrätt eller nationell rätt, i synnerhet unionsrätten om skydd av personuppgifter.

Tillhandahållare som är finansinstitut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster ska bevara loggar som en del av den dokumentation som ska bevaras enligt relevant unionsrätt om finansiella tjänster.

7. Innan ett AI-system med hög risk tas i bruk eller används på en arbetsplats ska tillhandahållare som är arbetsgivare informera arbetstagarrepresentanterna och de berörda arbetstagarna om att de kommer att vara föremål för användning av AI-systemet med hög risk. Denna information ska, i tillämpliga fall, tillhandahållas i enlighet med de regler och förfaranden som fastställs i unionsrätten och nationell rätt samt praxis i fråga om information till arbetstagare och deras representanter.

8. Tillhandahållare av AI-system med hög risk som är offentliga myndigheter eller unionens institutioner, organ eller byråer ska fullgöra de registreringsskyldigheter som avses i artikel 49. Om dessa tillhandahållare finner att det AI-system med hög risk som de avser att använda inte har registrerats i den EU-databas som avses i artikel 71 får de inte använda det systemet och ska informera leverantören eller distributören.

9. I tillämpliga fall ska tillhandahållare av AI-system med hög risk använda den information som tillhandahålls enligt artikel 13 i denna förordning för att fullgöra sin skyldighet att genomföra en konsekvensbedömning avseende dataskydd enligt artikel 35 i förordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680.

10. Inom ramen för en utredning för målinriktad sökning av en person som misstänks ha begått ett brott eller som har dömts för att ha begått ett brott ska tillhandahållaren av ett AI-system med hög risk för biometrisk fjärridentifiering i efterhand, utan att det påverkar tillämpningen av direktiv (EU) 2016/680, på förhand eller utan oskäligt dröjsmål och senast inom 48 timmar, av en rättslig myndighet eller en administrativ myndighet vars beslut är bindande och föremål för rättslig prövning begära tillstånd för användning av det systemet, utom när det används för den inledande identifieringen av en potentiell misstänkt på grundval av objektiva och verifierbara fakta med direkt anknytning till brottet. Varje användning ska begränsas till vad som är absolut nödvändigt för att utreda ett specifikt brott.

Om det tillstånd som begärts enligt första stycket nekas ska användningen av det system för biometrisk fjärridentifiering i efterhand som är kopplat till det begärda tillståndet upphöra med omedelbar verkan, och de personuppgifter som är kopplade till användningen av det AI-system med hög risk för vilket tillståndet begärdes ska raderas.

Under inga omständigheter får ett sådant AI-system med hög risk för biometrisk fjärridentifiering i efterhand användas för brottsbekämpande ändamål på ett icke målinriktat sätt, utan koppling till ett brott, ett straffrättsligt förfarande, ett verkligt och aktuellt eller verkligt och förutsebart hot om ett brott eller sökning efter en specifik försvunnen person. Det ska säkerställas att inget beslut som har negativa rättsliga följder för en person får fattas av de brottsbekämpande myndigheterna enbart på grundval av utdata från sådana system för biometrisk fjärridentifiering i efterhand.

Denna punkt påverkar inte tillämpningen av artikel 9 i förordning (EU) 2016/679 och artikel 10 i direktiv (EU) 2016/680 avseende behandling av biometriska uppgifter.

Oavsett ändamål eller tillhandahållare ska varje användning av sådana AI-system med hög risk dokumenteras i den relevanta polisakten och på begäran göras tillgänglig för den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten, med undantag för utlämnande av känsliga operativa uppgifter som rör brottsbekämpning. Detta stycke påverkar inte de befogenheter som tilldelas tillsynsmyndigheterna genom direktiv (EU) 2016/680.

Tillhandahållare ska lämna in årliga rapporter till de berörda marknadskontrollmyndigheterna och nationella dataskyddsmyndigheterna om sin användning av system för biometrisk fjärridentifiering i efterhand, med undantag för utlämnande av känsliga operativa uppgifter som rör brottsbekämpning. Rapporterna får aggregeras för att täcka mer än en användning.

Medlemsstaterna får införa mer restriktiva lagar om användningen av system för biometrisk fjärridentifiering i efterhand i enlighet med unionsrätten.

11. Utan att det påverkar tillämpningen av artikel 50 i denna förordning ska tillhandahållare av AI-system med hög risk som avses i bilaga III och som fattar beslut eller hjälper till att fatta beslut som rör fysiska personer informera de fysiska personerna om att de är föremål för användning av AI-systemet med hög risk. När det gäller AI-system med hög risk som används för brottsbekämpande ändamål ska artikel 13 i direktiv (EU) 2016/680 tillämpas.

12. Tillhandahållare ska samarbeta med de berörda behöriga myndigheterna i alla åtgärder som dessa myndigheter vidtar med avseende på AI-systemet med hög risk i syfte att genomföra denna förordning.

Artikel 27

Konsekvensbedömning avseende grundläggande rättigheter när det gäller AI-system med hög risk

1. Innan ett AI-system med hög risk som avses i artikel 6.2, med undantag för AI-system med hög risk som är avsedda att användas inom det område som anges i punkt 2 i bilaga III, införs ska tillhandahållare som är offentligrättsliga organ eller som är privata enheter som tillhandahåller offentliga tjänster, och tillhandahållare av AI-system med hög risk som avses i punkt 5 b och c i bilaga III, göra en bedömning av den inverkan på grundläggande rättigheter som användningen av ett sådant system kan ge upphov till. För detta ändamål ska tillhandahållare göra en bedömning bestående av följande:

a) En beskrivning av tillhandahållarens processer där AI-systemet med hög risk kommer att användas i linje med dess avsedda ändamål.

b) En beskrivning av den tidsperiod inom vilken och den frekvens med vilken varje AI-system med hög risk är avsett att användas.

c) De kategorier av fysiska personer och grupper som sannolikt kommer att påverkas av användningen av systemet i det specifika sammanhanget.

d) De specifika risker för skada som sannolikt kommer att påverka de kategorier av fysiska personer eller grupper av personer som har identifierats enligt led c i denna punkt, med beaktande av den information som leverantören har tillhandahållit enligt artikel 13.

e) En beskrivning av genomförandet av åtgärder för mänsklig kontroll, i enlighet med bruksanvisningen.

f) De åtgärder som ska vidtas om dessa risker förverkligas, inbegripet arrangemangen för intern styrning och klagomålsmekanismer.

2. Den skyldighet som fastställs i punkt 1 gäller för den första användningen av AI-systemet med hög risk. Tillhandahållaren får i liknande fall förlita sig på tidigare genomförda konsekvensbedömningar avseende grundläggande rättigheter eller befintliga konsekvensbedömningar som har utförts av leverantören. En tillhandahållare som under användningen av AI-systemet med hög risk anser att något av de element som anges i punkt 1 har ändrats eller inte längre är aktuellt ska vidta nödvändiga åtgärder för att uppdatera informationen.

3. När den bedömning som avses i punkt 1 i denna artikel har utförts ska tillhandahållaren underrätta marknadskontrollmyndigheten om sina resultat, inbegripet lämna in den ifyllda mall som avses i punkt 5 i denna artikel som en del av underrättelsen. I det fall som avses i artikel 46.1 får tillhandahållare undantas från den underrättelseskyldigheten.

4. Om någon av de skyldigheter som fastställs i denna artikel redan uppfylls genom den konsekvensbedömning avseende dataskydd som genomförs enligt artikel 35 i förordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680, ska den konsekvensbedömning avseende grundläggande rättigheter som avses i punkt 1 i den här artikeln komplettera den konsekvensbedömningen avseende dataskydd.

5. AI-byrån ska utarbeta en mall för ett frågeformulär, inbegripet genom ett automatiserat verktyg, för att underlätta för tillhandahållare att på ett förenklat sätt fullgöra sina skyldigheter enligt denna artikel.

AVSNITT 4

Anmälande myndigheter och anmälda organ

Artikel 28

Anmälande myndigheter

1. Varje medlemsstat ska utse eller inrätta minst en anmälande myndighet med ansvar för att fastställa och genomföra de förfaranden som krävs för bedömning, utseende och anmälan av organ för bedömning av överensstämmelse och för övervakning av dessa. Dessa förfaranden ska utvecklas i samarbete mellan de anmälande myndigheterna i alla medlemsstater.

2. Medlemsstaterna får bestämma att den bedömning och övervakning som avses i punkt 1 ska utföras av ett nationellt ackrediteringsorgan i den mening som avses i, och i enlighet med, förordning (EG) nr 765/2008.

3. Anmälande myndigheter ska vara inrättade och organiserade och fungera på ett sådant sätt att det inte uppstår någon intressekonflikt med organen för bedömning av överensstämmelse och att det garanteras att deras verksamhet är objektiv och opartisk.

4. Anmälande myndigheter ska vara organiserade på ett sådant sätt att beslut som rör anmälan av organ för bedömning av överensstämmelse fattas av annan behörig personal än den som har gjort bedömningen av dessa organ.

5. Anmälande myndigheter får varken erbjuda eller utföra sådan verksamhet som utförs av organ för bedömning av överensstämmelse eller erbjuda eller utföra konsulttjänster på kommersiell eller konkurrensmässig grund.

6. Anmälande myndigheter ska säkerställa att den information som de erhåller behandlas konfidentiellt, i enlighet med artikel 78.

7. Anmälande myndigheter ska förfoga över tillräckligt med personal med lämplig kompetens för att kunna utföra sina uppgifter. Kompetent personal ska, i tillämpliga fall, ha nödvändig sakkunskap med tanke på sin funktion, på områden som informationsteknik, AI och juridik, inbegripet övervakning av grundläggande rättigheter.

Artikel 29

Ansökan om anmälan från ett organ för bedömning av överensstämmelse

1. Organ för bedömning av överensstämmelse ska lämna in en ansökan om anmälan till den anmälande myndigheten i den medlemsstat där de är etablerade.

2. Ansökan om anmälan ska åtföljas av en beskrivning av de bedömningar av överensstämmelse, den eller de moduler för bedömning av överensstämmelse och de typer av AI-system som organet för bedömning av överensstämmelse anser sig ha kompetens för samt ett ackrediteringsintyg, om sådant finns, som ska ha utfärdats av ett nationellt ackrediteringsorgan och i vilket det intygas att organet för bedömning av överensstämmelse uppfyller kraven i artikel 31.

Alla giltiga dokument som rör fall av befintliga utseenden av det ansökande anmälda organet enligt annan unionsharmoniseringslagstiftning ska läggas till.

3. Om det berörda organet för bedömning av överensstämmelse inte kan uppvisa något ackrediteringsintyg ska det ge den anmälande myndigheten alla skriftliga underlag som krävs för kontroll, erkännande och regelbunden övervakning av att det uppfyller kraven i artikel 31.

4. För anmälda organ som utsetts enligt annan unionsharmoniseringslagstiftning får alla dokument och intyg kopplade till dessa fall av utseende användas som stöd för deras utseendeförfarande enligt denna förordning, beroende på vad som är lämpligt. Det anmälda organet ska uppdatera den dokumentation som avses i punkterna 2 och 3 i denna artikel när det sker relevanta ändringar, för att myndigheten med ansvar för anmälda organ ska kunna övervaka och kontrollera att samtliga krav som föreskrivs i artikel 31 alltid uppfylls.

Artikel 30

Anmälningsförfarande

1. Anmälande myndigheter får endast anmäla de organ för bedömning av överensstämmelse som uppfyller kraven i artikel 31.

2. Anmälande myndigheter ska till kommissionen och övriga medlemsstater, med hjälp av det elektroniska anmälningsverktyg som har utvecklats och förvaltas av kommissionen, anmäla varje organ för bedömning av överensstämmelse som avses i punkt 1.

3. Den anmälan som avses i punkt 2 i denna artikel ska innehålla fullständiga uppgifter om bedömningarna av överensstämmelse, modulen eller modulerna för bedömning av överensstämmelse, de berörda typerna av AI-system samt ett relevant intyg om kompetens. Om en anmälan inte grundar sig på ett sådant ackrediteringsintyg som avses i artikel 29.2 ska den anmälande myndigheten ge kommissionen och övriga medlemsstater styrkande handlingar som visar att organet för bedömning av överensstämmelse har tillräcklig kompetens och att de system har inrättats som behövs för att säkerställa att organet övervakas regelbundet och fortsätter att uppfylla kraven i artikel 31.

4. Det berörda organet för bedömning av överensstämmelse får bedriva verksamhet som anmält organ endast om kommissionen och övriga medlemsstater inte har gjort några invändningar inom två veckor från en anmälan från en anmälande myndighet, i de fall ett ackrediteringsintyg enligt artikel 29.2 används, eller inom två månader från anmälan från den anmälande myndigheten, i de fall då styrkande handlingar som avses i artikel 29.3 används.

5. Om invändningar görs ska kommissionen utan dröjsmål inleda samråd med de berörda medlemsstaterna och organet för bedömning av överensstämmelse. Med beaktande av detta ska kommissionen besluta om tillståndet är motiverat eller inte. Kommissionen ska rikta sitt beslut till den berörda medlemsstaten och till det berörda organet för bedömning av överensstämmelse.

Artikel 31

Krav avseende anmälda organ

1. Ett anmält organ ska inrättas enligt en medlemsstats nationella rätt och ska vara en juridisk person.

2. Anmälda organ ska uppfylla de organisatoriska krav och krav på kvalitetsstyrning, resurser och processer som är nödvändiga för att de ska kunna fullgöra sina uppgifter, samt lämpliga cybersäkerhetskrav.

3. Det anmälda organets organisationsstruktur, ansvarsfördelning, rapporteringsvägar och driftsätt ska säkerställa förtroende för dess prestationer och för resultaten av de aktiviteter avseende bedömning av överensstämmelse som det anmälda organet bedriver.

4. Anmälda organ ska vara oberoende av den leverantör av AI-system med hög risk som är föremål för dess bedömning av överensstämmelse. Anmälda organ ska också vara oberoende av varje annan operatör som har ett ekonomiskt intresse i AI-system med hög risk som bedöms samt av eventuella konkurrenter till leverantören. Detta hindrar inte att bedömda AI-system med hög risk som är nödvändiga för verksamheten inom organet för bedömning av överensstämmelse används, eller att sådana AI-system med hög risk används för personligt bruk.

5. Varken ett organ för bedömning av överensstämmelse, dess högsta ledning eller den personal som ansvarar för att utföra bedömningen av överensstämmelse får vara direkt delaktig i konstruktionen, utvecklingen, saluföringen eller användningen av AI-system med hög risk, och de får inte heller företräda de parter som bedriver sådan verksamhet. De får inte delta i någon verksamhet som kan påverka deras objektivitet eller integritet i samband med den bedömning av överensstämmelse för vilken de har anmälts. Detta ska särskilt gälla konsulttjänster.

6. Anmälda organ ska vara organiserade och drivas på ett sådant sätt att deras verksamhet är oberoende, objektiv och opartisk. Anmälda organ ska dokumentera och genomföra en struktur och förfaranden som garanterar opartiskheten och främjar och tillämpar principerna om opartiskhet i hela organisationen, hos alla anställda och i all bedömningsverksamhet.

7. Anmälda organ ska ha infört dokumenterade förfaranden som ska säkerställa att deras personal, kommittéer, dotterbolag, underentreprenörer och andra associerade organ eller personal vid externa organ i enlighet med artikel 78 upprätthåller konfidentialiteten för den information som organen får kännedom om i samband med bedömning av överensstämmelse, utom när informationen måste lämnas ut enligt lag. De anmälda organens personal ska omfattas av tystnadsplikt i fråga om all information som de erhåller under utförandet av sina uppgifter enligt denna förordning, utom gentemot de anmälande myndigheterna i den medlemsstat där deras verksamhet utförs.

8. Anmälda organ ska ha förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till en leverantörs storlek, sektor och struktur samt det berörda AI-systemets komplexitet.

9. Anmälda organ ska teckna en lämplig ansvarsförsäkring för sin verksamhet avseende bedömningar av överensstämmelse, såvida inte den medlemsstat i vilken de är etablerade tar på sig ansvaret i överensstämmelse med nationell rätt eller den medlemsstaten är direkt ansvarig för bedömningen av överensstämmelse.

10. Anmälda organ ska kunna utföra alla sina uppgifter enligt denna förordning med största möjliga yrkesmässiga integritet och nödvändig kompetens på det specifika området, oavsett om dessa uppgifter utförs av de anmälda organen själva eller av annan part för deras räkning och under deras ansvar.

11. Anmälda organ ska ha tillräcklig intern kompetens för att effektivt kunna utvärdera de uppgifter som utförs av externa parter å organens vägnar. Det anmälda organet ska ha permanent tillgång till tillräcklig administrativ, teknisk, juridisk och vetenskaplig personal med erfarenhet av och kunskaper om de relevanta typerna av AI-system, relevanta data och relevant databehandling och om de krav som fastställs i avsnitt 2.

12. Anmälda organ ska delta i den samordningsverksamhet som avses i artikel 38. De ska också delta direkt, eller vara företrädda i, europeiska standardiseringsorganisationer, eller säkerställa att de är medvetna om och har aktuella kunskaper om relevanta standarder.

Artikel 32

Presumtion om överensstämmelse med krav som rör anmälda organ

För ett organ för bedömning av överensstämmelse som kan visa att det uppfyller kriterierna i de relevanta harmoniserade standarderna eller delar av dem, till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, ska en presumtion om överensstämmelse med kraven i artikel 31 gälla, på villkor att dessa krav omfattas av de tillämpliga harmoniserade standarderna.

Artikel 33

Dotterbolag till anmälda organ och underentreprenad

1. Om det anmälda organet lägger ut specifika uppgifter med anknytning till bedömningen av överensstämmelse på underentreprenad eller anlitar ett dotterbolag ska det säkerställa att underentreprenören eller dotterbolaget uppfyller kraven i artikel 31 och informera den anmälande myndigheten om detta.

2. Anmälda organ ska ta det fulla ansvaret för de uppgifter som utförs av underentreprenörer eller dotterbolag.

3. Verksamhet får läggas ut på underentreprenad eller utföras av ett dotterbolag endast om leverantören samtycker till det. Anmälda organ ska offentliggöra en förteckning över sina dotterbolag.

4. De relevanta dokumenten rörande bedömningen av underentreprenörens eller dotterbolagets kvalifikationer och det arbete som dessa har utfört enligt denna förordning ska hållas tillgängliga för den anmälande myndigheten under en period av fem år från och med dagen för avslutandet av underentreprenaden.

Artikel 34

Anmälda organs operativa skyldigheter

1. Anmälda organ ska kontrollera överensstämmelsen hos AI-system med hög risk i enlighet med de förfaranden för bedömning av överensstämmelse som föreskrivs i artikel 43.

2. Anmälda organ ska motverka uppkomsten av onödiga administrativa bördor för leverantörer när de utövar sin verksamhet och ta vederbörlig hänsyn till en leverantörs storlek, den sektor där denna är verksam, dess struktur samt komplexiteten i det berörda AI-systemet med hög risk, särskilt i syfte att minimera de administrativa bördorna och efterlevnadskostnaderna för mikroföretag och småföretag i den mening som avses i rekommendation 2003/361/EG. Det anmälda organet ska emellertid respektera den grad av noggrannhet och den skyddsnivå som krävs för att AI-systemet med hög risk ska överensstämma med kraven i denna förordning.

3. Anmälda organ ska tillhandahålla och på begäran lämna över all relevant dokumentation, inbegripet leverantörens dokumentation, till den anmälande myndighet som avses i artikel 28, så att denna myndighet kan utföra sin verksamhet avseende bedömning, utseende, anmälan och övervakning och för att underlätta den bedömning som beskrivs i detta avsnitt.

Artikel 35

Identifikationsnummer och förteckningar över anmälda organ

1. Kommissionen ska tilldela varje anmält organ ett enda identifikationsnummer, även om ett organ anmäls enligt mer än en unionsakt.

2. Kommissionen ska offentliggöra förteckningen över de organ som anmälts enligt denna förordning, inklusive deras identifikationsnummer och den verksamhet som de har anmälts för. Kommissionen ska säkerställa att förteckningen hålls uppdaterad.

Artikel 36

Ändringar i anmälan

1. Den anmälande myndigheten ska underrätta kommissionen och övriga medlemsstater om alla relevanta ändringar beträffande anmälan av ett anmält organ via det elektroniska anmälningsverktyg som avses i artikel 30.2.

2. De förfaranden som föreskrivs i artiklarna 29 och 30 ska tillämpas på utvidgningar av anmälans tillämpningsområde.

När det gäller andra ändringar av anmälan än utvidgningar av dess tillämpningsområde ska de förfaranden som fastställs i punkterna 3–9 tillämpas.

3. Om ett anmält organ beslutar att upphöra med sin verksamhet avseende bedömning av överensstämmelse, ska det så snart som möjligt och, om upphörandet är planerat, minst ett år innan det upphör med verksamheten underrätta den anmälande myndigheten och de berörda leverantörerna om detta. Det anmälda organets intyg får förbli giltiga under en period på nio månader efter det att det anmälda organets verksamhet upphört på villkor att ett annat anmält organ skriftligen har bekräftat att det kommer att åta sig ansvaret för de AI-system med hög risk som omfattas av intygen. Det sistnämnda anmälda organet ska utföra en fullständig bedömning av de AI-system med hög risk det gäller före utgången av denna niomånadersperiod, innan det utfärdar nya intyg för dem. Om det anmälda organet har upphört med sin verksamhet ska den anmälande myndigheten återkalla utseendet.

4. Om en anmälande myndighet har tillräckliga skäl att anse att ett anmält organ inte längre uppfyller de krav som anges i artikel 31 eller att det underlåter att fullgöra sina skyldigheter, ska den anmälande myndigheten utan dröjsmål undersöka frågan med största möjliga omsorg. I detta sammanhang ska den anmälande myndigheten underrätta det berörda anmälda organet om de invändningar som framförts och ge det möjlighet att framföra sina synpunkter. Om den anmälande myndigheten drar slutsatsen att ett anmält organ inte längre uppfyller de krav som anges i artikel 31 eller att det underlåter att fullgöra sina skyldigheter, ska den anmälande myndigheten, beroende på hur allvarlig underlåtenheten att uppfylla kraven eller fullgöra skyldigheterna är, begränsa utseendet, tillfälligt återkalla det eller återkalla det slutgiltigt beroende på vad som är lämpligt. Myndigheten ska omedelbart informera kommissionen och de andra medlemsstaterna om detta.

5. Om utseendet av ett anmält organ har återkallats tillfälligt eller begränsats, eller helt eller delvis återkallats slutgiltigt, ska det anmälda organet underrätta de berörda leverantörerna inom tio dagar.

6. I händelse av begränsningar eller tillfällig eller slutgiltig återkallelse av ett utseende ska den anmälande myndigheten vidta lämpliga åtgärder för att säkerställa att det berörda anmälda organets dokumentation bevaras och göra den tillgänglig för de anmälande myndigheterna i andra medlemsstater och för marknadskontrollmyndigheterna på deras begäran.

7. I händelse av begränsningar eller tillfällig eller slutgiltig återkallelse av ett utseende ska den anmälande myndigheten

a) bedöma påverkan på de intyg som det anmälda organet har utfärdat,

b) överlämna en rapport om sina iakttagelser till kommissionen och de andra medlemsstaterna senast tre månader efter att ha anmält ändringarna av utseendet,

c) ålägga det anmälda organet att, inom en rimlig tid som myndigheten fastställer, tillfälligt eller slutgiltigt dra tillbaka intyg som utfärdats på felaktiga grunder för att säkerställa fortsatt överensstämmelse för AI-system med hög risk på marknaden,

d) informera kommissionen och medlemsstaterna om intyg som den har krävt ska dras tillbaka tillfälligt eller slutgiltigt,

e) förse de nationella behöriga myndigheterna i den medlemsstat där leverantören har sitt säte med all relevant information om de intyg den har krävt ska dras tillbaka tillfälligt eller slutgiltigt. Denna myndighet ska vidta lämpliga åtgärder, om så är nödvändigt för att undvika en potentiell risk för hälsa, säkerhet eller grundläggande rättigheter.

8. Med undantag för intyg som utfärdats på felaktiga grunder, och om ett utseende har återkallats tillfälligt eller begränsats, ska intygen vara fortsatt giltiga i något av följande fall:

a) Om den anmälande myndigheten inom en månad från den tillfälliga återkallelsen eller begränsningarna har bekräftat att det inte finns någon risk för hälsa, säkerhet eller grundläggande rättigheter när det gäller intyg som berörs av den tillfälliga återkallelsen eller begränsningarna, och den anmälande myndigheten har angett en tidsfrist för åtgärder som ska leda till att den tillfälliga återkallelsen eller begränsningarna hävs.

b) Om den anmälande myndigheten har bekräftat att inga intyg av betydelse för den tillfälliga återkallelsen ska utfärdas, ändras eller utfärdas på nytt under den tid som den tillfälliga återkallelsen eller begränsningarna gäller, och anger huruvida det anmälda organet har kapacitet att fortsätta att övervaka och ansvara för de befintliga intyg som utfärdats för den period som den tillfälliga återkallelsen eller begränsningarna gäller. Om den anmälande myndigheten fastställer att det anmälda organet inte har kapacitet att upprätthålla befintliga utfärdade intyg, ska leverantören av det system som omfattas av intyget inom tre månader efter den tillfälliga återkallelsen eller begränsningarna skriftligen bekräfta för de nationella behöriga myndigheterna i den medlemsstat där leverantören har sitt säte att ett annat kvalificerat anmält organ tillfälligt tar på sig det anmälda organets uppgifter att övervaka och fortsätta att ansvara för intygen under den tid som den tillfälliga återkallelsen eller begränsningarna gäller.

9. Med undantag för intyg som utfärdats på felaktiga grunder och fall där ett utseende har återkallats ska intygen fortsätta att vara giltiga i nio månader under följande omständigheter:

a) Den nationella behöriga myndigheten i den medlemsstat där leverantören av det AI-system med hög risk som omfattas av intyget har sitt säte har bekräftat att det inte finns någon risk för hälsa, säkerhet eller grundläggande rättigheter i samband med de berörda AI-systemen med hög risk.

b) Ett annat anmält organ har bekräftat skriftligen att det omedelbart kommer att åta sig ansvaret för dessa AI-system och att det slutför sin bedömning inom tolv månader från det att utseendet har återkallats slutgiltigt.

Under de omständigheter som avses i första stycket får den nationella behöriga myndigheten i den medlemsstat där leverantören av det system som omfattas av intyget har sitt säte förlänga intygens provisoriska giltighet med ytterligare perioder av tre månader i taget, dock längst i tolv månader sammanlagt.

Den nationella behöriga myndighet eller det anmälda organ som tagit på sig de uppgifter som skulle utföras av det anmälda organ som berörs av ändringen av utseendet ska omedelbart informera kommissionen, de andra medlemsstaterna och de andra anmälda organen om ändringen av dessa uppgifter.

Artikel 37

Ifrågasättande av anmälda organs kompetens

1. Kommissionen ska vid behov undersöka alla fall där det finns skäl att betvivla att ett anmält organ har tillräcklig kompetens eller att ett anmält organ fortsätter att uppfylla kraven i artikel 31 och fullgöra sitt tillämpliga ansvar.

2. Den anmälande myndigheten ska på begäran ge kommissionen all relevant information om anmälan eller upprätthållandet av det berörda anmälda organets kompetens.

3. Kommissionen ska säkerställa att all känslig information som den erhåller under sina undersökningar enligt denna artikel behandlas konfidentiellt i enlighet med artikel 78.

4. Om kommissionen konstaterar att ett anmält organ inte uppfyller eller inte längre uppfyller kraven för anmälan ska den informera den anmälande medlemsstaten om detta och anmoda den att vidta nödvändiga korrigerande åtgärder, inbegripet att om så är nödvändigt återkalla anmälan tillfälligt eller slutgiltigt. Om medlemsstaten inte vidtar nödvändiga korrigerande åtgärder får kommissionen genom en genomförandeakt begränsa utseendet eller återkalla det tillfälligt eller slutgiltigt. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

Artikel 38

Samordning av anmälda organ

1. Kommissionen ska för AI-system med hög risk säkerställa att lämplig samordning och ett lämpligt samarbete införs mellan de anmälda organ som är verksamma i förfaranden för bedömning av överensstämmelse enligt denna förordning och att samordningen och samarbetet bedrivs på ett tillfredsställande sätt genom en sektorsspecifik grupp av anmälda organ.

2. Varje anmälande myndighet ska säkerställa att de organ som den har anmält deltar i arbetet i en grupp som avses i punkt 1 direkt eller genom utsedda representanter.

3. Kommissionen ska se till att det förekommer utbyte av kunskap och bästa praxis mellan anmälande myndigheter.

Artikel 39

Organ för bedömning av överensstämmelse i tredjeländer

Organ för bedömning av överensstämmelse som inrättats enligt ett tredjelands rätt med vilket unionen har ingått ett avtal får bemyndigas att utföra den verksamhet som bedrivs av anmälda organ enligt denna förordning, förutsatt att de uppfyller kraven i artikel 31 eller säkerställer en likvärdig nivå av överensstämmelse.

AVSNITT 5

Standarder, bedömning av överensstämmelse, intyg, registrering

Artikel 40

Harmoniserade standarder och standardiseringsprodukter

1. AI-system med hög risk eller AI-modeller för allmänna ändamål som överensstämmer med harmoniserade standarder eller delar av dem till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, ska förutsättas överensstämma med de krav som fastställs i avsnitt 2 i detta kapitel eller, i tillämpliga fall, skyldigheterna i kapitel V avsnitten 2 och 3 i den här förordningen, i den utsträckning som de standarderna omfattar dessa krav eller skyldigheter.

2. I enlighet med artikel 10 i förordning (EU) nr 1025/2012 ska kommissionen utan oskäligt dröjsmål utfärda begäranden om standardisering som omfattar alla krav i avsnitt 2 i detta kapitel och, i tillämpliga fall, begäranden om standardisering som omfattar skyldigheterna i kapitel V avsnitten 2 och 3 i den här förordningen. I begäran om standardisering ska det också begäras produkter för rapporterings- och dokumentationsprocesser i syfte att förbättra AI-systemens resursprestanda, till exempel genom att minska förbrukningen av energi och andra resurser hos AI-systemet med hög risk under dess livscykel, och för energieffektiv utveckling av AI-modeller för allmänna ändamål. När kommissionen utarbetar en begäran om standardisering ska den samråda med styrelsen och relevanta berörda parter, inklusive det rådgivande forumet.

När kommissionen utfärdar en begäran om standardisering till europeiska standardiseringsorganisationer ska den ange att standarderna måste vara tydliga, samstämmiga, inbegripet med de standarder som utvecklas i de olika sektorerna för produkter som omfattas av den befintliga unionsharmoniseringslagstiftning som förtecknas i bilaga I, och syfta till att säkerställa att AI-system med hög risk eller AI-modeller för allmänna ändamål som släpps ut på marknaden eller tas i bruk i unionen uppfyller relevanta krav eller skyldigheter i denna förordning.

Kommissionen ska kräva att de europeiska standardiseringsorganisationerna påvisar att de har gjort sitt yttersta för att uppnå de mål som avses i första och andra styckena i denna punkt i enlighet med artikel 24 i förordning (EU) nr 1025/2012.

3. Deltagarna i standardiseringsprocessen ska sträva efter att främja investeringar och innovation inom AI, inbegripet genom ökad rättssäkerhet, samt konkurrenskraften och tillväxten på unionsmarknaden, att bidra till att stärka det globala samarbetet om standardisering och ta hänsyn till befintliga internationella standarder på AI-området som är förenliga med unionens värden, grundläggande rättigheter och intressen, och att stärka flerpartsstyrningen i syfte att säkerställa en balanserad representation av intressen och ett faktiskt deltagande av alla relevanta berörda parter i enlighet med artiklarna 5, 6 och 7 i förordning (EU) nr 1025/2012.

Artikel 41

Gemensamma specifikationer

1. Kommissionen får anta genomförandeakter om fastställande av gemensamma specifikationer för de krav som anges i avsnitt 2 i detta kapitel eller, i tillämpliga fall, för de skyldigheter som anges i kapitel V avsnitten 2 och 3, om följande villkor är uppfyllda:

a) Kommissionen har enligt artikel 10.1 i förordning (EU) nr 1025/2012 begärt att en eller flera europeiska standardiseringsorganisationer ska utarbeta en harmoniserad standard för de krav som anges i avsnitt 2 i detta kapitel eller, i tillämpliga fall, för de skyldigheter som anges i kapitel V avsnitten 2 och 3, och

   i) begäran har inte godtagits av någon av de europeiska standardiseringsorganisationerna, eller

ii) de harmoniserade standarder som tillgodoser begäran har inte lämnats inom den tidsfrist som fastställts i enlighet med artikel 10.1 i förordning (EU) nr 1025/2012, eller

iii) de relevanta harmoniserade standarderna tar inte i tillräckligt hög grad hänsyn till frågor som rör grundläggande rättigheter, eller

iv) de harmoniserade standarderna överensstämmer inte med begäran, och

b) ingen hänvisning till harmoniserade standarder som omfattar de krav som anges i avsnitt 2 i detta kapitel eller, i tillämpliga fall, de skyldigheter som anges i kapitel V avsnitten 2 och 3, har offentliggjorts i *Europeiska unionens officiella tidning* i enlighet med förordning (EU) nr 1025/2012, och ingen sådan hänvisning förväntas offentliggöras inom rimlig tid.

Vid utarbetandet av de gemensamma specifikationerna ska kommissionen samråda med det rådgivande forum som avses i artikel 67.

De genomförandeakter som avses i första stycket i denna punkt ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

2. Innan kommissionen utarbetar ett utkast till genomförandeakt ska den informera den kommitté som avses i artikel 22 i förordning (EU) nr 1025/2012 om att den anser att villkoren i punkt 1 i den här artikeln är uppfyllda.

3. AI-system med hög risk eller AI-modeller för allmänna ändamål som överensstämmer med de gemensamma specifikationer som avses i punkt 1, eller delar av dessa specifikationer, ska förutsättas överensstämma med de krav som anges i avsnitt 2 i detta kapitel eller, i tillämpliga fall, fullgöra de skyldigheter som anges i kapitel V avsnitten 2 och 3, i den omfattning som de gemensamma specifikationerna omfattar dessa krav eller skyldigheter.

4. Om en harmoniserad standard antas av en europeisk standardiseringsorganisation och föreslås för kommissionen för offentliggörande av hänvisningen till den i *Europeiska unionens officiella tidning*, ska kommissionen bedöma den harmoniserade standarden i enlighet med förordning (EU) nr 1025/2012. När en hänvisning till en harmoniserad standard offentliggörs i *Europeiska unionens officiella tidning* ska kommissionen upphäva de genomförandeakter som avses i punkt 1, eller delar av dem som omfattar samma krav som anges i avsnitt 2 i detta kapitel eller, i tillämpliga fall, samma skyldigheter som anges i kapitel V avsnitten 2 och 3.

5. Om leverantörer av AI-system med hög risk eller AI-modeller för allmänna ändamål inte följer de gemensamma specifikationer som avses i punkt 1 ska de vederbörligen motivera att de har antagit tekniska lösningar som uppfyller de krav som anges i avsnitt 2 i detta kapitel eller, i tillämpliga fall, fullgör de skyldigheter som anges i kapitel V avsnitten 2 och 3, till en nivå som åtminstone är likvärdig med dem.

6. Om en medlemsstat anser att en gemensam specifikation inte helt uppfyller de krav som anges i avsnitt 2 eller, i tillämpliga fall, de skyldigheter som anges i kapitel V avsnitten 2 och 3, ska den underrätta kommissionen om detta med en detaljerad förklaring. Kommissionen ska bedöma denna information och när så är lämpligt ändra genomförandeakten om fastställande av den berörda gemensamma specifikationen.

Artikel 42

Presumtion om överensstämmelse med vissa krav

1. AI-system med hög risk som har tränats och testats på data som återspeglar den specifika geografiska, beteendemässiga, kontextuella eller funktionella miljö inom vilken de är avsedda att användas ska förutsättas uppfylla de relevanta kraven i artikel 10.4.

2. AI-system med hög risk som har certifierats, eller för vilka en försäkran om överensstämmelse har utfärdats inom ramen för en ordning för cybersäkerhetscertifiering enligt förordning (EU) 2019/881, och till vilka hänvisningar har offentliggjorts i *Europeiska unionens officiella tidning*, ska förutsättas uppfylla de cybersäkerhetskrav som anges i artikel 15 i den här förordningen, förutsatt att cybersäkerhetscertifikatet eller försäkran om överensstämmelse eller delar därav omfattar dessa krav.

Artikel 43

Bedömning av överensstämmelse

1. För AI-system med hög risk som förtecknas i punkt 1 i bilaga III ska leverantören, när den vill visa att ett AI-system med hög risk uppfyller kraven i avsnitt 2 och den har tillämpat de harmoniserade standarder som avses i artikel 40 eller, i tillämpliga fall, de gemensamma specifikationer som avses i artikel 41, välja ett av följande förfaranden för bedömning av överensstämmelse grundat på

a) intern kontroll som avses i bilaga VI, eller

b) en bedömning av kvalitetsstyrningssystemet och en bedömning av den tekniska dokumentationen, med deltagande av ett anmält organ, som avses i bilaga VII.

När leverantören vill visa att ett AI-system med hög risk uppfyller de krav som fastställs i avsnitt 2 ska leverantören följa det förfarande för bedömning av överensstämmelse som fastställs i bilaga VII i följande fall:

a) De harmoniserade standarder som avses i artikel 40 saknas, och de gemensamma specifikationer som avses i artikel 41 är inte tillgängliga.

b) Leverantören har inte tillämpat eller har endast tillämpat en del av den harmoniserade standarden.

c) De gemensamma specifikationer som avses i led a finns men leverantören har inte tillämpat dem.

d) En eller flera av de harmoniserade standarder som avses i led a har offentliggjorts med en begränsning och endast för den del av standarden som begränsades.

För det förfarande för bedömning av överensstämmelse som avses i bilaga VII får leverantören välja vilket av de anmälda organen som helst. Om AI-systemet med hög risk är avsett att tas i bruk av brottsbekämpande myndigheter, migrationsmyndigheter eller asylmyndigheter eller av unionens institutioner, organ eller byråer ska dock den marknadskontrollmyndighet som avses i artikel 74.8 eller 74.9, beroende på vad som är tillämpligt, fungera som anmält organ.

