

# Innehåll

<b>1</b>	<b>Promemorians huvudsakliga innehåll.....</b>	<b>13</b>
<b>2</b>	<b>Författningsförslag .....</b>	<b>15</b>
2.1	Förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet.....	15
2.2	Förslag till lag om polisens allmänna spaningsregister .....	42
2.3	Förslag till lag om ändring i rättegångsbalken .....	49
2.4	Förslag till lag om ändring i sekretesslagen (1980:100).....	51
2.5	Förslag till lag om ändring i säkerhetsskyddslagen (1996:627).....	59
2.6	Förslag till lag om ändring i lagen (1998:620) om belastningsregister .....	62
2.7	Förslag till lag om ändring i lagen (1998:621) om misstankeregister .....	64
2.8	Förslag till lag om ändring i lagen (2000:344) om Schengens informationssystem.....	66
2.9	Förslag till lag om ändring i lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet .....	67

<b>3</b>	<b>Bakgrund.....</b>	<b>69</b>
<b>4</b>	<b>Gällande rätt m.m. ....</b>	<b>71</b>
4.1	Inledning.....	71
4.2	Internationella överenskommelser och personupp- giftslagen.....	72
4.2.1	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna .....	72
4.2.2	Dataskyddskonventionen m.m. ....	73
4.2.3	Europarådets rekommendation No. R (87) 15 .....	75
4.2.4	Europeiska unionens stadga om de grund- läggande rättigheterna.....	75
4.2.5	Dataskyddsdirektivet och personuppgiftslagen.....	76
4.2.6	Europol.....	79
4.3	Den nuvarande polisregisterlagstiftningen .....	80
4.3.1	Allmänt om polisregisterlagstiftningen .....	80
4.3.2	Särskilt om polisdatalagen .....	80
4.4	EU-initiativ m.m. ....	81
<b>5</b>	<b>Polisens register.....</b>	<b>85</b>
5.1	Register och ärendehanteringssystem.....	85
5.2	Allmänt om polisens register.....	86
<b>6</b>	<b>En ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet .....</b>	<b>89</b>
6.1	Bestämmelserna om polisens användning av personuppgifter behöver reformeras .....	89
6.2	En ny lag införs .....	93

6.3	Lagens tillämpningsområde.....	95
6.4	Skyddet för den personliga integriteten .....	100
6.5	Den nya lagen och personuppgiftslagen.....	106
6.5.1	Förhållandet till personuppgiftslagen.....	106
6.5.2	Tillämpliga bestämmelser i personuppgifts- lagen.....	110
6.6	Personuppgiftsansvar.....	124
6.7	Tillgången till personuppgifter.....	125
<b>7</b>	<b>Tillåtna ändamål för behandlingen .....</b>	<b>127</b>
7.1	Tydliga och konkreta ändamål för behandling av personuppgifter.....	127
7.2	Förebygga, förhindra och upptäcka brottslig verk- samhet.....	130
7.3	Utreda och beivra brott .....	136
7.4	Internationellt samarbete .....	138
7.5	Behandling av uppgifter för diarieföring m.m.....	141
7.6	Behandling av uppgifter för att tillhandahålla information till andra.....	143
<b>8</b>	<b>Behandling av känsliga personuppgifter m.m. ....</b>	<b>151</b>
<b>9</b>	<b>Gemensamt tillgängliga uppgifter .....</b>	<b>155</b>
9.1	Särskilda regler bör gälla för behandling av gemen- samt tillgängliga uppgifter .....	155
9.2	Förebygga, förhindra och upptäcka brottslig verk- samhet.....	161

9.3	Utreda och beivra brott .....	170
9.4	Särskilt om behandlingen av uppgifter som rapporterats till polisens kommunikationscentraler .....	173
9.5	Gemensamt tillgängliga uppgifter i det internationella samarbetet .....	175
<b>10</b>	<b>Särskilda upplysningar för gemensamt tillgängliga uppgifter .....</b>	<b>179</b>
<b>11</b>	<b>Sökbegränsningar för gemensamt tillgängliga uppgifter .....</b>	<b>185</b>
11.1	Känsliga personuppgifter som sökbegrepp .....	185
11.2	Sökning på namn, firma, personnummer, samordningsnummer eller organisationsnummer .....	187
<b>12</b>	<b>Informationsutbyte mellan de brottsbekämpande myndigheterna .....</b>	<b>193</b>
12.1	Allmänt om behovet av ett effektivt informationsutbyte mellan svenska brottsbekämpande myndigheter .....	193
12.2	Allmänt om behovet av informationsutbyte i det internationella samarbetet .....	197
12.3	Elektroniskt informationsutbyte .....	198
12.3.1	Olika former av elektroniskt utlämnande av uppgifter .....	198
12.3.2	Begreppet direktåtkomst .....	199
12.3.3	Nuvarande möjligheter till direktåtkomst .....	201
12.3.4	De brottsbekämpande myndigheternas behov av tillgång till uppgifter i polisens brottsbekämpande verksamhet .....	202

12.3.5 Direktåtkomst för övriga brottsbekämpande myndigheter .....	216
12.3.6 Direktåtkomst för utländska myndigheter .....	223
<b>13 Sekretess och uppgiftsskyldighet m.m.....</b>	<b>225</b>
13.1 Allmänna utgångspunkter .....	225
13.2 Sekretessgenombrott .....	229
13.3 Uppgiftslämnande till utlandet .....	241
<b>14 Utlämnande av uppgifter på medium för automatiserad behandling.....</b>	<b>253</b>
<b>15 Särskilt om uppgifter på Internet .....</b>	<b>257</b>
<b>16 Gallring av uppgifter .....</b>	<b>261</b>
16.1 Gallring av uppgifter som inte har gjorts gemensamt tillgängliga .....	261
16.2 Gallring av gemensamt tillgängliga uppgifter.....	264
16.3 Särskilt om uppgifter i förundersökningar och liknande brottsutredningar.....	269
<b>17 Särskilda bestämmelser om vissa register .....</b>	<b>279</b>
17.1 Allmänna utgångspunkter .....	279
17.2 Register med uppgifter om resultat av DNA-analyser....	282
17.3 Fingeravtrycks- eller signalementsregister .....	284
17.4 Penningtvättsregister .....	288

<b>18</b>	<b>Behandling av personuppgifter i S�kerhetspolisens brottsbek�mpande verksamhet.....</b>	<b>293</b>
18.1	Bakgrund.....	293
18.1.1	S�kerhetspolisens organisation och uppgifter.....	293
18.1.2	Nuvarande behandling av personuppgifter hos S�kerhetspolisen.....	295
18.2	Behovet av s�rskilda best�mmelser f�r personuppgiftsbehandling hos S�kerhetspolisen .....	299
18.3	Den nya regleringen i huvuddrag.....	300
18.4	�ndam�len med behandlingen .....	302
18.4.1	Tydliga och konkreta �ndam�l.....	302
18.4.2	Prim�ra �ndam�l.....	303
18.4.3	Behandling av uppgifter f�r att tillhandah�lla information till andra.....	311
18.5	Vissa allm�nna best�mmelser som b�r g�lla �ven f�r S�kerhetspolisen.....	315
18.6	Gemensamt tillg�ngliga uppgifter.....	317
18.6.1	Allm�nna utg�ngspunkter .....	317
18.6.2	Utl�mnande av uppgifter p� medium f�r automatisk behandling.....	320
18.6.3	S�rskilda upplysningar .....	321
18.6.4	S�kbegr�nsningar.....	323
18.6.5	Gallring.....	327
<b>19</b>	<b>Tillsyn .....</b>	<b>331</b>
<b>20</b>	<b>En ny lag om polisens spaningsregister.....</b>	<b>339</b>
20.1	Behovet av det allm�nna spaningsregistret .....	339
20.2	En ny lagreglering .....	341

20.3	Utformningen av regleringen.....	343
20.3.1	Förhållandet till annan lagstiftning om polis- register och till personuppgiftslagen .....	343
20.3.2	Ändamålet med registret .....	344
20.3.3	Innehållet i registret .....	347
20.3.4	Behandling av känsliga personuppgifter.....	353
20.3.5	Särskilda upplysningar och sökbegränsningar .....	355
20.3.6	Utlämnande av uppgifter ur registret .....	357
20.3.7	Gallring.....	362
20.3.8	Övriga frågor.....	364
<b>21</b>	<b>Följändringar .....</b>	<b>367</b>
<b>22</b>	<b>Kustbevakningens åtkomst till vissa register.....</b>	<b>371</b>
<b>23</b>	<b>Ikraftträdande och övergångsbestämmelser .....</b>	<b>375</b>
23.1	Ikraftträdande.....	375
23.2	Övergångsbestämmelser.....	376
<b>24</b>	<b>Kustbevakningens personuppgiftsbehandling .....</b>	<b>381</b>
24.1	Bakgrund .....	381
24.2	Kustbevakningens verksamhet.....	381
24.2.1	Allmänt.....	381
24.2.2	Brottsbekämpande verksamhet.....	383
24.3	Regleringen av Kustbevakningens personuppgifts- behandling .....	385
24.4	Samverkan och informationsutbyte med andra brotts- bekämpande myndigheter .....	386

24.5	Enhetlig reglering av grundläggande principer för personuppgiftsbehandling i brottsbekämpande verksamhet .....	388
<b>25</b>	<b>Ekonomiska konsekvenser .....</b>	<b>393</b>
<b>26</b>	<b>Författningskommentar .....</b>	<b>395</b>
26.1	Förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet .....	395
26.2	Förslaget till lag om polisens allmänna spaningsregister .....	491
26.3	Förslaget till lag om ändring i rättegångsbalken .....	513
26.4	Förslaget till lag om ändring i sekretesslagen (1980:100) .....	514
26.5	Förslaget till lag om ändring i säkerhetsskyddslagen (1996:627) .....	519
26.6	Förslaget till lag om ändring i lagen (1998:620) om belastningsregister .....	521
26.7	Förslaget till lag om ändring i lagen (1998:621) om misstankeregister .....	523
26.8	Förslaget till lag om ändring i lagen (2000:344) om Schengens informationssystem .....	524
26.9	Förslaget till lag om ändring i lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet .....	524
<b>Bilaga 1</b>	<b>Sammanfattning av SOU 2001:92 Behandling av personuppgifter i polisens verksamhet .....</b>	<b>527</b>



<b>Bilaga 2</b>	<b>Polisdatautredningens lagförslag .....</b>	<b>541</b>
<b>Bilaga 3</b>	<b>Förteckning över de remissinstanser som yttrat sig över Polisdatautredningens betänkande .....</b>	<b>589</b>
<b>Bilaga 4</b>	<b>Kustbevakningens framställan om åtkomst till belastningsregistret och misstanke- registret .....</b>	<b>591</b>
<b>Bilaga 5</b>	<b>Förteckning över de remissinstanser som yttrat sig över Kustbevakningens framställan...</b>	<b>593</b>
<b>Bilaga 6</b>	<b>Polisens register .....</b>	<b>595</b>



# 1 Promemorians huvudsakliga innehåll

Promemorian innehåller förslag till en ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Lagen ersätter polisdatalagen (1998:622). Det övergripande syftet med den nya lagen är att skydda människor mot att deras personliga integritet kränks vid polisens behandling av personuppgifter.

Den nya lagen har tagits fram för att komma till rätta med olika problem som den nuvarande regleringen har visat sig ge upphov till, bl.a. när det gäller möjligheten att behandla personuppgifter för att förebygga, förhindra och upptäcka brottslig verksamhet. Den nya lagen skapar också förutsättningar för ett bättre samarbete mellan de brottsbekämpande myndigheterna genom ändrade bestämmelser om utlämnande av uppgifter. Regleringen är teknikneutral.

Lagen är heltäckande och reglerar, med några få undantag, all polisens behandling av personuppgifter i den brottsbekämpande verksamheten vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Personuppgifter ska få behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott, eller fullgöra de förpliktelser som följer av internationella åtaganden. Särskilda bestämmelser föreslås för sådan behandling som sker hos Säkerhetspolisen. För behandling av personuppgifter som fler än ett fåtal personer har åtkomst till (gemensamt tillgängliga uppgifter) föreslås olika begränsande bestämmelser för att trygga

den personliga integriteten. Det föreslås också en särskild lag som reglerar polisens allmänna spaningsregister.

Personuppgiftsbehandling i sådan verksamhet som inte är brottsbekämpande, exempelvis den hjälpande verksamheten, omfattas inte av lagförslagen utan förutsätts, liksom i dag, regleras av personuppgiftslagen (1998:204).

Den föreslagna lagregleringen medför följdändringar i ett antal andra författningar.

I promemorian övervägs också vissa frågor om Kustbevakningens behandling av personuppgifter. Bedömningen görs att de grundläggande principer som föreslås gälla för polisens behandling av personuppgifter i den brottsbekämpande verksamheten i flera avseenden bör gälla i en kommande reglering för Kustbevakningens behandling av personuppgifter i sådan verksamhet.

Vidare föreslås att Kustbevakningen ska få tillgång till uppgifter ur misstankeregistret och belastningsregistret i sin brottsbekämpande verksamhet.

Lagförslagen föreslås träda i kraft den 1 januari 2009.

Promemorian har tagits fram av en arbetsgrupp bestående av tjänstemän i Justitiedepartementet. Promemorians överväganden är därför skrivna i vi-form.

## 2 Författningsförslag

### 2.1 Förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet

Härigenom föreskrivs följande.

#### 1 kap. Lagens syfte och tillämpningsområde

##### *Lagens syfte*

1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i polisens brottsbekämpande verksamhet.

##### *Lagens tillämpningsområde m.m.*

2 § Denna lag gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten, om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 2 kap. 4 § andra stycket och 10 § gäller även vid andra myndigheters behandling av uppgifter som har lämnats ut genom direktåtkomst med stöd av denna lag.

Lagen gäller inte vid sådan behandling av personuppgifter som sker enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister eller lagen (2008:000) om polisens allmänna spaningsregister. Den gäller inte heller vid insamling av personuppgifter genom allmän kameraövervakning, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning.

**3 §** Följande bestämmelser gäller även vid behandling av uppgifter om juridiska personer:

1. 2 kap. 4 § om personuppgiftsansvar,
2. 2 kap. 5–7 §§ om ändamålen för behandlingen,
3. 2 kap. 11 § om gallring,
4. 3 kap. 1–18 §§ om gemensamt tillgängliga uppgifter,
5. 4 kap. 20–22 §§ om behandling av uppgifter i penningtvättsregister,
6. 5 kap. 2–4 §§ om ändamålen för behandlingen hos Säkerhetspolisen,
7. 5 kap. 6 § om Säkerhetspolisens personuppgiftsansvar,
8. 5 kap. 7 § om gallring hos Säkerhetspolisen, och
9. 5 kap. 8–17 §§ om gemensamt tillgängliga uppgifter hos Säkerhetspolisen.

Vad som sägs i de angivna paragraferna om personuppgifter ska därvid avse uppgifter om juridiska personer.

**4 §** I 2 kap. finns allmänna bestämmelser om sådan behandling av personuppgifter som omfattas av lagen. För behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga gäller även bestämmelserna i 3 kap. För behandling i register med uppgifter om resultat av DNA-analyser, fingeravtrycksregister, signalementsregister eller penningtvättsregister, gäller dock särskilda bestämmelser i 4 kap. i stället för bestämmelserna i 3 kap.

Bestämmelserna i 5 kap. gäller för behandling av personuppgifter i Säkerhetspolisens verksamhet. Vid sådan behandling ska

bestämmelserna i 2–4 kap. tillämpas endast i den utsträckning som framgår av 5 kap.

## 2 kap. Allmänna bestämmelser om personuppgiftsbehandling i polisens brottsbekämpande verksamhet

### *Förhållandet till personuppgiftslagen*

1 § Om inte annat anges i 2 §, gäller denna lag i stället för personuppgiftslagen (1998:204).

2 § När personuppgifter behandlas enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen, gäller följande bestämmelser i personuppgiftslagen (1998:204):

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 § första stycket a), b) och e)–h) om grundläggande krav på behandling,
4. 22 § om behandling av personnummer,
5. 23 § och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30–32 §§ om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 36 § andra stycket och 38–41 §§ om personuppgiftsombud m.m.,
10. 42 § om upplysningar till allmänheten om vissa behandlingar,
11. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,
12. 48 § om skadestånd, och
13. 51 § första stycket, 52 § första stycket och 53 § om överklagande.

Var och en av de myndigheter som avses i 1 kap. 2 § ska utse ett eller flera personuppgiftsombud.

Information enligt 23 § personuppgiftslagen behöver inte lämnas om uppgifterna samlas in i samband med larm och det

med hänsyn till omständigheterna inte finns tid att lämna informationen.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

#### *Tillsyn*

3 § Utöver de bestämmelser om tillsyn som avses i 2 § första stycket 11 finns bestämmelser om tillsyn i 1 § lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet.

#### *Personuppgiftsansvar m.m.*

4 § Rikspolisstyrelsen eller polismyndigheterna är personuppgiftsansvariga för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra.

En myndighet som har direktåtkomst till uppgifter enligt denna lag ansvarar för att åtkomsten begränsas enligt 10 §.

#### *Ändamål med behandlingen av personuppgifter*

5 § Personuppgifter får, om inte annat följer av 6 eller 7 §, behandlas endast om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller beivra brott, eller
3. fullgöra de förpliktelser som följer av internationella åtaganden.

6 § Om personuppgifter behandlas enligt 5 §, får de även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,
2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,



3. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen, eller

4. annan myndighets verksamhet, om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift.

Personuppgifter som behandlas enligt 5 § får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, till andra.

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 5 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter och att uppgifter som behandlas i en förundersökning får tillhandahållas konkursförvaltare.

7 § Personuppgifter får alltid behandlas om

1. behandlingen är nödvändig för diarieföring, eller
2. uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

#### *Behandling av känsliga personuppgifter*

8 § Uppgifter om en person får inte behandlas på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Trots bestämmelsen i första stycket får uppgifter om en person som behandlas på annan grund kompletteras med uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen. Uppgifter som avses i första stycket får också behandlas om

1. behandlingen är nödvändig för diarieföring, eller
2. uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Uppgifter som beskriver en persons utseende ska alltid utformas på ett objektiva sätt med respekt för människovärdet.

*Behandling av uppgifter om resultat av DNA-analyser*

9 § Uppgifter om resultat av DNA-analyser får endast behandlas

1. i en förundersökning, eller
2. enligt bestämmelserna i 4 kap. om behandling i DNA-register, utredningsregister och spårregister.

*Tillgången till personuppgifter*

10 § Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

*Gallring*

11 § Personuppgifter som behandlas automatiserat i ett ärende ska gallras senast ett år efter det att ärendet avslutades. Personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Bestämmelserna i första stycket gäller inte

1. uppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken,
2. uppgifter som har gjorts gemensamt tillgängliga, och
3. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

*Utlämnande av uppgifter och uppgiftsskyldighet*

12 § Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

13 § Personuppgifter får lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en interna-

tionell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Om det är förenligt med svenska intressen, får uppgifter vidare lämnas

1. till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott, eller
2. till utländsk underrättelse- eller säkerhetstjänst.

Av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) följer att uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation även i vissa andra fall.

**14 §** Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) ska personuppgifter som har gjorts gemensamt tillgängliga hos polisen lämnas till Rikspolisstyrelsen, polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet.

Första stycket gäller inte uppgifter som behandlas i särskilda register med stöd av 4 kap.

**15 §** Uppgift om huruvida en person förekommer i register med uppgifter om resultat av DNA-analyser ska utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) lämnas till polismyndighet, Åklagarmyndigheten och Ekobrottsmyndigheten, om den mottagande myndigheten har behov av uppgiften i sin brottsbekämpande verksamhet.

**16 §** Personuppgifter som behandlas i fingeravtrycks- eller signalementsregister med stöd av 4 kap. 14–19 §§ ska utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) lämnas till polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatte-

verket, om den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet

17 § Regeringen meddelar föreskrifter om att personuppgifter får lämnas ut även i andra fall än som sägs i 12–16 §§.

### 3 kap. Gemensamt tillgängliga uppgifter

1 § Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet. Uppgifter som endast ett fåtal bestämda personer inom polisen har rätt att ta del av anses inte som gemensamt tillgängliga.

#### *Personuppgifter som får göras gemensamt tillgängliga*

2 § Endast följande personuppgifter får göras gemensamt tillgängliga.

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten

a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av en person, om han eller hon

a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver, och

b) är allvarligt kriminellt belastad eller kan antas vara farlig för annans personliga säkerhet.

3. Uppgifter som förekommer i ett ärende om utredning eller beivrande av brott.

4. Uppgifter som behövs för att fullgöra de förpliktelser som följer av internationella åtaganden.

5. Uppgifter som har rapporterats till polisens kommunikationscentraler.

Uppgifter om resultat av DNA-analyser får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 4 kap.

Uppgifter som avses i första stycket 4 får göras gemensamt tillgängliga endast om det behövs för att fullgöra den aktuella förpliktelsen.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om huruvida en person är föremål för övervakning får dock göras tillgänglig för flera.

### *Särskilda upplysningar*

3 § Vid behandling enligt 1 § ska personuppgifterna föras med en särskild upplysning om det närmare ändamålet med behandlingen. Har uppgifterna gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, ska det också lämnas upplysning om detta. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

4 § Om uppgifter, som behandlas enligt 1 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska uppgifterna föras med en särskild upplysning om att personen inte är misstänkt. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

Uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska föras med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte detta på grund av särskilda omständigheter är onödigt. Detsamma gäller uppgifter om personer som avses i 2 § första stycket 2.

*Sökning*

5 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp.

Vad som sägs i första stycket hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

6 § Vid sökning i gemensamt tillgängliga uppgifter på namn, firma, personnummer, samordningsnummer, organisationsnummer eller andra liknande identitetsbeteckningar får endast sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är misstänkt för brott eller för brottslig verksamhet som avses i 2 § första stycket 1,
3. övervakas enligt 2 § första stycket 2,
4. har anmält ett brott eller är målsägande i ett ärende som rör ansvar för brott,
5. är vittne eller annars ska höras eller avge yttrande i ett ärende,
6. har gett in eller tillhandahållits en handling, eller
7. är anmäld försvunnen.

7 § Bestämmelsen i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller
2. sökning i en uppgiftssamling som har skapats för att undersöka vissa preciserade slag av brottslighet eller vissa preciserade kriminella grupperingar och som enbart de som arbetar i undersökningen eller som omfattas av andra stycket 2 har åtkomst till.

Bestämmelsen i 6 § gäller inte heller vid sökning som

1. sker för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra år eller däröver eller för sådant ändamål som avses i 2 § första stycket 2, och

2. utförs av särskilt angivna tjänstemän med uppgift att undersöka den brottsliga verksamheten eller övervaka personer enligt 2 § första stycket 2.

Om det finns särskilda skäl får, trots bestämmelsen i 6 §, sökning även ske för att utreda brott för vilket är föreskrivet fängelse i fyra år eller däröver, om sökningen utförs av särskilt angivna tjänstemän.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om och under vilka förutsättningar sökning får äga rum med stöd av andra eller tredje stycket.

#### *Utlämnande av uppgifter på medium för automatiserad behandling*

8 § Endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall.

#### *Direktåtkomst*

9 § Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får i den brottsbekämpande verksamheten medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

10 § Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

komsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

*Behandling av uppgifter i brottsanmälningar*

11 § Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i polisens brottsbekämpande verksamhet. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får uppgifterna inte behandlas i polisens brottsbekämpande verksamhet efter det att det påstådda brottet har preskriberats.

*Behandling av uppgifter i avslutade förundersökningar*

12 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får uppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år sedan domen, eller det beslut som meddelades med anledning av talan, vunnit laga kraft.

Om en förundersökning har lagts ned eller avslutats på annat sätt än genom åtal får uppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter åklagarens eller förundersökningsledarens beslut. Om det i samband med beslutet anges att brottet, trots nedläggningsbeslutet, kan komma att bli föremål för lagföring, får dock behandling ske även senare fram till dess att brottet har preskriberats.

Vad som sägs i första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

13 § Trots bestämmelserna i 12 § får personuppgifter i en förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken behandlas i polisens brottsbekämpande verksamhet, om det behövs för att återuppta förun-



dersökningen eller utredningen eller för en prövning enligt 58 eller 59 kap. rättegångsbalken. Om det finns särskilda skäl, får uppgifterna även behandlas, om det behövs för en utredning som avser brott, för vilket är föreskrivet fängelse i fyra år eller däröver, eller för en undersökning av brottslig verksamhet som inefattar sådant brott.

**14 §** Om en förundersökning mot en person har lagts ned på grund av bristande bevisning, om åtal har lagts ned eller om frikännande dom, som har vunnit laga kraft, har meddelats, får en uppgift om att personen är misstänkt för brott inte längre vara sökbar, om inte förundersökningsledaren har beslutat att återuppta förundersökningen eller fråga är om prövning enligt 58 eller 59 kap. rättegångsbalken.

*Användning av arkiverade uppgifter m.m.*

**15 §** Bestämmelserna i 11–14 §§ hindrar inte att personuppgifter i brottanmälningar, förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken arkiveras och gallras enligt bestämmelserna i arkivlagen (1990:782). För användningen av arkiverade uppgifter i polisens brottsbekämpande verksamhet gäller dock de begränsningar som anges i 11–14 §§.

*Gallring*

**16 §** Personuppgifter som har gjorts gemensamt tillgängliga ska gallras enligt bestämmelserna i andra–sjätte styckena.

Uppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 2 § första stycket 1 ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om den person som uppgiften avser inte är eller varit misstänkt, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats i samband med sådan övervakning som avses i 2 § första stycket 2 ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende den övervakade personen gjordes. Om en uppgift inte avser den övervakade personen, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats med stöd av 2 § första stycket 4 ska gallras senast ett år efter det att ärendet i vilket uppgifterna behandlades avslutades.

Uppgifter som har behandlats med stöd av 2 § första stycket 5 ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i andra och tredje styckena.

#### 17 § Bestämmelserna i 16 § gäller inte

1. personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken, och

2. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

I fråga om behandling av sådana personuppgifter som anges i första stycket 1 gäller vad som sägs i 11–15 §§.

18 § Vad som föreskrivs i 11–16 §§ hindrar inte att regeringen meddelar föreskrifter om att uppgifter i vissa särskilda fall får behandlas och bevaras under längre tid än vad som anges där.

## 4 kap. Register

### Register med uppgifter om resultat av DNA-analyser

*Ändamål m.m.*

1 § Med DNA-analys förstås varje förfarande som kan användas för analys av deoxyribonukleinsyra.

2 § Rikspolisstyrelsen får föra register över uppgifter om resultat av DNA-analyser i enlighet med 3–13 §§ (DNA-register, utredningsregister och spårregister). Utöver för de ändamål som anges i 2 kap. får sådana register föras för att underlätta identifiering av avlidna personer.

*DNA-register*

3 § Ett DNA-register får innehålla uppgifter om resultatet av DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som

1. genom lagakraftvunnen dom har dömts till annan påföljd än böter, eller
2. har godkänt ett strafföreläggande som avser villkorlig dom.

4 § Registreringen av resultatet av en DNA-analys ska begränsas till uppgifter som ger information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får inte registreras.

Utöver vad som sägs i första stycket får DNA-registret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts och vem analysen avser.

*Utredningsregister*

5 § Ett utredningsregister får innehålla uppgifter om resultatet av DNA-analyser som har gjorts med stöd av bestämmelserna i

28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för brott på vilket fängelse kan följa.

Vad som anges i 4 § gäller också vid registrering i utredningsregistret.

#### *Spårregister*

6 § Ett spårregister får innehålla uppgifter om resultatet av DNA-analyser som har gjorts under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver uppgifter om analysresultat får spårregistret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts.

7 § Uppgifter i ett spårregister får endast jämföras med analysresultat

1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller
3. som kan hänföras till en person som är skäligen misstänkt för brott.

#### *Gallring*

8 § Uppgifter i DNA-registret ska gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter i utredningsregistret ska gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade har godkänt ett strafföreläggande som avser enbart böter.

Uppgifter i spårregistret ska gallras senast trettio år efter registreringen.

*Särskilda bestämmelser om prov för DNA-analys*

9 § Om det i samband med utredning av ett brott har tagits ett prov för DNA-analys, får provet inte användas för något annat ändamål än det för vilket det togs.

10 § Ett prov för DNA-analys som har tagits med stöd av bestämmelserna i 28 kap. 12–12 b §§ rättegångsbalken ska förstöras senast sex månader efter det att provet togs.

Om uppgifterna i utredningsregistret ska gallras vid en tidigare tidpunkt enligt 8 §, ska även det prov som avser den registrerade förstöras senast vid samma tidpunkt.

Om provet har tagits från någon som inte är skäligen misstänkt för brott, ska provet förstöras så snart målet eller ärendet slutligt har avgjorts.

*Utlämnande av uppgifter på medium för automatiserad behandling*

11 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för utlämnande av uppgifter om resultat av DNA-analyser.

*Direktåtkomst*

12 § Statens kriminaltekniska laboratorium, polismyndigheter, Ekobrottsmyndigheten och Åklagarmyndigheten får medges direktåtkomst till register med uppgifter om resultat av DNA-analyser.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

13 § Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till register med uppgifter om resultat av DNA-analyser i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sve-

rige efter riksdagens godkännande har tillträtt. Åtkomsten ska begränsas till uppgift om huruvida någon förekommer i registret.

### Fingeravtrycks- eller signalementsregister

#### *Ändamål*

14 § Rikspolisstyrelsen får föra fingeravtrycks- eller signalementsregister i enlighet med 15–19 §§. Utöver för de ändamål som anges i 2 kap. får sådana register föras för att underlätta identifiering av okända personer.

#### *Innehåll*

15 § Ett fingeravtrycks- eller signalementsregister får endast innehålla uppgifter om den som är misstänkt eller dömd för brott eller som har fått lämna fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll. I ett sådant register får endast antecknas uppgifter om

1. fingeravtryck,
2. signalement,
3. identifieringsuppgifter,
4. ärendenummer, och
5. brottskoder.

Fingeravtrycks- eller signalementsregister får inte innehålla uppgifter som har lämnats av en person under femton år enligt 36 § första stycket 2 lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

#### *Gallring*

16 § Uppgifter i ett fingeravtrycks- eller signalementsregister om en misstänkt person ska gallras senast

1. tio år efter registreringen, om denna skett på grund av misstanke om brott för vilket det inte föreskrivs strängare straff än fängelse i två år,

2. femton år efter registreringen, om denna skett på grund av misstanke om brott för vilket det föreskrivs strängare straff än fängelse i två år men inte strängare straff än fängelse i åtta år,

3. tjugofem år efter registreringen, om denna skett på grund av misstanke om brott för vilket det föreskrivs strängare straff än fängelse i åtta år,

4. tre månader efter det att åtal mot personen har lagts ned eller efter att personen genom lagakraftvunnen dom har frikänts, eller

5. tre månader efter det att en förundersökning mot personen har lagts ned.

Om en person blir misstänkt för ett nytt brott före utgången av den tid som anges i första stycket 1, 2 eller 3 får de uppgifter som finns registrerade om personen bevaras till dess att den senare registreringen avseende personen ska gallras enligt första stycket.

Uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll ska gallras när uppgifterna inte längre behövs för ändamålet med behandlingen eller enligt föreskrifter som regeringen meddelar.

#### *Utlämnande av uppgifter på medium för automatiserad behandling*

17 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för utlämnande av uppgifter i ett fingeravtrycks- eller signalementsregister.

#### *Direktåtkomst*

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket får i den brottsbekämpande verksamheten medges direktåtkomst till personuppgifter i ett fingeravtrycks- eller signalementsregister.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

19 § Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till ett fingeravtrycks- eller signalementsregister i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Åtkomsten ska begränsas till uppgift om huruvida någon förekommer i registret.

### Penningtvätsregister

*Ändamål m.m.*

20 § Rikspolisstyrelsen får behandla uppgifter i penningtvätsregister om det behövs för att förebygga, förhindra eller upptäcka

1. brottslig verksamhet där penningtvätt är ett led för att dölja vinning av brott eller brottslig verksamhet, eller

2. brottslig verksamhet som innefattar brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

I ett sådant register får endast behandlas uppgifter som kan antas ha samband med sådan misstänkt brottslig verksamhet som avses i första stycket 1 och 2, uppgifter som har rapporterats till myndigheten med stöd av bestämmelser i lag eller annan författning och uppgifter som har lämnats av en utländsk myndighet som ansvarar för arbetet med att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses i första stycket 1 och 2 i det landet.

*Gallring*

21 § Personuppgifter i ett penningtvätsregister ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.



Första stycket gäller inte om regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter om att uppgifter ska bevaras för historiska, statistiska eller vetenskapliga ändamål.

#### *Utlämnande av uppgifter på medium för automatiserad behandling*

22 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för uppgifter i ett penningtvättsregister.

### **5 kap. Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet**

#### *Allmänna bestämmelser*

1 § Detta kapitel innehåller bestämmelser om behandling av personuppgifter hos Säkerhetspolisen i dess brottsbekämpande verksamhet.

#### *Ändamål*

2 § I Säkerhetspolisens brottsbekämpande verksamhet får, om inte annat följer av 3 eller 4 §, personuppgifter behandlas endast om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

a) brott mot rikets säkerhet,

b) terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott,

c) brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m., eller

d) tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,

2. utreda eller beivra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,

3. fullgöra bevaknings- och säkerhetsarbete avseende personskydd,

4. fullgöra de uppgifter som följer av säkerhetsskyddslagen (1996:627),

5. fullgöra de förpliktelser som följer av internationella åtaganden, eller

6. lämna tekniskt biträde till Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket.

**3 §** Om personuppgifter behandlas enligt 2 §, får de även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,

2. Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om det finns särskilda skäl att tillhandahålla informationen, eller

3. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation.

Personuppgifter som behandlas enligt 2 § får även behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, andra.

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 2 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter.

**4 §** Bestämmelserna i 2 kap. 7 § om diarieföring av personuppgifter m.m. gäller även för behandling av personuppgifter hos Säkerhetspolisen.

*Tillämpliga bestämmelser i 2 kap.*

5 § Följande bestämmelser i 2 kap. ska tillämpas vid behandling av personuppgifter hos Säkerhetspolisen:

1. 1 och 2 §§ om förhållandet till personuppgiftslagen,
2. 3 § om tillsyn,
3. 8 § om behandling av känsliga personuppgifter,
4. 9 § om behandling av uppgifter om resultatet av DNA-analyser,
5. 10 § om tillgången till uppgifter, och
6. 12, 13 och 17 §§ om utlämnande av uppgifter.

*Personuppgiftsansvar*

6 § Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra.

*Gallring*

7 § Personuppgifter som behandlas automatiserat i ett ärende hos Säkerhetspolisen ska gallras senast ett år efter det att ärendet avslutades. Personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Bestämmelserna i första stycket gäller inte

1. uppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken,
2. uppgifter som har gjorts gemensamt tillgängliga, och
3. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

## Gemensamt tillgängliga uppgifter

8 § Om det behövs för de ändamål som anges i 2 §, får personuppgifter göras gemensamt tillgängliga i Säkerhetspolisens verksamhet. Uppgifter om resultat av DNA-analyser får dock inte göras gemensamt tillgängliga. Uppgifter som endast ett fåtal bestämda personer hos Säkerhetspolisen har rätt att ta del av anses inte som gemensamt tillgängliga.

Bestämmelserna i 9–17 §§ gäller för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga.

### *Särskilda upplysningar*

9 § Vid behandling enligt 8 § ska personuppgifterna föras med en särskild upplysning om det närmare ändamålet med behandlingen. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

10 § Om uppgifter, som behandlas enligt 8 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska de föras med en särskild upplysning om att personen inte är misstänkt. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

Uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska föras med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Upplysning behöver dock inte lämnas, om det på grund av särskilda omständigheter är onödigt. Upplysning behöver inte heller lämnas om

1. uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till, och

2. bearbetningen och analysen befinner sig i ett inledande skede.

*Sökning*

11 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv användas som sökbegrepp endast om det är absolut nödvändigt för de ändamål som anges i 2 §.

Första stycket hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

12 § Vid sökning i gemensamt tillgängliga uppgifter får endast följande uppgifter tas fram:

1. identifieringsuppgifter,
2. uppgifter om grunden för registreringen, och
3. hänvisning till de ärenden där uppgifter om personen behandlas.

13 § Bestämmelsen i 12 § gäller inte vid sökning

1. i en viss handling eller i ett visst ärende, eller
2. i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om och under vilka förutsättningar sökning får ske enligt första stycket.

*Utlämnande av uppgifter på medium för automatiserad behandling*

14 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling ska tillämpas även vid utlämnande av uppgifter som behandlas hos Säkerhetspolisen.

*Behandling av uppgifter i avslutade förundersökningar m.m.*

15 § Bestämmelserna i 3 kap. 11–15 §§ om behandling av uppgifter i avslutade förundersökningar m.m. ska tillämpas även vid behandling av personuppgifter hos Säkerhetspolisen.

*Gallring*

16 § Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Personuppgifter som behandlas i en sådan uppgiftssamling som avses i 10 § andra stycket 1 ska dock gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Säkerhetspolisen får besluta att personuppgifter får behandlas längre tid än vad som sägs i första och andra styckena, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Om uppgifter bevaras med stöd av ett sådant beslut, ska de gallras, eller frågan om bevarande prövas på nytt, senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i andra stycket, senast vid utgången av det tredje kalenderåret efter beslutet.

17 § Bestämmelserna i 16 § gäller inte

1. personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken, och

2. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

I fråga om behandling av sådana personuppgifter som anges i första stycket 1 ska i stället 3 kap. 11–15 §§ tillämpas.

1. Denna lag träder i kraft den 1 januari 2009, då polisdatalagen (1998:622) upphör att gälla.

2. I fråga om behandling av personuppgifter i en särskild undersökning enligt 14 § första stycket 1 polisdatalagen (1998:622) som har beslutats före ikraftträdandet av denna lag gäller bestämmelserna i polisdatalagen i stället för bestämmelserna i denna lag till utgången av år 2010.

3. För de personregister som har förts med stöd av punkten 2 i övergångsbestämmelserna till polisdatalagen (1998:622) gäller bestämmelserna i datalagen (1973:289) i stället för bestämmelserna i denna lag till utgången av år 2010. Bestämmelserna i 2 kap. 12, 13 och 17 §§ denna lag ska dock tillämpas på uppgifterna i registren från lagens ikraftträdande.

Vad som sägs i första stycket gäller inte fingeravtrycksregistret, signalements- och känneteckensregistret och det allmänna spaningsregistret.

4. Datainspektionens tillstånd att föra sådana register som avses i punkten 3 andra stycket upphör att gälla vid ikraftträdandet av denna lag.

Datainspektionens tillstånd att föra övriga register som avses i punkten 3 upphör att gälla vid utgången av år 2010 eller vid den tidigare tidpunkt då den personuppgiftsansvarige avanmäler registret hos inspektionen.

5. Bestämmelserna om särskilda upplysningar i 3 kap. 3 och 4 §§ behöver inte tillämpas förrän den 1 januari 2011 i fråga om uppgifter som har samlats in före ikraftträdandet.

6. Bestämmelserna om gallring och om behandling av uppgifter i brottsanmälningar och avslutade förundersökningar i 3 kap. 11–17 och 5 kap. 15 §§ ska inte tillämpas förrän den 1 januari 2011 i fråga om uppgifter som har samlats in före ikraftträdandet. I stället ska motsvarande bestämmelser i polisdatalagen (1998:622) tillämpas. För uppgifter i ett register som har avanmälts enligt punkten 4 gäller dock bestämmelserna i denna lag.

## 2.2 Förslag till lag om polisens allmänna spaningsregister

Härigenom föreskrivs följande.

### *Allmänt spaningsregister*

1 § Rikspolisstyrelsen får med hjälp av automatiserad behandling föra ett allmänt spaningsregister.

Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret. En myndighet som har direktåtkomst enligt denna lag ansvarar för att åtkomsten begränsas enligt 11 §.

### *Ändamål*

2 § Det allmänna spaningsregistret ska ha till ändamål att underlätta tillgången till personuppgifter som behövs för spaning i polisens brottsbekämpande verksamhet.

### *Vilka personuppgifter som får behandlas*

3 § I det allmänna spaningsregistret får behandlas uppgifter som kan hänföras till en enskild person, om

1. den som uppgiften avser kan misstänkas för att ha begått ett brott som inte enbart har böter i straffskalan, och
2. behandlingen är av särskild betydelse för brottsbekämpningen.

4 § I registret får behandlas uppgifter som kan hänföras till en enskild person som inte kan misstänkas för brott, om uppgiften

1. har samband med en person som har registrerats enligt 3 §, och
2. är av särskild betydelse för polisens spaningsverksamhet.



5 § Utöver de uppgifter som får behandlas enligt 3 och 4 §§ får uppgifter behandlas om en juridisk person, ett transportmedel eller annat föremål som kan hänföras till en enskild person, om

1. uppgiften kan antas ha samband med ett brott som inte enbart har böter i straffskalan, och
2. behandlingen är av särskild betydelse för brottsbekämpningen.

#### *Innehåll*

6 § Det allmänna spaningsregistret ska innehålla uppgifter om

1. grunden för att en person registreras enligt 3 § eller att en juridisk person, ett transportmedel eller föremål enligt 5 § förs in i registret och omständigheterna i samband med registreringen,
2. de omständigheter och händelser som ger upphov till att andra uppgifter än sådana som avses i 1 tillförs registret,
3. den behandlade uppgiftens ursprung, och
4. uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

7 § Det allmänna spaningsregistret får, utöver vad som anges i 6 §, endast innehålla följande uppgifter om en person som har registrerats enligt 3 §:

1. uppgift som är ägnad att identifiera personen, dock inte uppgifter om resultat av DNA-analyser eller fingeravtryck,
2. uppgift om vistelseadress,
3. uppgift om verkställighet av påföljd för brott,
4. uppgift om att personen är eftersökt i samband med brott,
5. uppgift om att personen tidigare har varit beväpnad, våldsam eller flyktbenägen,
6. uppgift om att personen är föremål för sådan övervakning som avses i 3 kap. 2 § första stycket 2 lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet,
7. uppgift om anknytning till juridisk person,

8. uppgift om anknytning till andra personer som har registrerats enligt 3 § och som kan antas tillhöra samma gruppering som den registrerade,

9. uppgift om att personen har något speciellt tillvägagångssätt, och

10. ärendenummer.

8 § Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om de uppgifter som får registreras i det allmänna spaningsregistret och om förfarandet vid registreringen.

#### *Särskilda upplysningar*

9 § Uppgifter i det allmänna spaningsregistret som direkt kan hänföras till en person som inte misstänks för brott ska förses med en särskild upplysning om detta. Detsamma gäller uppgifter om en juridisk person eller ett transportmedel som indirekt kan hänföras till en sådan person. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

#### *Registrering av känsliga personuppgifter*

10 § Uppgifter om en person får inte registreras i det allmänna spaningsregistret på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Trots bestämmelsen i första stycket får uppgifter om en person som registreras på annan grund kompletteras med sådana uppgifter som avses i första stycket om det är absolut nödvändigt för syftet med registreringen.

Uppgifter som beskriver en persons utseende ska alltid utformas på ett objektivt sätt med respekt för människovärdet.

*Tillgången till personuppgifter*

11 § Tillgången till personuppgifter i det allmänna spaningsregistret ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

*Sökning*

12 § Uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv får inte användas som sökbegrepp vid sökning i det allmänna spaningsregistret. Detta hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

13 § Uppgifter i det allmänna spaningsregistret som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara.

*Utlämnande av uppgifter och uppgiftsskyldighet*

14 § Personuppgifter i det allmänna spaningsregistret som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

15 § Personuppgifter får lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Om det är förenligt med svenska intressen, får uppgifter vidare lämnas till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott.

Av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) följer att uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation även i vissa andra fall.

**16 §** Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) ska personuppgifter i det allmänna spaningsregistret lämnas till

1. polismyndighet, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet, eller

2. polismyndighet, om myndigheten har behov av uppgifterna i annan verksamhet än den brottsbekämpande verksamheten och det finns särskilda skäl för att lämna ut dem.

Regeringen meddelar föreskrifter om att uppgifter får lämnas ut till andra myndigheter än de som anges i första stycket.

#### *Utlämnande av uppgifter på medium för automatiserad behandling*

**17 §** Endast enstaka personuppgifter i det allmänna spaningsregistret får lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall har beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall.

#### *Direktåtkomst*

**18 §** Polismyndigheter, Ekobrottsmyndigheten, Tullverket och Kustbevakningen får medges direktåtkomst till det allmänna spaningsregistret.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

*Gallring*

19 § Uppgifter i det allmänna spaningsregistret om en person som har registrerats enligt 3 § ska gallras senast tre år efter det att uppgiften om misstanke om brott registrerades. Om uppgiften avser misstanke om brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver dock uppgifterna inte gallras förrän fem år efter registreringen.

Om en ytterligare uppgift om personen förs in i registret, behöver uppgifterna om den registrerade personen inte gallras förrän

1. fem år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,

2. tre år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om annat brott än i 1, eller

3. ett år från det att den nya uppgiften fördes in i registret, om uppgiften inte avser misstanke om brott.

Den tid under vilken en person som har registrerats enligt 3 § avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i första och andra styckena.

Uppgifter om en person som avses i 4 § ska gallras senast när uppgifterna om den person som har registrerats enligt 3 § och som uppgifterna har samband med gallras.

20 § Uppgifter om en juridisk person, ett transportmedel eller annat föremål som har registrerats enligt 5 § ska gallras senast tre år efter den senaste registreringen. Om den senaste införda uppgiften avser ett brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver dock uppgifterna inte gallras förrän fem år efter det att den senaste uppgiften infördes.

21 § Vad som föreskrivs i 19 och 20 §§ hindrar inte att regeringen eller den myndighet som regeringen bestämmer

1. meddelar föreskrifter om att uppgifter gallras vid en tidigare tidpunkt, eller bevaras för historiska, statistiska eller vetenskapliga ändamål, eller

2. i ett enskilt fall beslutar att en uppgift ska bevaras om det finns synnerliga skäl för det.

Ett beslut enligt första stycket 2 ska omprövas varje år.

#### *Rättelse och skadestånd*

22 § Bestämmelserna i 28 och 48 §§ personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen.

---

Denna lag träder i kraft den 1 januari 2009 och gäller till och med den 31 december 2014.

## 2.3 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 28 kap. 12 a och 12 b §§ rättegångsbalken ska ha följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

### 28 kap. 12 a §<sup>1</sup>

Kroppsbesiktning genom tagande av salivprov får ske på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera uppgifter om resultatet av analysen i det DNA-register eller det utredningsregister som förs enligt *polisdatalagen (1998:622)*.

Kroppsbesiktning genom tagande av salivprov får ske på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera uppgifter om resultatet av analysen i det DNA-register eller det utredningsregister som förs enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet*.

---

<sup>1</sup> Senaste lydelse 2005:878.

12 b §<sup>2</sup>

Kroppsbesiktning genom tagande av salivprov får ske på annan än den som skäligen kan misstänkas för ett brott, om

1. syftet är att genom en DNA-analys av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och

2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.

Analysresultatet får inte jämföras med de uppgifter som finns registrerade i register som förs enligt *polisdatalagen* (1998:622) eller i övrigt användas för annat ändamål än det för vilket provet har tagits.

Första stycket gäller inte den som är under 15 år.

Kroppsbesiktning genom tagande av salivprov får ske på annan än den som skäligen kan misstänkas för ett brott, om

1. syftet är att genom en DNA-analys av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och

2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.

Analysresultatet får inte jämföras med de uppgifter som finns registrerade i register som förs enligt *lagen* (2008:000) om *behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller i övrigt användas för annat ändamål än det för vilket provet har tagits.

Första stycket gäller inte den som är under 15 år.

---

Denna lag träder i kraft den 1 januari 2009.

---

<sup>2</sup> Senaste lydelse 2005:878.



## 2.4 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 5 kap. 1 och 7 §§, 7 kap. 41 § och 9 kap. 17 § sekretesslagen (1980:100)<sup>1</sup> ska ha följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

### 5 kap. 1 §<sup>2</sup>

Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,
2. angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,
3. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde,
4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott, eller
5. Finansinspektionens verksamhet som rör övervakning enligt lagen (2005:377) om straff för marknadsmissbruk vid handel med finansiella instrument,

om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot ri-

För uppgift som hänför sig till verksamhet hos polisen enligt 2 kap. 5 § 1 lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller till verksamhet hos Säkerhetspolisen

<sup>1</sup> Lagen omtryckt 1992:1474.

<sup>2</sup> Senaste lydelse 2006:697.

*kets säkerhet eller förebygga terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott* gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Detsamma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

*enligt 5 kap. 2 § 1 samma lag* gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Detsamma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott samt hos tillsynsmyndigheten i konkurs och hos Kronofogdemyndigheten för uppgift som angår misstanke om brott.

Utan hinder av sekretessen enligt andra stycket kan enskild få uppgift om huruvida han eller hon förekommer i Säkerhetspolisens register med anledning av den verksamhet som bedrevs med stöd av

1. personalkontrollkungörelsen (1969:446) och de tilläggsföreskrifter som utfärdats med stöd av den,
2. förordningen den 3 december 1981 med vissa bestämmelser om verksamheten vid Rikspolisstyrelsens säkerhetsavdelning, eller
3. motsvarande äldre bestämmelser.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i andra stycket om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling som hänför sig till sådan verksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

7 §<sup>3</sup>

Sekretess gäller i verksamhet som avser rättsligt samarbete på begäran av annan stat eller mellanfolklig domstol för uppgift som hänför sig till

1. utredning enligt bestämmelserna om förundersökning i brottmål, eller
2. angelägenhet som angår tvångsmedel,  
om det kan antas att det varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen (1998:622)* och lagen om Schengens informationssystem.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *lagen (2008:000) om behandling av personuppgifter i polisens brottbekämpande verksamhet*

<sup>3</sup> Senaste lydelse 2003:1161.

och lagen om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst fyrtio år.

## 7 kap.

### 41 §<sup>4</sup>

Sekretess gäller hos polismyndighet och åklagarmyndighet, samt hos Rikspolisstyrelsen, Tullverket, Kustbevakningen och Migrationsverket, för uppgift om enskilda personliga förhållanden i en angelägenhet som avser en framställning enligt 3 § lagen (2000:344) om Schengens informationssystem

1. om omhändertagande av en person som har efterlysts för överlämnande eller utlämning,

2. om att en person *skall* nekast tillträde till eller uppehållstillstånd i Schengenstaterna (spärlista),

2. om att en person *ska* nekast tillträde till eller uppehållstillstånd i Schengenstaterna (spärlista),

3. om tillfälligt omhändertagande av en person med hänsyn till dennes eller någon annans säkerhet, samt

4. om dold övervakning eller särskilda kontrollåtgärder, om det inte står klart att uppgiften kan lämnas ut utan att den enskilde eller någon honom närstående lider men.

Sekretess gäller hos myndighet som prövar ansökningar om visering och uppehållstillstånd för uppgift om enskilda personliga förhållanden i en angelägenhet som avser en sådan framställning som avses i första stycket 2 under samma förutsättningar som anges i första stycket.

Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen* (1998:622) och lagen (2000:344) om Schengens informationssystem.

Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i *lagen* (2008:000) om *behandling av personuppgifter i polisens brottsbekämpande verksamhet* och

<sup>4</sup> Senaste lydelse 2003:1161.

lagen (2000:344) om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

### 9 kap.

#### 17 §<sup>5</sup>

Sekretess gäller för uppgift om enskilds personliga och ekonomiska förhållanden, om inte annat följer av 18 §

1. i utredning enligt bestämmelserna om förundersökning i brottmål,

2. i angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,

3. i angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),

4. i åklagarmyndighets, polismyndighets, Skatteverkets, Statens kriminaltekniska laboratoriums, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,

5. i Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller polismyndighet i brottmål,

6. i register som förs av Rikspolisstyrelsen enligt *polisdatalagen* (1998:622) eller som annars behandlas där med stöd av samma lag,

6. i register som förs av Rikspolisstyrelsen enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottbekämpande verksamhet* eller som annars behandlas där med stöd av samma lag,

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

8. i det register som förs enligt *lagen (2008:000) om polisens allmänna spaningsregister*,

---

<sup>5</sup> Senaste lydelse 2006:697.

8. i register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,

9. i särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 15 kap. 1 §,

10. i register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas med stöd av samma lag,

om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider skada eller men.

Sekretess enligt första stycket 2 gäller hos domstol i dess rättsskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till den enskilde 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 annat allvarligt men om uppgiften röjs. Av 12 kap. 2 § andra stycket framgår att även sekretessen enligt första stycket 1 är begränsad hos domstol.

Sekretess enligt första stycket gäller hos tillsynsmyndigheten i konkurs för uppgift som angår misstanke om brott.

9. i register som förs av Skatteverket enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,

10. i särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 15 kap. 1 §,

11. i register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas med stöd av samma lag,

Sekretess gäller i verksamhet, som avses i första stycket, för anmälan eller utsaga från enskild, om det kan antas att fara uppkommer för att någon utsätts för våld eller annat allvarligt men om uppgiften röjs.

Utan hinder av sekretessen får en skadelidande, eller den som den skadelidande överlåtit sin rätt till, ta del av en uppgift

1. i en nedlagd förundersökning eller i en förundersökning som avslutats med ett beslut om att åtal inte *skall* väckas,

1. i en nedlagd förundersökning eller i en förundersökning som avslutats med ett beslut om att åtal inte *ska* väckas,

2. i en annan brottsutredning som utförts enligt bestämmelserna i 23 kap. rättegångsbalken och som avslutats på annat sätt än med beslut att väcka åtal, med strafföreläggande eller med föreläggande av ordningsbot, eller

3. i en avslutad utredning enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

om den skadelidande, eller den som den skadelidande överlåtit sin rätt till, behöver uppgiften för att kunna få ett anspråk på skadestånd eller på bättre rätt till viss egendom tillgodosett och det inte bedöms vara av synnerlig vikt för den som uppgiften rör eller någon närstående till honom eller henne att den inte lämnas ut.

Utan hinder av sekretessen får en uppgift också lämnas ut

1. till enskild enligt vad som föreskrivs i den särskilda lagstiftningen om unga lagöverträdare,

2. till enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) samt i förordning som har stöd i den lagen,

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, *polisdatalagen* (1998:622), lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och i lagen (2005:787) om behand-

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar, lagen (2005:787) om behandling av uppgifter i Tullverkets

ling av uppgifter i Tullverkets brottsbekämpande verksamhet och lagen (2008:000) om behandling av personuppgifter i samt i förordningar som har stöd i dessa lagar, samt i förordningar som har stöd i dessa lagar,

4. till enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

Utan hinder av sekretessen får polisen på begäran av den som lidit person- eller sakskada vid en trafikolycka lämna uppgift om identiteten hos en trafikant som haft del i olyckan.

Utan hinder av sekretessen enligt första stycket 1 får uppgift lämnas till konkursförvaltare, om uppgiften kan antas ha betydelse för konkursutredningen.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i första stycket 1–4 eller 6 eller motsvarande verksamhet enligt äldre bestämmelser, om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling gäller sekretessen i högst sjuttio år.

---

Denna lag träder i kraft den 1 januari 2009.



## 2.5 Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 12, 21 och 22 §§ säkerhetsskyddslagen (1996:627) ska ha följande lydelse.

### *Nuvarande lydelse*

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller polisdatatalagen (1998:622). Med registerkontroll avses också att sådana personuppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller särskild undersökning i kriminalunderrättelseverksamhet.

### *Föreslagen lydelse*

#### 12 §<sup>1</sup>

Med registerkontroll avses kontroll av om det förekommer uppgifter om en person i register som förs av polisen eller om sådana uppgifter annars behandlas där i den brottsbekämpande verksamheten.

Vid en registerkontroll ska uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister. Vidare ska uppgifter hämtas som Säkerhetspolisen behandlar med stöd av 5 kap. lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Uppgifter får också hämtas från register som omfattas av 4 kap. lagen om behandling av personuppgifter i polisens brotts-

---

<sup>1</sup> Senaste lydelse 1998:625.

*bekämpande verksamhet eller lagen (2008:000) om polisens allmänna spaningsregister. Vidare får uppgifter hämtas som polisen i övrigt behandlar med stöd av 2 kap. 5 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, om uppgifterna har gjorts gemensamt tillgängliga.*

*Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av registerkontrollen.*

21 §<sup>2</sup>

Utlämnande av uppgifter vid registerkontroll får omfatta

1. för säkerhetsklass 1 eller 2: varje uppgift som finns tillgänglig om den kontrollerade och, om det är oundgängligen nödvändigt, om make eller sambo, och
2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret, misstankeregistret, SÄPO-registret och uppgifter som *annars* behandlas hos Säkerhetspolisen.
2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret *och* misstankeregistret *samt* uppgifter som behandlas hos Säkerhetspolisen.

22 §<sup>3</sup>

Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastnings-

Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastnings-

<sup>2</sup> Senaste lydelse 1998:625.

<sup>3</sup> Senaste lydelse 2006:347.

registret, misstankeregistret, registret *och* misstankeregistret  
*SÄPO-registret och* uppgifter *samt* uppgifter som behandlas  
som *annars* behandlas hos Sä- hos Säkerhetspolisen.  
kerhetspolisen.

---

Denna lag träder i kraft den 1 januari 2009.

## 2.6 Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs att 2 och 6 §§ lagen (1998:620) om belastningsregister ska ha följande lydelse.

### *Nuvarande lydelse*

### *Föreslagen lydelse*

<p>Belastningsregistret <i>skall</i> föras för att ge information om sådana belastningsuppgifter som behövs i verksamhet hos</p> <ol style="list-style-type: none"> <li>1. polis-, skatte- och tullmyndigheter för att förebygga, upptäcka och utreda brott,</li> <li>2. åklagarmyndigheter för beslut om förundersökning och åtal samt för utfärdande av strafföreläggande,</li> <li>3. allmänna domstolar för straffmätning och val av påföljd och</li> <li>4. polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.</li> </ol> <p>Registret får användas också för att till enskild lämna uppgifter som är av särskild betydelse i dennes verksamhet.</p>	<p>2 §<sup>1</sup></p> <p>Belastningsregistret <i>ska</i> föras för att ge information om sådana belastningsuppgifter som behövs i verksamhet hos</p> <ol style="list-style-type: none"> <li>1. polismyndigheter, Skatteverket, Tullverket och Kustbevakningen för att förebygga, upptäcka och utreda brott,</li> <li>2. åklagarmyndigheter för beslut om förundersökning och åtal samt för utfärdande av strafföreläggande,</li> <li>3. allmänna domstolar för straffmätning och val av påföljd och</li> <li>4. polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.</li> </ol> <p>Registret får användas också för att till enskild lämna uppgifter som är av särskild betydelse i dennes verksamhet.</p>
---	---

<p>Personuppgifter ur belastningsregistret <i>skall</i> lämnas ut om det begärs av</p>	<p>6 §<sup>2</sup></p> <p>Personuppgifter ur belastningsregistret <i>ska</i> lämnas ut om det begärs av</p>
--	---

<sup>1</sup> Senaste lydelse 1999:91.

