

Polisens och Tullverkets användning av AI för biometrisk fjärridentifiering i efterhand

Ds 2025:32



Regeringskansliet
Justitiedepartementet

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss

Statsrådsberedningen, SB PM 2021:1.

Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Omslag: Regeringskansliets standard

Tryck och remisshantering: Åtta45, Stockholm 2025

ISBN 978-91-525-1435-1 (tryck)

ISBN 978-91-525-1436-8 (pdf)

ISSN 0284-6012

Innehåll

Sammanfattning	7
1 Författningsförslag.....	8
1.1 Förslag till lag om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål.....	8
1.2 Förslag till lag om ändring i lagen (1957:668) om utlämning för brott	10
1.3 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål.....	11
1.4 Förslag till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder	14
1.5 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).....	15
1.6 Förslag till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder	18
1.7 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder	19
1.8 Förslag till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket.....	21

1.9	Förslag till förordning om ändring i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten	22
2	Ärendet	24
3	AI-förordningens regler om användning av AI-system för biometrisk fjärridentifiering i efterhand	25
3.1	Kort om AI-förordningen	25
3.2	Artikel 26.10 i AI-förordningen.....	26
3.2.1	AI-system för biometrisk fjärridentifiering i efterhand.....	26
3.2.2	Krav på tillstånd	27
3.2.3	Otillåten användning i vissa fall	28
3.2.4	Tillståndsprövningen och övriga regler	30
4	Utgångspunkter för de fortsatta bedömningarna	32
4.1	Grundläggande fri- och rättigheter behöver beaktas	32
4.1.1	Rätten till privatliv	32
4.1.2	Skydd för personuppgifter	33
5	Användning av AI för biometrisk fjärridentifiering i efterhand ska regleras i en ny lag	35
5.1	En ny lag med bestämmelser som kompletterar AI-förordningen ska införas	36
5.2	Användningen måste vara proportionerlig	43
5.3	Beslut om tillstånd ska fattas av allmän åklagare	44
5.4	Beslutets innehåll.....	47
5.5	Om en begäran om tillstånd nekas	48
5.6	Det saknas behov av en underrättelseskyldighet	49
5.7	Förslagens förenlighet med grundläggande fri- och rättigheter.....	50

6	Behovet av följdändringar	55
6.1	Det krävs ändringar i offentlighets- och sekretesslagen.....	55
6.2	Integritetsskyddsmyndigheten ska vara marknadskontrollmyndighet.....	58
6.3	AI-system för biometrisk fjärridentifiering i efterhand och hemlig dataavläsning ska få användas inom det internationella straffrättsliga samarbetet	60
6.4	Det behöver inte göras någon ändring i befintlig dataskyddsreglering	64
7	Ikraftträdande- och övergångsbestämmelser	68
8	Konsekvenser av förslagen	70
8.1	Konsekvenser för det brottsbekämpande arbetet och för enskilda	70
8.2	Ekonomiska konsekvenser	72
8.3	Övriga konsekvenser	76
9	Författningskommentar	78
9.1	Förslaget till lag om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål.....	78
9.2	Förslag till lag om ändring i lagen (1957:668) om utlämning för brott	82
9.3	Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål.....	83
9.4	Förslag till lag om ändring i lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder	86
9.5	Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).....	87

9.6	Förslag till lag om ändring i lagen (2011:1165) om överlämnande från Sverige enligt en nordisk arresteringsorder.....	90
9.7	Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder.....	91
9.8	Förslag till lag om ändring i lagen (2021:709) med kompletterande bestämmelser om straffrättsligt samarbete mellan Europeiska unionen och Förenade kungariket	93

Sammanfattning

I denna promemoria lämnas förslag till en ny lag om en tillståndsprocess för sådan användning av AI-system för biometrisk fjärridentifiering i efterhand som omfattas av kravet på tillstånd enligt artikel 26.10 i AI-förordningen. Förslagen innebär att Polismyndigheten, Säkerhetspolisen och Tullverket i vissa fall kan medges tillstånd att använda tekniken i utredningar för att kunna göra målinriktade sökningar av personer som misstänks ha begått brott eller som har dömts för att ha begått brott.

Förslagen syftar till att ge polisen och Tullverket effektiva verktyg i dess brottsbekämpande verksamhet, samtidigt som enskildas fri- och rättigheter beaktas. Författningsförslagen föreslås träda i kraft den 1 januari 2027.

1 Författningsförslag

1.1 Förslag till lag om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål

Härigenom föreskrivs följande.

1 § I denna lag finns bestämmelser om tillståndsförfarandet vid viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål.

Lagen kompletterar 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.

2 § I artikel 26.10 i AI-förordningen finns bestämmelser om att viss användning av AI-system för biometrisk fjärridentifiering i efterhand kräver tillstånd.

Polismyndigheten, Säkerhetspolisen och Tullverket får ges ett sådant tillstånd.

3 § Tillstånd får endast medges 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.

4 § Ett tillstånd enligt 2 § prövas av allmän åklagare.

5 § Ett beslut om tillstånd gäller omedelbart. I beslutet ska det anges

- vilken person som tillståndet avser,
- vilket eller vilka brott eller brottsmisstankar som tillståndet avser, och
- vilket material som omfattas av tillståndet.

6 § I artikel 26.10 andra stycket i AI-förordningen finns bestämmelser om förfarandet när ett tillstånd enligt 2 § nekas och användningen av tekniken redan har påbörjats.

Denna lag träder i kraft den 1 januari 2027.

1.2 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 två nya paragrafer, 16 b och 16 c §§, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

16 b §

För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål användas i syfte att verkställa frihetsberövandet. Vid sådan användning tillämpas bestämmelserna i den lagen.

16 c §

För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får hemlig dataavläsning enligt 6 c § lagen (2020:62) om hemlig dataavläsning användas. Vid sådan användning tillämpas bestämmelserna i den lagen.

Denna lag träder i kraft den 1 januari 2027.

1.3 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 k och 28 l §§, och närmast före 4 kap. 28 k § en ny rubrik av följande lydelse.

Lydelse enligt lagrådsremissen Föreslagen lydelse
Polisens användning av AI för
ansiktsigenkänning i realtid

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 ansiktsgenkänning eller annan biometrisk fjärridentifiering i realtid.

14. rättsmedicinsk undersökning av en avliden person,

15. användning av AI-system för ansiktsgenkänning eller annan biometrisk fjärridentifiering i realtid, *och*

16. användning av AI-system för biometrisk fjärridentifiering i efterhand.

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.

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 1–10 *och* 14–16 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 §

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 6, 11 och 13 får lämnas även om den

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.

Nuvarande lydelse

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 14–16 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.

Föreslagen lydelse

4 kap.

Användning av AI-system för biometrisk fjärridentifiering i efterhand

28 k §

En ansökan om användning av AI-system för biometrisk fjärridentifiering i efterhand av någon som befinner sig i Sverige handläggs av åklagare.

28 l §

Om användning av AI-system för biometrisk fjärridentifiering i efterhand 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.

Denna lag träder i kraft den 1 januari 2027.

1.4 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 två nya paragrafer, 4 kap. 3 b och 7 a §§, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 kap.

3 b §

För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål användas i syfte att verkställa frihetsberövandet. Vid sådan användning tillämpas bestämmelserna i den lagen.

7 a §

För att lokalisera någon som är anhållen eller häktad enligt denna lag får hemlig dataavläsning enligt 6 c § lagen (2020:62) om hemlig dataavläsning användas. Vid sådan användning tillämpas bestämmelserna i den lagen.

Denna lag träder i kraft den 1 januari 2027.

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

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

Lydelse enligt lagrådsremissen Föreslagen lydelse
Polisens användning av AI för
ansiktsigenkänning i realtid

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. 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 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 *eller enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand 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.

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 säkerhets-skyddslagen (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 brottsdatalogens område eller som annars behandlas där med stöd av samma lag,

10. utredning om 10. utredning om självständigt förverkande, *eller* självständigt förverkande,

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

eller

12. angelägenhet som avser användning av AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand 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 2027.

1.6 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 två nya paragrafer, 3 kap. 3 b och 8 a §§, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

3 kap.

3 b §

För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål användas i syfte att verkställa frihetsberövandet. Vid sådan användning tillämpas bestämmelserna i den lagen.

8 a §

För att lokalisera någon som är anhållen eller häktad enligt denna lag får hemlig dataavläsning enligt 6 c § lagen (2020:62) om hemlig dataavläsning användas. Vid sådan användning tillämpas bestämmelserna i den lagen.

Denna lag träder i kraft den 1 januari 2027.

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

Härigenom föreskrivs att 1 kap. 4 §, 2 kap. 1 § och 3 kap. 4 § lagen (2017:1000) om en europeisk utredningsorder ska ha följande lydelse.

Lydelse enligt lagrådsremissen Föreslagen lydelse
Polisens användning av AI för
ansiktsigenkänning i realtid

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*
12. användning av AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering i realtid,
13. *användning av AI-system för biometrisk fjärridentifiering i efterhand, eller*

13. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.

14. 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 3–13.

En utredningsorder får utfärdas av åklagare för en utredningsåtgärd som avses i 1 kap. 4 § 1 och 3–14.

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.

En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10, 11, 12 *eller* 13 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.

Denna lag träder i kraft den 1 januari 2027.

1.8 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 två nya paragrafer, 3 kap. 6 b och 11 a §§, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

3 kap.

6 b §

I frågor om användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål tillämpas bestämmelserna i 4 kap.

3 b § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.

11 a §

I frågor om hemlig dataavläsning tillämpas bestämmelserna i 4 kap.

7 a § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.

Denna lag träder i kraft den 1 januari 2027.

1.9 Förslag till förordning om ändring i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten

Härigenom föreskrivs att 3 d § i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten¹ ska ha följande lydelse.

Förslag enligt Ds 2025:7 Polisens användning av AI för ansiktsigenkänning i realtid *Föreslagen lydelse*

3 d §

Myndigheten är marknadskontrollmyndighet i fråga om användning av system för artificiell intelligens för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål enligt 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).

Myndigheten är marknadskontrollmyndighet i fråga om användning av system för artificiell intelligens för biometrisk fjärridentifiering i realtid på allmänt tillgängliga platser för brottsbekämpande ändamål *och system för artificiell intelligens för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål* enligt 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).

¹ Senaste lydelse av förordningens rubrik 2020:1123.

Denna förordning träder i kraft 1 januari 2027.

2 Ärendet

I augusti 2024 trädde 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 kraft.

En särskild utredare har haft i uppdrag att se över behovet av nationella anpassningar till följd av AI-förordningen. Utredningen om AI-förordningen redovisade i oktober 2025 sitt betänkande Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation (SOU 2025:101), som har remitterats. I betänkandet konstateras att artikel 26.10 i AI-förordningen kräver att det finns en tillståndsprocess i nationell rätt för att en tillhandahållare av AI-system för biometrisk fjärridentifiering i efterhand ska kunna använda systemet för att söka efter en person som misstänks ha begått ett brott eller som har dömts för att ha begått ett brott. Utredningen lämnar emellertid inte några förslag i denna del (se avsnitt 14.5 i betänkandet).

I denna promemoria redogörs för Polismyndighetens, Säkerhetspolisens och Tullverkets behov av användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål och det lämnas förslag på bestämmelser beträffande en tillståndsprocess för användning av sådan teknik när det krävs enligt artikel 26.10 i AI-förordningen.

3 AI-förordningens regler om användning av AI-system för biometrisk fjärridentifiering i efterhand

3.1 Kort om AI-förordningen

Syftet med AI-förordningen är att harmonisera 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.

AI-förordningen bygger på en riskbaserad metod, vilket innebär att reglernas art och innehåll har anpassats med hänsyn till omfattningen av de risker som AI-systemen kan innebära inom vissa användningsområden. Exempelvis är vissa användningsområden förbjudna, medan vissa system är klassificerade som högrisksystem men tillåtna 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).

3.2 Artikel 26.10 i AI-förordningen

3.2.1 AI-system för biometrisk fjärridentifiering i efterhand

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. Exempel på sådana system är bl.a. AI-system som används för biometrisk fjärridentifiering. Ett system för *biometrisk fjärridentifiering* är enligt artikel 3.41 ett 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. Av skäl 15 i AI-förordningen framgår att 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.

I artikel 26.10 i AI-förordningen regleras viss användning av *system för biometrisk fjärridentifiering i efterhand*, vilket enligt artikel 3.43 definieras som ett annat system för biometrisk fjärridentifiering än ett system för biometrisk fjärridentifiering i realtid. Ett *system för biometrisk fjärridentifiering i realtid* är enligt artikel 3.42 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. När det gäller realtidsidentifiering sker alltså insamlingen av biometriska uppgifter, jämförelsen och identifieringen omedelbart, näst intill omedelbart eller under alla omständigheter utan betydande dröjsmål. Det ska inte finnas något utrymme för att kringgå förordningens 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. System för biometrisk

fjärridentifiering i efterhand 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 eller privat utrustning och som har genererats före användningen av systemet avseende de berörda fysiska personerna (skäl 17 i AI-förordningen). Begreppet ”utan betydande dröjsmål” måste bedömas från fall till fall. I allmänhet är ett dröjsmål betydande åtminstone när personen i fråga sannolikt har lämnat den plats där de biometriska uppgifterna samlades in (se Kommissionens riktlinjer den 29 juli 2025 om de förbjudna användningsområdena för artificiell intelligens som fastställs i förordning (EU) 2024/1689 [AI-förordningen] s. 107 f.).

3.2.2 Krav på tillstånd

Av artikel 26.10 i AI-förordningen följer att användning av AI-system för biometrisk fjärridentifiering i efterhand i vissa fall kräver ett tillstånd och att tekniken under vissa särskilt angivna förhållanden inte får användas. För övrig användning gäller inga specifika krav enligt artikel 26.10, men liksom för användning som kräver tillstånd, måste den vara förenlig med både övriga bestämmelser i AI-förordningen om högrisksystem och den dataskyddsrättsliga regleringen. Enligt artikel 26.10 är det tillhandahållaren som ska begära ett tillstånd när det krävs ett sådant för att använda tekniken enligt bestämmelsen. En *tillhandahållare* är enligt artikel 3.4 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. Det är alltså den som ska använda tekniken i sin brottsbekämpande verksamhet som ska begära ett tillstånd.