2. För de AI-system med hög risk som avses i punkterna 2–8 i bilaga III ska leverantörer följa det förfarande för bedömning av överensstämmelse grundat på intern kontroll som avses i bilaga VI, vilket inte föreskriver att ett anmält organ ska delta.

3. För AI-system med hög risk som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I ska leverantören följa det relevanta förfarande för bedömning av överensstämmelse som krävs enligt dessa rättsakter. Kraven i avsnitt 2 i detta kapitel ska tillämpas på de AI-systemen med hög risk och ska ingå i den bedömningen. Punkterna 4.3, 4.4 och 4.5 och punkt 4.6 femte stycket i bilaga VII ska också tillämpas.

Vid denna bedömning ska anmälda organ som har anmälts enligt de rättsakterna ha rätt att kontrollera att AI-systemen med hög risk överensstämmer med kraven i avsnitt 2, förutsatt att dessa anmälda organs överensstämmelse med kraven i artikel 31.4, 31.5, 31.10 och 31.11 har bedömts i samband med anmälningsförfarandet inom ramen för dessa rättsakter.

Om en rättsakt som förtecknas i avsnitt A i bilaga I gör det möjligt för produkttillverkaren att välja att inte delta i en tredjepartsbedömning av överensstämmelse får tillverkaren, om den har tillämpat alla harmoniserade standarder som omfattar alla relevanta krav, använda detta alternativ endast om den också har tillämpat harmoniserade standarder eller, i tillämpliga fall, de gemensamma specifikationer som avses i artikel 41, som omfattar samtliga krav som anges i avsnitt 2 i detta kapitel.

4. AI-system med hög risk som redan har varit föremål för ett förfarande för bedömning av överensstämmelse ska genomgå ett nytt förfarande för bedömning av överensstämmelse i fall av en väsentlig ändring, oavsett om det ändrade systemet är avsett att distribueras vidare eller fortsätter att användas av den nuvarande tillhandahållaren.

När det gäller AI-system med hög risk som fortsätter att lära sig efter att det har släppts ut på marknaden eller tagits i bruk, ska sådana ändringar av AI-systemet med hög risk och dess prestanda som leverantören på förhand har fastställt vid tidpunkten för den inledande bedömningen av överensstämmelse och som är en del av den information som ingår i den tekniska dokumentation som avses i punkt 2 f i bilaga IV inte utgöra en väsentlig ändring.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 för att ändra bilagorna VI och VII genom att uppdatera dem mot bakgrund av teknisk utveckling.

6. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 för att ändra punkterna 1 och 2 i den här artikeln i syfte att låta de AI-system med hög risk som avses i punkterna 2–8 i bilaga III omfattas av det förfarande för bedömning av överensstämmelse som avses i bilaga VII eller delar därav. Kommissionen ska anta sådana delegerade akter med beaktande av hur ändamålsenligt förfarandet för bedömning av överensstämmelse grundat på intern kontroll enligt bilaga VI är när det gäller att förebygga eller minimera de risker för hälsa, säkerhet och skyddet av grundläggande rättigheter som sådana system medför samt vilken tillgång det finns till tillräcklig kapacitet och tillräckliga resurser bland anmälda organ.

Artikel 44

Intyg

1. De intyg som anmälda organ utfärdar i enlighet med bilaga VII ska vara upprättade på ett språk som är lätt att förstå för de relevanta myndigheterna i den medlemsstat där det anmälda organet är etablerat.

2. Intyg ska gälla under den tid som anges i dem och högst i fem år för AI-system som omfattas av bilaga I, och fyra år för AI-system som omfattas av bilaga III. På begäran av leverantören får intygets giltighet förlängas med högst fem år i taget för AI-system som omfattas av bilaga I, och fyra år för AI-system som omfattas av bilaga III, på grundval av en ny bedömning i enlighet med det tillämpliga förfarandet för bedömning av överensstämmelse. Eventuella tillägg till ett intyg ska vara giltiga, förutsatt att intyget är giltigt.

3. Om ett anmält organ konstaterar att ett AI-system inte längre uppfyller de krav som fastställs i avsnitt 2, ska det, med beaktande av proportionalitetsprincipen, tillfälligt eller slutligt återkalla det utfärdade intyget eller införa begränsningar för det, om det inte säkerställs att dessa krav uppfylls genom att systemleverantören vidtar lämpliga korrigerande åtgärder inom en rimlig tidsgräns som fastställts av det anmälda organet. Det anmälda organet ska motivera sitt beslut.

Det ska finnas ett förfarande för överklagande av de anmälda organens beslut, inbegripet om utfärdade intyg om överensstämmelse.

Artikel 45

Anmälda organs informationsskyldighet

1. Anmälda organ ska informera den anmälande myndigheten om följande:

a) Alla eventuella unionsintyg om bedömning av teknisk dokumentation, tillägg till dessa intyg samt godkännanden av kvalitetsstyrningssystem som utfärdats i enlighet med kraven i bilaga VII.

b) Eventuella avslag, begränsningar, tillfälliga återkallelser eller tillbakadraganden av ett unionsintyg om bedömning av teknisk dokumentation eller av ett godkännande av kvalitetsstyrningssystem som utfärdats i enlighet med kraven i bilaga VII.

c) Omständigheter som inverkar på omfattningen av eller villkoren för anmälan.

d) Begäranden från marknadskontrollmyndigheterna om information om bedömningar av överensstämmelse.

e) På begäran, bedömningar av överensstämmelse som gjorts inom ramen för anmälan och all annan verksamhet, inklusive gränsöverskridande verksamhet och underentreprenad.

2. Varje anmält organ ska underrätta de övriga anmälda organen om följande:

a) Godkännanden av kvalitetsstyrningssystem som det har vägrat utfärda eller tillfälligt återkallat eller dragit tillbaka och, på begäran, godkännanden av kvalitetsstyrningssystem som det har utfärdat.

b) Unionsintyg om bedömning av teknisk dokumentation eller tillägg till dessa intyg som det har avslagit, tillfälligt återkallat eller dragit tillbaka eller på annat sätt begränsat och, på begäran, de intyg och/eller tillägg till dessa som det har utfärdat.

3. Varje anmält organ ska ge de andra anmälda organ som utför liknande bedömningar av överensstämmelse avseende samma typer av AI-system relevant information om frågor som rör negativa och, på begäran, positiva resultat av bedömningar av överensstämmelse.

4. Anmälda organ ska säkerställa att den information som de erhåller behandlas konfidentiellt, i enlighet med artikel 78.

Artikel 46

Undantag från förfarandena för bedömning av överensstämmelse

1. Genom undantag från artikel 43 och på vederbörligen motiverad begäran får varje marknadskontrollmyndighet, av exceptionella skäl som rör allmän säkerhet eller skydd av människors liv och hälsa, miljöskydd eller skydd av viktiga industriella och infrastrukturella tillgångar, tillåta att specifika AI-system med hög risk släpps ut på marknaden eller tas i bruk inom den berörda medlemsstatens territorium. Tillståndet ska gälla under en begränsad period, medan de nödvändiga förfarandena för bedömning av överensstämmelse genomförs, med beaktande av de exceptionella skäl som motiverar undantaget. Dessa förfaranden ska slutföras utan oskäligt dröjsmål.

2. I en vederbörligen motiverad brådskande situation får brottsbekämpande myndigheter eller civilskyddsmyndigheter av exceptionella skäl som rör allmän säkerhet eller vid ett specifikt, betydande och överhängande hot mot fysiska personers liv eller fysiska säkerhet ta ett specifikt AI-system med hög risk i bruk utan det tillstånd som avses i punkt 1, förutsatt att ett sådant tillstånd begärs under eller efter användningen utan oskäligt dröjsmål. Om det tillstånd som avses i punkt 1 nekas ska användningen av AI-systemet med hög risk avbrytas med omedelbar verkan, och alla resultat och utdata från sådan användning ska omedelbart kasseras.

3. Det tillstånd som avses i punkt 1 ska utfärdas endast om marknadskontrollmyndigheten konstaterar att AI-systemet med hög risk uppfyller kraven i avsnitt 2. Marknadskontrollmyndigheten ska informera kommissionen och de andra medlemsstaterna om eventuella tillstånd som utfärdats enligt punkterna 1 och 2. Denna skyldighet omfattar inte känsliga operativa uppgifter som rör de brottsbekämpande myndigheternas verksamhet.

4. Tillståndet ska anses vara motiverat om ingen medlemsstat eller kommissionen har gjort någon invändning inom 15 kalenderdagar från mottagandet av den information som avses i punkt 3 om ett tillstånd utfärdat av en marknadskontrollmyndighet i en medlemsstat i enlighet med punkt 1.

5. Om en medlemsstat inom 15 kalenderdagar från mottagandet av den anmälan som avses i punkt 3 gör en invändning mot ett tillstånd som utfärdats av en marknadskontrollmyndighet i en annan medlemsstat, eller om kommissionen anser att tillståndet strider mot unionsrätten, eller att medlemsstatens slutsats om systemets överensstämmelse som avses i punkt 3 är ogrundad, ska kommissionen utan dröjsmål inleda samråd med den berörda medlemsstaten. De berörda operatörerna ska rådfrågas och ha möjlighet att framföra sina åsikter. Med beaktande av detta ska kommissionen besluta om tillståndet är motiverat eller inte. Kommissionen ska rikta sitt beslut till den berörda medlemsstaten och till de berörda operatörerna.

6. Om kommissionen anser att tillståndet är omotiverat ska det dras tillbaka av den berörda medlemsstatens marknadskontrollmyndighet.

7. För AI-system med hög risk som är relaterade till produkter som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I ska endast de undantag från bedömningen av överensstämmelse som fastställs i den unionsharmoniseringslagstiftningen tillämpas.

Artikel 47

EU-försäkran om överensstämmelse

1. Leverantören ska upprätta en skriftlig maskinläsbar, fysisk eller elektroniskt undertecknad EU-försäkran om överensstämmelse för varje AI-system med hög risk och kunna uppvisa den för de nationella behöriga myndigheterna i tio år efter det att AI-systemet med hög risk har släppts ut på marknaden eller tagits i bruk. I EU-försäkran om överensstämmelse ska det anges för vilket AI-system med hög risk den har upprättats. En kopia av EU-försäkran om överensstämmelse ska på begäran lämnas in till de berörda nationella behöriga myndigheterna.

2. I EU-försäkran om överensstämmelse ska det anges att det berörda AI-systemet med hög risk uppfyller kraven i avsnitt 2. EU-försäkran om överensstämmelse ska innehålla den information som anges i bilaga V och ska översättas till ett språk som är lätt att förstå för de nationella behöriga myndigheterna i de medlemsstater där AI-systemet med hög risk släpps ut på marknaden eller tillhandahålls.

3. Om AI-system med hög risk omfattas av annan unionsharmoniseringslagstiftning som också kräver en EU-försäkran om överensstämmelse ska en enda EU-försäkran om överensstämmelse upprättas med avseende på all unionsrätt som är tillämplig på AI-systemet med hög risk. Försäkran ska innehålla all information som krävs för att identifiera vilken unionsharmoniseringslagstiftning som försäkran gäller.

4. Genom att upprätta EU-försäkran om överensstämmelse ska leverantören ta på sig ansvaret för att kraven i avsnitt 2 uppfylls. Leverantören ska hålla EU-försäkran om överensstämmelse uppdaterad på lämpligt sätt.

5. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 i för att ändra bilaga V genom att uppdatera innehållet i den EU-försäkran om överensstämmelse som anges i den bilagan, för att introducera element som blir nödvändiga mot bakgrund av teknisk utveckling.

Artikel 48

CE-märkning

1. CE-märkningen ska omfattas av de allmänna principer som fastställs i artikel 30 i förordning (EG) nr 765/2008.

2. För AI-system med hög risk som tillhandahålls digitalt ska en digital CE-märkning användas endast om den lätt kan nås via det gränssnitt från vilket det systemet är tillgängligt eller via en lättillgänglig maskinläsbar kod eller andra elektroniska medel.

3. CE-märkningen ska anbringas på AI-system med hög risk så att den är synlig, läsbar och outplånlig. Om detta inte är möjligt eller lämpligt på grund av arten av AI-system med hög risk, ska märkningen anbringas på förpackningen eller den medföljande dokumentationen, beroende på vad som är lämpligt.

4. CE-märkningen ska i tillämpliga fall åtföljas av identifikationsnumret för det anmälda organ som ansvarar för de förfaranden för bedömning av överensstämmelse som föreskrivs i artikel 43. Det anmälda organets identifikationsnummer ska anbringas av organet självt eller, enligt organets anvisningar, av leverantören eller av leverantörens ombud. Identifikationsnumret ska också anges i reklammaterial där det nämns att AI-systemet med hög risk uppfyller kraven för CE-märkning.

5. Om AI-system med hög risk omfattas av annan unionsrätt som också föreskriver anbringande av CE-märkning ska CE-märkningen visa att AI-systemet med hög risk också uppfyller kraven i den andra lagstiftningen.

Artikel 49

Registrering

1. Innan ett AI-system med hög risk som förtecknas i bilaga III, med undantag för AI-system med hög risk som avses i punkt 2 i bilaga III, släpps ut på marknaden eller tas i bruk ska leverantören eller, i tillämpliga fall, ombudet registrera sig självt och systemet i den EU-databas som avses i artikel 71.

2. Innan ett AI-system för vilket leverantören har fastställt att det inte är ett AI-system med hög risk enligt artikel 6.3 släpps ut på marknaden eller tas i bruk ska leverantören eller, i tillämpliga fall, ombudet registrera sig självt och detta system i den EU-databas som avses i artikel 71.

3. Innan ett AI-system med hög risk som förtecknas i bilaga III, med undantag för AI-system med hög risk som förtecknas i punkt 2 i bilaga III, tas i bruk eller används, ska tillhandahållare som är offentliga myndigheter, unionens institutioner, byråer eller organ eller personer som agerar på deras vägnar, registrera sig, välja systemet och registrera dess användning i den EU-databas som avses i artikel 71.

4. För AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III, på områdena brottsbekämpning, migration, asyl och gränskontrollförvaltning, ska den registrering som avses i punkterna 1, 2 och 3 i denna artikel vara i en säker, icke-offentlig del av den EU-databas som avses i artikel 71 och ska, beroende på vad som är tillämpligt, omfatta endast följande information som avses i

a) avsnitt A punkterna 1–10 i bilaga VIII, med undantag för punkterna 6, 8 och 9,

b) avsnitt B punkterna 1–5, 8 och 9 i bilaga VIII,

c) avsnitt C punkterna 1–3 i bilaga VIII,

d) punkterna 1, 2, 3 och 5 i bilaga IX.

Endast kommissionen och de nationella myndigheter som avses i artikel 74.8 ska ha åtkomst till de respektive begränsade delar av EU-databasen som förtecknas i första stycket i denna punkt.

5. De AI-system med hög risk som avses i punkt 2 i bilaga III ska registreras på nationell nivå.

KAPITEL IV

TRANSPARENSSKYLDIGHETER FÖR LEVERANTÖRER OCH TILLHANDAHÅLLARE AV VISSA AI-SYSTEM

Artikel 50

Transparensskyldigheter för leverantörer och tillhandahållare av vissa AI-system

1. Leverantörer ska säkerställa att AI-system som är avsedda att interagera direkt med fysiska personer utformas och utvecklas på ett sådant sätt att de berörda fysiska personerna informeras om att de interagerar med ett AI-system, såvida detta inte är uppenbart för en fysisk person som är normalt informerad och skäligen uppmärksam och medveten, med beaktande av användningens omständigheter och sammanhang. Denna skyldighet är inte tillämplig på AI-system som enligt lag får upptäcka, förebygga, förhindra, utreda eller lagföra brott, med förbehåll för lämpliga garantier för tredje parters rättigheter och friheter, såvida inte dessa system är tillgängliga för allmänheten för att anmäla ett brott.

2. Leverantörer av AI-system, inbegripet AI-system för allmänna ändamål, som genererar syntetiskt ljud-, bild-, video- eller textinnehåll ska säkerställa att AI-systemets utdata är märkta i ett maskinläsbart format och kan upptäckas som artificiellt genererade eller manipulerade. Leverantörer ska säkerställa att deras tekniska lösningar är effektiva, interoperabla, robusta och tillförlitliga i den mån det är tekniskt möjligt, med beaktande av särdragen och begränsningarna hos olika typer av innehåll, genomförandekostnaderna och den allmänt erkända senaste utvecklingen, vilket kan återspeglas i relevanta tekniska standarder. Denna skyldighet är inte tillämplig i den mån AI-systemen utför en hjälpfunktion för vanlig redigering eller inte väsentligt ändrar de indata som tillhandahålls av tillhandahållaren eller deras semantik, eller om systemen enligt lag får upptäcka, förebygga, förhindra, utreda eller lagföra brott.

3. Tillhandahållare av ett system för känsloigenkänning eller ett system för biometrisk kategorisering ska informera de fysiska personer som exponeras för systemet om systemets drift, och ska behandla personuppgifter i enlighet med förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680, beroende på vad som är tillämpligt. Denna skyldighet är inte tillämplig på AI-system som används för biometrisk kategorisering och känsloigenkänning och som enligt lag får upptäcka, förebygga eller utreda brott, med förbehåll för lämpliga garantier för tredje parters rättigheter och friheter, och i enlighet med unionsrätten.

4. Tillhandahållare av ett AI-system som genererar eller manipulerar bild-, ljud- eller videoinnehåll som utgör en deepfake ska upplysa om att innehållet har genererats artificiellt eller manipulerats. Denna skyldighet är inte tillämplig om användningen enligt lag är tillåten för att upptäcka, förebygga, förhindra, utreda eller lagföra brott. Om innehållet utgör en del av ett uppenbart konstnärligt, kreativt, satiriskt, skönlitterärt eller liknande verk eller program, ska de transparenskrav som anges i denna punkt begränsas till att upplysa om förekomsten av sådant genererat eller manipulerat innehåll på ett lämpligt sätt som inte hindrar visningen eller åtnjutandet av verket.

Tillhandahållare av ett AI-system som genererar eller manipulerar text som offentliggörs i syfte att informera allmänheten om frågor av allmänt intresse ska upplysa om att texten har genererats artificiellt eller manipulerats. Denna skyldighet är inte tillämplig om användningen enligt lag är tillåten för att upptäcka, förebygga, förhindra, utreda eller lagföra brott eller om det AI-genererade innehållet har genomgått en process med mänsklig granskning eller redaktionell kontroll och om en fysisk eller juridisk person bär det redaktionella ansvaret för offentliggörandet av innehållet.

5. Den information som avses i punkterna 1–4 ska lämnas till de berörda fysiska personerna på ett tydligt och urskiljbart sätt senast vid tidpunkten för den första interaktionen eller exponeringen. Informationen ska uppfylla de tillämpliga tillgänglighetskraven.

6. Punkterna 1–4 påverkar inte de krav och skyldigheter som fastställs i kapitel III, och påverkar inte andra transparensskyldigheter som fastställs i unionsrätten eller nationell rätt för tillhandahållare av AI-system.

7. AI-byrån ska uppmuntra och underlätta utarbetandet av förfarandekoder på unionsnivå för att underlätta ett effektivt genomförande av skyldigheterna avseende upptäckt och märkning av artificiellt skapat eller manipulerat innehåll. Kommissionen får anta genomförandeakter för att godkänna dessa förfarandekoder i enlighet med förfarandet i artikel 56.6. Om kommissionen anser att förfarandekoden inte är lämplig får den anta en genomförandeakt som specificerar gemensamma regler för genomförandet av dessa skyldigheter i enlighet med det granskningsförfarande som fastställs i artikel 98.2.

KAPITEL V

AI-MODELLER FÖR ALLMÄNNA ÄNDAMÅL

AVSNITT 1

Klassificeringsregler

Artikel 51

Klassificering av AI-modeller för allmänna ändamål som AI-modeller för allmänna ändamål med systemrisk

1. En AI-modell för allmänna ändamål ska klassificeras som en AI-modell för allmänna ändamål med systemrisk om den uppfyller något av följande villkor:

a) Den har kapacitet med hög påverkansgrad som utvärderats på grundval av lämpliga tekniska verktyg och metoder, inbegripet indikatorer och riktmärken.

b) Den har, baserat på ett beslut av kommissionen, på eget initiativ eller efter en kvalificerad varning från den vetenskapliga panelen, kapacitet eller inverkan som motsvarar den som avses i led a med beaktande av kriterierna i bilaga XIII.

2. En AI-modell för allmänna ändamål ska förutsättas ha kapacitet med hög påverkansgrad enligt punkt 1 a om den sammanlagda beräkningsmängd som används för dess träning mätt i flyttalsberäkningar är större än 10^{25}.

3. Kommissionen ska anta delegerade akter i enlighet med artikel 97 för att ändra de tröskelvärden som anges i punkterna 1 och 2 i den här artikeln samt för att komplettera riktmärken och indikatorer mot bakgrund av teknisk utveckling, såsom algoritmiska förbättringar eller ökad hårdvarueffektivitet, när så krävs för att dessa tröskelvärden ska återspegla den senaste utvecklingen.

Artikel 52

Förfarande

1. Om en AI-modell för allmänna ändamål uppfyller det villkor som avses i artikel 51.1 a ska den berörda leverantören underrätta kommissionen utan dröjsmål och under alla omständigheter inom två veckor efter att kravet är uppfyllt eller det blir känt att det kommer att uppfyllas. Anmälan ska innehålla den information som krävs för att visa att det relevanta kravet har uppfyllts. Om kommissionen får kännedom om en AI-modell för allmänna ändamål som medför systemrisker och som den inte har underrättats om får den besluta att klassificera den som en modell med systemrisk.

2. Leverantören av en AI-modell för allmänna ändamål som uppfyller de villkor som avses i artikel 51.1 a får tillsammans med sin anmälan lägga fram tillräckligt underbyggda argument för att visa att AI-modellen för allmänna ändamål, även om den uppfyller det kravet, i detta undantagsfall inte medför systemrisker på grund av sina särskilda egenskaper och därför inte bör klassificeras som en AI-modell för allmänna ändamål med systemrisk.

3. Om kommissionen konstaterar att de argument som lagts fram enligt punkt 2 inte är tillräckligt underbyggda och att den berörda leverantören inte har kunnat visa att AI-modellen för allmänna ändamål, på grund av sina särskilda egenskaper, inte medför systemrisker ska den avvisa dessa argument, och AI-modellen för allmänna ändamål ska anses vara en AI-modell för allmänna ändamål med systemrisk.

4. Kommissionen får, på eget initiativ eller efter en kvalificerad varning från den vetenskapliga panelen enligt artikel 90.1 a, klassificera en AI-modell för allmänna ändamål som en AI-modell för allmänna ändamål med systemrisk, på grundval av kriterierna i bilaga XIII.

Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97 för att ändra bilaga XIII genom att specificera och uppdatera kriterierna i den bilagan.

5. På motiverad begäran av en leverantör vars modell har klassificerats som en AI-modell för allmänna ändamål med systemrisk enligt punkt 4 ska kommissionen beakta begäran och kan besluta att ompröva huruvida AI-modellen för allmänna ändamål fortfarande kan anses medföra systemrisker på grundval av kriterierna i bilaga XIII. En sådan begäran ska innehålla objektiva, detaljerade och nya skäl som har tillkommit sedan klassificeringsbeslutet fattades. Leverantörer får begära en ny bedömning tidigast sex månader efter klassificeringsbeslutet. Om kommissionen efter sin nya bedömning beslutar att behålla klassificeringen som en AI-modell för allmänna ändamål med systemrisk får leverantörerna begära en ny bedömning tidigast sex månader efter det beslutet.

6. Kommissionen ska säkerställa att en förteckning över AI-modeller för allmänna ändamål med systemrisk offentliggörs och ska hålla denna förteckning uppdaterad, utan att det påverkar behovet av att respektera och skydda immateriella rättigheter och konfidentiell affärsinformation eller företagshemligheter i enlighet med unionsrätten och nationell rätt.

AVSNITT 2

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål

Artikel 53

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål

1. Leverantörer av AI-modeller för allmänna ändamål ska

a) utarbeta och uppdatera den tekniska dokumentationen för modellen, inbegripet tränings- och testningsförfarandet samt resultaten av utvärderingen, som åtminstone ska innehålla de uppgifter som anges i bilaga XI, i syfte att på begäran lägga fram den för AI-byrån och de nationella behöriga myndigheterna,

b) utarbeta, uppdatera och göra information och dokumentation tillgänglig för leverantörer av AI-system som avser att integrera AI-modellen för allmänna ändamål i sina AI-system; utan att det påverkar behovet av att respektera och skydda immateriella rättigheter och konfidentiell affärsinformation eller företagshemligheter i enlighet med unionsrätten och nationell rätt ska informationen och dokumentationen

   i) göra det möjligt för leverantörer av AI-system att ha en god förståelse av kapaciteten och begränsningarna hos AI-modellen för allmänna ändamål och att fullgöra sina skyldigheter enligt denna förordning, och

   ii) minst innehålla de uppgifter som anges i bilaga XII,

c) införa en policy för att följa unionsrätten om upphovsrätt och närstående rättigheter, och i synnerhet för att identifiera och efterleva, inbegripet med hjälp av den senaste tekniken, ett förbehåll för rättigheter som uttryckts enligt artikel 4.3 i direktiv (EU) 2019/790,

d) utarbeta och göra en tillräckligt detaljerad sammanfattning av det innehåll som använts för träning av AI-modellen för allmänna ändamål allmänt tillgänglig, i enlighet med en mall som tillhandahålls av AI-byrån.

2. De skyldigheter som anges i punkt 1 a och b är inte tillämpliga på leverantörer av AI-modeller som släpps ut med en kostnadsfri licens med öppen källkod som möjliggör åtkomst, användning, ändring och distribution av modellen, och vars parametrar, inbegripet vikter, information om modellarkitekturen och information om modellanvändning, görs allmänt tillgängliga. Detta undantag är inte tillämpligt på AI-modeller för allmänna ändamål med systemrisker.

3. Leverantörer av AI-modeller för allmänna ändamål ska vid behov samarbeta med kommissionen och de nationella behöriga myndigheterna vid utövandet av sin behörighet och sina befogenheter enligt denna förordning.

4. Leverantörer av AI-modeller för allmänna ändamål får förlita sig på förfarandekoder i den mening som avses i artikel 56 för att visa att de fullgjort de skyldigheter som anges i punkt 1 i den här artikeln, till dess att en harmoniserad standard har offentliggjorts. Efterlevnad av europeiska harmoniserade standarder ger leverantörer presumtion om överensstämmelse i den utsträckning som de standarderna omfattar dessa skyldigheter. Leverantörer av AI-modeller för allmänna ändamål som inte följer en godkänd förfarandekod eller en europeisk harmoniserad standard ska uppvisa alternativa lämpliga sätt att uppfylla skyldigheterna, vilka ska bedömas av kommissionen.

5. I syfte att underlätta efterlevnaden av bilaga XI, särskilt punkt 2 d och e i den bilagan, ges kommissionen befogenhet att anta delegerade akter i enlighet med artikel 97 för att närmare specificera mät- och beräkningsmetoder i syfte att möjliggöra jämförbar och verifierbar dokumentation.

6. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 97.2 för att ändra bilagorna XI och XII mot bakgrund av pågående teknisk utveckling.

7. All information eller dokumentation som har erhållits enligt denna artikel, inbegripet företagshemligheter, ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

Artikel 54

Ombud för leverantörer av AI-modeller för allmänna ändamål

1. Innan leverantörer som är etablerade i tredjeländer släpper ut en AI-modell för allmänna ändamål på unionsmarknaden ska de genom skriftlig fullmakt utse ett ombud som är etablerat i unionen.

2. Leverantören ska göra det möjligt för sitt ombud att utföra de uppgifter som anges i fullmakten från leverantören.

3. Ombudet ska utföra de uppgifter som anges i fullmakten från leverantören. Ombudet ska på begäran lämna en kopia av fullmakten till AI-byrån på ett av unionsinstitutionernas officiella språk. Vid tillämpningen av denna förordning ska fullmakten ge ombudet befogenhet att utföra följande uppgifter:

a) Kontrollera att den tekniska dokumentation som anges i bilaga XI har upprättats och att alla skyldigheter som avses i artiklarna 53 och, i tillämpliga fall, 55 har fullgjorts av leverantören.

b) Kunna uppvisa en kopia av den tekniska dokumentation som anges i bilaga XI för AI-byrån och de nationella behöriga myndigheterna under en period på 10 år efter det att AI-modellen för allmänna ändamål har släppts ut på marknaden, och kontaktuppgifter för den leverantör som utsett ombudet.

c) På motiverad begäran förse AI-byrån med all information och dokumentation, inbegripet den som avses i led b, som krävs för att visa att den fullgör skyldigheterna i detta kapitel.

d) Samarbeta med AI-byrån och behöriga myndigheter, på motiverad begäran, när det gäller alla åtgärder som de vidtar med avseende på AI-modellen för allmänna ändamål, inbegripet när modellen är integrerad i AI-system som släpps ut på marknaden eller tas i bruk i unionen.

4. Fullmakten ska ge ombudet befogenhet att utöver eller i stället för leverantören stå till förfogande inför AI-byrån eller de behöriga myndigheterna, i alla frågor som rör efterlevnaden av denna förordning.

5. Ombudet ska säga upp fullmakten om denne anser eller har skäl att tro att leverantören agerar i strid med sina skyldigheter enligt denna förordning. I sådana fall ska det också omedelbart informera AI-byrån om uppsägningen av fullmakten och skälen till detta.

6. Den skyldighet som anges i denna artikel är inte tillämpligt på leverantörer av AI-modeller för allmänna ändamål som släpps ut med en kostnadsfri licens med öppen källkod som möjliggör åtkomst, användning, ändring och distribution av modellen, och vars parametrar, inbegripet vikter, information om modellarkitekturen och information om modellanvändning, görs allmänt tillgängliga, såvida inte AI-modellen för allmänna ändamål medför systemrisker.

AVSNITT 3

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål med systemrisk

Artikel 55

Skyldigheter för leverantörer av AI-modeller för allmänna ändamål med systemrisk

1. Utöver de skyldigheter som förtecknas i artiklarna 53 och 54 ska leverantörer av AI-modeller för allmänna ändamål med systemrisk

a) genomföra utvärderingar av modeller i enlighet med standardiserade protokoll och verktyg som återspeglar den aktuella tekniska nivån, inbegripet genomförande och dokumentation av antagonistisk testning av modellen i syfte att identifiera och minska systemrisker,

b) bedöma och minska eventuella systemrisker på unionsnivå, inbegripet källorna till dem, som kan härröra från utveckling, utsläppande på marknaden eller användning av AI-modeller för allmänna ändamål med systemrisk,

c) bevaka, dokumentera och utan oskäligt dröjsmål rapportera till AI-byrån och, i förekommande fall, till nationella behöriga myndigheter, relevant information om allvarliga incidenter och möjliga korrigerande åtgärder för att hantera dem,

d) säkerställa en lämplig nivå av cybersäkerhetsskydd för AI-modellen för allmänna ändamål med systemrisk och modellens fysiska infrastruktur.

2. Leverantörer av AI-modeller för allmänna ändamål med systemrisk får förlita sig på förfarandekoder i den mening som avses i artikel 56 för att visa att de fullgjort de skyldigheter som anges i punkt 1 i den här artikeln, till dess att en harmoniserad standard har offentliggjorts. Efterlevnad av europeiska harmoniserade standarder ger leverantörer presumtion om överensstämmelse i den utsträckning som de standarderna omfattar dessa skyldigheter. Leverantörer av AI-modeller för allmänna ändamål med systemrisker som inte följer en godkänd förfarandekod eller en europeisk harmoniserad standard ska uppvisa alternativa lämpliga sätt att uppfylla skyldigheterna, vilka ska bedömas av kommissionen.

3. All information eller dokumentation som har erhållits enligt denna artikel, inbegripet företagshemligheter, ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

AVSNITT 4

Förfarandekoder

Artikel 56

Förfarandekoder

1. AI-byrån ska uppmuntra och underlätta utarbetandet av förfarandekoder på unionsnivå för att bidra till en korrekt tillämpning av denna förordning, med beaktande av internationella strategier.

2. AI-byrån och styrelsen ska sträva efter att säkerställa att förfarandekoderna åtminstone omfattar de skyldigheter som fastställs i artiklarna 53 och 55, inbegripet följande aspekter:

a) Metoder för att säkerställa att den information som avses i artikel 53.1 a och b hålls uppdaterad mot bakgrund av marknadsutveckling och tekniska utveckling.

b) Lämplig detaljnivå för sammanfattningen av det innehåll som använts för träning.

c) Identifiering av systemriskernas typ och art på unionsnivå, inbegripet källorna till dem, när så är lämpligt.

d) Åtgärderna, förfarandena och formerna för bedömning och hantering av systemriskerna på unionsnivå, inbegripet dokumentationen av dessa, som ska stå i proportion till riskerna samt ta hänsyn till deras allvar och sannolikhet och till de särskilda utmaningarna med att hantera dessa risker mot bakgrund av de möjliga sätt på vilka sådana risker kan uppstå och bli verklighet längs AI-värdekedjan.

3. AI-byrån får uppmana alla leverantörer av AI-modeller för allmänna ändamål, samt relevanta nationella behöriga myndigheter, att delta i utarbetandet av förfarandekoder. Det civila samhällets organisationer, industrin, den akademiska världen och andra berörda parter, såsom leverantörer i efterföljande led och oberoende experter, får stödja processen.

4. AI-byrån och styrelsen ska sträva efter att säkerställa att förfarandekoderna innehåller tydligt angivna specifika mål samt åtaganden eller åtgärder, inbegripet centrala resultatindikatorer när så är lämpligt, för att säkerställa att dessa mål uppnås, och att de tar vederbörlig hänsyn till alla intressenters, inbegripet berörda personers, behov och intressen på unionsnivå.

5. AI-byrån ska sträva efter att säkerställa att deltagarna i förfarandekoderna regelbundet rapporterar till AI-byrån om genomförandet av åtagandena samt de åtgärder som vidtagits och deras resultat, även i förhållande till de centrala resultatindikatorerna när så är lämpligt. Centrala resultatindikatorer och rapporteringsåtaganden ska återspegla skillnader i storlek och kapacitet mellan olika deltagare.

6. AI-byrån och styrelsen ska regelbundet övervaka och utvärdera hur deltagarna uppnår förfarandekodernas mål och hur de bidrar till en korrekt tillämpning av denna förordning. AI-byrån och styrelsen ska bedöma huruvida förfarandekoderna omfattar de skyldigheter som fastställs i artiklarna 53 och 55, och ska regelbundet övervaka och utvärdera om målen i dem uppnås. De ska offentliggöra sin bedömning av förfarandekodernas lämplighet.

Kommissionen får genom en genomförandeakt godkänna en förfarandekod och ge den allmän giltighet inom unionen. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

7. AI-byrån får uppmana alla leverantörer av AI-modeller för allmänna ändamål att följa förfarandekoderna. För leverantörer av AI-modeller för allmänna ändamål som inte medför systemrisker får denna efterlevnad begränsas till de skyldigheter som föreskrivs i artikel 53, såvida de inte uttryckligen förklarar att de vill ansluta sig till den fullständiga koden.

8. AI-byrån ska, när så är lämpligt, också uppmuntra och underlätta översynen och anpassningen av förfarandekoderna, särskilt mot bakgrund av nya standarder. AI-byrån ska bistå vid bedömningen av tillgängliga standarder.

9. Förfarandekoder ska vara utarbetade senast den 2 maj 2025. AI-byrån ska vidta nödvändiga åtgärder, bland annat genom att uppmana leverantörer enligt punkt 7.

Om en förfarandekod inte kan färdigställas senast den 2 augusti 2025, eller om AI-byrån efter sin bedömning enligt punkt 6 i denna artikel anser att den inte är lämplig, får kommissionen genom genomförandeakter fastställa gemensamma regler för genomförandet av de skyldigheter som föreskrivs i artiklarna 53 och 55, inbegripet de aspekter som anges i punkt 2 i den här artikeln. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

KAPITEL VI

ÅTGÄRDER TILL STÖD FÖR INNOVATION

Artikel 57

Regulatoriska sandlådor för AI

1. Medlemsstaterna ska säkerställa att deras behöriga myndigheter inrättar minst en regulatorisk sandlåda för AI på nationell nivå, som ska vara i drift senast den 2 augusti 2026. Denna sandlåda får också inrättas tillsammans med de behöriga myndigheterna i andra medlemsstater. Kommissionen får tillhandahålla tekniskt stöd, rådgivning och verktyg för inrättande och drift av regulatoriska sandlådor för AI.

Skyldigheten enligt första stycket får också fullgöras genom deltagande i en befintlig sandlåda i den mån deltagandet ger en likvärdig nivå av nationell täckning för de deltagande medlemsstaterna.

2. Ytterligare regulatoriska sandlådor för AI får också inrättas på regional eller lokal nivå eller tillsammans med andra medlemsstaters behöriga myndigheter.

3. Europeiska datatillsynsmannen får också inrätta en regulatorisk sandlåda för AI för unionens institutioner, organ och byråer och får utöva de nationella behöriga myndigheternas roller och uppgifter i enlighet med detta kapitel.

4. Medlemsstaterna ska säkerställa att de behöriga myndigheter som avses i punkterna 1 och 2 anslår tillräckliga resurser för att uppfylla kraven i denna artikel, på ett ändamålsenligt sätt och i god tid. När så är lämpligt ska de nationella behöriga myndigheterna samarbeta med andra relevanta myndigheter, och de får tillåta deltagande av andra aktörer inom AI-ekosystemet. Denna artikel påverkar inte andra regulatoriska sandlådor som inrättats enligt unionsrätten eller nationell rätt. Medlemsstaterna ska säkerställa lämpligt samarbete mellan de myndigheter som utövar tillsyn över dessa andra sandlådor och de nationella behöriga myndigheterna.