<sup>2</sup> Senaste lydelse 1999:91.

1. Riksdagens ombudsmän, Justitiekanslern eller Datainspektionen för deras tillsynsverksamhet,

2. polis-, skatte-, tull- eller åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3, 2. polismyndighet, Skatteverket, Tullverket, Kustbevakningen, åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,

3. förvaltningsdomstol för prövning enligt 2 § första stycket 4 eller

4. myndighet i övrigt i den utsträckning regeringen för vissa slag av ärenden föreskriver det eller för ett särskilt fall ger tillstånd till det.

Regeringen får föreskriva att en myndighet som avses i första stycket får ha direktåtkomst till registret.

---

Denna lag träder i kraft den 1 januari 2009.

## 2.7 Förslag till lag om ändring i lagen (1998:621) om misstankeregister

Härigenom föreskrivs att 2 och 5 §§ lagen (1998:621) om misstankeregister ska ha följande lydelse.

### *Nuvarande lydelse*

Misstankeregistret *skall* föras för att underlätta tillgången till sådana uppgifter om skäligen misstanke om brott som behövs i verksamhet hos

1. polis-, skatte- och tullmyndigheter för att samordna förundersökningar mot en person och för att förebygga, upptäcka och utreda brott,

2. åklagarmyndigheter för beslut om förundersökning och åtal och

3. polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.

Registret får användas också för att till enskild lämna uppgifter som är av särskild betydelse i dennes verksamhet.

### *Föreslagen lydelse*

#### 2 §<sup>1</sup>

Misstankeregistret *ska* föras för att underlätta tillgången till sådana uppgifter om skäligen misstanke om brott som behövs i verksamhet hos

1. polismyndigheter, Skatteverket, Tullverket och Kustbevakningen för att samordna förundersökningar mot en person och för att förebygga, upptäcka och utreda brott,

---

<sup>1</sup> Senaste lydelse 1999:92.

5 §<sup>2</sup>

Uppgifter ur misstankeregistret *skall* lämnas ut om det begärs av

1. polis-, skatte-, tull- eller åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,

2. myndighet i övrigt i den utsträckning regeringen för vissa slag av ärenden föreskriver det eller för ett särskilt fall ger tillstånd till det.

Regeringen får föreskriva att en myndighet som avses i första stycket får ha direktåtkomst till registret.

Att uppgifter får lämnas ut i vissa andra fall framgår av 14 kap. sekretesslagen (1980:100).

Uppgifter ur misstankeregistret *ska* lämnas ut om det begärs av

1. polismyndighet, Skatteverket, Tullverket, Kustbevakningen, åklagarmyndighet eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,

---

Denna lag träder i kraft den 1 januari 2009.

---

<sup>2</sup> Senaste lydelse 1999:92.

## 2.8 Förslag till lag om ändring i lagen (2000:344) om Schengens informationssystem

Härigenom föreskrivs att 5 § lagen (2000:344) om Schengens informationssystem ska ha följande lydelse.

### *Nuvarande lydelse*

Registret *skall* endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.

Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *polisdatalagen* (1998:622) eller annan svensk författning.

### *Föreslagen lydelse*

#### 5 §

Registret *ska* endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.

Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller annan svensk författning.

---

Denna lag träder i kraft den 1 januari 2009.



## 2.9 Förslag till lag om ändring i lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet

Härigenom föreskrivs att 1 § lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet ska ha följande lydelse.

*Lydelse enligt proposition Föreslagen lydelse  
2006/07:133*

### 1 §

Säkerhets- och integritets-  
skyddsnämnden (nämnden)  
*skall* utöva tillsyn över brotts-  
bekämpande myndigheters an-  
vändning av hemliga tvångs-  
medel och kvalificerade  
skyddsidentiteter och därmed  
sammanhängande verksamhet.

Nämnden *skall* även utöva  
tillsyn över *Säkerhetspolisens*  
behandling av uppgifter enligt  
*polisdatalagen (1998:622), sär-  
skilt med avseende på 5 § den  
lagen.*

Säkerhets- och integritets-  
skyddsnämnden (nämnden)  
*ska* utöva tillsyn över brotts-  
bekämpande myndigheters an-  
vändning av hemliga tvångs-  
medel och kvalificerade  
skyddsidentiteter och därmed  
sammanhängande verksamhet.

Nämnden *ska* även utöva  
tillsyn över *polisens* behandling  
av uppgifter enligt *lagen  
(2008:000) om behandling av  
personuppgifter i polisens brotts-  
bekämpande verksamhet och  
lagen (2008:000) om polisens  
allmänna spaningsregister.  
Tillsynen ska särskilt avse be-  
handlingen av sådana känsliga  
personuppgifter som avses i  
2 kap. 8 § lagen om behandling  
av personuppgifter i polisens  
brottsbekämpande verksamhet  
och 10 § lagen om polisens all-  
männa spaningsregister.*

Tillsynen *skall* särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

Tillsynen *ska* särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

---

Denna lag träder i kraft den 1 januari 2009.

### 3 Bakgrund

Polisdatalagen (1998:622) innehåller bestämmelser om behandling av personuppgifter hos polisen. Den bygger på personuppgiftslagen (1998:204) och innehåller de särregler som har ansetts nödvändiga i polisens verksamhet. I övrigt gäller personuppgiftslagen. Polisdatalagen utgör bara en del av lagstiftningen om behandling av personuppgifter i polisens verksamhet. Övriga lagar som reglerar sådan behandling är lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem och lagen (2006:444) om passagerarregister. En stor del av den behandling av personuppgifter som sker hos polisen är dock inte författningsreglerad. Enligt övergångsbestämmelserna till polisdatalagen gäller den upphävda datalagen (1973:289) fortfarande för de register som den 24 oktober 1998 fördes med Datainspektionens tillstånd. Detta gäller flera av de stora polisregistren. Övergångsbestämmelserna har förlängts och gäller till utgången av år 2007. En ytterligare förlängning till utgången av år 2008 har föreslagits i propositionen Övergångsbestämmelserna till polisdatalagen (prop. 2007/08:6).

Den 9 december 1999 tillkallades en särskild utredare med uppdrag att följa genomförandet av den nya polisregisterlagstiftningen och påtala eventuella brister. Utredaren skulle överväga om det behövde vidtas några åtgärder för att lagstiftningen skulle uppnå sitt syfte att ge en effektiv brottsbekämpning och samtidigt värna om den enskildes personliga integritet. Utredningen antog namnet Polisdatautredningen.

Den 19 december 2001 överlämnade utredningen betänkandet *Behandling av personuppgifter i polisens verksamhet* (SOU 2001:92). En sammanfattning av betänkandet finns i *bilaga 1*. Lagförslagen i betänkandet finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. En remissammanställning finns tillgänglig i Justitiedepartementet (dnr Ju2001/8624/PO).

Remissinstanserna godtog i allmänhet Polisdatautredningens förslag att den nuvarande polisdatalagen ska ersättas med en helt ny reglering. I fråga om enskildheter i förslagen var dock remissynpunkterna mera blandade. Flera remissinstanser efterlyste närmare analys angående olika delar av förslaget. Under den fortsatta beredningen av ärendet har det framkommit att förslaget behöver ändras och kompletteras i så många olika avseenden att ett nytt underlag måste tas fram och remitteras. Denna promemoria utgör det underlaget.

Inom Regeringskansliet (Försvarsdepartementet) pågår även ett arbete med att ta fram ett förslag till lag om Kustbevakningens behandling av personuppgifter. Med anledning av detta övervägs i vad mån de grundläggande principer som i denna promemoria förslås gälla för polisens behandling av personuppgifter bör gälla även för Kustbevakningen.

Kustbevakningen har i en framställan till Justitiedepartementet begärt att myndigheten i sin brottsbekämpande verksamhet ska få tillgång till uppgifter i belastningsregistret och misstanke- registret genom direktåtkomst (dnr Ju2005/319/PO), se *bilaga 4*. Kustbevakningens framställan har remitterats. En förteckning över remissinstanserna finns i *bilaga 5*. En remissammanställning finns tillgänglig i Justitiedepartementet (dnr Ju2005/319/PO). Promemorian innehåller förslag till ändringar i lagen om belastningsregister och lagen om misstankeregister som syftar till att tillgodose Kustbevakningens behov av tillgång till uppgifter ur registren.

## 4 Gällande rätt m.m.

### 4.1 Inledning

De grundläggande bestämmelserna om behandling av personuppgifter finns i personuppgiftslagen (1998:204). Genom lagen genomfördes Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Personuppgiftslagen är tillämplig generellt, om det inte i annan lag eller förordning har meddelats avvikande bestämmelser. Direktivet omfattar därmed inte all personuppgiftsbehandling. Verksamhet som rör allmän säkerhet och statens verksamhet på straffrättens område omfattas t.ex. inte. Sedan slutet av 1990-talet har det utöver personuppgiftslagen utarbetats en stor mängd författningar med bestämmelser om behandling av personuppgifter, däribland polisdatalagen (1998:622). Syftet har varit att anpassa lagstiftningen till de särskilda behov som myndigheterna har haft i sina respektive verksamheter och göra avvägningar mellan behovet av effektivitet i berörd verksamhet och behovet av skydd för enskildas integritet.

Utöver en beskrivning av gällande rätt innehåller detta kapitel en redogörelse för aktuella internationella överenskommelser och rekommendationer på dataskyddsområdet. Dessa utgör en utgångspunkt för arbetet. Vidare redovisas bl.a. vissa initiativ inom Europeiska unionen (EU).

## 4.2 Internationella överenskommelser och personuppgiftslagen

### 4.2.1 Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som svensk lag. Det är framförallt artiklarna 8 och 13 i konventionen som har betydelse för myndigheters rätt att behandla personuppgifter.

Enligt artikel 8 har var och en rätt till respekt bl.a. för sitt privat- och familjeliv. En offentlig myndighet får inte inskränka åtnjutandet av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

I kriteriet ”med stöd av lag” ligger, utöver att intrånget ska ha stöd i nationell lag, att den åberopade lagen måste uppfylla vissa minimikrav i fråga om kvalitet och tydlighet. En rättighetsinskränkande tolkning av lagen ska kunna förutses och lagen ska vara allmänt tillgänglig. De syften för vilka intrång tillåts har tolkats ganska extensivt av Europadomstolen, men domstolen avgör vad som kan anses nödvändigt för att tillgodose ett i och för sig legitimt syfte. Det som genomsyrar hela konventionen är att åtgärder som innefattar intrång i en skyddad rättighet kan godtas endast om de är proportionerliga. Det innebär att intrånget måste svara mot ett mycket angeläget socialt behov och stå i rimlig proportion till det syfte som ska uppnås.

I artikel 13 föreskrivs att var och en, vars i konventionen angivna fri- och rättigheter kränkts, ska ha tillgång till ett effektivt rättsmedel inför en nationell myndighet. Detta gäller även om kränkningen förövats av någon under utövning av offentlig myndighet. Innebörden av artikeln är att den enskilde ska ha till-

gång till en nationell instans för att kunna få saken prövad och kunna få rättelse. Prövningen kan utföras av domstol, men något krav på domstolsprövning uppställs inte. Prövning av en stats regering eller av en förvaltningsmyndighet kan vara tillräcklig.

#### 4.2.2 Dataskyddskonventionen m.m.

Bestämmelser av betydelse för automatisk databehandling av personuppgifter finns i bl.a. Europarådets konvention från 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen). Dataskyddskonventionen trädde i kraft den 1 oktober 1985. Samtliga medlemsstater i EU har ratificerat konventionen. Konventionen är alltså bindande för medlemsstaterna.

Dataskyddskonventionens innehåll kan ses som en precisering av skyddet för enskilda vid användning av automatisk databehandling enligt artikel 8 i Europakonventionen. Dataskyddskonventionens syfte är att säkerställa den enskildes rätt till personlig integritet i samband med behandling av personuppgifter och att förbättra förutsättningarna för ett fritt informationsflöde över gränserna.

Dataskyddskonventionen innehåller principer för dataskydd som de konventionsanslutna staterna måste uppfylla i sin nationella lagstiftning. Personuppgifter som är föremål för automatisk databehandling ska hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Uppgifterna måste vara relevanta för ändamålen och får inte senare användas på ett sätt som är oförenligt med dessa. Vidare måste uppgifterna vara riktiga och aktuella och uppgifterna får inte bevaras längre än vad som är nödvändigt för ändamålen.

Vissa typer av personuppgifter får behandlas endast om den nationella lagen ger ett ändamålsenligt skydd. Till sådana personuppgifter hör uppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, hälsa, sexualliv samt uppgifter om brott.

För att skydda personuppgifter mot bl.a. oavsiktlig eller otil-låten förstörelse föreskriver konventionen att lämpliga skyddsåtgärder ska vidtas. Vidare ska den registrerade ha möjlighet till insyn i register och till att få uppgifter rättade. I vissa fall får undantag göras från bestämmelserna om uppgifternas beskaffenhet och rätten till insyn. Sådana inskränkningar i den enskildes skydd förutsätter stöd i den nationella lagstiftningen och att inskränkningen är nödvändig i ett demokratiskt samhälle för vissa angivna ändamål, t.ex. statens ekonomiska intressen och brottsbekämpning samt för att skydda enskildas fri- och rättigheter.

Dataskyddskonventionens roll som riktmärke för automatiserad behandling av personuppgifter inom Europeiska unionen har i princip övertagits av dataskyddsdirektivet. Direktivet omfattar dock inte behandling av personuppgifter inom områden som t.ex. allmän säkerhet, försvar och statens säkerhet. På dessa områden är dataskyddskonventionen således fortfarande av betydelse.

Europarådets ministerkommitté har under år 2001 antagit ett tilläggsprotokoll till dataskyddskonventionen. Det innehåller bestämmelser om tillsynsmyndigheter och överföring av personuppgifter till länder som inte är bundna av konventionen. Sverige undertecknade och ratificerade tilläggsprotokollet den 8 november 2001. Tilläggsprotokollet trädde i kraft den 1 juli 2004.

Även Organisationen för ekonomiskt samarbete och utveckling (OECD) har utarbetat internationella riktlinjer om integritetsskydd och persondataflöde över gränserna. Ett antal internationella organisationer och företag har antagit egna regler om dataskydd som bygger på OECD:s riktlinjer. Riktlinjerna motsvarar i princip de bestämmelser som finns i dataskyddskonventionen.



### 4.2.3 Europarådets rekommendation No. R (87) 15

Utöver dataskyddskonventionen har Europarådet tagit fram rekommendationer om dataskydd sektorsvis, bl.a. en rekommendation, No. R (87) 15, som reglerar användningen av personuppgifter inom polissektorn. Rekommendationen innehåller speciella skyddsregler för personuppgifter som polisen samlar in, lagrar, använder eller överför med hjälp av automatiserad behandling i syfte att förhindra och bekämpa brott eller upprätthålla allmän ordning. Endast sådana uppgifter som är nödvändiga för att förhindra en verklig fara eller bekämpa ett visst brott får samlas in, om inte den nationella lagstiftningen tillåter ett mer omfattande uppgiftssamlande. Olika kategorier av lagrade uppgifter ska så långt som möjligt kunna skiljas från varandra efter graden av riktighet och tillförlitlighet ("the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability"). I synnerhet ska uppgifter som grundar sig på fakta kunna skiljas från uppgifter som grundar sig på omdömen eller personliga värderingar.

### 4.2.4 Europeiska unionens stadga om de grundläggande rättigheterna

Den 7 december 2000 tillkännagavs Europeiska unionens stadga om de grundläggande rättigheterna av parlamentet, rådet och kommissionen. I stadgan bekräftas de rättigheter som har sin grund i medlemsstaternas gemensamma författningstraditioner och internationella förpliktelser samt i Fördraget om Europeiska unionen och gemenskapsfördragen. Stadgans syfte är att kodifiera de grundläggande fri- och rättigheter som EU redan erkänner. För närvarande är stadgan inte mer än en viljeförklaring avseende de redan existerande rättigheterna.

I stadgans artikel 8 föreskrivs att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Personuppgifter ska behandlas lagenligt för bestämda ändamål och på

grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. En oberoende myndighet ska kontrollera att reglerna efterlevs. Stadgan avser endast verksamhet som utförs av EU:s egna organ och institutioner och blir tillämplig för medlemsstaterna endast i de fall de tillämpar EG-rätten. Stadgan är följaktligen inte tillämplig avseende nationell lagstiftning inom områden där EU inte har lagstiftningskompetens.

Såvitt avser de garanterade rättigheternas räckvidd anförs i stadgan att varje begränsning i utövningen av de rättigheter och friheter som erkänns i stadgan ska vara föreskrivna i lag och vara förenliga med proportionalitetsprincipen och det väsentliga innehållet i fri- och rättigheterna. Hänvisning görs också till de grundläggande fördragen och Europakonventionen. De rättigheter som skyddas i stadgan ska ha samma innebörd och räckvidd som de som skyddas i konventionen. Stadgans artiklar får inte tolkas som att de inskränker eller inkräktar på rättigheter enligt andra konventioner eller överenskommelser om fri- och rättigheter.

#### **4.2.5 Dataskyddsdirektivet och personuppgiftslagen**

Dataskyddsdirektivet (se avsnitt 4.1) syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna. Medlemsstaterna får inom den ram som anges i direktivet närmare precisera villkoren för när behandling av personuppgifter får förekomma. Sådana preciseringar får dock inte hindra det fria flödet av personuppgifter inom unionen. Direktivet gäller inte, som framgått, för sådan behandling av personuppgifter som rör allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Direktivet omfattar således inte statens behandling av person-

uppgifter i brottsbekämpande verksamhet. Detta kommer att beröras närmare i avsnitt 6.5.1.

Personuppgiftslagen, genom vilken dataskyddsdirektivet införlivats i svensk rätt, har däremot gjorts generellt tillämplig och omfattar även sådan verksamhet som faller utanför direktivets tillämpningsområde (prop. 1997/98:44, bet. 1997/98:KU18, rskr. 1997/98:180). Lagen innehåller de generella regler som följer av direktivet i fråga om vilka krav som ställs vid behandling av personuppgifter, när sådan behandling är tillåten, information till den registrerade, korrigering av personuppgifter, säkerheten vid behandlingen m.m. Lagen anger den grundläggande ramen för behandling av personuppgifter. Särreglering i lag eller förordning gäller framför bestämmelserna i personuppgiftslagen. Att det krävs en särskild författning för att avvika från det integritetsskydd som personuppgiftslagen ger, är en garanti för att behovet av särregler övervägs noga i den ordning som gäller för författningsgivning.

Tidigare fanns det grundläggande regler om inrättande och förande av personregister med hjälp av automatisk databehandling i datalagen (1973:289). I denna lag avsågs med personregister ett register, förteckning eller andra anteckningar som fördes med hjälp av automatisk databehandling och som innehöll personuppgift som kunde hänföras till den som avsågs med uppgiften. Bara den som anmält sig till Datainspektionen och fått licens fick inrätta och föra personregister. För att få registrera känsliga personuppgifter krävdes dessutom ett särskilt tillstånd från Datainspektionen. Ett sådant tillstånd behövdes t.ex. som regel för att inrätta och föra register med uppgifter om hälsotillstånd eller sexualliv, omdömen om den registrerade eller personuppgifter som hämtats från något annat register. Om ett personregister hade beslutats av riksdagen eller regeringen, krävdes dock inget tillstånd.

Genom personuppgiftslagen avskaffades det tidigare licens- och tillståndsförfarandet. Utgångspunkten för personuppgiftslagen är i stället att behandling av personuppgifter är tillåten i de fall och på de villkor lagen anger.

Personuppgiftslagen innehåller generella riktlinjer för all behandling av personuppgifter. Begreppet behandling av personuppgifter omfattar i stort sett allt man kan göra med sådana uppgifter, exempelvis att samla in, söka, bevara och sprida uppgifter. Lagen omfattar i princip endast behandling av personuppgifter som är helt eller delvis automatiserad, dvs. i första hand datoriserad. Även manuell behandling kan dock omfattas, nämligen om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter vilka är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Enligt personuppgiftslagen ska en personuppgiftsansvarig se till att personuppgifter behandlas bara om det är lagligt. Den personuppgiftsansvarige ska vidare se till *att* personuppgifter behandlas på ett korrekt sätt och i enlighet med god sed, *att* personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål, *att* de inte behandlas för något ändamål som är oförenligt med det för vilket de samlades in, *att* de personuppgifter som behandlas är riktiga och om nödvändigt aktuella, *att* alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen *och att* personuppgifter inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Vidare reglerar personuppgiftslagen, som nämnts, när behandling av uppgifter är tillåten. Detta är i princip fallet när den registrerade har lämnat sitt samtycke eller när behandlingen är nödvändig av olika angivna skäl, bl.a. för att den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet och för att den personuppgiftsansvarige, eller tredje man till vilken personuppgifter lämnas ut, ska kunna utföra en arbetsuppgift i samband med myndighetsutövning.

Personuppgiftslagen förbjuder andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Det finns dock ett bemyndigande för regeringen, eller den myndighet som regeringen bestämmer, att

meddela föreskrifter om undantag från förbudet. Datainspektionen har meddelat sådana föreskrifter i DIFS 1998:3, jfr 9 § personuppgiftsförordningen (1998:1191).

Den 1 januari 2007 trädde vissa ändringar av personuppgiftslagen i kraft, vilka innebär att lagen i viss utsträckning utformas enligt en missbruksmodell (SFS 2006:398). Regleringen tar därmed inte sikte på själva hanteringen av personuppgifterna utan på att uppgifterna inte får missbrukas till skada för någons personliga integritet.

Behandling av personuppgifter i ostrukturerat material, t.ex. löpande text och enstaka ljud- och bildupptagningar, undantas från de flesta av personuppgiftslagens detaljerade hanteringsregler. Sådan behandling tillåts utan andra restriktioner än att den registrerades personliga integritet inte får kränkas.

Bestämmelserna i personuppgiftslagen redovisas närmare i samband med de förslag som lämnas i avsnitt 6.5.2.

#### 4.2.6 Europol

Medlemsstaterna i EU har genom Europolkonventionen beslutat att upprätta en europeisk polisbyrå, Europol. Sverige har tillträtt konventionen (prop. 1996/97:164, bet. 1997/98:JuU02, rskr. 1997/98:22). Målsättningen med Europol är att förbättra effektiviteten hos behöriga myndigheter i medlemsstaterna och deras samarbete när det gäller att förebygga och motverka viss definierad brottslighet, t.ex. grova narkotikabrott eller gränsöverskridande handel med barn som utnyttjas sexuellt.

För närvarande pågår det inom EU förhandlingar om att ersätta den nuvarande konventionen med ett rådsbeslut, se kommissionens förslag (KOM[2006]817 slutlig). Ambitionen är att förhandlingarna ska kunna avslutas vid halvårsskiftet 2008.

## 4.3 Den nuvarande polisregisterlagstiftningen

### 4.3.1 Allmänt om polisregisterlagstiftningen

Polisdatalagen trädde i kraft den 1 april 1999. Lagen, som gäller utöver personuppgiftslagen, utgör en del av lagstiftningen om polisens register. Vid sidan av polisdatalagen finns också lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2000:343) om internationellt polisiärt samarbete och lagen (2006:444) om passagerarregister. Lagen om belastningsregister och lagen om misstankeregister trädde i kraft den 1 januari 2000 och lagen om Schengens informationssystem den 1 december 2000. Dessa lagar behandlas närmare i anslutning till beskrivningarna av registren i *bilaga 6*.

### 4.3.2 Särskilt om polisdatalagen

Polisens möjligheter att föra kriminal- och polisregister reglerades tidigare av lagen (1963:197) om allmänt kriminalregister och lagen (1965:94) om polisregister m.m. Dessa lagar skrevs med utgångspunkten att registren skulle föras manuellt. Det rättsliga stödet för att föra vissa datoriserade register, t.ex. person- och belastningsregistret, fanns i stället i förordningen (1970:517) om rättsväsendets informationssystem (RI-förordningen). Många polisregister fördes – och förs – i stor utsträckning fortfarande enligt övergångsbestämmelserna till polisdatalagen med stöd av Datainspektionens tillstånd enligt datalagen (1973:289).

Polisdatalagen utgår från personuppgiftslagen och innehåller endast de särbestämmelser som har ansetts nödvändiga för polisens verksamhet. Polisdatalagen innehåller både allmänna regler om behandling av personuppgifter i polisiärt arbete och regler om vissa särskilda register. Behandling av personuppgifter som sker med stöd av lagen om belastningsregister, lagen om miss-

tankeregister, lagen om Schengens informationssystem eller lagen om passagerarregister faller utanför polisdatalagen.

Polisdatalagen gäller vid behandling av personuppgifter i polisens verksamhet och i polisverksamhet vid Ekobrottsmyndigheten för att förebygga brott och andra störningar av den allmänna ordningen och säkerheten, övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när något sådant inträffat eller bedriva spaning och utredning i fråga om brott som hör under allmänt åtal. Lagen innehåller bl.a. regler om behandling av uppgifter i kriminalunderrättelseverksamhet. Lagen innehåller särskilda bestämmelser om vissa register som förs med hjälp av automatiserad behandling. Dessa register är kriminalunderrättelseregister, register med uppgifter om DNA-analyser, fingeravtrycks- och signalementsregister samt SÄPO-registret. Registren behandlas närmare i *bilaga 6*.

#### 4.4 EU-initiativ m.m.

Inom ramen för EU-samarbetet förhandlas för närvarande flera rambeslut och andra rådsbeslut som kan komma att påverka lagstiftningen om behandling av personuppgifter inom polisen. Inom Justitiedepartementet bereds också en departementspromemoria om preskription vid allvarliga brott som bl.a. innefattar förslag till ändringar i polisdatalagen.

##### *Förslag till rambeslut om skydd för personuppgifter*

Inom EU:s råd förhandlas ett rambeslut om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (KOM[2005]475 slutlig). Förslaget presenterades av kommissionen i oktober 2005. Syftet är att åstadkomma ett sammanhållet instrument med dataskyddsbestämmelser för EU:s brottsbekämpande och straffrättsliga samarbete (tredje pelaren). Rambeslutet innehåller bland annat bestämmel-

ser om när och hur personuppgifter mottagna från en annan medlemsstat får behandlas, villkor för att få utbyta personuppgifter mottagna från en annan medlemsstat med tredjeland och den registrerades rättigheter. Målsättningen är att rådet ska nå en politisk överenskommelse om rambeslutet före slutet av år 2007.

### VIS

Kommissionen presenterade i november 2005 ett förslag till rådsbeslut som ska möjliggöra att brottsbekämpande myndigheter i medlemsstaterna samt Europol efter förfrågan får tillgång till uppgifter i EU:s informationssystem för viseringar (VIS) i syfte att förebygga, upptäcka och utreda terroristbrott och andra grova brott (9320/07 CATS 46 ENFOPOL 82 EUROPOL 56 VISA 154 COMIX 452). En politisk överenskommelse nåddes vid möte med ministerrådet för rättsliga och inrikes frågor den 12–13 juni 2007. Enligt den nuvarande lydelsen av beslutet ska en förfrågan från en brottsbekämpande myndighet vara ändamålsenlig och syfta till att förebygga, upptäcka och utreda terroristbrott samt andra grova brott. Europol ska ha behörighet att söka i VIS för de brott som anges i Europokonventionen. Förfrågningar måste gälla enskilda ärenden och det måste finnas anledning att tro att en slagning i VIS väsentligen kan bidra till brottsbekämpning. De brottsbekämpande enheterna ska vända sig med en motiverad begäran till de i varje land utsedda centrala "åtkomstpunkterna". Dessa ska kontrollera att samtliga villkor för tillgång till VIS är uppfyllda. Om villkoren är uppfyllda, ska åtkomstpunkten söka i VIS och föra över de begärda uppgifterna till den enhet som begärt dem.



*Prüm*

Den 27 maj 2005 ingick Belgien, Tyskland, Spanien, Frankrike, Luxemburg, Nederländerna och Österrike ett fördrag om fördjupat gränsöverskridande samarbete för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration. Fördraget undertecknades i den tyska staden Prüm. Medlemsstaternas målsättning är att utveckla informationsutbytet inom hela EU, framför allt avseende DNA-uppgifter, fingeravtryck och bilregisteruppgifter. Fördraget är öppet för alla EU:s medlemsstater att tillträda. Vid RIF-rådet den 15 februari 2007 nåddes en politisk principöverenskommelse om att integrera stora delar av Prümfördragets tredjepelarfrågor i EU:s regelverk. Ordförandeskapet presenterade därefter ett förslag till rådsbeslut, "Utkast till rådets beslut om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet" (6566/2007 REV 1 CRIMORG 33 ENFOPOL 33). En politisk överenskommelse nåddes vid möte med ministerrådet för rättsliga och inrikes frågor den 12–13 juni 2007.

*Förslag till rambeslut om utbyte av uppgifter ur kriminalregister*

Inom EU:s råd förhandlas vidare sedan år 2006 ett rambeslut om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll (KOM[2005]690 slutlig/2 [5463/06 REV 1 COPEN 1]). Förslagets övergripande syfte är att förbättra utbytet av information från medlemsstaternas kriminalregister. I dag sker detta utbyte med stöd av Europarådets konvention från 1959 om ömsesidig rättslig hjälp i brottmål och dess första tilläggsprotokoll från 1978 samt rådets beslut från den 21 november 2005 om utbyte av uppgifter ur kriminalregister. Kommissionen föreslår i rambeslutet att varje medlemsstat, som meddelar en dom mot en annan medlemsstats medborgare, ska informera medborgarstaten om domen. Medborgarsta-

ten ska därvid lagra informationen. Tanken är att varje medlemsstat ska ha information om alla de domar som har meddelats inom EU mot de egna medborgarna. Vidare syftar rambeslutet till att förkorta förfarandet när uppgifter ur kriminalregister begärs i ett enskilt ärende. Vid möte med ministerrådet för rättsliga och inrikes frågor den 12–13 juni 2007 nåddes en politisk överenskommelse om innehållet i rambeslutet.

*Förslag i departementspromemorian Preskription vid allvarliga brott*

I departementspromemorian Preskription vid allvarliga brott (Ds 2007:1) har föreslagits att preskription avskaffas för vissa särskilt allvarliga brott. Som en följdändring har föreslagits att gallringsfristerna förlängs för uppgifter om vissa brott i polisens spårregister (27 § polisdatalagen). Förslagen bereds för närvarande inom Justitiedepartementet.

## 5 Polisens register

### 5.1 Register och ärendehanteringssystem

Genom datalagen (1973:289) introducerades begreppet personregister som ett centralt begrepp i svensk datalagstiftning. Med personregister avsågs register, förteckning eller andra anteckningar som förs med hjälp av automatisk databehandling och som innehåller personuppgift som kan hänföras till den som avses med uppgiften. Med personuppgift avsågs enligt den lagen upplysning avseende enskild person. Den allmänt använda termen för ADB-baserade uppgiftssamlingar blev därmed register. Ordet återfinns i många författningar som reglerar myndigheters användande av automatisk databehandling i verksamheten, t.ex. i polisdatalagen.

Det traditionella registerbegreppet har ibland kritiserats. En orsak har varit att begreppet även har en teknisk anknytning och därför kan ha olika innebörd för olika yrkesgrupper. Vidare för det tankarna till på visst sätt organiserade eller systematiserade samlingar av uppgifter. Detta är inte längre ett helt rättvisande sätt att se på samlingar av uppgifter i elektronisk form. Uppgifter kan t.ex. införas ostrukturerat och oorganiserat i olika filer i en dator utan att detta förhindrar en effektiv hantering av uppgifterna för olika sammanställningar. Sökning i sådana filer görs inte efter särskilda bestämda sökord utan genom fritextsökning.

I personuppgiftslagen används inte begreppet register utan det talas i stället om behandling av personuppgifter. Det skulle i och för sig vara möjligt att även i specialförfattningar undvika begreppet register utan att ersätta det med något specifikt alter-

nativ, dvs. att endast tala om behandling av personuppgifter. Datalagskommittén uttalade dock i sitt betänkande Offentlighet, Integritet, Informationsteknik (SOU 1997:39 s. 343) att tillämpningsproblem inte hindrar att det som är ett regelrätt datoriserat register också kallas för det. Denna fråga behandlades också vid tillkomsten av polisdatalagen. Regeringen tog där upp kritiken mot registerbegreppet men framhöll att det inte helt bör undvikas, eftersom polisen måste ha tillgång till traditionella register för att kunna bedriva sin verksamhet och att det därför även i fortsättningen bör finnas särskilda bestämmelser rörande upprättandet och förändret av sådana register (prop. 1997/98:97 s. 102).

Det kan konstateras att flera av polisens samlingar av personuppgifter i elektronisk form är register i ordets mer egentliga bemärkelse, dvs. uppgifter som förs in på ett systematiskt sätt efter vissa kriterier och är sökbara endast med särskilda sökord. Detta gäller i första hand de äldre system som fortfarande förs med stöd av Datainspektionens tillstånd. Nya system som också kan betraktas som register är misstankeregistret, belastningsregistret och den nationella enheten av Schengens informationssystem. Registerbegreppet har således fortfarande relevans i vissa fall.

Dagens system inom polisen byggs dock företrädesvis som ärendehanteringssystem och inte som traditionella register. I dessa ärendehanteringssystem registreras hela aktmaterial. Grundtanken vid utvecklingen av nya system inom polisen är att man i så stor utsträckning som möjligt bara ska anteckna en uppgift en gång samt att uppgiften, om det behövs, därefter ska vidarebefordras automatiserat till andra ärendehanteringssystem. Begreppet register blir då mindre träffande.

## 5.2 Allmänt om polisens register

Registerstrukturen har sin bakgrund i tiden före den nuvarande polisdatalagen, när Datainspektionen gav tillstånd för polisen att

föra olika enskilda register. Strukturen är således inte ett resultat av någon övergripande planering. Detta medför bl.a. att samma uppgifter förekommer i flera olika system.

Polisens register kan indelas i tre grupper beroende på vilka bestämmelser som styr behandlingen, nämligen

- register som förs med stöd av särskilda bestämmelser i polisdatalagen eller annan lagstiftning,
- register som förs med stöd av allmänna bestämmelser i polisdatalagen och personuppgiftslagen, och
- register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av datalagen och tillstånd från Datainspektionen.

En uppdelning kan också göras mellan centrala och lokala register. De centrala registren förs av Rikspolisstyrelsen och innehåller uppgifter från hela riket. De lokala registren förs av en polismyndighet och innehåller därmed bara uppgifter från ett polisdistrikt.

De register som regleras särskilt i polisdatalagen är kriminalunderrättelseregister, register med uppgifter om DNA-analyser i brottmål, fingeravtrycks- och signalementsregister samt SÄPO-registret. Kriminalunderrättelseregister kan föras både på lokal och central nivå, medan övriga register som regleras i polisdatalagen är centrala. Det finns även särskilda bestämmelser om register i lagstiftning som gäller vid sidan av polisdatalagen, t.ex. i lagen om belastningsregister och lagen om misstankeregister. Därutöver finns centrala och lokala register som saknar särskild författningsreglering. Registren förs då med stöd av personuppgiftslagen och de allmänna bestämmelserna i polisdatalagen eller med stöd av datalagen och Datainspektionens tillstånd enligt övergångsbestämmelserna till polisdatalagen. Exempel på sådana centrala register är det allmänna spaningsregistret, det centrala brottsspaningsregistret samt beslags- och analysregistren. Rationell anmälningsrutin (RAR) och datoriserad utredningsrutin-tvångsmedel (DurTvå) är exempel på register på lokal nivå.

Polisen utvecklar kontinuerligt nya system för att stödja verksamheten. En redovisning av polisens register kan därför

aldrig bli helt fullständig. I *bilaga 6* finns dock en redovisning som tar upp system av större betydelse i polisens verksamhet.

## 6 En ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet

### 6.1 Bestämmelserna om polisens användning av personuppgifter behöver reformeras

**Promemorians bedömning:** En reform av bestämmelserna om polisens behandling av personuppgifter är nödvändig.

**Utredningens bedömning** överensstämmer med promemorians bedömning.

**Remissinstanserna** har tillstyrkt eller inte haft några invändningar mot detta.

#### Skälen för promemorians bedömning

##### *Allmänna utgångspunkter*

Information är en av polisens viktigaste resurser för att uppnå statsmakternas mål i det brottsbekämpande arbetet. Sedan många år är modern informationsteknik en naturlig del i polisens arbete och numera utförs praktiskt taget allt arbete till någon del med hjälp av sådan teknik. En väl utnyttjad informationsteknik är givetvis av största betydelse för polisens möjligheter att bedriva sin verksamhet på ett effektivt sätt. Samtidigt bör självfallet

informationshanteringen ske med respekt för enskildas integritet. Det är mot den bakgrunden angeläget att polisdatalagstiftningen är väl avvägd.

#### *Oklarheter i den nuvarande lagstiftningen*

Ett effektivt brottsbekämpande arbete förutsätter att de brottsbekämpande myndigheterna har goda möjligheter att samla in och bearbeta information av olika slag. De uppgifter som behöver kunna samlas in och bearbetas är såväl uppgifter med anknytning till konkreta brott (dvs. uppgifter i *brotsutredningar*) som uppgifter som avser förväntad eller pågående brottslig verksamhet (dvs. uppgifter i *kriminalunderrättelseverksamhet*). Utformningen av polisdatalagen har emellertid gett upphov till problem i olika avseenden. Ett exempel är oklarheterna kring begreppet kriminalunderrättelseverksamhet. Enligt den nuvarande lagstiftningen får uppgifter i sådan verksamhet behandlas endast under vissa förutsättningar. Behandling får ske dels om en särskild undersökning har inletts under ledning av Rikspolisstyrelsen eller en polismyndighet och det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas, dels inom ramen för registrering i kriminalunderrättelseregister. Det har ifrågasatts om inte behandlingen av personuppgifter i vissa faktiskt existerande polisregister till viss del skulle kunna tolkas som kriminalunderrättelseverksamhet i polisdatalagens mening. Behandlingen skulle därmed inte vara tillåten annat än inom ramen för en särskild undersökning eller i kriminalunderrättelseregister. Det är vidare osäkert i vilken utsträckning behandling av underrättelseuppgifter får ske lokalt, dvs. av en enskild tjänsteman genom användning av ordbehandling och e-post m.m. Ytterligare ett exempel på problem som polisdatalagens utformning har gett upphov till gäller polisens tänkta utbyggnad av ett dokument- och ärendehanteringssystem för att hantera informationsutbytet med Europol. Som redovisas närmare i *bilaga 6* har Datainspektionen ansett att den planerade behandlingen



utgör behandling av personuppgifter i kriminalunderrättelseverksamhet som inte överensstämmer med rekvisiten för behandling av sådana uppgifter i polisdatalagen.

Det finns alltså behov av en ny reglering som undanröjer dessa och andra oklarheter.

#### *Det behövs en mera teknikneutral lagstiftning*

Den elektroniska informationshanteringen inom polisens verksamhet har utvecklats snabbt. I dag lagrar polisen personuppgifter i ett stort antal olika databaser. Samma personuppgift kan lagras på flera olika ställen, i olika ”register”. Rikspolisstyrelsen har gjort bedömningen att detta sätt att hantera uppgifter kan leda till kvalitetsbrister (se promemoria om behandling av personuppgifter i polisverksamheten, dnr Ju2007/478/PO). Styrelsen planerar därför en modernisering av polisens datasystem. Tanken är att de uppgifter som behandlas i polisens verksamhet ska lagras gemensamt på en plats i stället för i separata register. Uppgifterna ska alltså i princip inte lagras mer än en gång. Åtkomsten till uppgifterna ska i de allra flesta fall inte – såsom i polisens nuvarande system – vara beroende av att en uppgift finns i ett särskilt register utan vara avhängigt andra kriterier, hänförliga till uppgifterna som sådana. Enligt Rikspolisstyrelsen kommer det planerade datasystemet att möjliggöra ett bättre integritetsskydd. Det blir bl.a. lättare att bygga upp behörighetssystem som gör det möjligt att lättare avgränsa en enskild tjänstemans åtkomst till de uppgifter som han eller hon behöver för att kunna utföra sina arbetsuppgifter. Tjänstemannens behov av information kan därigenom tillgodoses på ett rättssäkert sätt. En annan fördel är att det blir enklare att hålla lagrad information uppdaterad och tillförlitlig, eftersom utgångspunkten är att varje uppgift ska lagras endast en eller ett fåtal gånger. Risker att uppgifter bevaras i systemet längre än nödvändigt minskar också. Enligt Rikspolisstyrelsen kommer det över huvud taget att bli

lättare att avgränsa, kontrollera och övervaka all elektronisk åtkomst till uppgifter.

Rikspolisstyrelsens arbete med att förändra polisens system har redan inletts. För att styrelsen ska kunna slutföra det arbetet krävs det en ny lagstiftning som är mera teknikneutral och mindre knuten till registerbegreppet än polisdatalagen.

#### *Polisdatalagen är varken heltäckande eller konsekvent*

En svaghet i den nuvarande regleringen är bl.a. att den inte är heltäckande. Många register i polisens verksamhet förs således fortfarande med stöd av Datainspektionens tillstånd enligt den numera upphävda datalagen. Det behövs därför en ny reglering som, så långt detta är möjligt, omfattar all behandling av personuppgifter i polisens brottsbekämpande verksamhet (med vissa särskilda undantag, se avsnitt 6.3).

Den nuvarande lagstiftningen innebär vidare ett hinder för polisen att använda digital utrustning vid bild- och ljudupptagningar, eftersom själva upptagningen av bilder och ljud med digital utrustning innebär behandling av personuppgifter. Detta hinder framstår inte som motiverat och bör därför undanröjas genom ändrad lagstiftning.

#### *De brottsbekämpande myndigheterna måste ges goda förutsättningar för att samverka i brottsbekämpningen*

Det är från brottsbekämpningssynpunkt angeläget att samhällets samlade resurser används rationellt och effektivt. En utvecklad samverkan mellan de brottsbekämpande myndigheterna ger bättre förutsättningar att klara upp brott. En utgångspunkt måste vara att, med beaktande av befogade krav på skydd för enskildas integritet, var och en av de brottsbekämpande myndigheterna i den egna verksamheten har tillgång till uppgifter från andra brottsbekämpande myndigheter, i den mån uppgifterna

behövs i verksamheten. Uppgifter måste också få behandlas om det behövs för att polisen ska kunna fullgöra sina internationella förpliktelser. De brottsbekämpande myndigheternas tillgång till information behöver effektiviseras. Som beskrivs närmare i avsnitt 12.1 är en utvecklad samverkan mellan de brottsbekämpande myndigheterna också en förutsättning för att genomföra det arbete som sedan mitten av 1990-talet bedrivs av Rådet för Rättsväsendets Informationsförsörjning (RIF).

### *Sammanfattning*

Mot bakgrund av vad som nu har sagts bör den nuvarande lagstiftningen reformeras. De brister i lagstiftningen som har nämnts ovan bör åtgärdas. Som vi återkommer till i avsnitt 6.4 måste dock den närmare utformningen av de nya bestämmelserna föregås av en noggrann avvägning mellan å ena sidan intresset av en effektiv brottsbekämpning och å andra sidan intresset av skyddet för den personliga integriteten.

## **6.2 En ny lag införs**

**Promemorians förslag:** Polisdatlagen ersätts av en ny lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

**Utredningens förslag** överensstämmer med promemorians förslag.

**Remissinstanserna** har tillstyrkt eller inte haft några invändningar mot förslaget.

**Skälen för promemorians förslag:** Behandling av personuppgifter regleras generellt i personuppgiftslagen. I den mån något annat inte föreskrivs gäller alltså den lagen för behandling av personuppgifter även i polisens brottsbekämpande verksamhet. I

det lagstiftningsärende som föregick personuppgiftslagen (prop. 1997/98:44 s. 40 f.) uttalade den dåvarande regeringen att lagen i princip bara bör innehålla generella regler och att behovet av undantag och särregler för mer speciella områden får tillgodoses genom andra författningar. Regeringen framhöll att registerförfattningarna innehåller många preciserade och viktiga regler som inte rimligen kan ersättas av de generella bestämmelser som den nya lagen innehåller. Vid utskottsbehandlingen av förslaget uttalade Konstitutionsutskottet att det saknades anledning att avvika från den tidigare fastlagda målsättningen, att myndighetsregister med ett stort antal registrerade och ett särskilt känsligt innehåll ska regleras särskilt i lag (bet. 1997/98:KU18 s. 43). För polisens del finns i dag sådana bestämmelser i bl.a. polisdatalagen.

Vi anser inte att det finns skäl att nu göra någon annan bedömning när det gäller behovet av en särlagstiftning för polisens behandling av personuppgifter. Det bör alltså även i fortsättningen finnas en särskild lag för den behandling av personuppgifter som sker hos polisen. De problem som den nuvarande lagstiftningen har gett upphov till är av sådant slag och sådan omfattning att den nuvarande lagen bör ersättas med en helt ny lag.

### 6.3 Lagens tillämpningsområde

**Promemorians förslag:** Den nya lagen ska gälla vid all behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Den personuppgiftsbehandling som sker med stöd av de särskilda lagarna om belastningsregister, misstankeregister, Schengens informationssystem samt passagerarregister ska dock inte omfattas av den nya lagen. Lagen ska inte heller reglera personuppgiftsbehandling inom ramen för polisens allmänna spaningsregister. Den ska inte heller gälla vid insamling av personuppgifter genom allmän kameraövervakning, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning.

Lagen ska innehålla vissa bestämmelser om behandling av uppgifter om juridiska personer.

**Utredningens förslag** överensstämmer delvis med promemorians förslag. Utredningen har dock inte föreslagit att lagen ska omfatta polisverksamhet vid Ekobrottsmyndigheten. Den har inte heller föreslagit att lagen ska omfatta behandling av uppgifter om juridiska personer. Den har däremot föreslagit att lagen, liksom den nuvarande polisdatalagen, ska omfatta all den personuppgiftsbehandling som faller in under 2 § 1–3 polislagen (1984:387).

**Remissinstanserna** har i huvudsak inte haft någon invändning mot utredningens förslag i denna del. *Rikspolisstyrelsen* har dock ansett att den nya lagen ska omfatta all polisverksamhet enligt 2 § polislagen, dvs. även 2 § 4 och 5.

**Skälen för promemorians förslag:** Den nya lagen bör liksom i dag gälla vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten. Polisdatalagen gäller vid behandling av personuppgifter i polisens verksamhet för att (1) förebygga brott och andra störningar av den allmänna ordningen

och säkerheten, (2) övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när sådana inträffat, och (3) bedriva spaning och utredning i fråga om brott som hör under allmänt åtal. Detta motsvarar polisens uppgifter enligt 2 § 1–3 polislagen. Polisdatalagen omfattar alltså inte enbart personuppgiftsbehandling inom den brottsbekämpande verksamheten utan även personuppgiftsbehandling inom viss annan polisiär verksamhet. Den omfattar dock inte personuppgiftsbehandling inom sådan polisverksamhet som faller in enbart under 2 § 4 och 5 polislagen, dvs. verksamhet som består i att lämna allmänheten skydd, upplysningar och annan hjälp och annan verksamhet som ankommer på polisen enligt särskilda bestämmelser. Sådan personuppgiftsbehandling faller i stället in under personuppgiftslagen.

Frågan är då om den nya lagen, såsom utredningen har föreslagit, bör ha samma tillämpningsområde som 2 § 1–3 polislagen. Ett alternativ är att, såsom *Rikspolisstyrelsen* har förordat, låta lagen omfatta all personuppgiftsbehandling i polisens verksamhet. Ett annat alternativ är att begränsa lagens tillämpningsområde till personuppgiftsbehandling inom polisens brottsbekämpande verksamhet.

Vid valet mellan dessa alternativ är det naturligt att beakta vilka omständigheter som gör att personuppgiftslagens allmänna regler inte är helt ändamålsenliga vid personuppgiftsbehandling i polisiär verksamhet. Här finns det anledning att peka på flera olika förhållanden. För det första är det nödvändigt att i polisiär verksamhet behandla en stor mängd uppgifter som, typiskt sett, är känsliga till sin natur och inte bör ges en vidare spridning. För det andra gör sig särskilt starka samhällsintressen gällande inom delar av polisens verksamhet, vilket medför att sedvanliga avvägningar mellan berörda intressen i viss mån måste göras på ett sätt som tillåter större intrång i integriteten än vad som annars från proportionalitetssynpunkt hade kunnat tillåtas. Omständigheter av detta slag kan göra det befogat med särskilda – från personuppgiftslagen avvikande – bestämmelser om personuppgiftsbehandling. Det sagda gäller dock i varierande grad beträffande

olika delar av polisens verksamhet. Behovet av en särreglering är tydligast på det brottsbekämpande området. I annan polisverksamhet, t.ex. tillståndsgivning av olika slag, är behovet av särregler i förhållande till personuppgiftslagen litet eller obefintligt.

Vidare måste beaktas att svensk lagstiftning måste vara förenlig med dataskyddsdirektivet inom dess tillämpningsområde. I den utsträckning polisens verksamhet enligt 2 § polislagen omfattas av gemenskapsrätten är det därför nödvändigt att säkerställa att lagen uppfyller de krav som direktivet ställer upp. Lagtekniskt görs detta säkrast genom att personuppgiftslagen görs tillämplig på verksamhet som inte är undantagen från direktivets tillämpningsområde, dvs. verksamhet som inte rör allmän säkerhet, statens säkerhet eller verksamheten på straffrättens område (jfr artikel 3.2 dataskyddsdirektivet).

Vi anser därför att den nya lagen bör gälla endast behandling av personuppgifter som utförs i sådan polisiär verksamhet där det finns påtagliga skäl att reglera behandlingen på annat sätt än vad som följer av personuppgiftslagen.

Med denna utgångspunkt har man härefter att ta ställning till om det finns skäl att avvika från personuppgiftslagen för sådan verksamhet som avses i 2 § 4 och 5 polislagen. Till denna verksamhet hör bl.a. hjälpåtgärder inom trafiken, medverkan vid katastrofer och liknande händelser, bl.a. biträde enligt räddningstjänstlagen (punkten 4). Hit hör också åligganden av skilda slag inom området för offentlig förvaltning, t.ex. tillstånds- och tillsynsärenden av olika slag (avseende exempelvis vapen, sprängämnen, offentliga tillställningar och nyttjande av allmän plats), passärenden och ärenden om delgivning eller annan handräckning (punkten 5). Hit hör också vissa verkställighetsåtgärder på kriminalvårdens och socialtjänstens område. Utredningen har ansett att dessa övriga verksamheter inte bör omfattas av en ny reglering. Enligt utredningen finns det i dessa fall inte något tydligt behov av särregler i förhållande till personuppgiftslagen.

Vi delar utredningens uppfattning. Det skulle i och för sig ha ett visst praktiskt värde om all personuppgiftshantering reglerades av en och samma lag, eftersom man därigenom skulle slippa

en del gränsdragningssvårigheter. Något mer påtagligt behov av en sådan samlad reglering har dock inte framkommit. Det är inte heller säkert att de begränsningar i personuppgiftsbehandlingen som bör finnas i den nya lagen skulle vara ändamålsenliga utanför den brottsbekämpande verksamheten. Som exempel kan nämnas att polisen när den biträder vid räddningsuppdrag bör ha samma möjligheter som övriga ansvariga myndigheter att behandla personuppgifter. Till detta kommer, som utredningen har påpekat, att det är tveksamt om polisens icke-brottsbekämpande verksamhet kan anses undantagen från dataskyddsdirektivets tillämpningsområde.

Nästa fråga är om all den verksamhet som omfattas av polisdatalagen också bör omfattas av den nya lagen. Som ovan har konstaterats gäller polisdatalagen också för behandling av personuppgifter i verksamhet som avser övervakning av allmän ordning och säkerhet (jfr 2 § 2 polislagen). Begreppet allmän ordning och säkerhet är vittomfattande. Det inrymmer större delen av den polisverksamhet som inte är inriktad på brottsbekämpning. Hit räknas bl.a. polisens allmänna övervakning i form av patrullering, trafikpolisverksamheten, utryckningsberedskapen, gränskontroll och skyldigheten att bedriva jakt- och fisketillsyn samt annan tillsyn över naturområden. Tillståndsgivning räknas inte hit, men däremot kan den kontroll som tillståndsgivande myndighet enligt vissa författningar ska utöva göra det, t.ex. kontrollen av att ett tillstånd för allmän sammankomst följs. I ett enskilt fall kan den ordningshållande verksamheten övergå i brottsbekämpning, t.ex. om en trafikpolis stoppar en fortkörare och utfärdar en ordningsbot eller om en efterlyst brottsling påträffas vid gränskontroll.

Enligt vår uppfattning är behovet av särregler i förhållande till personuppgiftslagen mycket tydligt när det gäller den brottsbekämpande verksamheten. Så är emellertid inte fallet när det gäller den ordningshållande verksamheten, som i dag till största delen styrs av personuppgiftslagen. Särreglerna i polisdatalagen rör nämligen i huvudsak brottsbekämpande verksamhet. Vi anser att



denna ordning bör gälla även fortsättningsvis. Den nya lagen bör således endast omfatta polisens brottsbekämpande verksamhet.

Med hänvisning till det som sagts ovan föreslår vi att den nya lagen ska omfatta polisens brottsbekämpande verksamhet. Med brottsbekämpande verksamhet avser vi verksamhet som syftar till att förebygga, förhindra eller upptäcka brottslig verksamhet eller till att utreda eller beivra brott.

Polisdatalagen omfattar inte personuppgiftsbehandling som sker med stöd av lagarna om belastningsregister, misstankeregister, Schengens informationssystem samt passagerarregister. Dessa lagar avser särskilda register eller informationssystem och har väl avgränsade tillämpningsområden. Några påtagliga tillämpningssvårigheter eller problem med denna särreglering har inte framkommit. Den nya lagen bör, i vart fall tills vidare, inte gälla på de områden som omfattas av dessa lagar.

Den nya lagen bör inte heller omfatta behandling inom ramen för polisens allmänna spaningsregister. Vi återkommer till denna fråga i avsnitt 20.

När det gäller insamling av personuppgifter genom hemlig teleavlyssning, hemlig teleövervakning och kameraövervakning finns redan bestämmelser i rättegångsbalken, lagen (1998:150) om allmän kameraövervakning, lagen (1995:1506) om hemlig kameraövervakning och lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål. Särskilda bestämmelser finns dessutom i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Som utredningen har föreslagit bör dessa bestämmelser också fortsättningsvis reglera förutsättningarna för sådan insamling. Från den nya lagens tillämpningsområde bör alltså undantas insamling av personuppgifter som utförs med stöd av dessa lagar. Sedan uppgifterna väl har samlats in bör de dock omfattas av den nya lagens bestämmelser. Om riksdagen godkänner de föreslagna reglerna om hemlig rumsavlyssning (prop. 2005/06:178), bör motsvarande gälla för den typen av tvångsmedel.

I den elektroniska hanteringen av uppgifter kan det vara svårt att skilja uppgifter om juridiska personer från uppgifter om fysiska personer som är ägare av eller ställföreträdare för dessa. När det gäller verksamhet som bedrivs i enskild firma är dessutom uppgifter som är hänförliga till firman, t.ex. organisationsnummer, även personuppgifter i personuppgiftslagens mening. Med hänsyn till detta anser vi att det finns skäl att låta även behandling av uppgifter om juridiska personer omfattas av vissa grundläggande bestämmelser i lagen, såsom bestämmelserna om tillåtna ändamål, personuppgiftsansvar, sökbegrepp, gallring och utlämnande av uppgifter. Samma bedömning gjordes vid tillkomsten av lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet (se prop. 2004/05:164, s. 55).

## 6.4 Skyddet för den personliga integriteten

**Promemorians bedömning:** Vid utformningen av de nya bestämmelserna bör intresset av en effektiv brottsbekämpning nogra vägas mot intresset av ett gott skydd för den personliga integriteten.

**Utredningens bedömning:** Utredningen har inte behandlat denna fråga särskilt.

**Remissinstanserna** har inte yttrat sig särskilt i frågan.

**Skälen för promemorians bedömning:** För att polisen ska kunna fullgöra sina uppgifter på ett effektivt sätt måste den ha lagliga förutsättningar att utnyttja en ändamålsenlig informationsteknik som gör det möjligt att samla in och i övrigt behandla stora informationsmängder. Uppgifter om både misstänkta, målsägande, vittnen och andra personer måste kunna behandlas. Polisen måste i olika typer av utredningar ha möjlighet att registrera och lagra uppgifter av vitt skilda slag. Uppgifterna måste vid behov kunna tillhandahållas ett större antal personer vid en eller flera polismyndigheter på automatiserad väg. Dess-

utom måste andra brottsbekämpande myndigheter som exempelvis Tullverket kunna få tillgång till uppgifter. Detsamma gäller de åklagare som leder förundersökningar. Uppgifter måste också – inom ramen för det internationella samarbetet – kunna utbytas med brottsbekämpande myndigheter i andra länder.

En effektiv brottsbekämpning förutsätter alltså att polisen har möjlighet att använda sig av en väl fungerande informationsteknik. Detta innebär dock – på motsvarande sätt som vissa inslag i den operativa polisverksamheten – en risk för intrång i den personliga integriteten. Varje behandling av personuppgifter kan per definition sägas utgöra ett intrång i den personliga integriteten och det är uppenbart att sådana intrång i viss utsträckning måste tillåtas. Intrånget måste dock stå i rimlig proportion till det intresse som ska tillgodoses med behandlingen.

De grundläggande bestämmelserna till skydd för den personliga integriteten finns i regeringsformen. Redan i 1 kap. 2 § slås fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet. I 2 kap. 3 § sägs att varje medborgare, i den utsträckning som anges i lag, ska skyddas mot att hans personliga integritet kränks genom att uppgifter om honom registreras med hjälp av automatisk databehandling. Den sistnämnda bestämmelsen riktar sig framförallt till den lagstiftande makten, som ska se till att den enskilde ges det skydd som behövs. Den lag som i dag har till syfte att i första hand uppfylla regeringsformens intentioner i fråga om integritetsskydd i automatiserad verksamhet är personuppgiftslagen. Den lagen kompletteras, såvitt nu är av intresse, av polisdatalagen. Integritetsskyddande bestämmelser om utlämnande av personuppgifter finns även i sekretesslagen samt i de andra registerlagar som reglerar polisens register.