Enligt artikel 26.10 första stycket i AI-förordningen krävs ett tillstånd om den brottsbekämpande myndigheten ska använda AI-system för biometrisk fjärridentifiering i efterhand 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. En begäran om tillstånd krävs dock inte när systemet används för den

inledande identifieringen av en potentiell misstänkt på grundval av objektiva och verifierbara fakta med direkt anknytning till brottet. Kravet på tillstånd gäller alltså inte när det är fråga om en tidig identifiering av en viss person, när fakta talar för att personen kan misstänkas för brottet. Ett exempel på inledande identifiering är när Nationellt forensiskt centrum efter beslut av åklagare får använda automatiserad ansikts- och fingeravtrycksjämförelse för att jämföra ansiktsbilder och fingeravtryck från en icke identifierad gärningsman med uppgifter i de register över fingeravtryck och fotografier som förs med stöd av utlänningsdatalagen (6 a kap. lagen [2018:1693] om polisens behandling av personuppgifter inom brottsdatalagens område).

Om den brottsbekämpande myndigheten i stället vill använda tekniken för en målinriktad sökning av en redan identifierad misstänkt, oavsett om identifieringen är fastställd eller inte, exempelvis för att inom ramen för en förundersökning söka igenom kameramaterial i syfte att kartlägga den misstänktes aktivitet före eller efter det aktuella brottstillfället, fastslå ett händelseförlopp eller en tid eller plats för en gärning, krävs däremot ett tillstånd för användningen enligt artikel 26.10 i AI-förordningen. Någon närmare förklaring av vad som utgör en inledande identifiering till skillnad från en tillståndspliktig sökning finns inte i förordningen. Det kommer därmed bli de rättstillämpande myndigheternas, och ytterst EU-domstolens, ansvar att klargöra var gränsen går mellan en inledande identifiering och en tillståndspliktig sökning.

Vad gäller användning av tekniken inom ramen för underrättelseverksamhet kan konstateras att i de fall det inte finns en för brott misstänkt person omfattas inte användningen av kravet på tillstånd. Under förutsättning att tekniken inte används på ett sätt som enligt artikel 26.10 tredje stycket är otillåtet (se nedan) kan tekniken därför användas i underrättelseverksamhet. Användningen måste dock vara förenlig med AI-förordningens övriga bestämmelser och dataskyddsregelverket.

3.2.3 Otillåten användning i vissa fall

Av artikel 26.10 tredje stycket i AI-förordningen framgår att viss användning av AI-system för biometrisk fjärridentifiering i

efterhand är otillåten. Enligt bestämmelsen får ett sådant system under inga omständigheter 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 är alltså inte tillåtet att för brottsbekämpande ändamål använda AI-system för biometrisk fjärridentifiering i efterhand på ett sätt som utgör allmän övervakning. Användningen måste syfta till att söka efter en specifik person (jfr skäl 95 i AI-förordningen).

En fråga som uppstår är vad som gäller för att söka efter en person som inte är misstänkt men ändå har koppling till ett straffrättsligt förfarande eller ett verkligt, aktuellt och förutsebart hot om ett brott eller som är försvunnen. Det kan t.ex. vara fråga om ett vittne eller en målsägande inom ramen för en brottsutredning. En sådan sökning bör inte anses utgöra otillåten användning – den är både målinriktad och har koppling till ett brott eller ett straffrättsligt förfarande. Detsamma gäller vid användning för sökning efter en försvunnen person, oavsett om personen tros ha utsatts för ett brott eller inte. I det förra fallet är det fråga om målinriktad sökning för brottsbekämpande ändamål efter en specifik försvunnen person, medan det i det senare fallet inte rör sig om brottsbekämpande ändamål varför artikel 26.10 överhuvudtaget inte blir tillämplig. Detta följer även av syftet att motverka att tekniken används på ett sätt som möjliggör en urskillningslös övervakning och att kravet på tillstånd gäller när användningen sker för ändamål som kan få negativa rättsliga konsekvenser för den som söks (jfr skäl 95 i AI-förordningen).

När tekniken används på ett sätt som inte är tillståndspliktigt enligt artikel 26.10 måste användningen, likt i dag, ha stöd i den dataskyddsrättsliga regleringen och därutöver uppfylla övriga krav på användning enligt bestämmelserna i AI-förordningen. Även om sådan användning inte träffas av artikel 26.10 medför AI-förordningen alltså skärpta krav också i dessa fall.

3.2.4 Tillståndsprövningen och övriga regler

Artikel 26.10 i AI-förordningen förutsätter att det finns nationella bestämmelser om tillståndsförfarandet på plats när den börjar tillämpas. Av artikeln framgår att en begäran om tillstånd för användning av AI-system med hög risk för biometrisk fjärridentifiering i efterhand ska göras hos en rättslig myndighet eller en administrativ myndighet vars beslut är bindande och föremål för rättslig prövning. Ett tillstånd ska sökas på förhand eller utan oskäligt dröjsmål och senast inom 48 timmar från det att användningen påbörjades. Begäran om tillstånd påverkar inte tillämpningen av 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).

Varje användning ska enligt artikel 26.10 första stycket begränsas till vad som är absolut nödvändigt för att utreda ett specifikt brott. Om det tillstånd som begärts nekas ska, enligt bestämmelsens andra stycke, 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. Av bestämmelsens tredje stycke framgår att beslut som har negativa rättsliga följder för en person inte får fattas av de brottsbekämpande myndigheterna enbart på grund av utdata från AI-system för biometrisk fjärridentifiering i efterhand.

Enligt artikel 26.10 femte stycket ska varje användning av AI-system för biometrisk fjärridentifiering i efterhand, oavsett ändamål eller tillhandahållare, 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. Tillhandahållare ska även, enligt bestämmelsens sjätte stycke, 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 enligt artikel 26.10 sjunde stycket införa mer restriktiva lagar om användningen av system för biometrisk fjärridentifiering i efterhand i enlighet med unionsrätten.

4 Utgångspunkter för de fortsatta bedömningarna

4.1 Grundläggande fri- och rättigheter behöver beaktas

4.1.1 Rätten till privatliv

När AI-system för biometrisk fjärridentifiering i efterhand används sker en biometrisk behandling av material från exempelvis en kamera eller en sökning mot ett register med biometriska uppgifter. Systemet bearbetar uppgifter om en potentiellt stor mängd människor. Det är nödvändigt att användningen av tekniken är förenlig med enskildas grundläggande fri- och rättigheter. Ett av syftena med AI-förordningen är att säkerställa en hög skyddsnivå för bl.a. grundläggande rättigheter såsom fastställs i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga). En sådan rättighet är skyddet för privatliv som regleras i artikel 7 i EU:s rättighetsstadga.

Ett skydd för privatlivet finns även i 2 kap. 6 § andra stycket regeringsformen som fastställer att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Rättigheten får enligt 2 kap. 20 och 21 §§ regeringsformen 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. 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.).

Enligt artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europa-konventionen) 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. Bestämmelsen 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 innebär 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 och säkerställa att brott kan utredas effektivt.

Sedan den 1 januari 2020 gäller Förenta nationernas konvention om barnets rättigheter (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). 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.

4.1.2 Skydd för personuppgifter

När AI-system för biometrisk fjärridentifiering i efterhand används behandlas en potentiellt stor mängd personuppgifter. Användningen måste därför vara förenlig med den dataskyddsreglering som finns

på området som bl.a. syftar till att värna om enskildas personliga integritet. När personuppgifter behandlas inom brottsbekämpningen ska 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 sätter 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 förhållande 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 biometrisk och genetisk 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 exempelvis 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). Brottsdatalagen innehåller också bestämmelser om Integritetsskyddsmyndighetens tillsyn och om 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 t.ex. lagen om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag). För Tullverkets behandling av personuppgifter på brottsdatalagens område gäller lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område (Tullverkets brottsdatalag). Lagarna innehåller bestämmelser som kompletterar, preciserar eller avviker från brottsdatalagen. Alla grundläggande bestämmelser finns dock i brottsdatalagen.

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. En särskild utredare har haft i uppdrag att se över regleringen av dessa delar av Säkerhetspolisens personuppgiftsbehandling. Det uppdraget redovisades den 23 april 2025 i betänkandet Säkerhetspolisens behandling av personuppgifter (SOU 2025:49), som för närvarande bereds i Regeringskansliet.

5 Användning av AI för biometrisk fjärridentifiering i efterhand ska regleras i en ny lag

5.1 En ny lag med bestämmelser som kompletterar AI-förordningen ska införas

Förslag: Det ska införas en ny lag som reglerar tillståndsförfarandet för Polismyndighetens, Säkerhetspolisens och Tullverkets användning av AI-system för biometrisk fjärridentifiering i efterhand enligt artikel 26.10 i AI-förordningen. Lagen ska komplettera AI-förordningen.

Skälen för förslaget

AI-system för ansiktsigenkänning eller annan biometrisk fjärridentifiering utgör en effektiv utredningsmetod

Polisen samlar in stora mängder information i sitt brottsbekämpande arbete, vilket kräver effektiva metoder och verktyg för att snabbt kunna sälla och filtrera fram den relevanta informationen för den aktuella situationen. Den insamlade informationen förväntas öka över tid. I dagsläget använder polisen teknik i sin brottsbekämpande verksamhet som faller in under AI-förordningens definition av AI-system för biometrisk fjärridentifiering i efterhand. Användningen sker med stöd av det dataskyddsrättsliga regelverket och innefattar bl.a. register-

slagningar och bildanalys av bild- och videomaterial.² Genom att använda tekniken kan polisen identifiera okända gärningsmän, få information om ytterligare brott som en misstänkt person har begått och om det finns fler personer som medverkat i brottet. Det kan även framkomma information som kan ligga till grund för en tänkbar motivbild eller för att avskriva en person från misstankar.

Nationellt forensiskt centrum använder bl.a. tekniken för att göra en automatisk jämförelse av ansiktsbilder, fingeravtryck och signalementsuppgifter m.m. mot olika register som innehåller biometriska uppgifter. Jämförelsen utförs på begäran av en utredare inom ramen för en brottsutredning, bl.a. i syfte att få fram ett uppslag till identitet eller få fram ett urval av personer med hjälp av biometriska uppgifter. Det görs även jämförelser med röstinspelningar från en gärningsperson mot ett röstprov från en misstänkt med hjälp av AI-system. Dessa görs som ett komplement till manuella jämförelser.

Polismyndigheten använder sig även av tekniken för s.k. bildanalys. Bildanalys innebär att bild- och videomaterial analyseras med hjälp av ansiktsgenkänningsteknik. Syftet med att använda tekniken är att på ett effektivt sätt söka igenom ett större kameramaterial efter en person av intresse och därmed leda utredningen framåt. Det kan bl.a. ske genom att en ansiktsbild extraheras från kameramaterialet och sedan analyseras. På detta sätt kan polisen exempelvis utreda om en okänd gärningsperson som fångats på en kamera syns i annat kameramaterial. Det går även att använda ansiktsbilder på kända personer som är intressanta för utredningen för att se om dessa förekommer i kameramaterialet. Tekniken används i dag av polisen inom förundersökning oavsett varifrån materialet har samlats in och främst för att utreda grov brottslighet. De flesta ansiktsbilder som används är på misstänkta, men ibland även målsägande. Tekniken används kontinuerligt och har använts för att utreda ett hundratal ärenden. Användningen av tekniken var bl.a. avgörande i utredningen av mordet i Almedalen 2022 eftersom den eftersökta person vid flera tillfällen bytte kläder i det kameramaterialet som analyserades och därmed omöjliggjorde alternativa söktekniker. Tekniken har även varit viktig i flera andra utredningar om mord. Polisen bedömer att tekniken har sparat in

² Se Datainspektionens förhandssamråd om Polismyndighetens planerade användning av bildanalysverktyg vid utredning av brott, 23 juli 2020, dnr DI-2020-6011.

tusentals timmar av manuellt granskningsarbete. Under 2025 har cirka fyra års filmmaterial analyserats varje månad. Användning av biometrisk fjärridentifiering i efterhand utgör således en väldigt effektiv utredningsmetod. Genom att använda tekniken kan utredningsarbetet dessutom utföras av färre tjänstemän än vid manuell granskning vilket dels ökar kvaliteten på analysarbetet, dels minimerar spridningen av uppgifterna och på så sätt även integritetsintrånget.

Det är angeläget att polisen kan fortsätta använda AI på det sätt som redan görs och att det finns möjligheter att i framtiden använda annan teknik som klassificeras som AI-system för biometrisk fjärridentifiering i efterhand i de fall som omfattas av artikel 26.10 i AI-förordningen, när kravet på tillstånd har börjat gälla. Det finns därmed ett behov av en nationell reglering som möjliggör att tekniken används i enlighet med vad som föreskrivs i artikel 26.10.

Tullverket har också framfört ett behov av att kunna använda tekniken i bl.a. de situationer där det krävs tillstånd enligt artikel 26.10 i AI-förordningen. De situationer när Tullverket behöver kunna använda tekniken uppstår normalt i myndighetens brottsutredande verksamhet, särskilt när det gäller smugglingsbrott. Smuggling av t.ex. narkotika, vapen och explosiva varor sker i betydande omfattning. Det är angeläget att kunna utreda misstänkta smugglingsbrott snabbt och effektivt. Ett exempel på när tekniken skulle vara ett värdefullt verktyg i en utredning är när ett smugglingsbrott uppdagas först när den aktuella varan befinner sig inne i landet och det finns en misstanke om att en viss person har fört varan över gränsen. För att kunna styrka ett smugglingsbrott behöver varans väg in i landet spåras bakåt. Det kan då krävas bl.a. att material från övervakningskameror vid gränspassager granskas för att kunna identifiera både varan och personen som smugglat in varan. I dag görs sökningar i material från övervakningskameror manuellt. Eftersom materialet ofta kan vara omfattande är sådana manuella genomgångar mycket tidskrävande. Det är Tullverkets erfarenhet att identifieringen av misstänkta personer ofta misslyckas på grund av dagens ineffektiva utredningsmetoder. Det finns därför ett stort värde i att Tullverket kan använda sig av AI-system för biometrisk fjärridentifiering i efterhand i sin brottsutredande verksamhet.