5. Regulatoriska sandlådor för AI som inrättats enligt punkt 1 ska tillhandahålla en kontrollerad miljö som främjar innovation och underlättar utveckling, träning, testning och validering av innovativa AI-system under en begränsad tid innan de släpps ut på marknaden eller tas i bruk i enlighet med en särskild sandlådeplan som leverantörerna eller de potentiella leverantörerna och den behöriga myndigheten kommer överens om. Sådana sandlådor får omfatta testning under verkliga förhållanden under tillsyn i sandlådorna.

6. De behöriga myndigheterna ska, beroende på vad som är lämpligt, tillhandahålla vägledning, tillsyn och stöd inom den regulatoriska sandlådan för AI i syfte att identifiera risker, särskilt när det gäller grundläggande rättigheter, hälsa och säkerhet, testning, riskreducerande åtgärder och deras effektivitet i förhållande till skyldigheterna och kraven i denna förordning samt, i förekommande fall, annan unionsrätt och nationell rätt som är föremål för tillsyn inom sandlådan.

7. De behöriga myndigheterna ska ge leverantörer och potentiella leverantörer som deltar i den regulatoriska sandlådan för AI vägledning om rättsliga förväntningar och hur de krav och skyldigheter som fastställs i denna förordning ska uppfyllas.

På begäran av leverantören eller den potentiella leverantören av AI-systemet ska den behöriga myndigheten tillhandahålla ett skriftligt bevis på den verksamhet som framgångsrikt utförts i sandlådan. Den behöriga myndigheten ska också tillhandahålla en slutrapport med uppgifter om den verksamhet som bedrivs i sandlådan och tillhörande resultat och lärdomar. Leverantörer får använda sådan dokumentation för att visa att de uppfyller kraven i denna förordning genom förfarandet för bedömning av överensstämmelse eller relevant marknadskontroll. I detta avseende ska marknadskontrollmyndigheter och anmälda organ beakta slutrapporterna och de skriftliga bevis som tillhandahålls av den nationella behöriga myndigheten på ett positivt sätt, i syfte att påskynda förfaranden för bedömning av överensstämmelse i rimlig utsträckning.

8. Om inte annat följer av konfidentialitetsbestämmelserna i artikel 78 och med godkännande från leverantören eller den potentiella leverantören ska kommissionen och styrelsen ha rätt att få tillgång till slutrapporterna och ska beakta dem, på lämpligt sätt, när de utför sina uppgifter enligt denna förordning. Om både leverantören eller den potentiella leverantören och den nationella behöriga myndigheten uttryckligen samtycker får slutrapporten göras allmänt tillgänglig via den enda informationsplattform som avses i den här artikeln.

9. Inrättandet av regulatoriska sandlådor för AI ska syfta till att bidra till följande mål:

a) Förbättra rättssäkerheten för att uppnå efterlevnad av denna förordning eller, i förekommande fall, annan tillämplig unionsrätt och nationell rätt.

b) Stödja utbyte av bästa praxis genom samarbete med de myndigheter som deltar i den regulatoriska sandlådan för AI.

c) Främja innovation och konkurrenskraft och underlätta utvecklingen av ett AI-ekosystem.

d) Bidra till evidensbaserat regulatoriskt lärande.

e) Underlätta och påskynda tillträdet till unionsmarknaden för AI-system, särskilt när de tillhandahålls av små och medelstora företag, inbegripet uppstartsföretag.

10. I den mån de innovativa AI-systemen inbegriper behandling av personuppgifter eller på annat sätt faller inom tillsynsområdet för andra nationella myndigheter eller behöriga myndigheter som tillhandahåller eller stöder åtkomst till data ska de nationella behöriga myndigheterna säkerställa att de nationella dataskyddsmyndigheterna och dessa andra nationella eller behöriga myndigheter är involverade i driften av den regulatoriska sandlådan för AI och i tillsynen över dessa aspekter så långt deras respektive uppgifter och befogenheter sträcker sig.

11. De regulatoriska sandlådorna för AI påverkar inte tillsynsbefogenheterna eller de korrigerande befogenheterna för de behöriga myndigheter som utövar tillsyn över sandlådorna, inbegripet på regional eller lokal nivå. Alla betydande risker för hälsa och säkerhet och grundläggande rättigheter som upptäcks under utvecklingen och testningen av sådana AI-system ska leda till adekvata begränsningsåtgärder. De nationella behöriga myndigheterna ska ha befogenhet att tillfälligt eller permanent avbryta testprocessen eller deltagandet i sandlådan om inga verkningsfulla begränsningsåtgärder är möjliga och ska informera AI-byrån om ett sådant beslut. De nationella behöriga myndigheterna ska utöva sina tillsynsbefogenheter inom ramen för relevant rätt, med användning av sitt utrymme för skönsmässig bedömning när de genomför rättsliga bestämmelser för ett specifikt regulatoriskt sandlådeprojekt för AI, i syfte att stödja innovation inom AI i unionen.

12. Leverantörer och potentiella leverantörer som deltar i den regulatoriska sandlådan för AI ska förbli ansvariga, enligt tillämplig unionsrätt och nationell rätt om ansvar för skada som åsamkas tredje part till följd av de experiment som äger rum i sandlådan. Under förutsättning att de potentiella leverantörerna följer den särskilda planen och villkoren för deras deltagande samt i god tro följer de riktlinjer som den nationella behöriga myndigheten ger, ska myndigheterna dock inte ålägga några administrativa sanktionsavgifter för överträdelser av denna förordning. Om andra behöriga myndigheter med ansvar för annan unionsrätt och nationell rätt aktivt deltog i tillsynen av AI-systemet i sandlådan och tillhandahöll vägledning för efterlevnad ska inga administrativa sanktionsavgifter åläggas avseende den rätten.

13. De regulatoriska sandlådorna för AI ska utformas och genomföras på ett sådant sätt att de i relevanta fall underlättar gränsöverskridande samarbete mellan de nationella behöriga myndigheterna.

14. De nationella behöriga myndigheterna ska samordna sin verksamhet och samarbeta inom ramen för styrelsen.

15. De nationella behöriga myndigheterna ska informera AI-byrån och styrelsen om inrättandet av en sandlåda och får begära stöd och vägledning av dem. AI-byrån ska göra en förteckning över planerade och befintliga sandlådor allmänt tillgänglig och hålla den uppdaterad för att uppmuntra till mer interaktion i regulatoriska sandlådor för AI och gränsöverskridande samarbete.

16. De nationella behöriga myndigheterna ska lämna årliga rapporter till AI-byrån och styrelsen, från och med ett år efter att den regulatoriska sandlådan för AI har inrättats och därefter varje år fram till dess att den avslutas samt en slutrapport. Dessa rapporter ska innehålla information om framstegen och resultaten av genomförandet av dessa sandlådor, inbegripet bästa praxis, incidenter, tillvaratagna erfarenheter och rekommendationer om deras etablering och, i relevanta fall, om tillämpningen och en eventuell översyn av denna förordning, inbegripet dess delegerade akter och genomförandeakter, och om tillämpningen av annan unionsrätt som står under tillsyn av de berörda myndigheterna inom sandlådan. De nationella behöriga myndigheterna ska göra dessa årliga rapporter eller sammanfattningar av dessa tillgängliga för allmänheten online. Kommissionen ska, när så är lämpligt, beakta årsrapporterna när den utför sina uppgifter enligt denna förordning.

17. Kommissionen ska utveckla ett gemensamt och särskilt gränssnitt som innehåller all relevant information om regulatoriska sandlådor för AI för att göra det möjligt för berörda parter att interagera med regulatoriska sandlådor för AI och ta upp frågor med behöriga myndigheter samt söka icke-bindande vägledning om överensstämmelse för innovativa produkter, tjänster och affärsmodeller med inbäddad AI-teknik, i enlighet med artikel 62.1 c. Kommissionen ska proaktivt säkerställa samordning med nationella behöriga myndigheter, där så är relevant.

Artikel 58

Närmare arrangemang och funktionssätt för regulatoriska sandlådor för AI

1. För att undvika fragmentering i hela unionen ska kommissionen anta genomförandeakter som specificerar de närmare arrangemangen för inrättande, utveckling, genomförande, drift och tillsyn av regulatoriska sandlådor för AI. Dessa genomförandeakter ska innehålla gemensamma principer i följande frågor:

a) Behörighets- och urvalskriterier för deltagande i den regulatoriska sandlådan för AI.

b) Förfarandet för tillämpning, deltagande, övervakning, utträde ur och avslutande av den regulatoriska sandlådan för AI, inbegripet sandlådeplanen och slutrapporten.

c) De villkor som gäller för deltagarna.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

2. De genomförandeakter som avses i punkt 1 ska säkerställa att

a) regulatoriska sandlådor för AI är öppna för alla ansökande leverantörer eller potentiella leverantörer av ett AI-system som uppfyller behörighets- och urvalskriterier, som ska vara transparenta och rättvisa, och nationella behöriga myndigheter ska informera sökande om sitt beslut inom tre månader efter ansökan,

b) regulatoriska sandlådor för AI möjliggör bred och likvärdig tillgång och håller jämna steg med efterfrågan på deltagande; leverantörer och potentiella leverantörer får också lämna in ansökningar i partnerskap med tillhandahållare och andra relevanta tredje parter,

c) närmare arrangemang och villkor för regulatoriska sandlådor för AI i möjligaste mån stöder de nationella behöriga myndigheternas flexibilitet att inrätta och driva sina regulatoriska sandlådor för AI,

d) tillgången till regulatoriska sandlådor för AI är kostnadsfri för små och medelstora företag, inbegripet uppstartsföretag, utan att det påverkar exceptionella kostnader som nationella behöriga myndigheter får återkräva på ett rättvist och proportionellt sätt,

e) de, genom lärdomar från de regulatoriska sandlådorna för AI, gör det lättare för leverantörer och potentiella leverantörer att fullgöra skyldigheterna avseende bedömning av överensstämmelse enligt denna förordning och den frivilliga tillämpningen av de uppförandekoder som avses i artikel 95,

f) regulatoriska sandlådor för AI underlättar deltagandet av andra relevanta aktörer inom AI-ekosystemet, såsom anmälda organ och standardiseringsorganisationer, små och medelstora företag, inbegripet uppstartsföretag och andra företag, innovatörer, test- och experimentfaciliteter, forsknings- och experimentlaboratorier och europeiska digitala innovationsknutpunkter, kompetenscentrum samt enskilda forskare, för att möjliggöra och underlätta samarbete med den offentliga och privata sektorn,

g) förfaranden, processer och administrativa krav för ansökan och urval till, deltagande i och utträde ur den regulatoriska sandlådan för AI ska vara enkla, lättbegripliga och tydligt kommunicerade för att underlätta deltagandet av små och medelstora företag, inbegripet uppstartsföretag, med begränsad rättslig och administrativ kapacitet och strömlinjeformas i hela unionen i syfte att undvika fragmentering, och att deltagande i en regulatorisk sandlåda för AI som inrättats av en medlemsstat eller av Europeiska datatillsynsmannen erkänns ömsesidigt och enhetligt och har samma rättsliga verkan i hela unionen,

h) deltagandet i den regulatoriska sandlådan för AI är begränsat till en period som är lämplig med tanke på projektets komplexitet och omfattning, vilken får förlängas av den nationella behöriga myndigheten,

i) de regulatoriska sandlådorna för AI underlättar utvecklingen av verktyg och infrastruktur för testning, riktmärkning, bedömning och förklaring av de aspekter av AI-systemen som är relevanta för regulatoriskt lärande, såsom riktighet, robusthet och cybersäkerhet samt minimering av riskerna för grundläggande rättigheter och samhället i stort.

3. Potentiella leverantörer i regulatoriska sandlådor för AI, särskilt små och medelstora företag och uppstartsföretag, ska, när så är relevant, hänvisas till tjänster före införandet, såsom vägledning om genomförandet av denna förordning, andra mervärdestjänster såsom hjälp med standardiseringsdokument och certifiering, test- och experimentfaciliteter, europeiska digitala innovationsknutpunkter och kompetenscentrum.

4. När nationella behöriga myndigheter överväger att godkänna testning under verkliga förhållanden som står under tillsyn inom ramen för en regulatorisk sandlåda för AI som ska inrättas enligt denna artikel, ska de särskilt komma överens med deltagarna om villkoren för sådan testning och i synnerhet om lämpliga garantier, i syfte att skydda grundläggande rättigheter, hälsa och säkerhet. När så är lämpligt ska de samarbeta med andra nationella behöriga myndigheter i syfte att säkerställa enhetlig praxis i hela unionen.

Artikel 59

Ytterligare behandling av personuppgifter för utveckling av vissa AI-system i allmänhetens intresse i den regulatoriska sandlådan för AI

1. Personuppgifter som lagligen samlats in för andra ändamål får behandlas i den regulatoriska sandlådan för AI enbart i syfte att utveckla, träna och testa vissa AI-system i sandlådan om samtliga följande villkor är uppfyllda:

a) AI-systemen ska utvecklas för att ett viktigt allmänt intresse ska skyddas av en offentlig myndighet eller annan fysisk eller juridisk person på ett eller flera av följande områden:

   i) Allmän säkerhet och folkhälsa, inbegripet upptäckt, diagnostisering, förebyggande, bekämpning och behandling av sjukdomar och förbättring av hälso- och sjukvårdssystemen.

   ii) En hög nivå av skydd och förbättring av miljöns kvalitet, skydd av den biologiska mångfalden, skydd mot föroreningar, åtgärder för grön omställning samt begränsning av och anpassning till klimatförändringar.

   iii) Energihållbarhet.

   iv) Säkerhet och resiliens när det gäller transportsystem och mobilitet, kritisk infrastruktur och nätverk.

   v) Den offentliga förvaltningens och de offentliga tjänsternas effektivitet och kvalitet.

b) De data som behandlas är nödvändiga för att uppfylla ett eller flera av de krav som avses i kapitel III avsnitt 2 i fall där dessa krav inte kan uppfyllas effektivt genom behandling av anonymiserade eller syntetiska data eller andra icke-personuppgifter.

c) Det finns effektiva övervakningsmekanismer för att fastställa om experimenten i sandlådan kan medföra höga risker för de registrerades rättigheter och friheter, enligt artikel 35 i förordning (EU) 2016/679 och artikel 39 i förordning (EU) 2018/1725, samt en svarsmekanism för att snabbt begränsa dessa risker och, vid behov, stoppa behandlingen.

d) Alla personuppgifter som ska behandlas inom ramen för sandlådan befinner sig i en funktionellt separat, isolerad och skyddad databehandlingsmiljö under den potentiella leverantörens kontroll, och endast behöriga personer har tillgång till dessa uppgifter.

e) Leverantörer kan endast dela vidare de ursprungligen insamlade uppgifterna i enlighet med unionens dataskyddslagstiftning. Personuppgifter som skapats i sandlådan får inte delas utanför sandlådan.

f) Behandling av personuppgifter i samband med sandlådan ska varken leda till åtgärder eller beslut som påverkar de registrerade eller påverka tillämpningen av deras rättigheter enligt unionsrätten om skydd av personuppgifter.

g) Alla personuppgifter som behandlas inom ramen för sandlådan ska skyddas genom lämpliga tekniska och organisatoriska åtgärder och raderas när deltagandet i sandlådan har avslutats eller personuppgifternas lagringstid har löpt ut.

h) Loggarna över behandlingen av personuppgifter inom ramen för sandlådan ska bevaras under den tid som deltagandet i sandlådan varar, om inte annat föreskrivs i unionsrätten eller nationell rätt,

i) En fullständig och detaljerad beskrivning av processen och motiveringen för träning, testning och validering av AI-systemet bevaras tillsammans med testresultaten som en del av den tekniska dokumentation som avses i bilaga IV.

j) En kort sammanfattning av AI-projektet som utvecklats i sandlådan, dess mål och förväntade resultat offentliggörs på den behöriga myndighetens webbplats. Denna skyldighet omfattar inte känsliga operativa uppgifter som rör brottsbekämpande myndigheters, gränskontrollmyndigheters, migrationsmyndigheters eller asylmyndigheters verksamhet.

2. I syfte att förebygga, förhindra, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inbegripet att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten, under brottsbekämpande myndigheters överinseende och ansvar, ska behandlingen av personuppgifter i regulatoriska sandlådor för AI baseras på specifik unionsrätt eller nationell rätt och omfattas av samma kumulativa villkor som dem som avses i punkt 1.

3. Punkt 1 påverkar inte tillämpningen av unionsrätt eller nationell rätt som utesluter behandling av personuppgifter för andra ändamål än dem som uttryckligen anges i den rätten eller av unionsrätt eller nationell rätt som fastställer grunden för behandling av personuppgifter som är nödvändig för att utveckla, testa eller träna innovativa AI-system, eller av någon annan rättslig grund, i överensstämmelse med unionsrätten om skydd av personuppgifter.

Artikel 60

Testning av AI-system med hög risk under verkliga förhållanden utanför regulatoriska sandlådor för AI

1. Testning av AI-system med hög risk under verkliga förhållanden utanför regulatoriska sandlådor för AI får utföras av leverantörer eller potentiella leverantörer av AI-system med hög risk som förtecknas i bilaga III, i enlighet med denna artikel och den plan för testning under verkliga förhållanden som avses i denna artikel, utan att det påverkar förbuden enligt artikel 5.

Kommissionen ska genom genomförandeakter specificera de närmare inslagen i planen för testning under verkliga förhållanden. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

Denna punkt påverkar inte tillämpningen av unionsrätten eller nationell rätt om testning under verkliga förhållanden av AI-system med hög risk som är relaterade till produkter som omfattas av unionens harmoniseringslagstiftning som förtecknas i bilaga I.

2. Leverantörer eller potentiella leverantörer får på egen hand eller i partnerskap med en eller flera tillhandahållare eller potentiella tillhandahållare utföra testning under verkliga förhållanden av AI-system med hög risk som avses i bilaga III när som helst innan AI-systemet släpps ut på marknaden eller tas i bruk.

3. Testning av AI-system med hög risk under verkliga förhållanden enligt denna artikel påverkar inte etisk granskning som krävs enligt nationell rätt eller unionsrätten.

4. Leverantörer eller potentiella leverantörer får utföra testningen under verkliga förhållanden endast om samtliga följande villkor är uppfyllda:

a) Leverantören eller den potentiella leverantören har utarbetat en plan för testning under verkliga förhållanden och lämnat in den till marknadskontrollmyndigheten i den medlemsstat där testningen under verkliga förhållanden ska utföras.

b) Marknadskontrollmyndigheten i den medlemsstat där testningen under verkliga förhållanden ska utföras har godkänt testningen under verkliga förhållanden och planen för testning under verkliga förhållanden. Om marknadskontrollmyndigheten inte har lämnat något svar inom 30 dagar ska testningen under verkliga förhållanden och planen för testning under verkliga förhållanden betraktas som godkänd. Om det i nationell rätt inte föreskrivs något tyst godkännande, ska testningen under verkliga förhållanden fortfarande förutsätta ett tillstånd.

c) Leverantören eller den potentiella leverantören, med undantag för leverantörer eller potentiella leverantörer av AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III på områdena brottsbekämpning, migration, asyl och gränskontrollförvaltning samt AI-system med hög risk som avses i punkt 2 i bilaga III, har registrerat testning under verkliga förhållanden i enlighet med artikel 71.4 med ett unikt unionsomfattande identifieringsnummer och med den information som anges i bilaga IX. Leverantören eller den potentiella leverantören av AI-system med hög risk som avses i punkterna 1, 6 och 7 i bilaga III på områdena brottsbekämpning, migration, asyl och gränskontrollförvaltning, har registrerat testning under verkliga förhållanden i den säkra icke-offentliga delen av EU-databasen enligt artikel 49.4 d med ett unikt unionsomfattande identifieringsnummer och med den information som anges däri. Leverantören eller den potentiella leverantören av AI-system med hög risk som avses i punkt 2 i bilaga III har registrerat testning under verkliga förhållanden i enlighet med artikel 49.5.

d) Den leverantör eller potentiella leverantör som utför testningen under verkliga förhållanden är etablerad i unionen eller har utsett ett juridiskt ombud som är etablerat i unionen.

e) Uppgifter som samlats in och behandlats för testning under verkliga förhållanden ska överföras till tredjeländer endast om lämpliga och tillämpliga skyddsåtgärder enligt unionsrätten vidtas.

f) Testningen under verkliga förhållanden varar inte längre än vad som är nödvändigt för att uppnå dess mål och under inga omständigheter längre än sex månader, med möjlighet till förlängning med ytterligare sex månader om leverantören eller den potentiella leverantören gör en förhandsanmälan till marknadskontrollmyndigheten, som ska åtföljas av en förklaring av behovet av en sådan förlängning.

g) Försökspersoner i testningen under verkliga förhållanden som tillhör sårbara grupper på grund av ålder eller funktionsnedsättning skyddas på lämpligt sätt.

h) Om en leverantör eller potentiell leverantör organiserar testningen under verkliga förhållanden i samarbete med en eller flera tillhandahållare eller potentiella tillhandahållare, har dessa informerats om alla aspekter av testningen som är relevanta för deras beslut att delta och fått den relevanta bruksanvisningen för det AI-system som avses i artikel 13. Leverantören eller den potentiella leverantören och tillhandahållaren eller den potentiella tillhandahållaren ska ingå ett avtal som anger deras roller och ansvar i syfte att säkerställa överensstämmelse med bestämmelserna om testning under verkliga förhållanden enligt denna förordning och enligt annan tillämplig unionsrätt och nationell rätt.

i) Försökspersonerna i testningen under verkliga förhållanden har gett sitt informerade samtycke i enlighet med artikel 61, eller, när det gäller brottsbekämpning, om en begäran om informerat samtycke skulle hindra AI-systemet att testas, får själva testningen och resultatet av testningen under verkliga förhållanden inte ha någon negativ inverkan på försökspersonerna, och deras personuppgifter ska raderas när testningen har utförts.

j) Testningen under verkliga förhållanden övervakas effektivt av leverantören eller den potentiella leverantören och av tillhandahållare eller potentiella tillhandahållare genom personer som har lämpliga kvalifikationer inom det berörda området och som har nödvändig kapacitet, utbildning och auktoritet för att utföra sina uppgifter.

k) AI-systemets förutsägelser, rekommendationer eller beslut kan effektivt upphävas eller ignoreras.

5. Försökspersoner inom testningen under verkliga förhållanden, eller deras lagligen utsedda företrädare, beroende på vad som är lämpligt, får, utan att detta medför nackdelar och utan att behöva lämna någon motivering, när som helst avsluta sitt deltagande i testningen genom att dra tillbaka sitt informerade samtycke och får begära omedelbar och permanent radering av sina personuppgifter. Tillbakadragandet av det informerade samtycket påverkar inte den verksamhet som redan utförts.

6. I enlighet med artikel 75 ska medlemsstaterna ge sina marknadskontrollmyndigheter befogenhet att kräva att leverantörer och potentiella leverantörer tillhandahåller information, att utföra oanmälda inspektioner på distans eller på plats och att utföra kontroller av utförandet av testningen under verkliga förhållanden och tillhörande AI-system med hög risk. Marknadskontrollmyndigheterna ska använda dessa befogenheter för att säkerställa en säker utveckling av testning under verkliga förhållanden.

7. Alla allvarliga incidenter som identifieras under testningen under verkliga förhållanden ska rapporteras till den nationella marknadskontrollmyndigheten i enlighet med artikel 73. Leverantören eller den potentiella leverantören ska vidta omedelbara riskbegränsningsåtgärder eller, om så inte sker, tillfälligt avbryta testningen under verkliga förhållanden tills sådan riskreducering äger rum eller i annat fall avsluta den. Leverantören eller den potentiella leverantören ska fastställa ett förfarande för snabb återkallelse av AI-systemet när testningen under verkliga förhållanden avslutas på detta sätt.

8. Leverantörer eller potentiella leverantörer ska underrätta den nationella marknadskontrollmyndigheten i den medlemsstat där testningen under verkliga förhållanden ska utföras om det tillfälliga avbrottet i eller avslutandet av testningen under verkliga förhållanden och om de slutliga resultaten.

9. Leverantören och den potentiella leverantören ska vara ansvariga enligt tillämplig unionsrätt och nationell rätt om ansvar för eventuella skador som orsakas under deras deltagande i testningen under verkliga förhållanden.

Artikel 61

Informerat samtycke till deltagande i testning under verkliga förhållanden utanför regulatoriska sandlådor för AI

1. För testning under verkliga förhållanden enligt artikel 60 ska frivilligt lämnat informerat samtycke erhållas från försökspersonerna innan de deltar i sådan testning och efter att de vederbörligen har informerats med koncis, tydlig, relevant och begriplig information om

a) vilken karaktär och vilka mål som testningen under verkliga förhållanden har och de eventuella olägenheter som kan vara förknippade med att delta,

b) de förhållanden under vilka testningen under verkliga förhållanden ska utföras, inbegripet den förväntade varaktigheten för försökspersonens eller försökspersonernas deltagande,

c) sina rättigheter och garantierna avseende sitt deltagande, särskilt sin rätt att vägra att delta och att när som helst avsluta sitt deltagande i testningen under verkliga förhållanden utan negativa följder och utan att behöva motivera sitt beslut,

d) formerna för begäran om upphävande eller ignorerande av AI-systemets förutsägelser, rekommendationer eller beslut,

e) det unika unionsomfattande identifieringsnumret för testningen under verkliga förhållanden i enlighet med artikel 60.4 c och kontaktuppgifter för leverantören eller dennes juridiska ombud från vilka ytterligare information kan erhållas.

2. Det informerade samtycket ska dateras och dokumenteras och en kopia ska ges till försökspersonerna i testningen eller till deras juridiska ombud.

Artikel 62

Åtgärder för leverantörer och tillhandahållare, särskilt små och medelstora företag, inbegripet uppstartsföretag

1. Medlemsstaterna ska vidta följande åtgärder:

a) Ge små och medelstora företag, inbegripet uppstartsföretag, som har ett säte eller en filial i unionen prioriterad tillgång till de regulatoriska sandlådorna för AI, i den mån de uppfyller behörighetskraven och urvalskriterierna. Den prioriterade tillgången hindrar inte andra små och medelstora företag, inbegripet uppstartsföretag, än dem som avses i denna punkt, att ha tillgång till den regulatoriska sandlådan för AI, förutsatt att de också uppfyller behörighetskraven och urvalskriterierna.

b) Anordna särskilda medvetandehöjande åtgärder och utbildning om tillämpningen av denna förordning anpassat till behoven hos små och medelstora företag, inbegripet uppstartsföretag, tillhandahållare och, när så är lämpligt, lokala offentliga myndigheter.

c) Använda befintliga särskilda kanaler och, när så är lämpligt, upprätta nya sådana för kommunikation med små och medelstora företag, inbegripet uppstartsföretag, tillhandahållare, andra innovatörer och, om lämpligt, lokala offentliga myndigheter, för att ge råd och svara på frågor om genomförandet av denna förordning, inbegripet när det gäller deltagande i regulatoriska sandlådor för AI.

d) Underlätta små och medelstora företags och andra berörda parters deltagande i processen för standardiseringsutveckling.

2. De särskilda intressen och behov som små och medelstora företag, inbegripet uppstartsföretag, har som leverantörer ska beaktas när avgifterna för bedömning av överensstämmelse enligt artikel 43 fastställs, och avgifterna ska minskas i proportion till deras storlek, marknadsstorlek och andra relevanta indikatorer.

3. AI-byrån ska vidta följande åtgärder:

a) Tillhandahålla standardiserade mallar för områden som omfattas av denna förordning, i enlighet med styrelsens anvisningar i dess begäran.

b) Utveckla och upprätthålla en enda informationsplattform som ger information som är lätt att använda om denna förordning till alla operatörer i hela unionen.

c) Anordna lämpliga kommunikationskampanjer för att öka medvetenheten om de skyldigheter som följer av denna förordning,

d) Utvärdera och främja konvergens av bästa praxis i förfaranden för offentlig upphandling när det gäller AI-system.

Artikel 63

Undantag för särskilda operatörer

1. Mikroföretag i den mening som avses i rekommendation 2003/361/EG får på ett förenklat sätt efterleva vissa delar av det kvalitetsstyrningssystem som krävs enligt artikel 17 i denna förordning, förutsatt att de inte har partnerföretag eller anknutna företag i den mening som avses i den rekommendationen. För detta ändamål ska kommissionen utarbeta riktlinjer för de delar av kvalitetsstyrningssystemet som får efterlevas på ett förenklat sätt med beaktande av mikroföretags behov, utan att det påverkar skyddsnivån eller behovet av efterlevnad av kraven med avseende på AI-system med hög risk.

2. Punkt 1 i denna artikel ska inte tolkas som att dessa operatörer undantas från att uppfylla andra krav eller fullgöra andra skyldigheter som fastställs i denna förordning, inbegripet dem som fastställs i artiklarna 9, 10, 11, 12, 13, 14, 15, 72 och 73.

KAPITEL VII

STYRNING

AVSNITT 1

Styrning på unionsnivå

Artikel 64

AI-byrån

1. Kommissionen ska utveckla unionens sakkunskap och kapacitet på AI-området genom AI-byrån.

2. Medlemsstaterna ska underlätta de uppgifter som anförtros AI-byrån, i enlighet med vad som återspeglas i denna förordning.

Artikel 65

Inrättande av och strukturen för den europeiska styrelsen för artificiell intelligens

1. En europeisk styrelse för artificiell intelligens (*styrelsen*) inrättas härmed.

2. Styrelsen ska bestå av en företrädare per medlemsstat. Europeiska datatillsynsmannen ska delta som observatör. Även AI-byrån ska närvara vid styrelsens möten, utan att delta i omröstningarna. Andra myndigheter, organ eller experter på nationell nivå och unionsnivå får bjudas in till mötena av styrelsen från fall till fall, om de frågor som diskuteras är relevanta för dem.

3. Varje företrädare ska utses av sin medlemsstat för en period på tre år som får förnyas en gång.

4. Medlemsstaterna ska säkerställa att deras företrädare i styrelsen

a) har relevant behörighet och relevanta befogenheter i sin medlemsstat för att aktivt bidra till fullgörandet av styrelsens uppgifter enligt artikel 66,

b) utses till gemensam kontaktpunkt gentemot styrelsen och när så är lämpligt, med beaktande av medlemsstaternas behov, till gemensam kontaktpunkt för de berörda parterna,

c) har befogenhet att underlätta enhetlighet och samordning mellan nationella behöriga myndigheter i sina medlemsstater när det gäller genomförandet av denna förordning, bland annat genom insamling av relevanta uppgifter och relevant information för att de ska kunna fullgöra sina uppgifter i styrelsen.

5. Medlemsstaternas utsedda företrädare ska anta styrelsens arbetsordning med två tredjedels majoritet. Arbetsordningen ska särskilt föreskriva förfaranden för urvalsprocessen, mandatets varaktighet och specifikationer för ordförandens uppgifter, närmare omröstningsregler och organisationen av styrelsens och dess undergruppers verksamhet.

6. Styrelsen ska inrätta två ständiga undergrupper som ska tillhandahålla en plattform för samarbete och utbyte mellan marknadskontrollmyndigheter och anmälande myndigheter i frågor som rör marknadskontroll respektive anmälda organ.

Den ständiga undergruppen för marknadskontroll bör fungera som grupp för administrativt samarbete (Adco-grupp) för denna förordning i den mening som avses i artikel 30 i förordning (EU) 2019/1020.

Styrelsen får inrätta andra ständiga eller tillfälliga undergrupper när så är lämpligt i syfte att granska specifika frågor. När så är lämpligt får företrädare för det rådgivande forum som avses i artikel 67 bjudas in till sådana undergrupper eller till särskilda möten i dessa arbetsgrupper som observatörer.

7. Styrelsen ska vara organiserad och fungera på ett sådant sätt att objektiviteten och opartiskheten i dess verksamhet skyddas.

8. En av företrädarna för medlemsstaterna ska vara ordförande i styrelsen. AI-byrån ska bistå styrelsen med ett sekretariat, sammankalla till möten på begäran av ordföranden och förbereda dagordningen i enlighet med styrelsens uppdrag enligt denna förordning och dess arbetsordning.

Artikel 66

Styrelsens uppgifter

Styrelsen ska ge råd till och bistå kommissionen och medlemsstaterna för att underlätta en konsekvent och effektiv tillämpning av denna förordning. För detta ändamål får styrelsen särskilt

a) bidra till samordningen mellan de nationella behöriga myndigheter som ansvarar för tillämpningen av denna förordning och, i samarbete med de berörda marknadskontrollmyndigheterna och med dessas samtycke, stödja marknadskontrollmyndigheternas gemensamma aktiviteter, som avses i artikel 74.11,

b) samla in och utbyta teknisk och regleringsmässig sakkunskap och bästa praxis bland medlemsstaterna,

c) ge råd om genomförandet av denna förordning, särskilt när det gäller kontroll av efterlevnaden av reglerna om AI-modeller för allmänna ändamål,

d) bidra till harmoniseringen av administrativ praxis i medlemsstaterna, inbegripet när det gäller det undantag från de förfaranden för bedömning av överensstämmelse som avses i artikel 46, funktionen hos de regulatoriska sandlådorna för AI och testning under verkliga förhållanden som avses i artiklarna 57, 59 och 60,

e) på begäran av kommissionen eller på eget initiativ utfärda rekommendationer och skriftliga yttranden om alla relevanta frågor som rör genomförandet av denna förordning och dess konsekventa och effektiva tillämpning, inbegripet

   i) om utarbetande och tillämpning av uppförandekoder och förfarandekoder enligt denna förordning samt av kommissionens riktlinjer,

   ii) utvärderingen och översynen av denna förordning enligt artikel 112, inbegripet när det gäller de rapporter om allvarliga incidenter som avses i artikel 73, och funktionen för den EU-databas som avses i artikel 71, utarbetandet av delegerade akter eller genomförandeakter, och vad gäller eventuella anpassningar av denna förordning till unionens harmoniseringslagstiftning som förtecknas i bilaga I,

   iii) om tekniska specifikationer eller befintliga standarder avseende de krav som anges i kapitel III avsnitt 2,

iv) om användning av harmoniserade standarder eller gemensamma specifikationer som avses i artiklarna 40 och 41,

v) trender, såsom europeisk global konkurrenskraft inom AI, användningen av AI i unionen och utvecklingen av digitala färdigheter,

vi) trender för AI-värdekedjors föränderliga typologi, särskilt när det gäller de därav följande konsekvenserna vad gäller ansvarsskyldighet,

vii) om det potentiella behovet av att ändra bilaga III i enlighet med artikel 7 och om det potentiella behovet av en eventuell översyn av artikel 5 enligt artikel 112, med beaktande av relevanta tillgängliga evidens och den senaste teknikutvecklingen,

f) stödja kommissionen med att främja AI-kunnighet, allmänhetens medvetenhet om och förståelsen av fördelar, risker, skyddsåtgärder och rättigheter och skyldigheter i samband med användningen av AI-system,

g) underlätta utvecklingen av gemensamma kriterier och en gemensam förståelse bland marknadsaktörer och behöriga myndigheter om de relevanta begrepp som anges i denna förordning, inbegripet genom att bidra till utvecklingen av riktmärken,

h) vid behov samarbeta med andra av unionens institutioner, organ, och byråer och med unionens relevanta expertgrupper och nätverk, särskilt på områdena produktsäkerhet, cybersäkerhet, konkurrenskraft, digitala tjänster och medietjänster, finansiella tjänster, konsumentskydd, dataskydd och skydd av grundläggande rättigheter,

i) bidra till ett effektivt samarbete med behöriga myndigheter i tredjeländer och med internationella organisationer,

j) bistå nationella behöriga myndigheter och kommissionen i utvecklingen av den organisatoriska och tekniska expertis som krävs för genomförandet av denna förordning, bland annat genom att bidra till bedömningen av utbildningsbehoven för den personal från medlemsstater som deltar i genomförandet av denna förordning.

k) bistå AI-byrån i stödet till nationella behöriga myndigheter vid inrättandet och utvecklingen av regulatoriska sandlådor för AI, och underlätta samarbete och informationsutbyte mellan regulatoriska sandlådor för AI,

l) bidra till och ge relevanta råd om utarbetandet av vägledande dokument,

m) ge kommissionen råd i internationella AI-frågor,

n) avge yttranden till kommissionen om kvalificerade varningar avseende AI-modeller för allmänna ändamål,

o) ta emot yttranden från medlemsstaterna om kvalificerade varningar om AI-modeller för allmänna ändamål och om nationella erfarenheter och nationell praxis när det gäller övervakning och kontroll av efterlevnad avseende AI-system, särskilt system som integrerar AI-modellerna för allmänna ändamål.

Artikel 67

Rådgivande forum

1. Ett rådgivande forum ska inrättas för att tillhandahålla teknisk expertis och ge råd till styrelsen och kommissionen och bidra till deras uppgifter enligt denna förordning.

2. Medlemmarna i det rådgivande forumet ska representera ett balanserat urval av berörda parter, däribland branschen, uppstartsföretag, små och medelstora företag, det civila samhället, och den akademiska världen. Sammansättningen av det rådgivande forumet ska vara balanserad med avseende på kommersiella och icke-kommersiella intressen samt, inom kategorin kommersiella intressen, med avseende på små och medelstora företag och andra företag.

3. Kommissionen ska utse medlemmarna i det rådgivande forumet i enlighet med kriterierna i punkt 2 bland berörda parter med erkänd sakkunskap på AI-området.

4. Mandatperioden för medlemmarna i det rådgivande forumet ska vara två år, som får förlängas med högst fyra år.

5. Europeiska unionens byrå för grundläggande rättigheter, Europeiska unionens cybersäkerhetsbyrå (Enisa), Europeiska standardiseringskommittén (CEN), Europeiska kommittén för elektroteknisk standardisering (Cenelec) och Europeiska institutet för telekommunikationsstandarder (Etsi) ska vara ständiga medlemmar i det rådgivande forumet.

6. Det rådgivande forumet ska själv utarbeta sin arbetsordning. Den ska välja två medordförande bland sina medlemmar i enlighet med kriterierna i punkt 2. Medordförandenas mandatperiod ska vara två år och får förlängas en gång.

7. Det rådgivande forumet ska hålla möten minst två gånger per år. Det rådgivande forumet får bjuda in experter och andra berörda parter till sina möten.

8. Det rådgivande forumet får utarbeta yttranden, rekommendationer och skriftliga bidrag på begäran av styrelsen eller kommissionen.