Begreppet personlig integritet är inte definierat vare sig i lag eller annan författning. Ett sätt att beskriva begreppet är dock att skilja mellan olika former av handlanden som kan anses kränka den personliga integriteten. Man kan då sortera in handlanden som utgör intrång i integriteten i tre huvudkategorier: 1) intrång i en persons privata sfär, oavsett om det sker i fysisk eller annan

mening; 2) insamlade av uppgifter om en persons privata förhållanden; 3) offentliggörande eller annan användning av uppgifter om en persons privata förhållanden (se Stig Strömholm, SvJT 1971 s. 695 och Individens skyddade personlighetsfär, i Om våra rättigheter. Antologi utgiven av Rättsfonden, 1980). Ett annat sätt att beskriva begreppet är att skilja mellan olika former av integritet med utgångspunkt från bl.a. de grundläggande fri- och rättigheterna i 2 kap. regeringsformen (se t.ex. SOU 1984:54 s. 42). Med denna utgångspunkt utgör regler om dataskydd bestämmelser som tar sikte på den personliga integriteten såvitt avser respekten för privatlivet. Bestämmelser om skydd för privatlivet kan också sägas vara inriktade på att tillvarata integriteten i ideell mening (se SOU 1992:84 s. 187). Gemensamt för beskrivningarna synes vara att de alla utgår från att en kränkning av integriteten innebär ett oönskat intrång i en fredad sfär som den enskilde bör vara tillförsäkrad (prop. 2005/06:173 s. 15).

Även om det alltså inte är möjligt att definiera vad som avses med begreppet personlig integritet torde det stå klart att vissa faktorer är särskilt viktiga att ta hänsyn till när det gäller att bedöma integritetskänsligheten vid automatiserad behandling av personuppgifter. Det gäller de ändamål för vilka behandling av personuppgifter ska få ske, arten av de personuppgifter som ska få behandlas, vilka som ska ha tillgång till uppgifterna – genom direktåtkomst eller på annat sätt –, hur sökning ska få ske samt hur lång tid personuppgifterna ska få sparas. Ju fler uppgifter som får behandlas, ju större möjligheter till sammanställningar och sökningar som ges och ju längre tid som uppgifterna får sparas, desto större är, typiskt sett, integritetsintrånget.

I 2 kap. 12 § regeringsformen finns en proportionalitetsprincip med innebörd att viss rättighetsinskränkande lagstiftning aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Även om bestämmelsen i formell mening inte gäller för just den paragraf i samma kapitel (3 § andra stycket) som reglerar integritetsskyddet vid automatisk behandling av personuppgifter, står det klart att en proportiona-

litetsprincip i vid mening gäller för all lagstiftning. En proportionalitetsprincip finns också i Europakonventionen (artikel 8).

Med hänvisning till det som sagts ovan måste alltså den närmare utformningen av de nya bestämmelserna föregås av en avvägning mellan å ena sidan intresset av en effektiv brottsbekämpning och å andra sidan intresset av skyddet för den personliga integriteten. Vid den avvägningen finns det anledning att hålla i minnet att de uppgifter som kan bli aktuella att behandla i brottsbekämpande verksamhet ofta är särskilt integritetskänsliga, dels därför att de kan peka ut personer såsom misstänkta för brott, dels därför att de inte sällan rör enskildas personliga sfär. För den enskilde kan blotta det förhållandet att omfattande uppgifter om hans eller hennes privata förhållanden kan komma att sammanställas och göras tillgängliga inom polisens verksamhet uppfattas som ett mycket allvarligt integritetsintrång.

I de följande avsnitten kommer vi att närmare redovisa hur polisens behov av att kunna behandla vissa uppgifter lämpligen bör vägas mot intresset av skyddet för den personliga integriteten. Vi vill dock redan här framhålla några allmänna utgångspunkter för våra bedömningar.

Det är till att börja med viktigt att lagen klart och tydligt anger för vilka ändamål behandling av personuppgifter ska få ske. Eftersom den nya lagen kommer att medge behandling av en stor mängd integritetskänsliga uppgifter, bör en utgångspunkt vara att lagen uttömmande ska ange för vilka ändamål behandling är tillåten. Detta gäller såväl vid sådan behandling som består i insamling av uppgifter som vid behandling av annat slag, exempelvis tillhandahållande av insamlad information till andra myndigheter. Vidare bör det, på samma sätt som i dag, finnas särskilda bestämmelser som begränsar möjligheterna att behandla s.k. känsliga personuppgifter, dvs. uppgifter om någons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Risken för otillbörliga intrång i den personliga integriteten är större när uppgifter registreras och lagras på ett sådant sätt att flera personer vid en eller flera myndigheter har möjlighet att ta

del av dem, än när en enskild person behandlar uppgifter vid sin egen dator utan att någon annan har åtkomst till uppgifterna. Det bör därför införas särskilda inskränkande bestämmelser för sådan behandling av personuppgifter som innebär att uppgifterna görs gemensamt tillgängliga i den brottsbekämpande verksamheten och för behandling av personuppgifter som har gjorts gemensamt tillgängliga.

En förutsättning för att polisen ska kunna bedriva ett framgångsrikt brottsförebyggande arbete är att polisen får behandla uppgifter om personer som inte är misstänkta för något konkret brott, men ändå misstänks ägna sig åt brottslig verksamhet. Bestämmelser som ger polisen möjligheter att bygga upp stora samlingar av uppgifter om enskilda, utan att det finns någon anknytning till ett visst brott, kan emellertid inge särskilda betänkligheter från integritetssynpunkt. En utgångspunkt bör därför vara att det för polisens del bör uppställas mera restriktiva bestämmelser för behandlingen av uppgifter som inte har samband med ett konkret brott än för behandlingen av uppgifter som behövs för att utreda och beivra ett konkret brott.

I ett integritetsskyddsperspektiv är det också viktigt att särskilja olika typer av uppgifter. Det är särskilt viktigt att det inte uppstår missuppfattningar om huruvida den person som en behandlad uppgift rör är brottsmisstänkt eller inte. Detta kommer bl.a. till uttryck i Europarådets rekommendation om användningen av personuppgifter inom polissektorn (se avsnitt 4.2.3). En utgångspunkt bör därför vara att det av varje behandlad personuppgift framgår huruvida behandlingen sker för att personen är misstänkt eller inte. Det bör också gå att utläsa om de behandlade uppgifterna kan anses tillförlitliga, exempelvis om informationen består av kontrollerade fakta eller av endast antaganden eller obekräftade rykten.

När man avgör vilket intrång i den personliga integriteten som olika former av behandling av personuppgifter innefattar, finns det anledning att särskilt beakta i vilken utsträckning uppgifterna finns tillgängliga för sökning och sammanställning. Ju större möjligheter det finns att söka och sammanställa insamlade

och lagrade uppgifter, desto större är risken för att behandlingen av personuppgifter leder till oproportionerliga intrång i de registrerades personliga integritet. Mot denna bakgrund bör särskilda regler gälla för användning av bl.a. namn och personnummer som sökbegrepp i polisens brottsbekämpande verksamhet.

De brottsbekämpande myndigheterna måste kunna utbyta information sinsemellan och, i viss utsträckning, lämna information till andra myndigheter. För att uppnå en hög effektivitet i informationsutbytet behöver myndigheterna kunna utnyttja tillgängliga tekniska hjälpmedel. Särskilt stor betydelse har möjligheten att vid behov snabbt kunna få tillgång till uppgifter hos andra myndigheter på automatiserad väg, exempelvis genom direktåtkomst. En sådan åtkomst kan dock samtidigt innebära ökade risker för integritetsintrång. Det beror dels på att system för direktåtkomst, typiskt sett, innebär att antalet personer som har tillgång till uppgifterna ökar, dels på att uppgifterna i ökad omfattning kan bli tillgängliga i andra myndigheters verksamhet även i situationer när detta inte är påkallat av strikta verksamhetsbehov i det enskilda fallet. Lagen bör därför begränsa tillgången till automatiserad information så att endast den som behöver en viss uppgift för att kunna fullgöra sina arbetsuppgifter kan få tillgång till den genom direktåtkomst.

Från brottsbekämpningssynpunkt kan det ibland vara av värde att uppgifter bevaras under en längre tid. För den enskilde innebär ett sådant bevarande emellertid att integritetsintrånget består. Att uppgifterna bevaras under lång tid medför också att den totala mängden information om en person kan komma att öka, vilket kan vara negativt från integritetsskyddssynpunkt. Det är därför nödvändigt att utforma bestämmelserna om gallring så att personuppgifter inte bevaras under längre tid än vad som är nödvändigt.

Vi återkommer i följande avsnitt till de frågor som vi nu har berört.

## 6.5 Den nya lagen och personuppgiftslagen

### 6.5.1 Förhållandet till personuppgiftslagen

**Promemorians förslag:** Den nya lagen ska gälla i stället för personuppgiftslagen. I lagen ska hänvisas till de bestämmelser i personuppgiftslagen som ska gälla vid behandling av personuppgifter i polisens brottsbekämpande verksamhet. Lagen ska, liksom personuppgiftslagen, ha till syfte att skydda människor mot att deras personliga integritet kränks genom behandlingen av personuppgifter.

**Utredningens förslag:** Utredningen har föreslagit att den nya lagen ska vara heltäckande och upprepa de bestämmelser i personuppgiftslagen som ska tillämpas i polisens verksamhet.

**Remissinstanserna:** Flertalet remissinstanser har tillstyrkt förslaget eller inte haft någon invändning mot det. *Ekobrottsmyndigheten* har uttalat att den föreslagna lagtekniska lösningen i och för sig framstår som tilltalande, men att det är förenat med svårigheter att bygga en lag om polisens behandling av personuppgifter på ett EG-direktiv som undantar behandling i polisverksamhet. *Kriminalvårdsstyrelsen* har ställt sig tveksam till förslaget och menat att det är lämpligare att den nya lagen endast hänvisar till personuppgiftslagen. *Statskontoret* har uttalat att förhållandet mellan personuppgiftslagen och den föreslagna polisdatalagen inte är tillräckligt utrett. Enligt Statskontoret bör det ytterligare övervägas om den nya polisdatalagen endast bör omfatta de bestämmelser som materiellt avviker från regleringen i personuppgiftslagen. *Riksarkivet* har ansett att bestämmelserna i personuppgiftslagen, som riktar sig mot en stor krets av handlingar inom skilda verksamhetsgrenar, kan bli missvisande om de rakt av överförs till en så speciell verksamhet som polisens. *Riksskatteverket* har ansett att lagen bör hänvisa till bestämmelserna i personuppgiftslagen, i stället för att upprepa dem. *Kammarrätten i Jönköping* och *Sveriges Domareförbund* har för-



ordat en lagstiftningsteknik som innebär att de bestämmelser som avviker från personuppgiftslagen regleras särskilt i den nya lagen och att det tydligt i denna hänvisas till de lagrum i personuppgiftslagen som är tillämpliga. *Malmö tingsrätt* har förklarat sig inte motsätta sig utredningens förslag men har påpekat att förslaget innebär att man får en reglering på polisområdet som avviker från vad som gäller i andra motsvarande fall.

**Skälen för promemorians förslag:** Personuppgiftslagen bygger, som nämnts i tidigare avsnitt, på EG:s dataskyddsdirektiv och är generellt tillämplig på behandling av personuppgifter. Eftersom direktivet inte omfattar behandling av personuppgifter som utförs på området för statens brottsbekämpande verksamhet, finns det ur EG-rättslig synvinkel i och för sig inte något som hindrar att en ny lag om behandling av personuppgifter inom polisens brottsbekämpande verksamhet utformas på annat sätt än vad som anges i dataskyddsdirektivet. I sammanhanget kan dock påpekas att direktivet i huvudsak bygger på och vidareutvecklar de bestämmelser som finns i Europarådets dataskyddskonvention. Konventionen, med dess tilläggsprotokoll, är Sverige folkrättsligt förpliktat att följa. Trots att direktivet inte är tillämpligt i fråga om behandling av personuppgifter som sker i den brottsbekämpande verksamheten bör mot den angivna bakgrunden en reglering som avviker från de grundläggande regler och principer som kommer till uttryck i personuppgiftslagen införas bara om det finns goda skäl för det. Det kan vidare bara ske under förutsättning att regleringen är förenlig med regeringsformen och med åtaganden som följer av andra bindande internationella förpliktelser, bl.a. Europakonventionen och dataskyddskonventionen. Systematiska skäl talar vidare för att den nya regleringen bör ansluta till personuppgiftslagen. Det är således önskvärt att de bestämmelser till skydd för enskilds integritet som uppställs i personuppgiftslagen så långt möjligt tillämpas även vid personuppgiftsbehandling inom polisens brottsbekämpande verksamhet.

Med hänvisning till det som sagts ovan förordar vi att personuppgiftslagens bestämmelser i väsentliga delar får gälla även i

polisens brottsbekämpande verksamhet. I denna verksamhet finns emellertid särskilda behov av att kunna behandla personuppgifter automatiserat och verksamhetens särdrag gör dessutom att personuppgiftslagens bestämmelser inte alltid är ändamålsenliga. I vissa delar bör det därför införas bestämmelser som avviker från den lagen.

Hur bör då de regler i personuppgiftslagen som bör gälla även i polisens brottsbekämpande verksamhet infogas i det nya regelverket? I tidigare lagstiftningsarbeten, där motsvarande fråga har uppkommit, har olika lösningar valts. En modell har varit att i den författning som reglerar behandling av personuppgifter i en viss verksamhet över huvud taget inte nämna personuppgiftslagen. Det innebär att personuppgiftslagens bestämmelser utan vidare kommer att vara tillämpliga, i den mån den särskilda författningen inte innehåller avvikande bestämmelser (jfr 2 § personuppgiftslagen). En liknande modell, som ger samma effekt, är att i den särskilda författningen ange att den gäller utöver personuppgiftslagen. Den modellen används i bl.a. polisdatalagen. Nackdelen med lösningar av dessa slag är att det kan vara svårt att överblicka vilka bestämmelser i personuppgiftslagen som är tillämpliga.

Utredningen har föreslagit en annan modell. Förslaget innebär att den nya lagen ska vara heltäckande och upprepa de bestämmelser i personuppgiftslagen som ska gälla för polisen. En liknande lösning gäller för personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt (prop. 2006/07:46; SFS 2007:258 och 2007:259). Fördelen med en sådan lösning är att tillämparen snabbt får klart för sig vilka bestämmelser som gäller utan att behöva gå till personuppgiftslagen. En nackdel är dock att det i viss mån blir fråga om en dubbelreglering, eftersom personuppgiftslagens bestämmelser ändå gäller om inget annat anges. En annan nackdel är att lagen blir omfattande.

Ytterligare en lösning har valts i lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Lagen innehåller, utöver de bestämmelser som avviker från personuppgiftslagen, en hänvisning till de lagrum i personupp-

giftslagen som ska vara tillämpliga. Lagrådet hade i det lagstiftningsärendet inte några invändningar mot den valda metoden. Samma lösning har nyligen också föreslagits för Kustbevakningens personuppgiftsbehandling (se SOU 2006:18). Fördelarna med en sådan koppling till personuppgiftslagen är att lagstiftningen blir mer överskådlig, tydlig och lättillämpad jämfört med om inga hänvisningar görs till personuppgiftslagen. Samtidigt undviks en omfattande dubbelreglering.

Utvecklingen går mot ökat samarbete mellan de brottsbekämpande myndigheterna. Det ligger ett värde i att använda samma lagstiftningsteknik för all behandling av personuppgifter inom den brottsbekämpande verksamheten, oavsett vilken myndighet det gäller. Vi föreslår därför att man väljer samma lagstiftningsteknik som i lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör alltså gälla i stället för personuppgiftslagen och innehålla tydliga hänvisningar till tillämpliga lagrum i den lagen. Lagen bör, liksom personuppgiftslagen, ha till syfte att skydda människor mot att deras personliga integritet kränks genom behandlingen av personuppgifter. En erinran om detta bör tas in i lagens inledande paragraf.

## 6.5.2 Tillämpliga bestämmelser i personuppgiftslagen

**Promemorians förslag:** Följande bestämmelser i personuppgiftslagen ska vara tillämpliga vid behandling av personuppgifter i polisens brottsbekämpande verksamhet:

- definitioner (3 §),
- förhållandet till offentlighetsprincipen m.m. (8 §),
- grundläggande krav på behandling (9 § första stycket a), b) och e)–h),
- behandling av personnummer (22 §),
- information till den registrerade (23 § och 25–27 §§),
- rättelse (28 §),
- säkerheten vid behandling (30–32 §§),
- överföring av personuppgifter till tredjeland (33–35 §§),
- personuppgiftsombud m.m. (36 § andra stycket och 38–41 §§),
- upplysningar till allmänheten om vissa behandlingar (42 §),
- tillsynsmyndighetens befogenheter (43 och 44 §§, 45 § första stycket och 47 §),
- skadestånd (48 §) och
- överklagande (51 § första stycket, 52 § första stycket och 53 §).

Var och en av de myndigheter för vilka lagen gäller ska utse ett eller flera personuppgiftsombud.

Bestämmelserna om informationsskyldighet i 23 § personuppgiftslagen ska dock inte gälla om uppgifterna samlas in i samband med ett larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen.

Tillsynsmyndigheten ska inte kunna förena ett förbud att utföra viss behandling med vite.

**Promemorians bedömning:** Straffbestämmelsen i 49 § personuppgiftslagen bör inte vara tillämplig.

**Utredningens förslag:** Överensstämmer i huvudsak med förslaget och bedömningen.

**Remissinstanserna:** Flertalet remissinstanser har tillstyrkt förslaget eller inte haft några invändningar mot det. *Ekobrottsmyndigheten* har framhållit att bestämmelsen i 15 kap. 5 § sekretesslagen, som reglerar en myndighets skyldighet att på begäran från en annan myndighet lämna ut uppgift som den förfogar över, i dag uppfattas som en särreglering som gäller före personuppgiftslagen och polisdatalagen. Myndigheten har påpekat att det därför är nödvändigt att det klart och tydligt uttalas att 15 kap. 5 § sekretesslagen kan tillämpas som i dag. Enligt Ekobrottsmyndigheten bör det även införas en bestämmelse i personuppgiftslagen eller sekretesslagen som säger att den s.k. finalitetsprincipen får vika i de fall uppgifter får lämnas till andra myndigheter med stöd av sekretesslagen.

### Skälen för promemorians förslag och bedömning

Nedan redovisar vi vår bedömning av i vilken utsträckning personuppgiftslagens bestämmelser bör vara tillämpliga vid behandling av personuppgifter i polisens brottsbekämpande verksamhet.

#### *Definitioner (3 §)*

I 3 § personuppgiftslagen definieras vissa begrepp som är centrala vid behandling av personuppgifter. Där definieras t.ex. vad personuppgifter är ("All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet") och vad som utgör behandling av personuppgifter ("Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning

eller samkörning, blockering, utplåning eller förstöring”). Definitionerna gäller i dag också för personuppgiftsbehandling enligt polisdatalagen. I likhet med utredningen anser vi att det är viktigt att terminologin i den nya lagen överensstämmer med personuppgiftslagens och att de begrepp som används i de båda författningarna har samma innebörd. En hänvisning till 3 § personuppgiftslagen bör därför tas in i den nya lagen.

#### *Förhållandet till offentlighetsprincipen (8 §)*

I 8 § första stycket personuppgiftslagen finns en erinran om att personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka en myndighets skyldighet att lämna ut personuppgifter enligt 2 kap. tryckfrihetsförordningen, som reglerar allmänna handlingars offentlighet. I paragrafens andra stycke anges att bestämmelserna inte hindrar att en myndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Paragrafen gäller i dag också för personuppgiftsbehandling hos polisen.

Enligt vår bedömning bör i klargörande syfte en hänvisning till bestämmelsen i 8 § personuppgiftslagen tas in i lagen, så att det inte råder någon tvekan om att tillämpningen av lagen inte får strida mot 2 kap. tryckfrihetsförordningen.

#### *Grundläggande krav på behandlingen av personuppgifter (9 §)*

Några av personuppgiftslagens viktigaste bestämmelser om behandling av personuppgifter finns i 9 §. Där uppställs vissa grundläggande krav på den personuppgiftsansvarige. I första stycket a) och b) anges att den personuppgiftsansvarige ska se till att personuppgifter endast behandlas om det är lagligt och att personuppgifter alltid ska behandlas på ett korrekt sätt och i enlighet med god sed. Enligt e)–h) ska den ansvarige se till att de personuppgifter som behandlas är adekvata och relevanta i för-

hållande till ändamålen med behandlingen, att inte fler personuppgifter behandlas än som är nödvändigt, att de personuppgifter som behandlas är riktiga och om nödvändigt aktuella samt att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålet med behandlingen.

Det är naturligt att dessa krav tillämpas även vid behandling av personuppgifter inom polisens brottsbekämpande verksamhet. Den nya lagen bör därför hänvisa till 9 § första stycket a), b) och e)–h) personuppgiftslagen.

I 9 § första stycket c) anges att personuppgifter får samlas in bara för särskilda, uttryckligt angivna ändamål och i punkten d) att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Punkten d) ger uttryck för den s.k. finalitetsprincipen. Enligt paragrafens andra stycke gäller att behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål generellt inte ska anses som oförenlig med de ändamål för vilka uppgifterna samlades in. Vi anser att det inte bör tas in några hänvisningar till dessa bestämmelser i den nya lagen. I stället bör den nya lagen – såsom vi återkommer till i avsnitt 7.1 – uttömmande ange för vilka ändamål uppgifter får behandlas i polisens brottsbekämpande verksamhet. En sådan ordning innebär andra slag av begränsningar av möjligheterna till personuppgiftsbehandling än de som anges i 9 § första stycket c) och d) personuppgiftslagen.

Ekobrottsmyndigheten har tagit upp frågan om förhållandet mellan 15 kap. 5 § sekretesslagen och utredningens lagförslag. Vi återkommer till denna fråga i författningskommentaren till 2 kap. 6 §.

I 9 § första stycket i) och tredje stycket personuppgiftslagen finns bestämmelser om hur länge uppgifter får bevaras. Enligt vår mening bör frågan om gallring regleras särskilt i den nya lagen. Någon hänvisning till personuppgiftslagens bestämmelser om hur länge uppgifter får bevaras behövs därför inte i den nya lagen.

*Behandling av personnummer (22 §)*

I 22 § personuppgiftslagen föreskrivs att uppgifter om personnummer eller samordningsnummer får behandlas bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Personnummer bör således inte användas av ren slentrian. Bestämmelsen innebär att den personuppgiftsansvarige måste göra en intresseavvägning. Tyngden av de skäl som talar för att behandlingen av personnummer är påkallad måste således vägas mot behovet av skydd för den personliga integriteten. Principen bör gälla även vid behandling inom polisens brottsbekämpande arbete. Den nya lagen bör därför hänvisa även till 22 § personuppgiftslagen.

*Information till den registrerade (23 och 25–27 §§)*

Personuppgiftslagens bestämmelser om information, som ska lämnas självant till den registrerade när uppgifter har samlats in från personen själv, och om information som ska lämnas efter ansökan av den registrerade (23 och 25–27 §§) tillämpas i dag vid behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Av 23 § personuppgiftslagen framgår att den personuppgiftsansvarige självant ska informera en enskild om behandling av uppgifter som samlas in från den enskilde själv. Den information som ska lämnas är enligt 25 § uppgift om den personuppgiftsansvariges identitet, ändamålen med behandlingen samt övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter. Information behöver dock inte lämnas om sådant som den registrerade redan känner till. Information ska också, enligt 26 § personuppgiftslagen, lämnas på begäran av den registrerade. Om uppgifter behandlas ska information lämnas om vilka uppgifter det rör sig om, varifrån uppgifterna har hämtats, ändamålen med behandlingen och till vilka mottagare eller



kategorier av mottagare som uppgifterna lämnas ut. Information behöver dock inte lämnas om personuppgifter i löpande text som inte har fått sin slutliga utformning när ansökan gjordes, eller som utgör minnesanteckning eller liknande, under förutsättning att uppgifterna inte har lämnats ut till tredje man. För information efter begäran av en registrerad gäller särskilda bestämmelser. Rätten till information gäller enligt 27 § personuppgiftslagen inte om det i lag eller annan författning, eller i beslut som har meddelats med stöd av författning, särskilt har föreskrivits att uppgifter inte får lämnas ut till den registrerade. Information behöver alltså inte lämnas om sådana förhållanden för vilka det gäller sekretess.

Dessa bestämmelser gäller, som nämnts ovan, vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet i dag. De utgör enligt vår bedömning i allt väsentligt en lämplig avvägning mellan den enskildes intresse av att få information om vilken behandling som sker av uppgifter om denne och polisens intresse av möjligheter till effektiva medel för brottsbekämpning. En hänvisning till bestämmelserna bör därför införas i den nya lagen.

I lagen bör det dock införas ett undantag från informationskyldigheten i 23 §. Av Datainspektionens allmänna råd om information framgår att information bör lämnas muntligt när personuppgifter samlas in vid telefonkontakt eller annan muntlig kontakt. I praktiken uppstår emellertid inte sällan svårigheter att lämna information om behandlingen till den som ringer upp en kommunikationscentral om behandlingarna i kommunikationscentralernas system (KC-systemet). När en person vänder sig till polisen med ett larm eller liknande underrättelse rör det sig typiskt sett om en brådskande situation som kräver omedelbar åtgärd. Både med hänsyn till risken för försening av den åtgärd som efterfrågas i det enskilda fallet och till risken för negativa konsekvenser i stort för den verksamhet som bedrivs vid en larmcentral är det, såsom utredningen har varit inne på, inte rimligt att kräva att polisen alltid lämnar information i samband med larm. Vi anser att information inte ska behöva lämnas om det

med hänsyn till omständigheterna inte finns tid att lämna informationen. Bedömningen av om information ska lämnas bör göras från fall till fall. I sådan verksamhet som uteslutande består i att ta emot larm torde det dock endast undantagsvis finnas tid att lämna information.

#### *Rättelse (28 §)*

I 28 § personuppgiftslagen anges att den personuppgiftsansvarige är skyldig att på begäran av den registrerade rätta, blockera eller utplåna sådana personuppgifter som inte behandlats i enlighet med personuppgiftslagens bestämmelser. När en personuppgiftsansvarig rättar en personuppgift, ska underrättelse lämnas till tredje man som har fått del av uppgiften, om den registrerade begär det eller om mer betydande skada eller olägenhet därigenom kan undvikas. Sådan underrättelse behöver dock inte lämnas om det visar sig vara omöjligt eller om det skulle innebära en oproportionerligt stor arbetsinsats. Dessa bestämmelser gäller idag vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet.

Det är viktigt att personuppgifter som behandlas felaktigt hos en myndighet rättas så att intrång i den personliga integriteten kan begränsas. Bedömningen av om en uppgift har behandlats på ett felaktigt sätt måste göras mot bakgrund av de bestämmelser som gäller för behandlingen, oavsett om det är grundläggande regler i personuppgiftslagen eller specialbestämmelser som gäller för polisen. Vi föreslår därför att bestämmelserna i 28 § personuppgiftslagen ska tillämpas vid behandling av personuppgifter i polisens brottsbekämpande verksamhet även i fortsättningen. I den nya lagen bör det alltså tas in en hänvisning till 28 § personuppgiftslagen.

*Säkerheten vid behandling (30–32 §§)*

I 30–32 §§ personuppgiftslagen finns bestämmelser om hur den personuppgiftsansvarige ska organisera arbetet med behandling av personuppgifter för att garantera säkerheten. Dessa bestämmelser är i dag tillämpliga vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet och de bör enligt vår bedömning gälla där även fortsättningsvis. En hänvisning till bestämmelserna bör alltså föras in i den nya lagen.

*Överföring av personuppgifter till tredjeland (33–35 §§)*

Personuppgifter som är under behandling får enligt 33 § personuppgiftslagen inte föras över till tredjeland, dvs. en stat som inte ingår i EU eller är ansluten till Europeiska ekonomiska samarbetsområdet (EES; 3 § personuppgiftslagen), om inte det mottagande landet har en adekvat nivå för skyddet av personuppgifter. Från förbudet finns vissa undantag i 34 §, bl.a. för överföring till länder som har anslutit sig till Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter. Överföring till ett land som inte ingår i EU eller är anslutet till EES får också ske om landet har en ”adekvat nivå” för skyddet av personuppgifter. Enligt 35 § har regeringen också möjlighet att föreskriva ytterligare undantag från förbudet, bl.a. om det behövs med hänsyn till ett viktigt allmänt intresse.

Vi anser att förbudet mot överföring till tredjeland som inte har acceptabla skyddsnivåer, och de undantag från förbudet som föreskrivs, bör vara tillämpliga även vid behandling enligt den här föreslagna lagstiftningen. Regeringen bör även ha möjlighet att föreskriva om undantag från förbudet.

*Upplysningar till allmänheten, personuppgiftsombudets uppgifter m.m. (36 § andra stycket och 38–42 §§)*

Automatiserade behandlingar av personuppgifter ska enligt 36 § första stycket personuppgiftslagen anmälas till tillsynsmyndigheten (Datainspektionen). Anmälan behöver dock enligt 3 § personuppgiftsförordningen (1998:1191) inte göras för behandlingar som regleras genom särskilda föreskrifter i lag eller förordning. Någon skyldighet att anmäla de behandlingar som utförs med stöd av den nya lagen finns således inte. Lagen bör därför inte innehålla någon hänvisning till 36 § första stycket personuppgiftslagen.

I dag har regeringen enligt 41 § personuppgiftslagen möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till Datainspektionen för förhandskontroll. Det gäller även vid personuppgiftsbehandling inom polisens brottsbekämpande verksamhet. Så bör det enligt vår mening vara även i fortsättningen. Den nya lagen bör därför innehålla en hänvisning till 41 §.

Enligt 42 § personuppgiftslagen ska den personuppgiftsansvarige lämna upplysningar om de behandlingar av personuppgifter som inte har anmälts till Datainspektionen till den som begär det. Bestämmelsen är i dag tillämplig på de behandlingar som utförs inom ramen för polisens brottsbekämpande verksamhet men innebär ingen skyldighet att lämna ut sekretesskyddad information. Det är från integritetsskyddssynpunkt viktigt att den enskilde på ett snabbt och enkelt sätt kan få besked av polisen om vilka behandlingar som utförs i den brottsbekämpande verksamheten även för sådana fall då den behandling som utförs inte omfattas av någon anmälningsskyldighet till Datainspektionen. En hänvisning till 42 § personuppgiftslagen bör därför tas in i den nya lagen.

Den personuppgiftsansvarige kan enligt 36 § andra stycket personuppgiftslagen utse ett personuppgiftsombud. Om ett sådant ombud utses, ska bestämmelserna om ombudets skyldigheter i 38–40 §§ personuppgiftslagen tillämpas. I personupp-

giftsombudets skyldigheter ingår bl.a. att se till att behandlingen av personuppgifter sker på ett lagligt sätt och att hjälpa registrerade att få rättelse. Den personuppgiftsansvarige ska anmäla ombudet hos Datainspektionen. Även ett entledigande ska anmälas hos inspektionen. Bestämmelserna gäller i dag för polisens behandling av personuppgifter.

Den nu beskrivna regleringen i personuppgiftslagen ger myndigheterna valfrihet när det gäller frågan om personuppgiftsombud ska utses. Den behandling av personuppgifter som förekommer i polisens brottsbekämpande verksamhet rör i stor utsträckning uppgifter som får anses integritetskänsliga, vilket gör det särskilt angeläget med den kontroll som kan utövas av ett personuppgiftsombud. Det är också viktigt att enskilda registrerade har lätt att vända sig till rätt person hos myndigheten bl.a. i frågor om information om behandlingen och om rättelse. Mot den bakgrunden bör det enligt vår mening ställas krav på att varje myndighet som omfattas av lagen ska utse personuppgiftsombud och anmäla dessa till Datainspektionen. Detta bör framgå direkt av den nya lagen. Det kan anmärkas att regeringen gjorde motsvarande bedömning i propositionen Personuppgiftsbehandling hos Försvarmakten och Försvarets radioanstalt (se prop. 2006/07:46 s. 98).

*Tillsynsmyndighetens befogenheter (43 och 44 §§, 45 § första stycket och 47 §)*

För att kunna säkerställa att personuppgifter behandlas på ett korrekt sätt har Datainspektionen vissa befogenheter gentemot personuppgiftsansvariga.

Enligt 43 § personuppgiftslagen har Datainspektionen möjlighet att på begäran få tillgång till personuppgifter, upplysningar och dokumentation om behandlingen och säkerheten samt tillträde till lokaler. Paragrafen gäller för polisen i dag och bör vara tillämplig även fortsättningsvis. En hänvisning till den ska alltså tas in i den nya lagen.

Om Datainspektionen inte efter en begäran enligt 43 § personuppgiftslagen kan få tillräckligt underlag för att konstatera att personuppgiftsbehandlingen är laglig, får myndigheten enligt 44 § vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än att lagra dem. Denna bestämmelse gäller i dag för polisens personuppgiftsbehandling och utredningen har föreslagit att den ska gälla även framdeles. Beträffande andra myndigheters personuppgiftsbehandling har man valt olika lösningar när det gäller Datainspektionens möjlighet att meddela sådana förbud. En sådan möjlighet finns exempelvis inte enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och inte heller enligt lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Däremot har Datainspektionen möjlighet att meddela sådana förbud enligt lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar.

När det gäller frågan om Datainspektionen bör ha rätt att förbjuda behandling av personuppgifter i polisens brottsbekämpande verksamhet kan det alltså inledningsvis konstateras att en sådan möjlighet finns redan enligt gällande rätt. I förhållande till de myndigheter där Datainspektionen enligt vad som redovisats ovan saknar sådan möjlighet har polisen en mycket mer omfattande personuppgiftsbehandling som dessutom omfattar flera olika myndigheter. Till detta kan anmärkas att polisen, med den nya lag som vi föreslår, kommer att få möjlighet att behandla vissa typer av personuppgifter i större utsträckning än i dag. Vårt förslag lämnar också större utrymme för polisen att fatta beslut om formerna för behandlingen och vilka strukturer den ska ske i. Det sagda talar enligt vår bedömning sammantaget för att Datainspektionen även fortsättningsvis bör kunna förbjuda viss behandling, om det någon gång skulle inträffa att inspektionen inte får tillgång till tillräckligt underlag för att kunna bedöma personuppgiftsbehandlingen. En hänvisning bör därför göras också till 44 §.

Frågan är sedan om det bör vara möjligt för Datainspektionen att förena ett sådant förbud med vite. Regeringen har i flera propositioner valt att inte ge Datainspektionen någon sådan möjlighet. Detta har motiverats med att regler om vite inte bör tillämpas i förhållandet mellan statliga myndigheter (prop. 2004/05:164 s. 54 och 2006/07:46 s. 105). Vi delar uppfattningen att vite inte bör användas mellan statliga myndigheter och föreslår därför att ett förbud enligt 44 § personuppgiftslagen inte får förenas med vite.

En hänvisning bör vidare göras till 45 § första stycket. Där anges att Datainspektionen, om den konstaterar att personuppgifter behandlas felaktigt, ska försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden. Om det inte går att få till stånd rättelse, eller om saken är brådsakande, får Datainspektionen förbjuda behandlingen. Bestämmelsen gäller redan i dag inom polisens brottsbekämpande verksamhet och bör gälla även fortsättningsvis av de skäl som angetts ovan. Däremot bör någon hänvisning till paragrafens andra stycke eller till 46 §, som båda behandlar frågor om vite, inte göras av skäl som vi nyss har nämnt.

Enligt 47 § personuppgiftslagen har Datainspektionen rätt att hos allmän förvaltningsdomstol ansöka om att sådana uppgifter som har behandlats på ett olagligt sätt ska utplånas. Bestämmelsen, som gäller i polisens verksamhet i dag, har sin grund i artikel 28.3 i dataskyddsdirektivet. Där anges att varje nationell tillsynsmyndighet ska ha särskild befogenhet att inleda rättsliga förfaranden när de nationella bestämmelser som antagits till följd av direktivet har överträtts eller att uppmärksamma de rättsliga myndigheterna på dessa överträdelser. I likhet med utredningen anser vi att bestämmelsen bör vara tillämplig vid behandling av uppgifter enligt den nya lagen. En hänvisning till bestämmelsen bör alltså tas in i lagen.

Frågan om tillsyn behandlas även i avsnitt 19.

*Skadestånd (48 §)*

Enligt 48 § personuppgiftslagen ska den personuppgiftsansvarige ersätta den registrerade för den skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med den lagen har orsakat. Bestämmelsen gäller i dag vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet.

Enligt vår mening bör det finnas en rätt till skadestånd vid skada och kränkning som uppstår när uppgifter behandlas i strid med den nya lagen. En hänvisning till 48 § personuppgiftslagen bör därför tas in i den nya lagen.

*Överklagande (51 § första stycket, 52 § första stycket och 53 §)*

I 51 § personuppgiftslagen finns en bestämmelse om att tillsynsmyndighetens beslut enligt lagen om annat än föreskrifter får överklagas hos allmän förvaltningsdomstol. Vårt förslag om att tillsynsmyndigheten ska kunna meddela förbud enligt 44 eller 45 § personuppgiftslagen innebär att en hänvisning också bör göras till 51 §.

Enligt 51 § andra stycket får tillsynsmyndigheten bestämma att dess beslut ska gälla även om det överklagas. Frågan är om denna bestämmelse ska gälla för polisens personuppgiftsbehandling. Det kan finnas skäl som talar både för och emot detta. Systematiska skäl kan synas tala för att regleringen bör utformas på samma sätt, oavsett vem beslutet gäller. Det är emellertid svårt att se något egentligt praktiskt behov av en sådan möjlighet. Vid en samlad bedömning anser vi att tillsynsmyndigheten inte bör ges möjlighet att meddela interimistiska beslut. Hänvisningen bör därför endast avse det första stycket i paragrafen.

En myndighets beslut om information, om rättelse och underrättelse till tredje man om rättelseåtgärder, om information om automatiserade beslut och om allmänna upplysningar om pågående behandlingar får, enligt 52 § personuppgiftslagen, överklagas hos allmän förvaltningsdomstol. Andra beslut enligt



personuppgiftslagen får inte överklagas (53 §). Prövningstillstånd krävs vid överklagande till kammarrätten. I förarbetena till dessa bestämmelser (prop. 2005/06:173 s. 53) uttalades att det efter införandet av en bestämmelse om överklagande i personuppgiftslagen inte är nödvändigt att ta in några överklagandebestämmelser i särskilda registerförfattningar, som hänvisar till personuppgiftslagen. I konsekvens med detta bör den nya lagen inte innehålla någon särskild bestämmelse om överklagande utan i stället enbart hänvisa till personuppgiftslagens bestämmelser om överklagande.

#### *Straffansvar (49 §)*

I 49 § personuppgiftslagen föreskrivs straffansvar för överträdelser av olika bestämmelser i personuppgiftslagen. Lagrådet har i ett tidigare lagstiftningsärende (prop. 2000/01:33 s. 346) ansett att legalitetsprincipen medför att paragrafen inte kan ges motsvarande tillämpning på bestämmelser som avviker från personuppgiftslagen och som har tagits in i särlagstiftning. Paragrafen kan alltså inte ges en generell tillämpning på de regler som förs in i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Däremot skulle i och för sig en hänvisning kunna tas in i den nya lagen med innebörd att straffbestämmelserna i personuppgiftslagen ska gälla i de delar som personuppgiftslagen ska tillämpas. En sådan ordning kan vid en första anblick förefalla naturlig. Å andra sidan kommer behandlingen av personuppgifter enligt den nya lagen att utföras av personer som är anställda vid statliga myndigheter och som redan omfattas av bestämmelserna om tjänstefel m.m. i brottsbalken. Som utredningen har uttalat torde det inte bli aktuellt att tillämpa straffbestämmelsen i personuppgiftslagen mot någon anställd inom polisen (se även prop. 1997/98:97 s. 109). Det bör därför inte införas någon hänvisning till den aktuella bestämmelsen i personuppgiftslagen. Det kan tilläggas att samma bedömning gjordes vid tillkomsten av lagen om behandling av uppgifter

i Tullverkets brottsbekämpande verksamhet (prop. 2004/05:164 s. 55).

## 6.6 Personuppgiftsansvar

**Promemorians förslag:** Rikspolisstyrelsen och polismyndigheterna ska vara personuppgiftsansvariga för den behandling av personuppgifter som myndigheterna utför eller som det åligger myndigheterna att utföra.

**Utredningens förslag:** Utredningen har föreslagit att Rikspolisstyrelsen ensam ska vara personuppgiftsansvarig för de centrala registren i polisens verksamhet.

**Remissinstanserna** har inte haft något att invända mot förslaget.

**Skälen för promemorians förslag:** Enligt 3 § personuppgiftslagen är det den personuppgiftsansvarige som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Personuppgiftsansvaret kan alltså delas mellan flera.

I registerförfattningar är det vanligt att man på ett tydligt sätt pekar ut vem som är ansvarig för den behandling av uppgifter som regleras. I polisdatalagen finns ingen generell bestämmelse om personuppgiftsansvar. I stället anges för respektive register vem som är ansvarig.

Vårt lagförslag bygger på tanken att såväl Rikspolisstyrelsen som de enskilda polismyndigheterna ska kunna hantera uppgifter elektroniskt. Det framstår därför som lämpligt att den myndighet som utför själva behandlingen också ska ha personuppgiftsansvaret. När det gäller polisverksamhet hos Ekobrottsmyndigheten bedrivs denna av poliser som har tillkallats av Rikspolisstyrelsen, som också leder sådan verksamhet som bara får utövas av anställda inom polisen. Man skulle kunna överväga om Ekobrottsmyndigheten trots detta bör ha personuppgiftsan-

svar för den behandling som sker i polisverksamheten där. Vi anser dock att personuppgiftsansvaret för behandling av uppgifter i den verksamheten, liksom i dag, bör utövas av Rikspolisstyrelsen.

I de fall där det rör sig om behandling av uppgifter i större nationella uppgiftssamlingar, bör liksom tidigare Rikspolisstyrelsen vara personuppgiftsansvarig. Om det å andra sidan handlar om personuppgiftsbehandling inom en enskild polismyndighet, bör ansvaret ligga på denna.

Denna ordning för personuppgiftsansvaret bör komma till uttryck i den nya lagen.

## 6.7 Tillgången till personuppgifter

**Promemorians förslag:** Tillgången till personuppgifter ska alltid begränsas till vad varje tjänsteman behöver för att fullgöra sina arbetsuppgifter. En myndighet som har direktåtkomst till personuppgifter ska ansvara för att tillgången begränsas på det sättet.

**Utredningens förslag:** Utredningen har inte föreslagit någon motsvarande bestämmelse.

**Remissinstanserna** har inte yttrat sig i frågan.

**Skälen för promemorians förslag:** Stora informationsmängder som är samlade så att uppgifter är enkelt sökbara på elektronisk väg utgör allmänt sett en betydande risk för intrång i den personliga integriteten. Risker för integritetsintrång är givetvis särskilt stora om det – såsom ofta är fallet i brottsbekämpande verksamhet – rör sig om känsliga uppgifter. Risker påverkas bl.a. av hur uppgifterna sprids och vem som har rätt att använda dem. Den nya lagen bör därför bygga på principen att enbart de som behöver uppgifterna för att fullgöra sitt arbete ska ha tillgång till dem. En bestämmelse med denna innebörd bör tas in i den nya lagen. Bestämmelsen bör omfatta både direkt tillgång till auto-

matiserade uppgiftssamlingar och tillgång i allmänhet och gälla såväl för polisen som för de myndigheter som har direktåtkomst till uppgifterna. Som en följd av denna bestämmelse kommer polisen och de myndigheter som har direktåtkomst till uppgifterna att vara skyldiga att organisera sin verksamhet på ett sådant sätt att obefogad spridning av personuppgifter inte förekommer. Bestämmelsen får också till följd att enskilda tjänstemän blir förhindrade att lämna uppgifterna vidare till den som inte behöver dem för sitt arbete.

Det kan i detta sammanhang framhållas att modern teknik gör det enklare att organisera verksamheten så att tillgången till uppgifter som behandlas automatiserat begränsas på ett lämpligt sätt. En av grundtankarna bakom de nya datasystem som planeras inom polisen är således att tillgången till uppgifter ska kunna begränsas på ett mer precist sätt. Rikspolisstyrelsen har under hand förklarat att en enskild tjänstemans rätt till åtkomst (behörighet) i större utsträckning kommer att knytas till viss information än till olika slags register. Därmed kan tillgången till information om en person eller uppgifter knutna till en person begränsas med utgångspunkt från tjänstemannens arbetsuppgifter. De mest känsliga uppgifterna kommer lättare att kunna avgränsas och omges av de extra integritets- och säkerhetsskydd som dessa kräver. Vidare kommer kunskapen om och kontrollen av varje tjänstemans informationstillgång att öka. På förhand bestämda behörigheter som avgör tillgången till uppgifter kommer att tas fram. Behörigheterna kommer att anpassas till olika befattningshavares behov med hänsyn till tjänstenivå och arbetsuppgifter.

## 7 Tillåtna ändamål för behandlingen

### 7.1 Tydliga och konkreta ändamål för behandling av personuppgifter

**Promemorians förslag:** I lagen anges för vilka ändamål behandling av personuppgifter får ske. Uppgifter ska inte få behandlas för några andra ändamål än dessa.

**Utredningens förslag:** Utredningen har föreslagit att personuppgifter ska få behandlas bara om behandlingen är nödvändig för att sådan polisverksamhet som omfattas av lagen ska kunna utföras. Utredningen har vidare föreslagit att personuppgifter ska få samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål och att senare behandling inte får ske för något ändamål som är oförenligt med det för vilket uppgifterna samlades in.

**Remissinstanserna:** Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

**Skälen för promemorians förslag:** Polisdatalagen innehåller bestämmelser om ändamålen för de olika register som regleras i lagen, men saknar en generell ändamålsbestämmelse. Det innebär att bestämmelserna om ändamål i 9 § första stycket c) och d) personuppgiftslagen gäller för sådan behandling av personuppgifter inom polisen som inte omfattar de särskilt reglerade registren. Enligt dessa bestämmelser får personuppgifter samlas in

bara för särskilda, uttryckligt angivna och berättigade ändamål. Vilka dessa ändamål är anges inte i lagen. Vidare gäller att senare behandling inte får ske för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (den s.k. finalitetsprincipen).

Det är, som vi redan har varit inne på, naturligt att den nya lagen, liksom personuppgiftslagen, utgår från att personuppgifter får behandlas enbart för vissa berättigade ändamål. Därmed kan användningen och spridningen av uppgifterna begränsas. Det är också naturligt att arten av tillåtna ändamål anges i lagen. Reglerna om ändamålen med personuppgiftsbehandlingen kan utformas på två principiellt olika sätt. Det ena innebär att man i lagen anger att uppgifter får samlas in enbart för vissa angivna ändamål och att senare behandling inte får ske för något ändamål som är oförenligt med det i lagen angivna ändamålet (jfr finalitetsprincipen). Det andra sättet är att i lagen uttömmande ange de ändamål för vilka behandling (vare sig det är fråga om insamling av uppgifter eller efterföljande behandling) får ske.

Vi förordar att reglerna utformas enligt det senare alternativet. Det förra alternativet innebär visserligen en viss praktisk flexibilitet och har dessutom en förebild i personuppgiftslagen och flera andra registerlagar. I förarbetena till personuppgiftslagen har det emellertid inte närmare preciserats vad som kan anses oförenligt med de ursprungliga ändamålen. Det skulle därför bli svårt att avgöra om denna förutsättning är uppfylld. Som en följd därav skulle det inte alltid gå att förutse vilken behandling som kan komma att ske. Eftersom den nya lagen ska gälla ifråga om uppgifter som, typiskt sett, är av integritetskänsligt slag är det inte tillfredsställande att låta en så oprecis bestämmelse avgöra i vilken utsträckning senare behandling av uppgifterna är tillåten. Ökad tydlighet kommer också att underlätta för tillämparna.

Lagen bör således uttömmande reglera även tillåtligheten av senare behandling av insamlade uppgifter. I lagen bör därför anges ett antal *primära* ändamål för behandlingen av personuppgifter i polisens brottsbekämpande verksamhet. I avsnitten 7.2–

7.4 diskuterar vi vilka dessa ändamål bör vara. Redan här ska sägas att dessa primära ändamål enligt vår mening bör avse brottsbekämpning.

Av verksamhetsskäl bör polisen emellertid ha vissa möjligheter att behandla uppgifter som har samlats in för sådana primära ändamål även för andra ändamål. Det kan vara fråga om att polisen behöver använda uppgifterna i annan verksamhet som polisen bedriver eller att uppgifterna behövs i brottsbekämpande verksamhet som någon annan myndighet än polisen bedriver. Också dessa *sekundära* ändamål bör anges i lagen. Vi återkommer i avsnitt 7.6 till vilka dessa sekundära ändamål bör vara.

Bestämmelserna om att personuppgifter inte får behandlas annat än för vissa i lagen angivna ändamål bör inte få hindra rationella rutiner för diarieföring och ärendehantering. Det har föranlett oss till särskilda överväganden som vi redovisar i avsnitt 7.5.

Vi har tidigare beskrivit behovet av en mer teknikneutral lagstiftning (se avsnitt 6.1). En utgångspunkt måste därför vara att lagen, så långt det är möjligt, inte innehåller regler för vissa särskilda register. För vissa fall anser vi dock att det bör införas regler för särskilda register. Detta gäller register med uppgifter om DNA-analyser, fingeravtrycks- eller signalementsregister och penningtvättsregister. Våra överväganden i denna del redovisar vi i avsnitt 17.

Vilka närmare bestämmelser som bör gälla vid behandling av personuppgifter i Säkerhetspolisens verksamhet kommer vi in på i avsnitt 18.

I 8 § första stycket personuppgiftslagen, som enligt vårt förslag i avsnitt 6.5 ska vara tillämplig, finns en erinran om att bestämmelserna i personuppgiftslagen inte ska tillämpas i den utsträckning det skulle inskränka skyldigheten enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. Bestämmelser i grundlag tar alltid över bestämmelser i vanlig lag. Tryckfrihetsförordningens bestämmelser har därför på motsvarande sätt företräde framför bestämmelserna i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Behandling kommer därmed alltid att vara tillåten för att uppfylla de krav som offentlighetsprincipen ställer.

## 7.2 Förebygga, förhindra och upptäcka brottslig verksamhet

**Promemorians förslag:** Personuppgifter ska, med vissa begränsningar, få behandlas i polisens brottsbekämpande verksamhet, om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet.

**Utredningens förslag** överensstämmer delvis med promemorians förslag. Utredningen har föreslagit att bestämmelserna om kriminalunderrättelseverksamhet och kriminalunderrättelseregister ersätts med bestämmelser om behandling av uppgifter om andra personer än sådana som är misstänkta för brott. Enligt utredningen ska sådana uppgifter få behandlas för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer. Utredningen har vidare föreslagit att det under vissa förutsättningar ska vara tillåtet att behandla uppgifter om det är nödvändigt för att underlätta övervakning av vissa grovt kriminellt belastade personer och personer som kan antas vara farliga.

**Remissinstanserna:** Flertalet remissinstanser har tillstyrkt eller inte invänt mot förslaget att utmönstra begreppen kriminalunderrättelseverksamhet och kriminalunderrättelseregister. *Datainspektionen* har dock ansett att nuvarande regler är väl avvägda. Majoriteten av remissinstanserna har ställt sig positiva till förslaget om att införa bestämmelser om behandling av uppgifter om personer som inte är misstänkta för brott.



## Skälen för promemorians förslag

### *Allmänna utgångspunkter*

Vi har ovan föreslagit att den nya lagen ska vara tillämplig i polisens brottsbekämpande verksamhet. Inom ramen för den verksamheten förekommer personuppgiftsbehandling av vitt skilda slag.

*Dels* förekommer mycket sedvanligt kontorsarbete som tidigare inte utgjorde behandling av personuppgifter, men som gör det i dag med den ordbehandlingsteknik som numera används. Självklart måste den nya lagen ge polisen samma möjligheter som andra myndigheter har att använda modern teknik för att upprätta vanliga dokument, göra löpande noteringar i arbetet m.m. Det slaget av normalt teknikutnyttjande innefattar inte heller i sig några påtagliga integritetsrisker.

*Dels* förekommer mycket kvalificerad personuppgiftsbehandling, t.ex. i form av uppbyggandet och förandet av stora uppgiftssamlingar som är tillgängliga för ett större antal personer. Det slaget av behandling ger givetvis upphov till avsevärt större risker för intrång i den personliga integriteten.

Ett sätt att komma tillrätta med sådana integritetsrisker kan vara att generellt begränsa möjligheterna till behandling av personuppgifter, t.ex. genom att uppställa mycket snäva ändamålsbestämmelser för alla slag av behandling. Mycket snäva ändamålsbestämmelser kan emellertid allvarligt försämra polisens möjligheter att använda sig av modern kontorsteknik i arbetet med att komma tillrätta med olika slag av vardagsbrottslighet. Ett generellt förbud mot behandling av uppgifter som gäller mindre allvarlig brottslighet, t.ex. snatteri, skulle sålunda innebära att polisen överhuvudtaget inte skulle kunna använda sig av sedvanlig ordbehandling i arbetet med att förebygga eller utreda sådan brottslighet. Detta är uppenbarligen inte rimligt. Ändamålsbestämmelserna bör därför utformas så att de ger utrymme för att bedriva normalt polisarbete med modern teknik.

De särskilda risker som vissa slag av personuppgiftsbehandling kan ge upphov till bör alltså motverkas på annat sätt. I avsnitt 9 föreslår vi att bestämmelserna om personuppgiftsbehandling ska göra skillnad mellan *å ena sidan* sådan behandling som avser uppgifter som har gjorts gemensamt tillgängliga och *å andra sidan* annan behandling. Vid behandling av det förra slaget bör det gälla särskilda bestämmelser som kan minimera de integritetsrisker som mera kvalificerad personuppgiftsbehandling kan ge upphov till.

*Begreppet kriminalunderrättelseverksamhet bör inte användas i den nya lagen*

Frågan som ska besvaras i detta avsnitt är i vilken utsträckning behandling av personuppgifter bör få ske inom ramen för sådan brottsbekämpande verksamhet som inte avser utredandet eller beivrandet av ett bestämt brott. Hittills har detta slag av personuppgiftsbehandling skett inom ramen för polisdatalagens bestämmelser om kriminalunderrättelseverksamhet och kriminalunderrättelseregister.

Dessa bestämmelser utgör resultatet av en avvägning mellan effektivitetsintressena i brottsbekämpningen och skyddet för den enskildes personliga integritet. Å ena sidan måste polisen för att kunna bedriva ett framgångsrikt brottsförebyggande arbete, få behandla uppgifter om personer som inte är misstänkta för något konkret brott men väl för att utöva eller ta del i pågående eller planerad brottslig verksamhet. Å andra sidan skulle en möjlighet för polisen att utan någon närmare begränsning behandla personuppgifter som inte har samband med något konkret brott öppna vägen för en mycket omfattande behandling av personuppgifter med betydande risker för intrång i den personliga integriteten.

Med *underrättelseverksamhet* avses i polisdatalagen den polisverksamhet som består i att samla in, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats

eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap. rättegångsbalken. Motsvarande definition finns i lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar och i den numera upphävda lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. I polisdatalagen tar begreppet sikte på all underrättelseverksamhet som bedrivs hos polisen. För sådan underrättelseverksamhet som bedrivs av annan än Säkerhetspolisen används i lagen begreppet *kriminalunderrättelseverksamhet*.

Som ovan har nämnts (avsnitt 6.1) tillåter polisdatalagen inte att personuppgifter behandlas i kriminalunderrättelseverksamhet annat än under vissa förutsättningar som anknyter till hur polisen ska bedriva sådan verksamhet. En första förutsättning är således att en *särskild undersökning* har inletts. Med begreppet särskild undersökning avses en undersökning i kriminalunderrättelseverksamhet som innebär insamling, bearbetning och analys av uppgifter i syfte att ge underlag för beslut om förundersökning eller om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. Har en sådan undersökning inletts, får personuppgifter behandlas, om det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas. Vid sådana undersökningar får personuppgifter också behandlas i kriminalunderrättelseregister, som bl.a. ska föras för att ge underlag för de nyss nämnda särskilda undersökningarna.

Som utredningen har framhållit är polisdatalagens systematik med en reglering av kriminalunderrättelseverksamhet, och i anslutning härtill av kriminalunderrättelseregister, ägnad att ge upphov till tillämpningssvårigheter. Definitionen av kriminalunderrättelseverksamhet täcker även sådan behandling av personuppgifter som rimligen inte är så känslig att den behöver regleras särskilt. Den omfattar således, utöver det arbete som sker inom ramen för särskilda undersökningar, även polisens dagliga löpande arbete med att hantera information som på olika sätt kan förebygga, förhindra eller upptäcka brottslig verksamhet. Eftersom lagen utgår från att all behandling av uppgifter för de nu

aktuella ändamålen ska ske inom ramen för särskilda undersökningar eller kriminalunderrättelseregister, har den kommit att försvåra polisens arbete med att verka problemorienterat och brottsförebyggande. Samtidigt har regleringen föranlett oklarheter beträffande flera av de andra register som polisen för. Utredningen har pekat på att det kan ifrågasättas om inte behandlingen av personuppgifter i vissa existerande polisregister till viss del skulle kunna tolkas som kriminalunderrättelseverksamhet i polisdatalagens mening. Behandlingen skulle därmed inte vara tillåten annat än under de särskilda förutsättningar som gäller för behandling av uppgifter i kriminalunderrättelseverksamhet.

Av dessa skäl har utredningen föreslagit att den nya lagen inte ska innehålla bestämmelser om kriminalunderrättelseverksamhet och kriminalunderrättelseregister. I stället ska, enligt utredningens förslag, lagen innehålla bestämmelser om polisens behandling av uppgifter om personer som inte är misstänkta för brott.

Vi delar utredningens bedömning att begreppet kriminalunderrättelseverksamhet bör utmönstras från polisdataregleringen och att den nya lagen således inte ska innehålla några särskilda bestämmelser om kriminalunderrättelseregister och s.k. särskilda undersökningar. Som kommer att framgå av det följande anser vi dock att regleringen i denna del bör utformas på ett något annorlunda sätt än vad utredningen har föreslagit.

*Ändamålet bör vara att förebygga, förhindra och upptäcka brottslig verksamhet*

Som nyss har nämnts användes begreppet underrättelseverksamhet i den numera upphävda lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet. Begreppet fördes dock inte över till den nuvarande lagen i samma ämne. Den lagen innehåller i stället bestämmelser om behandling av personuppgifter för ändamålet *att förhindra eller upptäcka brottslig verksamhet*. Vi anser att samma lösning bör väljas för polisens del. I förtydligande syfte bör bestämmelsen även inne-

hålla ordet förebygga. Av den nya lagen bör alltså framgå att personuppgifter får behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet. Därmed kommer bestämmelsen att ge utrymme för personuppgiftsbehandling inom all egentlig brottsbekämpande verksamhet inom polisen som inte direkt kan knytas till en brottsutredning, däribland behandling i polisens underrättelseverksamhet. Både behandling av mera rutinmässig karaktär, t.ex. ordbehandling, och behandling av mera kvalificerat slag kommer att omfattas av bestämmelsen.

Behandling av personuppgifter i brottsbekämpande verksamhet där det inte finns någon misstanke om konkret brott är särskilt känslig ur integritetssynpunkt. Vi redovisar nedan under vilka närmare förutsättningar sådan behandling bör få ske. Vi kommer för enkelhetens skull att använda oss av uttrycket underrättelseverksamhet för att beskriva all den verksamhet som inryms i detta ändamål.