Artikel 26.10 i AI-förordningen är direkt tillämplig men det krävs en nationell reglering

En EU-förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater. Det betyder att en förordning ska tillämpas direkt av alla nationella myndigheter på samma sätt som lagar och andra nationella föreskrifter. Artikel 26.10 i AI-förordningen måste förstås så att den är direkt tillämplig och ska alltså likställas med svensk lag. Bestämmelsen förutsätter dock kompletterande nationella regler om tillståndsförfarandet och att en myndighet utses att vara den berörda marknadskontrollmyndighet som rapportering m.m. ska ske till vid användning av AI-system för biometrisk fjärridentifiering i efterhand. Den berörda marknadskontrollmyndigheten är den myndighet som utses att vara marknadskontrollmyndighet över sådana AI-system som används inom biometri och närmare bestämt system för biometrisk fjärridentifiering (se AI-förordningen, bilaga III, punkt 1 a). Eftersom användning av tekniken innebär ett intrång i grundläggande fri- och rättigheter bör regler om tillståndsförfarandet finnas i lag. Det föreslås därför att det införs en ny lag som reglerar tillståndsförfarandet vid sådan användning av AI-system för biometrisk fjärridentifiering i efterhand som kräver tillstånd enligt artikel 26.10.

Den nya lagen måste läsas tillsammans med artikel 26.10 i AI-förordningen. För att undvika dubbelreglering bör den nya lagen hänvisa till förordningen. Det är lämpligast att använda en dynamisk hänvisningsteknik som innebär att lagen hänvisar till förordningsartikeln i den vid varje tidpunkt gällande lydelsen. Därigenom får eventuella framtida ändringar i AI-förordningen direkt genomslag i nationell rätt.

Den nya lagens tillämpningsområde

För att fortsatt kunna bedriva ett effektivt utredningsarbete har polisen ett stort behov av att kunna använda AI-system för biometrisk fjärridentifiering i efterhand, även på sådana sätt som kan vara tillståndspliktiga enligt artikel 26.10 i AI-förordningen när den börjar tillämpas. Vid granskning av ett material med hjälp av AI-system för biometrisk fjärridentifiering i efterhand sällar AI-

systemet bort information som inte är av intresse för utredningen. Det innebär att färre poliser behöver granska materialet manuellt, vilket gör det möjligt för polisen att utreda fler brott. Det är även fördelaktigt för den enskilde eftersom det innebär att färre personer tar del av uppgifterna. AI-systemets analys kan förse utredningen med information som behövs för att fastslå ett händelseförlopp, tid eller plats för en gärning och vilka gärningar som misstänkta personer kan knytas till. Det kan även framkomma information som gör att en person kan avskrivas som misstänkt i ett tidigt skede i utredningen och ge information som är intressant för en motivbild. Det finns vidare ett stort behov av att kunna använda tekniken för att söka efter personer som har dömts för brott eftersom det är viktigt för tilltron till rättssystemet att utdömda straff verkställs. En möjlighet till användning av AI-system för biometrisk fjärridentifiering i efterhand som artikel 26.10 medger bedöms även svara väl mot den behovsbeskrivning som Tullverket lagt fram i fråga om dess brottsutredande verksamhet. Den nya lagen bör därför omfatta både Polismyndigheten och Tullverket.

Säkerhetspolisen har i uppdrag att förebygga, förhindra, upptäcka, utreda och beivra brottslig verksamhet, specifikt brott mot rikets säkerhet eller terrorbrott (3 § polislagen [1984:387]). Säkerhetspolisens användning av AI-system för nationell säkerhet ligger utanför AI-förordningens tillämpningsområde. Det gäller även om det är så att Säkerhetspolisen delar eller använder andra aktörers systemlösningar såväl som om det är en annan aktör som står för det faktiska utförandet, så länge användningen sker för Säkerhetspolisens räkning och syftet med användningen är nationell säkerhet. 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. Det kan inte uteslutas att Säkerhetspolisen någon gång i ett sådant ärende skulle ha behov av att använda AI-system

för biometrisk fjärridentifiering i efterhand och lagen bör därför även omfatta Säkerhetspolisen.

Av artikel 26.10 i AI-förordningen framgår att tillhandahållaren måste begära ett tillstånd för att använda AI-system med hög risk för biometrisk fjärridentifiering i efterhand 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. Som framgår av avsnitt 3.2.2 krävs inget tillstånd när tekniken ska användas för en inledande identifiering av en potentiell misstänkt på grundval av objektiva och verifierbara fakta med direkt anknytning till brottet. Tillhandahållaren är den aktör som ska använda tekniken i sin utredning och är alltså den som ska begära ett tillstånd, dvs. Polismyndigheten, Säkerhetspolisen och Tullverket enligt de förslag som lämnas i denna promemoria (jfr artikel 3.4 i AI-förordningen).

Tillstånd krävs när tekniken används på ett målinriktat sätt inom ramen för en brottsutredning för att söka efter en misstänkt person. Det är alltså fråga om ett brott som har begåtts och som utreds av Polismyndigheten, Säkerhetspolisen eller Tullverket. Enligt 23 kap. 1 § rättegångsbalken ska en förundersökning inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. Det vanliga bör därmed vara att frågan om tillstånd aktualiseras när tekniken används inom ramen för en förundersökning. Tillstånd kan vidare medges för att söka efter en person som har dömts för ett brott. Det kan exempelvis handla om en person som inte har inställt sig till eller avvikit från verkställigheten av ett straff.

Av artikel 26.10 sjunde stycket i AI-förordningen framgår att medlemsstaterna får införa mer restriktiva lagar om användning av AI-system för biometrisk fjärridentifiering i efterhand i enlighet med unionsrätten. Som nämns ovan använder Polismyndigheten redan teknik som likställs med AI-förordningens definition av AI-system för biometrisk fjärridentifiering i efterhand i sin brottsbekämpande verksamhet. Användningen har gett goda resultat och sparat in tusentals timmar av manuellt granskningsarbete. Användningen sker i dagsläget med stöd av den dataskyddsrättsliga regleringen och AI-förordningens krav på tillstånd innebär därmed ett skärpt krav. Artikel 26.10 innehåller inte någon begränsning i fråga om vilka brott som tekniken får användas för att utreda, till skillnad från AI-förordningens reglering om

användning av AI-system för biometrisk fjärridentifiering i realtid. Skälen till den begränsningen är att användning av teknik för realtidsidentifiering som utgångspunkt är förbjuden och endast får användas när det är strikt nödvändigt för att uppnå ett väsentligt allmänintresse vars betydelse är större än riskerna för de grundläggande rättigheterna. Endast allvarliga brott motiverar att tekniken används (jfr skäl 33 i AI-förordningen). I denna promemoria föreslås att AI-system för biometrisk fjärridentifiering i efterhand endast ska få användas när det är proportionerligt, vilket innebär att det vid tillståndsprövningen bl.a. kan få betydelse vad det är för typ av brottslighet det är fråga om (se avsnitt 5.2). Av artikel 26.10 tredje stycket framgår också att inget beslut som har negativa rättsföljder för en person får fattas enbart på grundval av utdata från ett AI-system för biometrisk fjärridentifiering i efterhand. Det gäller både för sådan användning som enligt artikeln är tillståndspliktig och för sådan som inte kräver tillstånd. Förordningen ger alltså inte utrymme för annat än att tekniken får användas som stöd i den brottsbekämpande verksamheten. Ett sådant tekniskt stöd kan alltså leda till bl.a. effektivare utredningar och att fler brott kan klaras upp (jfr Statskontorets rapport Myndigheterna och AI, s. 27). Det finns därför inga skäl att begränsa användningen mer än vad som följer av artikel 26.10 i AI-förordningen och de krav som i övrigt gäller för sådana högrisksystem.

I en inledande bestämmelse bör framgå att lagen innehåller bestämmelser om tillståndsförfarandet vid viss användning av AI-system för biometrisk fjärridentifiering i efterhand och att den kompletterar AI-förordningen. Eftersom artikel 26.10 i AI-förordningen är direkt tillämplig behöver inte återges vad som anges i den bestämmelsen i den nya lagen. De kompletterande bestämmelserna bör uttryckligen avgränsas till det tillämpningsområde som följer av nämnda artikel. Såsom beskrivs i avsnitt 3.2.3 innebär det att bestämmelserna bör reglera tillståndsförfarandet vid viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål. Av de kompletterande bestämmelserna bör det framgå att myndigheterna får ges sådant tillstånd att använda AI-system som avses i artikel 3.43 i AI-förordningen när det krävs enligt artikel 26.10 i AI-förordningen. På så sätt framgår att lagen endast reglerar sådan användning som är tillståndspliktig enligt artikel 26.10.

5.2 Användningen måste vara proportionerlig

Förslag: För tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand ska det krävas att 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.

Skälen för förslaget: Enligt artikel 26.10 första stycket i AI-förordningen ska varje användning av AI-system för biometrisk fjärridentifiering i efterhand begränsas till vad som är absolut nödvändigt för att utreda ett specifikt brott. Det följer direkt av bestämmelsen och behöver därför inte anges i den föreslagna lagen. Kravet på absolut nödvändighet i AI-förordningen bör i första hand tolkas som ett krav på rimliga begränsningar avseende t.ex. tid eller material. Bestämmelsen ger uttryck för att det krävs ingående bedömningar av om användningen verkligen är nödvändig. Ett motsvarande krav gäller även för den personuppgiftsbehandling som sker när tekniken används. Enligt 2 kap. 12 § brottsdatalagen får polisen och Tullverket behandla biometriska uppgifter, förutsatt att behandlingen är absolut nödvändig för ändamålet med behandlingen. Bestämmelsen blir tillämplig på den behandling av personuppgifter som sker när polisen och Tullverket använder tekniken. Detta gäller även i de fall användningen enligt artikel 26.10 inte är tillståndspliktig (jfr skäl 94 i AI-förordningen). Att användning av AI-tekniken bedöms absolut nödvändig för polisen eller Tullverket inom ramen för en tillståndsprocess enligt den nya lagen framtar alltså inte myndigheten ansvaret att själv göra motsvarande bedömning av nödvändigheten i att behandla biometriska personuppgifter – en annan sak är att även denna bedömning i regel kommer att landa i samma slutsats. Personuppgiftsbehandlingen måste förstås även uppfylla övriga dataskyddsrättsliga krav.

Utöver att användningen ska begränsas till vad som är absolut nödvändigt ska det även vara proportionerligt att använda tekniken i det specifika fallet. Av skäl 95 till AI-förordningen framgår att system för biometrisk fjärridentifiering i efterhand alltid bör 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. Att användningen av tekniken ska vara proportionerlig följer även av bl.a. artikel 8.2 Europeiska konventionen om mänskliga rättigheter och 2 kap. 21 § regeringsformen.

Kravet på proportionalitet bör komma till uttryck i den nya lagen. Proportionalitetskravet bör utformas som att tekniken endast får användas 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 den riktar sig mot (jfr prop. 2022/23:126 s. 177). Vid avvägningen ska samtliga relevanta omständigheter beaktas. Det ska finnas ett påtagligt behov av att använda tekniken och andra möjligheter ska bedömas vara utsiktslösa, medföra en orimligt stor arbetsinsats eller ta för lång tid. Vid bedömningen måste beaktas att åtgärden kan påverka andra än den eftersökte. Det bör även beaktas bl.a. vad det är för typ av brottslighet, eventuellt utdömd påföljd samt vilken geografisk och tidsmässig omfattning det är på materialet som den aktuella begäran om tillstånd avser.

5.3 Beslut om tillstånd ska fattas av allmän åklagare

Förslag: Allmän åklagare ska pröva en begäran om tillstånd från Polismyndigheten, Säkerhetspolisen eller Tullverket, när ett sådant krävs enligt artikel 26.10 i AI-förordningen. Ett beslut om tillstånd ska gälla omedelbart.

Skälen för förslaget

En begäran om tillstånd enligt artikel 26.10 i AI-förordningen att använda AI-system för biometrisk fjärridentifiering i efterhand ska enligt bestämmelsen prövas av en rättslig myndighet eller en administrativ myndighet vars beslut är bindande och föremål för rättslig prövning.

Användning av AI-system för biometrisk fjärridentifiering i efterhand utgör en polisiär utredningsmetod. När det gäller polisiära utredningsåtgärder är utgångspunkten i svensk rätt att åklagare beslutar om sådana i de fall polisen, och i förekommande fall Tullverket, inte själv bör göra det (se t.ex. prop. 2024/25:37 s. 142 om biometriska registerjämförelser). Från den 1 juli 2025 får t.ex. dna-baserad släktforskning användas i vissa brottsutredningar efter ett tillstånd av åklagare (se prop. 2024/25:37 s. 160 f.). Användning av AI-system för biometrisk fjärridentifiering i efterhand aktualiserar liknande typer av skyddsintressen och kommer inte sällan kräva att frågan om tillstånd kan avgöras snabbt. Det talar för att välja åklagare som prövningsinstans, under förutsättning 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).

Åklagare är i en svensk och EU-rättslig kontext att betrakta som en rättslig myndighet. De agerar självständigt i förhållande till den verkställande makten och ska vara objektiva. Exempelvis har Sverige inom ramen för överlämnande till Sverige enligt en europeisk arresteringsorder angett svensk åklagare både när det gäller en europeisk arresteringsorder och en europeisk utredningsorder.

Åklagare bör därmed kunna besluta om tillstånd till användning av AI-system för biometrisk fjärridentifiering i efterhand i en förundersökning eller andra situationer som kräver tillstånd enligt artikel 26.10 i AI-förordningen. Det är också mest ändamålsenligt att åklagaren fattar sådana beslut då det är fråga om en polisiär utredningsmetod. Alternativet att domstol skulle fatta beslut om tillstånd bedöms inte lämpligt då tillståndsprocessen skulle behöva omgärdas av fler regler, bl.a. om förfarandet i domstolen, och därmed riskera att bli mer tidskrävande. Användning av tekniken innebär inte heller ett sådant integritetsintrång som motiverar en domstolsprocess. Åklagaren bör därmed pröva frågan om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand.

Av 7 kap. 8 § rättegångsbalken framgår att det, utöver allmänna åklagare, även finns särskilda åklagare. En särskild åklagare är bl.a. tullåklagare som får föra talan i mål om vissa brott (jfr 9 kap. 1 §

tullbefogenhetslagen [2024:710]). Frågan är om en tullåklagare bör kunna fatta beslut om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand. Tullåklagarens befogenheter är emellertid begränsade. Vid en tillståndsprövning enligt 26.10 i AI-förordningen gör sig liknande skyddsskäl gällande som vid tillstånd till användning av dna-baserad släktforskning och AI-system för biometrisk fjärridentifiering i realtid. Det är alltså fråga om kvalificerade rättsliga ställningstaganden. Till detta ska läggas att behovet av en enhetlig praxis på området innebär att det bör vara samma aktör som prövar alla tillstånd för de myndigheter som omfattas av lagens tillämpningsområde. En begäran om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand bör därför endast kunna prövas av allmän åklagare, dvs. åklagare vid Åklagarmyndigheten och Ekobrottsmyndigheten. Detta bör framgå av en bestämmelse i den nya lagen.