9. Det rådgivande forumet får inrätta permanenta eller tillfälliga undergrupper enligt vad som är lämpligt för att utreda specifika frågor med avseende på målen för denna förordning.

10. Det rådgivande forumet ska utarbeta en årsrapport om sin verksamhet. Den rapporten ska göras allmänt tillgänglig.

Artikel 68

Vetenskaplig panel av oberoende experter

1. Kommissionen ska genom en genomförandeakt fastställa bestämmelser om inrättandet av en vetenskaplig panel av oberoende experter (*den vetenskapliga panelen*) som ska stödja verksamheten för efterlevnadskontroll enligt denna förordning. Genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

2. Den vetenskapliga panelen ska bestå av experter som valts ut av kommissionen på grundval av aktuell vetenskaplig eller teknisk expertis på AI-området och som är nödvändiga för de uppgifter som anges i punkt 3, och de ska kunna visa att de uppfyller samtliga följande villkor:

a) Särskild sakkunskap och kompetens samt vetenskaplig eller teknisk expertis på AI-området.

b) Oberoende ställning i förhållande till leverantörer av AI-system eller AI-modeller för allmänna ändamål.

c) Förmåga att bedriva verksamhet aktsamt, korrekt och objektivt.

Kommissionen ska i samråd med styrelsen fastställa antalet experter i panelen i enlighet med vad som krävs och säkerställa en rättvis könsfördelning och geografisk representation.

3. Den vetenskapliga panelen ska ge råd till och stödja AI-byrån, särskilt när det gäller följande uppgifter:

a) Stödja genomförandet och kontrollen av efterlevnaden av denna förordning vad gäller AI-modeller och AI-system för allmänna ändamål, särskilt genom att

   i) varna AI-byrån för eventuella systemrisker på unionsnivå för AI-modeller för allmänna ändamål, i enlighet med artikel 90,

   ii) bidra till utvecklingen av verktyg och metoder för utvärdering av kapaciteten hos AI-modeller och AI-system för allmänna ändamål, bland annat genom riktmärken,

   iii) ge råd om klassificeringen av AI-modeller för allmänna ändamål med systemrisk,

   iv) ge råd om klassificeringen av olika AI-modeller för allmänna ändamål och AI-system för allmänna ändamål,

v) bidra till utvecklingen av verktyg och mallar.

b) På begäran av marknadskontrollmyndigheterna stödja deras arbete.

c) Stödja gränsöverskridande marknadskontrollsverksamhet enligt artikel 74.11, utan att det påverkar marknadskontrollmyndigheternas befogenheter.

d) Stödja AI-byrån när den utför sina uppgifter inom ramen för unionsförfarandet för skyddsåtgärder enligt artikel 81.

4. Experterna i den vetenskapliga panelen ska utföra sina uppgifter opartiskt och objektivt och säkerställa att den information och de uppgifter som de erhåller vid utförandet av sina uppgifter och sin verksamhet behandlas konfidentiellt. De får varken begära eller ta emot instruktioner från någon när de utövar sina uppgifter enligt punkt 3. Varje expert ska avge en intresseförklaring, som ska göras allmänt tillgänglig. AI-byrån ska fastställa system och förfaranden för att aktivt hantera och förebygga potentiella intressekonflikter.

5. Den genomförandeakt som avses i punkt 1 ska innehålla bestämmelser om villkor, förfaranden och närmare arrangemang för att den vetenskapliga panelen och dess medlemmar ska utfärda varningar och begära bistånd från AI-byrån för utförandet av den vetenskapliga panelens uppgifter.

Artikel 69

Medlemsstaternas tillgång till poolen av experter

1. Medlemsstaterna får anlita experter i den vetenskapliga panelen för att stödja deras verksamhet för efterlevnadskontroll enligt denna förordning.

2. Medlemsstaterna får åläggas att betala avgifter för experternas rådgivning och stöd. Avgifternas struktur och nivå samt de ersättningsgilla kostnadernas omfattning och struktur ska anges i den genomförandeakt som avses i artikel 68.1, med beaktande av målen att få till stånd ett korrekt genomförande av denna förordning, kostnadseffektivitet och behovet av att säkerställa att alla medlemsstater har faktisk tillgång till experter.

3. Kommissionen ska vid behov underlätta för medlemsstaterna att i tid få tillgång till experterna och ska säkerställa att kombinationen av den stödverksamhet som utförs av unionens stödstrukturer för AI-testning enligt artikel 84 och experter enligt denna artikel organiseras effektivt och tillför bästa möjliga mervärde.

AVSNITT 2

Nationella behöriga myndigheter

Artikel 70

Utseende av nationella behöriga myndigheter och gemensamma kontaktpunkter

1. Varje medlemsstat ska vid tillämpning av denna förordning som nationella behöriga myndigheter inrätta eller utse minst en anmälande myndighet och minst en marknadskontrollmyndighet. Dessa nationella behöriga myndigheter ska utöva sina befogenheter på ett oberoende, objektivt och opartiskt sätt för att säkerställa objektiviteten i sina aktiviteter och uppgifter och för att säkerställa tillämpningen och genomförandet av denna förordning. Personalen vid dessa myndigheter ska avhålla sig från varje handling som är oförenlig med deras uppdrag. Förutsatt att dessa principer respekteras får sådana aktiviteter och uppgifter utföras av en eller flera utsedda myndigheter, i enlighet med medlemsstatens organisatoriska behov.

2. Medlemsstaterna ska meddela kommissionen identiteten på de anmälande myndigheterna och marknadskontrollmyndigheterna och dessa myndigheters uppgifter samt eventuella senare ändringar av dessa. Medlemsstaterna ska göra information om hur behöriga myndigheter och gemensamma kontaktpunkter kan kontaktas genom elektroniska kommunikationsmedel allmänt tillgänglig senast 2 augusti 2025. Medlemsstaterna ska utse en marknadskontrollmyndighet som ska fungera som gemensam kontaktpunkt för denna förordning och underrätta kommissionen om den gemensamma kontaktpunktens identitet. Kommissionen ska göra en förteckning över gemensamma kontaktpunkter allmänt tillgänglig.

3. Medlemsstaterna ska säkerställa att deras nationella behöriga myndigheter har tillräckliga tekniska och ekonomiska resurser samt personalresurser, och infrastruktur för att kunna fullgöra sina uppgifter på ett ändamålsenligt sätt enligt denna förordning. I synnerhet ska de nationella behöriga myndigheterna ha ett tillräckligt antal anställda till ständigt förfogande, vars kompetens och sakkunskap ska inbegripa en ingående förståelse av AI-teknik, data och databehandling, skydd av personuppgifter, cybersäkerhet, grundläggande rättigheter, hälso- och säkerhetsrisker och kunskap om befintliga standarder och rättsliga krav. Medlemsstaterna ska varje år bedöma och, vid behov, uppdatera de kompetens- och resurskrav som avses i denna punkt.

4. De nationella behöriga myndigheterna ska vidta lämpliga åtgärder för att säkerställa en lämplig nivå av cybersäkerhet.

5. De nationella behöriga myndigheterna ska när de utför sina uppgifter agera i enlighet med de konfidentialitetskrav som anges i artikel 78.

6. Senast den 2 augusti 2025 och därefter vartannat år ska medlemsstaterna rapportera till kommissionen om statusen för de nationella behöriga myndigheternas ekonomiska resurser och personalresurser, med en bedömning av deras tillräcklighet. Kommissionen ska översända denna information till styrelsen för diskussion och eventuella rekommendationer.

7. Kommissionen ska underlätta erfarenhetsutbytet mellan nationella behöriga myndigheter.

8. Nationella behöriga myndigheter får ge vägledning och råd om genomförandet av denna förordning, i synnerhet till små och medelstora företag, inbegripet uppstartsföretag, med beaktande av styrelsens och kommissionens vägledning och rådgivning beroende på vad som är lämpligt. När de nationella behöriga myndigheterna avser att ge vägledning och rådgivning om ett AI-system på områden som omfattas av annan unionsrätt, ska samråd ske med de nationella behöriga myndigheterna enligt den unionsrätten, när så är lämpligt.

9. Om unionens institutioner, organ och byråer omfattas av denna förordning ska Europeiska datatillsynsmannen fungera som behörig tillsynsmyndighet för dessa.

KAPITEL VIII

EU-DATABAS FÖR AI-SYSTEM MED HÖG RISK

Artikel 71

EU-databas för AI-system med hög risk som förtecknas i Bilaga III

1. Kommissionen ska i samarbete med medlemsstaterna inrätta och upprätthålla en EU-databas som innehåller den information som avses i punkterna 2 och 3 i denna artikel om AI-system med hög risk som avses i artikel 6.2 och som är registrerade i enlighet med artiklarna 49 och 60 och AI-system som inte betraktas som AI-system med hög risk enligt artikel 6.3 och som är registrerade i enlighet med artiklarna 6.4 och 49. När kommissionen fastställer de funktionella specifikationerna för en sådan databas ska den samråda med relevanta experter och när den uppdaterar de funktionella specifikationerna för en sådan databas ska den samråda med styrelsen.

2. De uppgifter som förtecknas i bilaga VIII avsnitten A och B ska föras in i EU-databasen av leverantören eller, i tillämpliga fall, av ombudet.

3. De uppgifter som förtecknas i avsnitt C i bilaga VIII ska föras in i EU-databasen av den tillhandahållare som är, eller agerar på uppdrag av, en offentlig myndighet eller byrå eller ett offentligt organ, i enlighet med artikel 49.3 och 49.4.

4. Med undantag för det avsnitt som avses i artiklarna 49.4 och 60.4 c ska informationen i den EU-databas som registrerats i enlighet med artikel 49 vara åtkomlig och allmänt tillgänglig på ett användarvänligt sätt. Det ska vara lätt att navigera i informationen, som ska vara maskinläsbar. Den information som registreras i enlighet med artikel 60 ska vara tillgänglig endast för marknadskontrollmyndigheter och kommissionen, såvida inte den potentiella leverantören eller leverantören har gett sitt samtycke till att denna information också görs tillgänglig för allmänheten.

5. EU-databasen ska innehålla personuppgifter endast i den mån det är nödvändigt för insamling och behandling av information i enlighet med denna förordning. Denna information ska omfatta namnen på och kontaktuppgifter för fysiska personer som ansvarar för att registrera systemet och som har rättslig behörighet att företräda leverantören eller tillhandahållaren, beroende på vad som är tillämpligt.

6. Kommissionen ska vara personuppgiftsansvarig för EU-databasen. Den ska göra tillräckligt tekniskt och administrativt stöd tillgängligt för leverantörer, potentiella leverantörer och tillhandahållare. EU-databasen ska uppfylla de tillämpliga tillgänglighetskraven.

KAPITEL IX

ÖVERVAKNING EFTER UTSLÄPPANDE PÅ MARKNADEN, INFORMATIONSDELNING OCH MARKNADSKONTROLL

AVSNITT 1

Övervakning efter utsläppande på marknaden

Artikel 72

Leverantörers övervakning efter utsläppande på marknaden och planen för övervakning efter utsläppande på marknaden när det gäller AI-system med hög risk

1. Leverantörer ska inrätta och dokumentera ett system för övervakning efter utsläppande på marknaden på ett sätt som står i proportion till AI-teknikens beskaffenhet och riskerna med AI-systemet med hög risk.

2. Systemet för övervakning efter utsläppande på marknaden ska aktivt och systematiskt samla in, dokumentera och analysera relevanta uppgifter som kan tillhandahållas av tillhandahållare eller som kan samlas in via andra källor om prestandan för AI-systemen med hög risk under hela deras livstid, och som gör det möjligt för leverantören att utvärdera AI-systemens fortlöpande överensstämmelse med kraven i kapitel III avsnitt 2. I förekommande fall ska övervakningen efter utsläppande på marknaden omfatta en analys av interaktionen med andra AI-system. Denna skyldighet omfattar inte känsliga operativa uppgifter om tillhandahållare som är brottsbekämpande myndigheter.

3. Systemet för övervakning efter utsläppande på marknaden ska baseras på en plan för övervakning efter utsläppande på marknaden. Planen för övervakning efter utsläppande på marknaden ska vara en del av den tekniska dokumentation som avses i bilaga IV. Kommissionen ska anta en genomförandeakt med detaljerade bestämmelser som fastställer en mall för planen för övervakning efter utsläppande på marknaden och en förteckning över de element som ska ingå i planen senast den 2 februari 2026. Den genomförandeakten ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

4. För AI-system med hög risk som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I ska leverantörer, om ett system och en plan för övervakning efter utsläppande på marknaden redan har inrättats enligt den lagstiftningen, för att säkerställa samstämmighet, undvika dubbelarbete och minimera ytterligare bördor, ha möjlighet att, beroende på vad som är lämpligt, integrera de nödvändiga delar som beskrivs i punkterna 1, 2 och 3 med hjälp av den mall som avses i punkt 3 i system och planer som redan finns enligt den lagstiftningen, förutsatt att den uppnår en likvärdig skyddsnivå.

Första stycket i denna punkt ska också tillämpas på AI-system med hög risk som avses i punkt 5 i bilaga III och som släpps ut på marknaden eller tas i bruk av finansiella institut som omfattas av krav avseende sina interna styrelseformer, arrangemang eller processer enligt unionsrätten om finansiella tjänster.

AVSNITT 2

Informationsdelning om allvarliga incidenter

Artikel 73

Rapportering av allvarliga incidenter

1. Leverantörer av AI-system med hög risk som släpps ut på unionsmarknaden ska rapportera alla allvarliga incidenter till marknadskontrollmyndigheterna i de medlemsstater där incidenten inträffade.

2. Den rapport som avses i punkt 1 ska göras omedelbart efter det att leverantören har fastställt ett orsakssamband mellan AI-systemet och den allvarliga incidenten eller den rimliga sannolikheten för att det finns ett sådant samband och, under alla omständigheter, senast 15 dagar efter det att leverantören eller, i tillämpliga fall, tillhandahållaren fått kännedom om den allvarliga incidenten.

Den rapporteringsperiod som avses i första stycket ska ta hänsyn till hur allvarligt den allvarliga incidenten är.

3. Trots vad som sägs i punkt 2 i denna artikel ska, i händelse av en utbredd överträdelse eller en allvarlig incident enligt definitionen i artikel 3.49 b, den rapport som avses i punkt 1 i den här artikeln tillhandahållas omedelbart och senast två dagar efter det att leverantören eller, i tillämpliga fall, tillhandahållaren fått kännedom om incidenten.

4. Trots vad som sägs i punkt 2 ska rapporten, om en person avlider, tillhandahållas omedelbart efter det att leverantören eller tillhandahållaren har fastställt, eller så snart den misstänker, ett orsakssamband mellan AI-systemet med hög risk och den allvarliga incidenten, dock senast tio dagar efter den dag då leverantören eller, i tillämpliga fall, tillhandahållaren fått kännedom om den allvarliga incidenten.

5. Om det är nödvändigt för att säkerställa snabb rapportering får leverantören eller, i tillämpliga fall, tillhandahållaren, lämna in en inledande rapport som är ofullständig, följd av en fullständig rapport.

6. Efter rapporteringen av en allvarlig incident enligt punkt 1 ska leverantören utan dröjsmål utföra de nödvändiga utredningarna med avseende på den allvarliga incidenten och det berörda AI-systemet. Detta ska inbegripa en riskbedömning av incidenten och korrigerande åtgärder.

Leverantören ska samarbeta med de behöriga myndigheterna, och i förekommande fall med det berörda anmälda organet, under de utredningar som avses i första stycket, och får inte utföra någon utredning som inbegriper att ändra det berörda AI-systemet på ett sätt som kan påverka eventuella efterföljande utvärderingar av orsakerna till incidenten, innan den underrättar de behöriga myndigheterna om en sådan åtgärd.

7. Efter att ha mottagit en underrättelse om en allvarlig incident enligt artikel 3.49 c ska den berörda marknadskontrollmyndigheten informera de nationella offentliga myndigheter eller organ som avses i artikel 77.1. Kommissionen ska utarbeta särskilda vägledning för att underlätta fullgörandet av de skyldigheter som anges i punkt 1 i den här artikeln. Dessa riktlinjer ska utfärdas senast den 2 augusti 2025 och ska bedömas regelbundet.

8. Marknadskontrollmyndigheten ska vidta lämpliga åtgärder i enlighet med vad som föreskrivs i artikel 19 i förordning (EU) 2019/1020 inom sju dagar från den dag som den mottog den underrättelse som avses i punkt 1 i den här artikeln och ska följa de underrättelseförfaranden som föreskrivs i den förordningen.

9. För AI-system med hög risk som avses i bilaga III och som släpps ut på marknaden eller tas i bruk av leverantörer som omfattas av unionslagstiftningsinstrument som föreskriver rapporteringsskyldigheter som är likvärdiga med dem som anges i denna förordning ska anmälan av allvarliga incidenter vara begränsade till dem som avses i artikel 3.49 c.

10. För AI-system med hög risk som utgör säkerhetskomponenter i enheter, eller som själva är enheter, vilka omfattas av förordningarna (EU) 2017/745 och (EU) 2017/746, ska anmälan av allvarliga incidenter begränsas till sådana som avses i artikel 3.49 c i den här förordningen och göras till den nationella behöriga myndighet som utsetts för detta ändamål av de medlemsstater där incidenten inträffade.

11. Nationella behöriga myndigheter ska omedelbart underrätta kommissionen om alla allvarliga incidenter, oavsett om de har vidtagit åtgärder med anledning av dessa, i enlighet med artikel 20 i förordning (EU) 2019/1020.

AVSNITT 3

Kontroll av efterlevnad

Artikel 74

Marknadskontroll och kontroll av AI-system på unionsmarkanden

1. Förordning (EU) 2019/1020 ska tillämpas på AI-system som omfattas av den här förordningen. För att effektivt kunna kontrollera efterlevnaden av den här förordningen gäller följande:

a) Alla hänvisningar till en ekonomisk aktör enligt förordning (EU) 2019/1020 ska förstås som hänvisningar som omfattar alla operatörer som identifieras artikel 2.1 i den här förordningen.

b) Alla hänvisningar till en produkt enligt förordning (EU) 2019/1020 ska förstås som hänvisningar som omfattar alla AI-system som omfattas av den här förordningen.

2. Som en del av sina rapporteringsskyldigheter enligt artikel 34.4 i förordning (EU) 2019/1020 ska marknadskontrollmyndigheterna årligen rapportera till kommissionen och berörda nationella konkurrensmyndigheter all information som framkommit i samband med marknadskontrollen och som kan vara av potentiellt intresse för tillämpningen av unionens konkurrenslagstiftning. De ska också årligen rapportera till kommissionen om användning inom förbjudna användningsområden som ägt rum det året och om de åtgärder som vidtagits.

3. För AI-system med hög risk som är relaterade till produkter som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I ska marknadskontrollmyndigheten vid tillämpning av denna förordning vara den myndighet ansvarig för marknadskontroll som utsetts enligt de rättsakterna.

Genom undantag från första stycket och under lämpliga omständigheter får medlemsstaterna utse en annan berörd myndighet att fungera som marknadskontrollmyndighet under förutsättning att de säkerställer samordning med de berörda sektorsspecifika marknadskontrollmyndigheter som är ansvariga för kontroll av efterlevnaden av unionens harmoniseringslagstiftning som förtecknas i bilaga I.

4. De förfaranden som avses i artiklarna 79–83 i denna förordning är inte tillämplig på AI-system som är relaterade till produkter som omfattas av unionens harmoniseringslagstiftning som förtecknas i avsnitt A i bilaga I om sådana rättsakter redan föreskriver förfaranden som säkerställer en likvärdig skyddsnivå och har samma syfte. I sådana fall ska dessa relevanta sektorsspecifika förfaranden tillämpas i stället.

5. Utan att det påverkar marknadskontrollmyndigheternas befogenheter enligt artikel 14 i förordning (EU) 2019/1020 får marknadskontrollmyndigheterna i syfte att säkerställa en effektiv kontroll av efterlevnaden av den här förordningen på distans och när så är lämpligt utöva de befogenheter som avses i artikel 14.4 d och j i den förordningen.

6. För AI-system med hög risk som släpps ut på marknaden, tas i bruk eller används av finansinstitut som regleras av unionsrätten om finansiella tjänster ska marknadskontrollmyndigheten vid tillämpning av denna förordning vara den berörda nationella myndighet som enligt den lagstiftningen ansvarar för den finansiella tillsynen över dessa institut, i den mån utsläppandet på marknaden, ibruktagandet eller användningen av AI-systemet står i direkt samband med tillhandahållandet av dessa finansiella tjänster.

7. Genom undantag från punkt 6 får en annan berörd myndighet, under lämpliga omständigheter och under förutsättning att samordning säkerställs, av medlemsstaten identifieras som marknadskontrollmyndighet vid tillämpning av denna förordning.

Nationella marknadskontrollmyndigheter som utövar tillsyn över reglerade kreditinstitut reglerade enligt direktiv 2013/36/EU och som deltar i den gemensamma tillsynsmekanism som inrättats genom förordning (EU) nr 1024/2013, ska utan dröjsmål till Europeiska centralbanken rapportera all information som identifierats i samband med deras marknadskontroll och som kan vara av potentiellt intresse för Europeiska centralbankens tillsynsuppgifter enligt den förordningen.

8. För AI-system med hög risk som förtecknas i punkt 1 i bilaga III till denna förordning ska medlemsstaterna, i den mån systemen används för brottsbekämpande ändamål, gränsförvaltning och rättvisa och demokrati, och för AI-system med hög risk som förtecknas i punkterna 6, 7 och 8 i bilaga III till denna förordning, till marknadskontrollmyndigheter för tillämpning av denna förordning utse antingen de behöriga tillsynsmyndigheterna för dataskydd enligt förordning (EU) 2016/679 eller direktiv (EU) 2016/680, eller någon annan myndighet som utsetts enligt de villkor som fastställs i artiklarna 41–44 i direktiv (EU) 2016/680. Marknadskontrollen påverkar inte på något sätt rättsliga myndigheters oberoende eller på annat sätt inkräkta på deras verksamhet när de agerar inom ramen för sin dömande verksamhet.

9. När unionens institutioner, byråer eller organ omfattas av denna förordning ska Europeiska datatillsynsmannen fungera som marknadskontrollmyndighet för dessa, med undantag av när Europeiska unionens domstol agerar i dess rättskipande funktion.

10. Medlemsstaterna ska underlätta samordningen mellan marknadskontrollmyndigheter som utses enligt denna förordning och andra relevanta nationella myndigheter eller organ som utövar tillsyn över tillämpningen av unionens harmoniseringslagstiftning som förtecknas i bilaga I eller annan unionsrätt som kan vara relevant för de AI-system med hög risk som avses i bilaga III.

11. Marknadskontrollmyndigheter och kommissionen ska kunna föreslå gemensamma aktiviteter, inbegripet gemensamma undersökningar, som ska genomföras antingen av marknadskontrollmyndigheterna själva eller av marknadskontrollmyndigheter tillsammans med kommissionen, och som syftar till att främja överensstämmelse, identifiera bristande överensstämmelse, öka medvetenheten och ge vägledning om denna förordning med avseende på specifika kategorier av AI-system med hög risk som befinns utgöra en allvarlig risk i två eller flera medlemsstater i enlighet med artikel 9 i förordning (EU) 2019/1020. AI-byrån ska tillhandahålla samordningsstöd för gemensamma utredningar.

12. Utan att det påverkar de befogenheter som föreskrivs enligt förordning (EU) 2019/1020, och när så är relevant och begränsat till vad som är nödvändigt för att marknadskontrollmyndigheterna ska kunna fullgöra sina uppgifter, ska leverantörer bevilja dessa fullständig åtkomst till den dokumentation och de tränings-, validerings- och testdataset som används för utvecklingen av AI-system med hög risk, inbegripet, när så är lämpligt och med förbehåll för säkerhetsgarantier, genom applikationsprogrammeringsgränssnitt (API) eller andra relevanta tekniska medel och verktyg som möjliggör fjärråtkomst.

13. Marknadskontrollmyndigheterna ska beviljas tillgång till källkoden för AI-systemet med hög risk på motiverad begäran och endast om båda följande villkor är uppfyllda:

a) Tillgång till källkod är nödvändig för att bedöma om ett AI-system med hög risk uppfyller kraven i kapitel III avsnitt 2.

b) Testnings- eller revisionsförfaranden och kontroller som grundas på uppgifter och dokumentation från leverantören har uttömts eller visat sig vara otillräckliga.

14. All information eller dokumentation som har erhållits av marknadskontrollmyndigheter ska behandlas i enlighet med de konfidentialitetskrav som anges i artikel 78.

Artikel 75

Ömsesidigt bistånd, marknadskontroll och kontroll av AI-system för allmänna ändamål

1. Om ett AI-system bygger på en AI-modell för allmänna ändamål och modellen och systemet har utvecklats av samma leverantör ska AI-byrån ha befogenhet att övervaka och utöva tillsyn över AI-systemets efterlevnad av skyldigheter enligt denna förordning. För att utföra sina övervaknings- och tillsynsuppgifter ska AI-byrån ha alla befogenheter som en marknadskontrollmyndighet har enligt detta avsnitt och förordning (EU) 2019/1020.

2. Om de relevanta marknadskontrollmyndigheterna har tillräckliga skäl att anse att AI-system för allmänna ändamål som kan användas direkt av tillhandahållare för minst ett ändamål som klassificeras som AI-system med hög risk enligt denna förordning inte uppfyller de krav som fastställs i denna förordning, ska de samarbeta med AI-byrån för att utföra bedömningar av överensstämmelse och informera styrelsen och andra marknadskontrollmyndigheter om detta.

3. Om en marknadskontrollmyndighet inte kan slutföra sina utredningar av AI-system med hög risk på grund av att den inte fått tillgång till viss information avseende AI-modellen för allmänna ändamål, trots att den har vidtagit alla lämpliga åtgärder för att inhämta den informationen, får den lämna en motiverad begäran till AI-byrån, genom vilken tillgång till denna information ska verkställas. I detta fall ska AI-byrån utan dröjsmål, och under alla omständigheter inom 30 dagar, förse den begärande myndigheten med all information som AI-byrån anser vara relevant för att fastställa om ett AI-system med hög risk inte uppfyller kraven. Marknadskontrollmyndigheter ska säkerställa att den information som de erhåller i enlighet med artikel 78 i denna förordning behandlas konfidentiellt. Det förfarande som föreskrivs i kapitel VI i förordning (EU) 2019/1020 ska gälla i tillämpliga delar.

Artikel 76

Marknadskontrollmyndigheters tillsyn av testning under verkliga förhållanden

1. Marknadskontrollmyndigheterna ska ha behörigheter och befogenheter att säkerställa att testning under verkliga förhållanden sker i enlighet med denna förordning.

2. Om testning under verkliga förhållanden utförs för AI-system som står under tillsyn inom ramen för en regulatorisk sandlåda för AI enligt artikel 58, ska marknadskontrollmyndigheterna kontrollera efterlevnaden av artikel 60 som en del av sin tillsynsroll för den regulatoriska sandlådan för AI. Dessa myndigheter får, beroende på vad som är lämpligt, tillåta att testning under verkliga förhållanden utförs av leverantören eller den potentiella leverantören med avvikelse från de villkor som anges i artikel 60.4 f och g.

3. Om en marknadskontrollmyndighet har informerats av den potentiella leverantören, leverantören eller någon tredje part om en allvarlig incident eller har andra skäl att anse att villkoren i artiklarna 60 och 61 inte är uppfyllda, får den, beroende på vad som är lämpligt, fatta något av följande beslut på sitt territorium:

a) Tillfälligt avbryta eller avsluta testningen under verkliga förhållanden.

b) Kräva att leverantören eller den potentiella leverantören och tillhandahållaren eller den potentiella tillhandahållaren ändrar någon aspekt av testningen under verkliga förhållanden.

4. Om en marknadskontrollmyndighet har fattat ett beslut som avses i punkt 3 i denna artikel eller har gjort en invändning i den mening som avses i artikel 60.4 b, ska skälen till beslutet eller invändningen anges i beslutet eller invändningen liksom information om hur leverantören eller den potentiella leverantören kan bestrida beslutet eller invändningen.

5. I tillämpliga fall ska en marknadskontrollmyndighet, om den har fattat ett beslut som avses i punkt 3, meddela skälen till detta till marknadskontrollmyndigheterna i andra medlemsstater där AI-systemet har testats i enlighet med planen för testning.

Artikel 77

Myndigheters befogenheter att skydda grundläggande rättigheter

1. Nationella offentliga myndigheter eller organ som utövar tillsyn över eller kontrollerar efterlevnaden av skyldigheter enligt unionsrätt om skydd av grundläggande rättigheter, inbegripet rätten till icke-diskriminering, i samband med användningen av AI-system med hög risk som avses i bilaga III, ska ha befogenhet att begära och få åtkomst till all dokumentation som skapas eller upprätthålls enligt denna förordning på ett språk och i ett format som är lättillgängligt när åtkomst till sådan dokumentation är nödvändig för att effektivt fullgöra sina mandat inom ramen för deras jurisdiktion. Den berörda offentliga myndigheten eller det berörda offentliga organet ska informera marknadskontrollmyndigheten i den berörda medlemsstaten om en sådan begäran.

2. Senast den 2 november 2024 ska varje medlemsstat identifiera de offentliga myndigheter eller organ som avses i punkt 1 och offentliggöra en förteckning över dem. Medlemsstaterna ska anmäla förteckningen till kommissionen och de andra medlemsstaterna och hålla förteckningen uppdaterad.

3. Om den dokumentation som avses i punkt 1 är otillräcklig för att fastställa huruvida ett åsidosättande av skyldigheter enligt unionsrätt om skydd av grundläggande rättigheter har ägt rum, får den offentliga myndighet eller det offentliga organ som avses i punkt 1 lämna en motiverad begäran till marknadskontrollmyndigheten om organisering av testning av AI-systemet med hög risk genom tekniska medel. Marknadskontrollmyndigheten ska organisera testningen i nära samarbete med den begärande offentliga myndigheten eller det begärande offentliga organet inom rimlig tid efter begäran.

4. All information eller dokumentation som de nationella offentliga myndigheter eller organ som avses i punkt 1 i denna artikel erhåller enligt denna artikel ska behandlas i enlighet med de konfidentialitetskrav som fastställs i artikel 78.

Artikel 78

Konfidentiell behandling

1. Kommissionen, marknadskontrollmyndigheterna och anmälda organ och alla andra fysiska eller juridiska personer som deltar i tillämpningen av denna förordning ska, i enlighet med unionsrätten eller nationell rätt, respektera konfidentialiteten för den information och de data som de erhåller när de utför sina uppgifter och sin verksamhet på ett sådant sätt att de särskilt skyddar följande:

a) Immateriella rättigheter och en fysisk eller juridisk persons konfidentiella affärsinformation eller företagshemligheter, inklusive källkod, utom i de fall som avses i artikel 5 i Europaparlamentets och rådets direktiv (EU) 2016/943 ([57]).

b) Ett effektivt genomförande av denna förordning, särskilt med avseende på inspektioner, utredningar eller revisioner.

c) Offentliga och nationella säkerhetsintressen.

d) Genomförandet av straffrättsliga eller administrativa förfaranden.

e) Uppgifter som säkerhetsskyddsklassificerats enligt unionsrätten eller nationell rätt.

2. De myndigheter som deltar i tillämpningen av denna förordning enligt punkt 1 ska endast begära sådana data som är strikt nödvändiga för bedömningen av den risk som AI-system utgör och för utövandet av deras befogenheter i enlighet med denna förordning och med förordning (EU) 2019/1020. De ska vidta tillräckliga och effektiva cybersäkerhetsåtgärder för att skydda säkerheten och konfidentialiteten för den information och de data som inhämtats, och ska radera inhämtade data så snart dessa inte längre behövs för det ändamål för vilket de inhämtats, i enlighet med tillämplig unionsrätt eller nationell rätt.

3. Utan att det påverkar tillämpningen av punkterna 1 och 2 får information som på konfidentiell basis utbyts mellan de nationella behöriga myndigheterna eller mellan nationella behöriga myndigheter och kommissionen inte lämnas ut utan föregående samråd med den nationella behöriga myndighet som lämnat informationen och med tillhandahållaren när sådana AI-system med hög risk som avses i punkt 1, 6 eller 7 i bilaga III används av brottsbekämpande myndigheter, gränskontrollmyndigheter, migrationsmyndigheter eller asylmyndigheter, om ett sådant röjande skulle äventyra allmänna och nationella säkerhetsintressen. Detta informationsutbyte får inte omfatta känsliga operativa uppgifter som rör brottsbekämpande myndigheters, gränskontrollmyndigheters, migrationsmyndigheters eller asylmyndigheters verksamhet.

Om brottsbekämpande myndigheter, migrationsmyndigheter eller asylmyndigheter är leverantörer av sådana AI-system med hög risk som avses i punkt 1, 6 eller 7 i bilaga III ska den tekniska dokumentation som avses i bilaga IV finnas kvar i dessa myndigheters lokaler. Dessa myndigheter ska säkerställa att de marknadskontrollmyndigheter som avses i artikel 74.8 och 74.9, beroende på vad som är tillämpligt, på begäran omedelbart kan få åtkomst till eller få en kopia av dokumentationen. Endast personal vid marknadskontrollmyndigheten som innehar säkerhetsgodkännande på tillräckligt hög nivå ska ha åtkomst till denna dokumentation eller kopior av denna.

4. Punkterna 1, 2 och 3 påverkar inte kommissionens, medlemsstaternas och deras relevanta myndigheters samt anmälda organs rättigheter eller skyldigheter när det gäller att utbyta information och utfärda varningar, inbegripet i samband med gränsöverskridande samarbete, och inte heller påverkas de berörda parternas straffrättsliga skyldighet att lämna information enligt medlemsstaternas straffrätt.

5. Kommissionen och medlemsstaterna får, om det är nödvändigt och förenligt med relevanta bestämmelser i internationella avtal och handelsavtal, utbyta konfidentiell information med de tillsynsmyndigheter i tredjeländer med vilka de har slutit bilaterala eller multilaterala avtal om konfidentialitet som garanterar en tillräcklig nivå av konfidentialitet.

Artikel 79

Förfaranden för att hantera AI-system som utgör en risk på nationell nivå

1. AI-system som utgör en risk ska förstås som en *produkt som utgör en risk* enligt definitionen i artikel 3.19 i förordning (EU) 2019/1020 i den mån de utgör risker för personers hälsa eller säkerhet eller grundläggande rättigheter.

2. Om en medlemsstats marknadskontrollmyndighet har tillräckliga skäl att anse att ett AI-system utgör en sådan risk som avses i punkt 1 i denna artikel, ska den utvärdera om det berörda AI-systemet är förenligt med alla krav och skyldigheter som fastställs i denna förordning. Särskild uppmärksamhet ska ägnas åt AI-system som utgör en risk för sårbara grupper. Om risker för grundläggande rättigheter identifieras ska marknadskontrollsmyndigheten även omedelbart informera och till fullo samarbeta med de berörda nationella offentliga myndigheter eller organ som avses i artikel 77.1. De berörda operatörerna ska vid behov samarbeta med marknadskontrollmyndigheten och andra nationella offentliga myndigheter eller organ som avses i artikel 77.1.

([57]) Europaparlamentets och rådets direktiv (EU) 2016/943 av den 8 juni 2016 om skydd mot att icke röjd know-how och företagsinformation (företagshemligheter) olagligen anskaffas, utnyttjas och röjs (EUT L 157, 15.6.2016, s. 1).

Om marknadskontrollsmyndigheten eller, när så är lämpligt, marknadskontrollsmyndigheten i samarbete med den nationella offentliga myndighet som avses i artikel 77.1, vid utvärderingen konstaterar att AI-systemet inte uppfyller kraven och skyldigheterna i denna förordning ska den utan oskäligt dröjsmål kräva att berörda operatörer vidtar alla lämpliga korrigerande åtgärder för att AI-systemet ska uppfylla dessa krav, dra tillbaka AI-systemet från marknaden eller återkalla det inom en period som marknadskontrollsmyndigheten får fastställa, och under alla omständigheter senast inom 15 arbetsdagar eller såsom fastställts i relevant unionsharmoniseringslagstiftning.

Marknadskontrollmyndigheten ska informera det berörda anmälda organet om detta. Artikel 18 i förordning (EU) 2019/1020 ska tillämpas på de åtgärder som avses i andra stycket i denna punkt.

3. Om marknadskontrollmyndigheten anser att den bristande överensstämmelsen inte bara gäller det nationella territoriet, ska den utan oskäligt dröjsmål informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt operatören att vidta.

4. Operatören ska säkerställa att alla lämpliga korrigerande åtgärder vidtas i fråga om alla berörda AI-system som den har tillhandahållit på unionsmarknaden.

5. Om operatören av ett AI-system inte vidtar lämpliga korrigerande åtgärder inom den tid som avses i punkt 2, ska marknadskontrollmyndigheten vidta alla lämpliga provisoriska åtgärder för att förbjuda eller begränsa tillhandahållandet eller ibruktagandet av AI-systemet på sin nationella marknad, dra tillbaka produkten eller det fristående AI-systemet från den marknaden eller återkalla det. Myndigheten ska utan oskäligt dröjsmål anmäla dessa åtgärder till kommissionen och de andra medlemsstaterna.

6. I den anmälan som avses i punkt 5 ska alla tillgängliga data ingå, särskilt den information som krävs för att kunna identifiera det AI-system som inte uppfyller kraven, dess ursprung och leveranskedjan, vilken typ av bristande överensstämmelse som görs gällande och den risk systemet utgör, vilken typ av nationell åtgärd som vidtagits och dess varaktighet samt den berörda operatörens synpunkter. Marknadskontrollmyndigheterna ska särskilt ange om den bristande överensstämmelsen beror på en eller flera av följande orsaker:

a) Bristande efterlevnad av förbudet mot de AI-användningsområden som avses i artikel 5.

b) AI-systemet med hög risk uppfyller inte kraven i kapitel III avsnitt 2.

c) Brister i de harmoniserade standarder eller gemensamma specifikationer som avses i artiklarna 40 och 41 och som ger presumtion om överensstämmelse.

d) Bristande efterlevnad av artikel 50.