Den verksamhet som nu är aktuell består främst i att samla in, bearbeta och analysera information. Automatiserad behandling av personuppgifter i polisens underrättelseverksamhet är, som nyss nämnts, i dag tillåten endast i två särskilt angivna fall, dels inom ramen för en särskild undersökning, dels i underrättelseregister (14–21 §§ polisdatalagen). Särskilda undersökningar kan sägas utgöra projekt inom vilka olika slag av brottslig verksamhet och brottsliga fenomen utreds. Inom ramen för en särskild undersökning byggs automatiserade uppgiftssamlingar upp där de uppgifter som samlas in bearbetas och analyseras. Inom ramen för särskilda undersökningar får, till skillnad mot vad som gäller för kriminalunderrättelseregister, uppgifter om personer som inte är skäligen misstänkta för brottslig verksamhet behandlas. Möjligheten att behandla personuppgifter är överhuvudtaget friare inom ramen för en sådan undersökning. Det antal personer som arbetar med en särskild undersökning varierar kraftigt, allt från en eller ett par personer till över hundra.

Enligt vad polisen upplyst under hand finns ett fortsatt stort behov av att arbeta med särskilda undersökningar i projektform. Man anser dock att förutsättningarna för sådant arbete inte bör

regleras i den nya lagen annat än om det är nödvändigt för regleringen av själva personuppgiftsbehandlingen. Polisen har vidare uttalat att det finns ett fortsatt behov av att behandla personuppgifter i större uppgiftssamlingar utanför särskilda projekt och att det för vissa fall kan vara aktuellt att möjliggöra en nationell spridning av uppgifter. I anslutning härtill har påpekats att det i praktiken endast är ett begränsat antal personer som kommer att få tillgång till uppgifter som sprids nationellt, eftersom det allmänt sett innebär en fara att sprida uppgifter av underrättelsekaraktär till en vidare krets. Den faktiska åtkomsten till uppgifterna kommer alltså att variera beroende på hur känsliga uppgifterna bedöms vara.

Polisen har också behov av att behandla personuppgifter i arbetet med att ta emot och bedöma information som kommer till polisens kännedom, exempelvis genom tips från allmänheten, och i allt annat arbete som en enskild polisman bedriver utanför ett visst projekt för att förebygga, förhindra eller upptäcka brottslig verksamhet.

Såsom har nämnts inledningsvis, och som kommer att utvecklas närmare i avsnitt 9, anser vi att det bör gälla olika regler för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga och annan behandling. Vi föreslår också att skillnad görs mellan behandling som sker i större och mindre projekt. Vilka utgångspunkter som enligt vår mening bör gälla för gränsdragningen mellan större och mindre projekt framgår av det avsnittet.

### 7.3 Utreda och beivra brott

<p><b>Promemorians förslag:</b> Personuppgifter ska få behandlas i polisens brottsbekämpande verksamhet om det behövs för att utreda och beivra brott.</p>
--

**Utredningens förslag:** Utredningen har föreslagit att personuppgifter alltid ska få behandlas om det är nödvändigt för att bl.a. bedriva utredning i fråga om brott som hör under allmänt åtal.

**Remissinstanserna** har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

**Skälen för promemorians förslag:** Att utreda och beivra brott utgör ett av polisens främsta uppdrag. Arbete av detta slag sker framför allt inom ramen för en förundersökning enligt 23 kap. rättegångsbalken, exempelvis spaning, förhör, informationsbearbetning och olika former av beslutsfattande, bl.a. om tvångsmedelsanvändning. Till uppgiften att utreda och beivra brott hör emellertid också sådant arbete som sker inom ramen för förenklade förfaranden och vanligen utmynnar i utfärdande av strafföreläggande och föreläggande av ordningsbot. Hit hör även utredningar som polisen gör enligt reglerna i 23 kap. rättegångsbalken med stöd av bestämmelser i särskilda författningar, t.ex. utredningar enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, 9 § lagen (1988:688) om besöksförbud, 8 § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang, 16 § lagen (1957:668) om utlämning för brott, 10 § lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge och 3 § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder. I ändamålet innefattas också behandling som sker med stöd av 23 kap. 3 § och 8 §§ rättegångsbalken, innan förundersökning har inletts, samt andra åtgärder som vidtas i syfte att samla in underlag för beslut om huruvida förundersökning ska inledas eller inte, s.k. förutredning.

Vad som skiljer arbetet med att utreda eller beivra brott från arbetet med att förhindra eller upptäcka brottslig verksamhet är att arbetet i det förra fallet utförs med anledning av att ett konkret brott har eller misstänks ha begåtts, medan arbetet i det senare fallet avser misstankar om pågående brottslig verksamhet som inte kan konkretiseras eller allmänna misstankar om framtida brott. Det är självklart att personuppgifter måste få behand-

las även inom ramen för arbetet med att utreda och beivra brott. En förutsättning bör givetvis vara att behandlingen behövs för ändamålet. I övrigt är det emellertid enligt vår mening inte lämpligt att ställa upp några särskilda begränsningar i fråga om vilka uppgifter som ska få behandlas. På samma sätt som vi har föreslagit ovan i fråga om personuppgiftsbehandling för att förebygga, förhindra och upptäcka brottslig verksamhet bör endast de grundläggande bestämmelserna i den nya lagen vara tillämpliga så länge uppgifterna inte görs gemensamt tillgängliga. Förutom uppgifter om den misstänkte bör således behandling av uppgifter om andra personer tillåtas om det har betydelse för ärendet. Det kan vara fråga om uppgifter om målsägande, vittne, anhöriga och andra som på olika sätt berörs av utredningen. Det kan även vara fråga om indirekta personuppgifter såsom fastighetsbeteckningar, registreringsnummer på bilar eller kontonummer.

#### 7.4 Internationellt samarbete

**Promemorians förslag:** Personuppgifter ska få behandlas i polisens brottsbekämpande verksamhet om detta krävs för att fullgöra ett internationellt åtagande.

**Utredningen** har inte föreslagit några särskilda ändamålsbestämmelser för det internationella samarbetet.

**Remissinstanserna** har inte yttrat sig i saken.

**Skälen för promemorians förslag:** Med ökad internationalisering och större rörlighet för såväl personer som kapital följer större krav på polisiärt samarbete över gränserna, särskilt om allvarlig och organiserad brottslighet ska kunna bekämpas effektivt. Det polisiära samarbetet regleras i stor utsträckning genom olika internationella överenskommelser, såväl multilaterala som bilaterala. En självklar utgångspunkt för vårt arbete är att Sverige på bästa sätt ska kunna fullgöra sina internationella



åtaganden i fråga om framför allt polisiärt samarbete över gränserna. Med internationella åtaganden avses här folkrättsligt bindande förpliktelser. Sådana åtaganden kan avse samarbete med en utländsk myndighet eller med en mellanfolklig organisation. Samarbetet behöver inte avse brott eller brottslig verksamhet inom den svenska polisens ansvarsområde. Det krävs därför en särskild ändamålsbestämmelse som ger stöd för sådan behandling av personuppgifter som sker inom ramen för det internationella samarbetet.

Polisens internationella samarbete regleras i en rad olika författningar. Några av de viktigaste är lagen (2000:343) om internationellt polisiärt samarbete, lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar och lagen (2000:344) om Schengens informationssystem. Dessa lagar tar direkt sikte på polisiärt samarbete över gränserna. För att fullgöra bindande åtaganden om polisiärt samarbete måste polisen kunna behandla personuppgifter i den utsträckning som den konkreta arbetsuppgiften kräver det. Det som regleras i nyssnämnda författningar är främst vilka typer av samarbete som ska förekomma. Hur kommunikationen ska ske ägnas mindre utrymme.

Lagar som reglerar rättslig hjälp, bl.a. lagen (2000:562) om internationell rättslig hjälp i brottmål, lagen (1957:668) om utlämning för brott, lagen (1959:294) om utlämning för brott till Danmark, Finland, Island och Norge och lagen (2005:500) om erkännande och verkställighet inom Europeiska unionen av frysningbeslut, bygger också på folkrättsligt bindande överenskommelser. Indirekt ställs det samma krav på behandling av personuppgifter vid rättslig hjälp som vid polisiärt samarbete över gränserna. Enligt den svenska regleringen är det visserligen åklagare som ger rättslig hjälp, men i det praktiska utredningsarbetet och vid verkställighet av tvångsmedel anlitar åklagaren biträde av polisen på samma sätt som sker i en svensk brottsutredning. Det innebär att polisen i princip måste kunna behandla personuppgifter i ett ärende om rättslig hjälp i samma utsträckning som i en förundersökning.

Det internationella samarbetet äger i allt större utsträckning rum genom direktkontakter mellan myndigheterna. En stor del av det polisiära samarbetet sker dock via den internationella kriminalpolisorganisationen ICPO-Interpol (Interpol) eller det polisiära samarbetsorganet inom Europeiska unionen, Europol. Det finns inte några särskilda författningar som reglerar polisens samarbete med dessa mellanfolkliga organisationer. De författningsbestämmelser som reglerar samarbetet, och som är av intresse i detta sammanhang, rör informationsutbyte och finns i polisdatalagen, lagen om belastningsregister, lagen om misstankeregister samt (såvitt gäller Europol) lagen om Schengens informationssystem.

Det kan anmärkas att det rör sig om utbyte av stora mängder information. Enligt Polisdatautredningen (SOU 2001:92 s. 131) uppgick antalet meddelanden till det svenska nationella sambandskontoret från Interpol till nästan 45 000 år 1999 och antalet meddelanden och ärenden m.m. från Europol till närmare 6 500. Dessa siffror ger tydligt besked om att det rör sig om så stora volymer att materialet omöjligen kan hanteras manuellt. Åtagandena att lämna och ta emot information måste således kunna fullgöras med hjälp av modern teknik.

Det sagda innebär att det krävs en bestämmelse som medger behandling av personuppgifter för att fullgöra internationella åtaganden. Den behandling som åsyftas kan bestå i insamlande av skriftligt material, sammanställning av förhørsutsagor, kontroll i register eller annat. Det kan röra sig om arbete som sträcker sig över en längre tid.

En stor del av det polisiära samarbetet över gränserna äger emellertid rum som ett led i utredning eller lagföring av svensk brottslighet, t.ex. när en svensk myndighet begär rättslig hjälp i en annan stat. Behandlingen av personuppgifter och utlämnandet av information sker då med stöd av det primära ändamålet att utreda och beivra brott i Sverige (jfr avsnitt 7.3).

På sikt kommer sannolikt en del av dagens informationsutbyte att ersättas av system där polismyndigheter i olika länder får direktåtkomst till vissa uppgifter i varandras register. Detta in-

verkar dock inte på polisens behov av att kunna behandla uppgifter som ett led i internationellt samarbete.

## 7.5 Behandling av uppgifter för diarieföring m.m.

**Promemorians förslag:** Personuppgifter ska alltid få behandlas om behandlingen är nödvändig för diarieföring eller om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

**Utredningens förslag** överensstämmer delvis med förslaget.

**Remissinstanserna** har inte haft någon invändning mot förslaget.

**Skälen för promemorians förslag:** Som framgått av avsnitt 7.1 ovan föreslår vi att den nya lagen ska ange för vilka ändamål personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Bestämmelserna kommer att ge polisen möjlighet att behandla uppgifter som *behövs* för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller beivra brott. De kommer dock inte med nödvändighet att ge stöd för behandling av alla de personuppgifter som kan komma in till polisen i form av anmälningar, tips och meddelanden av olika slag. Rikspolisstyrelsen och polismyndigheterna tar dagligen emot stora mängder av information av vitt skilda slag, ofta i elektronisk form. En del av denna information lämnas till polisen i dess brottsbekämpande verksamhet men den kan inte alltid anses behövlig för denna verksamhet. Behandlingen av uppgifterna kommer därmed inte att ligga inom ramen för de primära ändamål som vi har diskuterat i föregående avsnitt.

De inkommande personuppgifterna kan utgöra en del av en allmän handling i tryckfrihetsförordningens mening. Enligt 15 kap. 1 § sekretesslagen (1980:100) gäller som huvudregel att allmänna handlingar som har kommit in till eller upprättats hos en myndighet ska registreras, dvs. diarieföras, utan dröjsmål.

Syftet med bestämmelsen är bl.a. att garantera allmänhetens rätt att få tillgång till allmänna handlingar. I 15 kap. 2 § sekretesslagen uppställs vissa minimikrav beträffande uppgifterna i ett register. När en handling registreras ska det av registret framgå (1) datum då handlingen kom in eller upprättades, (2) diarie-nummer eller annan beteckning som åsatts handlingen, (3) i förekommande fall från vem handlingen har kommit in eller till vem den har expedierats samt (4) i korthet vad handlingen rör. Utgångspunkten är att dessa uppgifter ska vara tillgängliga för allmänheten. Uppgifterna under punkterna 3 och 4 får utelämnas eller särskiljas, om det behövs för att registret i övriga delar ska kunna företes för allmänheten.

Vid sidan av skyldigheten att registrera allmänna handlingar gäller enligt förvaltningslagen (1986:223) att en myndighet ska se till att det är möjligt för enskilda att kontakta myndigheten med hjälp av bl.a. e-post och att svar kan lämnas på samma sätt.

Utredningen har föreslagit att det ska införas en särskild bestämmelse enligt vilken det alltid ska vara tillåtet att diarieföra personuppgifter och behandla dem i löpande text, om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det. Med löpande text avses enligt utredningen text som inte har strukturerats så att sökning av personuppgifter underlättas.

Vi delar utredningens bedömning att det bör införas en bestämmelse som säkerställer att polisen alltid kan diarieföra allmänna handlingar. Den nya bestämmelsen måste också tillåta att polisen kan leva upp till de krav på kommunikation med enskilda som ställs i förvaltningslagen. Det måste alltså vara möjligt att ta emot en handling i elektronisk form liksom att behandla den i det ärende som handlingen föranleder. Vi föreslår att bestämmelsen utformas i huvudsaklig överensstämmelse med utredningens förslag. Dock bör uttrycket "löpande text" inte användas, eftersom informationstekniken medger att även texter som inte på förhand har strukturerats på ett visst bestämt sätt blir föremål för detaljerade och preciserade sökningar. Av bestämmelsen bör framgå att personuppgifter alltid ska få behandlas *dels* om be-

handlingen är nödvändig för diarieföring, *dels* om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

## 7.6 Behandling av uppgifter för att tillhandahålla information till andra

**Promemorians förslag:** Uppgifter som behandlas i polisens brottsbekämpande verksamhet ska också få behandlas om det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,

2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,

3. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl, eller

4. annan myndighets verksamhet, om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift.

Uppgifterna ska även få behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt till andra, om uppgiftsskyldighet följer av lag eller förordning. Regeringen ska även få meddela föreskrifter om att personuppgifter som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter samt att uppgifter som behandlas i en förundersökning under vissa förutsättningar får tillhandahållas en konkursförvaltare.

**Utredningens förslag:** Utredningen har inte föreslagit några särskilda bestämmelser om behandling av uppgifter för dessa ändamål.

**Remissinstanserna:** Flera remissinstanser, bl.a. *Tullverket*, har påtalat att polisen och övriga brottsbekämpande myndigheter i allt större omfattning samarbetar inom ramen för brottsbekämpningen och att dessa myndigheter i sin egen brottsbekämpande verksamhet har behov av att få del av uppgifter som finns hos polisen.

### Skälen för promemorians förslag

#### *Allmänna utgångspunkter*

En viktig fråga är i vilken utsträckning uppgifter som har samlats in i polisens brottsbekämpande verksamhet ska få användas även av andra myndigheter eller i annan verksamhet som polisen bedriver. Det rör sig alltså om behandling för ett annat ändamål än det ursprungliga. Intresset av en effektiv brottsbekämpning talar givetvis för att uppgifterna kan tillhandahållas bl.a. andra brottsbekämpande myndigheter. En vid spridning av uppgifter, insamlade i brottsbekämpande verksamhet, inger emellertid betänkligheter från integritetssynpunkt. Lagen bör därför innehålla bestämmelser om i vilken utsträckning personuppgifter får behandlas för att tillhandahållas andra än de som arbetar i polisens brottsbekämpande verksamhet.

#### *Tillhandahållande av information till andra brottsbekämpande myndigheter*

Polisdatalagen innehåller inte någon särskild bestämmelse om att behandling av personuppgifter får ske för att tillhandahålla information till övriga brottsbekämpande myndigheter. I lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och i den förordning som avser behandling av personuppgifter i Åklagarmyndighetens verksamhet finns dock sådana bestämmelser.

Det är från brottsbekämpningssynpunkt angeläget att samhällets samlade resurser används på ett så rationellt och effektivt sätt som möjligt. En väl utvecklad samverkan mellan de olika myndigheter som har ett ansvar för brottsbekämpningen ger förutsättningar att klara upp brott som annars skulle riskera att förbli ouppklarade. Ett väl fungerande informationsutbyte skapar förutsättningar att se kopplingar mellan brottsliga aktiviteter inom skilda myndigheters ansvarsområden. Det är därför viktigt att den moderna teknikens möjligheter kan tas tillvara för sådant informationsutbyte. Så bör t.ex. möjligheterna att få tillgång till underrättelseinformation genom direktåtkomst förbättras. De särskilda integritetsrisker som direktåtkomst och andra former av elektroniskt informationsutbyte i och för sig kan ge upphov till torde kunna balanseras genom särskilda bestämmelser som vi kommer att diskutera i avsnitt 12.

Enligt vår bedömning bör det därför i den nya lagen uttryckligen anges att de uppgifter som behandlas i polisens brottsbekämpande verksamhet får användas för att tillhandahålla information som andra brottsbekämpande myndigheter behöver i sin brottsbekämpande verksamhet.

#### *Tillhandahållande av information till annan polisiär verksamhet*

För att polisen ska kunna fullgöra arbetsuppgifter som faller utanför den brottsbekämpande verksamheten behöver man ibland ha tillgång till uppgifter som har samlats in för brottsbekämpande ändamål. Uppgifter som behandlas inom den brottsbekämpande verksamheten behöver alltså i viss utsträckning användas även i annan polisverksamhet. En mera generell användning av information, insamlad för brottsbekämpande ändamål, i annan polisverksamhet inger emellertid betänkligheter från integritetssynpunkt, bl.a. därför att det skulle leda till ytterligare spridning av informationen.

De områden där polisen, typiskt sett, kan ha behov av att få del av information som har samlats in i den brottsbekämpande

verksamheten gäller bl.a. arbete med att (1) förordna vissa befattningshavare, (2) pröva tillståndsärenden, (3) fullgöra sin skyldighet enligt författning att bistå andra myndigheter (handräckningsskyldighet), och (4) besluta om att en tvångsåtgärd ska verkställas när fara är i dröjsmål enligt t.ex. djurskyddslagen (1988:534) och utlänningslagen (2005:716).

I polisens arbete med att förordna befattningshavare ställs ofta krav på att förordnande eller liknande endast får beslutas om personen är lämplig med hänsyn till laglydnad och övriga omständigheter. Det kan vara fråga om befattningshavare som till följd av förordnandet får utöva tvångsbefogenheter mot medborgarna, t.ex. ordningsvakter, vägtransportledare och arrestantvakter. Vid bedömningen av en persons lämplighet för en sådan befattning kan uppenbarligen information som har kommit polismyndigheten tillhanda genom den brottsbekämpande verksamheten vara av betydelse.

I tillståndsärenden ska det ofta göras en prövning av sökandens "laglydnad och övriga omständigheter". Prövningen kan vara av betydelse för om tillstånd ska ges eller ej eller avgöra om polis av ordningsskäl bör närvara när verksamheten äger rum. Exempel på sådana ärenden är tillstånd enligt 2 kap. ordningslagen (1993:1617) till allmän sammankomst och offentlig tillställning, tillstånd enligt 3 kap. ordningslagen till användande av offentlig plats, skjutbana, pyrotekniska varor, luft- eller fjädervapen och tillstånd att skjuta med eldvapen inom detaljplanlagt område, tillstånd att bedriva hotell- och pensionatsrörelse, tillstånd att handha explosiva varor och tillstånd att inneha vapen.

Ett tredje område där information från den brottsbekämpande verksamheten kan vara av betydelse avser polisens handräckningsskyldighet i förhållande till andra myndigheter. Att polisen är skyldig att bistå andra myndigheter med hjälp i deras verksamhet motiveras oftast med att endast några få yrkeskategorier bör få utöva legitimt våld i samhället (våldsmonopol). Handräckningsskyldigheten uppstår därför ofta i situationer där begärande myndighet ska vidta någon åtgärd i strid med en enskilds vilja. Det kan då vara viktigt att den polis som utför upp-



draget kan få del av information om den som handräckningen gäller, t.ex. om hans eller hennes våldsbenägenhet. Exempel på en författning som innehåller bestämmelser om handräcknings-skyldighet är lagen (1991:1128) om psykiatrisk tvångsvård.

I en del fall är polisen enligt författning antingen skyldig att besluta och verkställa en tvångsåtgärd, som därefter ska överprövas av annan myndighet, eller skyldig att verkställa en tvångsåtgärd till följd av en annan myndighets beslut. Ett exempel på en sådan författning är djurskyddslagen. Ett annat exempel är utlänningslagen (verkställighet av avvisnings- och utvisningsbeslut). Också här kan polisen ha behov av information från polisens brottsbekämpande verksamhet om exempelvis den aktuella personens farlighet.

Att polisen enligt vad som sagts ovan kan ha behov av att få del av information som samlats in i den brottsbekämpande verksamheten bör givetvis inte föranleda ett rutinmässigt tillhandahållande av sådana uppgifter. I de flesta ärenden kan polisens informationsbehov tillgodoses genom tillgången till uppgifter i misstanke- och belastningsregistren. Möjligheten att få tillgång till uppgifter som har samlats in i den brottsbekämpande verksamheten bör därför begränsas till sådana fall där det i det enskilda fallet finns *särskilda skäl* som talar för att sådana uppgifter tillhandahålls. En bestämmelse av denna innebörd bör tas in i den nya lagen.

#### *Tillhandahållande av information till utländska brottsbekämpande myndigheter eller organisationer*

Polisen måste kunna behandla personuppgifter i den utsträckning det behövs för att fullgöra internationella åtaganden. Det kan exempelvis vara fråga om översändande av uppgifter till Interpol. Likaså måste polisen kunna utföra sådan behandling som krävs för att lämna upplysningar till en utländsk myndighet om vilka åtgärder som har vidtagits i Sverige med anledning av utländsk information. Eftersom det internationella informations-

utbytet förutsätter att uppgifter i vissa fall kan lämnas utan föregående förfrågan från en annan stat, bör det vara möjligt att behandla och lämna ut uppgifter även om detta är ett allmänt åtagande enligt överenskommelsen men inte ett bindande krav. I lagen bör därför tas in en bestämmelse om att uppgifter får behandlas om det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation. Vi återkommer i det följande till olika frågor som rör informationsutbyte och sekretess i det internationella samarbetet (avsnitten 12.3.6 och 13.3).

*Tillhandahållande till riksdagen eller regeringen eller till annan myndighet med stöd av bestämmelser om uppgiftsskyldighet*

Enligt 14 kap. 1 § sekretesslagen hindrar sekretess inte att uppgift lämnas till regeringen eller riksdagen. Detsamma gäller lämnande av uppgifter till annan myndighet, om det finns en uppgiftsskyldighet i lag eller förordning. Mot bakgrund härav bör det i den nya lagen anges att uppgifter får behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen. Det bör även anges att uppgifter får behandlas för att tillhandahållas annan myndighets verksamhet om det enligt lag eller förordning åligger polisen att tillhandahålla sådan information. En motsvarande bestämmelse finns i lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

I sammanhanget bör 15 kap. 5 § sekretesslagen uppmärksammas. Enligt denna paragraf ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång. Bestämmelsen i 15 kap. 5 § sekretesslagen innefattar enligt vår mening ingen uppgiftsskyldighet i nu aktuellt hänseende. Den föreslagna bestämmelsen ger därför inte utrymme för sådan behandling

som enbart syftar till att möjliggöra ett utlämnande med stöd av 15 kap. 5 § sekretesslagen.

*Tillhandahållande av information till annan myndighet i andra fall*

Ovan har vi föreslagit att personuppgifter ska få behandlas för att lämnas ut till en annan myndighet, om detta följer av en uppgiftsskyldighet i lag eller förordning. Dessutom måste polisen ha möjlighet att behandla personuppgifter, om det behövs för att fullgöra författningsenliga förpliktelser att biträda en annan svensk myndighet. Detta kan exempelvis bli aktuellt när polisen bistår Riksdagens ombudsmän och Justitiekanslern med uppgifter i de fall där dessa uppträder som förundersökningsledare och åklagare. En bestämmelse om detta bör tas in i den nya lagen.

*Bemyndigande för regeringen att meddela föreskrifter om behandling för tillhandahållande av uppgifter i vissa särskilda fall*

Enligt 17 § polisdataförordningen har polisen möjlighet att till vissa myndigheter lämna ut uppgifter om efterlysta personer och avlägsnanden ur riket. Det finns även en möjlighet att till konkursförvaltare lämna ut uppgifter i en förundersökning som kan antas ha betydelse för en konkursutredning. Den nya lagen bör innehålla en bestämmelse som erinrar om att regeringen får meddela nya sådana bestämmelser.



## 8 Behandling av känsliga personuppgifter m.m.

**Promemorians förslag:** Uppgifter om en person ska inte få behandlas på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (känsliga personuppgifter). Uppgifter om en person som behandlas på annan grund ska dock få kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för syftet med behandlingen. Känsliga personuppgifter ska också få behandlas, om detta är nödvändigt för diarieföring eller om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Uppgifter om en persons utseende ska alltid utformas på ett objektivt sätt med respekt för människovärdet.

Utöver den behandling som har stöd i de särskilda bestämmelser som vi föreslår om register med uppgifter om resultatet av DNA-analyser (se avsnitt 17) ska uppgifter om resultat av sådana analyser endast få behandlas inom ramen för en förundersökning.

**Utredningens förslag:** Överensstämmer i huvudsak med promemorians förslag.

**Remissinstanserna:** Flertalet remissinstanser har tillstyrkt förslaget eller inte haft några invändningar mot det.

## Skälen för promemorians förslag

### *Känsliga personuppgifter*

Enligt 5 § polisdatalagen får uppgifter om en person inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexuella läggning. Om uppgifter om en person redan behandlas på annan grund, får dock uppgifterna kompletteras med sådana uppgifter, om det är oundgängligen nödvändigt för syftet med behandlingen. Denna bestämmelse överensstämmer med Europarådets rekommendation om användning av personuppgifter inom polis-sektorn m.m. Innebörden av bestämmelsen är t.ex. att det inte är tillåtet att föra särskilda register över personer med viss sexuell läggning. Förekommer personen i en förundersökning eller något annat ärende, får dock uppgiften om sexuell läggning antecknas, om det bedöms vara oundgängligen nödvändigt för syftet med behandlingen.

Vi föreslår att bestämmelserna i 5 § polisdatalagen överförs till den nya lagen. På motsvarande sätt som enligt personuppgiftslagen och lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet bör dock, som en remissinstans har påpekat, uttrycket sexualliv användas i stället för sexuell läggning. Vidare bör uttrycket oundgängligen ersättas med absolut. Slutligen bör det i lagtexten anges att uppgifter som beskriver en persons utseende alltid ska utformas på ett objektivet sätt och med respekt för människovärdet. Detta överensstämmer med den motsvarande bestämmelsen i lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Polisen bör ha möjlighet att diarieföra och handlägga inkommande anmälningar och liknande även om dessa innehåller känsliga personuppgifter. Det bör därför anges i lagtexten att känsliga personuppgifter får behandlas om behandlingen är nödvändig för diarieföring eller om uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. I

avsnitt 11.1 behandlas frågan om användandet av känsliga personuppgifter som sökbegrepp.

#### *Behandling av uppgifter om resultat av DNA-analyser*

En helt annan typ av uppgifter som också brukar betraktas som särskilt känsliga är uppgifter om det slutliga resultatet av DNA-analyser i form av DNA-profiler. Skälet till att just sådana uppgifter brukar anses vara känsliga är det förhållandet att en DNA-profil kan innehålla annan genetisk information än enbart den som krävs för identifiering, t.ex. uppgift om sjukdomsanlag och liknande. I den nuvarande lagstiftningen finns det regler för provtagning för DNA-analys i brottmål, för hur proven ska hanteras, för vilka uppgifter som får tas fram vid analys av DNA-prov samt för registreringen av resultatet av analysen.

De skäl som tidigare har anförts för att kringgärda provtagning och analys av DNA-prov samt registrering av DNA-profiler och DNA-spår med särskilda regler har alltså bärkraft. Den nuvarande regleringen innebär att från levande människor får prov för DNA-analys enbart tas inom ramen för en förundersökning för brott på vilket fängelse kan följa (28 kap. 12–12 b §§ rättegångsbalken).

Den nya lagen bör enligt vår mening innehålla en reglering som gör tydlig skillnad mellan dels behandling av DNA-profilen, dels uppgifter som enbart återger analysarbetet och den eventuella identifiering som detta har lett fram till. Enligt vår mening bör behandlingen av DNA-profilen, dvs. hantering av DNA-prov, analysarbete och jämförelser med uppgifter i befintliga DNA-register, endast få förekomma inom ramen för en förundersökning. Detta bör komma till uttryck i lagen. I praktiken rör det sig framför allt om den hantering som sker hos Statens kriminaltekniska laboratorium. Som vi återkommer närmare till i avsnitt 17 bör de särskilda DNA-registren, där DNA-profiler och DNA-spår registreras, regleras på i huvudsak samma sätt som i dag.

När det gäller behandlingen av den information som slutligen kan utvinnas av ett DNA-prov, dvs. utlåtandet över analysarbetet och uppgifter om eventuell identifiering, behövs det enligt vår mening inte några särskilda regler. Frågan om en uppgift om att någon förekommer i ett DNA-register eller utlåtanden över DNA-analyser får behandlas i polisens verksamhet får således avgöras av den allmänna regleringen i den av oss föreslagna lagen. Detta innebär att sådana uppgifter kan behandlas inte bara för att utreda och beivra brott utan även för att förebygga, förhindra eller upptäcka brottslig verksamhet, om förutsättningarna i övrigt för en sådan behandling är uppfyllda.

Enligt 22 § andra stycket polisdatalagen får uppgifter om resultatet av DNA-analyser även behandlas inom ramen för särskilda undersökningar. Av förarbetena kan inte utläsas i vilka situationer en sådan behandling, dvs. behandlingen av DNA-profilen, skulle kunna aktualiseras och vilket praktiskt behov bestämmelsen avser att fylla. Våra underhandskontakter med myndigheter inom polisväsendet har inte heller kunnat bidra med några uppgifter om detta. Som vi tidigare redovisat kommer begreppet särskild undersökning inte att föras över till den nya lagen. Mot den bakgrunden och då vi inte kunnat finna något sakligt behov som motiverar att så känsliga uppgifter får behandlas utanför förundersökningar, föreslår vi inte någon motsvarighet till bestämmelsen om behandling av sådana uppgifter i särskilda undersökningar.

I avsnitt 17 överväger vi särskilda bestämmelser om register med uppgifter om resultatet av DNA-analyser.



## 9 Gemensamt tillgängliga uppgifter

### 9.1 Särskilda regler bör gälla för behandling av gemensamt tillgängliga uppgifter

**Promemorians förslag:** I stället för bestämmelser om register och databaser ska den nya lagen innehålla särskilda bestämmelser om behandling av uppgifter som *görs eller har gjorts gemensamt tillgängliga i den brottsbekämpande verksamheten*. Bestämmelserna ska framför allt reglera sådan behandling av uppgifter som sker i för verksamheten gemensamma uppgiftssamlingar. Behandling som utförs av en enskild tjänsteman eller inom en begränsad grupp personer, t.ex. genom vanlig ordbehandling eller genom e-postkommunikation mellan ett fåtal tjänstemän, ska inte omfattas av dessa bestämmelser. Registerbegreppet behålls för vissa särskilda fall.

**Utredningens förslag:** Utredningens förslag innehåller inte några bestämmelser som särskilt avser gemensamt tillgängliga uppgifter.

**Remissinstanserna** har inte yttrat sig i frågan.

## Skälen för promemorians förslag

### *Gemensamt tillgängliga uppgifter – ett nytt begrepp*

Den nya lagen kommer att gälla för all automatiserad behandling av personuppgifter i polisens brottsbekämpande arbete. Detta innebär att inte bara uppgifter som behandlas i för verksamheten gemensamma uppgiftssamlingar, t.ex. register eller ärendehanteringssystem, ska omfattas utan även sådan behandling som utförs av en enskild eller begränsad grupp personer, t.ex. vanlig ordbehandling och e-postkommunikation. Som framhållits i andra lagstiftningsärenden är risken för otillbörliga intrång i den personliga integriteten större när personuppgifter används av flera gemensamt i verksamheten än när behandlingen sker av en enskild tjänsteman vid den egna datorn utan att någon annan har åtkomst till uppgifterna. Därför är det enligt vår mening nödvändigt att införa särskilda och mer begränsande regler för behandling av uppgifter som används av eller i vart fall är tillgängliga för fler än ett fåtal personer.

Frågan är då hur man bör avgränsa den personuppgiftsbehandling för vilken mera begränsande regler är nödvändiga.

I tidigare lagstiftning om personuppgiftsbehandling har begreppen register och databas använts för att definiera uppgifter som har gjorts tillgängliga för en större krets. Till respektive register har sedan knutits regler om åtkomst, sökmöjligheter m.m. Registerbegreppet har dock kritiserats, bland annat därför att det har en teknisk anknytning och därför att dagens datasystem normalt inte byggs som traditionella register. Också begreppet databas har en stark teknisk anknytning och leder tanken till ett visst, i tekniskt avseende avgränsat, informationssystem. Även om registerbegreppet fortsättningsvis kommer att användas inom polisen för vissa särskilda fall (bl.a. några av de register som vi vill undanta från den nya lagens tillämpningsområde samt DNA-register) går utvecklingen mot att registerformen överges för mer sofistikerade datasystem.

Som en följd av detta bör den nya regleringen inte bygga på att behandlingen av personuppgifter sker i olika slag av register eller databaser utan i stället ges en mera generell utformning. Regleringen bör vara teknikneutral. Ett tänkbart alternativ är att skapa särskilda begränsande regler för personuppgiftsbehandling som avser "samlingar av uppgifter" eller "uppgiftssamlingar". Beteckningen uppgiftssamling används i den nyligen antagna lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Vi anser dock inte att det begreppet är ändamålsenligt för polisens del, bl.a. därför att det kan ge intryck av att det finns i förväg definierade och avgränsade uppgiftssamlingar för all behandling i den brottsbekämpande verksamheten, trots att så inte är fallet. Eftersom den nya regleringen ska omfatta all automatiserad behandling, bör ett annat begrepp väljas. I betänkandet Kustbevakningens personuppgiftsbehandling Integritet – Effektivitet (SOU 2006:18) föreslås i stället för databas, register eller uppgiftssamling uttrycket *gemensamt tillgängliga uppgifter* för att uttrycka samma sak. Enligt vår bedömning är en sådan konstruktion mera ändamålsenlig för de förhållanden som gäller inom polisen. Vi anser därför att den nya lagen bör innehålla särskilda bestämmelser för *behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet*. Med den formuleringen görs det klart att det viktiga inte är var uppgiften rent tekniskt är lagrad eller behandlas, utan om ett flertal personer har möjlighet att ta del av uppgiften.

*Gränsdragningen mellan behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga och annan behandling*

Det ligger i sakens natur att det inte är enkelt att dra en tydlig gräns mellan uppgifter som är gemensamt tillgängliga och andra uppgifter. I det följande anger vi dock några principer som enligt vår bedömning bör ligga till grund för gränsdragningen.

En grundläggande förutsättning för att personuppgifter ska anses vara gemensamt tillgängliga bör vara att de kan användas gemensamt av flera, dvs. att fler än en person har åtkomst till uppgifterna. Uppgifter som endast ett fåtal personer har rätt att ta del av bör dock inte anses som gemensamt tillgängliga. Att en uppgift ”är tillgänglig” för en viss person bör förstås så att personen har såväl faktisk möjlighet att ta del av uppgiften som rättslig behörighet till det. Det bör däremot inte spela någon roll hur många som faktiskt tar del av de aktuella uppgifterna. Det bör inte heller spela någon roll om den som har tillgång till uppgiften kan påverka den eller bara läsa den.

Det här innebär till att börja med att uppgifter blir att anse som gemensamt tillgängliga om behandlingen sker för att en obestämd krets – t.ex. hela polisorganisationen – ska kunna ta del av uppgifterna. De centrala register som Rikspolisstyrelsen för har just syftet att tillgodose informationsbehovet inom olika delar av organisationen. Som exempel på sådana register kan nämnas det allmänna spaningsregistret, det centrala kriminalunderrättelsesregistret och det centrala brottspaningsregistret. I dessa och liknande system lagras uppgifter på ett sådant sätt att många anställda har möjlighet att vid behov kunna ta del av uppgifterna, t.ex. under arbetet med en förundersökning eller för att genomföra ett underrättelseprojekt. På liknande sätt blir uppgifter som är avsedda för en hel polismyndighet eller för en viss enhet inom polisorganisationen normalt att anse som gemensamt tillgängliga. Som exempel kan nämnas lokala system som Rationell anmälningsrutin (RAR) och Datoriserad utredningsrutin (DurTvå). Detsamma gäller diariet och andra lokala register. Också andra uppgifter som är tillgängliga för en i förväg obestämd krets av personer bör, som huvudregel, anses gemensamt tillgängliga. Det innebär exempelvis att de flesta förundersökningar redan från början kommer att vara gemensamt tillgängliga, även om det bara är ett fåtal handläggare som arbetar med förundersökningen. Överhuvudtaget kommer begreppet ”gemensamt tillgängliga uppgifter” att täcka inte enbart register i

traditionell bemärkelse utan alla uppgiftssamlingar, avsedda för en obestämd krets av personer.

Vidare bör uppgifter givetvis vara att anse som gemensamt tillgängliga även i vissa fall när den personkrets som har tillgång till uppgifterna är bestämd och avgränsad. Om uppgifterna är tillgängliga för ett stort antal bestämda personer, bör de således anses vara gemensamt tillgängliga. De personuppgifter som behandlas i brottsbekämpande verksamhet som involverar ett flertal tjänstemän som gemensamt behandlar viss information bör alltså regelmässigt anses som gemensamt tillgängliga. Uppgifter bör dock inte anses som gemensamt tillgängliga enbart därför att två eller flera personer har tillgång till dem. Kan man redan från början konstatera att uppgifterna endast kommer att vara tillgängliga för en avgränsad krets av ett handfull personer, bör uppgifterna alltså *inte* anses som gemensamt tillgängliga. De integritetsskyddsintressen som motiverar särskilda regler för gemensamt tillgängliga uppgifter gör sig inte lika starkt gällande när bara ett fåtal personer har tillgång till uppgifterna. En jämförelse kan härvid göras med den relativt omfattande personuppgiftsbehandling som i dag tillåts inom ramen för en särskild undersökning med stöd av 14–16 §§ polisdatalagen.

En förutsättning för att uppgifterna inte ska anses vara gemensamt tillgängliga måste dock vara att kretsen omfattar endast ett litet antal personer. Så kan vara fallet t.ex. med ett mindre underrättelseprojekt. Om projektet enbart engagerar en avgränsad krets, bestående av ett fåtal på förhand utpekade personer eller funktioner, bör de uppgifter som behandlas inom ramen för projektet normalt inte betraktas som gemensamt tillgängliga. Så snart det är fråga om mer än ett fåtal personer som har tillgång till uppgifterna bör utgångspunkten vara den motsatta. En lämplig tumregel kan vara att uppgifter anses som gemensamt tillgängliga när fler än ett tiotal personer har tillgång till dem.

Det är emellertid inte bara antalet personer som har tillgång till uppgifterna som är av betydelse. Från integritetssynpunkt har det också betydelse om uppgifterna stannar inom polisen eller

om de sprids till andra myndigheter. I det senare fallet har polisen inte längre någon kontroll över hur uppgifterna används. Som vi återkommer till i avsnittet om direktåtkomst förutsätter sådan åtkomst för andra myndigheter att uppgifterna har gjorts gemensamt tillgängliga.

I viss utsträckning kan också tidsaspekten ha betydelse för om uppgifter ska anses vara gemensamt tillgängliga eller inte. En del brottsbekämpande verksamhet, främst underrättelseverksamhet, leder inte alltid till ett bestämt avslut av ett visst konkret ärende. Ett underrättelseprojekt har inte sällan en obestämmd varaktighet och kan därför komma att löpa över en längre tid. Som exempel kan nämnas projekt riktade mot ungdomsbrottsligheten på en viss ort eller underrättelseprojekt avseende viss typ av m-kriminalitet eller häleriverksamhet i en viss bransch. Det ligger i sakens natur att i sådana långvariga projekt kan den personal som sysslar med projektet komma att bytas ut under arbetets gång. Även om tanken från början har varit att endast en liten avgränsad krets ska syssla med projektet, är det därför långtifrån alltid möjligt att upprätthålla det kravet. Underrättelsematerial som tas fram i ett sådant projekt, t.ex. en sammanställning över gängbrottsligheten på en viss ort, bör därför också anses som gemensamt tillgängliga uppgifter. Motsvarande bör i princip gälla andra typer av uppgifter som behandlas för att användas under en längre tid. Det kan t.ex. vara fråga om sammanställningar av uppgifter ur förundersökningar eller annat material som samlats in i den brottsbekämpande verksamheten.

Givetvis bör detta inte gälla undantagslöst. Om en enskild tjänsteman gör sammanställningar av olika slag för eget bruk, bör detta inte göra att uppgifterna anses vara gemensamt tillgängliga, även om han eller hon har för avsikt använda dem under längre tid. På samma sätt bör man se det om några enstaka tjänstemän sammanställer material från vissa förundersökningar för att själva kunna använda det i sina framtida utredningar. Vi återkommer i författningskommentaren till den närmare avgränsningen mellan gemensamt tillgängliga och icke gemensamt tillgängliga uppgifter.

*Behovet av enhetlig tillämpning*

Eftersom man enligt vår mening inte bör i författning lägga fast en formell gräns mellan de uppgifter som ska anses gemensamt tillgängliga och de uppgifter som inte är det, kommer det att finnas ett stort behov av interna riktlinjer för polisens tillämpning av det nya begreppet. Vi utgår därför från att Rikspolisstyrelsen nog ser till behovet av riktlinjer och utbildning av personalen.

## 9.2 Förebygga, förhindra och upptäcka brottslig verksamhet

**Promemorians förslag:** I verksamhet som avser att förebygga, förhindra och upptäcka brottslig verksamhet ska enbart följande personuppgifter få göras gemensamt tillgängliga.

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet som

a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver eller

b) sker systematiskt.

2. Uppgifter som behövs för övervakningen av personer som

a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver och

b) är allvarligt kriminellt belastade eller kan antas vara farliga för annans personliga säkerhet.

Tillgången till uppgifter om övervakning av personer ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om att en person är föremål för övervakning ska dock få göras tillgänglig för flera.

**Utredningens förslag** överensstämmer delvis med promemorians förslag. Utredningen har föreslagit att bestämmelserna om

kriminalunderrättelseverksamhet och kriminalunderrättelseregister ersätts med bestämmelser om behandling av uppgifter om andra personer än sådana som är misstänkta för brott. Enligt utredningen ska sådana uppgifter få behandlas för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer. Utredningen har vidare föreslagit att det under vissa förutsättningar ska vara tillåtet att behandla uppgifter om det är nödvändigt för att underlätta övervakning av vissa grovt kriminellt belastade personer och personer som kan antas vara farliga. Utredningen har dock inte föreslagit att man ska skilja på gemensamt tillgängliga uppgifter och andra uppgifter.

**Remissinstanserna:** *Rikspolisstyrelsen* har uttalat att det bör vara tillräckligt att fängelse ingår i straffskalan för den misstänkta brottsliga verksamheten för att behandling ska få ske. *Riksdagens ombudsmän* har ifrågasatt om nyttan med en bestämmelse som möjliggör registrering av uppgifter om övervakade personer väger över intresset av att skydda den enskilde mot integritetsintrång. *Justitiekanslern* har ansett att utformningen av bestämmelsen bör övervägas närmare och att en närmare precisering krävs av när en registrering får ske. *Riksåklagaren* har ansett att den tillåtna behandlingen bör begränsas till att avse personer som har dömts för allvarliga brott riktade mot en persons liv, hälsa eller frihet.

### Skälen för promemorians förslag

#### *Uppgifter som har samband med brottslig verksamhet*

Som vi tidigare har berört medför behandling av gemensamt tillgängliga uppgifter särskilda risker för den enskildes personliga integritet. Det är därför naturligt att begränsa möjligheterna till sådan behandling till de fall där behovet av att göra informationen gemensamt tillgänglig är mera påtagligt.



En första fråga är om den brottsliga verksamhet som underrättelsearbetet avser måste vara av allvarligare slag för att personuppgifter ska få göras gemensamt tillgängliga. Utredningen har i denna del föreslagit att det ska vara fråga om brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer. Det motsvarar vad som i dag gäller för behandling av uppgifter i kriminalunderrättelseregister. I lagen (2005:787) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet uppställs ett liknande krav. Enligt den lagen får uppgifter behandlas om de ger anledning att anta att verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer eller brott som sker systematiskt har utövats eller kan komma att utövas. *Rikspolisstyrelsen* har ansett att en sådan bestämmelse skulle medföra alltför stora begränsningar i förhållande till polisens behov av att kunna behandla uppgifter. Styrelsen har i stället förordat att personuppgiftsbehandling ska vara tillåten om det finns fängelse i straffskalan för det brott som innefattas i den misstänkta brottsliga verksamheten.

En förändring av det slag som Rikspolisstyrelsen har förordat innebär att det kommer att utföras kvalificerad personuppgiftsbehandling inom ramen för underrättelseverksamhet i betydligt större utsträckning än vad som nu är fallet. Detta kan framstå som betänkligt från integritetsskyddssynpunkt. Redan det förhållandet att uppgifter om brottslig verksamhet normalt har mindre konkretion än uppgifter om konkreta brott talar också för att polisen bör ges mindre utrymme för behandling av personuppgifter i underrättelseverksamhet än för behandling i t.ex. förundersökningar. Behovet av att behandla personuppgifter i underrättelseverksamhet framstår också som mindre, ju lägre straffvärde den brottsliga verksamhet som underrättelseverksamheten avser har. Det innebär emellertid inte att den nuvarande avgränsningen för när sådan behandling är tillåten – brottslig verksamhet som innefattar brott med minst två års fängelse i straffskalan – är den lämpligaste. Den nuvarande avgränsningen måste ses mot bakgrund av att underrättelseverksamhet var ett ganska nytt arbetssätt när polisdatlagen tillkom

och att det då var naturligt att sätta upp förhållandevis snäva gränser för den behandling av personuppgifter som tilläts. Med tiden har den nuvarande avgränsningen visat sig vara en hämmande faktor i polisarbetet. Vi bedömer därför att det är nödvändigt att utveckla polisens underrättelseverksamhet genom att ge större utrymme än tidigare för behandling av uppgifter i underrättelseverksamhet.

I linje med Rikspolisstyrelsens förslag skulle man i och för sig kunna tänka sig att – vad gäller verksamhet som avser att förebygga, förhindra och upptäcka brottslig verksamhet – tillåta att personuppgifter görs gemensamt tillgängliga så snart den brottsliga verksamheten innefattar brott för vilket fängelse ingår i straffskalan. En sådan reglering skulle dock enligt vår mening föra alltför långt, eftersom många brott med fängelse i straffskalan normalt endast leder till bötesstraff.

Ett annat alternativ är att liksom hittills anknyta till straffskalan för de brott som den misstänkta verksamheten antas innefatta, men dra gränsen vid ett i stället för två års fängelse. Det innebär bl.a. att polisen får större möjlighet att behandla personuppgifter i underrättelseverksamhet angående brott som regleras inom specialstraffrätten. Av tradition har många sådana brott en annan straffskala än brottsbalksbrott, samtidigt som det är fråga om brott som kan drabba enskilda brottsoffer mycket hårt och som av det skälet bör kunna beivras effektivare. Ett exempel på det är s.k. inkassoverksamhet som bedrivs utan tillstånd. Det är en brottstyp som förekommer allt oftare och som förknippas med organiserad brottslighet, främst s.k. mc-kriminalitet. Brotten består i att driva in pengar under förtäckta hot. Även i de fall där brotten rubriceras som olaga hot är straffmaximum ett års fängelse. En annan brottstyp där det också kan vara angeläget att kunna samla och på annat sätt behandla underrättelseinformation för att kunna förebygga brott är överträdelse av besöksförbud. Även bland brottsbalksbrotten finns det sådana som bör kunna angripas genom en effektiv underrättelseverksamhet, men som med dagens gränsdragning faller utanför möjligheterna till behandling av personuppgifter, t.ex. skadegörelse i

form av klotter. Denna brottstyp begås av ett fåtal personer men vållar stor skada för samhället. För att kunna lagföra klottrare krävs det normalt att de ertappas på bar gärning, vilket många gånger förutsätter ett noggrant underrättelsearbete. Andra brottsbalksbrott som i vissa fall kan kräva ett effektivt underrättelsearbete är skyddande av brottsling och främjande av flykt. Detta gäller särskilt i de fall där det finns misstanke om kommande fritagning av allvarligt brottsbelastade personer.

Mot denna bakgrund föreslår vi att det i verksamhet för att förebygga, förhindra och upptäcka brott ska vara möjligt att göra uppgifter gemensamt tillgängliga så snart den brottsliga verksamheten innefattar brott med minst ett års fängelse i straffskalan.

Det förekommer även brottslighet där det enskilda brottet inte i sig är av sådan art att det kan leda till fängelse i ett år, men där verksamheten kan misstänkas ske systematiskt. Det kan exempelvis vara fråga om ligor som har satt i system att begå snatterier. Andra exempel står att finna inom den ekonomiska brottsligheten, där bl.a. osant intygande utgör ett betydande problem och där brottsligheten ofta bedrivs systematiskt och kan kräva kartläggning. Ett tredje exempel är barnpornografibrott som är ringa. Enligt vår mening talar intresset av en effektiv brottsbekämpning för att polisen bör kunna göra även uppgifter med anknytning till sådan systematisk brottslighet gemensamt tillgängliga. En motsvarande ordning gäller för övrigt i dag för Tullverket. Vi föreslår att detta får komma till uttryck i den nya lagen.

En annan fråga är *vilka* personuppgifter som bör få göras gemensamt tillgängliga och därefter behandlas gemensamt. Det är en självklarhet att uppgifter om brottsmisstankar och om de personer som är misstänkta för delaktighet i brottslig verksamhet ska få behandlas. Men även uppgifter om den som inte kan misstänkas måste enligt vår mening kunna få behandlas. Som exempel kan nämnas uppgifter om den som har informerat polisen om den misstänkta brottsliga verksamheten, uppgifter om en juridisk person som äger ett garage eller annan lokal där den

misstänkt brottslig verksamheten bedrivs och uppgifter om anhöriga eller andra som genom sitt samröre med den misstänkte kan vara av intresse i underrättelsearbetet. Som förutsättning för att detta slag av uppgifter ska få behandlas bör dock gälla att uppgifterna har en koppling till misstänkt brottslig verksamhet. Vi föreslår därför att uppgifter som *kan antas ha samband* med den misstänkta brottsliga verksamheten får behandlas.

Vårt förslag innebär att det i vissa fall kommer att vara möjligt att göra uppgifter om personer som inte själva är misstänkta för vare sig ett konkret brott eller viss brottslig verksamhet gemensamt tillgängliga. Att sådan behandling bör omgärdas av särskilda bestämmelser till skydd för den enskildes integritet är självklart. Det behövs bl.a. bestämmelser som förhindrar att uppgifterna ges omotiverad spridning. Frågan är då hur sådana skyddsregler lämpligen bör utformas. I lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet anges att personuppgifter av det nu diskuterade slaget får behandlas endast i ett ärende som rör viss preciserad brottslig verksamhet. Dessutom uppställs den begränsningen att endast de som arbetar med ärendet ska få ha direkt tillgång till uppgifterna. Sådana begränsningar framstår dock som mindre ändamålsenliga för polisens del. De skulle i alltför hög grad begränsa polisens möjlighet att förebygga, förhindra och upptäcka brottslig verksamhet. Det är således inte ovanligt att samma personer är inblandade i flera brottsliga aktiviteter som pågår i olika delar av landet vid en och samma tidpunkt. Om endast de som arbetar med det ärende, där en viss uppgift har kommit fram, ges tillgång till uppgiften, kommer det normalt inte att vara möjligt att upptäcka sambanden med brottsliga aktiviteter som bedrivs på andra håll. Sådana samband kan utgöra grunden för en brottsmisstanke mot en person som förekommer som ”kringperson” i flera utredningar om likartad brottslig verksamhet. Uppgifter om personer som har samband med brottslig verksamhet utan att vara misstänkta bör således kunna behandlas gemensamt inom polisen även utanför ett visst ärende.

De särskilda risker för intrång i den personliga integriteten som detta skulle kunna innebära bör kunna motverkas genom bl.a. begränsningar i möjligheterna att genom sökning få fram särskilda slag av uppgifter. Till den frågan återkommer vi i avsnitt 11.2. Dessutom bör det beträffande uppgifter som görs eller har gjorts gemensamt tillgängliga alltid framgå huruvida en person är misstänkt eller inte samt för vilket närmare slag av brottslig verksamhet som behandlingen sker (se avsnitt 10). Av stor betydelse i detta sammanhang är också den allmänna bestämmelse som vi föreslagit i avsnitt 6.7 om att endast personer som behöver uppgifterna för sitt arbete får ges tillgång till dem.

#### *Uppgifter som behövs för övervakningen av vissa personer*

I anslutning till bestämmelserna om behandling av uppgifter avseende brottslig verksamhet har utredningen föreslagit särskilda bestämmelser som klargör att polisen i vissa fall har rätt att behandla uppgifter för övervakning av personer. Det handlar då om övervakning av personer som är allvarligt kriminellt belastade eller som kan antas vara farliga för annans personliga säkerhet.

Även Registerutredningen föreslog sådana bestämmelser (SOU 1997:65 s. 230 ff.). Enligt det förslaget skulle kriminalunderrättelseregister få innehålla uppgifter om dömda personer som antingen var allvarligt kriminellt belastade eller som kunde antas vara farliga för annans personliga säkerhet. Personuppgifterna skulle gallras senast när samtliga uppgifter om personen hade gallrats ur belastningsregistret. Den dåvarande regeringen ansåg dock inte att några sådana bestämmelser borde införas (prop. 1997/98:97 s. 113 f). Som skäl angavs att det var svårt att se något behov av ett sådant register, varvid det bl.a. hänvisades till registreringen i belastningsregistret. Regeringen menade också att det skulle vara svårt att fastställa vilka kriterier som skulle gälla för att en person skulle anses vara allvarligt kriminellt belastad eller farlig för annans säkerhet.

Vi anser liksom utredningen att det är befogat att, under vissa förutsättningar, genom behandling av personuppgifter utöva särskild kontroll över personer som är allvarligt kriminellt belastade eller som har visat sig vara särskilt farliga för andra personers säkerhet. Sådan övervakning kan utgöra ett betydelsefullt inslag i polisens samlade insatser för att förebygga, förhindra eller upptäcka brottslig verksamhet. De uppgifter som finns i misstanke- och belastningsregistren ger inte all den information som kan krävas för att övervakningen ska vara effektiv. Det förekommer i dag att övervakning av detta slag sker inom ramen för särskilda undersökningar. Med hjälp av ett särskilt analysverktyg kan informationen analyseras och kopplingar mellan exempelvis olika grupperingar, händelser och brottsliga verksamheter upptäckas. Denna form av uppgiftssamling har i något fall benämnts Y-databas, där bokstaven Y står för yrkeskriminell. Datainspektionen har nyligen i ett tillsynsärende inspekterat behandlingen av personuppgifter i en sådan databas vid Polismyndigheten i Skåne. Efter att inledningsvis ha ifrågasatt om Y-databasen omfattades av polisdatalagens bestämmelser om särskilda undersökningar, har inspektionen slutligen kommit fram till att så var fallet. Inspektionen har dock framfört vissa synpunkter på gallringen av uppgifterna (Datainspektionens beslut 25 maj 2007, dnr 686-2006).

I många fall torde personuppgiftsbehandling av detta slag rymmas inom de bestämmelser om behandling vid misstanke om brottslig verksamhet som vi har föreslagit ovan. De uppgifter som behöver göras gemensamt tillgängliga kommer således med stor sannolikhet att ha samband med misstänkt brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver eller som sker systematiskt. Det kan dock förekomma fall där dessa rekvisit inte är uppfyllda, samtidigt som starka skäl talar för att behandling bör kunna ske.

Frågan är då om den nya lagen bör ge polisen möjlighet att skapa gemensamma uppgiftssamlingar avseende personer som uppfattas som särskilt brottsbenägna men mot vilka det inte finns några konkreta misstankar om brottslig verksamhet. Vi

anser att den frågan bör besvaras jakande. Detta slag av uppgifts-samlingar är av mycket stor betydelse för att polisen ska kunna bedriva ett effektivt brottsbekämpande arbete. Utan en sådan möjlighet skulle det vara svårt för polisen att bemästra den brottslighet som förekommer i kriminella nätverk såsom mc-brottsligheten. Från integritetssynpunkt är i och för sig person-uppgiftsbehandling av detta slag ägnad att inge särskilda betänkligheter. Detta intrång måste dock ställas mot den kränkning som det innebär för människor att bli utsatta för brott av allvarligt slag.

För att det integritetsintrång som personuppgiftsbehandlingen kan ge upphov till inte ska bli oproportionerligt bör möjligheten till personuppgiftsbehandling för övervakning inskränkas till att avse uppgifter om och kring de personer som uppfattas som särskilt brottsaktiva eller farliga. Mot denna bakgrund föreslår vi att det i lagen tas in bestämmelser av innebörd att uppgifter får göras gemensamt tillgängliga om det *behövs för övervakningen av personer som är allvarligt kriminellt belastade eller kan antas vara farliga för annans personliga säkerhet*. Som förutsättning bör gälla att personen *kan antas komma att begå brott av mera allvarligt slag*; att han eller hon tidigare är dömd för sådana brott bör alltså inte vara tillräckligt. Med brott av mera allvarligt slag avser vi brott som kan ge fängelse i två år eller mera.

Lika lite som utredningen eller Registerutredningen anser vi att det är ändamålsenligt att i lagtexten närmare precisera uttrycken ”allvarlig kriminell belastning” och ”farlig för annans säkerhet”. Innebörden i dessa begrepp kommer att beröras närmare i författningskommentaren.