Till skillnad från om ett beslut om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand meddelats av en administrativ myndighet vars beslut är bindande, uppställs det inget krav i artikel 26.10 på att ett sådant beslut ska kunna överklagas när det meddelats av en rättslig myndighet. När tekniken används utgör det en polisiär utredningsmetod där redan tillgängligt material bearbetas med stöd av ett AI-system i stället för en fullständig manuell granskning av en polis- eller tulltjänsteman. Eftersom användning av tekniken innebär att personuppgifter behandlas kommer den enskildes rättigheter, precis som när tekniken används i dagsläget, tillgodoses bl.a. genom de möjligheter som finns att begära rättelse, radering eller begränsning av behandlingen av personuppgifterna enligt 4 kap. 9 och 10 §§ brottsdatalagen. Det innebär bl.a. att den enskilde kan överklaga ett beslut från en myndighet att inte vidta rättelse eller att radera en uppgift och att 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). Det bör därför inte införas en möjlighet att överklaga åklagarens beslut om tillstånd. Detta innebär att ett beslut om tillstånd för polisen eller Tullverket att använda AI-system för biometrisk fjärridentifiering i efterhand gäller omedelbart, vilket bör framgå i den nya lagen.

Av artikel 26.10 i AI-förordningen följer att ett tillstånd ska begäras på förhand eller utan oskäligt dröjsmål och senast inom 48

timmar. Det kan undantagsvis tänkas förekomma situationer när användning av tekniken påbörjas och avslutas inom 48 timmar exempelvis på grund av att syftet med användningen uppnåtts eller att det av annan anledning inte längre är aktuellt att använda tekniken. Av artikel 26.10 andra stycket följer att polisen eller Tullverket även i en sådan situation ska begära ett tillstånd hos åklagaren.

5.4 Beslutets innehåll

Förslag: Ett beslut om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand ska innehålla uppgift om vilken person och vilket eller vilka brott eller brottsmisstankar, samt vilket material tillståndet gäller.

Skälen för förslaget: Vissa krav måste vara uppfyllda när AI-system för biometrisk fjärridentifiering i efterhand ska användas på ett sätt som är tillståndspliktigt enligt artikel 26.10 i AI-förordningen. För att säkerställa att användningen i varje enskilt fall uppfyller dessa krav bör åklagarens beslut innehålla vissa uppgifter. Den nya lagen bör därför innehålla en bestämmelse som reglerar vad ett beslut om tillstånd ska innehålla. Det bör till att börja med krävas att det i beslutet anges vilken person som tillståndet avser. Eftersom den person som användningen avser kan vara okänd bör det inte alltid krävas att det i beslutet anges identiteten på personen. Det måste dock på något sätt framgå vilken person som avses eftersom en förutsättning enligt artikel 26.10 är att användningen sker på ett målinriktat sätt för att söka efter en person som är misstänkt eller dömd för brott. Det kan t.ex. ske genom att det i beslutet anges att det rör en oidentifierad person som är misstänkt för ett visst brott vid en viss tidpunkt. Om identiteten är känd bör det alltid anges i beslutet.

När tillståndet gäller användning för att söka efter en misstänkt person bör också krävas att det anges vilken eller vilka brottsmisstankar som avses. Ska sökningen i stället göras efter en person som är dömd för brott bör det på motsvarande sätt framgå vilket eller vilka brott som tillståndet avser – i regel genom angivande av brottmålsdomen eller domarna. Det bör även anges vilket material

tillståndet avser. För användning av AI-system för biometrisk fjärridentifiering i realtid gäller enligt artikel 5.2 i AI-förordningen att användningen ska begränsas till vad som är strikt nödvändigt när det gäller bl.a. tidsperioden och det geografiska tillämpningsområdet. Något krav motsvarande det i artikel 5.2 finns inte i artikel 26.10. Användning av AI-system för biometrisk fjärridentifiering i efterhand måste dock vara absolut nödvändig och proportionerlig. Det är alltså viktigt att beslutet om tillstånd avgränsar vilket material, exempelvis vilket kameramaterial, som tekniken får användas på. I den mån det är möjligt bör det framgå i beslutet från vilken eller vilka geografiska platser och vilken tidsperiod materialet härrör.

5.5 Om en begäran om tillstånd nekas

Förslag: En bestämmelse ska tas med i den nya lagen som hänvisar till artikel 26.10 andra stycket, där det framgår vad som gäller när en begäran om tillstånd nekas när användning av AI-system för biometrisk fjärridentifiering i efterhand redan har påbörjats.

Skälen för förslaget: Av artikel 26.10 andra stycket i AI-förordningen framgår att om ett tillstånd som begärts 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. Det bör innebära att resultatet av behandlingen av bildmaterialet som AI-systemet utfört ska raderas, och inte materialet som sådant eller referensdatabasen. Eftersom bestämmelsen är direkt tillämplig och inte förutsätter någon kompletterande nationell reglering bör det i den nya lagen tas in en bestämmelse som hänvisar till denna.

5.6 Det saknas behov av en underrättelseskyldighet

Bedömning: Det saknas behov av att införa en skyldighet att underrätta den som har varit föremål för ett tillstånd enligt den nya lagen om åtgärden.

Skälen för bedömningen: Vid hemliga tvångsmedel ska som huvudregel en enskild underrättas om att den varit föremål för åtgärden, även om det finns vissa undantag (se t.ex. 27 kap. 31–33 §§ rättegångsbalken och 16 § lagen [2007:979] om åtgärder för att förhindra vissa särskilt allvarliga brott). En underrättelseskyldighet har vidare föreslagits avseende möjligheten för polisen att använda AI-system för ansiktsgenkänning och annan biometrisk fjärridentifiering i realtid på allmän plats för brottsbekämpande ändamål (se avsnitt 12 i lagrådsremissen Polisens användning av AI för ansiktsgenkänning i realtid).

Frågan är om det bör införas en underrättelseskyldighet även i förslaget till ny lag om viss användning av AI-system för biometrisk fjärridentifiering i efterhand. I AI-förordningen regleras en skyldighet för tillhandahållare av bl.a. de AI-system som omfattas av artikel 26.10 att informera fysiska personer om att de är föremål för användning av AI-system med hög risk (artikel 26.11). För AI-system som används för brottsbekämpande ändamål gäller genom en hänvisning i artikeln i stället en informationsskyldighet enligt vad som framgår av artikel 13 i dataskyddsdirektivet (se även skäl 93). Artikel 13 har i svensk rätt implementerats genom bestämmelser i brottsdatalagen. Av 4 kap. 1 § brottsdatalagen följer en mer allmän informationsskyldighet. Det rör sig om en skyldighet att på lämpligt sätt, t.ex. genom information på myndighetens hemsida, informera om exempelvis dataskyddsombudets kontaktuppgifter och möjligheten att lämna in klagomål till tillsynsmyndigheten. Av 4 kap. 2 § brottsdatalagen följer vidare en skyldighet för en personuppgiftsansvarig att i enskilda fall lämna ut viss information till en registrerad så att den ska kunna ta till vara sina dataskyddsrättsliga rättigheter. Båda dessa bestämmelser utgör en del av implementeringen av artikel 13 i dataskyddsdirektivet.

Att utöver en sådan allmän – och i enskilda fall specifik – informationsskyldighet införa en generell underrättelseskyldighet framstår inte som motiverat. En sådan skyldighet syftar typiskt sett

till att uppmärksamma en enskild på att staten använt sig av ett för den enskilde ingripande verktyg som den i regel inte har någon vetskap om. Användning av AI-system för biometrisk fjärridentifiering i efterhand kan inte jämföras med ett hemligt tvångsmedel och kan därmed inte anses utgöra ett sådant ingripande verktyg, utan är i stället ett utredningsverktyg som framför allt medför effektivitetsvinster för olika brottsbekämpande myndigheter. Vid användning av AI-system för biometrisk fjärridentifiering i efterhand samlas inte heller något nytt material in utan AI-systemet används för hantering av befintligt material. Verktöget skiljer sig väsentligt även mot föreslagna ordning för AI-system för ansiktsgenkänning och annan biometrisk fjärridentifiering i realtid. Skillnaden mellan AI-system för biometrisk fjärridentifiering i efterhand och AI-system för ansiktsgenkänning och annan biometrisk fjärridentifiering i realtid framgår också direkt av AI-förordningen, där det föregående som regel är tillåtet men kräver ett tillståndsförfarande men där det senare som utgångspunkt är förbjudet (artikel 5.1 h). Det kan i sammanhanget också noteras att AI-system för biometrisk fjärridentifiering i efterhand redan används som ett hjälpmedel av Polismyndigheten, utan att vara förenad med en underrättelseskyldighet. Sammantaget finns det inte tillräckliga skäl att föreslå en underrättelseskyldighet i den nya lagen.

5.7 Förslagets förenlighet med grundläggande fri- och rättigheter

Bedömning: Användning av tekniken är ett effektivt verktyg i brottsbekämpningen och utgör ett godtagbart intrång i den enskildes skydd för sin personliga integritet och sitt privatliv.

Skälen för bedömningen: Vid framtagandet av AI-förordningen har syftet bl.a. varit att säkerställa ett enhetligt skydd för grundläggande rättigheter enligt EU:s rättighetsstadga, inte minst vid användning av högrisksystem som exempelvis biometrisk fjärridentifiering i efterhand (se bl.a. skäl 7 i AI-förordningen). Artikel 26.10 är således ett resultat av EU-lagstiftarens avvägning mellan medlemsstaternas behov av att kunna använda AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål i vissa

fall och det intrång i de fri- och rättigheter som skyddas i EU:s rättighetsstadga som användningen utgör. Användning av tekniken berör flera grundläggande fri- och rättigheter, bl.a. skyddet för den personliga integriteten och rätten till privatliv. Utöver EU:s rättighetsstadga skyddas dessa rättigheter även av bl.a. regeringsformen och Europakonventionen (se vidare avsnitt 4.1). Begränsningar i dessa fri- och rättigheter får endast ske genom lag och för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Det krävs även att begränsningen är nödvändig och proportionerlig (2 kap. 21 § regeringsformen 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.

Artikel 26.10 i AI-förordningen uppställer ett krav på tillstånd för viss användning av AI-system för biometrisk fjärridentifiering i efterhand och föreskriver även att viss typ av användning är otillåten. Förslagen som lämnas i denna promemoria innebär att polisen och Tullverket kommer att kunna använda tekniken på det sätt som artikel 26.10 medger, dvs. för att söka efter en person som är misstänkt för eller dömd för brott när det sker på ett målinriktat sätt.

I avsnitt 5.1 redogörs närmare för polisens och Tullverkets behov av att kunna använda AI-system för biometrisk fjärridentifiering i efterhand. Tekniken är ett sådant effektivt verktyg som ger polisen och Tullverket bättre möjligheter att bedriva sin brottsbekämpande verksamhet. Även den brottslighet som Tullverket har att utreda är i många fall mycket allvarlig i form av t.ex. smuggling av narkotika, vapen och explosiva varor. Den olagliga narkotikahandeln äventyrar såväl människors hälsa och livskvalitet som staters lagliga ekonomi, stabilitet och säkerhet. Den för med sig även annan, ofta grov, brottslighet och utgör en bas för organiserad brottslighet (se prop. 2015/16:111 s. 18). Tillgången till explosiva varor och skjutvapen utgör många gånger en förutsättning för att grova våldsbrott ska komma till stånd och ökar också risken för att en uppkommen våldssituation ska få svåra följder (se prop. 2016/17:92 s. 9). Genom smuggling förses kriminella grupperingar med en stor del av de vapen som används vid skjutningar och den narkotika som säljs i landet. Det finns ett mycket starkt samhällsintresse av att bekämpa denna typ av brottslighet. För att kunna göra det är det nödvändigt

att både polisen och Tullverket ges möjlighet att på ett effektivt sätt bedriva sin brottsbekämpande verksamhet. Detta är ett ändamål som är godtagbart i ett demokratiskt samhälle och som väger tungt i förhållande till enskildas intresse av rätten till skydd för privat- och familjelivet.

När AI-system för biometrisk fjärridentifiering i efterhand används granskas ett redan insamlat material av systemet i stället för att en fullständig manuell granskning görs av en polis- eller tulltjänsteman. Bestämmelserna i artikel 26.10 i AI-förordningen och de förslag som lämnas i denna promemoria innebär att en åklagare kommer att bedöma om det är absolut nödvändigt och proportionerligt att använda tekniken när det sker på ett sätt som är tillståndspliktigt enligt artikel 26.10. Därutöver kommer polisen och Tullverket behöva göra en bedömning av om det är förenligt med det dataskyddsrättsliga regelverket att använda tekniken. Tekniken används redan av polisen och utgör en mycket effektiv utredningsmetod som sparar in tusentals timmar av manuellt granskningsarbete och ökar kvaliteten på analysarbetet, samtidigt som spridningen av uppgifterna minimeras vilket innebär ett mindre integritetsintrång för den enskilde. Användningen sker i dagsläget med stöd av det dataskyddsrättsliga regelverket. Regleringen innebär bl.a. att vissa skyddsåtgärder måste vidtas och att personuppgifter måste behandlas på sådant sätt att risken för diskriminering och felaktig identifiering minimeras. Enligt dataskyddsregleringen får biometriska uppgifter endast behandlas när det är absolut nödvändigt (se 2 kap. 12 § brottsdatalagen, 2 kap. 4 § polisens brottsdatalag och 2 kap. 4 § Tullverkets brottsdatalag). 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. Den dataskyddsrättsliga regleringen utgör ett omfattande skydd för den enskildes personliga integritet. Artikel 26.10 och den nu föreslagna lagen innebär ett skärpt krav på användningen i vissa fall jämfört med i dag, vilket ytterligare stärker den enskildes rättssäkerhet och skyddet för den enskildes personliga integritet och rätt till privatliv.

Artikel 26.10 tredje stycket föreskriver att beslut som har negativa rättsliga följder för en person inte får fattas enbart på grundval av utdata från AI-system för biometrisk fjärridentifiering i efterhand. Det innebär att systemet enbart kan fungera som ett stöd

i utredningsarbetet och att en viss mänsklig kontroll alltid måste ske. Vidare ska årliga rapporter av användningen lämnas till dataskyddsmyndigheten och marknadskontrollmyndigheten – som föreslås bli Integritetsskyddsmyndigheten (se avsnitt 6.2). Användningen ska även dokumenteras i den berörda akten i ärendet hos polisen eller Tullverket samt på begäran göras tillgänglig för den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten (se artikel 26.10 femte och sjätte stycket). Detta möjliggör insyn och därigenom en effektiv kontroll över hur tekniken används. Integritetsskyddsmyndigheten kan vidare på ett bättre sätt uppfylla sitt uppdrag som tillsynsmyndighet över personuppgiftsbehandlingen.