7. Andra marknadskontrollmyndigheter än marknadskontrollmyndigheten i den medlemsstat som inledde förfarandet ska utan oskäligt dröjsmål informera kommissionen och de andra medlemsstaterna om alla vidtagna åtgärder och eventuella kompletterande uppgifter som de har tillgång till med avseende på AI-systemets bristande överensstämmelse och, vid oenighet om den anmälda nationella åtgärden, om sina invändningar.

8. Åtgärden ska anses vara berättigad om ingen marknadskontrollmyndighet i en medlemsstat eller kommissionen har gjort invändningar inom tre månader efter mottagandet av den anmälan som avses i punkt 5 mot en provisorisk åtgärd som vidtagits av en marknadskontrollmyndighet i en annan medlemsstat. Detta påverkar inte den berörda operatörens processuella rättigheter i enlighet med artikel 18 i förordning (EU) 2019/1020. Den tremånadersperiod som avses i detta stycke ska minskas till 30 dagar vid bristande efterlevnad av förbudet mot de AI-användningsområden som avses i artikel 5 i den här förordningen.

9. Marknadskontrollmyndigheterna ska säkerställa att lämpliga begränsande åtgärder, till exempel att produkten eller AI-systemet dras tillbaka från marknaden, vidtas i fråga om den berörda produkten eller det berörda AI-systemet utan oskäligt dröjsmål.

Artikel 80

Förfarande för hantering av AI-system som av leverantören klassificeras som AI-system utan hög risk vid tillämpning av BILAGA III

1. Om en marknadskontrollmyndighet har tillräckliga skäl att anse att ett AI-system som av leverantören klassificeras som AI-system utan hög risk enligt artikel 6.3 faktiskt är ett AI-system med hög risk, ska marknadskontrollmyndigheten genomföra en utvärdering av det berörda AI-systemet med avseende på dess klassificering som AI-system med hög risk på grundval av de villkor som anges i artikel 6.3 och kommissionens riktlinjer.

2. Om marknadskontrollmyndigheten vid utvärderingen konstaterar att det berörda AI-systemet är ett system med hög risk ska den utan oskäligt dröjsmål ålägga den berörda leverantören att vidta alla nödvändiga åtgärder för att AI-systemet ska uppfylla de krav och skyldigheter som fastställs i denna förordning samt vidta lämpliga korrigerande åtgärder inom en period som marknadskontrollmyndigheten får föreskriva.

3. Om marknadskontrollmyndigheten anser att användningen av det berörda AI-systemet inte är begränsad till det nationella territoriet, ska den utan oskäligt dröjsmål informera kommissionen och de andra medlemsstaterna om utvärderingsresultaten och om de åtgärder som den har ålagt operatören att vidta.

4. Leverantören ska säkerställa att alla nödvändiga åtgärder vidtas för att AI-systemet ska uppfylla de krav och skyldigheter som fastställs i denna förordning. Om leverantören av ett berört AI-system inte bringar AI-systemet i överensstämmelse med dessa krav och skyldigheter inom den period som avses i punkt 2 i denna artikel ska leverantören bli föremål för sanktionsavgifter i enlighet med artikel 99.

5. Leverantören ska säkerställa att alla lämpliga korrigerande åtgärder vidtas i fråga om alla berörda AI-system som den har tillhandahållit på unionsmarknaden.

6. Om leverantören av det berörda AI-systemet inte vidtar lämpliga korrigerande åtgärder inom den period som avses i punkt 2 i denna artikel ska artikel 79.5–79.9 tillämpas.

7. Om marknadskontrollmyndigheten vid utvärderingen enligt punkt 1 i denna artikel fastställer att AI-systemet av leverantören felaktigt klassificerats som ett system utan hög risk i syfte att kringgå tillämpningen av kraven i kapitel III avsnitt 2, ska leverantören bli föremål för sanktionsavgifter i enlighet med artikel 99.

8. När marknadskontrollmyndigheterna utövar sina befogenheter att övervaka tillämpningen av denna artikel, och i enlighet med artikel 11 i förordning (EU) 2019/1020, får de utföra lämpliga kontroller, med särskilt beaktande av information som lagras i den EU-databas som avses i artikel 71 i den här förordningen.

Artikel 81

Unionsförfarande för skyddsåtgärder

1. Om marknadskontrollmyndigheten i en medlemsstat inom tre månader efter mottagandet av den anmälan som avses i artikel 79.5, eller inom 30 dagar vid bristande efterlevnad av förbudet mot de AI-användningsområden som avses i artikel 5, har gjort invändningar mot en åtgärd som vidtagits av marknadskontrollmyndigheten i en annan medlemsstat, eller om kommissionen anser att åtgärden strider mot unionsrätten, ska kommissionen utan oskäligt dröjsmål inleda samråd med den berörda medlemsstatens marknadskontrollmyndighet och operatören eller operatörerna och ska utvärdera den nationella åtgärden. På grundval av utvärderingsresultaten ska kommissionen besluta om den nationella åtgärden är berättigad eller inte inom sex månader, eller inom 60 dagar vid bristande efterlevnad av förbudet mot de AI-användningsområden som avses i artikel 5, från och med den anmälan som avses i artikel 79.5 och meddela beslutet till marknadskontrollmyndigheten i den berörda medlemsstaten. Kommissionen ska också underrätta alla de övriga marknadskontrollmyndigheterna om ett sådant beslut.

2. Om kommissionen anser att den åtgärd som vidtagits av den berörda medlemsstaten är motiverad ska samtliga medlemsstater säkerställa att de vidtar lämpliga restriktiva åtgärder med avseende på det berörda AI-systemet, såsom att kräva att AI-systemet dras tillbaka från deras marknad utan oskäligt dröjsmål, och underrätta kommissionen om detta. Om kommissionen anser att den nationella åtgärden är omotiverad ska den berörda medlemsstaten dra tillbaka åtgärden och underrätta kommissionen om detta.

3. Om den nationella åtgärden anses vara berättigad och AI-systemets bristande överensstämmelse kan tillskrivas brister i de harmoniserade standarder eller gemensamma specifikationer som avses i artiklarna 40 och 41 i denna förordning, ska kommissionen tillämpa det förfarande som föreskrivs i artikel 11 i förordning (EU) nr 1025/2012.

Artikel 82

AI-system som uppfyller kraven och som utgör en risk

1. Om en marknadskontrollmyndighet i en medlemsstat har gjort en utvärdering enligt artikel 79 och, efter samråd med den nationella offentliga myndighet som avses i artikel 77.1, konstaterar att ett AI-system med hög risk uppfyller kraven i denna förordning men ändå utgör en risk för personers hälsa och säkerhet, för grundläggande rättigheter eller för andra aspekter av skyddet av allmänintresset, ska den ålägga den berörda operatören att, utan oskäligt dröjsmål och inom en period som den får fastställa, vidta alla lämpliga åtgärder för att säkerställa att det berörda AI-systemet när det släpps ut på marknaden eller tas i bruk inte längre utgör en sådan risk.

2. Leverantören eller en annan berörd operatör ska säkerställa att korrigerande åtgärder vidtas i fråga om alla berörda AI-system som den har tillhandahållit på marknaden i unionen inom den tidsplan som föreskrivs av marknadskontrollmyndigheten i den medlemsstat som avses i punkt 1.

3. Medlemsstaterna ska omedelbart informera kommissionen och de andra medlemsstaterna om ett konstaterande enligt punkt 1. Den informationen ska innehålla alla tillgängliga närmare uppgifter, särskilt de data som krävs för att kunna identifiera det berörda AI-systemet, dess ursprung och leveranskedja, den risk som AI-systemet utgör samt vilken typ av nationella åtgärder som vidtagits och deras varaktighet.

4. Kommissionen ska utan oskäligt dröjsmål inleda samråd med de berörda medlemsstaterna och de berörda operatörerna samt utvärdera de nationella åtgärderna. På grundval av utvärderingsresultaten ska kommissionen besluta om åtgärden är berättigad, och vid behov föreslå andra lämpliga åtgärder.

5. Kommissionen ska omedelbart meddela sitt beslut till de berörda medlemsstaterna och till de berörda operatörerna. Den ska också informera övriga medlemsstater.

Artikel 83

Formell bristande överensstämmelse

1. Om marknadskontrollmyndigheten i en medlemsstat konstaterar något av följande ska den ålägga den berörda leverantören att åtgärda den bristande överensstämmelsen inom en tid som den får föreskriva:

a) CE-märkningen har anbringats i strid med artikel 48.

b) CE-märkningen saknas.

c) Den EU-försäkran om överensstämmelse som avses i artikel 47 har inte upprättats.

d) Den EU-försäkran om överensstämmelse som avses i artikel 47 har inte upprättats på ett korrekt sätt.

e) Den registrering i EU-databasen som avses i artikel 71 har inte genomförts.

f) I tillämpliga fall, ett ombud har inte utsetts.

g) Teknisk dokumentation är inte tillgänglig.

2. Om den bristande överensstämmelse som avses i punkt 1 kvarstår ska marknadskontrollmyndigheten i den berörda medlemsstaten vidta lämpliga och proportionella åtgärder för att begränsa eller förbjuda tillhandahållandet av AI-systemet med hög risk på marknaden eller säkerställa att det utan dröjsmål återkallas eller dras tillbaka från marknaden.

Artikel 84

Unionsstödstrukturer för testning av AI

1. Kommissionen ska utse en eller flera unionsstödstrukturer för testning av AI enligt artikel 21.6 i förordning (EU) 2019/1020 på AI-området.

2. Utan att det påverkar de uppgifter som avses i punkt 1 ska unionsstödstrukturerna för testning av AI även tillhandahålla oberoende teknisk eller vetenskaplig rådgivning på begäran av styrelsen, kommissionen eller marknadskontrollmyndigheterna.

AVSNITT 4

Rättsmedel

Artikel 85

Rätt att lämna in klagomål till en marknadskontrollmyndighet

Utan att det påverkar andra administrativa eller rättsliga rättsmedel får varje fysisk eller juridisk person som har skäl att anse att bestämmelserna i denna förordning har överträtts lämna klagomål till den berörda marknadskontrollmyndigheten.

I enlighet med förordning (EU) 2019/1020 ska sådana klagomål beaktas vid genomförandet av marknadskontrollen och hanteras i enlighet med de särskilda förfaranden som fastställts för detta av marknadskontrollmyndigheterna.

Artikel 86

Rätt till förklaring av individuellt beslutsfattande

1. Varje berörd person som är föremål för ett beslut som fattas av tillhandahållaren på grundval av utdata från ett AI-system med hög risk som förtecknas i bilaga III, med undantag för system som förtecknas i punkt 2 i den bilagan, och som har rättslig verkan eller på liknande sätt i betydande grad påverkar den personen på ett sätt som de anser ha en negativ inverkan på deras hälsa, säkerhet eller grundläggande rättigheter, ska ha rätt att erhålla tydliga och meningsfulla förklaringar av AI-systemets roll i beslutsförfarandet och de viktigaste delarna av det beslut som fattats.

2. Punkt 1 är inte tillämplig på användning av AI-system för vilka undantag från eller begränsningar av skyldigheten enligt den punkten följer av unionsrätten eller nationell rätt i överensstämmelse med unionsrätten.

3. Denna artikel är endast tillämplig i den utsträckning som den rättighet som avses i punkt 1 inte på annat sätt föreskrivs i unionsrätten.

Artikel 87

Rapportering av överträdelser och skydd av personer som rapporterar överträdelser

Direktiv (EU) 2019/1937 ska tillämpas på rapportering av överträdelser av denna förordning och skydd för personer som rapporterar sådana överträdelser.

AVSNITT 5

Tillsyn, utredning, efterlevnadskontroll och övervakning av leverantörer av AI-modeller för allmänna ändamål

Artikel 88

Kontroll av efterlevnaden av skyldigheterna för leverantörer av AI-modeller för allmänna ändamål

1. Kommissionen ska ha exklusiv befogenhet att utöva tillsyn avseende och kontrollera efterlevnaden av kapitel V, med beaktande av rättssäkerhetsgarantierna enligt artikel 94. Kommissionen ska anförtro genomförandet av dessa uppgifter till AI-byrån, utan att det påverkar kommissionens organisationsbefogenheter och befogenhetsfördelningen mellan medlemsstaterna och unionen på grundval av fördragen.

2. Utan att det påverkar tillämpningen av artikel 75.3 får marknadskontrollmyndigheterna begära att kommissionen utövar de befogenheter som fastställs i detta avsnitt, om detta är nödvändigt och proportionellt för att hjälpa dem att fullgöra sina uppgifter enligt denna förordning.

Artikel 89

Övervakningsåtgärder

1. För att utföra de uppgifter som tilldelas den enligt detta avsnitt får AI-byrån vidta nödvändiga åtgärder för att övervaka att leverantörer av AI-modeller för allmänna ändamål genomför och efterlever denna förordning på ett effektivt sätt, inbegripet deras efterlevnad av godkända uppförandekoder.

2. Leverantörer i efterföljande led ska ha rätt att lämna in ett klagomål om överträdelse av denna förordning. Ett klagomål ska vara vederbörligen motiverat och innehålla åtminstone följande uppgifter:

a) Kontaktpunkten för leverantören av den berörda AI-modellen för allmänna ändamål.

b) En beskrivning av relevanta fakta, de berörda bestämmelserna i denna förordning och skälet till att leverantören i efterföljande led anser att leverantören av den berörda AI-modellen för allmänna ändamål har överträtt denna förordning.

c) All övrig information som den leverantör i efterföljande led som skickade begäran anser vara relevant, inbegripet, i förekommande fall, information som samlats in på eget initiativ.

Artikel 90

Varningar från den vetenskapliga panelen om systemrisker

1. Den vetenskapliga panelen får lämna en kvalificerad varning till AI-byrån om den har anledning att misstänka att

a) en AI-modell för allmänna ändamål utgör en konkret identifierbar risk på unionsnivå, eller

b) en AI-modell för allmänna ändamål uppfyller de villkor som anges i artikel 51.

2. Efter en sådan kvalificerad varning får kommissionen, genom AI-byrån och efter att ha informerat styrelsen, utöva de befogenheter som fastställs i detta avsnitt i syfte att bedöma ärendet. AI-byrån ska informera styrelsen om alla åtgärder enligt artiklarna 91–94.

3. En kvalificerad varning ska vara vederbörligen motiverad och innehålla åtminstone följande uppgifter:

a) Kontaktpunkten för leverantören av den berörda AI-modellen för allmänna ändamål med systemrisk.

b) En beskrivning av relevanta fakta och skälen till den vetenskapliga panelens varning.

c) All övrig information som den vetenskapliga panelen anser vara relevant, inbegripet, i förekommande fall, information som samlats in på eget initiativ.

Artikel 91

Befogenhet att begära dokumentation och information

1. Kommissionen får begära att leverantören av den berörda AI-modellen för allmänna ändamål tillhandahåller den dokumentation som utarbetats av leverantören i enlighet med artiklarna 53 och 55, eller all ytterligare information som är nödvändig för att bedöma leverantörens efterlevnad av denna förordning.

2. Innan begäran om information skickas får AI-byrån inleda en strukturerad dialog med leverantören av AI-modellen för allmänna ändamål.

3. På en vederbörligen motiverad begäran från den vetenskapliga panelen får kommissionen utfärda en begäran om information till en leverantör av en AI-modell för allmänna ändamål, om tillgången till information är nödvändig och proportionell för fullgörandet av den vetenskapliga panelens uppgifter enligt artikel 68.2.

4. Begäran om information ska innehålla uppgifter om den rättsliga grunden för och syftet med begäran, en specifikation av vilken information som begärs, en tidsfrist inom vilken informationen ska tillhandahållas samt de sanktionsavgifter som föreskrivs i artikel 101 för tillhandahållande av oriktig, ofullständig eller vilseledande information.

5. Leverantören av den berörda AI-modellen för allmänna ändamål, eller dennes företrädare, ska tillhandahålla den begärda informationen. När det gäller juridiska personer, företag eller firmor, eller om leverantören inte är en juridisk person, ska de personer som är behöriga att företräda dem enligt lag eller deras stadgar tillhandahålla den begärda informationen på uppdrag av leverantören av den berörda AI-modellen för allmänna ändamål. I behörig ordning befullmäktigade jurister får lämna information på sina huvudmäns vägnar. Huvudmännen förblir dock fullt ut ansvariga om den tillhandahållna informationen är ofullständig, oriktig eller vilseledande.

Artikel 92

Befogenhet att genomföra utvärderingar

1. AI-byrån får, efter samråd med styrelsen, genomföra utvärderingar av den berörda AI-modellen för allmänna ändamål i syfte att

a) bedöma leverantörens efterlevnad av skyldigheterna enligt denna förordning, om den information som samlats in enligt artikel 91 är otillräcklig, eller

b) undersöka systemrisker på unionsnivå för AI-modeller för allmänna ändamål med systemrisk, särskilt efter en kvalificerad varning från den vetenskapliga panelen i enlighet med artikel 90.1 a.

2. Kommissionen får besluta att utse oberoende experter som ska utföra utvärderingar på dess vägnar, inbegripet från den vetenskapliga panel som inrättats enligt artikel 68. Oberoende experter som utses för denna uppgift ska uppfylla de kriterier som anges i artikel 68.2.

3. Vid tillämpningen av punkt 1 får kommissionen begära åtkomst till den berörda AI-modellen för allmänna ändamål genom applikationsprogrammeringsgränssnitt (API) eller ytterligare lämpliga tekniska medel och verktyg, inbegripet källkod.

4. I begäran om åtkomst ska anges den rättsliga grunden, syftet med och skälen till begäran, den tidsfrist inom vilken åtkomsten ska tillhandahållas samt de sanktionsavgifter som föreskrivs i artikel 101 för underlåtenhet att ge åtkomst.

5. Leverantörerna av den berörda AI-modellen för allmänna ändamål eller deras ombud ska lämna den information som krävs. När det gäller juridiska personer, företag eller firmor, eller om leverantören inte är en juridisk person, ska de personer som är behöriga att företräda dem enligt lag eller stadgar tillhandahålla den begärda åtkomsten på uppdrag av leverantören av den berörda AI-modellen för allmänna ändamål.

6. Kommissionen ska anta genomförandeakter som fastställer närmare arrangemang och villkor för utvärderingarna, inbegripet närmare bestämmelser för deltagande av oberoende experter, och förfarandet för att välja ut dem. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

7. Innan AI-byrån begär åtkomst till den berörda AI-modellen för allmänna ändamål får den inleda en strukturerad dialog med leverantören av AI-modellen för allmänna ändamål för att samla in mer information om den interna testningen av modellen, interna skyddsåtgärder för att förebygga systemrisker och andra interna förfaranden och åtgärder som leverantören har vidtagit för att minska sådana risker.

Artikel 93

Befogenhet att begära åtgärder

1. När det är nödvändigt och lämpligt får kommissionen begära att leverantörer

a) vidtar lämpliga åtgärder för att fullgöra de skyldigheter som föreskrivs i artiklarna 53 och 54,

b) genomför riskreducerande åtgärder, om den utvärdering som utförts i enlighet med artikel 92 har gett upphov till allvarliga och väl underbyggda farhågor om en systemrisk på unionsnivå,

c) begränsa tillhandahållandet på marknaden, dra tillbaka eller återkalla modellen.

2. Innan en åtgärd begärs får AI-byrån inleda en strukturerad dialog med leverantören av AI-modellen för allmänna ändamål.

3. Om leverantören av AI-modellen för allmänna ändamål med systemrisk under den strukturerade dialog som avses i punkt 2 erbjuder att åta sig att genomföra riskreducerande åtgärder för att hantera en systemrisk på unionsnivå, får kommissionen genom beslut göra dessa åtaganden bindande och förklara att det inte finns några ytterligare skäl till åtgärder.

Artikel 94

Processuella rättigheter för ekonomiska operatörer av AI-modellen med allmänna ändamål

Artikel 18 i förordning (EU) 2019/1020 ska i tillämpliga delar gälla för leverantörer av AI-modellen för allmänna ändamål, utan att det påverkar de mer specifika processuella rättigheter som föreskrivs i den här förordningen.

KAPITEL X

UPPFÖRANDEKODER OCH RIKTLINJER

Artikel 95

Uppförandekod för frivillig tillämpning av specifika krav

1. AI-byrån och medlemsstaterna ska uppmuntra och underlätta utarbetandet av uppförandekoder, inbegripet tillhörande styrningsmekanismer, som är avsedda att främja frivillig tillämpning på AI-system, utom AI-system med hög risk, av vissa eller alla av de krav som anges i kapitel III avsnitt 2, med beaktande av tillgängliga tekniska lösningar och bästa branschpraxis som möjliggör tillämpning av sådana krav.

2. AI-byrån och medlemsstaterna ska underlätta utarbetandet av uppförandekoder för frivillig tillämpning, inbegripet av tillhandahållare, av särskilda krav på alla AI-system, på grundval av tydliga mål och centrala resultatindikatorer för att mäta uppnåendet av dessa mål, inbegripet men inte begränsat till, sådana inslag som

a) tillämpliga inslag som föreskrivs i unionens etiska riktlinjer för tillförlitlig AI,

b) bedöma och minimera AI-systemens inverkan på miljömässig hållbarhet, inbegripet när det gäller energieffektiv programmering och teknik för effektiv utformning, träning och användning av AI,

c) främja AI-kunnighet, särskilt hos personer som arbetar med utveckling, drift och användning av AI,

d) underlätta en inkluderande och diversifierad utformning av AI-system, bland annat genom att inrätta inkluderande och diversifierade utvecklingsteam och främja berörda parters deltagande i den processen,

e) bedöma och förebygga AI-systemens negativa inverkan på sårbara personer eller grupper av sårbara personer, inbegripet när det gäller tillgänglighet för personer med funktionsnedsättning, samt på jämställdheten.

3. Uppförandekoder får utarbetas av enskilda leverantörer eller tillhandahållare av AI-system eller av organisationer som företräder dem eller av båda dessa, inbegripet genom att eventuella berörda parter och deras representativa organisationer involveras, inbegripet organisationer i civilsamhället och den akademiska världen. Uppförandekoder får omfatta ett eller flera AI-system med beaktande av likheten mellan de berörda systemens avsedda ändamål.

4. När AI-byrån och medlemsstaterna uppmuntrar och underlättar utarbetandet av uppförandekoder ska de ta hänsyn till de särskilda intressen och behov som små och medelstora företag, inbegripet uppstartsföretag, har.

Artikel 96

Riktlinjer från kommissionen om genomförandet av denna förordning

1. Kommissionen ska utarbeta riktlinjer för det praktiska genomförandet av denna förordning, särskilt avseende

a) tillämpningen av de krav och skyldigheter som avses i artiklarna 8–15 och i artikel 25,

b) de förbjudna användningsområden som avses i artikel 5,

c) det praktiska genomförandet av bestämmelserna om väsentliga ändringar,

d) det praktiska genomförandet av de transparensskyldigheter som fastställs i artikel 50,

e) detaljerad information om denna förordnings förhållande till unionens harmoniseringslagstiftning som förtecknas i bilaga I samt med annan relevant unionsrätt, inbegripet när det gäller enhetlighet i efterlevnaden av den,

f) tillämpningen av definitionen av ett AI-system enligt artikel 3.1.

När kommissionen utfärdar sådana riktlinjer ska den ägna särskild uppmärksamhet åt behoven hos små och medelstora företag, inbegripet uppstartsföretag, lokala offentliga myndigheter och sektorer som mest sannolikt kommer att beröras av denna förordning.

De riktlinjer som avses i första stycket i denna punkt ska ta vederbörlig hänsyn till den allmänt erkända senaste utvecklingen när det gäller AI samt till relevanta harmoniserade standarder och gemensamma specifikationer som avses i artiklarna 40 och 41, eller till de harmoniserade standarder eller tekniska specifikationer som fastställs enligt unionens harmoniseringslagstiftning.

2. På begäran av medlemsstaterna eller AI-byrån, eller på eget initiativ, ska kommissionen uppdatera redan antagna riktlinjer när det anses nödvändigt.

KAPITEL XI

DELEGERING AV BEFOGENHETER OCH KOMMITTÉFÖRFARANDE

Artikel 97

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artiklarna 6.6, 6.7, 7.1, 7.3, 11.3, 43.5, 43.6, 47.5, 51.3, 52.4, 53.5 och 53.6 ska ges till kommissionen för en period på fem år från och med den 1 AUGUSTI 2024. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av perioden på fem år. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i artiklarna 6.6, 6.7, 7.1, 7.3, 11.3, 43.5, 43.6, 47.5, 51.3, 52.4, 53.5 och 53.6 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 6.6 eller 6.7, artikel 7.1 eller 7.3, artikel 11.3, artikel 43.5 eller 43.6, artikel 47.5, 51.3, 52.4 eller 53.5 eller artikel 53.6 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av tre månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med tre månader på Europaparlamentets eller rådets initiativ.

Artikel 98

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL XII

SANKTIONER

Artikel 99

Sanktioner

1. Medlemsstaterna ska i enlighet med de villkor som fastställs i denna förordning fastställa bestämmelser om sanktioner och andra efterlevnadsåtgärder som också kan innefatta varningar och icke-monetära åtgärder som ska tillämpas vid operatörers överträdelser av bestämmelserna i denna förordning och vidta alla nödvändiga åtgärder för att se till att de tillämpas korrekt och effektivt, varvid hänsyn ska tas till de riktlinjer som kommissionen utfärdat enligt artikel 96. Sanktionerna ska vara effektiva, proportionella och avskräckande. De ska ta hänsyn till små och medelstora företags, inbegripet uppstartsföretags, intressen och deras ekonomiska bärkraft.

2. Medlemsstaterna ska utan dröjsmål och senast den dag då denna förordning börjar tillämpas underrätta kommissionen om de regler om sanktioner och andra efterlevnadsåtgärder som avses i punkt 1 och utan dröjsmål underrätta den om eventuella senare ändringar av dem.

3. Bristande efterlevnad av förbudet mot de AI-användningsområden som avses i artikel 5 ska vara föremål för administrativa sanktionsavgifter på upp till 35 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 7 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

4. Bristande efterlevnad av någon av följande bestämmelser som hör samman med operatörer eller anmälda organ utöver de bestämmelser som fastställs i artikel 5 ska medföra administrativa sanktionsavgifter på upp till 15 000 000 EUR eller, om överträdelsen begås av ett företag, upp till 3 % av dess totala globala årsomsättning under det föregående räkenskapsåret, beroende på vilket som är högst:

a) Leverantörers skyldigheter enligt artikel 16.

b) Ombuds skyldigheter enligt artikel 22.

c) Importörers skyldigheter enligt artikel 23.

d) Distributörers skyldigheter enligt artikel 24.

e) Tillhandahållares skyldigheter enligt artikel 26.

f) Kraven och skyldigheterna för anmälda organ enligt artikel 31, 33.1, 33.3, 33.4 eller 34.

g) Transparensskyldigheterna för leverantörer och tillhandahållare enligt artikel 50.

5. Tillhandahållande av oriktig, ofullständig eller vilseledande information till anmälda organ eller nationella behöriga myndigheter som svar på en begäran ska medföra administrativa sanktionsavgifter på upp till 7 500 000 EUR eller, om överträdelsen begås av ett företag, upp till 1 % av dess totala globala årsomsättning för det föregående räkenskapsåret, beroende på vilket som är högst.

6. När det gäller små och medelstora företag, inbegripet uppstartsföretag, ska varje sanktionsavgift som avses i denna artikel uppgå till högst de procentsatser eller belopp som avses i punkterna 3, 4 och 5, beroende på vilket belopp som är lägre.

7. Vid beslut om huruvida administrativa sanktionsavgifter ska åläggas och beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn, i förekommande fall, tas till

a) överträdelsens art, svårighetsgrad och varaktighet samt dess konsekvenser med beaktande av det berörda AI-systemets syfte samt, när så är lämpligt, antalet berörda personer och omfattningen av den skada som de har lidit,

b) huruvida administrativa sanktionsavgifter redan har tillämpats av andra marknadskontrollmyndigheter på samma operatör för samma överträdelse,

c) huruvida administrativa sanktionsavgifter redan har tillämpats av andra myndigheter på samma operatör för överträdelser av annan unionsrätt eller nationell rätt, när sådana överträdelser beror på samma verksamhet eller underlåtenhet som utgör en relevant överträdelse av denna förordning,

d) storleken på, årsomsättningen och marknadsandelen för den operatör som begått överträdelsen,

e) eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen,

f) graden av samarbete med nationella behöriga myndigheter för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter,

g) operatörens grad av ansvar med beaktande av de tekniska och organisatoriska åtgärder som genomförts av denne,

h) det sätt på vilket överträdelsen kom till den nationella behöriga myndighetens kännedom, särskilt huruvida, och i sådana fall i vilken mån, operatören anmälde överträdelsen,

i) om överträdelsen skett med uppsåt eller genom oaktsamhet,

j) alla åtgärder som vidtagits av operatören för att minska den skada som de berörda personerna lidit.

8. Varje medlemsstat ska fastställa regler om i vilken utsträckning administrativa sanktionsavgifter får påföras offentliga myndigheter och organ som är inrättade i medlemsstaten.

9. Beroende på medlemsstatens rättssystem får reglerna om administrativa sanktionsavgifter tillämpas på ett sådant sätt att sanktionsavgifterna utdöms av behöriga nationella domstolar eller andra organ, beroende på vad som är tillämpligt i dessa medlemsstater. Tillämpningen av sådana regler i dessa medlemsstater ska ha motsvarande verkan.

10. Utövandet av befogenheter enligt denna artikel ska omfattas av lämpliga rättssäkerhetsgarantier i enlighet med unionsrätten och nationell rätt, inbegripet effektiva rättsmedel och rättssäkerhet.

11. Medlemsstaterna ska årligen underrätta kommissionen om de administrativa sanktionsavgifter som de har utfärdat under det året, i enlighet med denna artikel, och om eventuella relaterade rättstvister eller rättsliga förfaranden.

Artikel 100

Administrativa sanktionsavgifter för unionens institutioner, organ och byråer

1. Europeiska datatillsynsmannen får ålägga administrativa sanktionsavgifter för de av unionens institutioner, organ och byråer som omfattas av denna förordning. Vid beslut om huruvida administrativa sanktionsavgifter ska åläggas och beslut om storleken på den administrativa sanktionsavgiften i varje enskilt fall ska alla relevanta omständigheter i den specifika situationen beaktas och vederbörlig hänsyn ska tas till följande:

a) Överträdelsens art, svårighetsgrad och varaktighet samt dess konsekvenser, med beaktande av det berörda AI-systemets syfte samt, när så är lämpligt, antalet berörda personer och omfattningen av den skada som de har lidit.

b) Graden av unionsinstitutionens, unionsorganets eller unionsbyråns ansvar, med beaktande av de tekniska och organisatoriska åtgärder som de har genomfört.

c) Alla åtgärder som unionsinstitutionen, unionsorganet eller unionsbyrån vidtar för att mildra den skada som de berörda personerna lidit.

d) Graden av samarbete med Europeiska datatillsynsmannen för att åtgärda överträdelsen och minska dess potentiella negativa effekter, inbegripet efterlevnad av någon av de åtgärder som tidigare förordnats av Europeiska datatillsynsmannen mot unionens berörda institution, organ eller byrå med avseende på samma fråga.

e) Eventuella liknande tidigare överträdelser som begåtts av unionens institution, organ eller byrå.

f) Det sätt på vilket överträdelsen kom till Europeiska datatillsynsmannens kännedom, särskilt huruvida och i så fall i vilken omfattning unionsinstitutionen, unionsorganet eller unionsbyrån anmälde överträdelsen.

g) Den årliga budgeten för unionsinstitutionen, unionsbyrån eller unionsorganet.

2. Bristande efterlevnad av det förbud mot AI-användningsområden som avses i artikel 5 ska medföra administrativa sanktionsavgifter på upp till 1 500 000 EUR.

3. AI-systemets bristande efterlevnad av andra krav eller skyldigheter enligt denna förordning än de som fastställs i artikel 5 ska medföra administrativa sanktionsavgifter på upp till 750 000 EUR.

4. Innan ett beslut fattas enligt denna artikel ska Europeiska datatillsynsmannen ge den eller det av unionens institutioner, organ eller byråer som är föremål för förfarandet som genomförs av Europeiska datatillsynsmannen möjlighet att höras om den möjliga överträdelsen. Europeiska datatillsynsmannen ska grunda sina beslut endast på inslag och omständigheter som de berörda parterna har getts möjlighet att yttra sig om. Eventuella klagande ska vara nära knutna till förfarandet.

5. De berörda parternas rätt till försvar ska iakttas fullständigt i förfarandena. De ska ha rätt att få tillgång till Europeiska datatillsynsmannens akt, med förbehåll för enskildas eller företags berättigade intresse av skydd av sina personuppgifter eller affärshemligheter.

6. De medel som samlats in genom åläggande av sanktionsavgifter i denna artikel ska bidra till unionens allmänna budget. Sanktionsavgifterna får inte påverka den ändamålsenliga funktionen för den unionsinstitution, det unionsorgan eller unionsbyrå som ålagts sanktionsavgiften.

7. Europeiska datatillsynsmannen ska årligen underrätta kommissionen om de administrativa sanktionsavgifter som den ålagt enligt denna artikel och om eventuella rättstvister eller rättsliga förfaranden den inlett.

Artikel 101

Sanktionsavgifter för leverantörer av AI-modeller för allmänna ändamål

1. Kommissionen får ålägga leverantörer av AI-modeller för allmänna ändamål sanktionsavgifter på upp till 3 % av deras totala globala årsomsättning under det föregående räkenskapsåret eller 15 000 000 EUR, beroende på vilket som är högst, om kommissionen konstaterar att leverantören uppsåtligen eller av oaktsamhet har

a) överträtt de relevanta bestämmelserna i denna förordning,

b) underlåtit att tillmötesgå en begäran om en handling eller om information enligt artikel 91, eller lämnat oriktiga, ofullständiga eller vilseledande uppgifter,

c) underlåtit att följa en åtgärd som begärts enligt artikel 93,

d) underlåtit att ge kommissionen tillgång till AI-modellen för allmänna ändamål eller AI-modellen för allmänna ändamål med systemrisk i syfte att genomföra en utvärdering enligt artikel 92.

Vid fastställandet av sanktionsavgiften eller det löpande vitesbeloppet ska hänsyn tas till överträdelsens art, allvarlighet och varaktighet, varvid vederbörlig hänsyn ska tas till principerna om proportionalitet och lämplighet. Kommissionen ska också beakta åtaganden som gjorts i enlighet med artikel 93.3 eller som gjorts i relevanta uppförandekoder i enlighet med artikel 56.

2. Innan kommissionen antar beslutet enligt punkt 1 ska den meddela sina preliminära iakttagelser till leverantören av AI-modellen för allmänna ändamål och ge denne möjlighet att höras.

3. Sanktionsavgifter som åläggs i enlighet med denna artikel ska vara effektiva, proportionella och avskräckande.

4. Information om sanktionsavgifter som ålagts enligt denna artikel ska också lämnas till styrelsen när så är lämpligt.

5. Europeiska unionens domstol ska ha obegränsad behörighet att pröva kommissionens beslut om fastställande av sanktionsavgifter enligt denna artikel. Den får upphäva, sänka eller höja ålagda sanktionsavgifter.

6. Kommissionen ska anta genomförandeakter med närmare bestämmelser och rättssäkerhetsgarantier för förfaranden inför ett eventuellt antagande av beslut enligt punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 98.2.

KAPITEL XIII

SLUTBESTÄMMELSER

Artikel 102

Ändring av förordning (EG) nr 300/2008

I artikel 4.3 i förordning (EG) nr 300/2008 ska följande stycke läggas till:

"Vid antagandet av detaljerade bestämmelser avseende tekniska specifikationer och förfaranden för godkännande och användning av säkerhetsutrustning som rör system för artificiell intelligens i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/1689 (*), ska kraven i kapitel III avsnitt 2 i den förordningen beaktas.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 103

Ändring av förordning (EU) nr 167/2013

I artikel 17.5 i förordning (EU) nr 167/2013 ska följande stycke läggas till:

"Vid antagandet av delegerade akter enligt första stycket rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/1689 (*) ska kraven i kapitel III avsnitt 2 i den förordningen beaktas.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 104

Ändring av förordning (EU) nr 168/2013

I artikel 22.5 i förordning (EU) nr 168/2013 ska följande stycke läggas till:

"Vid antagandet av delegerade akter enligt första stycket rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/1689 (*) ska kraven i kapitel III avsnitt 2 i den förordningen beaktas.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 105

Ändring av direktiv 2014/90/EU

I artikel 8 i direktiv 2014/90/EU ska följande punkt läggas till:

"5. För system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/1689 (*) ska kommissionen, när den utför sin verksamhet enligt punkt 1 och när den antar tekniska specifikationer och provningsstandarder i enlighet med punkterna 2 och 3, beakta de krav som anges i kapitel III avsnitt 2 i den förordningen.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, ELI: 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 106

Ändring av direktiv (EU) 2016/797

I artikel 5 i direktiv (EU) 2016/797 ska följande punkt läggas till:

"12. Vid antagandet av delegerade akter enligt punkt 1 och genomförandeakter enligt punkt 11 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/1689 (*) ska kraven i kapitel III avsnitt 2 i den förordningen beaktas.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, ELI: 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 107

Ändring av förordning (EU) 2018/858

I artikel 5 i förordning (EU) 2018/858 ska följande punkt läggas till:

"4. Vid antagandet av delegerade akter enligt punkt 3 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/1689 (*) ska kraven i kapitel III avsnitt 2 i den förordningen beaktas.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, ELI: 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 108

Ändringar av förordning (EU) 2018/1139

Förordning (EU) 2018/1139 ska ändras på följande sätt:

1. I artikel 17 ska följande punkt läggas till:

"3. Utan att det påverkar tillämpningen av punkt 2 ska vid antagandet av genomförandeakter enligt punkt 1 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/ 1689 (*) kraven i kapitel III avsnitt 2 i den förordningen beaktas.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, ELI: 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/ reg/2024/1689/oj)."

2. I artikel 19 ska följande punkt läggas till:

"4. Vid antagandet av delegerade akter enligt punkterna 1 och 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/ 1689 ska kraven i kapitel III avsnitt 2 i den förordningen beaktas."

3. I artikel 43 ska följande punkt läggas till:

"4. Vid antagandet av genomförandeakter enligt punkt 1 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/1689 ska kraven i kapitel III avsnitt 2 i den förordningen beaktas."