För att en bestämmelse av detta slag ska bli meningsfull bör polisens möjlighet att göra uppgifter gemensamt tillgängliga omfatta inte bara uppgifter som direkt avser de övervakade personerna utan även uppgifter om personer som har samband med de övervakade personerna. Uppgifter måste exempelvis kunna behandlas om att en övervakad person är anställd hos en viss annan person och att den övervakade personen regelbundet

besöker vissa personer. Men, som nyss har nämnts, en förutsättning för behandlingen bör vara att uppgiften *behövs för* övervakningen.

Åtkomsten till de behandlade uppgifterna bör liksom i dag vara starkt begränsad. Endast de tjänstemän som har till uppgift att arbeta med övervakningen bör kunna medges åtkomst. Information om huruvida en viss person är föremål för övervakning bör dock kunna spridas till flera. Att personuppgifter som behandlas för detta ändamål bör vara märkta på visst sätt återkommer vi till i avsnitt 10.

### 9.3 Utreda och beivra brott

**Promemorians förslag:** Personuppgifter som förekommer i ärenden om utredning och beivrande av brott ska alltid få göras gemensamt tillgängliga. Detta ska dock inte gälla uppgifter om resultat av DNA-analyser.

**Utredningens förslag:** Utredningen har inte föreslagit att man ska skilja på uppgifter som är gemensamt tillgängliga och andra uppgifter.

**Remissinstanserna** har inte yttrat sig i frågan.

**Skälen för promemorians förslag:** Det är självklart att uppgifter som behandlas för att utreda och beivra brott måste kunna göras gemensamt tillgängliga för de tjänstemän som arbetar med utredningen. Att sådana uppgifter kan göras gemensamt tillgängliga är också en förutsättning för att direktåtkomst ska kunna ges till åklagare, som ofta leder förundersökningar (se avsnitt 12.3.5). Enligt vår uppfattning finns det inte anledning att ställa upp något krav på att det ska vara fråga om utredning av allvarligare brott för att sådan behandling ska vara tillåten. Flertalet förundersökningar, oavsett misstänkt brott, är redan i dag lagrade i digital form i ett särskilt system (DurTvå; se *bilaga 6*).



Av lagen bör det således framgå att samtliga uppgifter som förekommer i ett ärende som avser utredning eller beivrande av brott får göras gemensamt tillgängliga. Det bör dock göras ett undantag från denna huvudregel, nämligen när det gäller resultatet av DNA-analyser. Vi återkommer till den frågan.

I lagen om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet föreskrivs som huvudregel att endast de personer som arbetar med ett ärende får ha direkt tillgång till uppgifterna som behandlas i ärendet. En följd av detta är att möjligheten att utnyttja uppgifter som behandlas inom ramen för en utredning i en annan utredning eller i underrättelseverksamhet försvåras. Vi anser inte att det är rimligt att ställa upp någon motsvarande begränsning för polisen. I en brottsutredning kan det vara av den största betydelse att uppgifter snabbt kan inhämtas från andra brottsutredningar, så att polisen kan bedöma om det finns några samband mellan utredningarna. Uppgifter i en förundersökning måste således kunna göras gemensamt tillgängliga för andra än de som arbetar i förundersökningen. Redan i dag är uppgifter av detta slag i viss utsträckning gemensamt tillgängliga. Åtkomsten till uppgifterna i Datoriserad utredningsrutin (DurTvå) är sålunda inte begränsad till de personer som arbetar med en viss förundersökning. I dag registreras även samtliga brottsanmälningar i Rationell anmälningsrutin (RAR; se *bilaga 6*). Samtliga personuppgifter läggs in i systemet, låt vara att endast vissa uppgifter får göras sökbara. Från RAR och DurTvå hämtas uppgifter till andra register, t.ex. till det centrala brottspaningsregistret som innehåller uppgifter om anmälda brott, tillvägagångssätt, signalement beträffande personer som setts på brottsplatsen m.m. Uppgifter från förundersökningar hämtas också till andra register. Att uppgifter i en brottsanmälan eller en förundersökning görs tillgängliga inom polisen för andra än de som arbetar i ärendet är alltså något som förekommer redan i dag i stor utsträckning och är en förutsättning för ett effektivt polisarbete. Det kan här noteras att det i de flesta fall endast är fråga om att göra vissa typer av uppgifter åt-

komliga för andra än de som arbetar i förundersökningen, inte hela förundersökningen.

Det förhållandet att det öppnas möjlighet att göra uppgifter om utredning av brott gemensamt tillgängliga innebär naturligtvis inte någon skyldighet att göra det. Uppgifter i vissa förundersökningar av särskilt känsligt slag bör sannolikt överhuvudtaget inte göras åtkomliga för andra än de som arbetar med förundersökningen. I vilken utsträckning möjligheten bör utnyttjas bör dock överlämnas till polisen att avgöra i det enskilda fallet.

En särskild fråga i sammanhanget är om uppgifter om resultat av DNA-analyser ska kunna göras gemensamt tillgängliga. Med begreppet ”resultat av DNA-analyser” avser vi här DNA-profiler. Behandlingen av DNA-profiler sker i princip i två faser. Den ena är när DNA-profilen tas fram och eventuellt jämförs med andra DNA-profiler och DNA-spår och den andra är vid registreringen i DNA-register. Som vi tidigare framhållit (se avsnitt 8) anses uppgifter om DNA-profiler vara extra känsliga genom den information de innehåller. All behandling av DNA inom brottsmålsförfarandet kringgärdas därför av särskilda regler. Detta talar för att uppgifter om DNA-profiler inte bör kunna göras gemensamt tillgängliga. Vi kan inte heller se något direkt behov av att göra sådana uppgifter gemensamt tillgängliga. Ett förbud mot att göra uppgifter om DNA-profiler gemensamt tillgängliga innebär inte något hinder mot att annan information som erhållits med hjälp av DNA-profilen, t.ex. utlåtandet angående identiteten på den person som avsatt DNA-spåret, kan göras gemensamt tillgänglig.

I avsnitt 17.2 överväger vi särskilda bestämmelser om register med uppgifter om resultatet av DNA-analyser.

## 9.4 Särskilt om behandlingen av uppgifter som rapporterats till polisens kommunikationscentraler

**Promemorians förslag:** Uppgifter som har rapporterats till polisens kommunikationscentraler ska få göras gemensamt tillgängliga i polisens brottbekämpande verksamhet.

**Utredningens förslag:** Utredningen har inte behandlat frågan.

**Remissinstanserna** har inte yttrat sig i frågan.

**Skälen för promemorians förslag:** I varje län ska det finnas en kommunikationscentral med uppgift att effektivisera och samordna bl.a. alarmeringsåtgärder. Kommunikationscentralerna tar emot och vidarebefordrar inkommande larm och andra meddelanden samt vidtar och samordnar inledningsvis polisåtgärder med anledning av larm. Som stöd för denna verksamhet finns det ett särskilt datasystem för kommunikationscentralerna, det s.k. KC-systemet (se bilaga 6). Till kommunikationscentralerna rapporterar poliser in även händelser, iakttagelser och utförda uppdrag. KC-systemet syftar till att dokumentera, bevaka och följa upp händelser och iakttagelser som rapporteras till kommunikationscentralerna. Syftet är också att på ett tidigt stadium kunna få signaler om pågående och återkommande brottslig verksamhet. Vidare har behandlingen till ändamål att ge underlag för planering av polisens resurser och för uppföljning av verksamheten. Systemet stöder inte endast polisens brottbekämpande verksamhet utan även annan polisiär verksamhet. Uppgifterna som antecknas i systemet får endast vara tillgängliga i tretton månader.

När kommunikationscentralen tar emot larm och meddelanden, antecknas det som rapporteras in. Vidare antecknas vilka åtgärder som vidtas med anledning av ett larm, t.ex. om en polispatrull skickas till platsen där ett brott påstås ha begåtts. När polispatrullen har varit på platsen, rapporterar den till kommuni-

kationscentralen vad som har hänt och vilka ytterligare åtgärder som bedöms vara nödvändiga. Det finns i dag inte några begränsningar i fråga om vilka uppgifter som får antecknas i systemet. Uppgifter registreras således om brotts- eller händelseplatser med besked om tid, plats, händelsetyp, brottskod och övrig information som kan vara till hjälp vid en kommande insats. Systemet innehåller också personuppgifter. Enkelt uttryckt kan man säga att det fungerar som en inledande postcentral där alla inrapporterade uppgifter antecknas för att senare sorteras och vidarebefordras till polisens olika verksamhetsgrenar. Uppgifter om misstänkta brott vidarebefordras till polisens utredningsrotlar, medan uppgifter om misstänkt brottslig verksamhet förs över till polisens underrättelserotlar. Systemet används normalt inte i den brottsbekämpande verksamheten för att söka efter information. Det förekommer emellertid att sökningar sker inom i systemet för att få fram uppgifter till en pågående brottsutredning, t.ex. om vad som har rapporterats in till polisen under en viss kortare tidsperiod eller på en viss plats. Det är dock endast ett begränsat antal tjänstemän som har behörighet att söka i systemet.

Vi anser att polisen även fortsättningsvis bör få dokumentera händelser och iakttagelser som har rapporterats till polisens kommunikationscentraler. För att en sådan dokumentation ska tillgodose polisens informationsbehov är det också nödvändigt att uppgifterna kan göras gemensamt tillgängliga. Som framgått av redogörelsen ovan kan emellertid det som rapporteras in till systemet innehålla vilka personuppgifter som helst. Meddelandena kan således mycket väl innehålla uppgifter som överhuvudtaget inte får behandlas eller göras gemensamt tillgängliga enligt de bestämmelser som vi nyss har föreslagit. Det kan t.ex. röra sig om uppgifter om personer som enbart misstänks för brottslig verksamhet som inte innefattar brott för vilket är föreskrivet ett års fängelse eller mer. Att i detta sammanhang göra skillnad på den eller andra typen av uppgifter framstår dock som praktiskt ogörligt. Den personal som tar emot och dokumente-

rar uppgifterna har inte någon möjlighet att pröva hur uppgifterna får behandlas.

Vi föreslår därför att det i den nya lagen tas in en särskild bestämmelse som ger ett generellt stöd för den behandling av personuppgifter som sker vid polisens kommunikationscentraler. Uppgifterna bör få göras gemensamt tillgängliga i polisens brottsbekämpande verksamhet.

I avsnitt 10 överväger vi om uppgifter som behandlas för nu aktuellt ändamål ska förse med en särskild upplysning om ändamålet med behandlingen. I avsnitt 16.2 överväger vi vilka särskilda gallringsbestämmelser som bör gälla för uppgifterna.

## 9.5 Gemensamt tillgängliga uppgifter i det internationella samarbetet

**Promemorians förslag:** Uppgifter i det internationella samarbetet får göras gemensamt tillgängliga om det behövs för att fullgöra den aktuella förpliktelsen.

**Utredningens förslag:** Utredningen har inte behandlat frågan.

**Remissinstanserna** har inte yttrat sig i frågan.

**Skälen för promemorians förslag:** En särskild fråga är hur man ska se på begreppet gemensamt tillgängliga uppgifter när det gäller internationellt samarbete. Enligt vår mening bör man i princip kunna utgå från samma kriterier i det arbetet som vid personuppgiftsbehandling för nationella behov.

En viktig del av det dagliga internationella samarbetet via Interpol består i utbyte av information om stulna pass, stulna fordon, stulen konst och efterlysta personer. Interpol för olika register över sådana uppgifter och medlemsstaterna utbyter fortlöpande sådan information med varandra. Syftet med s.k. internationell efterlysning av personer eller föremål är att man genom det förfarandet försvarar för brottslingarna. Man vidgar möjlig-

heterna att påträffa personer som försöker hålla sig undan rättvisan. Likaså förbättrar man förutsättningarna för att kunna återställa stulen egendom eller att åtminstone förhindra att obehörig vinst görs på att värdefulla stulna föremål avyttras i andra länder.

När en svensk myndighet sänder en internationell efterlysning till Interpol sker detta som ett led i den svenska brottsbekämpningen. Uppgifterna har då gjorts gemensamt tillgängliga med stöd av de regler som vi tidigare har redogjort för. När en svensk myndighet tar emot uppgifter från andra länder om internationella efterlysningar beror det på att den andra staten vill ha bistånd med upplysningar om var det efterlysta föremålet finns (och eventuellt med ett ingripande i form av beslag) eller hjälp med att ingripa mot den efterlysta personen om denne påträffas i Sverige. Upplysningarna om efterlysta personer och efterlysta föremål måste därför kunna vidarebefordras till i princip all polispersonal. Detta görs genom att uppgifterna tillförs de nationella registren över efterlysningar. För att vi ska kunna fullgöra våra internationella åtaganden i nu aktuella hänseenden måste således personuppgifter i viss utsträckning kunna göras gemensamt tillgängliga.

Ett annat exempel där det kan krävas att uppgifter görs gemensamt tillgängliga är förundersökningar som bedrivs parallellt i Sverige och i en annan stat och som gäller brott och brottsmisstankar som har samband med varandra. Även underrättelseuppgifter som lämnas till Sverige som ett led i allmänt informationsutbyte kan behöva behandlas gemensamt för att den svenska polisen ska kunna bidra med sina kunskaper.

Ett viktigt skäl till att uppgifter måste kunna göras gemensamt tillgängliga inom ramen för det internationella samarbetet är att Sverige i flera internationella överenskommelser har åtagit sig att inom polisen ha en kontaktpunkt som myndigheter i andra länder kan nå dygnet runt, året om (vad som brukar kallas 24/7-kontakt). En sådan kontaktpunkt ska bl.a. kunna besvara förfrågningar, förmedla kontakter inom polisorganisationen (och eventuellt till andra myndigheter som åklagare) samt bistå andra länder i brådskande angelägenheter av annat slag. Den in-

ternationella enheten på Rikspolisstyrelsen utgör en sådan kontaktpunkt. Detta får till följd att tjänstemän vid enheten måste kunna ha tillgång till personuppgifter i alla de internationella ärenden som förekommer vid enheten.

Den nya lagen bör alltså göra det möjligt att göra uppgifter som har mottagits inom ramen för internationellt samarbete gemensamt tillgängliga, om det behövs för att fullgöra det internationella åtagandet. Vi föreslår att det tas in en uttrycklig bestämmelse om detta i den nya lagen.





## 10 Särskilda upplysningar för gemensamt tillgängliga uppgifter

**Promemorians förslag:** Personuppgifter som görs eller har gjorts gemensamt tillgängliga ska förses med en särskild upplysning om det närmare ändamålet med behandlingen. De ska vidare förses med en särskild upplysning om att personen som uppgiften avser inte är misstänkt, om de direkt kan hänföras till en person som inte är misstänkt vare sig för visst brott eller för att ha utövat eller komma att utöva allvarlig eller systematisk brottslig verksamhet. Upplysning behöver dock inte lämnas om sådana förhållanden som ändå framgår tydligt av omständigheterna.

Uppgifter, som avser en person som kan antas ha samband med misstänkt brottslig verksamhet, ska som regel förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Detsamma gäller för personuppgifter som behandlas inom ramen för övervakning av brottsmisstänkta personer.

**Utredningens förslag:** Utredningen har föreslagit att uppgifter om personer som det inte finns någon misstanke om brott mot ska förses med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

**Remissinstanserna** har inte haft några invändningar mot utredningens förslag.

## Skälen för promemorians förslag

### *Upplysning om ändamålet med behandlingen*

Vårt förslag innebär att uppgifter av olika slag kan göras gemensamt tillgängliga utan att de för den skull behöver ingå i ett särskilt register av vilket de närmare skälen för behandlingen av personuppgifterna framgår. Det är dock viktigt att man alltid kan utläsa för vilket ändamål en uppgift som har gjorts gemensamt tillgänglig behandlas. Detta har betydelse bl.a. för möjligheterna att genom tekniska förfaranden eller administrativa bestämmelser kunna styra åtkomsten till vissa uppgifter. Vidare har det betydelse för att tillsynsmyndigheterna ska kunna kontrollera om viss behandling är berättigad och sker i enlighet med lagens bestämmelser.

En särskild bestämmelse bör därför tas in i den nya lagen med innebörd att det alltid ska framgå för vilket ändamål en personuppgift behandlas. Om en personuppgift behandlas inom ramen för den ovan föreslagna bestämmelsen om övervakning av vissa personer, bör detta framgå särskilt. Detsamma gäller om en uppgift behandlas med stöd av bestämmelsen om rapportering till polisens kommunikationscentraler.

### *Upplysning om att personen inte är misstänkt för brott eller brottslig verksamhet*

Av stor betydelse för skyddet av den personliga integriteten är att polisen behandlar uppgifter på ett sådant sätt att det klart framgår om en person behandlas som misstänkt för brott eller brottslig verksamhet eller om behandlingen sker av någon annan anledning. Vi föreslår därför att det i lagen slås fast att uppgifter om personer som inte är misstänkta vare sig för ett konkret brott eller för att ha utövat eller komma att utöva brottslig verksamhet ska förses med en upplysning om detta förhållande. Vissa

sådana bestämmelser finns redan i polisdatalagen (se 14 och 19 §§).

Behovet av en sådan upplysning är dock mindre påtagligt när det gäller uppgifter som ännu inte har gjorts gemensamt tillgängliga, t.ex. uppgifter som bara förekommer i en enskild tjänstemans dator eller i en liten, klart avgränsad projektgrupp. De handläggande tjänstemännen vet då varifrån uppgiften har kommit, varför den behandlas och om en omnämnd person är misstänkt för brott eller brottslig verksamhet eller inte. Upplysningsskyldigheten bör därför gälla endast i fråga om uppgifter som görs eller har gjorts gemensamt tillgängliga.

Ibland kan det redan av det sammanhang där en personuppgift förekommer framgå att personen inte är misstänkt. I en förundersökning som gäller misshandel kan det t.ex. framgå att A berörs av förundersökningen endast i egenskap av målsägande. En viss uppgiftssamling kan också ha sådan natur att det är uppenbart att de personer som ingår i samlingen inte är registrerade som misstänkta för brott eller brottslig verksamhet. Som exempel kan nämnas ett sådant diarium över inkomna eller upprättade handlingar som myndigheter enligt 15 kap. sekretesslagen (1980:100) ska föra. I ett sådant diarium ska bl.a. registreras vem en handling har inkommit från eller expedierats till. I fråga om sådana uppgifter har en särskild upplysning om att den aktuella personen inte är misstänkt inget värde. Vi föreslår därför att upplysning inte ska behöva lämnas om det redan av omständigheterna klart framgår att personen inte är misstänkt.

#### *Upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak*

I Europarådets rekommendation om användningen av personuppgifter inom polissektorn (se avsnitt 4.2.3) anges att skilda kategorier av lagrade uppgifter så långt som möjligt ska kunna skiljas från varandra efter graden av riktighet och tillförlitlighet. I synnerhet ska uppgifter som grundar sig på fakta kunna skiljas

från uppgifter som har sin grund i omdömen eller personliga värderingar. Det ska således gå att utläsa om den som lämnat uppgifter som sedan registreras kan anses vara tillförlitlig samt graden av riktighet i sak, t.ex. om informationen består av kontrollerade fakta eller endast icke styrkta antaganden. I lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet finns en bestämmelse om att uppgifter om en person som kan antas ha samband med brottslig verksamhet ska förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Vid tillkomsten av polisdatalagen övervägdes om en motsvarande bestämmelse borde tas in i den lagen. Den dåvarande regeringen lämnade dock inte något förslag om detta. Regeringen hänvisade till att den då föreslagna uppdelningen på belastningsregister, misstankeregister och kriminalunderrättelseregister innebar att bekräftade och konkreta uppgifter kom att skiljas från uppgifter som grundades på skäligen misstanke respektive på kriminalunderrättelseverksamhet. Att därutöver i lag ta in bestämmelser om att behandlade uppgifter även skulle förse med upplysning om uppgiftslämnarens trovärdighet ansågs inte befogat.

I vårt förslag ingår det inte några särskilda bestämmelser om personuppgiftsbehandling i kriminalunderrättelseverksamhet eller om kriminalunderrättelseregister. Tvärtom kommer det att vara möjligt att i en och samma uppgiftssamling sammanföra uppgifter med skiftande trovärdighet. Mot den bakgrunden finns det fog för att i den nya lagen uppställa ett krav på tilläggsupplysningar motsvarande det som uppställs i 16 § andra stycket lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. I den nya lagen bör det alltså tas in en bestämmelse om att uppgifter om personer som kan antas ha samband med brottslig verksamhet ska förse med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Bestämmelsen bör dock enligt vår mening inte vara generell.

För det första är behovet av en upplysning av detta slag ganska litet så länge den behandlade uppgiften inte har gjorts

gemensamt tillgänglig (se ovan). Vi föreslår därför att bestämmelsen inte ska gälla i fråga om uppgifter som ännu inte är – eller genom behandlingen blir – gemensamt tillgängliga.

För det andra – när det gäller personuppgiftsbehandling som sker inom ramen för en brottsutredning – framgår det som regel direkt av sammanhanget varför det har ansetts finnas fog för att behandla den, t.ex. av förhørsprotokoll eller vittneslistor. Risken för missuppfattningar inom ramen för handläggningen av utredningen torde därför vara liten. Vi föreslår därför att personuppgiftsbehandling inom ramen för en brottsutredning inte ska omfattas av den nya bestämmelsen.

För det tredje bör det finnas ett utrymme för att inte lämna någon tilläggsupplysning i sådana fall där upplysningen framstår som helt överflödigt. Så kan vara fallet beträffande personuppgifter av helt "neutral" karaktär, exempelvis uppgifter som har inhämtats från folkbokföringen. Vi föreslår därför att upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak inte behöver lämnas när detta på grund av särskilda omständigheter skulle sakna betydelse.



# 11 Sökbegränsningar för gemensamt tillgängliga uppgifter

## 11.1 Känsliga personuppgifter som sökbegrepp

**Promemorians förslag:** Känsliga personuppgifter ska inte få användas som sökbegrepp vid sökning i gemensamt tillgängliga uppgifter. Det ska dock inte finnas något hinder mot att använda uppgifter som beskriver en persons utseende som sökbegrepp.

**Utredningens förslag:** Utredningen har inte lämnat några förslag i denna del.

**Remissinstanserna** har inte berört frågan närmare.

**Skälen för promemorians förslag:** Vissa slag av uppgifter är till sin natur särskilt integritetskänsliga, i synnerhet uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och uppgifter som rör hälsa eller sexualliv. I avsnitt 8 har vi därför föreslagit att sådana uppgifter som huvudregel inte ska få behandlas. Men vi har också föreslagit att uppgifter om en person som behandlas på annan grund ska få kompletteras med känsliga uppgifter om det är absolut nödvändigt för syftet med behandlingen. Det innebär att det också i polisens olika uppgiftssamlingar kommer att finnas känsliga personuppgifter.

Från integritetssynpunkt är en av de viktigaste aspekterna med behandling av personuppgifter i vilken utsträckning uppgifterna kan sökas fram och sammanställas. Ju större möjligheter det finns att genom olika slag av sökningar och sammanställningar kartlägga enskildas privata förhållanden, desto större integritetsintrång kan personuppgiftsbehandlingen innebära. Sökningar på personuppgifter av de nyss nämnda slagen, dvs. ”känsliga personuppgifter”, är ägnade att inge särskilda betänkligheter. Mot den bakgrunden har det i 20 § lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, m.m. tagits in ett förbud mot att använda sådana känsliga uppgifter som sökbegrepp (prop. 2004/05:164 s. 89 f.).

Det kan i och för sig förekomma situationer då en möjlighet att göra sökningar på känsliga uppgifter skulle vara av värde för det brottsbekämpande arbetet, t.ex. vid en utredning om ett sexualbrott. I det alldeles övervägande antalet fall måste emellertid de möjligheter som polisen kommer att ha att söka i belastnings- och misstankeregistren på motsvarande brott antas vara tillräckliga. Vi anser därför att integritetsintresset i denna del måste väga över och att det i den nya lagen bör tas in en bestämmelse motsvarande den som finns i lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

I polisens brottsbekämpande verksamhet har signalementsuppgifter stor betydelse. Vid exempelvis eftersökning av misstänkta gärningsmän behöver polisen kunna använda sig av uppgifter om t.ex. kroppsbyggnad, ansiktsform, hår- eller hudfärg, klädsel och fysiska kännetecken såsom födelsemärken och tatueringar. Förbudet mot att använda känsliga personuppgifter som sökbegrepp bör därför inte hindra att uppgifter som beskriver en persons utseende används som sökbegrepp. Detta – som överensstämmer med vad som gäller enligt lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet – bör komma till uttryck i den nya lagen.



## 11.2 Sökning på namn, firma, personnummer, samordningsnummer eller organisationsnummer

**Promemorians förslag:** Vid sökning i gemensamt tillgängliga uppgifter på namn, firma, personnummer, samordningsnummer, organisationsnummer eller andra liknande identitetsbe-teckningar, får endast sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott eller är misstänkt för brott eller för brottslig verksamhet,

2. övervakas på grund av allvarlig kriminell belastning eller befarad farlighet för annans personliga säkerhet,

3. har anmält ett brott eller är målsägande i ett ärende som rör ansvar för brott,

4. är vittne eller annars ska höras eller avge yttrande i ett ärende,

5. har gett in eller tillsänts en handling, eller

6. är anmäld försvunnen.

Dessa begränsningar ska dock inte gälla vid sökning som sker i en viss handling eller i ett visst ärende. De ska inte heller gälla vid sökning i en uppgiftssamling som har skapats för att undersöka vissa preciserade slag av brottslighet eller vissa preciserade kriminella grupperingar och som enbart de som arbetar i undersökningen eller vissa särskilt angivna tjänstemän har åtkomst till.

Begränsningarna ska inte heller gälla vid sökning som sker för att förebygga, förhindra eller upptäcka särskilt allvarlig brottslig verksamhet eller för övervakning av personer som kan antas komma att begå brott och som är allvarligt kriminellt belastade eller kan antas vara farliga för annans personliga säkerhet, om sökningen utförs av särskilt angivna tjänstemän som har till uppgift att utreda den brottsliga verksamheten respektive sköta övervakningen.

Om det finns särskilda skäl, ska sökning utan begränsning även få ske för att utreda särskilt allvarliga brott, under förutsättning att sökningen utförs av särskilt angivna tjänstemän.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om och under vilka förutsättningar sökning får ske.

**Utredningens förslag:** Utredningen har inte lämnat några förslag i denna fråga.

**Remissinstanserna** har inte närmare berört frågan.

**Skälen för promemorians förslag:** Namn, firma, personnummer och organisationsnummer är viktiga för identifieringen av en person och kontrolleras regelmässigt i samband med brottsutredningar och annat brottsbekämpande arbete. Det samma gäller samordningsnummer, dvs. sådana identitetsbeteckningar som enligt 18 a § folkbokföringslagen (1991:481) kan tilldelas personer som inte är eller har varit folkbokförda i Sverige. Samtidigt är det tydligt att användandet av detta slag av uppgifter som sökbegrepp ger upphov till särskilda risker från integritets synpunkt. En sökning på exempelvis ett personnummer ger, i vart fall om den sker i den samlade informationsmängd som polisen har tillgång till, möjlighet till ingående kartläggningar av en persons privata förhållanden. Från ett integritetsperspektiv är därför sådana sökningar ägnade att inge stora betänkligheter.

Samtidigt är det uppenbart att möjligheten att göra detta slag av sökningar kan vara av stor betydelse i samband med kriminalunderrättelse- och brottsutredningsverksamhet. Det bör vara möjligt att inom ramen för det arbete som bedrivs i en undersökning som avser viss misstänkt brottslig verksamhet söka fram uppgifter om huruvida de personer som figurerar i det ärendet också är eller har varit misstänkta i andra ärenden. Det ökar möjligheterna att förhindra, upptäcka och beivra brott väsentligt. Vi anser därför att den nya lagen måste ge utrymme för sökningar på namn, personnummer eller liknande identitetsuppgifter.

En helt obegränsad möjlighet att använda detta slag av uppgifter som sökbegrepp bör emellertid inte komma i fråga. Vi har därför övervägt om det i den nya lagen bör tas in en bestämmelse motsvarande 21 § lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Enligt den bestämmelsen får namn, personnummer och samordningsnummer användas som sökbegrepp bara om uppgifterna avser en person som är misstänkt för något visst brott eller för viss verksamhet. Vi är dock inte övertygade om att en sådan bestämmelse är ändamålsenlig på polisens område. Å ena sidan tillåter en sådan bestämmelse att det vid sökningen tas fram information som är uppenbart betydelselös i sammanhanget (exempelvis att en för misshandel misstänkt person vid ett tidigare tillfälle har varit målsägande i en bedrägeriutredning). Å andra sidan tillåter bestämmelsen inte att det görs sådana sökningar som kan vara nödvändiga inom ramen för ett kriminalunderrättelseprojekt eller en brottsutredning. I ett sådant ärende kan det vara av stor vikt att kunna klarlägga om personer som har anknytning till den undersökta verksamheten – men som i det aktuella utredningsläget inte är misstänkta – förekommer som misstänkta i utredningar som gäller liknande brott. Det kan också vara viktigt att få fram uppgifter om att en viss person frekvent anmäler brott, eftersom det kan ha betydelse för dennes trovärdighet. Likaså kan uppgifter om att samma person gång på gång uppträder som vittne i vissa sammanhang påverka personens tillförlitlighet och trovärdighet.

Vi föreslår därför att möjligheten att söka på namn, personnummer och liknande identitetsuppgifter inte begränsas till misstänkta. Men vid sökningar på sådana uppgifter bör enbart vissa slag av uppgifter om den person som sökningen avser kunna tas fram. Först och främst bör det vara möjligt att få fram uppgifter som anger att den sökta har anmälts för brott eller är misstänkt för brott eller för allvarlig brottslig verksamhet. Med allvarlig brottslig verksamhet avser vi här detsamma som i avsnitt 9.2, dvs. verksamhet som innefattar brott för vilket kan följa fängelse i ett år eller däröver. Vidare bör det vara möjligt att få

fram uppgift om huruvida en person övervakas på grund av allvarlig kriminell belastning eller befarad farlighet för annans personliga säkerhet. En annan uppgift som bör vara möjlig att få fram är om personen har anmält ett brott eller att han eller hon är målsägande eller vittne i en brottsutredning. Detsamma gäller om någon är anmäld försvunnen. Det bör också vara möjligt att få fram uppgift om en handling har lämnats in av eller expedierats till personen i fråga.

Det som nu har sagts avser endast begränsningar av den initiala sökningen. En generell sökning av de uppgifter som behandlas hos polisen avseende en viss person ska alltså, enligt vårt förslag, endast ge uppgifter om huruvida vederbörande tillhör någon eller några av de kategorier som nyss angetts. Sedan man väl har fått träff på en viss person, exempelvis som misstänkt för brott i en viss förundersökning, ska dock ytterligare uppgifter kunna tas fram genom en fortsatt sökning i den uppgiftsmängden. Möjligheten att få åtkomst till ytterligare uppgifter, kanske hela förundersökningen, avgörs dock av vilken behörighet den berörda tjänstemannen har och om behandlingen behövs för något av lagens ändamål.

De integritetsrisker som motiverar den nu föreslagna inskränkningen i möjligheten att söka fritt gör sig dock inte gällande när det är fråga om sökningar i ett begränsat material. Den bör därför inte gälla vid sökning som sker inom ramen för ett visst ärende eller en viss handling.

För vissa delar av den brottsbekämpande verksamheten kan en begränsningsregel av den nu föreslagna arten leda till stora problem. Det gäller en del sådant arbete som i dag sker inom ramen för en särskild undersökning enligt 14 § polisdatalagen och som avser vissa preciserade slag av brottslighet (t.ex. narkotikabrottslighet i viss region) eller vissa preciserade kriminella grupperingar (t.ex. ett visst kriminellt mc-gäng). I sådant arbete upprättas ofta särskilda uppgiftssamlingar som syftar till att kartlägga brottsligheten eller de kriminella grupperingarna. Endast de tjänstemän som deltar i undersökningen har tillgång till dessa uppgiftssamlingar. Enligt vår mening bör det vara möjligt för de

deltagande tjänstemännen att göra sökningar i en sådan uppgiftssamling utan någon sådan begränsning som vi ovan har föreslagit. Vi föreslår därför att begränsningsregeln inte ska gälla vid sökning i en uppgiftssamling som har skapats för att undersöka vissa preciserade slag av brottslighet eller vissa preciserade kriminella grupperingar och som enbart de som arbetar i undersökningen har åtkomst till (med det undantag som följer av nästa stycke).

När det gäller underrättelseverksamhet som avser särskilt allvarlig brottslighet t.ex. grova narkotikabrott, terroristbrott och människohandel, finns det ett motsvarande behov av att kunna göra sökningar utan de begränsningar som har föreslagits ovan. Vi anser därför att sökbegränsningarna inte ska gälla vid sökning som sker för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra år eller däröver. Vid övervakning av personer som kan antas komma att begå brott och som är allvarligt kriminellt belastade eller kan antas vara farliga för annans personliga säkerhet finns ett likartat behov. I sådana fall är det viktigt för polisen att ha kännedom om var personen brukar befinna sig, vilka kontakter han eller hon har, vilka transportmedel personen förfogar över etc., för att polisen ska kunna ingripa i tid mot nya brott. De angivna begränsningarna bör därför inte gälla i dessa fall, under förutsättning att sökningen utförs av särskilt angivna tjänstemän som har till uppgift att hantera det aktuella ärendet. Sådana tjänstemän bör även få utföra sökningar i uppgiftssamlingar i undersökningar av viss preciserad brottslighet eller vissa preciserade kriminella grupperingar. Det bör meddelas föreskrifter om att myndigheten ska dokumentera vilka tjänstemän som har beviljats denna utökade möjlighet att söka efter uppgifter.

Ibland kan det också finnas behov av att göra mera omfattande sökningar inom ramen för en förundersökning. Som exempel kan nämnas utredningar om ouppklarade allvarliga seriebrott, t.ex. upprepade våldtäkter eller mordbränder. Detsamma kan gälla vissa mordutredningar. Förundersökningar om sådana brott kan pågå under mycket lång tid, om gärningsmannen är okänd.

Om det är fråga om mycket allvarliga brott, där samhällets intresse av att gärningsmannen lagförs är stort, är det enligt vår mening försvarligt att tillåta generella sökningar, om dessa kan bidra till att polisen kan spåra gärningsmannen och det är fråga om brott för vilket är föreskrivet fängelse i fyra år eller däröver. I likhet med vad som föreslagits i fråga om sökningar i underrätelseverksamheten eller vid övervakning av vissa personer bör emellertid sådana sökningar enbart få utföras av på förhand utpekade personer med särskilda arbetsuppgifter.

Det är viktigt att de sökbegränsningar som vi har föreslagit tillämpas korrekt och att tillsynsmyndigheterna kan kontrollera att så varit fallet. Regeringen bör meddela föreskrifter om att det vid myndigheten ska framgå av en förteckning eller motsvarande vilka tjänstemän som har tilldelats behörighet att utföra sådana särskilda sökningar.

## 12 Informationsutbyte mellan de brottsbekämpande myndigheterna

### 12.1 Allmänt om behovet av ett effektivt informationsutbyte mellan svenska brottsbekämpande myndigheter

**Promemorians bedömning:** En effektiv brottsbekämpning förutsätter att de brottsbekämpande myndigheterna kan utbyta information på ett rationellt sätt.

**Utredningen** har inte behandlat frågan särskilt.

**Remissinstanserna:** Flera remissinstanser, bl.a. *Riksåklagaren*, *Riksskatteverket*, *Tullverket* och *Kustbevakningen*, har påtalat behovet av ett effektivt informationsutbyte mellan de brottsbekämpande myndigheterna. Av remissvaren framgår att de brottsbekämpande myndigheterna anser sig ha ett påtagligt behov av att i ökad utsträckning få direktåtkomst till varandras uppgifter.

**Skälen för promemorians bedömning:** Samarbetet mellan de brottsbekämpande myndigheterna har blivit allt viktigare i det brottsförebyggande och brottsutredande arbetet. Ett effektivt och framgångsrikt arbete mot allvarlig och organiserad brottslighet förutsätter att man kan dra nytta av den samlade kunskap om brott och brottslingar som finns inte bara inom olika delar av polisorganisationen utan också hos andra brottsbekämpande myndigheter. Uppdelningen av den brottsbekämpande verksam-

heten på flera fristående myndigheter har emellertid i stor utsträckning kommit att styra möjligheterna till informationsutbyte, eftersom det kan råda sekretess mellan myndigheterna. Det är allmänt omvittnat att detta har lett till nackdelar när det gäller effektiviteten i brottsbekämpningen. Behovet av informationsutbyte mellan de brottsbekämpande myndigheterna är särskilt stort när det gäller att kartlägga och begränsa organiserad brottslighet, men det finns även behov av sådant samarbete för att angripa brottslighet av mera vardagligt slag. Av samma skäl som det är viktigt att man inom polisen på ett effektivare sätt än i dag kan tillgodogöra sig den information som finns inom den egna organisationen, är det viktigt att nyttiggöra informationen i samarbetet med andra brottsbekämpande organ.

Möjligheten till informationsutbyte mellan olika myndigheter är således av central betydelse i det brottsbekämpande arbetet. Ett förbättrat informationsutbyte skapar bättre förutsättningar för att utnyttja de samlade resurserna effektivt och därmed också för att brott i större utsträckning och snabbare kan klaras upp.

Mot de fördelar som ett ökat informationsutbyte innebär ska ställas att ett ökat flöde av uppgifter mellan myndigheter kan skapa risker för ökat intrång i den personliga integriteten, särskilt som de uppgifter som polisen behandlar ofta är av känsligt slag. Ett väl fungerande informationsutbyte mellan brottsbekämpande myndigheter behöver emellertid inte vara till nackdel för de personer som berörs av en brottsutredning. Tvärtom kan brottsoffren och den eller de misstänkta ibland ha ett gemensamt intresse av att brott klaras upp snabbt och att lagföring kommer till stånd i de fall där bevisningen är tillräcklig samt att felaktiga eller otillräckligt underbyggda brottsmisstankar avförs så snabbt som möjligt. I detta sammanhang är det också viktigt att påminna om det självklara att polisens arbete ytterst syftar till att skydda enskilda från att utsättas för den kränkning som ett brott utgör.

Risken för ökade intrång i den personliga integriteten genom informationsutbyte mellan myndigheter måste också ses i ljuset av att de andra brottsbekämpande myndigheterna redan i dag i



stor utsträckning har tillgång till de uppgifter hos polisen som kan anses vara några av de allra mest känsliga, nämligen uppgifter ur misstankeregistret. Vidare måste man väga in att det numera i princip råder samma sekretess för uppgifter om brottsbekämpning hos alla berörda myndigheter. Även om det således kan finnas nackdelar med ett ökat informationsflöde mellan de brottsbekämpande myndigheterna väger fördelarna över.

Det ligger i sakens natur att informationsutbytet till stor del avser uppgifter som omfattas av sekretess, eftersom de flesta av de uppgifter som behandlas inom polisens brottsbekämpande verksamhet skyddas av sekretess. En grundläggande förutsättning för att uppgifter ska få lämnas till en annan myndighet är att sekretess inte hindrar att uppgifterna lämnas ut. Detta gäller oberoende av om det rör sig om elektroniskt lagrade uppgifter eller uppgifter på papper. I sekretesslagen finns ett antal bestämmelser som innebär att sekretess inte hindrar utbyte av uppgifter mellan nationella brottsbekämpande myndigheter.

Med stöd av hänvisningar i sekretesslagen finns det dessutom en möjlighet att meddela sekretessbrytande föreskrifter i andra lagar och förordningar, se 14 kap. 1 § sekretesslagen. I polisdatlagen och polisdataförordningen finns bestämmelser om utlämnande av uppgifter som har en sekretessbrytande effekt. Det måste övervägas om sådana bestämmelser bör införas även i den nya lagen. Behovet av sekretessbrytande bestämmelser behandlas i avsnitt 13.

Det pågår ett fortlöpande arbete med att utveckla system för informationsutbyte inom och mellan brottsbekämpande myndigheter, bl.a. inom ramen för det arbete som bedrivs av Rådet för rättsväsendets informationsförsörjning (där Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Kriminalvården, Brottsförebyggande rådet, Brottsoffermyndigheten, Tullverket och Skatteverket ingår). Flera utredningar har också under senare år betonat att det måste skapas förutsättningar för ett förbättrat utbyte av information mellan de brottsbekämpande myndigheterna, se bl.a. SOU 2002:113, 2005:117 och 2006:18. Den gemensamma uppfattningen hos

dessa utredningar har varit att en brottsbekämpande myndighet ska kunna lämna information till en annan sådan myndighet, om den senare myndigheten behöver informationen i sin brottsbekämpande verksamhet.

Informationsutbytet sker i dag framförallt på manuell väg, efter en begäran från en myndighet i ett enskilt fall eller genom spontant uppgiftslämnande. Det kan röra sig både om utlämnande av uppgifter i pappersform och om olika former av elektroniskt utlämnande, t.ex. via e-post. I viss utsträckning förekommer elektroniskt utlämnande genom att mottagaren ges rätt att själv söka efter information som den utlämnande myndigheten har tillgång till (direktåtkomst), men det gäller för närvarande bara vissa register.

En ordning som innebär att informationsutbytet i huvudsak sker genom manuell behandling skapar praktiska problem, särskilt som brottsbekämpningen bedrivs dygnet runt. Uppgifter som en tjänsteman behöver omedelbart för att kunna genomföra en tjänsteåtgärd måste vara lätt tillgängliga även utanför vanlig kontorstid. Elektronisk åtkomst till uppgifter utan föregående begäran är således inte bara ett enkelt och arbetsbesparande sätt att lämna ut information utan ibland det enda i praktiken möjliga sättet att göra uppgifterna tillgängliga när de behövs.

Mot denna bakgrund står det klart att det finns ett ökande behov av ett effektivt informationsutbyte mellan de brottsbekämpande myndigheterna och att detta måste kunna tillgodoses genom ökad användning av elektronisk kommunikation.

En fråga som måste övervägas särskilt är i vilken form uppgifterna ska få lämnas ut, t.ex. om utlämnande bör få ske genom direktåtkomst. Den frågan behandlas i avsnitt 12.3. Utlämnande på medium för automatiserad behandling – både till svenska och utländska mottagare – behandlas i avsnitt 14.

## 12.2 Allmänt om behovet av informationsutbyte i det internationella samarbetet

**Promemorians bedömning:** Det internationella utbytet av information spelar en viktig roll för bekämpningen av framför allt allvarlig och gränsöverskridande brottslighet. Det arbetet bör kunna bedrivas i huvudsak på samma sätt som hittills.

**Utredningen** har gjort samma bedömning.

**Remissinstanserna** har inte haft någon invändning eller inte kommenterat saken närmare.

**Skälen för promemorians bedömning:** Av samma skäl som ett ökat informationsutbyte mellan svenska brottsbekämpande myndigheter bidrar till ett effektivare polisarbete gör internationellt samarbete i brottsbekämpande syfte det. Det är framför allt vid bekämpningen av allvarlig och gränsöverskridande brottslighet som det internationella informationsutbytet har betydelse. Utan sådant informationsutbyte skulle exempelvis bekämpningen av grov narkotikasmuggling, människohandel, penningtvätt och många andra typer av allvarliga brott inte kunna bedrivas lika framgångsrikt. Dessutom har Sverige, som framgått tidigare, genom olika internationella överenskommelser åtagit sig att överlämna information som härrör från brottsbekämpande verksamhet dels till polismyndigheter i andra länder, dels till Interpol och Europol.

Under senare år har det polisiära samarbetet mellan länderna inom EU utvecklats snabbt. I Europeiska rådets rekommendation om utarbetande av avtal mellan polis, tull och andra specialiserade brottsbekämpande organ, som antogs i april 2006 (6856/1/06 REV 1 ENFOCUSTOM 27 ENFOPOL 35 CRIMORG 40 CORDROGUE 15) betonar rådet vikten av ett förbättrat samarbete och informationsutbyte mellan de nationella brottsbekämpande myndigheterna. Hinder mot informationsutbyte på nationell nivå riskerar naturligtvis att påverka även det internationella informationsutbytet negativt. Det kan anmärkas

att Sverige har ådragit sig kritik avseende informationsutbyte såväl nationellt som internationellt vid utvärdering av Europols verksamhet (se SOU 2005:117 s. 153).

Nyligen antogs rådets rambeslut 2006/960/RIF av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater. Som tidigare nämnts pågår förhandlingar om flera rambeslut m.m. som påverkar det framtida informationsutbytet (se avsnitt 4.4). Ett av dessa är rambeslutet om dataskydd inom tredje pelaren, vars syfte är att förbättra integritetsskyddet. Ett likvärdigt integritetsskydd för uppgifter som översänds mellan medlemsstaterna kommer att underlätta det framtida informationsutbytet.

Det finns också anledning att erinra om att det polisiära samarbete över gränserna i stor utsträckning sker som led i *svenskt* underrättelsearbete eller *svensk* förundersökning eller lagföring. Sammantaget talar mycket för att polisen kommer att ha ett fortsatt stort behov av att kunna utbyta uppgifter med andra länder. En ny lag om behandling av uppgifter i polisens brottsbekämpande verksamhet bör inte ställa upp onödiga hinder för ett sådant utbyte utan möjligheterna att utbyta uppgifter bör i huvudsak motsvara vad som gäller i dag. I avsnitt 12.3.6 övervägs om utländska myndigheter även bör kunna medges direktåtkomst till svenska register. En sådan möjlighet skulle innebära en utvidgning i förhållande till vad som gäller i dag. I avsnitt 13.3 övervägs vilka sekretessbrytande bestämmelser om utlämnande som lagen bör innehålla. I det sammanhanget berörs det internationella informationsutbytet närmare.

## **12.3 Elektroniskt informationsutbyte**

### **12.3.1 Olika former av elektroniskt utlämnande av uppgifter**

I många författningar om behandling av personuppgifter regleras frågor om utlämnande av personuppgifter i elektronisk form

genom särskilda bestämmelser i lag eller förordning. Enligt gängse begreppsbildning kan personuppgifter lämnas ut i elektronisk form endera på s.k. medium för automatiserad behandling eller genom direktåtkomst.

Ett utlämnande på medium för automatiserad behandling kan innebära t.ex. att elektronisk information överförs via e-post, genom utlämnande av uppgifter på diskett, cd-rom, DVD, USB-minne eller genom direkt överföring från ett datorsystem till ett annat via allmänna kommunikationsnät. I sådana fall tar den utlämnande myndigheten i varje enskilt fall ställning till om uppgifter kan lämnas ut och vilka uppgifter som ska lämnas. En eventuell sekretessprövning kan därmed ske i samband med utlämnandet i det enskilda fallet. Utlämnande av uppgifter kan även ske genom direktåtkomst. Vid direktåtkomst fattas beslutet om överföring i varje enskilt fall av mottagaren.

Av dessa olika varianter av elektroniskt utlämnande är direktåtkomst den mest känsliga. Denna fråga kommer därför att beröras mer ingående i det följande. Utlämnande på medium för automatiserad behandling tas upp i avsnitt 14.

### 12.3.2 Begreppet direktåtkomst

Det finns ingen legaldefinition av begreppet direktåtkomst. Den grundläggande innebörden av begreppet är att någon har direkt tillgång till någon annans register eller databaser och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. I begreppet direktåtkomst ligger också att den som är personuppgiftsansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av. Den myndighet som lämnar ut uppgifter genom direktåtkomst fattar således inte beslut om utlämnande av de uppgifter som den enskilde tar del av i varje enskilt fall. I stället måste en förhandsprövning göras av förutsättningarna för utlämnande. En sådan prövning innefattar alla de uppgifter som mottagaren har möjlighet att ta del av ge-

nom sin direktåtkomst. Den faktiska begränsningen av direktåtkomsten görs sedan med hjälp av olika tekniska lösningar, beroende på hur omfattningen av direktåtkomsten har begränsats i det enskilda fallet, exempelvis genom olika behörighetsnivåer. Det är den personuppgiftsansvariga myndigheten som ska se till att åtkomsten rent faktiskt begränsas på det sätt som föreskrivs.

Eftersom begreppet direktåtkomst avser ett tillvägagångssätt för utlämnande av uppgifter i elektronisk form, är det vid reglering av direktåtkomst typiskt sett inte nödvändigt att reglera den åtkomst som en myndighet har till sina egna register och databaser. Myndighetens egen tillgång till information i databasen innefattar normalt behörighet att såsom personuppgiftsansvarig påverka innehållet i databasen, dvs. behörighet att vidta åtgärder som sträcker sig längre än att medge direktåtkomst. I fråga om den åtkomst som personalen vid en myndighet har till myndighetens egna register och databaser är det därför lämpligare att tala om direkt tillgång till registren och databaserna i stället för direktåtkomst (se prop. 2004/05:164 s. 73). Finns det flera självständiga verksamhetsgrenar inom en och samma myndighet, mellan vilka det råder sekretess (jfr 1 kap. 3 § första och andra styckena sekretesslagen), behövs dock normalt – när direktåtkomsten är författningsreglerad – även bestämmelser om direktåtkomst för den eller de verksamhetsgrenar som inte ansvarar för själva databasen för att sådan åtkomst ska kunna medges. Detta beror på att uppgifterna i sådana fall anses utlämnade från en verksamhetsgren till en annan.

Vid författningsreglering av direktåtkomst till uppgifter anges ofta att någon får ha direktåtkomst. Innebörden av detta är inte att den eller de angivna myndigheterna har en ovillkorlig rätt att få ut uppgifterna, utan att den myndighet som innehar informationen har en rätt att medge sådan åtkomst. Den utlämnande myndigheten har ett principiellt ansvar att förvissa sig om att den myndighet som beviljas direktåtkomst vidtar de åtgärder som bedöms vara nödvändiga från säkerhetssynpunkt. I några författningar tydliggörs detta genom bestämmelser som anger att myndigheten i fråga inte får medge andra direktåtkomst till sina

register innan den har försäkrat sig om att behörighets- och säkerhetsfrågorna är lösta på ett sätt som är tillfredsställande ur integritetssynpunkt (se t.ex. 4 kap. 4 § förordningen [2001:650] om vägtrafikregister). Medgivandet av direktåtkomst förutsätter också att utlämnande får ske enligt den gällande sekretessregleringen för berörda myndigheter, vilket utvecklas närmare i avsnitt 13.

### 12.3.3 Nuvarande möjligheter till direktåtkomst

#### *Polisens direktåtkomst till uppgifter hos andra brottsbekämpande myndigheter*

Polisens möjlighet att ta del av uppgifter som behandlas hos andra brottsbekämpande myndigheter styrs genom de författningar som gäller för dessa myndigheter.

Beträffande uppgifter som behandlas av Tullverket föreskrivs i 6 § förordningen (2005:791) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet att Ekobrottsmyndigheten, Rikspolisstyrelsen, polismyndigheterna, Kustbevakningen och Skatteverket får ha direktåtkomst till sådana uppgifter i tullbrottsdatabasen som behandlas för ändamålen att förhindra och upptäcka brottslig verksamhet. Enligt 7 § får Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och polismyndigheterna ha direktåtkomst till sådana uppgifter som behandlas för ändamålen att utreda och beivra visst brott, om uppgifterna förekommer i en förundersökning som leds av åklagare.

Enligt 18 § förordningen (2003:188) om behandling av personuppgifter inom Kustbevakningen får övriga brottsbekämpande myndigheter ha direktåtkomst till uppgifter hos Kustbevakningen. Tullverkets åtkomst omfattar dock inte uppgifter om vattenföroreningsavgift. Skatteverkets åtkomst är begränsad till de brott som Skatteverket får utreda och Åklagarväsendets åtkomst är begränsad till uppgifter om utredning av brott, om utredningen leds av åklagare. I betänkandet Kustbevakningens per-

sonuppgiftsbehandling (SOU 2006:18) uttalade Utredningen om Kustbevakningens personuppgiftsbehandling att det framstår som uppenbart att övriga brottsbekämpande myndigheter ska kunna medges direktåtkomst till uppgifter hos Kustbevakningen. Utredningen föreslog därför att sådan åtkomst ska beviljas till uppgifter som Kustbevakningen behandlar för att förhindra och upptäcka brottslig verksamhet och för att utreda och beivra brott. Betänkandet bereds för närvarande inom Regeringskansliet (Försvarsdepartementet).

*Andra myndigheters direktåtkomst till uppgifter som polisen behandlar*

De övriga brottsbekämpande myndigheterna har redan i dag i varierande utsträckning direktåtkomst till uppgifter som polisen behandlar i vissa register, framför allt misstankeregistret och belastningsregistret. I närmast följande avsnitt, där andra myndigheters behov av direktåtkomst till polisens uppgifter behandlas närmare, redovisas vad som gäller i dag i fråga om direktåtkomst till polisens register.

#### **12.3.4 De brottsbekämpande myndigheternas behov av tillgång till uppgifter i polisens brottsbekämpande verksamhet**

**Promemorians bedömning:** Samtliga brottsbekämpande myndigheter har behov av att kunna få direktåtkomst till uppgifter som behandlas av polisen.

**Utredningens förslag:** Utredningen har inte närmare behandlat frågan om övriga brottsbekämpande myndigheters allmänna behov av direktåtkomst till uppgifter som behandlas i polisens brottsbekämpande verksamhet. Däremot har utred-



ningen lagt förslag om att andra myndigheter ska ha direktåtkomst till vissa utpekade register.

**Remissinstanserna:** Flera remissinstanser, bl.a. *Riksåklagaren*, *Riksskatteverket*, *Tullverket* och *Kustbevakningen*, har påtalat att de har behov av att kunna ta del av uppgifter som behandlas i polisens brottsbekämpande verksamhet genom direktåtkomst.

### Skälen för promemorians bedömning

Vittgående möjligheter till direktåtkomst ökar riskerna för intrång i den personliga integriteten. Typiskt sett innebär direktåtkomst att känsliga uppgifter blir tillgängliga för en större krets personer och att den personuppgiftsansvariga myndighetens möjligheter att kontrollera användningen av uppgifterna minskar. Det är visserligen möjligt att genom särskilda åtgärder motverka dessa risker. Likväl är det viktigt att myndigheternas behov av direktåtkomst övervägs noga och att behoven vägs mot integritetsriskerna.

#### *Polismyndigheters behov av direktåtkomst till varandras uppgifter*

Det är angeläget att den brottsbekämpande verksamheten kan bedrivas effektivt. Med utnyttjande av modern teknik ökar möjligheterna att skapa överblick och samordning i det brottsbekämpande arbetet och att utnyttja tillgänglig information på ett effektivt sätt. Det är angeläget att dessa möjligheter kan utnyttjas. En tjänsteman vid en polismyndighet som arbetar med en utredning eller något annat projekt som avser en misstänkt person eller en viss företeelse bör på ett enkelt sätt kunna skaffa sig kunskap om existerande anmälningar och om huruvida det bedrivs brottsutredningar eller underrättelseprojekt riktade mot samma person eller samma företeelse inom någon annan del av myndigheten eller i en annan del av landet. Likaså måste den lokala polisorganisationen lätt kunna tillgodogöra sig den kunskap

och erfarenhet som specialenheter eller den centrala polisorganisationen besitter när det gäller exempelvis bekämpning av vissa brottstyper eller utvecklingen av den internationella brottsligheten.

Polisanställda som arbetar i den brottsbekämpande verksamheten vid Rikspolisstyrelsen, polismyndigheter och Ekobrottsmyndigheten har således ofta ett legitimt behov av att kunna få tillgång till uppgifter som har gjorts gemensamt tillgängliga inom polisen. Deras behov av att få tillgång till uppgifter som behandlas inom andra delar av polisorganisationen avser ofta inte enbart uppgifter i vissa register. Behovet kan i princip avse alla typer av uppgifter som förekommer i polisens brottsbekämpande verksamhet. Ett så omfattande behov kan, med hänsyn till den arbetsinsats som krävs för att hantera uppgifterna, bara tillgodoses genom direktåtkomst.

Eftersom Rikspolisstyrelsen, de enskilda polismyndigheterna och Ekobrottsmyndigheten utgör sinsemellan självständiga myndigheter behövs en reglering av direktåtkomsten även inom polisen.

#### *Säkerhetspolisens behov av direktåtkomst till uppgifter hos polisen*

Som utvecklas närmare i avsnitt 18 skiljer sig Säkerhetspolisens verksamhet från den övriga polisverksamheten i olika avseenden. Säkerhetspolisen tillhör organisatoriskt Rikspolisstyrelsen, men har en självständig ställning. En av Säkerhetspolisens uppgifter är att inom Rikspolisstyrelsen leda och bedriva viss polisverksamhet, nämligen brottsbekämpande verksamhet rörande brott mot rikets säkerhet, terrorismbekämpning, bevaknings- och säkerhetsarbete som rör statsledningen och statsbesök samt personskydd i vissa andra fall. När Säkerhetspolisen för Rikspolisstyrelsens räkning leder och bedriver sådan polisverksamhet har Säkerhetspolisen ställning som polismyndighet (se 7 § andra stycket polislagen [1984:387] jämförd med 2 § förordningen [2002:1050] med instruktion för Säkerhetspolisen).

I sin egenskap av polismyndighet, där bl.a. brottsutredning ingår, har Säkerhetspolisen samma behov som andra polismyndigheter att få tillgång till exempelvis belastningsregistret och misstankeregistret och till andra uppgifter av betydelse för brottsutredning och för att förebygga och upptäcka brott och brottslig verksamhet.

Säkerhetspolisen har enligt sin instruktion också vissa andra uppgifter, där myndigheten inte leder och bedriver polisverksamhet i den mening som avses i 7 § polislagen (se 3 § förordningen med instruktion för Säkerhetspolisen). Till dessa uppgifter hör bl.a. att fullgöra de uppgifter som ankommer på Rikspolisstyrelsen enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). En viktig uppgift i det sammanhanget är registerkontroll. För att fullgöra den uppgiften behöver Säkerhetspolisen tillgång till information som behandlas inom den övriga polisen. I de fall där Säkerhetspolisen inte har ställning som polismyndighet ingår myndigheten som en del i Rikspolisstyrelsen.

#### *Åklagarväsendets behov av direktåtkomst till uppgifter hos polisen*

Åklagarväsendet (Åklagarmyndigheten och Ekobrottsmyndigheten) har för närvarande direktåtkomst till misstankeregistret och belastningsregistret samt till uppgift om en person förekommer i DNA-register. Åklagarväsendet kan vidare ges direktåtkomst till sådana uppgifter i tullbrottsdatabasen som förekommer i en brottsutredning som leds av åklagare. I den polisiära verksamheten hos Ekobrottsmyndigheten har man direktåtkomst bl.a. till det centrala kriminalunderrättelsesregistret och det allmänna spaningsregistret.