AI-system för biometrisk fjärridentifiering i efterhand måste även uppfylla AI-förordningens övriga krav på högrisksystem, däribland krav på riskhanteringssystem och dokumentation (se bl.a. artikel 9 och 49).

Precis som när polisen använder tekniken i dag kommer Riksdagens ombudsmän (JO) och Justitiekanslern inom ramen för sin respektive tillsyn, kunna uttala sig i frågor om användningen av tekniken. När tekniken används för att söka efter 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.

I sammanhanget bör även beaktas att när en kamera har satts upp med stöd av 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 biometrisk fjärridentifiering i efterhand, ska användas. Detta innebär att skyddet för den enskildes personliga integritet i sådana fall har beaktats redan när kameran sattes upp. Utöver att sådana hänsyn i dessa fall redan tagits kommer användningen av AI-system för biometrisk fjärridentifiering i efterhand kräva ändringar i offentlighets- och sekretesslagen (2009:400) som innebär att spridning av uppgifter hänförliga till användningen begränsas.

AI-förordningen innehåller inte något förbud mot att tillåta användning av AI-system för biometrisk fjärridentifiering i efterhand för att utreda brott som har begåtts av barn eller för att hitta barn som dömts för brott. Det föreslås inte heller någon sådan

begränsning 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. Dessa risker vägs dock upp av det angelägna ändamålet att polisen och Tullverket har effektiva verktyg för att utreda brott även i de fall det är fråga om ett barn som har begått brottet. I sammanhanget bör beaktas den oroande samhällsutveckling som har skett där barn i större utsträckning begår allvarliga brott. Den föreslagna regleringen bedöms därmed vara förenlig med barnkonventionen, däribland principen om barnets bästa.

Sammantaget bedöms en reglering som medger att AI-system för biometrisk fjärridentifiering i efterhand får användas på det sätt som artikel 26.10 tillåter vara förenlig med grundläggande fri- och rättigheter.

6 Behovet av följdändringar

6.1 Det krävs ändringar i offentlighets- och sekretesslagen

Förslag: Sekretess ska gälla för uppgift som hänför sig till angelägenhet som avser användning av AI-system för biometrisk fjärridentifiering i efterhand 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.

Skälen för förslaget: I ärenden enligt den nya lagen kommer det att finnas uppgifter som, om de blir offentliga, kan äventyra syftet med användningen av tekniken. Förutom uppgifter i förhållande till enskilda personer kan det också handla om uppgifter som skulle kunna äventyra pågående brottsutredningar. Det kan bl.a. komma att finnas känsliga uppgifter om enskilda personer. Polisen, Tullverket och åklagaren kommer alltså hantera uppgifter inom ramen för ett ärende som behöver skyddas.

Frågan är då om det med anledning av detta finns behov av att införa en ny reglering i offentlighets- och sekretesslagen. Enligt den nya lagen krävs tillstånd för användning av tekniken 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. Den sekretess som gäller hos myndigheterna för uppgifter som hänför sig till förundersökning i brottmål regleras i 18 kap. 1 § och 35 kap. offentlighets- och sekretesslagen. Av 18 kap. 1 § andra stycket 2 följer att sekretess även gäller för uppgifter i verksamhet hos bl.a.

Polismyndigheten som inte rör förundersökning men som syftar till att förebygga, uppdaga, utreda eller beivra brott. Sådan sekretess till skydd för det allmännas intresse anses omfatta uppgifter i ärenden som rör användning av teknik för att utreda ett brott, t.ex. teknik för ansiktsgenkänning. I vissa fall anses 18 kap. 1 § offentlighets- och sekretesslagen gälla även för uppgifter i ett ärende som rör användning av tekniken för att söka efter personer som dömts för att ha begått ett brott. Detta gäller dock endast i den mån uppgifterna har generell betydelse för spaning och brottsutredning (jfr RÅ 1989 ref. 56). För att ändamålet med användningen av tekniken inte ska gå förlorat bedöms det viktigt att uppgifter i ett tillståndsärende om användning av tekniken omfattas av sekretess, oavsett om användningen sker för att söka efter en misstänkt person eller en person som är dömd för brott. Den befintliga sekretessregleringen bedöms inte ge ett tillräckligt tydligt skydd för uppgifter i samtliga ärenden enligt den nya lagen.

Enligt offentlighetsprincipen är huvudregeln offentlighet för uppgifter i allmänna handlingar och alla inskränkningar i offentligheten måste vara motiverade. Rätten att ta del av allmänna handlingar får begränsas endast om det krävs med hänsyn till intresset av att förebygga eller beivra brott eller skyddet för enskildas personliga eller ekonomiska förhållanden (2 kap. 2 § tryckfrihetsförordningen). 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.

Användning av AI-system för biometrisk fjärridentifiering i efterhand utgör dock en polisiär utredningsmetod och det finns därför starka skyddsintressen och behov av att inskränka allmänhetens insyn. Det är därför av vikt att uppgifter om användningen är sekretessreglerade hos berörda myndigheter. Ett tillstånd att använda tekniken motiveras av allmänna intressen i form av att utreda och verkställa straffrättslig påföljd för brott. Det finns ett starkt allmänt intresse av att kunna skydda uppgifter i ett sådant ärende. 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 biometrisk fjärridentifiering i efterhand 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. Det bedöms lämpligt och ändamålsenligt att införa en ändring i 18 kap. 1 § offentlighets- och sekretesslagen.

Det föreslås att den sekretess som enligt bestämmelsen gäller för bl.a. uppgift som hänför sig till förundersökning i brottmål, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs, även ska gälla för en uppgift som hänför sig till angelägenhet som avser användning av AI-system för biometrisk fjärridentifiering i efterhand enligt den nya lagen. Sekretessen gäller med ett rakt skaderekvisit, vilket innebär en presumtion för offentlighet. Eftersom sekretess 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.

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).

I en begäran om tillstånd enligt den nya lagen kan känsliga uppgifter om en enskilds personliga förhållanden förekomma varför behovet av skydd är detsamma för enskilda oavsett om tekniken används för att söka efter en misstänkt person eller en person som dömts för brott. Det bör därmed 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 biometrisk fjärridentifiering i efterhand. Sekretess gäller därmed för sådana uppgifter med ett omvänt skaderekvisit, vilket innebär en presumtion för sekretess. För uppgift i en allmän handling gäller

sekretessen enligt 35 kap. 1 § fjärde stycket offentlighets- och sekretesslagen i högst sjuttio år.

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 stycket offentlighets- och sekretesslagen.

I ett annat lagstiftningsärende gällande användning av AI-system för biometrisk fjärridentifiering i realtid föreslås att sekretessen ska begränsa rätten att meddela och offentliggöra uppgifter bl.a. eftersom det annars finns risk för att en gärningsman som begått ett allvarligt brott inte kan lokaliseras eller att ett hot om skada mot människors liv eller säkerhet realiserar. Med beaktande av den restriktivitet som ska gälla vid inskränkningar av meddelandefriheten och då risken att ändamålet går förlorat om uppgifter offentliggörs inte är lika stor vid användning av AI-system för biometrisk fjärridentifiering i efterhand bedöms det inte motiverat att låta sekretessen begränsa meddelarfriheten.

6.2 Integritetsskyddsmyndigheten ska vara marknadskontrollmyndighet

Förslag: Integritetsskyddsmyndigheten ska ansvara för marknadskontroll i fråga om användning av AI-system för biometrisk fjärridentifiering i efterhand.

Skälen för förslaget: Artikel 26.10 sjätte stycket i AI-förordningen uppställer ett krav på att tillhandahållaren 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. Enligt bestämmelsen får rapporterna aggregeras för att täcka mer än en användning. Vidare framgår av bestämmelsens femte stycke att oavsett ändamål eller tillhandahållare ska varje användning av sådana AI-system på begäran göras tillgänglig för den berörda marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten, med

undantag för utlämnande av känsliga operativa uppgifter som rör brottsbekämpning. Det ankommer på varje medlemsstat att utse vilken eller vilka myndigheter som ska vara ansvariga marknadskontrollmyndigheter enligt förordningen (artikel 70.1). System för biometrisk fjärridentifiering i efterhand definieras som AI-system med hög risk (se artikel 6.2 och punkt 1 a i bilaga III). Av artikel 74.8 följer att marknadskontrollmyndigheten för AI-system med hög risk som förtecknas i punkt 1 i bilaga III, i den mån systemen används för brottsbekämpande ändamål, 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 26.10. 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 2–2 a §§ förordningen med instruktion för Integritetsskyddsmyndigheten). Det föreslås därför att Integritetsskyddsmyndigheten utses till marknadskontrollmyndighet i fråga om användning av AI-system för biometrisk fjärridentifiering i efterhand enligt artikel 26.10 i AI-förordningen, vilket alltså överensstämmer med Utredningen om AI-förordningens förslag. Eftersom det följer direkt av bestämmelsen att tillhandahållaren ska lämna in årliga rapporter till marknadskontrollmyndigheten och den nationella dataskyddsmyndigheten om sin användning av AI-system för biometrisk

fjärridentifiering i efterhand bedöms detta inte behöva framgå i den nya lagen.

Vad avser förordningens krav på marknadskontrollmyndighet gällande övriga användningsområden lämnas förslag om detta i betänkandet Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation (SOU 2025:101). I betänkandet föreslås Integritetsskyddsmyndigheten utses till marknadskontrollmyndighet för bl.a. användningsområdet biometri. Oaktat detta förslag bör det framgå av förordningen med instruktion för Integritetsskyddsmyndigheten att myndigheten är marknadskontrollmyndighet för användning av AI-system för biometrisk fjärridentifiering i efterhand. Integritetsskyddsmyndigheten är vidare nationell dataskyddsmyndighet och kommer få del av de årliga rapporterna även i den egenskapen.

6.3 AI-system för biometrisk fjärridentifiering i efterhand och hemlig dataavläsning ska få användas inom det internationella straffrättsliga samarbetet

Förslag: AI-system för biometrisk fjärridentifiering i efterhand och hemlig dataavläsning 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. AI-system för biometrisk fjärridentifiering i efterhand ska också få användas inom ramen för det internationella straffrättsliga samarbetet för bevisinhämtning.

Skälen för förslaget

Överlämnande och utlämning

Brottsligheten blir alltmer gränsöverskridande, 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 befinner sig utanför Sveriges gränser, och att svensk polis effektivt kan lokalisera personer i Sverige som eftersöks av polisen i andra länder.

AI-system för biometrisk fjärridentifiering i efterhand är en mycket effektiv utredningsmetod. Genom den föreslagna lagen kommer den svenska polisen och Tullverket kunna ges tillstånd att använda tekniken bl.a. för att lokalisera såväl misstänkta som dömda personer, vilket vanligen görs i syfte att verkställa ett beslut om anhållning, häktning eller en straffrättslig påföljd. Det bör vara möjligt att använda samma utredningsåtgärd inom ramen för det internationella straffrättsliga samarbetet i syfte att lokalisera 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. 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 biometrisk fjärridentifiering i efterhand bör också kunna tillämpas för att lokalisera någon som häktats i ett överlämnings- eller utlämningsärende i syfte att verkställa frihetsberövandet eftersom detta sker i syfte att lokalisera någon 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.

AI-system för biometrisk fjärridentifiering i efterhand är närmast att likna vid en polisiär utredningsmetod inom ett område som inte tidigare har reglerats och bestämmelserna placeras i en ny lag. Det krävs därför 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 biometrisk fjärridentifiering i efterhand för att lokalisera någon som anhållits eller häktats i ett ärende om utlämning eller överlämnande i syfte att verkställa frihetsberövandet. Användningen bör ske enligt de förutsättningar som anges i den nya lagen.

Hemlig dataavläsning vid överlämnande och utlämning

Användning av AI-system för biometrisk fjärridentifiering i efterhand kompletterar de åtgärder som brottsbekämpande myndigheter redan i dag kan använda sig av för att lokalisera personer som är anhållna eller häktade för brott. Hemlig dataavläsning är ett annat sådant verktyg. Enligt 6 c § lagen (2020:62) om hemlig dataavläsning får hemlig dataavläsning användas om det är av synnerlig vikt för att kunna lokalisera någon som är anhållen eller häktad för brott som avses i 27 kap. 19 b § andra stycket rättegångsbalken och åtgärden syftar till att möjliggöra verkställighet av frihetsberövandet. Bestämmelsen kan användas för att lokalisera någon som är anhållen eller häktad även i ett utlämnings- eller överlämnandeärende (se prop. 2023/24:108 s. 45–

46. Eftersom den bestämmelsen är placerad i en särskild lag och inte i rättegångsbalken skulle dock oklarheter om detta kunna uppstå vid tillämpningen. Det finns därför skäl att tydliggöra att bestämmelsen kan tillämpas även i ärenden om utlämning eller överlämnande. Det bör därför införas en ny bestämmelse i lagarna om utlämning och överlämnande som klargör det. Användningen bör ske enligt de förutsättningar som anges i lagen om hemlig dataavläsning.

Bevisinhämtning

Bevisinhämtning i en annan stat eller i Sverige under en pågående brottsutredning är många gånger av stor betydelse, bl.a. vid utredning av grov organiserad brottslighet. Med anledning av det bör det vara möjligt att på samma sätt som i en svensk förundersökning använda AI-system för biometrisk fjärridentifiering i efterhand 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 biometrisk fjärridentifiering i efterhand för bevisinhämtning.

Användning av AI-system för biometrisk fjärridentifiering i efterhand 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. Rättslig hjälp med användning av AI-system för biometrisk fjärridentifiering i efterhand ska lämnas under de förutsättningar som gäller för åtgärden i en svensk utredning (2 kap. 1 § första stycket). 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 §).

En ansökan om rättslig hjälp för användning av AI-system för biometrisk fjärridentifiering i efterhand för någon som befinner sig i Sverige bör handläggas av åklagare. 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, när det gäller en ansökan om hemliga tvångsmedel, 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. AI-system för biometrisk fjärridentifiering i efterhand är visserligen inte ett hemligt tvångsmedel men för det fall andra stater kräver ett domstolsbeslut bör en regel införas i lagen om internationell rättslig hjälp i brottmål som ger domstol möjlighet att i en sådan situation pröva frågan om användning av AI-system för biometrisk fjärridentifiering i efterhand.