4. I artikel 47 ska följande punkt läggas till:

"3. Vid antagandet av delegerade akter enligt punkterna 1 och 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/1689 ska kraven i kapitel III avsnitt 2 i den förordningen beaktas."

5. I artikel 57 ska följande punkt läggas till:

"Vid antagandet av dessa genomförandeakter rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/1689 ska kraven i kapitel III avsnitt 2 i den förordningen beaktas."

6. I artikel 58 ska följande punkt läggas till:

"3. Vid antagandet av delegerade akter enligt punkterna 1 och 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i förordning (EU) 2024/1689 ska kraven i kapitel III avsnitt 2 i den förordningen beaktas."

Artikel 109

Ändring av förordning (EU) 2019/2144

I artikel 11 i förordning (EU) 2019/2144 ska följande punkt läggas till:

"3. Vid antagandet av genomförandeakter enligt punkt 2 rörande system för artificiell intelligens som är säkerhetskomponenter i den mening som avses i Europaparlamentets och rådets förordning (EU) 2024/1689 (*) ska kraven i kapitel III avsnitt 2 i den förordningen beaktas.

(*) Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, ELI: 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 110

Ändring av direktiv (EU) 2020/1828

I bilaga I till Europaparlamentets och rådets direktiv (EU) 2020/1828 ([58]) ska följande punkt läggas till:

"68. Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens) (EUT L, ELI: 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj)."

Artikel 111

AI-system som redan släppts ut på marknaden eller tagits i bruk och AI-modeller för allmänna ändamål som redan släppts ut på marknaden

1. Utan att det påverkar tillämpningen av artikel 5 enligt artikel 113.3 a ska AI-system som är komponenter i de stora it-system som inrättats genom de rättsakter som förtecknas i bilaga X och som har släppts ut på marknaden eller tagits i bruk före den 2 augusti 2027 bringas i överensstämmelse med denna förordning senast den 31 december 2030.

De krav som fastställs i denna förordning ska beaktas vid den utvärdering av varje stort it-system inrättat genom de rättsakter förtecknade i bilaga X som ska utföras i enlighet med de rättsakterna och i de fall dessa rättsakter ersätts eller ändras.

2. Utan att det påverkar tillämpningen av artikel 5 enligt artikel 113.3 a ska denna förordning tillämpas på andra operatörer av AI-system med hög risk än de system som avses i punkt 1 i den här artikeln och som har släppts ut på marknaden eller tagits i bruk före den 2 augusti 2026, endast om dessa system från och med den dagen förändras betydligt när det gäller sin utformning. Under alla omständigheter ska leverantörer och tillhandahållare av AI-system med hög risk som är avsedda att användas av offentliga myndigheter vidta nödvändiga åtgärder för att uppfylla kraven och skyldigheterna i denna förordning senast den 2 augusti 2030.

3. Leverantörer av AI-modeller för allmänna ändamål som har släppts ut på marknaden före den 2 augusti 2025 ska vidta nödvändiga åtgärder för att uppfylla de skyldigheter som fastställs i denna förordning senast den 2 augusti 2027.

([58]) Europaparlamentets och rådets direktiv (EU) 2020/1828 av den 25 november 2020 om grupptalan för att skydda konsumenters kollektiva intressen och om upphävande av direktiv 2009/22/EG (EUT L 409, 4.12.2020, s. 1).

Artikel 112

Utvärdering och översyn

1. Kommissionen ska bedöma behovet av att ändra förteckningen i bilaga III och av förteckningen i artikel 5 över förbjudna AI-användningsområden en gång om året efter det att denna förordning har trätt i kraft och fram till utgången av perioden för delegering av befogenhet i artikel 97. Kommissionen ska lägga fram resultaten av denna bedömning för Europaparlamentet och rådet.

2. Senast den 2 augusti 2028 och därefter vart fjärde år ska kommissionen utvärdera och rapportera till Europaparlamentet och rådet om följande:

a) Behovet av ändringar som utvidgar befintliga områdesrubriker eller lägger till nya områdesrubriker i bilaga III.

b) Ändringar av förteckningen över AI-system som kräver ytterligare transparensåtgärder i enlighet med artikel 50.

c) Ändringar som ökar tillsyns- och styrningssystemets effektivitet.

3. Kommissionen ska senast den 2 augusti 2029 och därefter vart fjärde år överlämna en rapport om utvärderingen och översynen av denna förordning till Europaparlamentet och rådet. Rapporten ska innehålla en bedömning av efterlevnadskontrollens struktur och det eventuella behovet av att en unionsbyrå kommer till rätta med eventuella konstaterade brister. På grundval av resultaten ska denna rapport vid behov åtföljas av ett förslag till ändring av denna förordning. Rapporten ska offentliggöras.

4. I de rapporter som avses i punkt 2 ska särskild uppmärksamhet ägnas åt

a) statusen för de nationella behöriga myndigheternas ekonomiska resurser, tekniska utrustning och personal för att effektivt kunna utföra de uppgifter som de tilldelas enligt denna förordning,

b) tillståndet för sanktionerna, särskilt de administrativa sanktionsavgifter som avses i artikel 99.1 och som tillämpas av medlemsstaterna på överträdelser av bestämmelserna i denna förordning,

c) antagna harmoniserade standarder och gemensamma specifikationer som utarbetats till stöd för denna förordning,

d) antalet företag som kommer in på marknaden efter det att denna förordning har börjat tillämpas och hur många av dem som är små och medelstora företag.

5. Senast den 2 augusti 2028 ska kommissionen utvärdera AI-byråns funktion, huruvida AI-byrån har fått tillräckliga befogenheter och tillräcklig behörighet för att fullgöra sina uppgifter och huruvida det skulle vara relevant och nödvändigt för ett korrekt genomförande och en korrekt kontroll av efterlevnaden av denna förordning att uppgradera byrån och dess befogenheter när det gäller efterlevnadskontroll och öka dess resurser. Kommissionen ska överlämna en rapport om sin utvärdering till Europaparlamentet och rådet.

6. Senast den 2 augusti 2028 och därefter vart fjärde år ska kommissionen lägga fram en rapport om översynen av framstegen med utvecklingen av standardiseringsprodukter för energieffektiv utveckling av AI-modeller för allmänna ändamål, och utvärdera behovet av ytterligare åtgärder eller insatser, inbegripet bindande åtgärder eller insatser. Rapporten ska överlämnas till Europaparlamentet och rådet, och den ska offentliggöras.

7. Senast den 2 augusti 2028 och därefter vart tredje år ska kommissionen utvärdera de frivilliga uppförandekodernas inverkan och effektivitet för att främja tillämpningen av kraven i kapitel III avsnitt 2 för andra AI-system än AI-system med hög risk och eventuellt andra ytterligare krav för AI-system andra än AI-system med hög risk, inbegripet vad gäller miljömässig hållbarhet.

8. Vid tillämpning av punkterna 1–7 ska styrelsen, medlemsstaterna och de nationella behöriga myndigheterna vid begäran tillhandahålla information till kommissionen utan oskäligt dröjsmål.

9. Kommissionen ska när den utför de utvärderingar och översyner som avses i punkterna 1 till 7 ta hänsyn till ståndpunkter och slutsatser från styrelsen, Europaparlamentet, rådet och andra relevanta organ eller källor.

10. Kommissionen ska om nödvändigt överlämna lämpliga förslag om ändring av denna förordning, med särskild hänsyn till teknikens utveckling och AI-systems inverkan på hälsa och säkerhet och grundläggande rättigheter och mot bakgrund av tendenserna inom informationssamhället.

11. För att vägleda de utvärderingar och översyner som avses i punkterna 1–7 ska AI-byrån åta sig att ta fram en objektiv och deltagandebaserad metod för utvärdering av risknivåerna på grundval av de kriterier som anges i de relevanta artiklarna och införandet av nya system i

a) förteckningen i bilaga III, inbegripet utvidgning av befintliga områdesrubriker eller tillägg av nya områdesrubriker i denna bilaga,

b) förteckningen över de förbjudna användningsområden som fastställs i artikel 5, och

c) förteckningen över AI-system som kräver ytterligare transparensåtgärder enligt artikel 50.

12. Varje ändring av denna förordning enligt punkt 10, eller relevanta delegerade akter eller genomförandeakter, som rör unionens sektorsspecifika harmoniseringslagstiftning som förtecknas i bilaga I avsnitt B, ska ta hänsyn till särdragen i lagstiftningen inom varje sektor och befintliga mekanismer för styrning, bedömning av överensstämmelse och efterlevnadskontroll samt myndigheter som inrättats inom denna.

13. Senast den 2 augusti 2031 ska kommissionen göra en bedömning av efterlevnadskontrollen av denna förordning och lämna en rapport om detta till Europaparlamentet, rådet samt Europeiska ekonomiska och sociala kommittén med beaktande av de första åren av tillämpningen av denna förordning. På grundval av resultaten ska denna rapport vid behov åtföljas av ett förslag till ändring av denna förordning med avseende på efterlevnadskontrollens struktur och behovet av att en EU-byrå kommer till rätta med eventuella konstaterade brister.

Artikel 113

Ikraftträdande och tillämpning

Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Den ska tillämpas från och med den 2 augusti 2026.

Emellertid gäller att

a) kapitlen I och II ska tillämpas från och med den 2 februari 2025, att

b) kapitel III avsnitt 4, kapitlen V, VII och XII samt artikel 78 ska tillämpas från och med den 2 augusti 2025, med undantag för artikel 101, och att

c) artikel 6.1 och motsvarande skyldigheter i denna förordning ska tillämpas från och med den 2 augusti 2027.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 13 juni 2024.

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*
R. METSOLA	M. MICHEL

BILAGA I

Förteckning över unionens harmoniseringslagstiftning

Avsnitt A – Förteckning över unionens harmoniseringslagstiftning som bygger på den nya lagstiftningsramen

1. 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).

2. Europaparlamentets och rådets direktiv 2009/48/EG av den 18 juni 2009 om leksakers säkerhet (EUT L 170, 30.6.2009, s. 1).

3. Europaparlamentets och rådets direktiv 2013/53/EU av den 20 november 2013 om fritidsbåtar och vattenskotrar och om upphävande av direktiv 94/25/EG (EUT L 354, 28.12.2013, s. 90).

4. Europaparlamentets och rådets direktiv 2014/33/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om hissar och säkerhetskomponenter till hissar (EUT L 96, 29.3.2014, s. 251).

5. Europaparlamentets och rådets direktiv 2014/34/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om utrustning och skyddssystem som är avsedda för användning i potentiellt explosiva atmosfärer (EUT L 96, 29.3.2014, s. 309).

6. Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG (EUT L 153, 22.5.2014, s. 62).

7. Europaparlamentets och rådets direktiv 2014/68/EU av den 15 maj 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av tryckbärande anordningar (EUT L 189, 27.6.2014, s. 164).

8. Europaparlamentets och rådets förordning (EU) 2016/424 av den 9 mars 2016 om linbaneanläggningar och om upphävande av direktiv 2000/9/EG (EUT L 81, 31.3.2016, s. 1).

9. Europaparlamentets och rådets förordning (EU) 2016/425 av den 9 mars 2016 om personlig skyddsutrustning och om upphävande av rådets direktiv 89/686/EEG (EUT L 81, 31.3.2016, s. 51).

10. Europaparlamentets och rådets förordning (EU) 2016/426 av den 9 mars 2016 om anordningar för förbränning av gasformiga bränslen och om upphävande av direktiv 2009/142/EG (EUT L 81, 31.3.2016, s. 99).

11. 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).

12. Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för *in vitro*-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117, 5.5.2017, s. 176).

Avsnitt B. Förteckning över annan unionsharmoniseringslagstiftning

13. Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

14. Europaparlamentets och rådets förordning (EU) nr 168/2013 av den 15 januari 2013 om godkännande av och marknadstillsyn för två- och trehjuliga fordon och fyrhjulingar (EUT L 60, 2.3.2013, s. 52).

15. Europaparlamentets och rådets förordning (EU) nr 167/2013 av den 5 februari 2013 om godkännande och marknadstillsyn av jordbruks- och skogsbruksfordon (EUT L 60, 2.3.2013, s. 1).

16. Europaparlamentets och rådets direktiv 2014/90/EU av den 23 juli 2014 om marin utrustning och om upphävande av rådets direktiv 96/98/EG (EUT L 257, 28.8.2014, s. 146).

17. Europaparlamentets och rådets direktiv (EU) 2016/797 av den 11 maj 2016 om driftskompatibiliteten hos järnvägssystemet inom Europeiska unionen (EUT L 138, 26.5.2016, s. 44).

18. Europaparlamentets och rådets förordning (EU) 2018/858 av den 30 maj 2018 om godkännande av och marknadskontroll över motorfordon och släpfordon till dessa fordon samt av system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, om ändring av förordningarna (EG) nr 715/2007 och (EG) nr 595/2009 samt om upphävande av direktiv 2007/46/EG (EUT L 151, 14.6.2018, s. 1).

19. Europaparlamentets och rådets förordning (EU) 2019/2144 av den 27 november 2019 om krav för typgodkännande av motorfordon och deras släpvagnar samt de system, komponenter och separata tekniska enheter som är avsedda för sådana fordon, med avseende på deras allmänna säkerhet och skydd för personer i fordonet och oskyddade trafikanter, om ändring av Europaparlamentets och rådets förordning (EU) 2018/858 och om upphävande av Europaparlamentets och rådets förordningar (EG) nr 78/2009, (EG) nr 79/2009 och (EG) nr 661/2009 samt kommissionens förordningar (EG) nr 631/2009, (EU) nr 406/2010, (EU) nr 672/2010, (EU) nr 1003/2010, (EU) nr 1005/2010, (EU) nr 1008/2010, (EU) nr 1009/2010, (EU) nr 19/2011, (EU) nr 109/2011, (EU) nr 458/2011, (EU) nr 65/2012, (EU) nr 130/2012, (EU) nr 347/2012, (EU) nr 351/2012, (EU) nr 1230/2012 och (EU) 2015/166 (EUT L 325, 16.12.2019, s. 1).

20. Europaparlamentets och rådets förordning (EU) nr 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1), i den mån det rör sig om konstruktion, produktion och utsläppande på marknaden av luftfartyg som avses i artikel 2.1 a och b i den förordningen, när det gäller obemannade luftfartyg och deras motorer, propellrar, delar och utrustning för att kontrollera dem på distans

BILAGA II

Förteckning över de brott som avses i artikel 5.1 första stycket h iii

Brott som avses i artikel 5.1 första stycket h iii:

— Terrorism.

— Människohandel.

— Sexuell exploatering av barn och barnpornografi.

— Olaglig handel med narkotika och psykotropa ämnen.

— Olaglig handel med vapen, ammunition och sprängämnen.

— Mord och grov misshandel.

— Olaglig handel med mänskliga organ eller vävnader.

— Olaglig handel med nukleära och radioaktiva ämnen.

— Människorov, olaga frihetsberövande och tagande av gisslan.

— Brott som omfattas av Internationella brottmålsdomstolens behörighet.

— Kapning av flygplan eller fartyg.

— Våldtäkt.

— Miljöbrott.

— Organiserad stöld eller väpnat rån.

— Sabotage.

— Deltagande i en kriminell organisation inblandad i ett eller flera av de brott som förtecknas ovan.

BILAGA III

AI-system med hög risk som avses i artikel 6.2

AI-system med hög risk enligt artikel 6.2 är de AI-system som används inom något av följande områden:

1. Biometri, i den mån användningen är tillåten enligt relevant unionsrätt eller nationell rätt:

   a) System för biometrisk fjärridentifiering.

      Detta omfattar inte de AI-system som är avsedda att användas för biometrisk verifiering och vars enda syfte är att bekräfta att en viss fysisk person är den person som han eller hon påstår sig vara.

   b) AI-system som är avsedda att användas för biometrisk kategorisering enligt känsliga eller skyddade attribut eller egenskaper som grundar sig på inferens av dessa attribut eller egenskaper.

   c) AI-system som är avsedda att användas för känsloigenkänning.

2. Kritisk infrastruktur: AI-system som är avsedda att användas som säkerhetskomponenter i samband med förvaltning och drift av kritisk digital infrastruktur, vägtrafik eller i samband med tillhandahållande av vatten, gas, värme och el.

3. Utbildning och yrkesutbildning:

   a) AI-system som är avsedda att användas för att fastställa tillgång eller antagning eller för att anvisa fysiska personer till institutioner för yrkesutbildning eller annan utbildning på alla nivåer.

   b) AI-system som är avsedda att användas för att utvärdera läranderesultat, även när dessa resultat används för att styra fysiska personers lärandeprocess vid institutioner för yrkesutbildning eller annan utbildning på alla nivåer.

   c) AI-system som är avsedda att användas för att bedöma den lämpliga utbildningsnivå som en person kommer att erhålla eller kommer att kunna få tillgång till, inom ramen för eller vid institutioner för yrkesutbildning eller annan utbildning på alla nivåer.

   d) AI-system som är avsedda att användas för att övervaka och upptäcka förbjudet beteende bland studerande under provtillfällen inom ramen för eller vid institutioner för yrkesutbildning eller annan utbildning på alla nivåer.

4. Anställning, arbetsledning och tillgång till egenföretagande:

   a) AI-system som är avsedda att användas för rekrytering eller urval av fysiska personer, särskilt för att publicera riktade platsannonser, analysera och filtrera platsansökningar och utvärdera kandidater.

   b) AI-system som är avsedd att användas för att fatta beslut som påverkar villkoren för arbetsrelaterade förhållanden, befordringar och uppsägningar av arbetsrelaterade avtalsförhållanden, för uppgiftsfördelning på grundval av individuellt beteende eller personlighetsdrag eller egenskaper eller för att övervaka och utvärdera personers prestationer och beteende inom ramen för sådana förhållanden.

5. Tillgång till och åtnjutande av väsentliga privata tjänster och väsentliga offentliga tjänster och förmåner:

   a) AI-system som är avsedda att användas av offentliga myndigheter eller för offentliga myndigheters räkning för att utvärdera fysiska personers rätt till väsentliga förmåner och tjänster i form av offentligt stöd, inbegripet hälso- och sjukvårdstjänster, samt för att bevilja, minska, upphäva eller återkalla sådana förmåner och tjänster.

   b) AI-system som är avsedda att användas för att utvärdera fysiska personers kreditvärdighet eller fastställa deras kreditbetyg, med undantag för AI-system som används i syfte att upptäcka ekonomiska bedrägerier.

   c) AI-system som är avsedda att användas för riskbedömning och prissättning i förhållande till fysiska personer när det gäller livförsäkring och sjukförsäkring.

d) AI-system som är avsedda att utvärdera och klassificera nödsamtal från fysiska personer eller användas för att sända ut eller för att fastställa prioriteringsordningen för utsändning av larmtjänster, inbegripet polis, brandkår och ambulans, samt av patientsorteringssystem för akutsjukvård.

6. Brottsbekämpning, i den mån användningen är tillåten enligt relevant unionsrätt eller nationell rätt:

a) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer till stöd för brottsbekämpande myndigheter eller för deras räkning för att bedöma risken för att en fysisk person ska falla offer för brott.

b) AI-system som är avsedda att användas som lögndetektorer eller liknande verktyg av brottsbekämpande myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer till stöd för brottsbekämpande myndigheter.

c) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer till stöd för brottsbekämpande myndigheter för att bedöma hur pass tillförlitlig bevisningen är i samband med utredning eller lagföring av brott.

d) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer till stöd för brottsbekämpande myndigheter för att bedöma risken för att en fysisk person begår eller på nytt begår ett brott, inte enbart på grundval av profilering av fysiska personer i enlighet med artikel 3.4 i direktiv (EU) 2016/680 eller för att bedöma fysiska personers eller gruppers personlighetsdrag och egenskaper eller tidigare brottsliga beteende.

e) AI-system som är avsedda att användas av brottsbekämpande myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer till stöd för brottsbekämpande myndigheter för profilering av fysiska personer enligt artikel 3.4 i direktiv (EU) 2016/680 vid upptäckt, utredning eller lagföring av brott.

7. Migration, asyl och gränskontrollförvaltning, i den mån användningen är tillåten enligt relevant unionsrätt eller nationell rätt:

a) AI-system som är avsedda att användas som lögndetektorer eller liknande verktyg av behöriga offentliga myndigheter eller för deras räkning, eller av unionens institutioner, organ och byråer.

b) AI-system som är avsedda att användas av behöriga offentliga myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer för att bedöma en risk, inbegripet en säkerhetsrisk, en risk för irreguljär migration eller en hälsorisk som utgörs av en fysisk person som avser resa in på eller har rest in på en medlemsstats territorium.

c) AI-system som är avsedda att användas av behöriga offentliga myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer för att bistå behöriga offentliga myndigheter vid prövningen av ansökningar om asyl, visering eller uppehållstillstånd och för därmed sammanhängande klagomål om huruvida de fysiska personer som ansöker om status uppfyller kraven, inbegripet relaterade bedömningar av bevisens tillförlitlighet.

d) AI-system som är avsedda att användas av behöriga offentliga myndigheter eller för deras räkning, eller av unionens institutioner, organ eller byråer, i samband med migrations-, asyl- eller gränskontrollförvaltning, i syfte att upptäcka, känna igen eller identifiera fysiska personer, med undantag för verifiering av resehandlingar.

8. Rättskipning och demokratiska processer:

a) AI-system som är avsedda att användas av en rättslig myndighet eller på dess vägnar för att hjälpa en rättslig myndighet att undersöka och tolka fakta och lagstiftning och att tillämpa lagen på konkreta fakta, eller som är avsedda att användas på ett likande sätt i alternativa tvistlösningar.

b) AI-system som är avsedda att användas för att påverka resultatet av ett val eller en folkomröstning eller fysiska personers röstningsbeteende när dessa utövar sin rätt att rösta i val eller folkomröstningar. Detta omfattar inte AI-system vars utdata fysiska personer inte är direkt exponerade för, såsom verktyg som används för att organisera, optimera eller strukturera politiska kampanjer ur administrativ eller logistisk synvinkel.

BILAGA IV

Teknisk dokumentation som avses i artikel 11.1

Den tekniska dokumentation som avses i artikel 11.1 ska minst innehålla följande information, beroende på vad som är tillämpligt för det relevanta AI-systemet:

1. En allmän beskrivning av AI-systemet, inklusive

   a) det avsedda syftet, namnet på leverantören och version av systemet, som återspeglar dess samband med tidigare versioner,

   b) hur AI-systemet interagerar eller kan användas för att interagera med maskinvara eller programvara, inbegripet med andra AI-system som inte ingår i själva AI-systemet, i tillämpliga fall,

   c) versioner av relevant programvara eller fast programvara och eventuella krav med koppling till uppdatering av versioner,

   d) en beskrivning av alla format i vilka AI-systemet släpps ut på marknaden eller tas i bruk, såsom programvarupaket inbäddat i maskinvara, nedladdningar eller API,

   e) en beskrivning av den maskinvara som AI-systemet är avsett att köras på,

   f) om AI-systemet är en produktkomponent, fotografier eller illustrationer där de yttre egenskaperna framgår, samt dessa produkters märkning och interna utformning,

   g) en grundläggande beskrivning av det användargränssnitt som tillhandahålls tillhandahållaren,

   h) bruksanvisningar för tillhandahållaren och, i tillämpliga fall, en grundläggande beskrivning av det användargränssnitt som tillhandahålls tillhandahållaren.

2. En utförlig beskrivning av komponenterna i AI-systemet och av processen för utveckling av detta, inklusive

   a) de metoder och åtgärder som vidtas för att utveckla AI-systemet, inbegripet, i relevanta fall, användningen av förtränade system eller verktyg som tillhandahålls av tredje parter och hur dessa har använts, integrerats eller ändrats av leverantören,

   b) systemets designspecifikationer, dvs. AI-systemets och algoritmernas allmänna logik, de viktigaste valen vid utformningen, bl.a. motiveringen och de antaganden som gjorts, inbegripet med avseende på de personer eller grupper av personer som systemet är avsett att användas för, de viktigaste klassificeringsvalen, vad systemet har utformats för att optimera och de olika parametrarnas relevans, beskrivningen av systemets förväntade utdata och utdatakvalitet, de beslut om eventuella avvägningar mellan de tekniska lösningarna som valts för att uppfylla kraven i kapitel III avsnitt 2,

   c) en beskrivning av systemarkitekturen som förklarar hur programvarukomponenter bygger på eller påverkar varandra och integreras i den övergripande behandlingen, de dataresurser som används för att utveckla, träna, testa och validera AI-systemet,

   d) i relevanta fall uppgiftskraven i form av datablad som beskriver de träningsmetoder och träningstekniker och de träningsdataset som används, inbegripet en allmän beskrivning av dessa dataset, information om var dessa kommer från, deras omfattning och huvudsakliga egenskaper, hur uppgifterna inhämtades och valdes ut, märkningsförfaranden (t.ex. för övervakad inlärning), datarensningsmetoder (t.ex. upptäckt av avvikande värden),

   e) en bedömning av de åtgärder för mänsklig kontroll som krävs i enlighet med artikel 14, inbegripet en bedömning av de tekniska åtgärder som krävs för att underlätta tillhandahållarnas tolkning av AI-systemens resultat, i enlighet med artikel 13.3 d,

   f) i tillämpliga fall, en utförlig beskrivning av sådana ändringar av AI-systemet och dess prestanda som fastställts på förhand, tillsammans med all relevant information om de tekniska lösningar som har valts för att säkerställa att AI-systemet kontinuerligt uppfyller de relevanta kraven i kapitel III avsnitt 2,

   g) de validerings- och testningsförfaranden som används, inklusive information om de validerings- och testdata som har använts och deras huvudsakliga egenskaper, mått som används för att mäta riktighet, robusthet och överensstämmelse med andra relevanta krav som anges i kapitel III avsnitt 2 samt potentiellt diskriminerande effekter; testloggar och alla testrapporter, daterade och undertecknade av de ansvariga personerna, även med avseende på de på förhand fastställda ändringar som avses i led f.

h) de cybersäkerhetsåtgärder som vidtagits.

3. Detaljerade uppgifter om övervakning, drift och kontroll av AI-systemet, särskilt med avseende på dess kapacitet och prestandabegränsningar, inbegripet graden av riktighet för specifika personer eller grupper av personer som systemet är avsett att användas för och den övergripande förväntade riktighetsnivån i förhållande till det avsedda ändamålet, de förutsebara oavsiktliga resultaten och källorna till risker för hälsa och säkerhet, grundläggande rättigheter och diskriminering med tanke på AI-systemets avsedda ändamål, de åtgärder för mänsklig kontroll som krävs i enlighet med artikel 14, inbegripet de tekniska åtgärder som har vidtagits för att underlätta tillhandahållarnas tolkning av AI-systemens resultat, specifikationerna av indata, beroende på vad som är lämpligt.

4. En beskrivning av lämpligheten hos resultatmåtten för det specifika AI-systemet.

5. En utförlig beskrivning av riskhanteringssystemet i enlighet med artikel 9.

6. En beskrivning av relevanta ändringar av systemet som görs av leverantören under dess livscykel.

7. En förteckning över de harmoniserade standarder som helt eller delvis tillämpas och som det hänvisas till i *Europeiska unionens officiella tidning*. Om inga sådana harmoniserade standarder har tillämpats, en utförlig beskrivning av de lösningar som har valts för att uppfylla kraven i kapitel III avsnitt 2, inklusive en förteckning över andra relevanta standarder och tekniska specifikationer som har tillämpats.

8. En kopia av den EU-försäkran om överensstämmelse som avses i artikel 47.

9. En utförlig beskrivning av det system som har inrättats för att utvärdera AI-systemets prestanda efter det att systemet har släppts ut på marknaden i enlighet med artikel 72, inklusive den plan för övervakning efter utsläppande på marknaden som avses i artikel 72.3.

BILAGA V

EU-försäkran om överensstämmelse

Den EU-försäkran om överensstämmelse som avses i artikel 47 ska innehålla samtliga följande uppgifter:

1. AI-systemets namn och typ och eventuella ytterligare entydiga hänvisningar som gör det möjligt att identifiera och spåra AI-systemet.
2. Namn på och adress till leverantören eller, i förekommande fall, dennes ombud.
3. En uppgift om att den EU-försäkran om överensstämmelse som avses i artikel 47 utfärdas på leverantörens eget ansvar.
4. En uppgift om att AI-systemet överensstämmer med denna förordning och, i tillämpliga fall, med annan relevant unionsrätt som föreskriver att den EU-försäkran om överensstämmelse som avses i artikel 47 ska utfärdas.
5. Om ett AI-system inbegriper behandling av personuppgifter, en förklaring om att AI-systemet uppfyller kraven i förordningarna (EU) 2016/679 och (EU) 2018/1725 och direktiv (EU) 2016/680.
6. Hänvisningar till relevanta harmoniserade standarder som används eller till andra gemensamma specifikationer för vilka överensstämmelse deklareras.
7. I tillämpliga fall, det anmälda organets namn och identifikationsnummer, en beskrivning av det förfarande för bedömning av överensstämmelse som har genomförts och uppgifter om det utfärdade intyget.
8. Ort och datum för utfärdande av försäkran, namn på och befattning för den person som undertecknade den, uppgift om på vems vägnar personen undertecknade försäkran samt namnteckning.

BILAGA VI

Förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll

1. Med förfarande för bedömning av överensstämmelse som grundar sig på intern kontroll avses det förfarande för bedömning av överensstämmelse som grundar sig på punkterna 2, 3 och 4.
2. Leverantören ska kontrollera att det inrättade kvalitetsstyrningssystemet uppfyller kraven i artikel 17.
3. Leverantören ska granska uppgifterna i den tekniska dokumentationen för att bedöma om AI-systemet uppfyller de relevanta grundläggande kraven i kapitel III avsnitt 2.
4. Leverantören ska också kontrollera att utformnings- och utvecklingsprocessen för AI-systemet och övervakningen av detta efter utsläppande på marknaden enligt artikel 72 överensstämmer med den tekniska dokumentationen.

BILAGA VII

Bedömning av överensstämmelse grundad på en bedömning av kvalitetsstyrningssystemet och en bedömning av den tekniska dokumentationen

1. Inledning

Med överensstämmelse som grundar sig på en bedömning av kvalitetsstyrningssystem och en bedömning av den tekniska dokumentationen avses det förfarande för bedömning av överensstämmelse som grundar sig på punkterna 2–5.

2. Översikt

Det godkända kvalitetsstyrningssystemet för utformning, utveckling och testning av AI-system enligt artikel 17 ska granskas i enlighet med punkt 3 och övervakas i enlighet med punkt 5. Den tekniska dokumentationen för AI-systemet ska granskas i enlighet med punkt 4.

3. Kvalitetsstyrningssystem

3.1 Leverantörens ansökan ska innehålla

a) leverantörens namn och adress och, om ansökan lämnas in av ett ombud, även dennes namn och adress,

b) en förteckning över de AI-system som omfattas av samma kvalitetsstyrningssystem,

c) den tekniska dokumentationen för varje AI-system som omfattas av samma kvalitetsstyrningssystem,

d) dokumentationen om kvalitetsstyrningssystemet, som ska omfatta samtliga aspekter som anges i artikel 17,

e) en beskrivning av de förfaranden som har införts för att säkerställa att kvalitetsstyrningssystemet förblir lämpligt och effektivt,

f) en skriftlig försäkran om att samma ansökan inte har lämnats till något annat anmält organ.

3.2 Kvalitetsstyrningssystemet ska bedömas av det anmälda organet, som ska fastställa om det uppfyller kraven i artikel 17.

Beslutet ska meddelas leverantören eller dennes ombud.

Meddelandet ska innehålla slutsatserna från bedömningen av kvalitetsstyrningssystemet och det motiverade bedömningsbeslutet.

3.3 Det godkända kvalitetsstyrningssystemet ska fortsätta att användas och underhållas av leverantören så att det förblir lämpligt och effektivt.

3.4 Leverantören ska underrätta det anmälda organet om alla planerade ändringar av det godkända kvalitetsstyrningssystemet eller förteckningen över de AI-system som omfattas av detta.

De föreslagna ändringarna ska granskas av det anmälda organet, som ska besluta om huruvida det ändrade kvalitetsstyrningssystemet fortfarande uppfyller kraven i punkt 3.2 eller om en ny bedömning är nödvändig.

Det anmälda organet ska meddela leverantören sitt beslut. Meddelandet ska innehålla slutsatserna från granskningen av ändringarna och det motiverade bedömningsbeslutet.

4. Kontroll av den tekniska dokumentationen.

4.1 Utöver den ansökan som avses i punkt 3 ska leverantören lämna in en ansökan till ett valfritt anmält organ för bedömning av den tekniska dokumentationen för det AI-system som leverantören avser att släppa ut på marknaden eller ta i bruk och som omfattas av det kvalitetsstyrningssystem som avses i punkt 3.

4.2 Ansökan ska innehålla

a) leverantörens namn och adress,

b) en skriftlig försäkran om att samma ansökan inte har lämnats in till något annat anmält organ,

c) den tekniska dokumentation som avses i bilaga IV,

4.3 Den tekniska dokumentationen ska granskas av det anmälda organet. När så är relevant och begränsat till vad som är nödvändigt för att det anmälda organet ska kunna fullgöra sina uppgifter ska det beviljas fullständig åtkomst till de tränings-, valideringss- och testdataset som används, inbegripet, när så är lämpligt och med förbehåll för säkerhetsgarantier, genom API eller andra relevanta tekniska medel och verktyg som möjliggör fjärråtkomst.

4.4 Vid granskningen av den tekniska dokumentationen får det anmälda organet kräva att leverantören lämnar ytterligare bevis eller utför ytterligare tester för att möjliggöra en korrekt bedömning av om AI-systemet uppfyller kraven i kapitel III avsnitt 2. Om det anmälda organet inte nöjer sig med de tester som leverantören har utfört ska det anmälda organet självt direkt utföra lämpliga tester på lämpligt sätt.

4.5 Om det är nödvändigt för att bedöma om AI-systemet med hög risk uppfyller kraven i kapitel III avsnitt 2 ska det anmälda organet, efter det att alla andra rimliga sätt att kontrollera överensstämmelse har uttömts och har visat sig vara sig vara otillräckliga, och på motiverad begäran också beviljas tillgång till AI-systemets träningsmodeller och intränade modeller, inbegripet dess relevanta parametrar. Sådan åtkomst ska omfattas av befintlig unionslagstiftning om skyddet av immateriella rättigheter och företagshemligheter.

4.6 Det anmälda organets beslut ska meddelas leverantören eller dennes ombud. Anmälan ska innehålla slutsatserna från bedömningen av den tekniska dokumentationen och det motiverade bedömningsbeslutet.

Om AI-systemet uppfyller kraven i kapitel III avsnitt 2 ska ett unionsintyg om bedömning av teknisk dokumentation utfärdas av det anmälda organet. Intyget ska innehålla leverantörens namn och adress, slutsatserna från undersökningen, eventuella giltighetsvillkor och de uppgifter som krävs för att identifiera AI-systemet.

Intyget och dess bilagor ska innehålla alla relevanta uppgifter för att AI-systemets överensstämmelse ska kunna utvärderas och för att AI-systemet ska kunna kontrolleras under användning, i tillämpliga fall.

Om AI-systemet inte uppfyller kraven i kapitel III avsnitt 2 ska det anmälda organet vägra att utfärda ett unionsintyg om bedömning av teknisk dokumentation, underrätta sökanden om detta och utförligt motivera avslaget.

Om AI-systemet inte uppfyller kraven för de data som används för att träna det måste AI-systemet tränas på nytt innan ansökan om en ny bedömning av överensstämmelse lämnas in. I detta fall ska det motiverade bedömningsbeslutet från det anmälda organ som vägrar att utfärda unionsintyget om bedömning av teknisk dokumentation innehålla särskilda överväganden om de kvalitativa data som används för att träna AI-systemet, särskilt om skälen till att kraven inte uppfylls.

4.7 Varje ändring av AI-systemet som kan påverka AI-systemets överensstämmelse med kraven eller dess avsedda ändamål ska bedömas av det anmälda organ som utfärdade unionsintyget om bedömning av teknisk dokumentation. Leverantören ska underrätta det anmälda organet om sin avsikt att utföra någon av de ovannämnda ändringarna eller om den på annat sätt blir medveten om att sådana ändringar har skett. De avsedda ändringarna ska bedömas av det anmälda organet, som ska besluta om dessa ändringar kräver en ny bedömning av överensstämmelse i enlighet med artikel 43.4 eller om de kan åtgärdas genom ett tillägg till unionsintyget om bedömning av teknisk dokumentation. I det senare fallet ska det anmälda organet bedöma ändringarna, underrätta leverantören om sitt beslut och, om ändringarna godkänns, utfärda ett tillägg till unionsintyget om bedömning av teknisk dokumentation, som ska överlämnas till leverantören.

5. Övervakning av det godkända kvalitetsstyrningssystemet.

5.1 Syftet med övervakningen som utförs av det anmälda organ som avses i punkt 3 är att säkerställa att leverantören vederbörligen uppfyller villkoren för det godkända kvalitetsstyrningssystemet.

5.2 För bedömningsändamål ska leverantören ge det anmälda organet tillträde till de lokaler där utformningen, utvecklingen och testningen av AI-systemen äger rum. Leverantören ska vidarebefordra alla nödvändiga uppgifter till det anmälda organet.

5.3 Det anmälda organet ska genomföra periodiskt återkommande revisioner för att försäkra sig om att leverantören upprätthåller och tillämpar kvalitetsstyrningssystemet, samt lämna en revisionsrapport till leverantören. I samband med dessa revisioner får det anmälda organet utföra ytterligare tester av de AI-system för vilka ett unionsintyg om bedömning av teknisk dokumentation har utfärdats.

BILAGA VIII

Uppgifter som ska lämnas in i samband med registreringen av AI-system med hög risk i enlighet med artikel 49

Avsnitt A – Uppgifter som ska lämnas av leverantörer av AI-system med hög risk i enlighet med artikel 49.1

Följande uppgifter ska lämnas och därefter hållas uppdaterade för de AI-system med hög risk som ska registreras i enlighet med artikel 49.1.