När åklagaren leder en förundersökning eller annan utredning har han eller hon givetvis behov av att kunna ha direktåtkomst till materialet i förundersökningen. Detsamma gäller alla andra typer av utredningar som görs med stöd av 23 kap. rättegångsbalken. Behovet gör sig gällande i alla typer av förundersök-

ningar och andra liknande utredningar; åklagare har ju rätt att leda förundersökningar angående alla typer av brott som hör under allmänt åtal. Det enda undantaget kan sägas vara utredningar om tryckfrihetsbrott och yttrandefrihetsbrott, där endast Justitiekanslern är behörig åklagare. Denne brukar emellertid i stor utsträckning uppdra åt åklagare att utföra förundersökning, varför åklagarens behov av att få direktåtkomst till förundersökningsmaterial i praktiken är lika stort beträffande sådana brott. Eftersom åklagare med stöd av 23 kap. 3 § rättegångsbalken har en ovillkorlig rätt att ta över förundersökningsledningen i en förundersökning som har inletts av polisen, och polisen dessutom har en skyldighet att hålla åklagare underrättad om förundersökningens gång beträffande sådana förundersökningar som leds av polisen och som rör allvarlig eller svårbedömd brottslighet (2 § förundersökningskungörelsen [1947:948]), har åklagaren behov av direktåtkomst även till uppgifter i sådana förundersökningar. I princip har således åklagarväsendet samma behov som polisen att ha direktåtkomst till uppgifter i förundersökningar.

Åklagaren har också genom sitt uppdrag behov av kunna få tillgång till allmänna uppgifter om polisens brottsbekämpande och brottsutredande verksamhet. Det kan exempelvis vara fråga om information, som rör en viss brottstyp eller en viss arbetsmetod, eller statistik eller liknande. Behovet ska ses mot bakgrund av åklagarens roll i förhållande till polisen, som i princip utgör den enda resursen för att åklagaren ska kunna fullgöra en av sina huvuduppgifter, att utreda brott. Åklagarens särställning återspeglas dels i 3 § polislagen (1984:387), dels i 2 kap. 9 § och 3 kap. 14 § polisförordningen (1998:1558).

När det gäller underrättelseuppgifter kan åklagarens behov av direktåtkomst inte generellt sägas vara lika stort. Ett skäl till det är att det endast är ett begränsat antal åklagare som sysslar med utredning av särskilt allvarliga brott som utförs i mer eller mindre organiserade former, vilket är ett av underrättelseverksamhetens huvudområden. Å andra sidan har dessa åklagare stort behov av att kunna få tillgång till underrättelseinformation även

när det ännu inte finns några konkreta misstankar om brott. Det är nämligen för den enskilde en viktig rättssäkerhetsfråga att förundersökning inleds så snart det finns grund för det. Först då aktualiseras de rättssäkerhetsgarantier som är inbyggda i en förundersökning. Mot den bakgrunden får också åklagare anses ha legitimt behov av direktåtkomst till underrättelseuppgifter. Behovet torde framför allt avse uppgifter i det som i dag benämns särskild undersökning. Det kan även i enskilda fall finnas ett visst behov av att låta åklagare få tillgång till den behandling som i dag sker inom ramen för kriminalunderrättelseregister. Ett exempel kan vara Ekobrottsmyndigheten, där poliser och åklagare arbetar tillsammans på ett närmare sätt än inom verksamheten i övrigt. Inom ramen för en förundersökning om allvarliga brott, som exempelvis upprepade mordbränder eller serievåldtäkter, finns det, som tidigare nämnts, inte sällan behov av att bedriva registerkontroll, göra omfattande sökningar på tidigare brott och kontroll av personer som tidigare har dömts för liknande brott. Sådana undersökningar, som normalt görs inom ramen för underrättelseprojekt, kan således ibland vara nödvändiga inslag i en pågående förundersökning.

#### *Tullverkets behov av direktåtkomst till uppgifter hos polisen*

Tullverket har i dag direktåtkomst till misstankeregistret, belastningsregistret, Schengens informationssystem, analys- och beslagsregistret samt fingeravtrycks- och signalementsregistren. Vidare har enskilda tulltjänstemän fått behörighet att ta del av vissa uppgifter i det allmänna spaningsregistret, godsregistret och registret över efterlysta fordon.

På samma sätt som polisen har Tullverket till uppdrag att förebygga, förhindra och upptäcka brottslig verksamhet samt att utreda och beivra brott. I sin brottsbekämpande verksamhet utför tulltjänstemännen i allt väsentligt samma uppgifter som polismän i motsvarande verksamhet inom polisväsendet. Tullverket har därigenom samma behov av personuppgiftsbehandling och

tillgång till vissa typer av uppgifter som polisen när det gäller brottstyper inom tullens behörighetsområde.

Tullverket har emellertid ett snävare arbetsfält än polisen. Ansvarsområdet är dels brott mot lagen (2000:1225) om straff för smuggling och författningar som anges i den lagen (bl.a. vissa brott mot narkotikastrafflagen och brott mot vissa skatteförfattningar), dels brott som rör införsel eller utförsel enligt vissa skatteförfattningar, dels brott mot tullagstiftning. Något förenklat utreder Tullverket framför allt smugglingsbrott, gränsöverskridande narkotikabrott och ekonomisk brottslighet i form av tullbrott. Tullverkets brottsbekämpande verksamhet har således ett ganska brett spektrum, men fokus ligger på brott som begås när varor, personer och annat passerar landets gränser.

I de fall där Tullverket biträder en åklagare med utredningsåtgärder i en förundersökning kan en tjänsteman vid Tullverket ha samma behov av att kunna få tillgång till uppgifter som behandlas i polisens brottsbekämpande verksamhet som en polisman. Sådant biträde innebär ibland att polismän och tulltjänstemän arbetar tillsammans i samma utredning. I sådana fall är det angeläget att det finns en möjlighet för dem att på ett enkelt sätt utbyta information.

Tullverkets roll är sådan att den brottsutredande verksamheten ofta förutsätter samarbete med andra myndigheter såväl inom Sverige som över gränserna. När det gäller brott till sjöss och i kustnära områden sker ett nära samarbete med Kustbevakningen. Bekämpningen av allvarlig narkotikabrottslighet kräver ett mycket nära samarbete mellan Tullverket och polisen. Narkotikan tillverkas normalt utomlands och förs till Sverige. Vidare har organiserad narkotikabrottslighet i mycket stor utsträckning internationella förgreningar. Det kan ibland vara en slump om det är polisen eller Tullverket som först upptäcker spår av sådan brottslighet och inleder underrättelseverksamhet eller förundersökning. Det bör också nämnas att Tullverket genom sitt internationella samarbete samlar bred kunskap om bl.a. narkotikabrottsligheten och dess utveckling internationellt, vilket kan vara till stor nytta för polisen i dess brottsutredande verksamhet. Be-

hovan av informationsutbyte mellan dessa myndigheter är således mycket stort. I sammanhanget bör också nämnas att polisen har direktåtkomst till tullbrottsdatabasen, som är den databas där Tullverket behandlar uppgifter som rör brottsbekämpning.

Vid skilda tidpunkter har personal från bl.a. Tullverket och polisen samlokaliseras, i syfte att effektivisera informationsutbytet och att utveckla den gemensamma uppgiften att bekämpa allvarlig brottslighet. I flera fall har sådant samarbete, som i sig ansetts öka effektiviteten och ge andra positiva effekter, avbrutits därför att möjligheten att bevilja direktåtkomst till uppgifter i den andra myndighetens verksamhet har varit alltför begränsad. Detta visar att behovet av direktåtkomst till uppgifter hos andra brottsbekämpande myndigheter kan vara en grundläggande förutsättning för att utveckla samarbetet myndigheterna emellan. Under senare år har regionala underrättelsecenter bildats där tjänstemän från flera brottsbekämpande myndigheter arbetar tillsammans i gemensamma ärenden. Det är önskvärt att man inom ramen för sådant samarbete har möjlighet att bygga upp uppgiftssamlingar som samtliga inblandade har direkt tillgång till.

En annan aspekt på samarbetet mellan polisen och Tullverket är att statsmakterna under senare år i allt större utsträckning har övervägt möjligheterna att låta tulltjänstemän och kustbevakningstjänstemän göra ingripanden som normalt ankommer på polismän på platser där polisen inte finns till hands men där Tullverket eller Kustbevakningen utövar sin kontrollverksamhet, t.ex. i hamnar och vid gränspassager. Ett aktuellt exempel gäller nykterhetskontroll och ingripanden mot personer som gör sig skyldiga till rattfylleri. En utredning har föreslagit att personal inom Tullverket och Kustbevakningen ska ges rätt att ingripa mot sådana brott och att utföra nykterhetskontroller utan någon misstanke om brott (se SOU 2006:47). En sådan ordning skulle påverka behovet av direktåtkomst till uppgifter hos polisen.

*Kustbevakningens behov av direktåtkomst till uppgifter hos polisen*

Kustbevakningen har i dag direktåtkomst till Schengens informationssystem. Däremot har Kustbevakningen ingen direktåtkomst till belastningsregistret, endast en rätt att i vissa fall få ut uppgifter ur registret. Kustbevakningen har i en särskild framställning begärt att få direktåtkomst till både detta register och misstankeregistret. Denna fråga behandlas i avsnitt 22.

Via Tullverkets system har Kustbevakningen tillgång till polisens godsregister och register för efterlysta fordon. Kustbevakningen har också direktåtkomst till tullbrottsdatabasen. Dessutom har Kustbevakningen rätt att få uppgifter ur det allmänna spaningsregistret, om uppgifterna kan antas ha särskild betydelse för en pågående utredning eller andra brottsbekämpande åtgärder.

Kustbevakningen har, i likhet med Tullverket och Skatteverket, brottsbekämpande uppgifter enbart beträffande vissa i författning angivna typer av brott. Kustbevakningens brottsbekämpande verksamhet anknyter till dess uppgift att svara för övervakningen till sjöss och i sjönära områden. Kustbevakningens brottsbekämpande verksamhet innehåller så vitt skilda uppgifter som att ingripa mot brott mot regler om skyddsobjekt och militära skyddsområden, miljöregler och regler om skydd mot dumpning och oljeskador, jakt- och fiskeregler, trafikregler och säkerhetsregler till sjöss, regler om fornminnen och sjöfynd, regler om skydd av hotade arter samt regler om utlänningars in- och utresa. För en närmare beskrivning av Kustbevakningens verksamhet, se avsnitt 24.2.

I likhet med Tullverket har Kustbevakningen i sin brottsbekämpande verksamhet i princip samma uppgifter som polisväsendet. En kustbevakningstjänsteman har i denna verksamhet samma arbetsuppgifter och i huvudsak samma befogenheter som en polisman. Kustbevakningen har således i grunden samma behov av att få tillgång till vissa typer av uppgifter som behandlas i polisens brottsbekämpande verksamhet som Tullverket har.



Kustbevakningen liknar Tullverket även i det avseendet att det ofta krävs nära samverkan mellan Kustbevakningen och polisen i det brottsbekämpande arbetet. Det finns dock en skillnad på grund av att Kustbevakningens rätt att inleda och bedriva förundersökning är mycket begränsad. I flertalet fall ska Kustbevakningen snabbt lämna över ärendet till polisen (eller annan myndighet) för fortsatt handläggning. Det förhållandet att myndigheten har ansvar för att omedelbart ingripa på platsen, samtidigt som det sällan finns möjlighet för polisen att ta över ansvaret förrän efter viss tid, gör dock att Kustbevakningens behov av att snabbt kunna kontrollera vissa uppgifter beträffande personer, varor eller fartyg generellt sett är mycket stort. Det kan ibland vara helt avgörande att ha tillgång till vissa uppgifter för att exempelvis kunna bedöma om en person ska tillåtas passera in i eller ut ur landet.

När Kustbevakningen biträder en åklagare med utredningsåtgärder i en förundersökning, har tjänstemannen vid Kustbevakningen ofta samma behov av att kunna få tillgång till uppgifter som behandlas i polisens brottsbekämpande verksamhet som en polisman eller en tulltjänsteman. Sådant biträde innebär ibland att polismän och kustbevakningstjänstemän arbetar tillsammans i samma utredning. I sådana fall är det angeläget att det finns möjlighet för dem att på ett enkelt sätt utbyta information.

I sammanhanget bör också nämnas att det sedan några år finns ett för Tullverket, polisväsendet och Kustbevakningen gemensamt maritimt underrättelsecentrum (MUC) i Karlskrona. Syftet med detta underrättelsecentrum är att effektivisera myndigheternas brottsbekämpning genom gemensam riskanalysbaserad kontrollverksamhet. Verksamheten är inriktad på att upptäcka och förhindra brott (för en närmare beskrivning av verksamheten, se SOU 2006:18 s. 51). Den är ett exempel på hur man kan utnyttja och stärka underrättelseverksamheten inom en myndighet och samtidigt förbättra förutsättningarna för en effektiv underrättelseverksamhet inom andra brottsbekämpande myndigheter. Det visar också att Kustbevakningen har behov av såväl att kunna utbyta information i enskilda ärenden eller be-

träffande enskilda frågor som att systematiskt kunna dra nytta av den underrättelseverksamhet som bedrivs inom andra brottsbekämpande myndigheter.

#### *Skatteverkets behov av direktåtkomst till uppgifter hos polisen*

Skatteverket har i dag rätt till direktåtkomst till misstankeregistret, belastningsregistret och tullbrottsdatabasen.

Skatteverkets brottsbekämpande verksamhet bedrivs i en särskild organisation, de s.k. skattebrottsenheterna. Deras verksamhet omfattar bara vissa i lagen (1997:1024) om Skatteverkets medverkan i brottsutredningar angivna typer av brott. Utöver brott enligt skattebrottslagen (1971:69), bokföringsbrott, brott mot näringsförbud och brott mot folkbokföringslagen (1991:481) rör det sig enbart om några få brottstyper.

Skatteverket får bedriva spaning och underrättelseverksamhet i fråga om brott som angetts ovan. Det ingår i Skatteverkets uppgifter att förebygga sådan brottslighet. Verket får även utreda sådana brott, om den misstänkte kan antas erkänna brottet och utredningen kan genomföras med stöd av det förenklade förfarande som anges i 23 kap. 22 § rättegångsbalken.

En åklagare kan anlita biträde av en skattebrottsenhet vid utredning av brott. Det gäller både sådana brott som Skatteverket ska bekämpa och andra typer av brott.

En skattebrottsutredare vid en skattebrottsenhet har dock snävare befogenheter än en polisman eller en tjänsteman vid Tullverket eller Kustbevakningen. Utredaren får t.ex. inte använda våld eller besluta om tvångsmedel. Han eller hon får dock verkställa beslut om beslag, om det kan ske utan våld, och även medverka aktivt vid husrannsakan.

När en skattebrottsenhet biträder åklagaren i en förundersökning, deltar ofta polismän eller tulltjänstemän i utredningsarbetet samtidigt. I sådana fall är det angeläget att det finns en möjlighet att på ett enkelt sätt utbyta information mellan utredningsmännen. Det är också viktigt att det finns goda möjligheter

till utbyte av underrättelseinformation mellan skattebrottsenheterna och dem som svarar för underrättelseverksamhet vid de andra brottsbekämpande myndigheterna.

Eftersom Skatteverkets personal inte ingriper mot pågående brott på samma sätt som tjänstemän från Tullverket och Kustbevakningen, får Skatteverkets behov av direktåtkomst till uppgifter inom polisen allmänt sett anses vara mindre än de andra myndigheternas. Ett behov av direktåtkomst kan likväl konstateras.

#### *Direktåtkomst till DurTvå*

Datoriserad utredningsrutin (DurTvå) är ett datasystem där förundersökningar lagras. En närmare beskrivning av systemet finns i *bilaga 6*. Varje polismyndighet har ett eget sådant system. De anställda vid polismyndigheten som har behov av uppgifter i systemet har tillgång till det. Åtkomsten är dock indelad i olika behörighetsnivåer. Det går även att medge direktåtkomst till anställda vid någon annan polismyndighet eller vid Rikspolisstyrelsen, om det finns behov av det. Det kan behövas t.ex. om anställda vid flera polismyndigheter arbetar tillsammans i samma förundersökning. Åklagare, som i sin egenskap av förundersökningsledare har mycket stort behov av tillgång till uppgifterna i sina förundersökningar, har ännu inte någon direktåtkomst till sådana uppgifter i DurTvå. Polisen arbetar emellertid med att ta fram en teknisk lösning som medger att sådan åtkomst kan beviljas. I de fall där tjänstemän från Tullverket, Kustbevakningen eller Skatteverket arbetar tillsammans med polismän i en förundersökning har tjänstemännen från de andra myndigheterna behov av att kunna få tillgång till sådana uppgifter som lagrats i DurTvå.

*Direktåtkomst till DNA-register*

Statens kriminaltekniska laboratorium, polismyndigheter och åklagare kan för närvarande medges direktåtkomst till register över resultatet av DNA-analyser. Åtkomsten för polismyndigheter och åklagare är dock begränsad till uppgifter om huruvida en person förekommer i något av registren eller inte.

Lagstiftningen om DNA-register har ganska nyligen ändrats (se prop. 2005/06:29). Det är i dag svårt att överblicka hur omfattande registren kommer att bli när den nya lagstiftningen har fått full effekt. Mot den bakgrunden bör man avvakta med att göra några omfattande förändringar i fråga om direktåtkomsten till DNA-register. De myndigheter som redan har direktåtkomst till DNA-register torde även fortsättningsvis ha samma behov av direktåtkomst som i dag. Däremot bör övriga brottsbekämpande myndigheters behov av uppgifter ur registret kunna tillgodoses utan att myndigheterna medges direktåtkomst.

*Direktåtkomst till fingeravtrycksregistret samt signalements- och känneteckensregistret*

Förutom Statens kriminaltekniska laboratorium har hittills bara de största polismyndigheterna getts direktåtkomst till fingeravtrycksregistret, trots att 5 § polisdataförordningen ger utrymme för att ge alla polismyndigheter sådan åtkomst. Detta beror på att endast de största polismyndigheterna anses ha utrustning för och kompetens att jämföra fingeravtryck med spår av fingeravtryck. Rikspolisstyrelsen förbereder emellertid en ändring av befintliga system så att det blir möjligt för alla polismyndigheter att sända fingeravtryck via dator till registret och i samband därmed även kontrollera om personen förekommer i registret. Redan nu har polismyndigheterna via befintliga datorsystem möjlighet att få svar på frågor om när ett fingeravtryck togs och vilken kvalitet det har. Sådana uppgifter behövs för att polisen ska kunna bedöma om nytt fingeravtryck ska tas.

För närvarande har alla polismyndigheter och Tullverket samt polismän vid Ekobrottsmyndigheten direktåtkomst till signalements- och känneteckensregistret.

De myndigheter som i framtiden kan behöva ha direktåtkomst till uppgifter i fingeravtrycks- eller signalementsregister är, förutom de myndigheter som redan i dag har sådan åtkomst, framför allt Kustbevakningen. Myndigheten har, i likhet med Tullverket och polismyndigheterna, behov av att kunna få tillgång till uppgifter dygnet runt och detta behov tillgodoses enklast genom möjlighet till direktåtkomst. Åklagarväsendet och Skatteverket har också visst behov av tillgång till uppgifter ur registren, även om det inte är lika påtagligt.

### 12.3.5 Direktåtkomst för övriga brottsbekämpande myndigheter

**Promemorians förslag:** Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket ska i den brottsbekämpande verksamheten kunna medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Till register med uppgifter om DNA-analyser ska endast Statens kriminaltekniska laboratorium, polismyndigheter, Ekobrottsmyndigheten och Åklagarmyndigheten kunna medges direktåtkomst.

Till fingeravtrycks- och signalementsregister ska polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket kunna medges direktåtkomst.

Säkerhetspolisen ska kunna medges direktåtkomst i samma utsträckning som gäller för Rikspolisstyrelsen i övrigt och för polismyndigheterna.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

**Promemorians bedömning:** Det bör inte vara möjligt att medge direktåtkomst till uppgifter som behandlas hos Säkerhetspolisen eller till uppgifter i penningtvättsregister.

**Utredningens förslag:** Utredningen har föreslagit att polismyndigheter ska få ha direktåtkomst till det allmänna spaningsregistret och att Statens kriminaltekniska laboratorium, polismyndigheter och åklagarmyndigheter ska få ha direktåtkomst till register med DNA-analyser i brottmål. Vidare har utredningen föreslagit en allmän bestämmelse om att direktåtkomst till personuppgifter ska vara förbehållen de personer inom

polisen som på grund av sina arbetsuppgifter behöver tillgång till uppgifterna.

**Remissinstanserna:** Flera myndigheter, bl.a. *Riksåklagaren*, *Riksskatteverket*, *Tullverket* och *Kustbevakningen*, har ansett att de bör kunna medges direktåtkomst till uppgifter som behandlas i polisens brottsbekämpande verksamhet.

### Skälen för promemorians förslag och bedömning

*Bör övriga brottsbekämpande myndigheter kunna medges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet?*

Vi har ovan kunnat konstatera att de brottsbekämpande myndigheterna ofta har ett påtagligt behov av att få direktåtkomst till den information som andra brottsbekämpande myndigheter behandlar. En möjlighet till direktåtkomst skapar bättre förutsättningar för ett framgångsrikt brottsbekämpande arbete. För en sådan möjlighet talar också kostnads- och säkerhetsskäl. Det är inte kostnadseffektivt att myndigheter avsätter resurser för att manuellt administrera ett informationsutbyte när behovet av ett sådant utbyte kan konstateras redan på förhand. Utlämnande på annat sätt än genom direktåtkomst, exempelvis via fax eller e-post, innebär också allmänt sett ett mindre säkert överförande av uppgifter, eftersom obehöriga då lättare kan få tillgång till dem.

Mot det nu sagda måste dock integritetsskyddsintresset vägas. Integritetsaspekterna måste tillmätas en central betydelse vid bedömningen av i vilken omfattning myndigheter bör kunna medges direktåtkomst till varandras register och databaser. I de databaser och register som förs av brottsbekämpande myndigheter finns det ofta stora mängder personuppgifter. Många av dessa kan vara av känslig karaktär. För den enskilde kan enbart det förhållandet att omfattande uppgifter om hans eller hennes förhållanden samlas in och bevaras uppfattas som ett intrång i den personliga integriteten. Ju fler personer som har omedelbar tillgång till sådana uppgiftssamlingar, desto mera påtagligt torde

intrånget uppfattas av den enskilde. Direktåtkomst kan också minska den personuppgiftsansvariga myndighetens möjligheter att kontrollera den vidare användningen av uppgifterna. Dessa förhållanden utgör i sig skäl för en restriktiv hållning i fråga om direktåtkomst till uppgifter som polisen behandlar.

En viktig aspekt vid den avvägning som här måste göras är sekretesskyddet för uppgifterna hos den mottagande myndigheten. Om sekretesskyddet hos den mottagande myndigheten är lika långtgående som sekretesskyddet hos den utlämnande myndigheten, behöver ett utlämnande av uppgifterna genom direktåtkomst inte innebära någon ökning av integritetsriskerna i förhållande till allmänheten. En annan viktig aspekt är hur uppgifterna sprids och används inom den mottagande myndigheten. Om användandet av uppgifterna inom den mottagande myndigheten kan begränsas till en liten krets personer, innebär detta givetvis mindre integritetsrisker än om uppgifterna ges en vid spridning. En tredje betydelsefull aspekt är vilka bestämmelser om informationssäkerhet (exempelvis system för behörighet, loggning och tillsyn) som gäller hos den mottagande myndigheten. Om det finns en hög informationssäkerhet hos den mottagande myndigheten, så att det kan garanteras att informationen når endast dem som har rätt till den, inger naturligtvis system för direktåtkomst mindre betänkligheter från integritetssynpunkt än vad som annars hade varit fallet.

Vad först gäller sekretessregleringen kan det konstateras att denna i princip ger samma skydd för uppgifter i brottsbekämpningen hos samtliga brottsbekämpande myndigheter. Myndigheterna omfattas av således av bl.a. skyddet i 5 kap. 1 § och 9 kap. 17 § sekretesslagen (se avsnitt 13.2). De brottsbekämpande myndigheterna har även författningar som reglerar personuppgiftsbehandlingen på ett likartat sätt. Som nyss har nämnts pågår det inom EU förhandlingar om ett rambeslut med särskilda data-skyddsbestämmelser. När rambeslutet genomförs, kommer ett än mer likartat skydd att uppnås.

Vad sedan gäller tillgången till uppgifterna hos den mottagande myndigheterna vill vi erinra om den bestämmelse, som vi har



föreslagit i avsnitt 6.7, att en enskild tjänsteman ska ges tillgång endast till sådana uppgifter som han eller hon behöver för att kunna fullgöra sina arbetsuppgifter på ett ändamålsenligt sätt. En möjlighet till direktåtkomst kommer alltså inte att innebära att annat än en begränsad krets av tjänstemän – eller enbart en viss tjänsteman – hos den mottagande myndigheten får tillgång till uppgifterna. Givetvis bör, om en möjlighet till direktåtkomst skapas, det tekniska systemet för direktåtkomst utformas så att den enskilde tjänstemannens möjligheter till sådan åtkomst begränsas i motsvarande utsträckning.

Vad slutligen gäller informationssäkerhet i samband med direktåtkomst anser vi att regeringen eller den myndighet som regeringen bestämmer bör få meddela särskilda föreskrifter om detta. Om de brottsbekämpande myndigheterna ska ges möjlighet till direktåtkomst till varandras uppgifter, bör den myndighet som beslutar om sådan åtkomst således vara skyldig att försäkra sig om att den mottagande myndigheten har en acceptabel säkerhetsnivå, exempelvis vad gäller system för utlämnande av behörighet, för tillsyn och för loggning av transaktioner. Det kan i sammanhanget noteras att den tekniska utvecklingen fort-löpande ger bättre möjligheter att begränsa åtkomsten till olika uppgifter och att i efterhand genom bl.a. loggningsuppgifter kontrollera hur åtkomsten har utnyttjats. Ett av syftena med den nya tekniska struktur för lagring av personuppgifter som planeras av polisen är att göra det lättare att begränsa åtkomsten på detta sätt.

De ökade integritetsrisker som en möjlighet till direktåtkomst kan medföra kan alltså motverkas genom bestämmelser av annat slag, såsom bestämmelser om sekretess, om tillgång till uppgifter och om informationssäkerhet. Övervägande skäl talar därför för att den nya lagen bör tillåta att övriga brottsbekämpande myndigheter ges direktåtkomst till de personuppgifter som behandlas i polisens brottsbekämpande verksamhet. De närmare förutsättningarna för sådan direktåtkomst diskuteras i det följande.

*Direktåtkomst till uppgifter hos Säkerhetspolisen och till vissa särskilda register*

Som tidigare har angetts bör vissa register undantas från den nya lagens tillämpningsområde, bl.a. belastningsregistret och misstankeregistret. De lagar som reglerar dessa register innehåller särskilda bestämmelser om direktåtkomst. Frågan om direktåtkomst till de registren bör därför inte regleras i den nya lagen.

Eftersom Säkerhetspolisen behandlar särskilt känsliga uppgifter, bör det överhuvudtaget inte vara möjligt att medge direktåtkomst till uppgifter som behandlas där. Endast Säkerhetspolisens egna tjänstemän bör kunna ges direkt tillgång till uppgifterna.

I *bilaga 6* beskrivs Finanspolisens register, som i stor utsträckning innehåller underrättelseinformation. Denna underrättelseinformation är till sin natur sådan att det är viktigt att tillgången till den begränsas till ett fåtal personer. Det är fråga om känslig ekonomisk information, vilken i dag inte är åtkomlig för andra delar av polisorganisationen. Av samma skäl som direktåtkomst inte bör kunna ges till de uppgifter som Säkerhetspolisen behandlar, bör direktåtkomst inte heller kunna medges till uppgifter som behandlas med anledning av misstänkt penningtvätt eller misstänkt finansiering av särskilt allvarlig brottslighet.

När det gäller de register som innehåller resultatet av DNA-analyser (DNA-register, utredningsregister och spårregister) finns det knappast något behov av att kunna medge direktåtkomst till andra myndigheter än de som redan i dag har rätt till sådan åtkomst, dvs. polismyndigheterna, Ekobrottsmyndigheten, Åklagarmyndigheten samt Statens kriminaltekniska laboratorium (se 11 § polisdataförordningen). För polismyndigheter och åklagarmyndigheter bör åtkomsten, på samma sätt som i dag, begränsas till uppgifter om huruvida en person förekommer i registret eller inte. Regeringen bör meddela föreskrifter om en sådan begränsning. Säkerhetspolisen bör, när den utför uppgifter

som polismyndighet, ha samma möjlighet att få tillgång till uppgifterna i fråga som andra polismyndigheter.

Uppgifterna i fingeravtrycks- och signalementsregister är inte lika känsliga som uppgifter om DNA. Behovet av att snabbt kunna få tillgång till sådana uppgifter, för att kunna avgöra en persons identitet, är dessutom större. Samtliga brottsbekämpande myndigheter, med undantag för åklagare, bör därför kunna medges direktåtkomst till personuppgifter i fingeravtrycks- och signalementsregister.

#### *Hur bör direktåtkomsten till polisens uppgifter avgränsas?*

En första förutsättning för att en myndighet ska kunna ges direktåtkomst till uppgifter hos en annan myndighet bör vara att uppgifterna är gemensamt tillgängliga hos den senare myndigheten. Därmed kommer de särskilda bestämmelser som gäller vid behandling av gemensamt tillgängliga uppgifter att få genomslag vid utnyttjandet av direktåtkomsten, t.ex. vad gäller särskilda upplysningar och sökbegränsningar.

Ytterligare en förutsättning för att direktåtkomst ska kunna medges bör vara att den myndighet som beslutar om sådan åtkomst försäkras om att den mottagande myndigheten har en acceptabel säkerhetsnivå, exempelvis vad gäller system för utlämnande av behörighet, tillsyn och för loggning av transaktioner.

En annan förutsättning bör vara att en enskild tjänsteman ska få ha direktåtkomst endast till sådana uppgifter som han eller hon behöver för att kunna fullgöra sina arbetsuppgifter på ett ändamålsenligt sätt. Frågor av detta slag regleras lämpligen i förordning eller myndighetsföreskrifter.

Det kan diskuteras om det inte bör införas ytterligare begränsningar i möjligheten till direktåtkomst.

Det skulle t.ex. vara möjligt att införa bestämmelser som innebär att direktåtkomst får medges endast till vissa särskilda register eller uppgiftssamlingar. Vi bedömer dock inte att detta

är någon framkomlig väg. Förslaget till ny reglering bygger ju på att man i möjligaste mån ska frångå registerbegreppet och göra regleringen teknikneutral. En annan sak är att om ett visst register särregleras, så bör också frågan om direktåtkomst till detta register kunna särregleras.

En annan i och för sig tänkbar begränsning är att tillåta direktåtkomst enbart till en viss brottstyp eller en viss typ av ärenden. Eftersom brottslingar inte sällan ägnar sig åt olika typer av brottslighet, t.ex. både förmögenhetsbrott och våldsbrott eller både ekonomisk brottslighet och narkotikasmuggling, är det dock inte lämpligt att i författning avgränsa åtkomsten på detta sätt. En tjänsteman vid Tullverket som handlägger ett underrättelseärende om misstänkt narkotikabrottslighet kan ha ett befoगत intresse av att söka efter kopplingar till någon annan typ av brottslighet. Visserligen skulle några typer av brottslighet sannolikt kunna undantas, exempelvis sexualbrott som ytterst sällan kan ha intresse för andra brottsbekämpande myndigheter. En sådan avgränsning skulle dock lätt kunna bli slumpartad. Dessutom skulle man förmodligen bara kunna undanta ett fåtal brottstyper med en sådan avgränsning och den skulle därför inte innebära någon större vinst från integritetssynpunkt. Däremot är det givetvis inget som hindrar att den registeransvariga myndigheten, när den medger direktåtkomst, gör en mer detaljerad avgränsning, t.ex. genom att bevilja åtkomst bara till uppgifter om vissa typer av brott eller till uppgift om huruvida en person förekommer i en databas.

En annan möjlig begränsning skulle kunna ta sikte på det ändamål för vilket uppgifterna behandlas. En sådan avgränsning görs i 6–8 §§ förordningen (2005:791) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. Begränsningen innebär bl.a. att Åklagarmyndigheten inte kan medges direktåtkomst till uppgifter som behandlas för ändamålet förhindra eller upptäcka brottslig verksamhet. I sitt remissvar över Polisdatautredningens betänkande har Riksåklagaren betonat vikten av ett nära och effektivt samarbete mellan polis och åklagare vid bekämpning av internationell, gränsöverskridande och

organiserad brottslighet. Enligt Riksåklagaren måste åklagare därför ha möjlighet att ha direktåtkomst till personuppgifter som har betydelse för lagföringen av den allvarliga brottsligheten, alltså även uppgifter som behandlas för att förebygga, förhindra och upptäcka brottslig verksamhet. Vi anser att det finns fog för Riksåklagarens uppfattning och att den också är relevant vad gäller övriga brottsbekämpande myndigheter.

Sammantaget är det varken önskvärt eller möjligt att i den nya lagen uppställa andra begränsningar vad gäller de brottsbekämpande myndigheternas direktåtkomst än de behörighets- och behovsbegränsningar som vi har angett ovan. Vi återkommer i avsnitt 13 till frågan om sekretess hindrar direktåtkomst.

### 12.3.6 Direktåtkomst för utländska myndigheter

**Promemorians förslag:** Regeringen får meddela föreskrifter om att utländska myndigheter får medges direktåtkomst till uppgifter i polisens brottsbekämpande verksamhet, om det är nödvändigt för att kunna fullgöra förpliktelser som följer av en internationell överenskommelse som har godkänts av riksdagen. Åtkomsten till uppgifter i DNA-register, utredningsregister och spårregister samt fingeravtrycks- och signalementsregister ska begränsas till uppgift om huruvida någon förekommer i registret eller inte.

**Utredningen** har inte behandlat frågan.

**Remissinstanserna** har inte heller yttrat sig i saken.

**Skälen för promemorians förslag:** Numera finns så gott som all polisiär informationen på medium för automatiserad behandling. Det aktualiserar frågan om elektronisk informationsöverföring till andra länder. Frågan har särskild betydelse i det allt viktigare internationella polissamarbetet. I juni 2007 nåddes en politisk överenskommelse inom EU om ett rambeslut, som bygger på det s.k. Prümfördraget. Beslutet innehåller bestämmelser

om ett fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism, gränsöverskridande brottslighet och olaglig migration. En av de frågor som tas upp är direktåtkomst till vissa uppgifter i nationella polisregister. Rambeslutet behandlas ovan i avsnitt 4.4.

Den nya lagen bör ge utrymme för regeringen att meddela föreskrifter om direktåtkomst till vissa uppgifter i polisens register, om det finns ett folkrättsligt bindande åtagande att medge sådan åtkomst. Av de skäl som utvecklas närmare i avsnitt 13.3 bör bemyndigandet enbart omfatta överenskommelser som riksdagen har godkänt.

I avsnitt 14 behandlas frågan om uppgifter ska kunna lämnas ut till en utländsk mottagare på medium för automatiserad behandling på annat sätt än genom direktåtkomst.

## 13 Sekretess och uppgiftsskyldighet m.m.

### 13.1 Allmänna utgångspunkter

**Promemorians bedömning:** Det krävs sekretessbrytande regler för att skapa förutsättningar för en myndighet att medge andra brottsbekämpande myndigheter direktåtkomst.

**Utredningens förslag:** Utredningen har föreslagit en sekretessbrytande regel som medger att uppgifter som behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet och uppgifter ur det allmänna spaningsregistret i vissa fall får lämnas ut till övriga brottsbekämpande myndigheter. Utredningen har i övrigt inte diskuterat frågan.

**Remissinstanserna** har inte haft någon invändning mot utredningens förslag. Flera remissinstanser, däribland Riksåklagaren, Riksskatteverket, Tullverket och Kustbevakningen, har dock ifrågasatt varför inte utredningen i större utsträckning har beaktat behovet av informationsutbyte mellan brottsbekämpande myndigheter.

## Skälen för promemorians bedömning

### *Sekretess mellan brottsbekämpande myndigheter*

Ansvar för brottsbekämpningen i Sverige är, som redan har framgått, organisatoriskt uppdelat mellan flera myndigheter. Gemensamt för dessa myndigheter är att sekretess i större eller mindre utsträckning gäller för flertalet av de personuppgifter som behandlas inom ramen för den brottsbekämpande verksamheten. När uppgifter ska lämnas mellan myndigheterna måste därför hänsyn tas till bl.a. sekretesslagstiftningen.

Det finns ett antal bestämmelser i sekretesslagen som möjliggör utbyte av uppgifter mellan myndigheter utan hinder av sekretess. Av 1 kap. 5 § sekretesslagen (1980:100) framgår att sekretessbelagda uppgifter får lämnas från en myndighet till en annan om det är nödvändigt för att den *utlämnande* myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen, som är avsedd att tillämpas restriktivt, medger således inte sekretessgenombrott på den grunden att den *mottagande* myndigheten behöver uppgifterna i sin verksamhet. Ytterligare sekretessbrytande bestämmelser finns i 14 kap. sekretesslagen. I 14 kap. 1 § föreskrivs bl.a. att sekretess inte hindrar ett utlämnande till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Uppgifter kan vidare, med vissa undantag, lämnas ut med stöd av 14 kap. 2 § när uppgifterna behövs i bl.a. förundersökningar. Enligt 14 kap. 3 § första stycket, den s.k. generalklausulen, gäller som huvudregel att uppgifter får lämnas ut till en annan myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Bedömningen av om uppgiften kan lämnas ut görs av den myndighet som innehar uppgiften, utom i de fall där utlämnandebestämmelsen har konstruerats så att uppgiften alltid ska lämnas ut om det begärs.

Av stor betydelse i sammanhanget är vidare bestämmelsen i 15 kap. 5 §, som innebär att en myndighet på begäran av en annan myndighet ska lämna ut uppgifter i den mån hinder inte



möter på grund av sekretess eller arbetets behöriga gång. Det innebär att om en myndighet begär att få del av uppgifter från en annan myndighet och någon av de ovan nämnda sekretessbrytande bestämmelserna är tillämplig, så ska uppgifterna lämnas ut. Detsamma gäller givetvis om de begärda uppgifterna är offentliga.

Ytterligare en bestämmelse av betydelse i sammanhanget finns i 9 kap. 17 § sjätte stycket 3 sekretesslagen. Där föreskrivs att en uppgift, utan hinder av sekretessen i 9 kap. 17 §, får lämnas ut enligt vad som föreskrivs i bl.a. polisdatalagen och i förordningar som meddelats med stöd av den lagen. Bestämmelsen infördes i samband med att den absoluta sekretessen för polisregister avskaffades (se prop. 1997/98:97). Syftet med bestämmelsen var bl.a. att myndigheterna inte skulle behöva förlita sig på en sekretessprövning i de fall där det i författning anges att uppgifter får lämnas ut. I 6–8 §§ polisdatalagen finns bestämmelser om att uppgifter får lämnas ut. Sådana bestämmelser finns även i polisdataförordningen, se bl.a. 8, 10, 17, 17 a och 18 §§.

Frågan om informationsutbyte och sekretess har behandlats bl.a. vid översyn av de registerförfattningar som gäller för andra brottsbekämpande myndigheter. Det senaste ställningstagandet gällde personuppgiftsbehandlingen i Tullverkets brottsbekämpning. I prop. 2004/05:164 (s. 84–88) analyserades vilken sekretess som gäller vid informationsutbyte mellan myndigheter i brottsutredningar respektive i underrättelseverksamhet. I propositionen gjordes bedömningen att en möjlighet för Tullverket att lämna ut uppgifter till övriga brottsbekämpande myndigheter genom direktåtkomst förutsatte att det infördes en sekretessbrytande uppgiftsskyldighet i förhållande till övriga myndigheter. Därför infördes en sådan sekretessbrytande bestämmelse i 2 § förordningen (2005:791) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

I betänkandet Kustbevakningens personuppgiftsbehandling (SOU 2006:18) har samma bedömning gjorts avseende Kustbevakningens möjlighet att lämna ut uppgifter.

Beredningen för rättsväsendets utveckling har i betänkandet Ett effektivare brottmålsförfarande – några ytterligare åtgärder (SOU 2005:117) föreslagit att sekretessen i 9 kap. 17 § sekretesslagen till skydd för enskilda inte ska gälla vid informationsutbyte mellan de brottsbekämpande myndigheterna. I betänkandet sägs att dessa myndigheter anser att den nuvarande regleringen inte är tillräckligt långtgående för att täcka det behov som myndigheterna har av att utbyta information med varandra (se s. 152 f.). Betänkandet bereds för närvarande inom Regeringskansliet (Justitiedepartementet).

#### *Förhållandet mellan direktåtkomst och sekretess*

En bestämmelse om direktåtkomst reglerar endast tillåtligheten av ett visst tillvägagångssätt för utlämnande av personuppgifter. En sådan bestämmelse har alltså inte någon självständig sekretessbrytande effekt; den är inte att se som en uppgiftsskyldighet enligt 14 kap. 1 § andra meningen sekretesslagen (se bl.a. prop. 2004/05:164 s. 83 och 2006/07:46 s. 80). Möjligheterna för t.ex. en myndighet att vid informationsutbyte med en annan myndighet överföra uppgifter genom att medge den myndigheten direktåtkomst till uppgifter som behandlas automatiserat begränsas därför inte sällan av bestämmelser i sekretesslagen.

Eftersom direktåtkomst innebär att den mottagande myndigheten fritt kan avgöra vilka uppgifter – inom ramen för den beviljade direktåtkomsten – den vill ta del av, blir uppgifterna att anse som utlämnade i och med att direktåtkomst lämnas. Det spelar i det avseendet ingen roll om den mottagande myndigheten faktiskt tar del av en viss uppgift eller inte. En förutsättning för att direktåtkomst ska kunna medges är således att åtkomsten endast avser antingen offentliga uppgifter eller uppgifter som får lämnas ut till mottagaren med stöd av någon sekretessbrytande bestämmelse.

Den dåvarande regeringen gjorde bl.a. i prop. 2004/05:164 såvitt gäller Tullverket den bedömningen att det krävs en tydlig

sekretessbrytande reglering för att en myndighet utan risk för problem från sekretessynpunkt ska kunna medge andra brottsbekämpande myndigheter direktåtkomst, om direktåtkomsten ska avse annat än uppgifter som inte omfattas av sekretess. Denna bedömning har bärkraft även såvitt gäller uppgiftslämnande från polismyndigheterna. Det är därför nödvändigt att införa en sekretessbrytande regel i den nya lagen.

## 13.2 Sekretessgenombrott

**Promemorians förslag:** Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen ska uppgifter som har gjorts gemensamt tillgängliga hos den öppna polisen och uppgifter i fingeravtrycks- eller signalementsregister kunna lämnas till Rikspolisstyrelsen, polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen eller Skatteverket, om myndigheten behöver uppgiften i sin brottsbekämpande verksamhet.

Uppgift om huruvida någon förekommer i register med uppgifter om DNA-analyser ska dock under samma förutsättningar lämnas ut endast till polis- och åklagarmyndigheter.

Bestämmelserna om sekretessgenombrott gäller även i förhållande till Säkerhetspolisen.

Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Regeringen meddelar föreskrifter om uppgiftslämnande för andra ändamål.

**Utredningens förslag:** Utredningen har föreslagit att uppgifter som behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet och uppgifter ur det allmänna spaningsregistret ska få lämnas ut till övriga brottsbekämpande myndighe-

ter, men endast om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder (se 3 och 4 §§ förslaget till förordning, SOU 2001:92, s. 209).

**Remissinstanserna** har inte haft någon invändning mot utredningens förslag.

### Skälen för promemorians förslag

#### *Sekretessgenombrott mellan de brottsbekämpande myndigheterna*

För att skapa rättsliga förutsättningar för att polisens ska kunna medge direktåtkomst till uppgifter som gjorts gemensamt tillgängliga i dess brottsbekämpande verksamhet krävs, som nyss nämnts, att en sekretessbrytande regel införs. Frågan är då hur denna regel bör utformas.

Utredningens förslag tar enbart sikte på utlämnande av en viss typ av information, underrättelseinformation, och täcker således bara en del av behovet av informationsutbyte. Vidare ska sådan information enligt utredningens förslag bara kunna utbytas när den mottagande myndigheten själv har en pågående undersökning, dvs. bedriver viss underrättelseverksamhet, och dessutom krävs det att uppgiften kan antas ha betydelse för den undersökningen. Detta innebär sammantaget att förslaget ger alltför begränsat utrymme för informationsutbyte i underrättelseverksamheten och inget utrymme alls när det gäller andra viktiga delar av brottsbekämpningen, exempelvis brottsutredning. Förslaget kan därför inte läggas till grund för lagstiftningsarbetet.

Beredningen för rättsväsendets utveckling har i betänkandet SOU 2005:117 föreslagit att sekretessen enligt 9 kap. 17 § sekretesslagen inte ska gälla mellan åklagarmyndigheter, polismyndigheter, Tullverket, Kustbevakningen och Skatteverket. Bestämmelsen, som har utformats som en ovillkorlig rätt för nämnda myndigheter att ta del av uppgifter hos varandra, har

under remissbehandlingen fått viss kritik av bl.a. Datainspektionen för de konsekvenser som den riskerar att få från integritets-synpunkt. Den har också kritiserats av Integritetsskyddskommittén för bristen på intresseavvägning. De brottsbekämpande myndigheterna har varit positiva till förslaget som sådant, men flera har haft invändningar mot den lagtekniska utformningen. Inte heller det förslaget bör därför läggas till grund för den nya regleringen.

Det ligger i sakens natur att en sekretessbrytande bestämmelse som ska möjliggöra direktåtkomst mellan brottsbekämpande myndigheter måste vara generellt utformad, eftersom det vid direktåtkomst saknas möjlighet att göra en sekretessprövning i varje enskilt fall. Prövningen måste i stället göras i förväg. Med hänsyn till intresset av ett gott skydd för den personliga integriteten kan det emellertid ifrågasättas om ett fullständigt sekretessgenombrott mellan de brottsbekämpande myndigheterna kan accepteras. Även om sekretessen består gentemot allmänheten och effektivitetsaspekterna väger tungt, finns det anledning att överväga om inte någon form av begränsning i den sekretessbrytande bestämmelsen bör göras.

Enligt 14 kap. 1 § sekretesslagen utgör sekretess inte hinder mot att uppgift lämnas med stöd av en uppgiftsskyldighet i lag eller förordning. En bestämmelse, som innebär att uppgifter som gjorts gemensamt tillgängliga hos polisen under en eller flera angivna förutsättningar ska lämnas till olika verksamhetsgrenar inom polisen och till övriga brottsbekämpande myndigheter, har således sekretessbrytande effekt enligt den nämnda bestämmelsen.

Eftersom uppgifter som omfattas av sekretess till skydd för enskilda kan vara mycket integritetskänsliga, är det viktigt att andra enheter inom polisen och andra brottsbekämpande myndigheter får tillgång till sådana uppgifter bara när de har behov av det för att kunna bedriva den brottsbekämpande verksamhet som de är ålagda enligt lag eller annan författning. Enligt vår bedömning bör just detta behov kunna utgöra det rekvisit som begränsar den sekretessbrytande bestämmelsen.

Eftersom den sekretessbrytande bestämmelsen ska möjliggöra direktåtkomst, måste sekretessprövningen göras innan direktåtkomsten beviljas. Sekretessprövningen kan därför inte vara alltför komplicerad. Den sekretessbrytande regeln måste således tillåta ett relativt brett sekretessgenombrott men i gengäld kommer den, som utvecklas närmare i det följande, att kompletteras med andra integritetsskyddande bestämmelser. Det sekretessgenombrott som föreslås i den nya lagen bör mot denna bakgrund endast vara villkorat av ett behovsrekvisit.

Då den föreslagna regeln har det uttryckliga syftet att tillåta frekvent utlämnande bör behovsbedömningen kunna göras inom tämligen vida ramar. Bedömningen av vad mottagaren har behov av får i ett sådant fall göras främst utifrån myndighetens brottsbekämpande uppgifter och med utgångspunkt i de behov som typiskt sett föreligger. Personuppgifter som en myndighet typiskt sett inte har behov av bör alltså inte vara åtkomliga. Exempelvis får Skatteverkets brottsenheter typiskt sett anses ha behov av att få tillgång till uppgifter som rör ekonomisk brottslighet och andra brott som kan ha anknytning till sådan brottslighet (framför allt förmögenhetsbrott och vissa specialstraffrättsliga brott), medan dessa enheter mycket sällan torde ha behov av att ta del av uppgifter i t.ex. förundersökningar om brott mot person, brott mot allmänheten eller miljöbrott. När det gäller Tullverket kan myndigheten typiskt sett antas ha behov av bl.a. uppgifter om brott som rör varor som är förbjudna att föra in eller ut ur landet exempelvis narkotika, dopningsmedel och vissa typer av vapen. Detsamma gäller uppgifter om brott som rör ekonomisk brottslighet och andra brott med anknytning till sådana brott (jfr vad som sagts angående Skatteverkets behov). För Åklagarmyndighetens del kan en avgränsning inte bygga på brottstyper, eftersom åklagare har behov av alla typer av brottsutredningar. Där kan i stället t.ex. en avgränsning som begränsar tillgången till vissa typer av uppgifter vara tänkbar. Man kan t.ex. göra skillnad mellan uppgifter om brottsutredningar och andra uppgifter. Ekobrottsmyndighetens behov får bedömas med utgångspunkt i myndighetens verksamhetsområde, som är betyd-

ligt smalare än Åklagarmyndighetens. Eftersom Ekobrottsmyndigheten sysselsätter både polismän och åklagare, måste å andra sidan beaktas myndighetens behov av tillgång till uppgifter som typiskt sett det särskilda samarbetet kräver. När Säkerhetspolisen för Rikspolisstyrelsens räkning leder och bedriver polisverksamhet har myndigheten ställning som polismyndighet och har likartade behov som övriga polismyndigheter av att få del av uppgifter (se avsnitt 12.3.4). Utöver att leda polisverksamhet har Säkerhetspolisen andra åligganden. Ett sådant är att fullgöra de uppgifter som ankommer på Rikspolisstyrelsen enligt säkerhetskylldslagen (1996:627) och säkerhetskylldsförordningen (1996:633). Vilka personuppgifter som Säkerhetspolisen har behov av att kunna få del av för detta ändamål följer av nämnda författningar och kompletterande föreskrifter.

Utgångspunkten för den sekretessbrytande regeln bör alltså vara att den kan täcka de behov av information som andra brottsbekämpande myndigheter typiskt sett har. Det kan självfallet uppkomma situationer där en brottsbekämpande myndighet i ett enskilt fall har behov av uppgifter som ligger utanför det normala. Uppgifter av det slaget kan, på samma sätt som nu, lämnas ut efter en prövning i det enskilda fallet med stöd av andra sekretessbrytande bestämmelser, t.ex. 14 kap. 2 § sekretesslagen. Den nu föreslagna regeln är alltså inte avsedd att innebära någon ändring i detta avseende.

Mot bakgrund av dessa överväganden bör den sekretessbrytande bestämmelsen utformas så att uppgifter som har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet ska lämnas till annan polismyndighet, åklagarmyndighet, Tullverket, Kustbevakningen eller Skatteverket utan hinder av viss närmare angiven sekretess, om den myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet.

Sekretessbrytande regler kan ges såväl i lag som förordning. Mot bakgrund av polisverksamhetens särskilda natur bör andra myndigheters tillgång till uppgifter som behandlas av polisen regleras i lag. Den sekretessbrytande bestämmelsen bör därför

tas in i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

*Vilka sekretessbestämmelser ska den nya regleringen omfatta?*

Frågan är då vilka slag av sekretess som ska kunna brytas. Uppgifter hos polisen omfattas vanligen av sekretess till skydd för verksamheten enligt 5 kap. 1 § sekretesslagen. Sådan sekretess gäller nära nog undantagslöst för underrättelseuppgifter och, i större eller mindre utsträckning, för de flesta pågående förundersökningar och motsvarande utredningar enligt 23 kap. rättegångsbalken. Eftersom den bestämmelsen är tillämplig hos alla brottsbekämpande myndigheter, bör det normalt inte innebära någon skada för polisens verksamhet att lämna ut uppgifterna. Utgångspunkten är således redan enligt gällande rätt att uppgifter som omfattas av sekretess enligt 5 kap. 1 § sekretesslagen normalt kan lämnas ut till en annan brottsbekämpande myndighet. Detta förutsätter emellertid att det är möjligt att på förhand bedöma om en viss förundersökning eller motsvarande kan lämnas ut. En sådan bedömning bör kunna göras för olika brottstyper eller olika slags underrättelseprojekt.

På motsvarande sätt bör det redan enligt gällande bestämmelser vara möjligt att bedöma den risk som kan vara förknippad med att lämna ut uppgifter som är sekretessbelagda med stöd av någon annan bestämmelse i 5 kap. sekretesslagen. Vi återkommer till 5 kap. 7 § i det följande.

Något generellt behov av att bryta den sekretess som kan gälla inom polisen mellan olika verksamhetsgrenar och gentemot andra brottsbekämpande myndigheter enligt 5 kap. 1 § kan således inte anses föreligga. I de fall där utlämnandet av en uppgift till en annan brottsbekämpande myndighet skulle innebära att polisens egen verksamhet riskerar att skadas bör direktåtkomst givetvis inte komma ifråga. I sådana fall får, som nyss nämnts, i stället övervägas om uppgiften kan lämnas ut med stöd av någon



annan sekretessbrytande bestämmelse, exempelvis 1 kap. 5 § eller 14 kap. 2 § sekretesslagen.

Det bör i detta sammanhang påpekas att det i 5 kap. 7 § sekretesslagen, som reglerar sekretess till skydd för rättsligt samarbete på begäran av annan stat eller mellanfolklig organisation, föreskrivs att en uppgift utan hinder av sekretessen får lämnas ut om detta har stöd i en bestämmelse i polisdatalagen eller i lagen (2000:344) om Schengens informationssystem.

När det sedan gäller sekretess med hänsyn till skyddet för enskilds förhållanden kan följande anmärkas. När en brottsutredning inleds gäller, som nyss nämnts, normalt sekretess enligt både 5 kap. 1 § och 9 kap. 17 § sekretesslagen. Den förstnämnda sekretessen minskar efter hand och brukar normalt upphöra senast i samband med att åtal väcks. Sekretessen i enligt 9 kap. 17 § sekretesslagen skyddar enskilds personliga och ekonomiska förhållanden bl.a. vid förundersökning och annan brottsutredning. Sekretessen upphör normalt om uppgiften lämnas till domstol med anledning av åtal, men i en förundersökning förekommer det ofta uppgifter t.ex. om andra brott som den misstänkte har begått eller om personer som inte berörs av åtalet. För sådana uppgifter upphör sekretessen inte. Därför är det mycket vanligt att det förekommer kvarstående sekretess till skydd för enskild. Även 9 kap. 17 § sjätte stycket sekretesslagen innehåller en utlämnanderegeln som innebär att uppgifter, trots sekretessen, får lämnas ut om det har stöd i bestämmelser i polisdatalagen eller lagen om Schengens informationssystem.

Mot bakgrund av att de allra flesta pågående eller avslutade förundersökningar och flertalet uppgifter i underrättelseverksamhet kringgärdas av sekretess enligt 9 kap. 17 § sekretesslagen krävs det sekretessprövning i varje enskilt fall där en sådan uppgift ska lämnas till en annan brottsbekämpande myndighet. Även om uppgifterna kan lämnas ut efter en sådan prövning innebär det att tid och kraft måste läggas på en prövning som normalt alltid ger samma resultat.

Det skulle därför underlätta informationsutbytet mellan de brottsbekämpande myndigheterna väsentligt om uppgifter som

omfattas av sekretess enligt 9 kap. 17 § sekretesslagen kunde lämnas över från en myndighet till en annan, i de fall där den mottagande myndigheten typiskt sett har behov av uppgiften i fråga. En sådan reglering, som har förutsetts i paragrafens sjätte stycke, innebär visserligen att fler kan få tillgång till sekretessskyddade uppgifter av detta slag. Eftersom uppgifterna har samma skydd gentemot utomstående hos den mottagande myndigheten som hos den utlämnande myndigheten, får dock integritetsintränet godtas, särskilt med hänsyn till de vinster för brottsbekämpningen som ett förenklat informationsutbyte skulle innebära.

Det finns emellertid fler sekretessbestämmelser i 7 och 9 kap. sekretesslagen som kan aktualiseras vid informationsöverföring mellan de brottsbekämpande myndigheterna. Mot den bakgrunden bör det övervägas sekretessbrytande regler som tar sikte på några av de i detta sammanhang vanligaste sekretessreglerna i 7 och 9 kap. sekretesslagen.

Frågan är då vilka sekretessregler som en ny sekretessbrytande bestämmelse bör ta sikte på. Ett antal av sekretessbestämmelserna i 7 kap. sekretesslagen kan vara tillämpliga hos polisen. Det gäller bl.a. 7 kap. 1 och 1 a–b §§, 14 § första och andra styckena, 15 § tredje stycket samt 19, 32, 41 och 50 §§.

Det finns inget skäl att meddela generellt undantag för uppgifter som omfattas av sekretess enligt 7 kap. 1 § (sekretess för uppgift som rör enskilds hälsa och sexualliv) eftersom den bestämmelsen inte gäller om det finns en starkare sekretess (i detta fall 9 kap. 17 §) och det i 7 kap. 1 § tredje stycket föreskrivs att, om en bestämmelse i den paragraf som reglerar den strängare sekretessen innehåller en utlämnanderegeln, den ska gälla.

Sekretessen i 7 kap. 1 a § gäller för uppgift om enskilds bostadsadress, telefonnummer och andra jämförbara uppgifter som kan användas för att komma i kontakt med den enskilde, om det finns särskild anledning att anta att han eller hon, eller någon närstående, kan komma att utsättas för våld eller annat allvarligt men om uppgiften röjs. Sekretessen gäller s.k. skyddade adresser. En person kan ansöka hos Skatteverket om en s.k. sekretessmar-

kering. En sådan markering innebär inget beslut i sekretessfrågan, men utgör en varningssignal om att en särskilt noggrann sekretessprövning måste göras, om uppgifterna begärs utlämnade. Den är inte heller bindande för en mottagande myndighet, som ska göra en självständig prövning av sekretessfrågan.

Paragrafen skyddar således personer som anser sig ha stort behov av att uppgifter om deras uppehållsort inte röjs. Sekretess enligt denna paragraf är relativt vanlig i brottsutredningar. Ibland gäller sekretessen för brottsoffret och ibland till skydd för den misstänkte. Sekretess enligt 7 kap. 1 a § gäller hos alla myndigheter. Det innebär att en uppgift som lämnas till en annan brottsbekämpande myndighet har samma skydd gentemot allmänheten hos den mottagande myndigheten. Hos dessa myndigheter finns det vana vid att hantera denna sekretess. Sekretessen enligt denna paragraf viker dessutom för annan starkare sekretess, exempelvis sekretessen enligt 9 kap. 17 §. Mot den nu angivna bakgrunden bör uppgifter som omfattas av sekretess enligt 7 kap. 1 a § kunna lämnas vidare utan hinder av sekretessen i dessa paragrafer.