För att omfattas av lagen om en europeisk utredningsorder bör användning av AI-system för biometrisk fjärridentifiering i efterhand 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. Det bör dessutom ställas upp ett krav på dubbel straffbarhet, dvs. den gärning som avses i den utländska brottsutredningen ska vara straffbar i Sverige (3 kap. 14 §).

6.4 Det behöver inte göras någon ändring i befintlig dataskyddsreglering

Bedömning: Det behövs inte någon ytterligare reglering för den personuppgiftsbehandling som författningsförslagen ger upphov till.

Skälen för bedömningen

Det finns rättslig grund för personuppgiftsbehandlingen

Polisen använder i dag ansiktsgenkänningsteknik med hjälp av AI i sin brottsbekämpande verksamhet. Användningen sker med stöd av det dataskyddsrättsliga regelverket. Brottsdatalagen innehåller övergripande och grundläggande bestämmelser om brottsbekämpande myndigheters behandling av personuppgifter. Enligt lagen, som genomför dataskyddsdirektivet, får Polismyndigheten, Säkerhetspolisen och Tullverket i sin brottsbekämpande verksamhet 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). För Säkerhetspolisen gäller lagen i den brottsbekämpande verksamheten som inte avser nationell säkerhet. 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. För Tullverkets del finns en sådan detaljerad reglering i Tullverkets brottsdatalag som gäller för behandling som sker i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa uppbörd. Enligt dessa regleringar får polisen och Tullverket 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 och 2 kap. 1 § Tullverkets brottsdatalag).

Polisen och Tullverket 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 och 2 kap. 4 § Tullverkets brottsdatalag. Bestämmelserna ger stöd för polisen och Tullverket att behandla biometriska uppgifter om det görs för ett syfte som anges i lagen (se 2 kap. 1 § polisens brottsdatalag och 2 kap. 1 § Tullverkets brottsdatalag). Det innebär att det finns rättsligt stöd för polisen och Tullverket att inom ramen för användning av AI-system för ansiktsigenkänning i efterhand behandla biometriska uppgifter om det sker för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda eller lagföra brott. Det är med stöd av denna reglering som polisen i dag använder tekniken i sin brottsutredande verksamhet.

Den föreslagna lagen innebär att AI-system för biometrisk fjärridentifiering i efterhand kan användas för att söka efter en person som har dömts för brott. Det är alltså fråga om att hitta en person i syfte att verkställa en straffrättslig påföljd. 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. Detta 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 promemoria. Det är dock nödvändigt att det finns rättsligt stöd för polisen att behandla biometriska uppgifter även när AI-tekniken används för att verkställa straffrättsliga påföljder. I avsnitt 5.3 föreslås en bestämmelse som innebär att polisen får medges tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand bl.a. för att söka efter en person som dömts för ett brott, dvs. i syfte att verkställa straffrättsliga påföljd. Den föreslagna bestämmelsen bedöms utgöra en sådan särskild föreskrift som möjliggör för polisen att behandla biometriska uppgifter när tekniken används för sådana ändamål.

Det krävs inget undantag från sökförbudet

Enligt 2 kap. 14 § brottsdatalagen är det förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. En fråga som aktualiseras med anledning av den föreslagna lagen är om det krävs ett undantag från detta förbud. Vid införandet av polisens brottsdatalag konstaterades att behandling av biometriska uppgifter i ett ansiktsgenkänningsprogram 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 lagrådsremissen Polisens användning av AI för ansiktsgenkänning i realtid görs därför bedömningen att sådan behandling av biometriska uppgifter som sker med stöd av den däri föreslagna lagen om användning av AI-system för ansiktsgenkänning i realtid för brottsbekämpande ändamål – som inte omfattar sökningar i register – måste ses som en sådan normal behandling av biometriska uppgifter som är tillåten om den är absolut nödvändig för ändamålet med behandlingen (s. 107). Detsamma måste anses gälla den behandling av biometriska uppgifter som sker vid användning av AI-system för biometrisk fjärridentifiering i efterhand enligt den nu föreslagna lagen, i de fall den inte innefattar registersökningar som kan anses syfta till att få fram ett urval av personer. Sådana sökningar träffas nämligen av förbudet i 2 kap. 14 § brottsdatalagen (se prop. 2024/25:37 s. 145 f.). I den mån AI-användning som innefattar

sådana sökningar alls kommer att omfattas av kravet på tillstånd krävs alltså att det görs undantag från sökförbudet. Sådana undantag finns för sökningar i de register som polisen i dag söker i med hjälp av biometriska uppgifter, se t.ex. 6 kap. 5 § och 6 a kap. 5 § polisens brottsdatalog, men saknas för Tullverket. Det är inte avsikten att i denna promemoria utvidga polisens möjligheter eller möjliggöra för Tullverket att – med eller utan användning av AI-tekniken – göra sådana sökningar i register som träffas av brottsdatalogens sökförbud. Det finns därför inte något behov av ett undantag från sökförbudet för att möjliggöra användning av AI-system för biometrisk fjärridentifiering i efterhand enligt artikel 26.10.

7 Ikraftträdande- och övergångsbestämmelser

Förslag: Den nya lagen och följdändringar i andra författningar ska träda i kraft den 1 januari 2027.

Bedömning: Det finns inte behov av övergångsbestämmelser.

Skälen för förslaget och bedömningen: Artikel 26.10 i AI-förordningen börjar tillämpas den 2 augusti 2026 (artikel 113 i AI-förordningen). Av artikel 111.2 i AI-förordningen framgår dock att för högrisksystem som har släppts ut på marknaden eller tagits i bruk före den 2 augusti 2026 gäller förordningens bestämmelser endast om systemet från och med den dagen förändras betydligt när det gäller sin utformning. Vidare framgår att under alla omständigheter ska leverantörer och tillhandahållare av bl.a. AI-system för biometrisk fjärridentifiering i efterhand, som är avsedda att användas av offentliga myndigheter, vidta nödvändiga åtgärder för att uppfylla kraven och skyldigheterna i förordningen senast den 2 augusti 2030. System som redan har tagits i bruk eller släppts ut på marknaden av en offentlig myndighet kan alltså fortsatt användas i dess befintliga form utan krav på tillstånd när det görs på ett målinriktat sätt inom ramen för en utredning för att söka efter en person som misstänks ha begått brott eller som har dömts för att ha begått brott fram till den 2 augusti 2030.

Det är dock angeläget att införa en reglering om en nationell tillståndsprocess för att möjliggöra användning av befintliga system vars utformning förändras i betydande omfattning och nya system som tas i bruk eller släpps ut på marknaden efter den 2 augusti 2026. Den nya lagen och följdändringar i andra författningar föreslås därför träda i kraft den 1 januari 2027.

Eftersom tidpunkten för när kravet på tillstånd ska börja gälla för olika system följer direkt av AI-förordningens bestämmelser bedöms det inte finnas något behov av några övergångsbestämmelser.

8 Konsekvenser av förslagen

8.1 Konsekvenser för det brottsbekämpande arbetet och för enskilda

Bedömning: Förslagen är en förutsättning för att polisen ska kunna fortsätta använda AI-system för biometrisk fjärridentifiering i efterhand i sin brottsutredande verksamhet, när tillstånd krävs för användningen enligt artikel 26.10 i AI-förordningen. Förslagen möjliggör även för polisen att kunna använda ny sådan teknik för att hitta misstänkta personer och personer dömda för brott. Vidare innebär förslagen bättre möjligheter för Tullverket att utreda brott genom att myndigheten föreslås kunna använda tekniken i sin brottsutredande verksamhet. Användning av tekniken utgör en mycket effektiv utredningsmetod. Förslagen utgår från AI-förordningens krav på användning av tekniken och 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 innebär vidare en ökad rättstrygghet för enskilda.

Förslagen är förenliga med principen om barnets bästa.

Skälen för bedömningen

Konsekvenser för det brottsbekämpande arbetet

Förslagen innebär att Polismyndigheten fortsatt kommer att kunna använda teknik som omfattas av AI-förordningens definition av AI-system för biometrisk fjärridentifiering i efterhand, såsom

ansiktsgenkänning, för att bl.a. utreda brott på det sätt som görs i dag och med annan framtida teknik som omfattas av förordningens definition, när tillstånd krävs för användningen enligt artikel 26.10. Polismyndigheten har bedömt att användning av tekniken har sparat in tusentals timmar av manuellt granskningsarbete. Under 2025 har cirka fyra års filmmaterial analyserats varje månad. Det är alltså fråga om en effektiv och resurssparande utredningsmetod. Tekniken har varit viktig i flera utredningar om bl.a. mord och har i vissa fall varit avgörande för att kunna leda utredningen fram till åtal. Användning av AI-system för biometrisk fjärridentifiering i efterhand i en brottsutredning bidrar således till att fler brott kan leda till åtal och fler personer lagföras.

Tullverket har bedömt att om myndigheten får använda tekniken i sin brottsutredande verksamhet skulle fler personer som är intressanta för en utredning kunna identifieras och identifieringen skulle kunna ske snabbare än i dag. Det innebär i sin tur att utredningsarbetet skulle gå fortare och kunna tas vidare till nästa steg tidigare. Det skulle dessutom innebära en stor tidsvinst i förhållande till den manuella granskning som görs i dag och som är mycket tidskrävande.

Genom förslagen kan tekniken även användas för att söka efter dömda personer när tillstånd för sådan användning krävs enligt artikel 26.10. Om fler personer verkställer straffrättslig påföljd kan det leda till minskad brottslighet och ökat förtroende för rättsväsendet.

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 4.2 och 13.2).

De förslag som lämnas om att polisen och Tullverket ska få använda AI-system för biometrisk fjärridentifiering i efterhand

innebär ett intrång i den personliga integriteten och privatlivet, se avsnitt 5.7. Som framgår där bedöms förslagen dock vara förenliga med regeringsformen, Europakonventionen och EU:s rättighetsstadga. Den föreslagna regleringen innebär ett stärkt rättssäkerhetsskydd för den enskilde genom att det införs krav på tillstånd för viss användning av tekniken som syftar till att begränsa integritetsintrånget och möjliggöra en effektivare tillsyn. Genom att använda tekniken kan relevanta uppgifter identifieras i det aktuella materialet, vilket innebär att en manuell granskning endast behöver ske av en mindre mängd information som är av mer direkt intresse för utredningen. Färre polis- eller tulltjänstemän behöver alltså gå igenom allt material manuellt, vilket minskar intrånget i den enskildas integritet och spridningen av personuppgifter.

Förslagen bedöms även leda till minskad brottslighet, både bland barn och vuxna, vilket innebär ett förstärkt skydd för enskildas personliga integritet och bidrar till ökad trygghet för enskilda. Som framgår av avsnitt 5.7 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. Sammantaget innebär förslagen som lämnas i promemorian en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sitt privatliv och sin personliga integritet.

Konsekvenser avseende hemlig dataavläsning

Förslagen om hemlig dataavläsning fastslår en ordning som redan gäller och bedöms därför inte medföra några konsekvenser.

8.2 Ekonomiska konsekvenser

Bedömning: Förslagen om en ny lag kan komma att medföra ökade kostnader för Åklagarmyndigheten. Kostnaderna rymms inom befintliga ekonomiska anslag. De kostnadsökningar som den nya lagen kan medföra för Polismyndigheten, Säkerhetspolisen, Tullverket och Säkerhets- och

integritetsskyddsnämnden samt Integritetsskyddsmyndigheten bedöms bli marginella, och ryms därför inom befintliga anslag.

Övriga förslag bedöms inte medföra några ekonomiska konsekvenser.

Skälen för bedömningen

Konsekvenser för Polismyndigheten och Säkerhetspolisen

Förslagen medför inte någon skyldighet för polisen att använda AI-system för ansiktsgenkänning i efterhand, men möjliggör att tekniken används på det sätt som artikel 26.10 i AI-förordningen medger, vilket till viss del redan görs av Polismyndigheten i dagsläget. Eftersom det är fråga om en ny reglering som utgår från en direkt tillämplig EU-förordning där viss användning är undantagen från kravet på tillstånd har Polismyndigheten svårt att uppskatta i hur stor omfattning myndigheten kommer behöva begära ett tillstånd för att använda tekniken. Vid en grov uppskattning som gjorts av Polismyndigheten bedöms det dock bli aktuellt att begära tillstånd för cirka 50–100 ärenden per vecka. Det bör dock påminnas om att inte all användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål kräver tillstånd enligt AI-förordningen, då framför allt användning för inledande identifiering faller utanför tillämpningsområdet. Vidare gäller för system som släppts ut före den 2 augusti 2026 kravet på tillstånd endast om systemet från och med den dagen förändrats betydligt (se avsnitt 7). För den teknik Polismyndigheten den 2 augusti 2026 redan har i bruk kommer det alltså inte krävas tillstånd förrän den 2 augusti 2030. Dessa omständigheter medför svårigheter avseende uppskattning av antal fall, men det är inte osannolikt att det inledningsvis kan väntas röra sig om relativt få fall där tillstånd krävs. Genom att användningsområdet för befintlig teknik kommer att breddas inom myndigheten och ny teknik tas fram kommer det dock bli aktuellt att söka tillstånd de kommande åren. De kostnadsökningar som förslagen kan medföra bedöms kunna finansieras inom befintliga ekonomiska ramar för Polismyndigheten.

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, och kan därmed finansieras inom befintliga ekonomiska ramar.

Konsekvenser för Tullverket

Förslagen medför inte någon skyldighet för Tullverket att använda AI-system för biometrisk fjärridentifiering i efterhand, men möjliggör att tekniken används på det sätt som artikel 26.10 i AI-förordningen medger. I nuläget använder myndigheten inte tekniken. För att använda tekniken krävs att Tullverket utvecklar nya tekniska lösningar. Eftersom det är fråga om en ny teknik för myndigheten och en ny reglering har Tullverket svårt att bedöma hur ofta under ett år som myndigheten kommer att behöva begära tillstånd för användning av tekniken, men uppskattningsvis kan det enligt myndigheten röra sig om 100–250 ansökningar om tillstånd det första året. Tullverket har uppskattat att antalet därefter stegvis kommer att öka, inom en treårsperiod upp till omkring 1 000 om året.