1. Leverantörens namn, adress och kontaktuppgifter.

2. Om uppgifterna lämnas av en annan person för leverantörens räkning, dennes namn, adress och kontaktuppgifter.

3. Ombudets namn, adress och kontaktuppgifter, i förekommande fall.

4. AI-systemets handelsnamn och eventuella ytterligare entydiga hänvisningar som gör det möjligt att identifiera och spåra AI-systemet.

5. En beskrivning av AI-systemets avsedda ändamål och av de komponenter och funktioner som stöds av detta AI-system.

6. En grundläggande och kortfattad beskrivning av den information som används av systemet (data, indata) och dess operativa logik.

7. AI-systemets status (på marknaden, eller i bruk; finns inte längre på marknaden/i bruk, har återkallats).

8. Typ, nummer och sista giltighetsdag för det intyg som utfärdats av det anmälda organet samt det anmälda organets namn eller identifikationsnummer, i tillämpliga fall.

9. En skannad kopia av det intyg som avses i punkt 8, i tillämpliga fall.

10. Medlemsstater där AI-systemet har släppts ut på marknaden, tagits i bruk eller tillhandahållits i unionen.

11. En kopia av den EU-försäkran om överensstämmelse som avses i artikel 47.

12. Elektroniska bruksanvisningar. Dessa uppgifter får inte lämnas för AI-system med hög risk inom områdena brottsbekämpning eller migration, asyl och gränskontrollförvaltning enligt punkterna 1, 6 och 7 i bilaga III.

13. En webbadress för ytterligare information (valfritt).

Avsnitt B – Uppgifter som ska lämnas av leverantörer av AI-system med hög risk i enlighet med artikel 49.2

Följande uppgifter ska lämnas och därefter hållas uppdaterade för de AI-system som ska registreras i enlighet med artikel 49.2.

1. Leverantörens namn, adress och kontaktuppgifter.

2. Om uppgifterna lämnas av en annan person för leverantörens räkning, dennes namn, adress och kontaktuppgifter.

3. Ombudets namn, adress och kontaktuppgifter, i förekommande fall.

4. AI-systemets handelsnamn och eventuella ytterligare entydiga hänvisningar som gör det möjligt att identifiera och spåra AI-systemet.

5. En beskrivning av AI-systemets avsedda ändamål.

6. Det eller de villkor enligt artikel 6.3 som ligger till grund för bedömningen att AI-systemet anses vara utan hög risk.

7. En kort sammanfattning av de grunder på vilka AI-systemet anses vara utan hög risk vid tillämpning av förfarandet i artikel 6.3.

8. AI-systemets status (på marknaden, eller i bruk; finns inte längre på marknaden/i bruk, har återkallats).

9. Medlemsstater där AI-systemet har släppts ut på marknaden, tagits i bruk eller tillhandahållits i unionen.

Avsnitt C – Uppgifter som ska lämnas in av tillhandahållare av AI-system med hög risk i enlighet med artikel 49.3

Följande uppgifter ska lämnas och därefter hållas uppdaterade för de AI-system med hög risk som ska registreras i enlighet med artikel 49.3.

1. Tillhandahållarens namn, adress och kontaktuppgifter.
2. Namn, adress och kontaktuppgifter för den person som lämnar uppgifter på tillhandahållarens vägnar.
3. Webbadressen för införandet av AI-systemet i EU-databasen av dess leverantör.
4. En sammanfattning av resultaten av den konsekvensbedömning avseende grundläggande rättigheter som genomförts i enlighet med artikel 27.
5. En sammanfattning av den konsekvensbedömning avseende dataskydd som genomförts i enlighet med artikel 35 i förordning (EU) 2016/679 eller artikel 27 i direktiv (EU) 2016/680, såsom anges i artikel 26.8 i den här förordningen, i tillämpliga fall.

BILAGA IX

Uppgifter som ska lämnas vid registrering av AI-system med hög risk som förtecknas i bilaga III i samband med testning under verkliga förhållanden i enlighet med artikel 60

Följande uppgifter ska lämnas och därefter hållas uppdaterade när det gäller testning under verkliga förhållanden som ska registreras i enlighet med artikel 60:

1. Ett unikt unionsomfattande identifieringsnumret för testningen under verkliga förhållanden.
2. Namn och kontaktuppgifter för den leverantör eller potentiella leverantör och de tillhandahållare som deltar i testningen under verkliga förhållanden.
3. En kort beskrivning av AI-systemet, dess avsedda ändamål och annan information som krävs för att identifiera systemet.
4. En sammanfattning av de viktigaste särdragen i planen för testning under verkliga förhållanden.
5. Information om tillfälligt avbrott eller avslutande av testningen under verkliga förhållanden.

BILAGA X

Unionslagstiftningsakter om stora it-system på området med frihet, säkerhet och rättvisa

1. Schengens informationssystem

a) Europaparlamentets och rådets förordning (EU) 2018/1860 av den 28 november 2018 om användning av Schengens informationssystem för återvändande av tredjelandsmedborgare som vistas olagligt i medlemsstaterna (EUT L 312, 7.12.2018, s. 1).

b) Europaparlamentets och rådets förordning (EU) 2018/1861 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området in- och utresekontroller, om ändring av konventionen om tillämpning av Schengenavtalet och om ändring och upphävande av förordning (EG) nr 1987/2006 (EUT L 312, 7.12.2018, s. 14).

c) Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU (EUT L 312, 7.12.2018, s. 56).

2. Informationssystemet för viseringar

a) Europaparlamentets och rådets förordning (EU) 2021/1133 av den 7 juli 2021 om ändring av förordningarna (EU) nr 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 och (EU) 2019/818 vad gäller fastställandet av villkoren för åtkomst till andra EU-informationssystem för ändamål som gäller Informationssystemet för viseringar (EUT L 248, 13.7.2021, s. 1).

b) Europaparlamentets och rådets förordning (EU) 2021/1134 av den 7 juli 2021 om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EG) nr 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 och (EU) 2019/1896 och om upphävande av rådets beslut 2004/512/EG och 2008/633/RIF, i syfte att reformera Informationssystemet för viseringar (EUT L 248, 13.7.2021, s. 11).

3. Eurodac

Europaparlamentets och rådets förordning (EU) 2024/1358 av den 14 maj 2024 om inrättande av *Eurodac* för jämförelse av biometriska uppgifter för att effektivt tillämpa Europaparlamentets och rådets förordningar (EU) 2024/1315 och (EU) 2024/1350 och rådets direktiv 2001/55/EG, och identifiera tredjelandsmedborgare och statslösa personer som vistas olagligt och om framställningar från medlemsstaternas brottsbekämpande myndigheter och Europol om jämförelse med Eurodacuppgifter för brottsbekämpande ändamål, om ändring av förordningarna (EU) 2018/1240 och (EU) 2019/818 och om upphävande av Europaparlamentets och rådets förordning (EU) nr 603/2013 (EUT L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. In- och utresesystemet

Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) 1077/2011 (EUT L 327, 9.12.2017, s. 20).

5. EU-systemet för reseuppgifter och resetillstånd

a) Europaparlamentets och rådets förordning (EU) 2018/1240 av den 12 september 2018 om inrättande av ett EU-system för reseuppgifter och resetillstånd (Etias) och om ändring av förordningarna (EU) nr 1077/2011, (EU) nr 515/2014, (EU) 2016/399, (EU) 2016/1624 och (EU) 2017/2226 (EUT L 236, 19.9.2018, s. 1).

b) Europaparlamentets och rådets förordning (EU) 2018/1241 av den 12 september 2018 om ändring av förordning (EU) 2016/794 i syfte att inrätta ett EU-system för reseuppgifter och resetillstånd (Etias) (EUT L 236, 19.9.2018, s. 72).

6. Det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister avseende tredjelandsmedborgare och statslösa personer

   Europaparlamentets och rådets förordning (EU) 2019/816 av den 17 april 2019 om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN) för att komplettera det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726 (EUT L 135, 22.5.2019, s. 1).

7. Interoperabilitet

   a) Europaparlamentets och rådets förordning (EU) 2019/817 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området gränser och viseringar, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 och (EU) 2018/1861 samt rådets beslut 2004/512/EG och 2008/633/RIF (EUT L 135, 22.5.2019, s. 27).

   b) Europaparlamentets och rådets förordning (EU) 2019/818 av den 20 maj 2019 om inrättande av en ram för interoperabilitet mellan EU-informationssystem på området polissamarbete och straffrättsligt samarbete, asyl och migration och om ändring av förordningarna (EU) 2018/1726, (EU) 2018/1862 och (EU) 2019/816 (EUT L 135, 22.5.2019, s. 85).

EUT L, 12.7.2024 SV

BILAGA XI

Teknisk dokumentation som avses i artikel 53.1 a – teknisk dokumentation för leverantörer av AI-modeller för allmänna ändamål

Avsnitt 1

Information som ska tillhandahållas av samtliga leverantörer av AI-modeller för allmänna ändamål

Den tekniska dokumentation som avses i artikel 53.1 a ska minst innehålla följande information, beroende på vad som är lämpligt med avseende på modellens storlek och riskprofil:

1. En allmän beskrivning av AI-systemet för allmänna ändamål, inklusive

   a) de uppgifter som modellen är avsedd att utföra och typen och arten av AI-system i vilka den kan integreras,

   b) tillämpliga riktlinjer för godtagbar användning,

   c) datum för frisläppande och distributionsmetoder,

   d) parametrarnas struktur och antal,

   e) metod (t.ex. text, bild) och format för in- och utdata,

   f) licensen.

2. En utförlig beskrivning av delarna i den modell som avses i punkt 1 och relevant information om utvecklingsprocessen, inbegripet följande:

   a) De tekniska medel (t.ex. bruksanvisningar, infrastruktur, verktyg) som krävs för att AI-modellen för allmänna ändamål ska integreras i AI-system.

   b) Modellens och träningsprocessens designspecifikationer, inbegripet metoder och teknik för träningen, de viktigaste designvalen, inklusive motiveringen och de antaganden som gjorts, vad modellen har utformats för att optimera och de olika parametrarnas relevans, i förekommande fall.

   c) Information om de data som används för träning, testning och validering, i tillämpliga fall, inbegripet datatyp och härkomst för data och kurateringsmetoder (t.ex. rensning, filtrering osv.), antal datapunkter, deras omfattning och huvudsakliga egenskaper, hur data inhämtades och valdes ut samt alla andra åtgärder för att upptäcka datakällor och metoder för att upptäcka identifierbara biaser, i tillämpliga fall.

   d) De dataresurser som används för att träna modellen (t.ex. antal flyttalsberäkningar), träningstid och andra relevanta uppgifter som rör träningen.

   e) Känd eller uppskattad energiförbrukning för modellen.

   När det gäller led e, om modellens energiförbrukning är okänd, får uppgiften om energiförbrukningen baseras på information om de dataresurser som används.

Avsnitt 2

Ytterligare information som ska tillhandahållas av samtliga leverantörer av AI-modeller för allmänna ändamål med systemrisk

1. En utförlig beskrivning av utvärderingsstrategierna, inklusive utvärderingsresultaten, på grundval av tillgängliga offentliga utvärderingsprotokoll och utvärderingsverktyg eller annars av andra utvärderingsmetoder. Utvärderingsstrategierna ska omfatta utvärderingskriterier, mått och metoder för identifiering av begränsningar.

2. I tillämpliga fall, en utförlig beskrivning av de åtgärder som vidtagits för att genomföra intern och/eller extern antagonistisk testning (t.ex. *red teaming*), modellanpassningar, inklusive harmonisering och finjustering.

3. I tillämpliga fall en utförlig beskrivning av systemarkitekturen som förklarar hur programvarukomponenter bygger på eller påverkar varandra och integreras i den övergripande behandlingen.

BILAGA XII

Transparensinformation som avses i artikel 53.1 b – teknisk dokumentation för leverantörer av AI-modeller för allmänna ändamål till leverantörer i efterföljande led som integrerar modellen i sina AI-system

Den information som avses i artikel 53.1 b ska minst innehålla följande:

1. En allmän beskrivning av AI-systemet för allmänna ändamål, inklusive
   a) de uppgifter som modellen är avsedd att utföra och typen och arten av AI-system i vilka den kan integreras,
   b) tillämpliga riktlinjer för godtagbar användning,
   c) datum för frisläppande och distributionsmetoder,
   d) hur modellen interagerar eller kan användas för att interagera med maskinvara eller programvara som inte ingår i själva modellen, i tillämpliga fall,
   e) versionerna av relevant programvara som rör användningen av AI-modellen för allmänna ändamål, i tillämpliga fall,
   f) parametrarnas struktur och antal,
   g) metod (t.ex. text, bild) och format för in- och utdata,
   h) licensen för modellen.
2. En beskrivning av modellens komponenter och dess utvecklingsprocess, inklusive
   a) de tekniska medel (t.ex. bruksanvisningar, infrastruktur, verktyg) som krävs för att AI-modellen för allmänna ändamål ska integreras i AI-system,
   b) metod (t.ex. text, bild osv.) och format för in- och utdata och deras maximala storlek (t.ex. kontextfönstrets längd osv.),
   c) information om de data som används för träning, testning och validering, i tillämpliga fall, inbegripet datatyp, varifrån dessa data kommer och kurateringsmetoder.

BILAGA XIII

Kriterier för utseende av AI-modeller för allmänna ändamål med systemrisk som avses i artikel 51

Vid fastställandet av att en AI-modell för allmänna ändamål har kapacitet eller effekter som motsvarar dem som anges i artikel 51.1 a ska kommissionen beakta följande kriterier:

a) Antalet parametrar i modellen.

b) Datasetets kvalitet eller storlek, till exempel mätt genom token.

c) Den beräkningsmängd som används för att träna modellen, mätt i flyttalsberäkningar eller angiven med en kombination av andra variabler, såsom beräknad träningskostnad, uppskattad tid som krävs för träningen eller uppskattad energiförbrukning för träningen.

d) Modellens in- och utmatningsmetoder, såsom text till text (stora språkmodeller), text till bild, multimodalitet och tröskelvärden som motsvarar den senaste utvecklingen för att fastställa kapacitet med hög påverkansgrad för varje metod, och den specifika typen av in- och utdata (t.ex. biologiska sekvenser).

e) Riktmärken för och utvärderingar av modellens kapacitet, inbegripet med beaktande av antalet uppgifter utan ytterligare träning, anpassningsförmåga att lära sig nya, distinkta uppgifter, dess grad av autonomi och skalbarhet samt de verktyg som den har tillgång till.

f) Huruvida modellen har stor inverkan på den inre marknaden på grund av sin räckvidd, vilket ska förutsättas om den har gjorts tillgänglig för minst 10 000 registrerade företagsanvändare som är etablerade i unionen.

g) Antalet registrerade slutanvändare.

Sammanfattning av promemorian Polisens användning av AI för ansiktsigenkänning i realtid (Ds 2025:7)

I denna promemoria lämnas förslag på en ny lag som möjliggör för Polismyndigheten och Säkerhetspolisen att använda AI-system för ansiktsigenkänning och annan biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpande ändamål. Förslagen innebär att tekniken ska få användas fullt ut i den utsträckning EU:s AI-förordning medger. Tekniken ska få användas endast för vissa specifika syften och det ska krävas tillstånd att använda den, men i brådskande fall ska användning få påbörjas utan tillstånd.

Förslagen syftar till att ge Polismyndigheten och Säkerhetspolisen effektiva verktyg för att kunna söka efter personer som misstänks ha utsatts för brott, förhindra allvarliga brott och utreda, lagföra och verkställa straffrättsliga påföljder för vissa allvarliga brott, samtidigt som enskildas fri- och rättigheter beaktas.

Författningsförslagen föreslås träda i kraft den 1 januari 2026.

Promemorians lagförslag

Förslag till lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

Härigenom föreskrivs följande.

Lagens tillämpningsområde

1 § Lagen gäller för Polismyndighetens och Säkerhetspolisens användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid på allmän plats (AI-system för ansiktsigenkänning i realtid) i verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177).

Uttryck i lagen

2 § Med AI-system avses i lagen den definition som framgår av artikel 3.1 i Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens), här benämnd AI-förordningen.

Användning av AI-system för ansiktsigenkänning i realtid

3 § AI-system för ansiktsigenkänning i realtid får användas för att lokalisera eller identifiera en person

1. som kan vara offer för människorov, människohandel eller människoexploatering enligt 4 kap. 1, 1 a eller 1 b § brottsbalken eller som är försvunnen och som misstänks ha utsatts för brott,
2. om det finns en påtaglig risk för att personen kommer att begå brott mot människors liv eller säkerhet,
3. som kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det är föreskrivet fängelse i fyra år eller mer, i syfte att utreda eller lagföra brottet, eller
4. som dömts för ett sådant brott som avses i 3, i syfte att verkställa den straffrättsliga påföljden.

4 § AI-system för ansiktsigenkänning i realtid får användas endast om

– det är av synnerlig vikt att lokalisera eller identifiera en person enligt 3 §, och

– skälen för användningen uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Tillståndsprövningen hos åklagaren

5 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att förebygga, förhindra eller upptäcka brottslig verksamhet prövas av åklagare på ansökan av Polismyndigheten eller Säkerhetspolisen.

Tillståndsprövningen i domstol

6 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att utreda eller lagföra brott eller verkställa påföljd prövas av rätten på ansökan av åklagare.

7 § En ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid för att utreda eller lagföra brott prövas av den domstol som anges i 19 kap. rättegångsbalken.

8 § En ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid för att verkställa påföljd prövas av den tingsrätt som har meddelat den dom som ska verkställas. Om domen har meddelats av högre rätt prövas ansökan av den tingsrätt som dömt i målet.

Om en ansökan om tillstånd avser flera domar meddelade av skilda domstolar, får ansökan tas upp vid någon av de tingsrätter som har dömt i målet. Om det inte finns någon domstol som är behörig ska ansökan prövas av Stockholms tingsrätt.

9 § Förfarandet i domstolen är skriftligt. På förfarandet tillämpas i övrigt reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor. Det som föreskrivs om offentliga ombud i 27 kap. 28 § rättegångsbalken ska dock inte tillämpas.

Skyndsam handläggning

10 § En ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska handläggas skyndsamt.

Beslut

11 § I ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska det anges

1. vilken person som tillståndet avser,
2. för vilket syfte användningen ska ske,
3. under vilken tid och i vilket eller vilka områden tillståndet gäller, och
4. skälen för beslutet.

Tiden för tillståndet får inte bestämmas längre än vad som är nödvändigt och får inte överstiga en månad från dagen för beslutet. Området eller områdena som tillståndet avser får inte vara större än vad som är nödvändigt.

12 § Ett beslut om tillstånd gäller omedelbart.

Tillfällig användning utan tillstånd

13 § Om det är fara i dröjsmål, får Polismyndigheten eller Säkerhetspolisen påbörja användningen av AI-system för ansiktsigenkänning i realtid utan tillstånd.

14 § En ansökan om tillstånd enligt 5 eller 6 § ska göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades.

15 § Om en ansökan om tillstånd avslås ska användning av AI-system för ansiktsigenkänning i realtid som har påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas.

Omedelbart upphörande

16 § Om det inte längre finns skäl för ett tillstånd att använda AI-system för ansiktsigenkänning i realtid ska den som har ansökt om tillståndet omedelbart upphäva beslutet.

17 § Om användning av AI-system för ansiktsigenkänning i realtid har påbörjats utan tillstånd och det inte längre finns skäl för användningen ska den som är skyldig att ansöka om tillstånd i enlighet med 14 § omedelbart besluta att användningen ska upphöra.

Konsekvensbedömning

18 § AI-system för ansiktsigenkänning i realtid får användas endast om Polismyndigheten eller Säkerhetspolisen har slutfört en konsekvensbedömning avseende grundläggande rättigheter såsom föreskrivs i artikel 27.1–27.4 i AI-förordningen, men med undantag för kravet i artikel 27.3 att lämna in en sådan mall som avses i artikel 27.5.

Underrättelse till enskild

19 § Den som har varit föremål för beslut enligt denna lag som gäller en brottsutredning, lagföring eller verkställighet av påföljd ska underrättas om åtgärden. Underrättelsen ska lämnas så snart det kan ske utan men för syftet som åtgärden vidtogs för.

Om uppgifterna omfattas av sekretess enligt 15 kap. 1 eller 2 §, 18 kap. 1, 2 eller 3 § eller 35 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400) ska en underrättelse skjutas upp till dess att sekretess inte längre gäller.

En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna. En underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse eller om identiteten på den som ska underrättas är okänd. Detsamma ska gälla om den personen som underrättelsen avser har avlidit.

20 § Om det på grund av sekretess eller risk för men för syftet som åtgärden vidtogs för inte har kunnat lämnas någon underrättelse inom ett år och sex månader från det att åtgärden avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess

inte längre gäller och om det kan ske utan men för syftet som åtgärden vidtogs för.

21 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om underrättelseskyldigheten enligt denna lag.

Denna lag träder i kraft den 1 januari 2026.

Förslag till lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

Härigenom föreskrivs att 18 § och rubriken närmast före 18 § i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska ha följande lydelse.

Lydelse enligt lagförslag 2.1	*Föreslagen lydelse*
Konsekvensbedömning	**Konsekvensbedömning *och registrering i AI-databas***
	18 §
AI-system för ansiktsigenkänning i realtid får användas endast om Polismyndigheten eller Säkerhetspolisen har slutfört en konsekvensbedömning avseende grundläggande rättigheter såsom föreskrivs i artikel *27.1–27.4* i AI-förordningen, *men med undantag för kravet i artikel 27.3 att lämna in en sådan mall som avses i artikel 27.5*.	AI-system för ansiktsigenkänning i realtid får användas endast om Polismyndigheten eller Säkerhetspolisen har slutfört en konsekvensbedömning avseende grundläggande rättigheter såsom före-skrivs i artikel *27* i AI-förordningen *och har registrerat AI-systemet i EU-databasen enligt artikel 49 i förordningen*. *AI-system för ansiktsigenkänning i realtid får dock användas utan registrering i EU-databasen om det är fara i dröjsmål. I sådana fall ska en registrering ske utan onödigt dröjsmål.*

Denna lag träder i kraft den 2 augusti 2026.

Förslag till lag om ändring i lagen (1957:668) om utlämning för brott

Härigenom föreskrivs att det i lagen (1957:668) om utlämning för brott ska införas en ny paragraf, 16 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	16 a § *För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får AI-system enligt 3 § 3 och 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål användas.* *Vid användning av AI-system enligt första stycket tillämpas bestämmelserna i lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål med undantag för 7 och 8 §§.*

Denna lag träder i kraft den 1 januari 2026.

Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om lagen (2000:562) om internationell rättslig hjälp i brottmål

dels att 1 kap. 2 § och 2 kap. 1 och 2 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 4 kap. 28 i och 28 j §§, och närmast före 4 kap. 28 i § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[1]	
Rättslig hjälp enligt denna lag omfattar följande åtgärder:	
1. förhör i samband med förundersökning i brottmål,	
2. bevisupptagning vid domstol,	
3. telefonförhör,	
4. förhör genom videokonferens,	
5. kvarstad, beslag, penningbeslag samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken,	
6. föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken,	
7. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	
8. hemlig kameraövervakning,	
9. hemlig rumsavlyssning,	
10. hemlig dataavläsning,	
11. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning,	
12. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,	
13. överförande av frihetsberövade för förhör m.m., *och*	13. överförande av frihetsberövade för förhör m.m.,
14. rättsmedicinsk undersökning av en avliden person.	14. rättsmedicinsk undersökning av en avliden person, *och*
	15. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

Vad som i denna lag sägs om beslag gäller även för penningbeslag.

Lagen hindrar inte att hjälp lämnas med någon annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

[1] Senaste lydelse 2024:839.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

2 kap.

1 §[2]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10 *och* 14 ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10, 14 *och 15* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.

Rättslig hjälp som avses i 1 kap. 2 § första stycket 11–13 lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

2 §[3]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 7–10, 12 *och* 14 får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, genomsökning på distans och beslag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 7–10, 12, 14 *och 15* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, genomsökning på distans och beslag.

4 kap.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

28 i §

En ansökan om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid av någon som befinner sig i Sverige handläggs av åklagare.

[2] Senaste lydelse 2021:239.
[3] Senaste lydelse 2022:321.

Ansökan får endast avse användning av AI-system enligt 3 § 1–3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd eller, när det får ske enligt 13 § lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål, själv besluta om åtgärden.

Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

I fråga om underrättelse till en enskild enligt 19–21 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 4 kap. 25 § tredje stycket denna lag tillämpas.

28 j §

Om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska äga rum av någon som befinner sig i en annan stat och den andra staten kräver att ansökan först ska prövas av domstol i Sverige, får rätten på begäran av svensk åklagare besluta att tillåta användningen.

Underrättelse enligt 19 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska inte lämnas.

Denna lag träder i kraft den 1 januari 2026.

Förslag till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder

Härigenom föreskrivs att det i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder ska införas en ny paragraf, 4 kap. 3 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	3 a §
	För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system enligt 3 § 3 och 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål användas.
	Vid användning av AI-system enligt första stycket tillämpas bestämmelserna i lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål med undantag för 7 och 8 §§.

Denna lag träder i kraft den 1 januari 2026.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 18 kap. 1 och 19 §§ och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
1 §[1]	
Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål *eller* till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångs-medel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.	Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål, till angelägenhet som avser användning av tvångsmedel i sådant mål *eller till angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål* eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångs-medel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till

1. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde, eller

2. annan verksamhet än sådan som avses i 1 eller i första stycket som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

19 §[2]

Den tystnadsplikt som följer av 5–7, 8, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra upp-	Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra upp-

[1] Senaste lydelse 2024:328.
[2] Senaste lydelse 2024:477.

gifter, när det är fråga om upp-gift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare *eller* inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	gifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *eller uppgift om användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

35 kap.

1 §[3]

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,
3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),
4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagar-

[3] Senaste lydelse 2024:788.

myndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag, *eller*

10. utredning om självständigt förverkande.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

10. utredning om självständigt förverkande, *eller*

11. angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

Sekretessen enligt första stycket 2 *och 11* gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 januari 2026.

Förslag till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder

Härigenom föreskrivs att det i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder ska införas en ny paragraf, 3 kap. 3 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	3 a §
	För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system enligt 3 § 3 och 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål användas.
	Vid användning av AI-system enligt första stycket tillämpas bestämmelserna i lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål med undantag för 7 och 8 §§.

Denna lag träder i kraft den 1 januari 2026.

Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder

dels att 1 kap. 4 §, 2 kap. 1 och 5 §§ och 3 kap. 4 och 10 §§ ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 2 kap. 19 c och d §§ och 3 kap. 37 c §, och närmast före 2 kap. 19 c § och 3 kap. 37 c § nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
4 §[1]	
En utredningsåtgärd enligt denna lag ska avse eller motsvara	
1. förhör under förundersökning,	
2. bevisupptagning vid domstol,	
3. förhör genom ljudöverföring eller ljud- och bildöverföring,	
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, en åtgärd enligt 27 kap. 15 § eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § samma balk,	
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning,	
7. tillfälligt överförande av en frihetsberövad person,	
8. rättsmedicinsk undersökning av en avliden person,	
9. kontrollerad leverans,	
10. bistånd i en brottsutredning med användning av en skyddsidentitet,	
11. inhämtande av bevis som finns hos en myndighet, *eller*	11. inhämtande av bevis som finns hos en myndighet,
	12. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid, eller
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.	*13.* andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.
2 kap.	
1 §	
En utredningsorder får utfärdas av åklagare för en utrednings-åtgärd som avses i 1 kap. 4 § 1 och 3–*12*.	En utredningsorder får utfärdas av åklagare för en utrednings-åtgärd som avses i 1 kap. 4 § 1 och 3–*13*.

[1] Senaste lydelse 2021:241.

5 §[2]

Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser

1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,

2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning, *eller*

3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller* 17 § lagen (2020:62) om hemlig dataavläsning utfärda en utredningsorder för en åtgärd som anges i första stycket 1 *eller* 2. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning,

3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m., *eller*

4. användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken, 17 § lagen (2020:62) om hemlig dataavläsning *eller 13 § lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål* utfärda en utredningsorder för en åtgärd som anges i första stycket 1, 2 *eller 4*. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, genomsökning på distans, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket, 10 d § andra stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller det som föreskrivs i rättegångsbalken eller annan författning för den åtgärd som avses.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

19 c §

En utredningsorder för användning av AI-system för ansikts-

[2] Senaste lydelse 2023:539.

	igenkänning eller annan biometrisk fjärridentifiering i realtid i en annan medlemsstat får endast avse en åtgärd enligt 3 § 1–3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.
	19 d § *När en utredningsorder för användning av AI-system har utfärdats, ska 16 och 17 §§ lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål tillämpas.*

3 kap.

4 §

En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10 *eller* 11 får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda.	En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10, 11 *eller 12* får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda.

10 §[3]

I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller* 17 § lagen (2020:62) om hemlig dataavläsning, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken *eller* för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning.	I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken, 17 § lagen (2020:62) om hemlig dataavläsning *eller 13 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål*, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, för hemlig avlyssning av elektronisk kommunikation, hemlig övervak-

[3] Senaste lydelse 2023:539.

ning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning *eller för användning av AI-system.*

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

37 c §

I fråga om underrättelse till en enskild enligt 19–21 §§ lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 36 § andra stycket tillämpas.

Denna lag träder i kraft den 1 januari 2026.

Förslag till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket

Härigenom föreskrivs att det i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket ska införas en ny paragraf, 3 kap. 6 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	6 a §
	För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system enligt 3 § 3 och 4 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål användas.
	Vid användning av AI-system enligt första stycket tillämpas bestämmelserna i lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål med undantag för 7 och 8 §§.

Denna lag träder i kraft den 1 januari 2026.

Förteckning över remissinstanserna

Efter remiss har yttranden över promemorian Polisens användning av AI för ansiktsigenkänning i realtid (Ds 2025:7) kommit in från Barnombudsmannen, Brottsförebyggande rådet, Centrum för rättvisa, Civil Rights Defenders, Diskrimineringsombudsmannen, Domstolsverket, Ekobrottsmyndigheten, Eskilstuna tingsrätt, Förvaltningsrätten i Härnösand, Förvaltningsrätten i Jönköping, Försvarsmakten, Hovrätten över Skåne och Blekinge, Institutet för mänskliga rättigheter, Integritetsskyddsmyndigheten, Journalistförbundet, Justitiekanslern, Kammarrätten i Göteborg, Kriminalvården, Kustbevakningen, Lunds universitet, Malmö tingsrätt, Migrationsverket, Myndigheten för digital förvaltning, Polisförbundet, Polismyndigheten, Post- och telestyrelsen, Region Stockholm, Riksdagens ombudsmän, Skatteverket, Statens institutionsstyrelse, Stockholms tingsrätt, Svea hovrätt, Sveriges advokatsamfund, Sveriges domareförbund, Sveriges Kommuner och Regioner, Swedac, Myndigheten för säkerhet och integritetsskydd, Säkerhetspolisen, Tidningsutgivarna, Trafikverket, Tullverket, Umeå universitet, Utredningen om AI-förordningen (Fi 2024:05) och Åklagarmyndigheten.

Regelrådet, Region Jämtland Härjedalen och Region Norrbotten har avstått från att lämna synpunkter på förslagen i promemorian.

Förvaltningsrätten i Härnösand, Region Kronoberg och Rädda barnen har inte svarat på remissen.

Lagrådsremissens lagförslag

Förslag till lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

Härigenom föreskrivs följande.

Lagens tillämpningsområde

1 § Lagen gäller för Polismyndighetens och Säkerhetspolisens användning av system för artificiell intelligens för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid på allmän plats (AI-system för ansiktsigenkänning i realtid) i verksamhet för vilken personuppgiftsbehandlingen omfattas av brottsdatalagen (2018:1177).

Inför användning av ett AI-system

2 § Med AI-system för ansiktsigenkänning i realtid avses i lagen sådana AI-system som omfattas av artikel 3.42 i Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens), här benämnd AI-förordningen.

3 § För att ett AI-system för ansiktsigenkänning i realtid ska få användas enligt denna lag ska Polismyndigheten eller Säkerhetspolisen först ha gjort en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen.

Användning av AI-system

4 § AI-system för ansiktsigenkänning i realtid får användas om det är absolut nödvändigt för att lokalisera eller identifiera en viss person

1. som kan vara offer för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken, människoexploatering enligt 4 kap. 1 b § brottsbalken om exploateringen avser sexuella tjänster, eller som är försvunnen och som misstänks ha utsatts för brott,
2. om det finns en överhängande fara för att personen kommer att begå ett allvarligt brott mot människors liv eller säkerhet,
3. som skäligen kan misstänkas ha begått ett sådant brott som avses i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott, i syfte att utreda eller lagföra brottet, eller
4. som dömts för ett sådant brott som avses i 3, i syfte att verkställa den straffrättsliga påföljden.

5 § AI-system för ansiktsigenkänning i realtid får användas endast om skälen för användningen uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Tillståndsprövningen hos åklagare

6 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd prövas av åklagare på ansökan av Polismyndigheten eller Säkerhetspolisen.

Tillståndsprövningen i domstol

7 § Ett tillstånd att använda AI-system för ansiktsigenkänning i realtid för att utreda eller lagföra brott prövas av rätten på ansökan av åklagare.

8 § En ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid för att utreda eller lagföra brott prövas av den domstol som anges i 19 kap. rättegångsbalken.

9 § Förfarandet i domstolen är skriftligt.

På förfarandet tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i denna lag. Det som föreskrivs om offentliga ombud i 27 kap. 28 § rättegångsbalken ska dock inte tillämpas.

Skyndsam handläggning

10 § En ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid ska prövas skyndsamt.

Beslut

11 § I ett beslut att tillåta användning av AI-system för ansiktsigenkänning i realtid ska det anges

1. vilken person som tillståndet avser,
2. för vilket syfte användningen ska ske,
3. under vilken tid och i vilket eller vilka områden tillståndet gäller, och
4. skälen för beslutet.

Tiden för tillståndet får inte bestämmas längre än vad som är absolut nödvändigt och får inte överstiga en månad från dagen för beslutet. Området eller områdena som tillståndet avser får inte vara större än vad som är absolut nödvändigt.

12 § Ett beslut om tillstånd att använda AI-system för ansiktsigenkänning i realtid får verkställas omedelbart.

Omedelbart upphörande

13 § Om det inte längre finns skäl för ett tillstånd att använda AI-system för ansiktsigenkänning i realtid ska åklagare omedelbart upphäva beslutet. Polismyndigheten eller Säkerhetspolisen ska omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

Tillfällig användning utan tillstånd

14 § Om det är fara i dröjsmål, får Polismyndigheten eller Säkerhetspolisen påbörja användning av AI-system för ansiktsigenkänning i realtid utan tillstånd.

Den myndighet som har påbörjat användning enligt första stycket ska dokumentera den samt skälen för att användningen påbörjades utan tillstånd.

15 § Om användning har påbörjats utan tillstånd ska en ansökan om tillstånd enligt 6 eller 7 § göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades.

Om användning har påbörjats utan tillstånd och det inte längre finns skäl för användningen ska den som är skyldig att ansöka om tillstånd i enlighet med 6 eller 7 § omedelbart besluta att användningen ska upphöra.

16 § Om en ansökan om tillstånd avslås ska användning som har påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas.

Underrättelse till enskild

17 § Den som har identifierats eller lokaliserats genom en åtgärd enligt denna lag som gäller en brottsutredning eller lagföring ska underrättas om åtgärden. Underrättelsen ska lämnas så snart det kan ske utan men för det syfte som åtgärden vidtogs för.

Om uppgifterna omfattas av sekretess enligt 15 kap. 1 eller 2 §, 18 kap. 1, 2 eller 3 § eller 35 kap. 1 eller 2 § offentlighets- och sekretesslagen (2009:400) ska en underrättelse skjutas upp till dess att sekretess inte längre gäller.

En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna. En underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse eller om identiteten på den som ska underrättas är okänd. Detsamma ska gälla om den personen som underrättelsen avser har avlidit.

18 § Om det på grund av sekretess eller risk för men för syftet som åtgärden vidtogs för inte har kunnat lämnas någon underrättelse inom ett år och sex månader från det att åtgärden avslutades, ska frågan om underrättelse prövas slutligt. En underrättelse ska då bara lämnas om sekretess inte längre gäller och om det kan ske utan men för syftet som åtgärden vidtogs för.

Denna lag träder i kraft den 1 maj 2026.

Förslag till lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

Härigenom föreskrivs att 3 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska ha följande lydelse.

Lydelse enligt lagförslag 2.1	*Föreslagen lydelse*
3 §	
För att ett AI-system för ansiktsigenkänning i realtid ska få användas enligt denna lag ska Polismyndigheten eller Säkerhetspolisen först ha gjort en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen.	För att ett AI-system för ansiktsigenkänning i realtid ska få användas enligt denna lag ska Polismyndigheten eller Säkerhetspolisen först ha gjort en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen *och registrerat systemet enligt artikel 49 i förordningen. Ett sådant system får dock användas utan registrering om användningen inte kan avvakta. I sådana fall ska en registrering ske så snart det är möjligt.*

Denna lag träder i kraft den dag som regeringen bestämmer.

Förslag till lag om ändring i lagen (1957:668) om utlämning för brott

Härigenom föreskrivs att det i lagen (1957:668) om utlämning för brott ska införas en ny paragraf, 16 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	16 a § *För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 8 §.*

Denna lag träder i kraft den 1 maj 2026.

Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

Härigenom föreskrivs i fråga om lagen (2000:562) om internationell rättslig hjälp i brottmål

dels att 1 kap. 2 § och 2 kap. 1 och 2 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 4 kap. 28 i och 28 j §§, och närmast före 4 kap. 28 i § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[18]	
Rättslig hjälp enligt denna lag omfattar följande åtgärder:	
1. förhör i samband med förundersökning i brottmål,	
2. bevisupptagning vid domstol,	
3. telefonförhör,	
4. förhör genom videokonferens,	
5. kvarstad, beslag, penningbeslag samt husrannsakan och andra åtgärder som avses i 28 kap. rättegångsbalken,	
6. föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § rättegångsbalken,	
7. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,	
8. hemlig kameraövervakning,	
9. hemlig rumsavlyssning,	
10. hemlig dataavläsning,	
11. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning,	
12. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,	
13. överförande av frihetsberövade för förhör m.m., *och*	13. överförande av frihetsberövade för förhör m.m.,
14. rättsmedicinsk undersökning av en avliden person.	14. rättsmedicinsk undersökning av en avliden person, *och*
	15. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

Vad som i denna lag sägs om beslag gäller även för penningbeslag.