Sekretessen i 7 kap. 1 b § gäller för kopplingen mellan fingerade personuppgifter och den enskildes verkliga personuppgifter, om det inte står klart att uppgiften kan röjas utan att han eller hon eller någon närstående lider men. Medan sekretess enligt 7 kap. 1 a § är relativt vanlig i brottsutredningar, är antalet fall där sekretess skyddar fingerade personuppgifter betydligt färre. I sistnämnda fall föreligger det dessutom ett av flera myndigheter konstaterat mycket stort skyddsbehov för den enskilde. I samband med att sekretessbestämmelsen infördes framhöll den dåvarande regeringen att, med hänsyn till den allvarliga hotbild som krävs för att någon ska få fingerade personuppgifter, sekretessintresset väger tyngre än andra viktiga intressen. Behovet av skydd för den enskilde får därför anses väga över behovet av sekretessgenombrott i dessa fall. Den nu aktuella sekretessen bör således inte kunna brytas.

Sekretess enligt 7 kap. 14 § första och andra styckena sekretesslagen torde framför allt förekomma i ärenden som handläggs

av Säkerhetspolisen. Sekretessen i första stycket skyddar uppgifter som rör utlänning, om det kan antas att röjande av uppgiften kan medföra fara för att någon utsätts för övergrepp eller annat allvarligt men som föranleds av förhållandet mellan utlänningen och utländsk stat eller myndighet eller organisation av utlänningar. Sekretessen i andra stycket skyddar verksamhet för kontroll av utlänningar. Eftersom informationsutbytet ska avse den öppna polisens verksamhet, finns det inte tillräckliga skäl att göra undantag för sekretessen i den aktuella paragrafen.

Något undantag bör inte heller göras för sekretessen i 7 kap. 15 § tredje stycket sekretesslagen, som gäller för fingerade personuppgifter, om uppgiften har lämnats till polisen av folkbokföringsmyndigheten. Intresset av skydd för den enskilde väger, som nyss nämnts, i dessa fall tyngre än intresset av ett ökat informationsutbyte mellan de brottsbekämpande myndigheterna. Motsvarande bedömning görs när det gäller sekretess enligt 7 kap. 50 § sekretesslagen. Sistnämnda sekretess avser säkerhetsarbete till skydd för bl.a. hotade vittnen.

Ärenden där det finns sekretess enligt 7 kap. 19 § andra stycket (ärenden om besöksförbud) torde sällan vara av den arten att det finns något generellt intresse av att kunna föra informationen vidare till andra brottsbekämpande myndigheter. Något undantag för denna sekretess bör således inte heller göras.

När det så slutligen gäller sekretess enligt 7 kap. 41 § sekretesslagen innehåller den paragrafen redan en bestämmelse som gör det möjligt att i vissa fall lämna uppgifter vidare utan hinder av sekretessen. Sekretessen skyddar vissa uppgifter om enskild i framställningar som görs med stöd av 3 § lagen om Schengens informationssystem. Den sekretessbrytande regel som nu föreslås behöver därför inte omfatta sekretess enligt 7 kap. 41 § sekretesslagen.

Av sekretessreglerna i 9 kap. sekretesslagen bör den nya regeln endast omfatta sekretess enligt 9 kap. 17 §. I den mån andra sekretessbestämmelser i kapitlet är tillämpliga får det, på samma sätt som nu, göras en bedömning i det enskilda fallet av huruvida

sekretessen hindrar att uppgifterna lämnas ut till en annan brottsbekämpande myndighet.

Den nu föreslagna regleringen innebär alltså att ett sekretessgenombrott ska tillåtas i vissa fall. Bestämmelsen om utlämnande måste emellertid ses tillsammans med hur regelsystemet i övrigt har byggts upp. För det första får utlämnande bara avse uppgifter som har gjorts gemensamt tillgängliga. Detta innebär i sig en begränsning, eftersom en stor del av de uppgifter som polisen behandlar aldrig kommer att göras gemensamt tillgängliga. För behandlingen av gemensamt tillgängliga uppgifter ska (som framgår av bl.a. avsnitten 9 och 11) gälla särskilda begränsningar, vilket bl.a. innebär att bara vissa typer av uppgifter ska vara åtkomliga vid sökning. Vidare ska vissa typer av uppgifter markeras i syfte att det tydligt ska kunna utläsas dels om upplysningar rör en icke misstänkt person, dels kvaliteten på upplysningarna. Upplysningar som rör brottslig verksamhet ska förse med upplysning om källans tillförlitlighet och uppgifternas riktighet i sak. Om direktåtkomst beviljas, kommer dessutom tillgången till olika typer av uppgifter att begränsas genom behörighetsregler. När en uppgift blir åtkomlig för en tjänsteman vid en annan myndighet, kommer den myndighetens registerförfattningar – som i likhet med polisens innehåller regler som syftar till att minska risken för integritetsintrång – att bli tillämpliga. Vidare kommer den föreslagna regeln inte att genombryta alla de regler om sekretess som kan vara tillämpliga i polisens verksamhet. Den sekretessbrytande regeln måste också ses tillsammans med bestämmelserna i 2 kap. 4 § andra stycket och 10 §, som begränsar den enskilde tjänstemannens tillgång till uppgifter till vad just denne behöver för sin verksamhet. Sammantaget innebär förslaget att den sekretessbrytande regeln skapar förutsättningar för bättre informationsutbyte i brottsbekämpningen, men samtidigt beaktas risken för integritetsintrång.

Sammanfattningsvis bör således uppgifter kunna lämnas till en annan brottsbekämpande myndighet utan hinder av sekretess enligt 7 kap. 1 a § samt 9 kap 17 § sekretesslagen om den motta-

gande myndigheten har behov av uppgiften i sin brottsbekämpande verksamhet.

#### *Särskilt om vissa register*

DNA-register, fingeravtrycksregister samt signalements- och känneteckensregister särregleras i polisdatalagen. I avsnitt 17 redovisas skälen för en fortsatt särreglering. Vad som är av intresse i detta sammanhang är att vissa myndigheter redan har direktåtkomst till uppgifter i registren. Det aktualiserar frågan om man bör införa motsvarande regler om sekretessgenombrott som nyss föreslagits även för DNA-register, fingeravtrycksregister samt signalementsregister. Förekomsten av en regel om sekretessgenombrott underlättar för den registeransvariga myndigheten när den ska ta ställning till om en annan brottsbekämpande myndighet kan medges direktåtkomst till registren. Som utvecklas närmare i avsnitt 17 bör utgångspunkten för den nya regleringen vara att inte göra någon förändring i sak beträffande de aktuella registren. Det talar för att man bör införa regler om sekretessgenombrott även för uppgifter i dessa register.

#### *Uppgiftsskyldighet till statistikmyndighet m.m.*

I 6 § polisdatalagen föreskrivs att uppgifter som är nödvändiga för att framställa rättstatistiken ska lämnas till den myndighet som ansvarar för att framställa sådan statistik. Enligt förordningen (2001:100) om den officiella statistiken är det Brottsförebyggande rådet som är statistikansvarig myndighet. En bestämmelse om att uppgifter ska lämnas ut för statistikändamål bör finnas även i den nya lagen. Det kan anmärkas att enligt 9 kap. 4 § sekretesslagen gäller absolut sekretess för personuppgifter i verksamheten hos myndighet som framställer statistik.

Regeringen bör, på samma sätt som i dag, ha möjlighet att meddela föreskrifter om att uppgifter får lämnas ut även i andra fall.

### 13.3 Uppgiftslämnande till utlandet

**Promemorians förslag:** Personuppgifter ska få lämnas till en utländsk myndighet eller mellanfolklig organisation, om det följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Uppgifter ska vidare, om det är förenligt med svenska intressen, få lämnas

1. till en polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott, eller

2. till en utländsk underrättelse- eller säkerhetstjänst.

Regeringen kan meddela föreskrifter om uppgiftslämnande för andra ändamål eller till andra utländska mottagare.

**Utredningens förslag** överensstämmer i sak med förslaget.

**Remissinstanserna** har antingen ställt sig bakom eller inte kommenterat förslaget.

#### Skälen för promemorians förslag

##### *Möjligheterna att lämna ut uppgifter*

En utgångspunkt i sekretesslagen är att en uppgift som omfattas av sekretess inte får röjas för en utländsk myndighet eller mellanfolklig organisation. I 1 kap. 3 § tredje stycket sekretesslagen (1980:100) finns dock bestämmelser som innebär att en sekretesskyddad uppgift får röjas för en utländsk myndighet eller mellanfolklig organisation i två situationer. Den ena är när ut-

lämnandet sker i enlighet med en särskild föreskrift i lag eller författning. En uttrycklig bestämmelse om att uppgifter får lämnas till en utländsk myndighet eller organisation bryter alltså sekretess enligt 1 kap. 3 § tredje stycket sekretesslagen. Den andra är när uppgiften i motsvarande fall skulle få lämnas till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas. Den sistnämnda bestämmelsen är, som framgår av lydelsen, avsedd att tillämpas restriktivt.

I 1 kap. 5 § sekretesslagen föreskrivs att sekretess inte hindrar att en uppgift lämnas ut om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Enligt de knapphändiga förarbetena är denna sekretessbrytande bestämmelse avsedd att tillämpas restriktivt. Inom vissa myndighetsområden, som exempelvis polisens brottsbekämpande verksamhet, är det dock i ganska stor utsträckning nödvändigt att lämna ut sekretessbelagda uppgifter för att över huvud taget kunna genomföra exempelvis förhör. I ett internationellt perspektiv är ett typiskt exempel att svenska myndigheter i samband med begäran om rättslig hjälp i en förundersökning lämnar uppgifter som omfattas av sekretess enligt 5 kap. 1 § och 9 kap. 17 § sekretesslagen till en utländsk åklagar- eller polismyndighet i syfte att få ett visst förhör genomfört. Om det är nödvändigt för en myndighet att lämna ut sekretessbelagda uppgifter för att myndigheten ska kunna fullgöra sin egen verksamhet står det i regel klart att det är förenligt med svenska intressen att lämna uppgifterna. I det följande diskuteras inte sådant internationellt samarbete som sker i svenskt intresse, utan uteslutande samarbete i syfte att bistå andra länder i deras brottsbekämpande verksamhet.

Enligt 7 § polisdatalagen (1998:622) får uppgifter lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Regeringen får vidare meddela föreskrifter om att uppgifter på begäran får lämnas till en polis- eller åklagarmyndighet i en stat som är ansluten



till Interpol, om det behövs för att myndigheten ska kunna förebygga, upptäcka, utreda eller beivra brott. Sådana föreskrifter finns i 18 § polisdataförordningen (1999:81). Där föreskrivs att uppgifter som behandlas enligt polisdatalagen får, om det är förenligt med svenska intressen, lämnas ut dels till utländsk under rättelse- eller säkerhetstjänst, dels till en utländsk polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott. De nu nämnda bestämmelserna är sekretessbrytande, vilket innebär att uppgifter får lämnas ut trots att de är sekretessbelagda.

Reglerna i 7 § polisdatalagen och 18 § polisdataförordningen dispenserar emellertid inte från bestämmelserna i personuppgiftslagen om överföring av personuppgifter till tredjeland. Vid utlämnande av personuppgifter till utlandet måste polisen därför också göra en bedömning av om reglerna i personuppgiftslagen hindrar utlämnande.

Enligt 33 § personuppgiftslagen (1998:204) är det förbjudet att till tredjeland, dvs. ett land utanför EU, föra över personuppgifter som är under behandling om landet inte har en adekvat nivå för skydd av personuppgifter. Förbudet omfattar även överföring av personuppgifter för behandling i tredjeland. Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständigheter. Särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredjelandet. Trots förbudet i 33 § är det enligt 34 § tillåtet att under vissa förutsättningar föra över uppgifter till tredjeland, men det förutsätter antingen att den registrerade gett sitt samtycke till överföringen eller att överföringen är nödvändig bl.a. för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras eller att vitala intressen för den registrerade ska kunna skyddas. Vidare är det tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen. Regeringen kan också meddela föreskrifter om undantag från förbudet

mot överföring av uppgifter till vissa stater eller till tredjeland. I avsnitt 6.5.2 har föreslagits att bl.a. reglerna i personuppgiftslagen om överföring av uppgifter till tredjeland ska tillämpas på polisens personuppgiftsbehandling i den brottsbekämpande verksamheten.

#### *Utgångspunkter för den nya regleringen*

Man kan urskilja tre olika situationer där informationsutbyte aktualiseras i internationellt polisiärt samarbete. Den första är där Sverige i en internationell överenskommelse, som har trätt i kraft, har förbundit sig att tillhandahålla information av visst slag utan särskild anmodan. Ett exempel på det är Schengens informationssystem. Den andra situationen är där Sverige i en sådan överenskommelse har åtagit sig att genomföra en viss åtgärd eller att lämna viss information på begäran av en annan stat eller mellanfolklig organisation. Rättslig hjälp i form av förhör, som hålls på begäran av en annan stat, är exempel på det förstnämnda. Reglerna om uppgiftslämnande i lagen om belastningsregister och lagen om misstankeregister är exempel på det senare.

Den tredje situationen är s.k. spontant uppgiftsutlämnande, där initiativet till informationsutbytet tas av den svenska polisen. Ett väl fungerande samarbete över gränserna förutsätter att den svenska polisen inte bara bistår polismyndigheter i andra länder med svar på konkreta förfrågningar eller med rättslig hjälp i enskilda ärenden utan även att svensk polis kan lämna uppgifter spontant i de fall där utbytet främst gagnar utländska intressen. Sverige har i olika internationella överenskommelser accepterat att medverka i sådant frivilligt informationsutbyte och har också varit pådrivande när det gäller att utveckla informationsutbytet.

Mot denna bakgrund är det tydligt att enbart de sekretessbrytande bestämmelserna i 1 kap. 3 § tredje stycket sekretesslagen inte är tillräckliga för att Sverige ska kunna fullgöra sina internationella åtagandena. Det krävs alltså särskilda sekretessbrytande bestämmelser i den nya lagen.

Tyngdpunkten i informationsutbytet ligger för närvarande på uppgifter som antingen förmedlas via Interpol eller utbyts genom Europol (se avsnitt 7.4). Som tidigare nämnts kan det t.ex. röra sig om efterlysningar av personer eller föremål eller konkreta förfrågningar om personer eller egendom. På sikt kommer emellertid det internationella samarbetet sannolikt att i ökad utsträckning ske direkt mellan polispersonalen i olika länder, på samma sätt som länge har varit fallet i det nordiska polis-samarbetet. För att ett sådant samarbete ska kunna fungera är det nödvändigt att den föreslagna lagen tydligt anger gränserna för vilka uppgifter som får lämnas ut.

Internationella överenskommelser reglerar normalt informationsutbyte på ett visst, begränsat område. En överenskommelse avser ofta informationsutbytet mellan vissa utpekade myndigheter eller informationsutbyte avseende viss typ av brottslighet. Regleringen i den nya lagen bör så långt möjligt vara generell.

Den första frågan är på vilken författningsnivå man ska reglera polisens uppgiftslämnande till utländska myndigheter och mellanfolkliga organisationer. Sakfrågan faller i och för sig inom regeringens restkompetens och skulle alltså kunna regleras i förordning. Ett av syftena med den nya lagen är emellertid att åstadkomma en tydligare reglering av förutsättningarna för uppgiftslämnandet mellan svenska brottsbekämpande myndigheter. Det framstår då som naturligt att också uppgiftslämnande till brottsbekämpande utländska myndigheter och organisationer i huvudsak regleras i lagen. Lagen bör därför innehålla de grundläggande reglerna om uppgiftslämnande, medan vissa kompletterande regler liksom nu kan finnas i förordning. Vad som är särskilt viktigt att reglera i lag är dels sådant uppgiftslämnande som följer direkt av bindande internationella åtaganden, dels sådant informationsutbyte som förekommer frekvent. Vidare bör övervägas i vilken utsträckning formerna för uppgiftslämnandet ska regleras.

*Bindande åtaganden om att lämna uppgifter*

Den nya lagens bestämmelse om utlämnande av uppgifter till utländska myndigheter och organisationer bör i huvudsak ha samma innehåll som nuvarande lagstiftning. Den bör omfatta alla folkrättsligt bindande åtaganden om att lämna viss information till en annan stat eller till en mellanfolklig organisation.

Interpol är ett mellanstatligt samarbete på folkrättslig grund. Interpol fungerar främst som ett kontaktorgan mellan stater som är medlemmar i organisationen och som en kanal för att sprida polisiär information till ett flertal länder.

Europol har en betydligt aktivare roll i det polisiära samarbetet över gränserna. Europol har som förstahandsuppgift att underlätta informationsutbytet mellan länderna och att inhämta, sammanställa och analysera information och underrättelser samt att genast informera medlemsländerna om sådant som berör dem, t.ex. upptäckta samband mellan brottsliga gärningar i olika länder. Europol bedriver underrättelse- och analysverksamhet och upprättar allmänna lägesrapporter om viss brottslighet. Europol kan också bistå enskilda medlemsländer med råd och forskning kring bl.a. utbildning, polisiära metoder och brottsförbyggande arbete.

Medlemsländerna är skyldiga att lämna vissa uppgifter till Europol, i vissa fall utan särskild anmodan. Skyldigheten omfattar uppgifter inom Europols verksamhetsområde men gäller inte för nationella säkerhetstjänster. Medlemsländerna förutsätts också kunna lämna över uppgifter till Europol spontant.

Polissamarbetet inom Europol tillhör den s.k. tredje pelaren. Det innebär att det är ett mellanstatligt samarbete, där Europol inte har några egentliga beslutsfunktioner. Europeiska unionen har emellertid nyligen meddelat ett rådsbeslut angående Europols framtida organisation och uppgifter (se avsnitt 4.2.6). Beslutet innebär att Europol ska inrättas som ett EU-organ, vilket kan komma att påverka formerna för samarbetet med medlemsstaterna. En reglering som täcker folkrättsligt bindande åtaganden fungerar emellertid även för nya åtaganden.

En viktig fråga är huruvida de nya bestämmelserna ska möjliggöra utlämnande av uppgifter oberoende av på vilken nivå de internationella överenskommelserna har ingåtts. Rikspolisstyrelsen har, efter bemyndigande från regeringen, ingått bilaterala avtal om polisiärt samarbete med vissa stater. Flertalet av dessa avtal gäller i förhållande till stater som numera är medlemmar av Europeiska unionen. I sådana avtal utgör informationsutbyte ofta en viktig del. Avtalen innehåller normalt hänvisningar till nationell lagstiftning. Det innebär att endast sådant informationsutbyte som är tillåtet enligt nationell lag omfattas av avtalet. Denna begränsning finns dock inte i alla avtal.

I propositionen med förslag om godkännande av Europolkonventionen (prop. 1996/97:164, s. 64) framhöll den dåvarande regeringen att det i fråga om utlämnande av uppgifter ur polisregister var nödvändigt att begränsa uppgiftslämnandet till överenskommelser som godtagits av riksdagen. Skälet till detta var att man ville förhindra ett mer extensivt utbyte av personuppgifter ur sådana register. Regeringen påpekade också att Registerutredningen hade föreslagit motsvarande begränsning i fråga om all databehandling av uppgifter inom polisens verksamhetsområde, vilket också riksdagen senare beslutade om. De uttalanden som gjordes i det lagstiftningsärendet har alltså viss bärkraft. Den allmänna regeln om uppgiftslämnande till en utländsk myndighet eller mellanfolklig organisation bör därför, på samma sätt som nu, endast omfatta internationella åtaganden som har godkänts av riksdagen. I fråga om informationsutbyte med utländska polis- och åklagarmyndigheter samt med utländsk underrättelse- eller säkerhetstjänst bör det, som utvecklas närmare nedan, dock inte ställas upp något krav på att utbytet ska följa av en internationell överenskommelse. Något sådant krav finns inte heller i dag.

*Informationsutbyte med polis- och åklagarmyndigheter m.m. på begäran*

Informationsutlämnande sker vanligtvis med anledning av en begäran från en utländsk myndighet om viss information. De som oftast mottar information från den svenska polisen är utländska polismyndigheter. I och med att varje land organiserar den brottsbekämpande verksamheten efter sina traditioner kan dock informationsutbyte också äga rum mellan en polismyndighet och en åklagarmyndighet eller vice versa eller med någon annan utländsk myndighet som har polisiära uppgifter.

Det förhållandet att uppgiftslämnande till utländska polis- och åklagarmyndigheter sker frekvent talar för att man bör reglera detta direkt i lagen, i stället för att som nu ha ett bemyndigande för regeringen att meddela föreskrifter om utlämnande till sådana myndigheter. Den nya regleringen bör således omfatta uppgiftslämnande till polis- eller åklagarmyndighet i andra stater.

När det gäller uppgiftslämnande till Europol kan noteras att de stater som tillhör organisationen samtliga har tillträtt Europarådets konvention om dataskydd och att reglerna i 33 § personuppgiftslagen därför inte hindrar överföring av personuppgifter (se 34 § andra stycket). Sverige har förbundit sig att på begäran lämna vissa uppgifter till andra stater som är anslutna till Europol. Det följer således redan av den föreslagna huvudregeln att information kan lämnas på begäran av en sådan stat, men en tydlig reglering av vilken det framgår att uppgifter alltid får lämnas till stater som tillhör Europol underlättar informationsutbytet. Regleringen bör också, på ett tydligare sätt än nu, omfatta uppgiftslämnandet till själva organisationen.

När det gäller uppgiftslämnande till stater som enbart är anslutna till Interpol kan noteras att vissa av dessa stater också har tillträtt Europarådets konvention om dataskydd och således har en dataskyddsnivå som medger överföring av personuppgifter utan någon särskild bedömning. Många andra stater har också en tillräcklig dataskyddsnivå, men det kräver en bedömning i det enskilda fallet. Interpol som organisation uppfyller också kraven

på tillräcklig dataskyddsnivå. Sverige har förbundit sig att inom ramen för Interpol lämna andra stater bistånd med information, men dessa åtaganden är inte lika långtgående som när det gäller åtagandena i förhållande till stater som är medlemmar i Europol. Likaså har Sverige förbundit sig att lämna viss information till Interpol i dess egenskap av samarbetsorganisation. Den nya lagen bör därför ge utrymme för att uppgifter kan lämnas både till en annan stat som är medlem i Interpol och till organisationen som sådan.

Ändamålet med att lämna uppgifter till en polis- eller åklagarmyndighet i en annan stat, eller till Europol eller Interpol, bör liksom nu vara att uppgiften behövs för att förebygga, upptäcka eller beivra brott. Ett grundläggande krav bör liksom i dag vara att utlämnandet är förenligt med svenska intressen.

Mot bakgrund av vad som sagts ovan bör framhållas att uppgiftslämnande till en polis- eller åklagarmyndighet i en annan stat som enbart är medlem i Interpol förutsätter en noggrannare bedömning, eftersom den utlämnande myndigheten då – utöver att bedöma om det ligger i svenskt intresse att lämna uppgiften – alltid måste avgöra om den andra staten har en tillräcklig dataskyddsnivå för att överföring av personuppgifter ska vara tillåten enligt personuppgiftslagen.

Bestämmelsen bör alltså utformas så att det direkt framgår att personuppgifter får lämnas till polis- och åklagarmyndigheter i stater som är anslutna till Interpol. Därmed täcks även motsvarande uppgiftslämnande till stater som ingår i Europol, eftersom staterna inom Europeiska unionen är medlemmar i båda. Vidare bör utlämnande få ske till båda organisationerna.

### *Spontant uppgiftslämnande*

Ytterligare en fråga som måste övervägas är om även spontant uppgiftslämnande ska omfattas och hur det i så fall ska regleras. Här kan inledningsvis konstateras att ett flertal konventioner och andra internationella överenskommelser som reglerar

brottsbekämpning och som Sverige har undertecknat, innehåller bestämmelser om sådant uppgiftslämnande. Som exempel på överenskommelser där det finns bestämmelser om spontant uppgiftslämnande kan nämnas Förenta nationernas konvention mot gränsöverskridande organiserad brottslighet (artikel 18 punkten 4), Europarådets konvention om IT-relaterad brottslighet (artikel 26), Europarådets straffrättsliga konvention om korruption (artikel 28) och 2000 års konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater (artikel 7). Eftersom bestämmelser om spontant uppgiftslämnande normalt hänvisar till vad som är tillåtet enligt nationell lagstiftning, brukar bestämmelser av detta slag inte betraktas om någon obligatorisk förpliktelse. Å andra sidan brukar det läggas stor vikt vid det spontana informationsutbytet vid utvärdering av internationella överenskommelser och deras effektivitet. Sverige har också i olika sammanhang varit pådrivande när det gäller att utöka det internationella informationsutbytet, bl.a. genom att ta initiativ till rambeslutet av den 18 december 2006 om förenklat informations- och underrättelseutbyte mellan de brottsbekämpande myndigheterna i Europeiska unionens medlemsstater (2006/960/RIF). Om uppgifter lämnas spontant kan informationen som regel föras med villkor att den mottagande staten bara får använda den på visst sätt eller för visst ändamål. Ett sådant villkor, som är bindande för mottagaren, kan underlätta informationsutbytet i enskilda fall. Ett villkor angående användningen kan bl.a. innebära ett skydd mot att uppgifterna sprids vidare och utgör därför ett integritetsskydd för den enskilde.

Om Sverige fullt ut ska kunna leva upp till sina internationella åtaganden, bör det finnas utrymme för den svenska polisen att spontant lämna ut information till en annan stats brottsbekämpande myndighet, om informationen är värdefull för den statens brottsbekämpning. Som exempel kan nämnas information om nya tillvägagångssätt vid allvarlig gränsöverskridande brottslighet eller upplysningar om konkreta brott för vilka det saknas svensk jurisdiktion.



Uppgifter bör således på samma sätt som i dag kunna lämnas till en utländsk polis- eller åklagarmyndighet, eller till Interpol eller Europol, utan föregående begäran. Det enda krav som bör ställas i den nya lagen, utöver att uppgifterna ska behövas i den mottagande statens brottsbekämpning, är att uppgiftslämnandet ska vara förenligt med svenska intressen. Som tidigare framhållits måste, innan en personuppgift lämnas ut, den utlämnande myndigheten också bedöma om det mottagande landet har en tillräcklig dataskyddsnivå.

*Utlämnande till utländsk underrättelse- eller säkerhetstjänst m.m.*

I Säkerhetspolisens arbete är internationellt informations- och erfarenhetsutbyte en viktig del. Samarbetet med utländska underrättelse- eller säkerhetstjänster har stor betydelse i arbetet med att förebygga brott mot rikets säkerhet och med att bekämpa terrorism. Den brottsliga verksamhet som Säkerhetspolisen har till uppgift att förebygga och avslöja är nämligen i många fall gränsöverskridande till sin natur. Terrorism bedrivs t.ex. ofta av löst sammansatta terrornätverk med omfattande internationella förgreningar. Spioneri och andra brott mot rikets säkerhet har av naturliga skäl normalt utländska kopplingar. Eftersom utbytet av underrättelseinformation är en förutsättning för Säkerhetspolisens arbete, bör uppgifter i samma utsträckning som i dag, kunna lämnas till utländsk underrättelse- eller säkerhetstjänst när det är förenligt med svenska intressen. Bestämmelsen om detta bör enligt vår mening tas in i den nya lagen i stället för i förordning, eftersom det är fråga om frekvent uppgiftslämnande.

Det skulle i och för sig ha varit önskvärt att, till skillnad från vad som gäller i dag, ge uttryck för under vilka närmare förutsättningar personuppgifter får lämnas ut till utländsk underrättelse- eller säkerhetstjänst. Med hänsyn till de olikartade behov som utländska underrättelse- eller säkerhetstjänster kan ha är dock en sådan begränsning knappast möjlig att utforma. Någon

annan begränsning än att ett utlämnande ska vara förenligt med svenska intressen bör därför inte uppställas för dessa fall.

Regeringen bör, på samma sätt som nu, ha möjlighet att meddela föreskrifter om utlämnande av uppgifter för andra ändamål eller till andra utländska mottagare.

#### *Utlämnande i andra fall*

Uppgifter kan även lämnas till en utländsk myndighet eller organisation med stöd av 1 kap. 3 § tredje stycket sekretesslagen, efter en sekretessprövning i det enskilda fallet. Det kan gälla uppgiftslämnande till någon annan mottagare än de som i dag anges i polisdatalagen och polisdataförordningen eller utlämnande för annat ändamål än som anges där. I den nya lagen bör tas in en erinran om den sekretessbrytande bestämmelsen i 1 kap. 3 § tredje stycket. En sådan erinran finns i 7 § tredje stycket polisdatalagen.

Avslutningsvis bör understrykas att det i samtliga fall, där det enligt den föreslagna lagen kommer att finnas ett utrymme för att föra över personuppgifter till ett annat land, före överföringen måste övervägas om denna är förenlig med bestämmelserna i 33 och 34 §§ personuppgiftslagen.

## 14 Utlämnande av uppgifter på medium för automatiserad behandling

**Promemorians förslag:** Endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall.

**Utredningens förslag:** Utredningen har inte lämnat något förslag om utlämnande av uppgifter på medium för automatiserad behandling.

**Remissinstanserna** har inte uttalat sig i frågan.

**Skälen för promemorians förslag:** Uppgifter kan som nämnts i föregående avsnitt lämnas ut från polisen i elektronisk form på medium för automatiserad behandling på flera sätt, bl.a. genom e-post, genom användandet av diskett, CD-ROM-skiva eller genom direkt överföring från ett datorsystem till ett annat via telekommunikationsnätet. Den utlämnande polismyndigheten fattar i dessa fall beslut om utlämnandet i varje enskilt fall. Eftersom den personuppgiftsansvarige vid medgivande av direktåtkomst i praktiken avhänder sig den konkreta kontrollen över vilka uppgifter mottagaren väljer att ta del av och i vilken omfattning detta sker, brukar direktåtkomst framhållas som den mest känsliga av de olika formerna av elektroniskt utlämnande. Emellertid innefattar även ett utlämnande av personuppgifter på

medium för automatiserad behandling särskilda risker från integritetssynpunkt. Sådant utlämnande innebär nämligen som regel att informationen lämnas ut på ett sådant sätt att mottagaren kan bearbeta informationen, t.ex. genom att samköra den mot elektroniska uppgifter som har hämtats från andra informationskällor. På så vis ökar riskerna för att uppgifterna ska behandlas i strid med de grundläggande kraven på dataskydd. Det finns också en möjlighet för myndigheterna att inrätta rutiner som innefattar dagliga överföringar av större mängder av uppgifter via t.ex. e-post. Även om direktåtkomst generellt får betraktas som den mest känsliga formen av elektroniskt utlämnande kan i vissa fall lika stora risker föreligga vid andra former av elektroniskt utlämnande. Med hänsyn härtill anser vi att förutsättningarna för utlämnande av personuppgifter på medium för automatiserad behandling bör författningsregleras (jfr prop. 2006/07:46 s. 77 f. och 124).

Polisen bör givetvis ha möjlighet att använda modern kommunikationsteknik för att utbyta information på elektronisk väg också på annat sätt än genom direktåtkomst. En utgångspunkt för en sådan reglering bör vara att den ska tillåta ett normalt informationsutbyte på elektronisk väg, samtidigt som regleringen inte får utformas så att den möjliggör ett kringgående av bestämmelserna om direktåtkomst. Enstaka uppgifter och handlingar bör alltså få lämnas ut på medium för automatiserad behandling, t.ex. genom e-post, när förutsättningarna för ett utlämnande i övrigt är uppfyllda. När det däremot gäller möjligheterna att lämna ut större mängder uppgifter i elektronisk form, bör de närmare förutsättningarna för det anges genom föreskrifter i förordning. Det bör också finnas utrymme för regeringen att i ett enskilt fall besluta om att uppgifter får lämnas ut på medium för automatiserad behandling i större omfattning även i annat fall. Detta bör gälla oberoende av om uppgifterna lämnas inom landet eller utomlands.

I den nya lagen bör detta komma till uttryck genom ett principiellt förbud att lämna ut annat än enstaka uppgifter på medium för automatiserad behandling. Förbudet bör komplette-

ras av en bestämmelse som medger att regeringen i förordning eller i ett enskilt fall kan besluta om att sådant utlämnande även får ske i andra fall. Därmed ges regeringen möjlighet att medge utlämnande i elektronisk form i vissa situationer där starka skäl kan tala för sådant utlämnande, t.ex. utlämnande av en förundersökning till en försvarare eller annat juridiskt biträde.



## 15 Särskilt om uppgifter på Internet

**Promemorians bedömning:** Det bör inte införas några särbestämmelser om polisens möjligheter att göra personuppgifter tillgängliga via Internet.

**Utredningens förslag:** Utredningen har föreslagit en särskild reglering av polisens möjligheter att efterlysa personer på Internet (se SOU 2001:92 s. 180 f.). Utredningens förslag innebär i övrigt inte några särskilda hinder mot att polisen publicerar uppgifter på Internet.

**Remissinstanserna:** *Justitiekanslern* har ifrågasatt om det finns tillräckliga skäl att ha olika syn på behandlingar som sker med stöd av personuppgiftslagen å ena sidan och med stöd av den föreslagna lagen å den andra. *Riksåklagaren* har ansett att det ska vara möjligt att göra en efterlysning tillgänglig på Internet även i vissa fall som inte omfattas av utredningens förslag. *Rikspolisstyrelsen* har ansett att utredningens förslag är otillräckligt. *Ekobrottsmyndigheten* har ifrågasatt om känsliga uppgifter ska få läggas ut på Internet. *Datainspektionen* har menat att även uppgifter som inte är föremål för sekretess kan vara känsliga att sprida via Internet och att de allmänna förutsättningarna för behandling av personuppgifter inte ger ett tillräckligt skydd för enskilda personers integritet. Inspektionen har ansett att det bör finnas närmare bestämmelser om vilka uppgifter som det är tillåtet att sprida till tredjeland via Internet. *Malmö tingsrätt* har

påpekat att det skulle vara lämpligt om vissa kriterier för tillåtligheten av ett sådant offentliggörande som det är frågan om direkt angavs i lagen. *Juridiska fakultetsnämnden vid Uppsala universitet* har ifrågasatt hur angeläget det är att skicka ut efterlysningar på Internet. *Kustbevakningen* har förordat stor försiktighet vid spridning av personuppgifter på Internet.

**Skälen för promemorians bedömning:** Utredningen har aktualiserat frågan om en särreglering av offentliggörande av personuppgifter på Internet i polisverksamheten. En utgångspunkt för utredningens överväganden var att publicering på Internet innebär en otillåten överföring av personuppgifter till tredjeland enligt 33 § personuppgiftslagen. Eftersom polisen ansågs ha behov av att kunna publicera uppgifter på Internet, föreslog utredningen inte någon motsvarande bestämmelse. Därmed skulle polisen kunna offentliggöra personuppgifter på Internet. Utredningen ansåg emellertid att polisens möjligheter att publicera personafterlysningar på Internet av integritetsskäl borde lagregleras.

Utgångspunkten i vårt förslag är att 33 § personuppgiftslagen ska tillämpas i polisens brottsbekämpande verksamhet (se avsnitt 6.5.2). Frågan är då om den bestämmelsen utgör hinder mot att publicera uppgifter på Internet. Utredningen har, i likhet med den dåvarande regeringen i ett tidigare lagstiftningsärende, utgått från att motsvarande bestämmelse i artikel 25.1 i dataskyddsdirektivet är generellt tillämplig bl.a. när det gäller offentliggörande av personuppgifter på Internet (prop. 1999/2000:11, bet. 1999/2000:KU7). Efter EG-domstolens dom i det s.k. konfirmandlärmålet (dom den 6 november 2003 i mål C-101/01, REG 2003 s. I-2971) har förbudet mot att överföra personuppgifter till ett tredjeland, som inte säkerställer en adekvat skyddsnivå, emellertid delvis förlorat i betydelse. I domen, som var ett förhandsavgörande, gjorde EG-domstolen bedömningen att det inte förelåg någon överföring i den mening som avses i artikel 25.1 i dataskyddsdirektivet när en person hade lagt ut personuppgifter på Internet. Avgörandet var i formell mening begränsat till den situationen att en enskild person lägger ut personupp-



gifter på en hemsida som är lagrad hos någon annan än denne och varifrån uppgifterna kan nås via Internet.

Förutsättningarna för polisens behandling av personuppgifter genom offentliggörande på Internet skiljer sig i vissa hänseenden från vad som gällde i målet vid EG-domstolen. Polisen innehar själv den server på vilken de uppgifter lagras som görs tillgängliga på Internet. Offentliggörandet sker dessutom, i motsats till vad som var fallet i det mål som EG-domstolen prövade, genom en åtgärd som vidtas av det allmänna. Vid bedömningen av om en polismyndighets offentliggörande av personuppgifter på Internet kan antas falla in under tillämpningsområdet för artikel 25.1 i dataskyddsdirektivet – och därmed 33 § personuppgiftslagen – bör enligt vår mening emellertid särskilt framhållas att EG-domstolens huvudargument för bedömningen i det berörda målet är av allmängiltig natur, något som också har påpekats av Personuppgiftslagsutredningen i dess analys av domen (SOU 2004:6 s. 233). Detta gäller i synnerhet det förhållandet att en tillämpning av överföringsbegreppet på Internetpublicering skulle kunna leda till den orimliga konsekvensen att inte en enda personuppgift kan göras allmänt tillgänglig på Internet. Mot den bakgrunden får det antas att EG-domstolen, i fråga om sådana åtgärder som vidtas av den som själv innehar den server som är ansluten till Internet eller av den som tillhandahåller en servertjänst, inte skulle göra någon annan bedömning av överföringsbegreppets innebörd än den som gjordes i det aktuella målet (jfr Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen, En kommentar, 3 uppl., 2007, s. 384). Denna bedömning framstår i allt fall som den enda rimliga för de situationer i vilka, liksom i målet vid EG-domstolen, tillgången till uppgifterna fordrar någon form av aktivitet från någon annan än den som har lagt ut uppgifterna på en webbplats. Domstolens argument är vidare i lika hög grad relevanta beträffande de åtgärder för offentliggörande av personuppgifter på Internet som en juridisk person vidtar som beträffande åtgärder vidtagna av enskilda individer.

Vi bedömer därför att det inte är nödvändigt att införa någon särreglering av polisens möjligheter att efterlysa personer på

Internet av den anledningen att det skulle vara fråga om ett överförande av personuppgifter till tredjeland.

Frågan är då om det ändå bör införas lagregler om när polisen får sprida uppgifter via Internet. Polisen måste naturligtvis vid eventuell publicering på Internet, som vid all annan behandling, överväga om de allmänna förutsättningarna för en sådan behandling av personuppgifterna är uppfyllda. Dessutom krävs en bedömning av det lämpliga, bl.a. från integritetssynpunkt, i en eventuell publicering. Att införa särregler för just sådan publicering är emellertid knappast lämpligt, än mindre för enbart en viss typ av uppgifter.

I den mån det finns behov av generella regler för vad myndigheter får publicera på Internet bör den frågan utredas i ett större sammanhang.

## 16 Gallring av uppgifter

### 16.1 Gallring av uppgifter som inte har gjorts gemensamt tillgängliga

**Promemorians förslag:** Personuppgifter som inte har gjorts gemensamt tillgängliga ska gallras senast ett år från det att de behandlades automatiserat första gången eller, om de har behandlats inom ett ärende, senast ett år från det att ärendet avslutades. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgifter ska bevaras under längre tid för historiska, statistiska eller vetenskapliga ändamål.

**Utredningens förslag** överensstämmer delvis med promemorians förslag. Utredningen har föreslagit att personuppgifter som behandlas automatiserat och som avser en enskild person mot vilken det inte finns någon misstanke om brott ska få bevaras högst tre år från det att uppgifterna om personen samlades in. I de fall där inga särskilda gallringsregler gäller ska enligt förslaget gallring ske om personuppgifterna inte längre behövs för ändamålet med behandlingen.

**Remissinstanserna:** Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft någon invändning mot det. *Rikspolisstyrelsen* har dock ansett att en gallringsfrist på tre år är för kort.

**Bakgrund:** I 13 § polisdatalagen föreskrivs att uppgifter som inte längre behövs för sitt ändamål ska gallras om inte annat

anges i lagen. Vidare anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska och vetenskapliga ändamål. Särskilda gallringsfrister gäller för de särskilda register som förs med stöd av lagen. För register som förs med stöd av övergångsbestämmelserna till polisdatalagen har Datainspektionen meddelat beslut om gallringsfrister.

Polisdatalagens bestämmelser om gallring gäller inte uppgifter i förundersökningar. Förundersökningar ska gallras i den utsträckning som följer av arkivlagen.

**Skälen för promemorians förslag:** Från integritetssynpunkt är det angeläget att personuppgifter som samlas in i brottsbekämpande verksamhet gallras så snart de inte längre behövs för det ändamål för vilket de samlades in. När det gäller information på ADB-medium anses visserligen gallring inte behöva innebära att själva informationen förstörs, utan det är tillräckligt att informationen överförs till papper, varefter själva ADB-mediet förstörs. Redan en gallring av detta slag är emellertid värdefull från integritetssynpunkt, eftersom den får till följd att informationen inte längre kan bli föremål för elektroniska sökningar och sammanställningar.

De bestämmelser om gallring som finns i eller följer av arkivlagen anger när gallring *får* ske och nödvändiggör alltså inte gallring. Arkivlagen tillgodoser därför inte integritetsskyddsintresset av att gallring sker. Den nya lagen bör mot den bakgrunden innehålla bestämmelser om när behandlade uppgifter *ska* gallras. Detta överensstämmer med hur regleringen ser ut i såväl polisdatalagen som en del annan registerlagstiftning, t.ex. lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Vi har övervägt om det i den nya lagen bör införas en allmän bestämmelse om att personuppgifter ska gallras så snart de inte längre behövs för sitt ändamål. En sådan bestämmelse skulle ligga väl i linje med den allmänna princip som vi har förordat ovan, nämligen att behandling enligt den nya lagen får ske enbart för vissa i lagen angivna ändamål. Mot en sådan bestämmelse kan

dock invändas att den ger föga ledning i det enskilda fallet, särskilt som en uppgift, insamlad i en viss underrättelseverksamhet eller en viss brottsutredning, så småningom kan visa sig ha betydelse i annan underrättelseverksamhet eller brottsutredning. Vi föreslår därför i stället att det i den nya lagen tas in gallringsbestämmelser som anger inom vilken tid gallring måste ske. Det hindrar naturligtvis inte att uppgifter som uppenbarligen har förlorat all betydelse i det brottsbekämpande arbetet bör gallras så snart som möjligt. Någon särskild bestämmelse om detta anser vi dock inte vara nödvändig.

Gallringsfristerna utgör alltså maximitider. I den mån det redan vid en tidigare tidpunkt står klart att uppgifterna saknar betydelse från brottsbekämpningssynpunkt ska de gallras redan då. Detta följer av lagens allmänna bestämmelser, bl.a. ändamålsbestämmelserna. En uppgift får inte behandlas om den inte behövs i den brottsbekämpande verksamheten. Av verksamhetskäl kan det dock inte ställas upp något krav på att den personuppgiftsansvariga myndigheten fortlöpande ska kontrollera om uppgifter måste gallras före gallringsfristens utgång. Om myndigheten uppmärksammas på saken av någon utomstående eller det annars står klart för myndigheten att en uppgift inte längre har någon relevans i den brottsbekämpande verksamheten, får den dock anses vara skyldig att se till att uppgiften gallras.

Hur lång bör då gallringsfristen vara? Enligt vår mening finns det här anledning att göra skillnad mellan uppgifter som har gjorts gemensamt tillgängliga och andra uppgifter. När det gäller uppgifter som inte har gjorts gemensamt tillgängliga, torde behovet av att behandla dem under längre tid typiskt sett vara begränsat. Dessutom är det från integritetssynpunkt särskilt angeläget att just dessa uppgifter inte behandlas under längre tid, eftersom det, enligt vårt förslag, inte kommer att gälla annat än ett fåtal begränsningar för behandlingen av dem. Det bör därför uppställas särskilt korta gallringsfrister för sådana uppgifter.

När det gäller uppgifter som behandlas *inom ramen för ett ärende* bör gallring lämpligen ske inom ett år från det att ärendet

avslutades. Uppgifter som *inte behandlas inom ramen för ett ärende* bör i stället gallras inom ett år från det att uppgifterna behandlades första gången. I likhet med vad som föreskrivs i polisdatalagen bör det finnas en möjlighet för regeringen att föreskriva att uppgifterna får bevaras för historiska, statistiska eller vetenskapliga ändamål.

När *uppgifter behandlas inom ramen för en förundersökning*, gör sig dock särskilda hänsyn gällande. De nu föreslagna gallringsfristerna bör därför inte gälla uppgifter i förundersökningar. Vi återkommer till denna fråga i avsnitt 16.3.

## 16.2 Gallring av gemensamt tillgängliga uppgifter

**Promemorians förslag:** Personuppgifter som har gjorts gemensamt tillgängliga och som kan antas ha samband med brottslig verksamhet ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om den person som en uppgift avser inte är eller har varit misstänkt, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats i samband med övervakning av brottsbelastade eller potentiellt farliga personer ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende den övervakade gjordes. Om en uppgift inte avser den övervakade personen, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av respektive gallringsfrist.

Uppgifter som har behandlats inom ramen för det internationella samarbetet ska gallras senast ett år efter det att ärendet i vilket uppgifterna behandlades avslutades.

Uppgifter som har behandlats enbart på den grunden att de har rapporterats till polisens kommunikationscentraler ska gallras senast ett år efter rapporteringen.

Regeringen får meddela föreskrifter om att uppgifter i vissa fall ska få behandlas och bevaras under längre tid. Regeringen eller den myndighet som regeringen bestämmer får också meddela föreskrifter om bevarande för historiska, statistiska eller vetenskapliga ändamål.

**Utredningens förslag:** Utredningen har föreslagit att personuppgifter som behandlas automatiserat och som avser enskild person mot vilket det inte finns någon misstanke om brott ska få bevaras högst tre år från det att uppgifterna om personen samlades in. Uppgifter om övervakade personer ska dock enligt förslaget få bevaras så länge personen finns med i belastningsregistret. Vidare har föreslagits särskilda gallringsregler för det spaningsregister som utredningen har föreslagit och för DNA-register och fingeravtrycks- och signalementsregister. I de fall där inga särskilda gallringsregler gäller ska enligt förslaget gallring ske om personuppgifterna inte längre behövs för ändamålet med behandlingen.

**Remissinstanserna:** Flertalet remissinstanser har tillstyrkt utredningens förslag eller inte haft någon invändning mot dem. *Rikspolisstyrelsen* har ansett att den föreslagna gallringsfristen om tre år är alltför kort.

**Skälen för promemorians förslag:** Vi har ovan konstaterat att det från integritetssynpunkt är viktigt att personuppgifter inte behandlas längre än nödvändigt och att det därför i lagen bör anges särskilda gallringsfrister. Vi har också konstaterat att gallringsfristerna bör bestämmas så att uppgifter inte bevaras längre än nödvändigt. Det kan dock vara svårt att generellt avgöra hur länge en uppgift fortfarande kan vara av betydelse för brottsbekämpningen. Uppgifter som har framkommit i ett avslutat kriminalunderrättelseprojekt kan senare få betydelse för ett annat projekt eller för en förundersökning. Alltför snäva gallringsfris-

ter kan därför få negativa konsekvenser för den brottsbekämpande verksamheten.

När det gäller gemensamt tillgängliga uppgifter delar vi därför utredningens och remissinstansernas allmänna uppfattning att gallring normalt bör ske senast tre år från det att uppgifterna samlades in. När det gäller personer som är misstänkta för brottslig verksamhet bör dock treårsfristen räknas från den senaste registreringen avseende den personen. Detta överensstämmer med vad som gäller för gallring av uppgifter i den s.k. tullbrotsdatabasen (se 27 § lagen [2005:787] om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet).

Liksom utredningen anser vi också att en gallringsfrist om tre år är alltför kort när det gäller personuppgifter som behandlas i samband med övervakning av kriminella personer. Utredningen har föreslagit att sådana personuppgifter ska kunna bevaras så länge uppgifter om den övervakade personen fortfarande finns i belastningsregistret. För belastningsregistret gäller i dag olika gallringsfrister, beroende på vilket brott den aktuella personen har dömts för. Enligt vår mening bör man inte välja den lösningen, dels därför att en sådan ordning skulle bli svåröverskådlig, dels därför att alla de personer som är föremål för övervakning inte kommer att finnas i belastningsregistret. Vi föreslår därför, vad gäller uppgifter om de personer som står under övervakning, en enhetlig gallringsfrist om tio år. Fristen bör räknas från utgången av det kalenderår då den senaste registreringen avseende den övervakade personen gjordes. Man skulle i och för sig kunna överväga en något kortare gallringsfrist, exempelvis fem eller sju år. Det är framför allt två saker som talar för detta. Den ena är att riskerna för enskildas integritet typiskt sett är större ju längre gallringsfristerna är. Den andra är att, enligt vårt förslag, fristen för gallring automatiskt förlängs, om det tillkommer nya uppgifter om den registrerade (se nedan). Mot en kortare frist talar framför allt verksamhetens behov. Det kan ta mycket lång tid att bygga upp kunskap om exempelvis personer som finansierar allvarlig brottslighet. Erfarenheterna visar också att brottslig verksamhet som bedrivs i mer eller mindre organiserade former nor-



malt måste övervakas under en avsevärd tid innan man har tillräckligt underlag för att ingripa. En alltför kort gallringsfrist skulle därför motverka syftet med behandlingen. Det förhållandet att personer som misstänks ägna sig åt mycket allvarlig brottslig verksamhet ibland håller sig undan under långa perioder, t.ex. vistas utomlands, bör också beaktas. En tioårig gallringsfrist tillgodoser dessa verksamhetsmässiga behov. Den stämmer också väl överens med vad vi föreslår ska gälla för Säkerhetspolisens register. Polisdatautredningens, och den tidigare Registerutredningens, förslag om anknytning till belastningsregistret medger, åtminstone i teorin, längre lagringstider.

Vid övervakningen kan det emellertid också ha samlats in uppgifter om andra personer än den som står under övervakning, t.ex. uppgifter om anhöriga eller bekanta till den övervakade personen. Av integritetsskäl bör sådana uppgifter gallras tidigare än uppgifterna som avser den övervakade personen själv. I den delen föreslår vi en gallringsfrist om tre år, räknat från det att uppgiften samlades in, dvs. samma frist som vi föreslår ska gälla i övrigt för behandling av icke misstänkta personer.

Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning bör inte räknas med vid beräkningen av de gallringsfrister som vi har föreslagit ovan.

Allt arbete som sker för att fullgöra internationella åtaganden är i princip ärendebaserat. När en förfrågan kommer från ett annat land hanteras denna inom ramen för någon form av ärende. Polisen har behov av att bevara ärenden en tid efter att ärendet har avslutats bl.a. för att i efterhand kunna svara på frågor om vidtagna åtgärder. När ett år har gått efter att ärendet har avslutats kan dock i allmänhet behovet inte vara så stort att det motiverar en fortsatt behandling. Uppgifterna bör därför gallras senast ett år efter det att ärendet har avslutats. Om en uppgift från ett internationellt ärende behöver bevaras för något annat av lagens ändamål, bör uppgiften givetvis kunna behandlas för det nya ändamålet i den utsträckning lagen tillåter en sådan behandling.

Vi har ovan föreslagit att också uppgifter som har rapporterats till polisens kommunikationscentraler ska kunna göras gemensamt tillgängliga, oavsett uppgifternas karaktär. Behovet av sådana uppgifter består dock normalt enbart under en kortare tid. Vi föreslår därför att uppgifterna ska gallras senast ett år efter rapporteringen.

En viktig fråga är vilken gallringsfrist som ska gälla om uppgifter som har samlats in i visst sammanhang före gallringsfristens utgång används i ett annat projekt eller ärende. Vad bör t.ex. gälla om uppgifter, som har rapporterats till polisens kommunikationscentral, kort tid efter rapporteringen tas tillvara i ett kriminalunderrättelseprojekt? Bör den ursprungliga gallringsfristen gälla eller bör man tillämpa den gallringsfrist som gäller i kriminalunderrättelseprojektet? Enligt vår uppfattning bör man tillämpa den gallringsfrist som gäller för uppgiften i dess nya sammanhang. Uppgifter i ett kriminalunderrättelseprojekt som har inhämtats via polisens kommunikationscentral bör alltså gallras enligt samma principer som gäller för uppgifter som har inhämtats på annat sätt. Vi återkommer till dessa och liknande frågor i författningskommentaren.

Vissa typer av uppgifter, t.ex. sådana uppgifter som i dag behandlas i det barnpornografiregister som Rikspolisstyrelsen för, bör kunna få behandlas under längre tid än vad som anges i lagen. Vi föreslår därför att regeringen får meddela föreskrifter om att uppgifter i vissa särskilda fall ska få behandlas och bevaras under längre tid. Regeringen eller den myndighet som regeringen bestämmer bör också få meddela föreskrifter om bevarande för historiska, statistiska eller vetenskapliga ändamål.

### 16.3 Särskilt om uppgifter i förundersökningar och liknande brottsutredningar

**Promemorians bedömning:** Det bör inte införas några särskilda gallringsbestämmelser för uppgifter i brottsanmälningar, förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken. Liksom i dag bör sådana uppgifter gallras enligt bestämmelserna i arkivlagen (1990:782). Det bör dock införas vissa begränsningar i möjligheten att använda uppgifterna i brottsbekämpningen efter det att ärendena har avslutats.

**Promemorians förslag:** Om en förundersökning har lagts ned på grund av bristande bevisning, om åtal har lagts ned eller om den misstänkte har frikänts genom en dom som har vunnit laga kraft, ska en uppgift om att personen är misstänkt vara sökbar endast om förundersökningsledaren har beslutat att återuppta förundersökningen eller fråga är om prövning av extraordinära rättsmedel.

När det har förflutit fem år från det att en dom, eller ett beslut med anledning av domstolsprövning, vann laga kraft, ska inte heller andra personuppgifter i förundersökningar eller liknande brottsutredningar få behandlas i polisens brottsbekämpande verksamhet. Uppgifter i en förundersökning som har lagts ned, eller avslutats på annat sätt än genom åtal, får enligt huvudregeln inte längre behandlas i den brottsbekämpande verksamheten när det förflutit fem år från beslutet. Detta ska dock inte gälla om förundersökningsledaren eller åklagaren vid nedläggningsbeslutet har angett att brottet, trots beslutet, kan komma att lagföras. I de fallen får behandling ske även efter femårstidens utgång, dock längst till dess att brottet preskriberas. Vad som nu har sagts om uppgifter i förundersökningar ska gälla även personuppgifter i andra utredningar som handläggs enligt 23 kap. rättegångsbalken.

Sedan de angivna tidsfristerna har löpt ut ska uppgifter i en förundersökning få behandlas endast om det behövs för att

förundersökningen ska återupptas eller för prövning av extraordinära rättsmedel. Om det finns särskilda skäl, ska uppgifterna även få behandlas för utredning av allvarliga brott eller undersökning av allvarlig brottslig verksamhet.

Uppgifter i en brottsanmälan, som inte har lett till förundersökning eller annan motsvarande utredning, får inte behandlas i polisens brottsbekämpande verksamhet när det brott som anmälan avser har preskriberats. Uppgifter i en anmälan som avser ett handlande som inte har bedömts utgöra brott ska över huvudtaget inte få behandlas.

Bestämmelserna om begränsningar i fråga om behandling av personuppgifter i brottsanmälningar eller förundersökningar eller andra utredningar som handläggs enligt 23 kap. rättegångsbalken ska inte hindra att uppgifterna arkiveras eller gallras enligt arkivlagens bestämmelser.

**Utredningens bedömning och förslag** överensstämmer delvis med promemorians bedömning och förslag. Utredningen har dock inte föreslagit någon särskild bestämmelse om behandling av uppgifter i brottsanmälningar eller om behandling av sådana uppgifter i förundersökningar eller liknande brottsutredningar som inte utgör uppgifter om brottsmisstanke.

**Remissinstanserna:** Flertalet remissinstanser har inte haft någon invändning mot utredningens förslag. *Rikspolisstyrelsen* har föreslagit att behandling av kvarstående misstankar ska vara tillåten även i andra fall, om det finns särskilda skäl. *Rikspolisstyrelsen* har härvid hänvisat till att uppgifterna i en nedlagd förundersökning kan vara av stort värde i arbetet med att kartlägga den organiserade brottsligheten. Styrelsen har också pekat på behovet av att kunna behandla uppgifter om kvarstående misstankar som gäller brott mot kvinnor som lever under hot.

## Skälen för promemorians bedömning och förslag

### *Inga gallringsregler för förundersökningar*

Polisdatalagen skiljer på gallring av uppgifter i förundersökningar och gallring av andra personuppgifter som behandlas av polisen. Förundersökningar arkiverades redan före polisdatalagens tillkomst enligt arkivlagens (1990:782) bestämmelser och frågan om gallring av förundersökningar avgjordes därmed av det arkivrättsliga regelverket. I förarbetena till polisdatalagen uttalades att frågan om gallring inte bör vara beroende av vilka tekniska hjälpmedel polisen väljer för sitt arbete (se prop. 1997/98:97 s. 109). Det ansågs att uppgifter som behandlas automatiserat i en förundersökning bör hanteras på samma sätt som motsvarande uppgifter som hanterats manuellt. Förundersökningsuppgifter som behandlas automatiserat omfattas alltså inte av polisdatalagens gallringsbestämmelser.

Skälen bakom den nuvarande ordningen gör sig fortfarande gällande. Vi föreslår därför, i likhet med utredningen, inte några särskilda gallringsbestämmelser i fråga om förundersökningar och liknande brottsutredningar, t.ex. utredningar enligt 31 § lagen med särskilda bestämmelser om unga lagöverträdare. Om en uppgift från en förundersökning behandlas för ett annat ändamål, t.ex. i ett underrättelseprojekt, bör dock uppgifterna i det sammanhanget gallras enligt de gallringsbestämmelser som gäller vid behandling för detta ändamål.

En möjlighet att utan några begränsningar behandla uppgifter i alla avslutade förundersökningar skulle emellertid kunna innebära särskilda integritetsrisker. I avsaknad av särskilda gallringsbestämmelser för förundersökningar bör det därför gälla vissa begränsningar bl.a. i fråga om hur länge uppgifter i en förundersökning får vara tillgängliga i den brottsbekämpande verksamheten. Dessa begränsningar bör dock givetvis inte hindra att uppgifterna arkiveras eller gallras enligt bestämmelserna i arkivlagen.

*Behandling av uppgifter om brottsmisstankar*

I 10 och 11 §§ polisdatalagen finns särskilda bestämmelser om behandling av uppgifter om brottsmisstankar som förekommer i avslutade förundersökningar. En sådan uppgift får, om förundersökningen har lagts ned på grund av bristande bevisning, behandlas enbart om den person som misstanken gällde fortfarande bedöms vara skäligen misstänkt för brottet och uppgifterna behövs för att förundersökningen ska kunna tas upp på nytt. Har åtal mot personen lagts ned eller ogillats, får uppgiften behandlas för annat ändamål än arkivering endast om förundersökningen tas upp på nytt eller för prövning av om resning bör ske.