Konsekvenser för Åklagarmyndigheten

Förslagen medför att Åklagarmyndigheten kommer fatta beslut om biometrisk fjärridentifiering i efterhand när ett sådant tillstånd krävs enligt artikel 26.10 i AI-förordningen. Sådana beslut om tillstånd kommer bli aktuella först när myndigheterna – efter den 2 augusti 2026 – tar i bruk nya system på marknaden eller gör betydande förändringar av befintliga system. De system som Polismyndigheten i nuläget har i drift kommer alltså inte kräva tillstånd för att kunna användas. Det är vidare möjligt att en del av sådan användning inte kommer kräva tillstånd då det rör sig om inledande identifiering. Det är till följd av detta svårt att göra uppskattningar av hur många begäran om tillstånd det på sikt kan antas röra sig om. En grov uppskattning är dock att det eventuellt kan bli relativt många fall per år. Förslaget om att allmän åklagare ska pröva beslut om tillstånd kan därmed på sikt väntas leda till framför allt ökade personalkostnader. De situationer där Polismyndigheten, Säkerhetspolisen eller Tullverket kan väntas begära tillstånd bör dock typiskt sett vara av

sådant slag där allmän åklagare redan i dag har en aktiv roll, inte minst som förundersökningsledare. Mot bakgrund av detta ryms de kostnader som kan tillkomma för Åklagarmyndigheten inom befintliga ekonomiska ramar.

Konsekvenser för Integritetsskyddsmyndigheten

Genom förslaget ska Integritetsskyddsmyndigheten utses till marknadskontrollmyndighet i fråga om användning av AI-system för biometrisk fjärridentifiering i efterhand. Integritetsskyddsmyndigheten utövar redan i dag tillsyn ur ett dataskyddsperspektiv över Polismyndighetens användning av AI-system för biometrisk fjärridentifiering i efterhand. Polismyndighetens användning av sådana AI-system bygger också på ett förhandssamråd mellan myndigheten och Integritetsskyddsmyndigheten. Förslaget i den här promemorian att Integritetsskyddsmyndigheten ska utses till marknadskontrollmyndighet i fråga om användning av AI-system för biometrisk fjärridentifiering i efterhand utgör visserligen en ny uppgift för myndigheten, men är alltså nära besläktad med uppgifter som myndigheten redan har i dag. Som framgår av Integritetsskyddsmyndighetens årsredovisning för 2024 har myndigheten tillsatt en arbetsgrupp som analyserar och hanterar olika delar av AI-förordningen samt genomfört särskilda utbildningsinsatser för chefer och medarbetare för att höja kunskapen om AI och de nya krav som ställs i AI-förordningen.

Förslaget i den här promemorian att Integritetsskyddsmyndigheten ska utses till marknadskontrollmyndighet i fråga om användning av AI-system för biometrisk fjärridentifiering i efterhand kan därför inte väntas leda till mer än begränsade kostnader för myndigheten, och ryms därför inom befintliga anslag. Det föreslås därför att Integritetsskyddsmyndigheten inte ska tillföras ökade resurser till följd av förslagen i den här promemorian.

Konsekvenser för Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden kommer att utöva tillsyn över den personuppgiftsbehandling som utförs av Polismyndigheten och Säkerhetspolisen vid användning av AI-system för biometrisk fjärridentifiering i efterhand. Förslagen innebär således att

omfattningen av nämndens tillsynsuppdrag kommer att öka något. De eventuella kostnadsökningar som det kan leda till bedöms dock vara marginella, och ryms därför inom befintliga ekonomiska anslag.

Konsekvenser avseende övriga förslag

Varken förslagen om att AI-system för biometrisk fjärridentifiering i efterhand ska få användas i det straffrättsliga systemet eller förslagen om hemlig dataavläsning, som fastslår en ordning som redan gäller, bedöms innebära några ekonomiska konsekvenser.

8.3 Övriga konsekvenser

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 straffrättsliga samarbeten. I övrigt bedöms inte förslagen leda till några konsekvenser.

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

Förslagen bedöms bidra till en ökad trygghet i samhället eftersom brott kommer kunna utredas på ett effektivt sätt. 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 eller vid verkställighet av påföljd enligt svenska domar, ska vara möjligt att använda AI-system för ansiktsigenkänning i efterhand 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.

9 Författningskommentar

9.1 Förslaget till lag om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål

1 § I denna lag finns bestämmelser om tillståndsförfarandet vid viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål.

Lagen kompletterar 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.

Paragrafen anger att lagen innehåller bestämmelser om tillståndsförfarandet vid viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål, som kompletterar AI-förordningen. Övervägandena finns i avsnitt 5.1.

Lagen, som är ny, reglerar tillståndsförfarandet för Polismyndighetens, Säkerhetspolisens och Tullverkets användning av AI-system för biometrisk fjärridentifiering i vissa fall. Den användning som avses regleras i artikel 26.10 i AI-förordningen. Bestämmelserna i artikel 26.10 är direkt tillämpliga och reglerar viss användning av AI-system för biometrisk fjärridentifiering i efterhand. Den nya lagen måste därför läsas tillsammans med artikel 26.10.

2 § I artikel 26.10 i AI-förordningen finns bestämmelser om att viss användning av AI-system för biometrisk fjärridentifiering i efterhand kräver tillstånd.

Polismyndigheten, Säkerhetspolisen och Tullverket får ges ett sådant tillstånd.

Paragrafen innehåller en upplysning om att det i artikel 26.10 i AI-förordningen finns bestämmelser om att viss användning av AI-system för biometrisk fjärridentifiering i efterhand kräver tillstånd, och reglerar vilka brottsbekämpande myndigheter som kan ges sådant tillstånd. Övervägandena finns i avsnitt 5.3.

Av första stycket följer att det i artikel 26.10 finns bestämmelser om att viss användning av AI-system för biometrisk fjärridentifiering i efterhand kräver tillstånd. Enligt artikel 26.10 får tillstånd medges när tekniken ska användas på ett målinriktat sätt inom ramen för en utredning för att söka efter en person som misstänks ha begått ett brott eller en person som har dömts för att ha begått ett brott. Tillstånd krävs dock inte när tekniken används för den inledande identifieringen av en potentiell misstänkt på grundval av objektiva och verifierbara fakta med direkt anknytning till brottet. Kravet på tillstånd gäller alltså inte när det är fråga om en tidig identifiering av en misstänkt gärningsperson, när fakta talar för att personen kan misstänkas för brottet. Om den brottsbekämpande myndigheten i stället vill använda tekniken för en målinriktad sökning av en redan identifierad misstänkt, exempelvis för att inom ramen för en förundersökning söka igenom kameramaterial i syfte att kartlägga den misstänktes aktivitet före eller efter det aktuella brottstillfället, fastslå ett händelseförlopp eller en tid eller plats för en gärning krävs däremot ett tillstånd för användningen enligt artikel 26.10 i AI-förordningen. Varje användning ska enligt artikel 26.10 begränsas till vad som är absolut nödvändigt för att utreda ett specifikt brott.

Polismyndigheten, Säkerhetspolisen och Tullverket kan enligt andra stycket ges tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand när sådant tillstånd krävs enligt artikel 26.10 i AI-förordningen.

Av artikel 26.10 följer att ett tillstånd ska begäras på förhand eller utan oskäligt dröjsmål. Av artikeln följer även att ett tillstånd ska begäras även i de fall användning av tekniken påbörjas och avslutas

inom 48 timmar, exempelvis på grund av att syftet med användningen uppnåtts.

3 § Tillstånd får endast medges 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.

I paragrafen anges att viss användning av AI-system för biometrisk fjärridentifiering i efterhand endast får användas om åtgärden är proportionerlig. Övervägandena finns i avsnitt 5.2.

Bestämmelsen innebär att ett tillstånd att använda tekniken endast får medges om det är proportionerligt. Det innebär att det i varje enskilt fall måste 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 riktas mot och för andra än den eftersökte som också kan påverkas av användningen. Vid bedömningen ska samtliga relevanta omständigheter vägas in. Det innebär att hänsyn bl.a. måste tas till vad det är för typ av brottslighet, eventuellt utdömd påföljd samt vilken geografisk och tidsmässig omfattning det är på materialet som den aktuella begäran om tillstånd avser. Konsekvenserna av användningen av tekniken för berörda personers rättigheter och friheter måste också beaktas.

4 § Ett tillstånd enligt 2 § prövas av allmän åklagare.

Paragrafen reglerar vem som ska pröva en begäran om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand och när ett sådant tillstånd ska begäras. Övervägandena finns i avsnitt 5.3.

I paragrafen anges att allmän åklagare ska pröva en begäran om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand. Enligt artikel 26.10 i AI-förordningen är det tillhandahållaren som ska begära ett tillstånd, dvs. Polismyndigheten, Säkerhetspolisen eller Tullverket (jfr 3 §) när det krävs för att använda tekniken. En tillhandahållare är enligt artikel 3.4 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. Det är alltså den som ska använda tekniken i sin brottsbekämpande verksamhet som ska begära ett tillstånd.

- 5 §** *Ett beslut om tillstånd gäller omedelbart. I beslutet ska det anges*
- *vilken person som tillståndet avser,*
 - *vilket eller vilka brott eller brottsmisstankar som tillståndet avser, och*
 - *vilket material som omfattas av tillståndet.*

Paragrafen reglerar vad ett beslut om tillstånd att använda AI-system för biometrisk fjärridentifiering i efterhand ska innehålla. Övervägandena finns av avsnitt 5.4.

Av bestämmelsen framgår att ett beslut om tillstånd gäller omedelbart. Vidare följer att det ska anges vilken person som tillståndet avser. Eftersom den person som användningen avser kan vara okänd krävs det inte alltid att det i beslutet anges identiteten på personen. Det måste dock på något sätt framgå vilken person som avses eftersom en förutsättning enligt artikel 26.10 i AI-förordningen är att användningen sker på ett målinriktat sätt för att söka efter en person som är misstänkt eller dömd för brott. Det kan t.ex. ske genom att det i beslutet anges att det rör en oidentifierad person som är misstänkt för ett visst brott vid en viss tidpunkt. Om identiteten är känd ska det alltid anges i beslutet. När tillståndet gäller användning för att söka efter en misstänkt person ska det i beslutet om tillstånd anges vilken eller vilka brottsmisstankar som avses. Ska sökningen i stället göras efter en person som är dömd för brott ska det på motsvarande sätt framgå vilket eller vilka brott som tillståndet avser – i regel genom angivande av brottmålsdomen eller domarna. Det ska även framgå i beslutet vilket material, exempelvis vilket kameramaterial, som omfattas av tillståndet. I den mån det är möjligt ska det framgå från vilken eller vilka geografiska platser och vilken tidsperiod materialet härrör.

6 § *I artikel 26.10 andra stycket i AI-förordningen finns bestämmelser om förfarandet när ett tillstånd enligt 2 § nekas och användningen av tekniken redan har påbörjats.*

Paragrafen innehåller en upplysning om vad som gäller när användning av AI-system för biometrisk fjärridentifiering i efterhand har påbörjats utan tillstånd och ett sådant tillstånd sedan nekas. Övervägandena finns i avsnitt 5.5.

Av artikel 26.10 andra stycket i AI-förordningen framgår att om ett tillstånd som har begärts 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. Det bör innebära att det som ska raderas endast ska vara resultatet av behandlingen av bildmaterialet som AI-systemet utfört och inte materialet som sådant eller referensdatabasen.

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

16 b § För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål användas i syfte att verkställa frihetsberövandet. Vid sådan användning tillämpas bestämmelserna i den lagen.

Paragrafen, som är ny, innehåller bestämmelser om att viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål får ske i syfte att lokalisera någon som är anhållen eller häktad i ett ärende om utlämning i syfte att verkställa frihetsberövandet. Övervägandena finns i avsnitt 6.3.

AI-system för biometrisk fjärridentifiering i efterhand ska kunna användas för att lokalisera någon som anhållits eller häktats i ett ärende om utlämning 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 utlämning för lagföring eller straffverkställighet. Vid användning av AI-system i dessa fall tillämpas bestämmelserna om tillståndsförfarande i lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål.

16 c § För att lokalisera någon som är anhållen eller häktad i ett utlämningsärende får hemlig dataavläsning enligt 6 c § lagen (2020:62) om hemlig dataavläsning användas. Vid sådan användning tillämpas bestämmelserna i den lagen.

Paragrafen, som är ny, innehåller bestämmelser om att hemlig dataavläsning får användas för att lokalisera någon som är anhållen eller häktad i ett ärende om utlämning för brott. Övervägandena finns i avsnitt 6.3.

Paragrafen innebär att hemlig dataavläsning får användas för att lokalisera personer som har anhållits eller häktas i sin frånvaro i ett ärende om utlämning i syfte att verkställa frihetsberövandet. Vid användning av hemlig dataavläsning tillämpas övriga bestämmelser i lagen om hemlig dataavläsning.

I övrigt hänvisas till författningskommentaren till 6 c § lag om hemlig dataavlyssning (se prop. 2023/24:108 s. 103).

9.3 Förslag 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,
 15. användning av AI-system för ansiktigenkänning eller annan biometrisk fjärridentifiering i realtid, och

16. *användning av AI-system för biometrisk fjärridentifiering i efterhand.*

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 uppräkningslista av vilka åtgärder som omfattas av rättslig hjälp. Övervägandena finns i avsnitt 6.3.

I paragrafens *första stycke* läggs användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål till i uppräkningslistan av åtgärder som omfattas av rättslig hjälp.

2 kap.

1 § Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–10 och 14–16 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 6.3.

Ändringen i *första stycket* innebär att rättslig hjälp i form av användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål kan lämnas under de förutsättningar som gäller för en motsvarande åtgärd enligt svensk rätt. Av lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål följer att det i vissa fall krävs tillstånd för sådan användning, nämligen när användningen omfattas av artikel 26.10 i AI-

förordningen. För annan användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål krävs inte tillstånd enligt lagen men användningen utgör sådan personuppgiftsbehandling som faller in under brottsdatalagen (2018:1177), lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område samt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område. Om det är tillåtet enligt det dataskyddsrättsliga regelverket kan rättslig hjälp i så fall lämnas även i sådana fall. Härtill gäller de särskilda bestämmelserna i 4 kap. 28 k och l §§.

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 och 14–16 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 6.3.

Ändringen innebär att rättslig hjälp i form av användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål endast får lämnas om kravet på dubbel straffbarhet är uppfyllt.

4 kap.

Användning av AI-system för biometrisk fjärridentifiering i efterhand

28 k § *En ansökan om användning av AI-system för biometrisk fjärridentifiering i efterhand av någon som befinner sig i Sverige handläggs av åklagare.*

I paragrafen, som är ny, regleras vem som handlägger en ansökan om rättslig hjälp i form av användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål avseende en person som befinner sig i Sverige. Övervägandena finns i avsnitt 6.3.