Lagen hindrar inte att hjälp lämnas med någon annan åtgärd än sådan som anges i första stycket om det kan ske utan tvångsmedel eller annan tvångsåtgärd.

[18] Senaste lydelse 2024:839.

I fråga om överlämnande, utlämning och delgivning finns särskilda bestämmelser. Det finns också särskilda bestämmelser om rättslig hjälp i brottmål åt vissa internationella organ.

2 kap.

1 §[19]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10 *och* 14 ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10, 14 *och 15* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.

Rättslig hjälp som avses i 1 kap. 2 § första stycket 11–13 lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

2 §[20]

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 7–10, 12 *och* 14 får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, genomsökning på distans och beslag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 7–10, 12, 14 *och 15* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan, genomsökning på distans och beslag.

4 kap.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

28 i §

En ansökan om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid som avser någon som befinner sig i Sverige handläggs av

[19] Senaste lydelse 2021:239.
[20] Senaste lydelse 2022:321.

åklagare. Ansökan får endast avse användning enligt 4 § 1–3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd. Om det är fara i dröjsmål får användningen påbörjas utan tillstånd enligt 14 § lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. I sådana fall ska en ansökan om tillstånd göras enligt 15 § samma lag.

Om användningen påbörjas utan tillstånd ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid.

I fråga om underrättelse till en enskild enligt 17 och 18 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 4 kap. 25 § tredje stycket denna lag tillämpas.

28 j §

Om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid ska avse någon som befinner sig i en annan stat och den andra staten kräver att ansökan först ska prövas av domstol i Sverige, får rätten på begäran av svensk åklagare besluta att tillåta användningen.

Underrättelse enligt 17 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska inte lämnas.

Denna lag träder i kraft den 1 maj 2026.

Förslag till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder

Härigenom föreskrivs att det i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder ska införas en ny paragraf, 4 kap. 3 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	3 a §
	För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 8 §.

Denna lag träder i kraft den 1 maj 2026.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 18 kap. 1 och 19 §§ och 35 kap. 1 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
1 §[1]	
Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.	Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. *Detsamma gäller för uppgift som hänför sig till angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Sekretess gäller, under motsvarande förutsättningar som anges i första stycket, för uppgift som hänför sig till

1. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde, eller

2. annan verksamhet än sådan som avses i 1 eller i första stycket som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

19 §[2]

Den tystnadsplikt som följer av 5–7, 8, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

[1] Senaste lydelse 2024:328.
[2] Senaste lydelse 2024:477.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra upp-gifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare *eller* inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra upp-gifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare, inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *eller uppgift om användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.*

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

35 kap.

1 §[3]

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller i ärende enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,

[3] Senaste lydelse 2024:788.

3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),

4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag, *eller*

10. utredning om självständigt förverkande.

Sekretessen enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

10. utredning om självständigt förverkande, *eller*

11. angelägenhet som avser användning av AI-system enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

Sekretessen enligt första stycket 2 *och 11* gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs. Vid förhandling om användning av tvångsmedel gäller sekretess för uppgift om vem som är misstänkt endast om det kan antas att fara uppkommer för att den misstänkte eller någon närstående till honom eller henne utsätts för våld eller lider annat allvarligt men om uppgiften röjs.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 maj 2026.

Förslag till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder

Härigenom föreskrivs att det i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder ska införas en ny paragraf, 3 kap. 3 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	3 a §
	För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid användas i syfte att verkställa frihetsberövandet. Användningen får ske enligt 4 § 3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Vid sådan användning tillämpas bestämmelserna i den lagen med undantag för 8 §.

Denna lag träder i kraft den 1 maj 2026.

Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder

dels att 1 kap. 4 §, 2 kap. 1 och 5 §§ och 3 kap. 4 § ska ha följande lydelse,

dels att det ska införas tre nya paragrafer, 2 kap. 19 c och 19 d §§ och 3 kap. 37 c §, och närmast före 2 kap. 19 c § och 3 kap. 37 c § nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
4 § [1]	
En utredningsåtgärd enligt denna lag ska avse eller motsvara	
1. förhör under förundersökning,	
2. bevisupptagning vid domstol,	
3. förhör genom ljudöverföring eller ljud- och bildöverföring,	
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, en åtgärd enligt 27 kap. 15 § eller ett föreläggande att bevara en viss lagrad uppgift enligt 27 kap. 16 § samma balk,	
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning,	
7. tillfälligt överförande av en frihetsberövad person,	
8. rättsmedicinsk undersökning av en avliden person,	
9. kontrollerad leverans,	
10. bistånd i en brottsutredning med användning av en skyddsidentitet,	
11. inhämtande av bevis som finns hos en myndighet, *eller*	11. inhämtande av bevis som finns hos en myndighet,
	12. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid, eller
12. andra åtgärder som inte innebär användning av tvångs-medel eller någon annan tvångsåtgärd.	*13.* andra åtgärder som inte innebär användning av tvångs-medel eller någon annan tvångsåtgärd.
2 kap.	
1 §	
En utredningsorder får utfärdas av åklagare för en utredningsåtgärd som avses i 1 kap. 4 § 1 och 3–*12*.	En utredningsorder får utfärdas av åklagare för en utredningsåtgärd som avses i 1 kap. 4 § 1 och 3–*13*.

[1] Senaste lydelse 2021:241.

5 §[2]

Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser

1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,

2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning, *eller*

3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.

2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning,

3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m., *eller*

4. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid enligt lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken eller 17 § lagen (2020:62) om hemlig dataavläsning utfärda en utredningsorder för en åtgärd som anges i första stycket 1 eller 2. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, genomsökning på distans, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket, 10 d § andra stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller det som föreskrivs i rättegångsbalken eller annan författning för den åtgärd som avses.

Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid

19 c §

En utredningsorder för användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid i en annan medlemsstat får endast avse en åtgärd enligt 4 § 1–3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i

[2] Senaste lydelse 2023:539.

	realtid för brottsbekämpande ändamål.
	19 d § *När en utredningsorder för användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid har utfärdats, ska 13 § lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål tillämpas.*
3 kap.	
4 §	
En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10 *eller* 11 får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda.	En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10, 11 *eller 12* får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda.
	Användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid
	37 c § *I fråga om underrättelse till en enskild enligt 17 och 18 §§ lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska bestämmelserna i 36 § andra stycket tillämpas.*

Denna lag träder i kraft den 1 maj 2026.

Förslag till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket

Härigenom föreskrivs att det i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket ska införas en ny paragraf, 3 kap. 6 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 kap.
	6 a §
	I frågor om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid tillämpas bestämmelserna i 4 kap. 3 a § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.

Denna lag träder i kraft den 1 maj 2026.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2025-12-18

Närvarande: F.d. justitieråden Sten Andersson och Kristina Svahn Starrsjö samt justitierådet Jonas Malmberg

Polisens användning av AI för ansiktsigenkänning i realtid

Enligt en lagrådsremiss den 27 november 2025 har regeringen (Justitiedepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål,
2. lag om ändring i lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål,
3. lag om ändring i lagen (1957:668) om utlämning för brott,
4. lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål,
5. lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder,
6. lag om ändring i offentlighets- och sekretesslagen (2009:400),
7. lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder,
8. lag om ändring i lagen (2017:1000) om en europeisk utredningsorder,
9. lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket.

Förslagen har inför Lagrådet föredragits av kanslirådet Ann-Sofie Winqvist.

Förslagen föranleder följande yttrande.

Allmänt

AI-förordningen, regeringsformen och Europakonventionen

Utgångspunkten i den s.k. AI-förordningen[26] är att användningen av system för biometrisk fjärridentifiering i realtid av fysiska personer på allmänt tillgängliga platser för brottsbekämpande ändamål ska vara förbjuden. Som skäl för detta anges bland annat att en sådan användning särskilt inkräktar på de berörda personernas rättigheter och friheter. Användningen kan påverka privatlivet för en stor del av befolkningen, kan skapa en känsla av konstant övervakning och indirekt avskräcka från utövande av mötesfrihet och andra grundläggande rättigheter. Det betonas

[26] Europaparlamentets och rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens och om ändring av förordningarna (EG) nr 300/2008, (EU) nr 167/2013, (EU) nr 168/2013, (EU) 2018/858, (EU) 2018/1139 och (EU) 2019/2144 samt direktiven 2014/90/EU, (EU) 2016/797 och (EU) 2020/1828 (förordning om artificiell intelligens).

att det förhållandet att kontrollerna sker i realtid innebär att effekterna av dem är omedelbara och att det finns begränsade möjligheter till ytterligare kontroll eller korrigering. Det lyfts också fram att tekniska brister i AI-system kan leda till snedvridning av resultat och medföra diskriminerande effekter. (Se skäl 32).

Trots att utgångspunkten i AI-förordningen alltså är att användning av AI-system för ansiktsigenkänning är förbjuden får en medlemsstat besluta att i sin nationella rätt föreskriva möjlighet att helt eller delvis tillåta användning av AI-system för ansiktsigenkänning i realtid på allmänt tillgängliga platser om användningen är absolut nödvändig för vissa uppräknade syften.

Enligt regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Riksdagen kan begränsa denna rätt genom lag, men bara för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och får inte sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen (se 2 kap. 6 andra stycket, 20 och 21 §§ regeringsformen). En följd av regleringen är att lagstiftaren noga bör ange sina skäl för att göra en rättighetsbegränsning, så att riksdagsledamöter, domstolar och myndigheter kan bedöma att begränsningen är motiverad (jfr t.ex. Thomas Bull & Fredrik Sterzel, Regeringsformen – en kommentar, Juno 2023, s. 98 f.).

Enligt artikel 8 i Europakonventionen har var och en rätt till respekt för bland annat sitt privat- och familjeliv. Denna rätt omfattar även skydd mot övervakning i olika former. Det allmänna får inte inskränka rättigheten annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt bland annat för att förebygga brott eller till skydd för andra personers fri- och rättigheter. När det gäller övervakning genom system för ansiktsigenkänning i realtid har Europadomstolen framhållit att det är väsentligt att det finns detaljerade regler som styr hur systemen får användas och att reglerna ger ett starkt skydd mot risken för missbruk och godtycklighet (se Glukhin mot Ryssland, mål nr 11519/20, dom den 4 juli 2023 p. 74 och 82).

Det angivna syftet med lagförslaget

I lagrådsremissen föreslås att det ska införas en ny lag som reglerar under vilka förutsättningar polisen i sin brottsbekämpande verksamhet – efter tillstånd av åklagare eller domstol – ska få använda AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid. Som skäl anges att allvarlig våldsbrottslighet, framför allt genom skjutningar och sprängningar inom den kriminella miljön, är ett svårt samhällsproblem och att polisen måste ha tillgång till effektiva och ändamålsenliga verktyg i sitt brottsbekämpande arbete för att kunna vända brottsutvecklingen.

Frågan om det ska införas ett AI-system för ansiktsigenkänning är i första hand rättspolitisk och Lagrådet invänder inte mot att ett sådant system föreslås. Samtidigt konstaterar Lagrådet att förslaget inte är begränsat till att vara ett verktyg enbart för att bekämpa allvarlig våldsbrottslighet i kriminella miljöer utan att det ger polisen förhållandevis

stora möjligheter att använda sig av system för ansiktsigenkänning även i andra sammanhang. Lagrådet återkommer till den frågan.

Behovet av en restriktiv tillämpning

Lagförslaget anger ett antal förutsättningar för att tekniken ska få användas. Dessa är delvis ganska vida. Tekniken ska kunna användas på allmänna platser, det vill säga överallt där allmänheten typiskt sett vistas. Som ytterligare förutsättningar gäller bland annat att tekniken får användas om det är absolut nödvändigt för att lokalisera eller identifiera en viss person om det finns en överhängande fara för att personen kommer att begå ett allvarligt brott mot människors liv eller säkerhet (se 4 § 2). I författningskommentaren anges att en utgångspunkt för bedömningen av om det är fråga om ett allvarligt brott är att det rör sig om ett konkret brott med ett straffvärde motsvarande fängelse i minst sex månader (se vidare under 4 §). Lagrådet konstaterar att många brott kan ha ett straffvärde på minst sex månader och att ribban för att polisen ska få använda sig av ansiktsigenkänning, i vart fall enligt den nu nämnda bestämmelsen, därmed inte är särskilt hög.

Sammantaget innebär detta att ett stort och obestämt antal personer förhållandevis ofta kan komma att bli föremål för tekniken med ansiktsigenkänning. Även om merparten av dessa personer inte kommer att vara eftersökta och systemet därmed inte ger någon ”träff”, väcker förslaget grundläggande frågor om vilka intrång i den personliga integriteten som den enskilde, i brottsbekämpningens intresse, ska behöva tåla och vilka medel för övervakning som staten bör ha tillgång till. I ljuset av regeringsformens och Europakonventionens bestämmelser om skydd mot övervakning och risken för att tekniken i framtiden kan komma att användas för andra ändamål än de som nu föreslås finns det enligt Lagrådets mening anledning att anlägga ett mer restriktivt perspektiv än vad förslaget ger uttryck för. Lagrådet vill här också framhålla att utgångspunkten i AI-förordningen är att användning av AI-system för ansiktsigenkänning i realtid är förbjuden och att de bestämmelser i förordningen som ändå gör det möjligt för medlemsstaterna att införa sådana system, ska tolkas restriktivt.

Beslutsordningen

Ytterligare en aspekt på lagrådsremissen avser den beslutsordning som föreslås. Enligt remissen ska en ansökan om tillstånd att använda AI-system för ansiktsigenkänning i realtid i vissa fall prövas av åklagare och i andra fall av domstol. Åklagare ska, som Lagrådet har uppfattat förslaget, pröva de fall som avser tillstånd att använda tekniken för att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd medan domstol ska pröva de fall som avser tillstånd att utreda och lagföra brott.

Det är alltså många fall som kommer att prövas av åklagare och sådana beslut kommer inte att kunna överklagas till domstol. I de fall en domstol ska besluta om tillstånd kommer ett beslut att bifalla en ansökan i praktiken inte att kunna överklagas av den som övervakningen berör. Den som tillståndet rör ska inte underrättas om beslutet förrän han eller hon har identifierats (se 17 §). Ett överklagande kan därmed ske först efter det att

åtgärden är helt verkställd och kommer då normalt inte prövas eftersom den anses överspelad (”desert”).

En person som anser sig vara utsatt för en felaktig, oproportionerlig eller annars rättsstridig övervakning har därmed inte någon faktisk möjlighet att ta tillvara sina rättigheter. Möjligheterna att genom rättspraxis få klarlagt var gränserna för vad som är tillåtet i dessa fall går, är följaktligen också begränsade.

I lagrådsremissen anges som skäl för att beslut om användning av AI-teknik för ansiktsigenkänning inte alltid ska gå att överklaga är att användningen omgärdas av rättssäkerhetsgarantier, bland annat tillståndsprövningen, och att tillsynsmyndigheten ges goda förutsättningar att utöva en effektiv och kvalificerad tillsyn.

Som Lagrådet återkommer till har möjligheten att ge tillstånd till användning av AI-teknik för ansiktsigenkänning i realtid getts ett vitt tillämpningsområde, där de närmare förutsättningarna för att tillstånd får meddelas lämnar ett betydande tolkningsutrymme åt den som ska tillämpa bestämmelserna. Lagens utformning gör det svårt för tillsynsmyndigheten att upptäcka och ingripa mot en alltför vidsträckt tillämpning av regleringen.

Även om det finns rättssäkerhetsskäl som talar emot den föreslagna ordningen är dessa inte tillräckliga för att Lagrådet ska avstyrka förslaget. Bristerna i detta avseende understryker dock att det för att motverka ett överutnyttjande av AI-teknik för ansiktsigenkänning, finns ett stort behov av tydlighet och precision i de materiella förutsättningarna för att använda tekniken.

Förslaget till lag om lag om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål

3 §

I paragrafen uppställs ett krav på att Polismyndigheten och Säkerhetspolisen gör en konsekvensbedömning innan den börjar använda ett AI-system för ansiktsigenkänning. Såsom paragrafen är utformad synes den innebära att den ena av myndigheterna inte behöver göra någon egen konsekvensbedömning om en sådan redan har gjorts av den andra myndigheten. Detta torde inte vara avsikten. Lagrådet föreslår därför att paragrafen ges följande lydelse.

Polismyndigheten och Säkerhetspolisen får inte ta ett AI-system för ansiktsigenkänning enligt denna lag i bruk, förrän myndigheten har gjort en konsekvensbedömning av systemet avseende grundläggande rättigheter enligt artikel 27 i AI-förordningen.

4 §

Paragrafen reglerar när AI-system för ansiktsigenkänning i realtid får användas. Paragrafen innebär att tekniken bara får användas om det är absolut nödvändigt för att lokalisera eller identifiera en viss person och bara i de situationer som beskrivs i punkterna 1–4.

Begreppet absolut nödvändigt är hämtat från artikel 5.1 h i AI-förordningen och från artikel 10 i EU:s dataskyddsdirektiv[27] (jfr skäl 94 till AI-förordningen) och kan inte ges en vidare innebörd än det har enligt dessa rättsakter. Som framhålls i förarbetena till brottsdatalagen (2018:1177), som genomför det nyss nämnda direktivet, ska uttrycket ”absolut nödvändigt” tolkas restriktivt och behovet av åtgärden måste prövas noga i det enskilda fallet (se prop. 2017/18:232 s. 447). Det kan enligt Lagrådets mening ifrågasättas om den beskrivning av begreppet ”absolut nödvändigt” som ges i författningskommentaren är förenlig med den restriktivitet som begreppet måste antas ha enligt AI-förordningen och dataskyddsdirektivet.

Punkt 1 avser möjligheten att lokalisera eller identifiera en person som kan vara offer för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken eller människoexploatering enligt 4 kap. 1 b § brottsbalken om exploateringen avser sexuella tjänster. Punkten omfattar även personer som är försvunna och som misstänks ha utsatts för brott. I lagtexten anges inte vilket syfte som användningen av tekniken enligt denna punkt ska ha.

Punkten motsvarar artikel 5.1 h i) i AI-förordningen som avser målinriktad sökning efter specifika offer för bland annat människorov. Det ligger närmast till hands att uppfatta att bestämmelsen i förordningen syftar till att göra det möjligt att hitta personer som utsätts för brott för att kunna avvärja och stoppa pågående brott. Det är tveksamt om bestämmelsen omfattar att söka efter personer som – i ett tidigare skede – har utsatts för brott i syfte att kunna lagföra dem som gjort sig skyldiga till brottet. Användning av AI-system för ansiktsigenkänning i realtid för att lagföra brott behandlas i stället i punkten iii) och omfattar där misstänkta gärningsmän, men inte målsäganden eller vittnen. Det är alltså tveksamt om bestämmelsen i AI-förordningen tillåter att sådana AI-system används för att söka efter någon som håller sig undan efter att (tidigare) ha utsatts för t.ex. människoexploatering.

Mot bakgrund härav bör lagtexten ändras så att det framgår att den omfattar enbart den som är föremål för ett pågående brott. Även författningskommentaren – där det på flera ställen talas om personer som har utsatts för brott – behöver justeras.

Punkt 2 gäller situationer då det finns en överhängande fara för att den eftersökta personen kommer att begå ett allvarligt brott mot människors liv eller säkerhet.

Punkten motsvarar artikel 5.1 h ii) första ledet i AI-förordningen. I den bestämmelsen talas dock inte om ”säkerhet”, utan om ”fysisk säkerhet” (physical safety, die körperliche Unversehrtheit respektive la sécurité physique).

Den föreslagna lagtexten ger alltså ett vidare tillämpningsområde för användningen av AI-system för ansiktsigenkänning i realtid än vad som är

[27] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF

tillåtet enligt den aktuella bestämmelsen i AI-förordningen. Lagtexten bör anpassas till AI-förordningen.

Bestämmelsen i AI-förordningen avser användning av de aktuella AI-systemen i syfte att förhindra hot mot fysiska personers liv eller fysiska säkerhet. Det avgörande för att bestämmelsen ska vara tillämplig är att det finns ett specifikt, betydande och överhängande sådant hot. Det är alltså inte tillräckligt att det finns en risk att en person begår en gärning som omfattas av en brottstyp som kan innefatta angrepp på annans liv och säkerhet.

Vissa av de brottstyper som nämns i författningskommentaren kan innefatta gärningar som inte innebär angrepp på annans liv och (fysiska) säkerhet. Olaga tvång, människohandel, utpressning, mordbrand och allmänfarlig ödeläggelse kan begås utan angrepp på annans liv och fysiska säkerhet.

För att bestämmelsen ska vara förenlig med AI-förordningen måste det tydliggöras att lagbestämmelsen är tillämplig enbart om det i det konkreta fallet finns ett specifikt, betydande och överhängande hot mot annans liv eller fysiska säkerhet. Med ett sådant klargörande är det inte nödvändigt att begränsa bestämmelsen till att omfatta vissa brottstyper.

I lagtexten talas om ”människors” (genitiv plural) liv eller säkerhet, vilket kan läsas som att det krävs att flera personers liv eller säkerhet ska vara i fara. Det torde inte vara avsikten, vilket bör framgå av bestämmelsen.

Punkt 3 avser personer som skäligen kan misstänkas ha begått brott som räknas upp i bilaga II till AI-förordningen och för vilket det i straffskalan ingår fängelse i fyra år eller mer eller sådant straff kan följa för försök, förberedelse eller stämpling till sådana brott. Syftet med åtgärden ska vara att utreda eller lagföra brottet.

AI-tekniken får alltså användas för brott som avses i bilaga II till AI-förordningen. Brott som upptas i den bilagan är bl.a. mord, grov misshandel, människohandel, våldtäkt, olaglig handel med narkotika samt olaglig handel med vapen och sprängämnen. De brott som nämns i bilagan har formulerats utifrån en europeisk kontext och motsvarar inte alltid utformningen av svenska straffstadganden. Enligt lagrådsremissen får det därför vid tillämpningen av lagen göras en bedömning av om de brott som anges i bilagan har en motsvarighet i svensk rätt och vilka brott det i så fall handlar om.

Det är inte en alldeles enkel uppgift att göra den bedömningen. Man kan t.ex. fråga sig om uttrycket våldtäkt (rape, Vergewaltigung och viol) bara omfattar våldtäkt (inklusive mindre grov sådan) eller även oaktsam våldtäkt och våldtäkt mot barn.

I lagrådsremissen görs alltså en hänvisning till bilagans uppräkning, i stället för en precisering av de svenska brott eller brottstyper som ska omfattas. Som skäl för detta anges att det i flera fall är svårt att göra en direkt översättning till svenska brott och det är en utmaning att säkerställa att alla svenska brott som kan omfattas också gör det, samtidigt som det är angeläget att en svensk brottskatalog inte går utöver vad AI-förordningen tillåter. Det framhålls också som en fördel att regleringen inte behöver ändras om det i den svenska lagstiftningen skulle införas nya brott med fyra års fängelse i straffskalan eller om straffskalan för vissa brott höjs.

Den valda tekniken innebär att lagstiftaren överlämnar till rättstillämpningen att i enskilda fall bedöma vilka svenska brott som kan tänkas rymmas inom bilagans förteckning. Som redan nämnts finns det i praktiken begränsade möjligheter att genom rättspraxis klarlägga bestämmelsens närmare innebörd.

Enligt Lagrådets mening framstår mot denna bakgrund hänvisningen till bilaga II i AI-förordningen som mindre väl förenlig med regeringsformens föreskrifter om att betydande intrång i den personliga integriteten ska beslutas av riksdagen i form av lag (se 2 kap. 6 § andra stycket och 20 § regeringsformen).

Det kan också noteras att lagförslagets hänvisning till AI-förordningen är avsedd att vara dynamisk. Den avser alltså förordningen i den vid varje tidpunkt gällande lydelsen. Om förordningen ändras så att medlemsstaterna får ett vidgat utrymme att använda AI-system för ansiktsigenkänning i realtid, kommer därmed åklagare och domstolar att kunna besluta om användning av ansiktsigenkänning i ytterligare fall, utan att riksdagen först har bedömt om det är befogat. Även detta framstår enligt Lagrådet som mindre väl förenligt med regeringsformen.

Utöver att det brott som misstanken avser ska finnas med på listan i förordningens bilaga gäller att det i straffskalan för brottet ska ingå fängelse i fyra år eller mer. Däremot ställs inget krav på att den aktuella gärningen ska ha ett särskilt högt straffvärde. Detta kan illustreras med vad som gäller för vapenbrott. Vapenbrott har en straffskala på upp till fem års fängelse och omfattas därmed av bestämmelsen. I det enskilda fallet kan emellertid ett misstänkt vapenbrott ha ett straffvärde på enbart några månaders fängelse.

Som Lagrådet redan har varit inne på har möjligheten att använda AI-system för ansiktsigenkänning i lagförslaget fått en utformning som går avsevärt längre än vad som är nödvändigt för att uppnå den angivna målsättningen att motverka allvarlig våldsbrottslighet, framför allt genom skjutningar och sprängningar inom den kriminella miljön. Lagförslaget innebär således ett betydligt större ingrepp i den rätt som skyddas i 2 kap. 6 § andra stycket regeringsformen samt artikel 8 i Europakonventionen än som är motiverat av det angivna ändamålet. I det fortsatta lagstiftningsarbetet bör enligt Lagrådets mening tydligt motiveras varför det är nödvändigt att tillåta system för ansiktsigenkänning i realtid i andra fall än när det krävs för att motverka allvarlig våldsbrottslighet inom den kriminella miljön.

När det gäller paragrafens närmare utformning föreslår Lagrådet att 4 § 1 och 2 får följande lydelse (där lagrådsremissens första punkt har delats upp i två punkter).

4 § AI-system för ansiktsigenkänning i realtid får användas om det är absolut nödvändigt för att lokalisera eller identifiera en viss person som

1. misstänks vara utsatt för människorov eller människohandel enligt 4 kap. 1 eller 1 a § brottsbalken eller för människoexploatering enligt 4 kap. 1 b § brottsbalken om exploateringen avser sexuella tjänster,

2. är försvunnen och misstänks vara utsatt för brott,

3. som misstänks komma att begå ett allvarligt brott som medför en specifik, överhängande och betydande risk för annans liv eller fysiska säkerhet,

Vidare anser Lagrådet att förslagets p. 3 bör utformas så att det tydligare framgår vilka svenska brott eller typer av brott som ska omfattas. Det bör vidare övervägas att införa ett krav på att de aktuella gärningarna ska ha ett visst minsta straffvärde. Det kan inte anses tillräckligt att frågan om hur allvarligt brottet är beaktas enbart inom ramen för den proportionalitetsbedömning som ska göras enligt 5 § i förslaget.

6 och 7 §§

I paragraferna anges när en ansökan om tillstånd att använda AI-system för ansiktsigenkänning ska prövas av åklagare och när den ska prövas av allmän domstol. Enligt 6 § ska en fråga om tillstånd prövas av åklagare om syftet med användningen är att förebygga, förhindra eller upptäcka brottslig verksamhet eller verkställa straffrättslig påföljd. I författningskommentaren sägs att detta innebär att åklagare kan pröva frågor om användning enligt 4 § 1, 2 och 4. Enligt 7 § ska frågan prövas av domstol om syftet med användningen är att utreda eller lagföra brott. I författningskommentaren sägs att detta innebär att domstol kan pröva frågor enligt 4 § 1–3.

Lagrådet konstaterar att den valda avgränsningen mellan åklagarens och domstolens behörighet är otydlig. Vid lagrådsföredragningen har diskuterats om avgränsningen skulle kunna göras på annat, tydligare sätt, t.ex. så att domstolens behörighet avgränsas till att gälla under förundersökning och att åklagaren i övriga fall är ensam behörig att pröva ansökan. Lagrådet har dock förståelse för att den lösningen inte har valts, eftersom den skulle innebära att en del situationer då det är rimligt att domstol prövar ansökan skulle falla utanför domstolens behörighet, t.ex. vid användning under förstadierna till en förundersökning. Lagrådet vill därför inte invända mot den föreslagna lagtexten.

Det som sägs i författningskommentarerna tyder emellertid på att det är tänkt att såväl åklagaren som rätten ska vara behörig att pröva ansökan i vissa fall, t.ex. så att en ansökan i fall som avses i 4 § 1 skulle kunna prövas av både åklagaren och rätten. Detta framstår dock enligt Lagrådets mening inte som lämpligt och är inte heller någon nödvändig konsekvens av den föreslagna lagtextens utformning. I själva verket synes ingen av de situationer som anges i 4 § 1 och 2 ha karaktären av utredning eller lagföring av (ett begånget) brott. Det bör innebära att domstolens behörighet normalt är begränsad till de fall som avses i 4 § 3, medan åklagaren är ensam behörig att besluta i de fall som avses i 4 § 1, 2 och 4. Givetvis kan det förekomma situationer då det finns anledning att överväga ansiktsigenkänning enligt flera av punkterna i 4 §. Om det i ett och samma ärende aktualiseras ett behov av att lokalisera en försvunnen person, som misstänks vara utsatt för brott, men också ett behov av att lokalisera en annan person som misstänks vara ansvarig för försvinnandet, blir enligt Lagrådets mening både 4 § 1 och 4 § 3 tillämpliga. Åklagaren är då ensam behörig att pröva ansökan om lokalisering av det förmodade brottsoffret, medan prövningen enligt 4 § 3 – lokaliseringen av den misstänkte – ankommer på domstol.

Lagrådet anser att frågan om avgränsningen mellan åklagarens respektive domstolens behörighet bör bli föremål för fortsatt uppmärksamhet i lagstiftningsarbetet.

14 §

Av 6 och 7 §§ i förslaget framgår att tillstånd att använda AI-system för ansiktsigenkänning i realtid bara får meddelas av åklagare och, i vissa fall, enbart av domstol. Bestämmelserna i 14 § innebär emellertid att Polismyndigheten eller Säkerhetspolisen får påbörja åtgärden utan tillstånd, om det är fara i dröjsmål. Enligt paragrafens andra stycke ska den myndighet som har påbörjat användning utan tillstånd dokumentera den samt skälen för att användningen påbörjades utan tillstånd.

Paragrafen innehåller alltså ett visst krav på dokumentation när ansiktsigenkänningen används utan föregående tillstånd. Lagrådet noterar att lagen inte innehåller något uttryckligt krav på dokumentation av den användning av AI-system för ansiktsigenkänning som sker efter tillstånd av åklagare eller domstol. Att sådan dokumentation bör ske är uppenbart. Lagrådet – som inte kunnat bedöma om sådan dokumentation ändå kommer till stånd enligt exempelvis polislagens (1984: 387) regler – anser att det i det fortsatta lagstiftningsarbetet bör övervägas att ta in en generell bestämmelse om dokumentation i lagförslaget.

15 §

Om Polismyndigheten eller Säkerhetspolisen med stöd av 14 § påbörjar användning av AI-system för ansiktsigenkänning utan tillstånd, ska – enligt 15 § första stycket – ansökan om tillstånd göras utan onödigt dröjsmål och senast inom 24 timmar från det att användningen påbörjades. Av paragrafens andra stycke följer att om användningen av ansiktsigenkänning har påbörjats utan tillstånd och det inte längre finns skäl för användningen, så ska Polismyndigheten eller Säkerhetspolisen – eller, i de fall då ansökan ska göras till domstol, åklagaren – omedelbart besluta att användningen ska upphöra.

Såvitt Lagrådet förstår får 15 § andra stycket betydelse såväl när fortsatt användning av ansiktsigenkänning inte längre fyller någon funktion, därför att syftet redan har uppnåtts (den försvunna personen har t.ex. redan återfunnits), som när den verkställande myndigheten har kommit fram till att ansiktsigenkänning inte är någon meningsfull åtgärd i det aktuella fallet.

Vid lagrådsföredragningen har upplysts att avsikten är att bestämmelsen i 15 § första stycket ska tillämpas även sedan den verkställande myndigheten har avbrutit åtgärden, i enlighet med 15 § andra stycket. Lagrådet har ingen invändning i sak mot detta. Det framstår tvärtom som naturligt att frågan om riktigheten av den vidtagna åtgärden blir föremål för en prövning av den instans som, enligt huvudreglerna i 6 och 7 §§, ska pröva frågan om användning av ansiktsigenkänning. Till detta kommer att bestämmelsen i 16 § – där det sägs att om en ansökan om tillstånd avslås ska användning som har påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas – synes förutsätta att varje användning av ansiktsigenkänning i något skede blir föremål för prövning av åklagare respektive domstol.

Enligt Lagrådets uppfattning framgår emellertid den tänkta ordningen inte på ett tillräckligt tydligt sätt av lagtexten. Det ligger vid en läsning av 15 § nära till hands att anta att tillstånd enligt första stycket behöver inhämtas enbart om den verkställande myndigheten vill fortsätta användningen av ansiktsigenkänning. I sammanhanget kan noteras att om det görs

en ansökan till en allmän domstol om tillstånd till en åtgärd som redan är vidtagen så torde domstolen som utgångspunkt betrakta den väckta frågan som överspelad (”desert”) och behandla ansökan som förfallen (se rättsfallet ”Den verkställda genomsökningen”, NJA 2023 s. 143).

Lagrådet noterar att motsvarande reglering angående bland annat hemlig avlyssning av elektronisk kommunikation (se 27 kap. 21 a § rättegångsbalken) har utformats på ett annat sätt än den nu föreslagna regleringen. Tillstånd till hemlig avlyssning av elektronisk kommunikation ska normalt ges av domstol. Om det kan antas att inhämtandet av sådant tillstånd skulle medföra en fördröjning av väsentlig betydelse för utredningen, får dock åklagaren ge tillstånd till åtgärden. Om åklagaren har gett sådant tillstånd, ska han eller hon genast anmäla det till rätten. I lagtexten anges därvid särskilt att om åklagarens beslut redan har verkställts innan rätten har prövat ärendet, ska rätten likväl pröva om det har funnits skäl för åtgärden.

Enligt Lagrådets mening bör regleringen i 27 kap. 21 a § i viss utsträckning kunna tjäna som förebild även för den nu aktuella regleringen.

Lagrådet föreslår därför att 15 § andra stycket kompletteras och att paragrafen också tillförs ett nytt tredje stycke enligt följande.

Om användning har påbörjats utan tillstånd och det inte längre finns skäl för åtgärden, ska den myndighet som har vidtagit åtgärden omedelbart besluta om att användningen ska upphöra. Om tillstånd inte redan har sökts, ska myndigheten också skriftligen anmäla användningen till åklagaren eller, i fall som avses i 7 §, rätten.

Om användning har påbörjats utan tillstånd men har upphört utan att tillståndsfrågan prövats, ska åklagaren eller, i fall som avses i 7 §, rätten pröva om det har funnits skäl för användningen.

16 §

Om Lagrådets förslag till justeringar av 15 § godtas, bör också 16 § kompletteras och ges följande lydelse.

Om en ansökan om tillstånd avslås, ska användning som har påbörjats utan tillstånd omedelbart upphöra och uppgifter från användningen raderas. Uppgifterna från användningen ska också raderas om, i fall som avses i 15 § tredje stycket, åklagaren eller rätten har funnit att det har saknats skäl för användningen.

Förslaget till lag om ändring i lagen om utlämning för brott

16 a §

Av paragrafen framgår att AI-system för ansiktsigenkänning får användas i ett utlämningsärende för att lokalisera någon som är anhållen eller häktad i ärendet. Syftet med användningen ska då vara att verkställa frihetsberövandet och användningen får ske ”enligt 4 § 3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål”.

Det framgår inte av vare sig lagtexten eller författningskommentaren om beslutet att använda ansiktsigenkänning i ett utlämningsärende ska beslutas av rätten eller av åklagare. Lagrådet noterar att hänvisningen till 4 § 3 ansiktsigenkänningslagen inte ger något entydigt besked i frågan. Enligt Lagrådet bör frågan klargöras i det fortsatta lagstiftningsarbetet.

Motsvarande klargörande bör göras i fråga om 4 kap. 3 a § i förslaget till lag om ändring i lagen om överlämnande från Sverige enligt en europeisk arresteringsorder och 3 kap. 3 a § i förslaget till lag om ändring i lagen om överlämnande från Sverige enligt en nordisk arresteringsorder.

Förslaget till lag om ändring i lagen om internationell rättslig hjälp i brottmål

4 kap. 28 i §

Paragrafen innehåller bestämmelser om vilka åtgärder enligt lagen om AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål som rättslig hjälp kan lämnas för och om handläggningen av en ansökan om detta.

I första stycket anges bland annat att om det är fara i dröjsmål får användningen påbörjas utan tillstånd enligt 14 § lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. En ansökan om tillstånd ska i sådana fall göras enligt 15 § samma lag. Det framgår dock inte tydligt vem det är som beslutar om sådan användning och inte heller om 16 § lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål ska tillämpas. Vid föredragningen har upplysts om att avsikten är att det är åklagaren som beslutar om att påbörja användning utan tillstånd och att även 16 § ska vara tillämplig.

Lagrådet föreslår att första stycket delas upp i två stycken som ges följande utformning.

> En ansökan om användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid som avser någon som befinner sig i Sverige handläggs av åklagare. Ansökan får endast avse användning enligt 4 § 1–3 lagen (2026:000) om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd.
>
> Om det är fara i dröjsmål, får åklagaren besluta att användningen får påbörjas utan tillstånd. I så fall tillämpas bestämmelserna i 14 § andra stycket samt 15 och 16 §§ lagen om användning av AI-system för ansiktsigenkänning i realtid för brottsbekämpande ändamål.

Övriga lagförslag

Lagrådet lämnar förslagen utan erinran.

Justitiedepartementet

Utdrag ur protokoll vid regeringssammanträde den 3 mars 2026

Närvarande: statsrådet Edholm, ordförande, och statsråden Waltersson Grönvall, Strömmer, Forssell, Wykman, Bohlin, Larsson, Britz, Mohamsson

Föredragande: statsrådet Strömmer

Regeringen beslutar proposition Polisens användning av AI för ansiktsigenkänning i realtid