Av paragrafen följer att en ansökan om rättslig hjälp om användning av AI-system för biometrisk fjärridentifiering i efterhand av en person som befinner sig i Sverige handläggs av en åklagare.

281 § Om användning av AI-system för biometrisk fjärridentifiering i efterhand 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.

I paragrafen, som är ny, finns en bestämmelse om rättens tillstånd till användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål av någon som finns i utlandet. Övervägandena finns i avsnitt 6.3.

Det är åklagaren som gör en sådan ansökan. Om den anmodade staten kräver ett svenskt domstolsbeslut får rätten dock på begäran av svensk åklagare besluta att tillåta användningen. Eftersom användningen ska verkställas utomlands ska den statens verkställighetsregler tillämpas.

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

4 kap.

3 b § För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål användas i syfte att verkställa frihetsberövandet. Vid sådan användning tillämpas bestämmelserna i den lagen.

Paragrafen, som är ny, innehåller bestämmelser om viss användning av AI-system för biometrisk fjärridentifiering i efterhand i syfte att lokalisera någon som är anhållen eller häktad enligt lagen. Övervägandena finns i avsnitt 6.3.

AI-system för biometrisk fjärridentifiering i efterhand ska kunna användas 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. Vid användning av sådana AI-system tillämpas övriga bestämmelser i lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål, t.ex. om tillståndsprövning.

7 a § För att lokalisera någon som är anhållen eller häktad enligt denna lag får hemlig dataavläsning enligt 6 c § lagen (2020:62) om hemlig dataavläsning användas. Vid sådan användning tillämpas bestämmelserna i den lagen.

Paragrafen, som är ny, innehåller bestämmelser om att hemlig dataavläsning får användas för att lokalisera någon som är anhållen eller häktad i ett ärende enligt lagen. Övervägandena finns i avsnitt 6.3.

Paragrafen innebär att hemlig dataavläsning ska kunna användas för att lokalisera personer som har anhållits eller häktas i sin frånvaro under en pågående utredning om överlämnande för lagföring eller straffverkställighet i syfte att verkställa frihetsberövandet. Vid användning av hemlig dataavläsning tillämpas övriga bestämmelser i lagen om hemlig dataavläsning.

I övrigt hänvisas till författningskommentaren till 6 c § lag om hemlig dataavlyssning (se prop. 2023/24:108 s. 103).

9.5 Förslag 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. 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 *eller enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand 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 6.1.

Ändringen innebär att sekretess gäller för uppgifter som hänför sig till angelägenhet som avser användning av AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand 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 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 innebär även att sekretessen kommer att gälla i annan verksamhet än sådan som avses i bestämmelsen hos en myndighet för att biträda exempelvis en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller Tullverket med att utreda brott (3 §).

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 brottsdatalogens 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 brottsdatalogens 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 brottsdatalogens område eller som annars behandlas där med stöd av samma lag,

10. utredning om självständigt förverkande,

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

12. *angelägenhet som avser användning av AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand 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 utreda brott. Övervägandena finns i avsnitt 6.1.

En ny punkt införs i första stycket som reglerar sekretess för uppgift som förekommer i angelägenhet som avser användning av AI-system enligt lagen (2026:000) om viss användning av AI-system

för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål. Ändringen innebär att sekretess gäller för uppgift som förekommer i angelägenhet som avser användning av AI-system för biometrisk fjärridentifiering i efterhand 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.

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

3 kap.

3 b § För att lokalisera någon som är anhållen eller häktad enligt denna lag får AI-system enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål användas i syfte att verkställa frihetsberövandet. Vid sådan användning tillämpas bestämmelserna i den lagen.

Paragrafen, som är ny, innehåller bestämmelser om viss användning av AI-system för biometrisk fjärridentifiering i efterhand i syfte att lokalisera någon som är anhållen eller häktad enligt lagen. Övervägandena finns i avsnitt 6.3.

Användning av AI-system för biometrisk fjärridentifiering i efterhand ska kunna tillämpas för att lokalisera någon som anhållits eller häktats enligt lagen i syfte att verkställa frihetsberövandet. Det innebär att tekniken får användas för att lokalisera personer som har anhållits eller häktats i sin frånvaro under en pågående utredning om överlämnande för lagföring eller straffverkställighet. Vid användning av AI-system tillämpas övriga bestämmelser i lagen om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål, t.ex. om tillståndsprovning.

8 a § För att lokalisera någon som är anhållen eller häktad enligt denna lag får hemlig dataavläsning enligt 6 c § lagen (2020:62) om hemlig dataavläsning användas. Vid sådan användning tillämpas bestämmelserna i den lagen.

Paragrafen, som är ny, innehåller bestämmelser om att hemlig dataavläsning får användas för att lokalisera någon som är anhållen eller häktad i ett ärende enligt lagen. Övervägandena finns i avsnitt 6.3.

Paragrafen innebär att tekniken ska kunna användas för att lokalisera personer som har anhållits eller häktas i sin frånvaro under en pågående utredning om överlämnande för lagföring eller straffverkställighet i syfte att verkställa frihetsberövandet. Vid sådan användning av hemlig dataavläsning tillämpas övriga bestämmelser i lagen om hemlig dataavläsning.

I övrigt hänvisas till författningskommentaren till 6 c § lag om hemlig dataavlyssning (se prop. 2023/24:108 s. 103).

9.7 Förslag 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 ansiktsgenkänning eller annan biometrisk fjärridentifiering i realtid,

13. användning av AI-system för biometrisk fjärridentifiering i efterhand, eller

14. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.

Paragrafen innehåller en uppräkningslista av de utredningsåtgärder som en europeisk utredningsorder ska avse eller motsvara. Övervägandena finns i avsnitt 6.3.

I paragrafen införs en ny punkt som anger att en utredningsåtgärd enligt lagen ska avse eller motsvara användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål. Det kan röra sig om användning av AI-system som kräver tillstånd för användning enligt lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål. Även annan användning av AI-system för biometrisk fjärridentifiering i efterhand, som inte kräver tillstånd men utgör sådan personuppgiftsbehandling som faller in under brottsdatalagen (2018:1177), lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område samt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område, kan omfattas.

2 kap.

1 § En utredningsorder får utfärdas av åklagare för en utredningsåtgärd som avses i 1 kap. 4 § 1 och 3–14.

I paragrafen anges vilka utredningsåtgärder en utredningsorder kan omfatta i de fall en svensk åklagare utfärdar ordern. Övervägandena finns i avsnitt 6.3.

En punkt läggs till i hänvisningen i paragrafen. Ändringen innebär att en åklagare får utfärda en utredningsorder som omfattar användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål.

3 kap.

4 § En utredningsorder för en åtgärd som avses i 1 kap. 4 § 6, 9, 10, 11, 12 eller 13 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 6.3.

Ändringen i paragrafen innebär att för att kunna erkänna och verkställa en utredningsorder från en annan stat för användning av AI-system för biometrisk fjärridentifiering i efterhand krävs att den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och att övriga förutsättningar är uppfyllda. Övriga förutsättningar finns t.ex. i lagen (2026:000) om viss användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål. Det kan för annan användning av AI-system för biometrisk fjärridentifiering i efterhand, som inte omfattas av nämnda lag, finnas dataskyddsrättsliga förutsättningar för att motsvarande åtgärd i en svensk förundersökning är uppfyllda.

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

3 kap.

6 b § I frågor om användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål tillämpas bestämmelserna i 4 kap. 3 b § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.

Paragrafen, som är ny, innebär att vid viss användning av AI-system för biometrisk fjärridentifiering i efterhand ska 4 kap. 3 b § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder tillämpas. Övervägandena finns i avsnitt 6.3.

Hänvisningen till 4 kap. 3 b § europeiska arresteringsorderlagen innebär att användning av AI-system för biometrisk fjärridentifiering i efterhand för brottsbekämpande ändamål får användas för att lokalisera personer som har anhållits eller häktats i sin frånvaro under en pågående utredning om överlämnande för lagföring eller straffverkställighet i syfte att verkställa frihetsberövandet. I övrigt hänvisas till kommentaren till nämnda bestämmelse i europeiska arresteringsorderlagen.

11 a § I frågor om hemlig dataavläsning tillämpas bestämmelserna i 4 kap. 7a § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder.

Paragrafen, som är ny, innebär att vid hemlig dataavläsning ska 4 kap. 7 a § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder tillämpas. Övervägandena finns i avsnitt 6.3.

Hänvisningen till 4 kap. 7 a § europeiska arresteringsorderlagen innebär att hemlig dataavläsning får användas för att lokalisera personer som har anhållits eller häktats i sin frånvaro under en pågående utredning om överlämnade för lagföring eller straffverkställighet i syfte att verkställa frihetsberövandet. I övrigt hänvisas till kommentaren till nämnda bestämmelse i europeiska arresteringsorderlagen.

Departementsserien 2025

Kronologisk förteckning

1. Hyra anstaltsplatser utomlands. Ju.
2. Moderna – en ny myndighet för modern konst, arkitektur och design. Ku.
3. Sveriges försvarsmaterielförvaltningsdirektör. En ny inriktning. Fö.
4. En ny lag om unga lagöverträdare. Ju.
5. Genomförande av direktivet om skydd för personer som deltar i den offentliga debatten. Ju.
6. En ändamålsenlig hantering av tillstånd och tillsyn av explosiva varor. Fö.
7. Polisens användning av AI för ansiktsgenkänning i realtid. Ju.
8. Administrativa sanktioner i socialförsäkringen. S.
9. Ett nationellt mobilförbud i de obligatoriska skolformerna och fritidshemmet. U.
10. En ändamålsenlig hantering av tillstånd och tillsyn av explosiva varor – slutredovisning. Fö.
11. En tydlig beslutsordning för deltagande i Natos samlade verksamhet för avskräckning och försvar. Fö.
12. Nordisk verkställighet i brottmål. Ju.
13. Rätt att installera laddpunkt hemma. Ju.
14. Kompletterande bestämmelser till EU:s förordning om överföring av straffrättsliga förfaranden. Ju.
15. Nya regler om aktier på multilaterala handelsplattformar. Ju.
16. Några frågor om ersättning vid gemensamhetsinrättningar. Ju.
17. Förbättrade förutsättningar för IVO – förslag för att motverka oseriösa och kriminella aktörer inom hälso- och sjukvården. S.
18. Nya regler om ansökningsförfarandet för vissa uppehålls- och arbetstillstånd. Ju.
19. Slutredovisning av uppdraget om förstärkningsteam inom socialtjänsten. S.
20. Utökade befogenheter för civilanställda vid Polismyndigheten att utreda brott. Ju.
21. Förbättrade förutsättningar för operativt militärt samarbete. Fö.
22. Sweden's tenth national report under the Convention on Nuclear Safety. KN.
23. Spellagens tillämpningsområde. Fi.
24. Utdelningsbart överskott i inkomstpensionssystemet. S.
25. En betald polisutbildning. Ju.
26. Administrativa sanktioner i den arbetsmarknadspolitiska verksamheten och i arbetslöshetsförsäkringen. S.
27. Åtgärder för att säkerställa veterinärberedskap under jourtid. LI
28. Stärkt trygghet i bostadsrätter. Ju.
29. Tredjelandslieferantörers tillträde till upphandlingsförfaranden. Fi.
30. Migrations- och asylpakten. Volym 1 & 2. Ju.
31. Utökade möjligheter för Kriminalvården att använda biometri m.m. Ju.
32. Polisens och Tullverkets användning av AI för biometrisk fjärridentifiering i efterhand. Ju.

Departementsserien 2025

Systematisk förteckning

Finansdepartementet

- Spellagens tillämpningsområde. [23]
- Tredjelandsleverantörers tillträde till upphandlingsförfaranden. [29]

Försvarsdepartementet

- Sveriges försvarsmaterieldirektör.
En ny inriktning. [3]
- En ändamålsenlig hantering av tillstånd och tillsyn av explosiva varor. [6]
- En ändamålsenlig hantering av tillstånd och tillsyn av explosiva varor – slutredovisning. [10]
- En tydlig beslutsordning för deltagande i Natos samlade verksamhet för avskräckning och försvar. [11]
- Förbättrade förutsättningar för operativt militärt samarbete. [21]

Justitiedepartementet

- Hyra anstaltsplatser utomlands.[1]
- En ny lag om unga lagöverträdare. [4]
- Genomförande av direktivet om skydd för personer som deltar i den offentliga debatten. [5]
- Polisens användning av AI för ansiktsigenkänning i realtid. [7]
- Nordisk verkställighet i brottmål. [12]
- Rätt att installera laddpunkt hemma. [13]
- Kompletterande bestämmelser till EU:s förordning om överföring av straffrättsliga förfaranden. [14]
- Nya regler om aktier på multilaterala handelsplattformar. [15]
- Några frågor om ersättning vid gemensamhetsinrättningar. [16]
- Nya regler om ansökningsförfarandet för vissa uppehålls- och arbetstillstånd. [18]

- Utökade befogenheter för civilanställda vid Polismyndigheten att utreda brott. [20]

- En betald polisutbildning. [25]
- Stärkt trygghet i bostadsrätter. [28]

- Migrations- och asylpakten.
Volym 1 & 2. [30]

- Utökade möjligheter för Kriminalvården att använda biometri m.m. [xx]
- Polisens och Tullverkets användning av AI för biometrisk fjärridentifiering i efterhand. [32]

Klimat- och näringslivsdepartementet

- Sweden's tenth national report under the Convention on Nuclear Safety. [22]

Kulturdepartementet

- Moderna – en ny myndighet för modern konst, arkitektur och design. [2]

Landsbygds- och infrastrukturdepartementet

- Åtgärder för att säkerställa veterinär beredskap under jourtid. [27]

Socialdepartementet

- Administrativa sanktioner i socialförsäkringen. [8]
- Förbättrade förutsättningar för IVO – förslag för att motverka oseriösa och kriminella aktörer inom hälso- och sjukvården. [17]
- Slutredovisning av uppdraget om förstärkningsteam inom socialtjänsten. [19]
- Utdelningsbart överskott i inkomstpensionssystemet . [24]
- Administrativa sanktioner i den arbetsmarknadspolitiska verksamheten och i arbetslöshetsförsäkringen. [26]

Utbildningsdepartementet

Ett nationellt mobilförbud i de
obligatoriska skolformerna och
fritidshemmet. [9]