En utgångspunkt för vårt arbete har varit att den nya lagen ska innehålla bestämmelser som fyller samma behov som reglerna i 10 och 11 §§ polisdatalagen. Motsvarande bestämmelser finns för övrigt även i 17 och 18 §§ lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Vi anser således att huvudregeln även i fortsättningen bör vara att i en förundersökning förekommande uppgifter om att en viss person är misstänkt för brott inte får behandlas efter det att förundersökningen har lagts ned på grund av bristande bevisning eller åtal mot den misstänkte har lagts ned eller ogillats. Att, som Rikspolisstyrelsen har föreslagit, tillåta fortsatt behandling så snart särskilda skäl talar för detta bör således inte komma i fråga. Av hänsyn till enskildas integritet bör givetvis en domstols dom eller beslut, som innebär att den åtalade frias från ansvar för brott, få genomslag även hos polisen på det sättet att en sådan person inte längre anges såsom misstänkt. Med detta avser vi inte att alla handlingar som rör brottsmisstanken måste rensas ut, utan enbart att den åtalade personen inte får utpekas såsom misstänkt och att man vid olika typer av sökningar inte ska få träff på honom eller henne i egenskap av misstänkt. Vi föreslår därför att regleringen i den nya lagen på ett tydligare sätt än i dag ska ge uttryck för att personer som har friats från ansvar inte längre får förekomma som misstänkta.

*Tillgång till avslutade förundersökningar*

I en förundersökning finns det givetvis även andra uppgifter än uppgifter om brottsmisstankar. Den nuvarande lagstiftningen uppställer inga särskilda hinder mot behandling av sådana uppgifter, fränsett de hinder som följer av de allmänna bestämmelserna i personuppgiftslagen.

I vilken utsträckning bör då polisen kunna behandla andra typer av uppgifter i avslutade brottsutredningar än de uppgifter som nyss har diskuterats? Här gör sig olika behov gällande.

Ett sådant är polisens behov av att kunna ha tillgång till uppgifterna en tid efter det att saken har avslutats för att lättare kunna utreda nya brott begångna av samma person eller mot samma person. Om en person återfaller i brott, har ofta tidigare brottsutredningar intresse. Vet man att det nya brottet har begåtts tillsammans med andra, okända gärningsmän, kan uppgifter om medgärningsmän i den tidigare brottsutredningen vara av intresse. Vidare kan det i den tidigare brottsutredningen finnas uppgifter om hur den misstänkte gjorde sig av med stöldgods eller om de tillvägagångssätt som han använde vid det tidigare brottet. En äldre utredning kan också underlätta framtagandet av personutredning. Vid upprepade brott mot samma offer kan äldre utredningar utnyttjas bl.a. för att belysa förhållandet mellan förövare och offer och förekomsten av påtryckningar. Det kan också vara av intresse att se hur offrets respektive förövarens trovärdighet har bedömts. Sådana uppgifter kan vidare ha stort intresse om frågan om besöksförbud aktualiseras, eftersom ett sådant förbud ofta grundar sig på tidigare brottslighet.

Dessutom har polisen behov av att ta vara på information från brottsutredningar för att samla information om vissa typer av brott eller vissa brottslingars beteenden. Sådan information har framför allt betydelse för det brottsförebyggande arbetet. Ett ytterligare behov är att kunna utnyttja tidigare brottsutredningar för utbildning och allmän kompetensutveckling inom polisen, eftersom både goda och dåliga exempel bör tas till vara.

Det är mot den angivna bakgrunden rimligt att uppgifter ur förundersökningar får vara tillgängliga i polisens brottsbekämpande verksamhet även en viss tid efter det att saken har avslutats. Denna tid bör dock inte vara alltför lång. Vi bedömer att fem år utgör en rimlig avvägning mellan integritetsintressena och polisens verksamhetsbehov. Vi föreslår därför att personuppgifter i förundersökningar eller liknande brottsutredningar inte ska få behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år från det att en dom, eller ett beslut med anledning av domstolsprövning, vunnit laga kraft.

I sammanhanget är det viktigt att påminna om att lagens övriga bestämmelser innebär att åtkomsten till uppgifterna i förundersökningar kommer att begränsas på olika sätt. Åtkomsten till uppgifter ska t.ex. anpassas till vilket behov olika tjänstemän har av att få tillgång till uppgifterna och alla uppgifter får inte vara sökbara.

#### *Särskilt om nedlagda förundersökningar*

När det gäller förundersökningar som har lagts ned eller avslutats genom annat beslut som inte lett till domstolsprövning (exempelvis beslut om förundersökningsbegränsning eller åtalsprövning), finns det också ett annat verksamhetsbehov, nämligen behovet av att kunna återuppta brottsutredningen. Ett beslut om att inte driva en brottsutredning vidare kan ha många olika orsaker, av vilka en del i princip utesluter att utredningen kan komma att tas upp på nytt medan det i andra fall är mer eller mindre troligt att förundersökningen kan komma att återupptas. En förundersökning som har lagts ned eller inte lett till åtal på grund av att bevisningen har bedömts vara otillräcklig kan när som helst aktualiseras på nytt, om det kommer fram nya uppgifter. Likaså kan ett beslut att lägga ned en förundersökning, därför att det inte finns något uppslag om vem gärningsmannen är, snabbt bli inaktuellt om det kommer fram nya vittnesuppgifter eller annan bevisning. Vidare bör givetvis en förundersökning



som har lagts ned för att den misstänkte har lämnat landet och inte kan förväntas återkomma kunna tas upp på nytt, om den misstänkte sedermera anträffas här i landet. Å andra sidan finns det andra situationer där man redan vid nedläggningsbeslutet kan konstatera att det inte finns några förutsättningar för att brottet ska kunna lagföras. Så blir t.ex. fallet om man vet att brottet förövats av en person som vid brottet var under 15 år eller av en person som senare har avlidit.

En regel som tar sikte på behandling av uppgifter i nedlagda förundersökningar i syfte att förundersökningen ska kunna tas upp på nytt bör därför utformas på ett sätt som tar större hänsyn till det enskilda fallet. Hänsyn måste för det första tas till brottets preskriptionstid, eftersom en förundersökning i princip kan återupptas när som helst, så länge brottet inte är preskriberat. För det andra bör hänsyn tas till om det, med hänsyn till omständigheterna, över huvud taget är lagligen möjligt att återuppta förundersökningen. Åklagare eller annan förundersökningsledare bör därför, i samband med nedläggningsbeslut, kunna ange om brottet trots nedläggningsbeslutet kan komma att bli föremål för lagföring.

#### *Tillgång till förundersökningar även efter angivna tidsfrister*

I undantagsfall kan det finnas behov av att kunna få tillgång till och använda uppgifter i en förundersökning som inte längre får behandlas på grund av de tidsbegränsningar som vi föreslår. Lagen bör därför ange i vilka situationer en sådan behandling trots allt ska vara möjlig. Det rör sig bl.a. om möjligheten att få tillgång till förundersökningar och andra utredningar som har överlämnats för arkivering. Undantag bör medges dels för fall där det är aktuellt att återuppta förundersökningen, dels för prövning av extraordinära rättsmedel. Vidare bör det finnas ett visst begränsat utrymme för behandling om uppgifterna behövs för utredning av allvarliga brott eller undersökning av allvarlig brottslig verksamhet. En sedan länge avslutad förundersökning

rörande mord, dråp, grova sexualbrott eller liknande kan vara intressant t.ex. om likartade brott begås och polisen söker efter en gärningsman. Vi föreslår därför att uppgifter i en förundersökning alltid ska få behandlas om det behövs för att en förundersökning ska återupptas eller för prövning av extraordinära rättsmedel samt, om det finns särskilda skäl, för utredning av allvarliga brott eller undersökning av allvarlig brottslig verksamhet. Med allvarlig brottslighet avser vi sådan som innefattar brott med fyra år eller mera i straffskalan.

En förutsättning för att en behandling ska vara möjlig i dessa fall är naturligtvis att uppgifterna i förundersökningen inte har gallrats enligt arkivlagens bestämmelser.

#### *Tillgång till brottsanmälningar som inte har lett till förundersökning*

En typ av uppgifter som förtjänar särskild reglering är anmälningar om brott. Ett stort antal brottsanmälningar leder till ett omedelbart beslut av polisen att inte inleda förundersökning. Skälet till detta är att det i flertalet fall saknas uppgifter om vem som kan misstänkas för brottet och att det inte heller i övrigt finns några uppgifter som kan bidra till utredningen om brottet. Detta utesluter emellertid inte att brottsanmälan kan aktualiseras senare, om det kommer fram nya omständigheter som kan leda till att brottet klaras upp, t.ex. om någon grips för likartade brott eller om gärningsmannen självmant erkänner brottet. Fram till den tidpunkt när brottet preskriberas finns det därför alltid ett latent behov av att kunna återuppta behandlingen av en brottsanmälan som inte har lett till förundersökning eller annan utredning. Mot den bakgrunden bör det inte införas några särskilda gallringsregler i den nya lagen för brottsanmälningar utan dessa bör, på samma sätt som förundersökningar, gallras efter de principer som anges i arkivlagen. Uppgifterna bör dock aldrig få behandlas i den brottsbekämpande verksamheten efter det att det

brott som anmälan avser har preskriberats. Vi föreslår en särskild bestämmelse om detta.

Vad som nu har sagts bör dock inte gälla för sådana brottsanmälningar som har avskrivits på den grunden att det inte har förekommit något brott. Bland sådana anmälningar finns bl.a. vad som brukar kallas okynnesanmälningar (som oftast sker i syfte att trakassera eller svärta ned den anmälda) och anmälningar som härrör från psykiskt störda personer, som inte sällan upplever att de utsätts för brott fastän så inte är fallet. Det skulle strida mot de allmänna principerna för behandling av personuppgifter i polisens verksamhet att tillåta en längre tids behandling av helt grundlösa brottsanmälningar. Dessa bör därför enligt huvudregeln inte kunna behandlas längre än vad som behövs för handläggningen.



# 17 Särskilda bestämmelser om vissa register

## 17.1 Allmänna utgångspunkter

**Promemorians förslag:** I den nya lagen införs särskilda bestämmelser om register med uppgifter om resultat av DNA-analyser. I lagen införs också särskilda bestämmelser om fingeravtrycksregister, signalementsregister och penningtvättsregister.

**Promemorians bedömning:** Det behöver inte i lagen tas in några särskilda bestämmelser om andra register som förs hos polisen. Det allmänna spaningsregistret bör regleras i en särskild lag.

**Utredningens förslag:** Överensstämmer delvis med promemorians förslag. Utredningen har dock föreslagit att även det allmänna spaningsregistret ska regleras särskilt i den nya lagen.

**Remissinstanserna:** De flesta remissinstanser har inte haft någon invändning mot utredningens förslag. *Datainspektionen* har ansett att även Rationell anmälningsrutin (RAR) bör författningsregleras. *Sveriges advokatsamfund* har ansett att särskilda regler bör övervägas beträffande ändamål, uppgiftsinnehåll och gallring när det gäller det digitala referensbiblioteket över barnpornografiska framställningar.

**Skälen för promemorians förslag och bedömning:** Utredningens förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet innehåller generella be-

stämmelser om i vilken utsträckning polisen får behandla personuppgifter i sådan verksamhet. Trots att utgångspunkten således har varit att åstadkomma en reglering med generell giltighet har utredningen föreslagit särbestämmelser för några av de nuvarande registren.

Målsättningen med vårt förslag är att i möjligaste mån undvika särregleringar av vissa speciella informationssamlingar eller viss personuppgiftsbehandling. Det huvudsakliga skälet för detta är, som vi närmare utvecklat i avsnitt 6.1, att den nya regleringen så långt som möjligt bör vara teknikneutral. Genom att utforma den nya lagen som en rättslig ram för vilka uppgifter som får behandlas och på vilket sätt uppgifterna får användas blir det möjligt för polisen att bygga upp datasystem som bättre tillgodoser både intresset av ett mer effektivt utnyttjande av informationen och intresset av att skydda enskildas personliga integritet. Inom den brottsbekämpande verksamheten finns det emellertid viss behandling av personuppgifter som svårigen låter sig inordnas under de generella bestämmelserna. Vi anser därför att det är nödvändigt att i några fall införa särskilda bestämmelser om vissa register. Dessa bestämmelser bör gälla i stället för de särskilda bestämmelser som vi har föreslagit ska gälla för gemensamt tillgängliga uppgifter.

Vi delar således utredningens uppfattning att det finns skäl att ha särskilda bestämmelser om dels register med uppgifter om resultat av DNA-analyser, dels fingeravtrycksregister och signalementsregister. Detsamma gäller enligt vår mening för behandling av uppgifter om misstänkt penningtvätt och misstänkt finansiering av särskilt allvarlig brottslighet i penningtvättsregister. Vi föreslår därför särskilda bestämmelser för dessa register.

Utredningen har också föreslagit att det allmänna spaningsregistret ska regleras särskilt. Vi delar utredningens uppfattning även i denna del. Vi anser emellertid att det registret bör regleras i en särskild lag och återkommer till den frågan i avsnitt 20.

Ett annat register, som det kan finnas anledning att nämna i detta sammanhang, är det centrala brottsspaningsregistret (se

*bilaga 6*). Det centrala brottspaningsregistret har till ändamål att skapa ett särskilt register över anmälda allvarligare brott och är avsett att utnyttjas för såväl spaning som brottsutredning.

En grundläggande fråga är om det finns något behov av det centrala brottspaningsregistret i polisens nya datamiljö, eller om detta på sikt kan ersättas med de nya möjligheter till behandling som öppnas genom förslaget till lag om personuppgiftsbehandling i polisens brottsbekämpande verksamhet. Enligt vår bedömning kommer de uppgifter som behandlas i centrala brottspaningsregistret i allt väsentligt att kunna behandlas även i fortsättningen, dock inte under lika lång tid. De gallringsregler som Rikspolisstyrelsen enligt uppgift tillämpar för registret medger att vissa uppgifter får bevaras under mycket lång tid, i vissa fall upp till 25 år. Vi anser att så långa gallringsfrister inte är lämpliga från integritetssynpunkt. Gamla uppgifter har dessutom begränsat värde från verksamhetssynpunkt eftersom de med tiden förlorar i aktualitet och adekvans. Mot den nu angivna bakgrunden har vi inte föreslagit några särskilda regler om det centrala brottspaningsregistret. Om det senare skulle visa sig att det finns ett påtagligt behov av att bevara visst slag av uppgifter, t.ex. om tillvägagångssätt vid brott (s.k. *modus operandi*), i brottanmälningar och förundersökningar under en längre tid än de i lagen föreslagna fristerna, bör regeringen kunna meddela föreskrifter om detta. Vi har i avsnitt 16.2 behandlat frågan om sådana föreskrifter bör meddelas för uppgifter som i dag finns i det barnpornografiregister som Rikspolisstyrelsen för.

I avsnitt 13 har vi behandlat frågor som rör sekretess, däribland sekretessen för uppgifterna i de särskilda register som vi diskuterar i detta kapitel.

## 17.2 Register med uppgifter om resultat av DNA-analyser

**Promemorians förslag:** Rikspolisstyrelsen får i särskilda register behandla uppgifter om resultatet av DNA-analyser för brottsbekämpande ändamål. Därutöver får sådana uppgifter behandlas för att underlätta identifiering av avlidna personer. Gallring ska ske på samma sätt som i dag.

**Utredningens förslag:** Överensstämmer i huvudsak med promemorians förslag. Sedan utredningen lämnade sitt förslag har dock bestämmelserna om DNA-register varit föremål för behandling i ett annat lagstiftningsärende, (se prop. 2005/06:29) och nya bestämmelser har trätt i kraft (SFS 2005:877).

**Remissinstanserna:** *Rikspolisstyrelsen* har föreslagit att DNA-register ska få innehålla uppgifter om resultatet av DNA-analyser som avser personer som har dömts till brott där fängelse ingår i straffskalan. *Riksarkivet* har föreslagit att det ska införas en möjlighet att föreskriva om undantag från gallring för historiska, vetenskapliga och statistiska ändamål.

**Skälen för promemorians förslag:** Nya bestämmelser om användning av DNA-analyser i brottmål trädde i kraft den 1 januari 2006 (prop. 2005/06:29). Bestämmelserna har tillämpats endast under en förhållandevis kort tid. Det har inte framkommit något som ger anledning att i detta sammanhang göra några mera omfattande ändringar i dem. Bestämmelserna i polisdatalagen om behandling av uppgifter som rör DNA bör därför i allt väsentligt oförändrade föras över till den nya lagen. I avsnitt 8 har vi redovisat skälen för att behandling av uppgifter om resultatet av DNA-analyser utanför registren bara får förekomma i förundersökningar.

Rikspolisstyrelsen har under hand påtalat att det finns ett behov av att kunna behandla uppgifter i DNA-registren även för att underlätta identifiering av avlidna personer som inte har utsatts för brott. Erfarenheterna från tsunamikatastrofen år 2004



visar att det finns ett sådant behov. Vi delar därför Rikspolisstyrelsens uppfattning. Behovet av att skydda den personliga integriteten gör sig inte heller lika starkt gällande när det är fråga om personer som inte längre är i livet. Vi föreslår därför att polisen genom en uttrycklig lagbestämmelse ges möjlighet att söka i DNA-register för att underlätta identifiering av avlidna personer även om detta inte sker i samband med utredning av brott.

*Riksarkivet* har föreslagit att det införs en möjlighet att föreskriva om undantag från gallring om det behövs för historiska, vetenskapliga och statistiska ändamål. Myndigheten framförde motsvarande synpunkt i det lagstiftningsärende som ledde fram till de nyss redovisade ändringarna (prop. 2005/06:29). I det ärendet föreslog myndigheten i första hand att gallringsbestämmelserna skulle utgå och att arkivlagen i stället ska gälla. Regeringen ansåg att gallringsbestämmelserna skulle kvarstå oförändrade i avvaktan på den pågående översynen av polisdatalagen (a. prop. sid. 32).

Vi konstaterar att syftet med de nu aktuella gallringsbestämmelserna är att skydda den enskildes personliga integritet. Detta intresse måste vägas mot intresset av att kunna behandla uppgifterna för historiska, vetenskapliga och statistiska ändamål när uppgifterna inte längre behövs i den brottsbekämpande verksamheten. Det historiska intresset av att behandla sådana referensuppgifter som finns i DNA-register måste typiskt sett vara litet jämfört med andra uppgifter som behandlas i den brottsbekämpande verksamheten. I det lagstiftningsärende som föregick polisdatalagen påpekade Riksarkivet att det inte finns något intresse av att bevara sådana uppgifter av historiska skäl (se prop. 1997/98:97 s 141). Vi kan inte heller se att de vetenskapliga eller statistiska intressen som eventuellt kan finnas skulle väga tyngre än integritetsintressena. Enligt vår bedömning finns det därför inte tillräckliga skäl att införa en möjlighet att föreskriva om undantag från gallringsbestämmelserna för DNA-registren.

I avsnitten 12.3.5 och 12.3.6 har vi behandlat frågan om direktåtkomst till registren. Det bör inte vara möjligt att lämna ut annat än enstaka uppgifter ur registren på medium för automa-

tisk behandling, utom i de fall där regeringen meddelat föreskrifter eller i ett enskilt fall beslutat att uppgifter får lämnas ut på sådant medium.

### 17.3 Fingeravtrycks- eller signalementsregister

**Promemorians förslag:** Bestämmelserna i polisdatalagen om ändamålet med och innehållet i fingeravtrycks- och signalementsregister förs i huvudsak oförändrade över till den nya lagen. Fingeravtrycks- och signalementsregister får dock i fortsättningen innehålla även uppgifter om brottskoder.

I den nya lagen tas in särskilda regler om gallring av uppgifter i fingeravtrycks- och signalementsregister. Gallringsfristen görs beroende av brottets svårhetsgrad.

**Utredningens förslag** överensstämmer delvis med promemorians förslag. Utredningen har dock föreslagit att även 31 § polisdatalagen, som innehåller bestämmelser om gallring av uppgifter i fingeravtrycks- och signalementsregister, ska föras över till den nya lagen.

**Remissinstanserna:** Flertalet remissinstanser har inte haft någon invändning mot utredningens förslag. *Riksarkivet* har föreslagit att det införs en möjlighet att föreskriva om undantag från kravet på gallring.

**Skälen för promemorians förslag:** I 29–31 §§ polisdatalagen finns bestämmelser om fingeravtrycks- och signalementsregister. Rikspolisstyrelsen får behandla uppgifter i sådana register för att underlätta identifiering av personer i samband med brott. Uppgifterna får vidare användas för identifiering av okända personer i andra fall. Sådana uppgifter får också behandlas i förundersökningar och särskilda undersökningar (29 §). I 30 § regleras under vilka förutsättningar som uppgifter får föras in i registren och vad registren får innehålla. Där sägs bl.a. att sådana register får innehålla endast uppgifter om den som är misstänkt eller dömd

för brott eller som har fått lämna fingeravtryck med stöd av en viss bestämmelse i lagen om särskild utlänningskontroll. Registren får inte innehålla uppgifter om fotografi och fingeravtryck som med stöd av lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare tagits av den som är under femton år. I registren får det endast antecknas uppgifter om fingeravtryck, signalement, identifieringsuppgifter och ärendenummer.

Bestämmelserna i 29–31 §§ polisdatalagen har dock i praktiken inte börjat tillämpas. Rikspolisstyrelsen för i stället ett fingeravtrycksregister och ett signalements- och känneteckensregister. Registren förs med stöd av datalagen och tillstånd från Datainspektionen enligt övergångsbestämmelserna till polisdatalagen (se *bilaga 6*). Det innebär att polisdatalagens bestämmelser inte gäller för registren. Polisdatalagens bestämmelser överensstämmer emellertid i stort med de föreskrifter som Datainspektionen har meddelat för registren. Gallringsbestämmelserna för signalements- och känneteckensregistret är dock något annorlunda utformade. Vi återkommer till detta i det följande.

I sammanhanget kan nämnas att Migrationsverket får föra ett register över fingeravtryck som tas med stöd av 9 kap. 8 § utlänningslagen (2005:716), se 9 § förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen.

Vi delar utredningens bedömning att man vid utformningen av den nya lagen bör utgå från de bestämmelser om registren som finns i den nu gällande lagen. Regleringen bör dock anpassas till den nya utformningen av polisens personuppgiftsbehandling i övrigt.

De personuppgifter som får förekomma i signalementsregister och fingeravtrycksregister kan inte anses vara så känsliga att man behöver begränsa behandlingen av uppgifterna till – som fallet är enligt gällande lag – enbart förundersökningar och särskilda undersökningar. Sådana uppgifter bör således få behandlas i polisens brottsbekämpande verksamhet i dess helhet. I avsnitten 12.3.5 och 12.3.6 har vi behandlat frågan om direktåtkomst till uppgifter ur de särskilda registren. I avsnitt 14 tar vi

upp frågan om det bör vara möjligt att lämna ut annat än enstaka uppgifter ur registren på medium för automatisk behandling.

Utredningen har föreslagit att registren ska få innehålla uppgifter om brottskoder. Sådana koder nämns inte i polisdatalagen bland de uppgifter som får registreras men får antecknas i signalements- och känneteckensregistret med stöd av ett beslut från Datainspektionen. Enligt vår mening finns det ett tydligt behov av att anteckna även brottskoder i signalementsregistret. Användningen av enbart uppgifter om signalement och andra kännetecken ger normalt ett alldeles för stort antal träffar i registret för att en sökning i registret ska vara effektiv. Genom att använda brottskoder vid sökningen kan man begränsa antalet träffar. Användandet av brottskoder innebär knappast heller några ytterligare risker för den enskildes personliga integritet. Tvärtom får det till följd att antalet träffar vid en sökning begränsas, något som från integritetsskyddssynpunkt är positivt. Den nya lagen bör därför enligt vår mening medge att brottskoder antecknas i de aktuella registren.

När det gäller frågan om vilka frister som ska gälla för gallring kan följande noteras. Enligt 31 § polisdatalagen ska uppgifter om en misstänkt person gallras när en förundersökning eller åtal mot personen läggs ned eller när åtal ogillas. Uppgifterna får dock bevaras längre om andra uppgifter om den misstänkte ska behandlas med stöd av polisdatalagens bestämmelser om behandling av kvarstående misstankar. Om den registrerade döms, ska uppgifterna gallras senast när uppgifterna om personen gallras ur belastningsregistret. Genom beslut i december 2005 meddelade Datainspektionen föreskrifter för fingeravtrycksregistret som överensstämmer med polisdatalagens gallringsbestämmelser. I juni 2006 meddelade myndigheten gallringsföreskrifter för signalements- och känneteckensregistret. Föreskrifterna bygger på ett förslag som Rikspolisstyrelsen lämnade i ärendet och tar sin utgångspunkt i brottets svårhetsgrad. Ett misstänkt brott av lindrigare karaktär innebär alltså att uppgifterna får behandlas under betydligt kortare tid än om det är fråga om ett allvarligt brott. Enligt vår mening är det lämpligt att utforma gallringsbe-

stämmelserna efter en sådan modell som både Rikspolisstyrelsen och Datainspektionen har funnit motiverad.

Mot bakgrund av vad som sagts ovan bör enligt vår bedömning följande gallringsfrister gälla. Om misstanken avser brott för vilket det strängaste straffet inte är mer än fängelse i två år, bör uppgifterna gallras senast tio år efter det att uppgift om personen behandlades första gången. Om det föreskrivs strängare straff för brottet, men inte strängare än fängelse i åtta år, bör gallringsfristen vara femton år och i de fall där det strängaste straffet för brottet är fängelse i mer än åtta år, bör gallringsfristen vara 25 år. Vid misstanke om nya brott ska redan registrerade uppgifter få bevaras utifrån vad den nya brottsmisstanken medger.

De angivna gallringsfristerna bör dock inte gälla när åtal mot den misstänkte har lagts ned eller när han eller hon har frikänts genom lagakraftvunnen dom. I sådana fall bör uppgifterna få sparas endast under en kortare tid. Den tiden bör bestämmas till tre månader. Detsamma bör gälla när förundersökningen mot en misstänkt har lagts ned.

Uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll bör gallras när uppgifterna inte längre behövs för ändamålet med behandlingen. På samma sätt som i dag bör regeringen ges möjlighet att meddela ytterligare föreskrifter om gallring för sådana fall.

*Riksarkivet* har föreslagit att det införs en möjlighet att föreskriva om undantag från gallring av samtliga uppgifter som behandlas i fingeravtrycks- och signalementsregister. Frågan måste avgöras efter en avvägning mellan å ena sidan intresset av att skydda den personliga integriteten och å andra sidan intresset av kunna bevara och behandla uppgifter för historiska, vetenskapliga och statistiska ändamål. När det gäller stora flertalet uppgifter som behandlas i polisens brottsbekämpande verksamhet har vi bedömt att intresset av att bevara uppgifter för historiska, vetenskapliga och statistiska ändamål väger tillräckligt tungt för att motivera ett sådant undantag som Riksarkivet har förordat.

När det gäller uppgifter i DNA-register har vi gjort den motsatta bedömningen. Beträffande uppgifter i fingeravtrycks- och signalementsregister kan vi inte se att det historiska, vetenskapliga och statistiska intresset av att bevara uppgifter i registren för framtiden är särskilt stort, eftersom uppgifterna främst utgör identifieringsuppgifter och inte berättar mycket om vår samtid. Integritetsintressena får anses väga tyngre. Därför bör det inte införas någon möjlighet att meddela föreskrifter om undantag från gallringsbestämmelserna.

## 17.4 Penningtvätsregister

**Promemorians förslag:** Rikspolisstyrelsen får behandla uppgifter i penningtvätsregister för att förebygga, förhindra och upptäcka

1. brottslig verksamhet där penningtvätt ingår som ett led för att dölja vinning av brott eller brottslig verksamhet, eller
2. brottslig verksamhet som innefattar brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

Uppgifterna ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att uppgifter ska bevaras under längre tid för historiska, statistiska eller vetenskapliga ändamål.

**Utredningens förslag:** Utredningen har inte lämnat något förslag i detta avseende.

**Remissinstanserna** har inte berört frågan.

**Skälen för promemorians förslag:** Fysiska och juridiska personer som omfattas av lagen (1993:768) om åtgärder mot penningtvätt är enligt 9 § samma lag skyldiga att granska alla trans-

aktioner som skäligen kan anses utgöra penningtvätt samt att under vissa förutsättningar följa upp denna granskning med en anmälan till Rikspolisstyrelsen. Inom Rikspolisstyrelsen har Finanspolisen pekats ut som ansvarig för hanteringen av uppgifter som anmäls enligt den lagen. Finanspolisen ska alltså ta emot anmälningar om penningtvätt.

Med penningtvätt avses enligt lagen om åtgärder mot penningtvätt sådana åtgärder med avseende på egendom som har förvärvats genom brott som kan medföra att denna egenskap hos egendomen fördöljs, att den brottslige får möjlighet att undandra sig rättsliga påföljder eller att återskaffandet av egendomen försvåras, samt sådana åtgärder som innefattar förfogande över och förvärv, innehav eller brukande av egendomen. Med penningtvätt avses även åtgärder med annan egendom än som nyss nämnts, om åtgärderna är ägnade att dölja att någon har berikat sig genom brottslig gärning. Penningtvätt utgör inget självständigt brott. De förfaranden som enligt lagen utgör penningtvätt är straffbelagda i 9 kap. 6–7a §§ brottsbalken som häleri eller penninghäleri.

Den som är anmälningspliktig enligt lagen om åtgärder mot penningtvätt är även skyldig att granska transaktioner som skäligen kan antas avse tillgångar som är föremål för brott enligt lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m. (terrorismfinansieringslagen). Därvid ska, på motsvarande sätt som gäller för penningtvätt, uppgifter lämnas till Finanspolisen om omständigheter som kan tyda på att en transaktion avser tillgångar som är föremål för brott enligt lagen. Terrorismfinansieringslagen innehåller bestämmelser som genomför konventionen om bekämpande av finansiering av terrorism (SÖ 2002:44).

De uppgifter som Finanspolisen tar emot av anmälningspliktiga organ behandlas i dag i ett särskilt analys- och spaningsregister (se *bilaga 6*). När Finanspolisen tar emot en uppgift är det inte klarlagt om den transaktion som uppgiften avser överhuvudtaget utgör brott eller brottslig verksamhet. Även om sådana uppgifter i och för sig torde rymmas inom de allmänna ändamå-

len med lagen i 2 kap. 5 och 7 §§, har de alltså inte det nödvändiga sambandet med konkreta brott eller med brottslig verksamhet som krävs för att få göra uppgifterna gemensamt tillgängliga. Det kan ibland krävas omfattande bearbetning av de anmälda uppgifterna innan transaktionerna kan knytas till brott eller brottslig verksamhet. För att behandlingen ska ha rättsligt stöd föreslår vi särskilda bestämmelser för den behandling som Finanspolisen utför i detta avseende.

Inom ramen för arbetet med att bekämpa penningtvätt och finansiering av särskilt allvarlig brottslig verksamhet tar Finanspolisen även emot uppgifter om misstänkta transaktioner från motsvarande enheter vid utländska myndigheter. Vidare tar Finanspolisen emot underrättelseinformation från övriga polisen och andra myndigheter samt uppgifter i anmälningar och tips från allmänheten. Den nya lagen bör ge stöd även för sådan behandling.

I den nya lagen bör således tas in bestämmelser som ger Rikspolisstyrelsen möjlighet att behandla uppgifter i särskilda register för att förebygga, förhindra och upptäcka dels brottslig verksamhet där penningtvätt utgör ett led för att dölja vinning av brott eller brottslig verksamhet, dels brottslig verksamhet som innefattar brott enligt 3 § terrorismfinansieringslagen. Den nuvarande benämningen på registret, ”analys- och spaningsregister”, ger inte någon information om vad som skiljer detta register från andra register i polisens brottsbekämpande verksamhet. Ett sådant register bör därför i fortsättningen lämpligen benämnas *penningtvättsregister*.

Vid Finanspolisen tjänstgör i dag ca 15 personer och det är endast dessa personer som har åtkomst till uppgifterna i det aktuella registret. Rikspolisstyrelsen har under hand uppgett att det även i framtiden kommer att vara endast ett fåtal personer inom polisen som behöver ha tillgång till uppgifterna för att kunna utföra sina arbetsuppgifter. Med hänsyn till detta behöver det inte införas några bestämmelser om särskilda upplysningar eller om sökbegränsningar i fråga om uppgifter som behandlas i Finanspolisens penningtvättsregister.



När det gäller gallring behövs dock särskilda regler. I lagen om åtgärder mot penningtvätt finns föreskrifter om under hur lång tid vissa uppgifter ska bevaras. En särskild gallringsbestämmelse som tar hänsyn till dessa bestämmelser bör tas in i den nya lagen. Andra uppgifter bör gallras när det står klart att uppgifterna inte längre behövs i den brottsbekämpande verksamheten.

Regeringen eller den myndighet som regeringen bestämmer bör få meddela föreskrifter om att uppgifter trots gallringsbestämmelsen ska bevaras för historiska, statistiska eller vetenskapliga ändamål. En motsvarande reglering föreslås för behandling av uppgifter för liknande ändamål i andra delar av lagen, nämligen för att förebygga, förhindra och upptäcka brottslig verksamhet. Det finns inte skäl att föreslå någon annan lösning för den behandling som sker med anledning av misstänkt penningtvätt m.m.

Som framgår av avsnitt 12.3.5 anser vi att penningtvättsregister är av sådan art att andra myndigheter inte bör kunna få direktåtkomst till ett sådant register. Det bör inte heller vara möjligt att lämna ut annat än enstaka uppgifter ur ett sådant register på medium för automatisk behandling, utom i de fall där regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat att uppgifter får lämnas ut på sådant medium.



# 18 Behandling av personuppgifter i Säkerhetspolisens brottsbe- kämpande verksamhet

## 18.1 Bakgrund

### 18.1.1 Säkerhetspolisens organisation och uppgifter

Säkerhetspolisen hör till Rikspolisstyrelsen men har en egen organisation. Av 4 § förordningen (1989:773) med instruktion för Rikspolisstyrelsen framgår att Säkerhetspolisen bedriver polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet m.m. I förordningen (2002:1050) med instruktion för Säkerhetspolisen preciseras dess uppgifter och organisation. Utöver att förebygga och avslöja brott mot rikets säkerhet ska Säkerhetspolisen bl.a. bekämpa terrorism, skydda personer i den centrala statsledningen och fullgöra de uppgifter som följer av säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Den verksamhet som bedrivs hos Säkerhetspolisen syftar till att skydda det demokratiska systemet, medborgarnas fri- och rättigheter och den nationella säkerheten.

Säkerhetspolisens verksamhet delas i dag in i fem huvudområden. *Kontraspionageverksamheten* har till uppgift att förebygga och avslöja spioneri, olaglig underrättelseverksamhet och andra brott mot rikets säkerhet. För att förebygga och avslöja olaglig underrättelseverksamhet mot Sverige och svenska intressen bedriver myndigheten operativt fältarbete samt arbetar med analyser och kontakter med olika delar av det svenska samhället. I

arbetet ing ar ocks a att avsl oja flyktingspionage och annan f rf ljelse av utl anningar i Sverige fr n utl andska regimer och organisationer som f rknippas med politiskt motiverat v ld.

Inom *kontraterroismverksamheten* har S akerhetspolisen till uppgift att f rebygga och avsl oja terrorism som riktas mot Sverige eller utl andska intressen h r i landet, terroristhandlingar i andra l nder samt f rekomsten av internationella terroristn tverks f rgreningar i Sverige. I denna verksamhet ing ar ocks a att f rebygga och utreda brott vid handel med produkter som kan anv ndas f r att framst lla massf rst relsevapen.

S akerhetspolisens *f rfattningsskyddande verksamhet* syftar till att f rebygga och avsl oja brott mot rikets inre s akerhet, dvs. olaglig verksamhet som syftar till att med v ld, hot eller tv ng  ndra v rt statsskick, f rm  beslutande politiska organ eller myndigheter att fatta beslut i en viss riktning eller att hindra enskilda medborgare fr n att ut va sina grundlagsf sta fri- och r ttigheter. Inom ramen f r den f rfattningsskyddande verksamheten kartl ggs ocks a brott som anv nds som medel f r att uttrycka en politisk  sikt eller f r att uppn  ett politiskt m l.

Hos S akerhetspolisen bedrivs  ven *personskyddsverksamhet* som handlar om bevaknings- och s akerhetsarbete. Verksamheten omfattar skyddet av den centrala statsledningen. Till den centrala statsledningen r knas statschefen, riksdagen, regeringen samt statssekreterarna och kabinetssekreteraren. I kretsen av personer som ska skyddas ing r  ven personer som vistas h r i samband med statsbes k och de som omfattas av s.k. annat personskydd. Med det sistn mnda avses skydd som S akerhetspolisen handhar efter s rskilt beslut, s som betr ffande kungafamiljen och fr mmande stats beskickningsmedlemmar.

Inom *s akerhetsskyddsverksamheten* ger S akerhetspolisen r d till och kontrollerar myndigheter och f retag f r att skydda hanteringen av uppgifter som har betydelse f r rikets s akerhet och f r att f rebygga terrorism. I arbetet ing r att genomf ra registerkontroll (tidigare ben mnt personalkontroll) efter framt llan fr n ber rda myndigheter eller i vissa fall annan stat eller mellanfolklig organisation.

Tyngdpunkten i S kerhetspolisens verksamhet ligger p  brottsf rebyggande arbete.

### 18.1.2 Nuvarande behandling av personuppgifter hos S kerhetspolisen

#### *Allm nt*

S kerhetspolisens behandling av personuppgifter sker med st d av bestämmelserna i personuppgiftslagen och den allm nna delen av polisdatalagen (1–9 och 13 §§). Ut ver detta finns det s rskilda bestämmelser om det s.k. S APO-registret i 32–35 §§ polisdatalagen och 12 och 13 §§ polisdataf rordningen. Best mmelserna inneb r att det ska f ras ett S APO-register som har till  ndam l att underl tta spaning i syfte att f rebygga och avsl ja brott mot rikets s kerhet och bek mpa terroristbrott samt utg ra underlag f r registerkontroll enligt s kerhetsskyddslagen. I lagen anges vilka uppgifter som f r f ras in i registret. Det finns ocks  bestämmelser om gallring. Best mmelserna i 10 och 11 §§ polisdatalagen om behandling av uppgifter om kvarst ende misstankar och 14–21 §§ om kriminalunderr ttelseverksamhet g ller d remot inte f r S kerhetspolisen.

En n rmare beskrivning av de databaser och  rendehanteringssystem som i dag f rs hos S kerhetspolisen finns i *bilaga 6*. D r framg r att den databas som huvudsakligen anv nds hos S kerhetspolisen  r S kerhetspolisens centralregister och att det vid sidan av denna f rs olika s rskilda uppgiftssamlingar f r bearbetning och analys (s.k. analysdatabaser). D rut ver f rs vissa diarium. S APO-registret anv nds inte l ngre. Registret f rs endast f r att uppfylla kravet i polisdatalagen p  att ett s dant register ska finnas. Best mmelserna om S APO-registrets  ndam l, inneh ll och gallring till mpas dock i fr ga om den personuppgiftsbehandling som sker i centralregistret.

Centralregistret kan s gas utg ra ing ngen till de samlade personuppgifter som finns lagrade hos S kerhetspolisen. Samti-

digt utg r registret ett arbetsverktyg. Beh riga befattningshavare f r in uppgifter i registret genom att bearbeta avslutade  renden och g r uppgifterna s kbara med st d av sammanst llningar och s rskilt utarbetade kodnycklar. Endast s dana uppgifter som enligt 33 och 34    polisdatalagen f r finnas i S PO-registret registreras. De flesta av personuppgifterna f rs in i registret p  den grunden att det med h nsyn till registrets  ndam l finns s rskilda sk l till det (33   f rsta stycket 3). Vid s kning visas endast identifieringsuppgifter, uppgifter om grunden f r registreringen och h nvisningar till de  renden d r uppgifter om den registrerade behandlas (34  ). S kerhetspolisen har i samr d med Registern mnden kommit  verens om de n rmare grunderna f r n r registrering av k nsliga uppgifter ska f  ske.

De enskilda handlingarna i varje  rende  terfinns inte i centralregistret men kan n as via registret genom en s kning p   rendet. I varje  rende finns det uppgift om uppgiftsl mnarens tillf rlitlighet. D r anges vidare om uppgifterna bygger p  uppgiftsl mnarens egna iakttagelser eller om det  r fr ga om andrahandsuppgifter. Dessutom klassificeras uppgifternas tillf rlitlighet enligt ett s rskilt system. Handlingarna och  rendena lagras digitalt i en databas som  r kopplad till registret. I centralregistret f r den t njesteman som utf r s kningen s rskilt ange om han eller hon vill  ppna n got av de  renden som det h nvisas till. En f ruts ttning f r att  rendet ska g  att  ppna  r att t njestemannen i fr ga har beh righet att g ra det. Det  r inte m jligt att utf ra fritexts kningar i handlingarna eller  rendena.

Tillg ngen till uppgifter i centralregistret begr nsas till vad var och en beh ver f r att kunna utf ra sina arbetsuppgifter (jfr 13   polisdataf rordningen). F r att f  beh righet till registret m ste personalen genomg  en utbildning som avslutas med ett prov. Efter godk nt prov f r den enskilde beh righet att anv nda registret. Beh righeten delas upp i olika niv er beroende p  vilka behov den anst llde har.

Alla transaktioner och fr gor i centralregistret loggas. Enhetscheferna kontrollerar regelbundet den egna personalens

loggningar i centralregistret. Daglig kontroll av all uppdatering som g rs i centralregistret utf rs av en s rskild enhet.

Beslut om nyregistrering av en fysisk eller juridisk person i centralregistret fattas av den enhetschef som ansvarar f r dokumentation. N r det g ller beslut om registrering av personer som  nnu inte fyllt 15  r fattas beslutet genom s rskild anteckning p  handlingen. Nyregistrering av en s dan person ska tillstyrkas av enhetschefen inom ber rd verksamhetsgren. Om en enhetschef inom en verksamhetsgren fattat beslut om komplettering av en k nslig personuppgift enligt 5   polisdatalagen ska beslutet  verpr vas av den enhetschef som ansvarar f r dokumentation. Beslutet, med angivande av sk l samt utg ngen av  verpr vningen, antecknas s rskilt p  den ifr gavarande handlingen.

Gallring genomf rs av enheten f r dokumentation efter yttrande fr n ansvarig enhet. Den ansvariga enheten bevakar sp rrtiden och beg r vid behov f rl ngd sp rrtid enligt 35   f rsta stycket polisdatalagen.

### *Analysdatabaser*

F r bearbetning och analys av olika underr ttelser behandlas personuppgifter hos S kerhetspolisen  ven i avgr nsade uppgiftssamlingar som ben mns analysdatabaser. En s rskild form av analysdatabas  r det analysverktyg som anv nds f r att behandla uppgifter som inh mtats genom hemlig teleavlyssning eller hemlig tele vervakning. Det r ttsliga st det f r att f ra analysdatabaser finns i personuppgiftslagen och den allm nna delen av polisdatalagen. Innan en analysdatabas f r skapas, kr vs det tillst nd fr n personuppgiftsombudet. Tillst ndet ompr vas  rligen.

Ett beslut om att inr tta en analysdatabas fattas av enhetschefen som ansvarar f r dokumentation. Beslutet ska ange databasens namn, personuppgiftsbehandlingens inneh ll, ansvarig enhetschef,  ndam let med behandlingen, rutiner f r uppdatering i centralregistret, hur l ng tid tillst ndet g ller och vilka  t-

gärder som vidtagits för att trygga säkerheten vid behandlingen. Ansvarig enhetschef ska förvissa sig om att databasen uppfyller förutsättningarna enligt 5 § polisdatalagen. De uppgifter i en analysdatabas som är av betydelse för registerkontroll och de uppgifter som av spanings skäl behöver göras tillgängliga för flera än de personer som har tillgång till analysdatabasen ska, när det finns grund för registrering, tillföras centralregistret. Kontrollen av att uppgifterna i en analysdatabas hanteras i enlighet med det särskilda tillståndet utförs av personuppgiftsombudet tillsammans med enhetschefen som ansvarar för dokumentation. Sådan kontroll sker dels stickprovvis, dels i samband med ansökan om förlängningen av tillståndet. Den enhet som ansvarar för analysdatabasen gallrar uppgifterna i databasen när de inte längre behövs för databasens ändamål och erforderliga anteckningar har överförts till centralregistret. Uppgifterna gallras senast när tillståndet för databasen upphör.

#### *Extern kontroll av personuppgiftsbehandlingen*

Registernämnden har till uppgift att granska Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen, särskilt med avseende på 5 § som gäller behandling av känsliga personuppgifter (se 1 § förordningen (2006:1076) med instruktion för Registernämnden).

Registernämndens granskning utförs såväl löpande i samband med enskilda registerkontrollärenden som vid särskilda granskningstillfällen vid olika enheter inom Säkerhetspolisen. Registernämnden går då igenom de olika verksamhetsområdena, genomför stickprov och granskar samtliga nyregistreringar i centralregistret inom området under en viss tid. Resultatet av granskningen redovisas årligen i nämndens verksamhetsberättelse.

Registernämnden har i sitt remissyttrande över Polisdatautredningens betänkande framhållit att möjligheterna att kontrollera tillåtligheten av personuppgifter i en analysdatabas och att



åstadkomma rättelse i enskilda fall i praktiken torde vara mycket begränsade. Nämnden har vidare ifrågasatt om de regler som utredningen föreslår är tillräckliga för att förhindra otillåten behandling av känsliga personuppgifter.

Säkerhetspolisen har, efter det att yttrandet avgavs, i samråd med Registernämnden utarbetat en särskild rutin för registreringen av känsliga personuppgifter. Syftet med detta är att undvika att känsliga personuppgifter behandlas i strid med gällande regler. Av den senaste verksamhetsberättelsen för Registernämnden, som avser år 2006, framgår att nämnden inte har gjort några iakttagelser som tyder på att registrering sker i strid med vad som är föreskrivet.

## 18.2 Behovet av särskilda bestämmelser för personuppgiftsbehandling hos Säkerhetspolisen

**Promemorians förslag:** Särdragen i Säkerhetspolisens verksamhet motiverar att det i den nya lagen införs särskilda bestämmelser för behandlingen av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet.

**Utredningens förslag:** Utredningen har föreslagit ett mindre antal särbestämmelser för Säkerhetspolisen.

**Remissinstanserna** har inte haft något att invända mot utredningens förslag.

**Skälen för promemorians förslag:** Verksamheten hos Säkerhetspolisen bedrivs i stor utsträckning på liknande sätt som verksamheten vid polisen i övrigt. Detta gör att den reglering som vi föreslår för polisen i övrigt i många avseenden bör kunna tillämpas även på Säkerhetspolisens verksamhet. Exempelvis bör det även för Säkerhetspolisens del göras en uppdelning på behandling av uppgifter som gjorts gemensamt tillgängliga och annan behandling. Likaså bör det finnas bestämmelser om t.ex. ändamål, sökning och gallring. Särdragen i Säkerhetspolisens

verksamhet motiverar dock att vissa bestämmelser, liksom hitills, utformas på ett sätt som är särskilt anpassat till denna verksamhet. I motsats till vad som gäller för polisen i övrigt är Säkerhetspolisens brottsutredande verksamhet mycket liten. Tyngdpunkten ligger i stället på underrättelseverksamhet och renodlat förebyggande arbete. Nedan redovisas i vilken utsträckning vi bedömer att särbestämmelser är befogade.

### 18.3 Den nya regleringen i huvuddrag

**Promemorians bedömning:** Bestämmelserna i den nya lagen om Säkerhetspolisens behandling av personuppgifter bör i huvudsak ha samma innebörd som i dag. De nuvarande bestämmelserna om det s.k. SÄPO-registret bör emellertid inte föras över till den nya lagen.

**Utredningens bedömning** överensstämmer i huvudsak med promemorians bedömning.

**Remissinstanserna:** *Registernämnden* har vitsordat att SÄPO-registret inte längre behöver föras i den form som den nuvarande polisdatalagen kräver.

**Skälen för promemorians bedömning:** Vi bedömer att Säkerhetspolisen har behov av att även i fortsättningen kunna behandla personuppgifter på i huvudsak det sätt som sker i dag. Utöver de föreskrifter som finns i lag och förordning har Säkerhetspolisen utarbetat interna bestämmelser för att garantera ett starkt dataskydd för den enskilde som registreras. Skyddet kontrolleras och utvärderas löpande såväl inom myndigheten som av *Registernämnden*. Sammantaget innebär det att vederbörliga integritetsskyddsintressen i dag tillgodoses väl vid Säkerhetspolisens personuppgiftsbehandling.

Liksom utredningen bedömer vi därför att de bestämmelser som finns i polisdatalagen i huvudsak utgör en lämplig reglering av Säkerhetspolisens verksamhet. Vi anser dock, liksom utred-

ningen, att den nya lagen inte bör innehålla några särskilda bestämmelser om SÄPO-registret. Ett skäl för det är att bestämmelserna om detta har visat sig inte fylla något egentligt syfte. Ett annat skäl är att den nya lagen i så stor utsträckning som möjligt bör vara teknikneutral och reglera behandlingen av personuppgifter, inte arbetsmetoderna. Den nya lagen bör alltså, som huvudregel, inte innehålla bestämmelser om vilka register som får föras. Den ska, på samma sätt som för polisen i övrigt, reglera all behandling av personuppgifter. Lagen bör innehålla särskilda bestämmelser om uppgifter som görs eller har gjorts gemensamt tillgängliga. Dessa bestämmelser syftar, på samma sätt som regleringen av SÄPO-registret, till att skydda den personliga integriteten för berörda personer, bl.a. genom att begränsa åtkomsten till och möjligheten att söka bland de behandlade uppgifterna och genom att säkerställa att det tydligt framgår varför en personuppgift behandlas.

Liksom nuvarande bestämmelser bör bestämmelserna i den nya lagen endast ge ramen för den tillåtna personuppgiftsbehandlingen hos Säkerhetspolisen. Någon detaljreglering av villkoren för behandlingen bör alltså inte införas. En förutsättning för att en sådan modell ska vara acceptabel från integritetsskyddssynpunkt är emellertid att verksamheten fortlöpande kontrolleras av någon med särskild insyn i verksamheten. Historiskt sett har bristen på insyn i Säkerhetspolisens verksamhet varit ett problem, se t.ex. betänkandet Rikets säkerhet och den personliga integriteten (SOU 2002:87). Frågan har dock kommit i ett annat läge efter Registernämndens tillkomst. Registernämnden har bl.a. till uppgift att granska Säkerhetspolisens behandling av uppgifter enligt polisdatalagen, särskilt med avseende på 5 § som avser känsliga personuppgifter. Den tillsyn som Registernämnden bedriver utgör en bra grund för att värna integritetsskyddet. I avsnitt 19 redogörs också för den ”dubbla” tillsyn som Säkerhetspolisens verksamhet är underkastad, dels av Datainspektionen, dels av Registernämnden. Det är angeläget att denna tillsyn, som fungerar väl, behålls. Som utvecklas närmare i avsnitt 19 har regeringen nyligen föreslagit att Registernämndens till-

synsuppgift  verf rs till en ny n mnd, S kerhets- och integritetsskyddsn mnden, se prop. 2006/07:133. F rslaget inneb r en ut kad tillsyn.

## 18.4  ndam len med behandlingen

### 18.4.1 Tydliga och konkreta  ndam l

**Promemorians f rslag:** I lagen anges utt mmande f r vilka  ndam l S kerhetspolisen f r behandla personuppgifter i den brottsbek mpande verksamheten.

**Utredningens f rslag:**  ven utredningen har f reslagit en utt mmande reglering av till tna  ndam l f r behandlingen.

**Remissinstanserna** har inte haft n gon inv ndning mot utredningens f rslag.

**Sk len f r promemorians f rslag:** Som vi har angett ovan i avsnitt 7.1 avseende polisen i  vrigt b r den nya lagen utt mmande ange de  ndam l f r vilken behandling f r ske i polisens brottsbek mpande verksamhet. Detta b r g lla  ven f r S kerhetspolisen. Lagen b r s ledes ange dels de prim ra  ndam l f r vilka S kerhetspolisen f r behandla personuppgifter, dels i vad m n personuppgifter f r behandlas f r att tillhandah lla information till andra. De n rmare  ndam l f r vilka behandling b r f  ske redovisas i avsnitten 18.4.2 och 18.4.3 nedan.

## 18.4.2 Primära ändamål

**Promemorians förslag:** Personuppgifter ska få behandlas i Säkerhetspolisens verksamhet endast om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, terroristbrott samt vissa yttrandefrihetsbrott och tryckfrihetsbrott,

2. utreda eller beivra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,

3. fullgöra bevaknings- och säkerhetsarbete avseende personskydd,

4. fullgöra uppgifter som följer av säkerhetsskyddslagen (1996:627),

5. fullgöra de förpliktelser som följer av internationella åtaganden och

6. lämna tekniskt biträde till Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket.

**Utredningens förslag:** Överensstämmer delvis med promemorians förslag. Utredningen har föreslagit att Säkerhetspolisen ska få behandla personuppgifter för att underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet, spaning i syfte att bekämpa terrorism samt registerkontroll enligt säkerhetsskyddslagen.

**Remissinstanserna** har inte haft någon invändning mot utredningens förslag.

### Skälen för promemorians förslag

#### *Allmänna utgångspunkter*

Som har konstaterats i föregående avsnitt bör all personuppgiftsbehandling i Säkerhetspolisens brottsbekämpande verksamhet omfattas av den nya lagen. De ändamål för vilka Säkerhetspolisen

har behov av att behandla personuppgifter framgår av ett antal olika lagar. För det första bör Säkerhetspolisen, liksom idag, få behandla personuppgifter för att förebygga, förhindra, upptäcka och utreda de typer av brott som hör till Säkerhetspolisens ansvarsområde. För det andra måste Säkerhetspolisen ha möjlighet att behandla personuppgifter inom ramen för det brottsbekämpande arbete som hör samman med personskydd. För det tredje måste Säkerhetspolisens ha möjlighet att behandla personuppgifter i den utsträckning det behövs för att man ska kunna fullgöra sina uppgifter enligt säkerhetsskyddslagen. Slutligen måste regleringen ge Säkerhetspolisen tillräckligt utrymme att delta i internationellt samarbete och lämna tekniskt biträde åt andra brottsbekämpande myndigheter, bl.a. vid verkställighet av hemliga tvångsmedel.

Som tidigare påpekats skiljer sig Säkerhetspolisens uppgifter delvis från den övriga polisens, vilket innebär att ändamålen måste utformas på ett något annorlunda sätt. I de delar där uppgifterna i huvudsak är desamma bör man dock sträva efter att göra regleringen så likformig som möjligt.

*Förebygga, förhindra eller upptäcka brott mot rikets säkerhet och terroristbrott*

En av Säkerhetspolisens viktigaste uppgifter är att förebygga, förhindra och upptäcka brott mot rikets säkerhet. Vidare ansvarar Säkerhetspolisen för att förebygga, förhindra och upptäcka dels terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, dels brott mot lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m. (terrorismfinansieringslagen) samt eventuella andra former av terroristbrott. Säkerhetspolisen måste på samma sätt som i dag kunna behandla personuppgifter för att fullgöra denna verksamhet.

Rikspolisstyrelsen har med stöd av 13 § första stycket 10 förordningen (1989:773) med instruktion för Rikspolisstyrelsen

meddelat f reskrifter bl.a. om i vilka fall S kerhetspolisen ska leda eller medverka i f runders kningar (Rikspolisstyrelsens f reskrifter och allm nna r d om skyldighet f r polismyndigheterna att underr tta S kerhetspolisen om vissa brottsmisstankar m.m.; RPSFS 1999:10, FAP 403-3). Eftersom S kerhetspolisen enligt dessa f reskrifter i vissa fall leder eller  r delaktig i f runders kningar avseende vissa yttrandefrihets- eller tryckfrihetsbrott (brott med rasistiska och fr mlingsfientliga motiv), torde myndigheten  ven ha r tt och skyldighet att f rebygga, f rhindra och uppt cka s dana brott. S kerhetspolisen b r d rvid ocks  kunna behandla personuppgifter n r detta beh vs.

Inom b de kontrapionageverksamheten och f rfattningsskyddsverksamheten har S kerhetspolisen behov av att kunna samla in, sammanst lla och analysera uppgifter  ven om dessa inte kan h nf ras vare sig till n got visst konkret brott eller till n gon mer konkret definierad brottslig verksamhet. Som exempel kan n mnas behovet att inom kontrapionaget fortl pande kunna f lja utvecklingen n r det g ller andra nationers n rvaro i form av underr ttelseagenter h r i landet, att kunna  vervaka s dana personer och att d rvid  ven behandla personuppgifter. S kerhetspolisen har ocks  behov av att, med utg ngspunkt i svenska intressen, f lja den politiska utvecklingen i andra l nder och verksamheten inom vissa grupper, som kan utg ra ett hot mot det svenska samh llet eller som kan komma att g ra sig skyldiga till terroristbrott. Inom f rfattningsskyddet kan S kerhetspolisen exempelvis beh va kartl gga hot som riktar sig mot vissa grupper i samh llet och fortl pande f lja den hotbild som finns mot vissa myndigheter eller organ. Inom ramen f r detta arbete har S kerhetspolisen behov av att kunna dokumentera och analysera b de information av underr ttelsekarakt r och annan information av olika slag, s v l fr n offentliga k llor som fr n polisens eget arbete. S kerhetspolisens behov av att kunna genomf ra och dokumentera olika typer av unders kningar och analyser av f reteelser, personer, platser etc.  r s ledes stort och skiljer sig i flera avseenden fr n det behov som finns inom den  vriga polisen. Den stora skillnaden  r att det inom S kerhets-

polisens brottsf rebyggande arbete inte g r att urskilja lika tydliga kopplingar till konkreta brott eller till brottslig verksamhet som inom den  ppna polisen. Man kan uttrycka det s  att den underr ttelseverksamhet som bedrivs inom S kerhetspolisen till sin natur ofta  r s dan att den ligger p  ett tidigare stadium  n den som bedrivs av polisen i  vrigt.   andra sidan  r den, genom S kerhetspolisens instruktion, inriktad mot ett f tal, v l avgr nsade f reteelser av s rskilt samh llsfarlig karakt r.

Vad som nu har sagts hindrar inte att  ndam lsbest mmelsen i denna del utformas p  samma s tt som den motsvarande  ndam lsbest mmelsen avseende personuppgiftsbehandling i polisens  vriga verksamhet. Den b r dock begr nsas s  att den enbart omfattar de typer av brott som S kerhetspolisen enligt f rfattning ansvarar f r.

#### *Utreda och beivra brott mot rikets s kerhet och terroristbrott m.m.*

S kerhetspolisen handl gger ett mindre antal f runders kningar per  r (f r n rvarande drygt ett hundratal) och endast ett f tal av dessa leder till lagf ring. Detta h r bl.a. samman med att verksamheten till allra st rsta delen best r av underr ttelsearbete. Underr ttelsearbetet leder ibland inte fram till misstanke om ett s  konkret brott att f runders kning inleds. I andra fall avslutas en inledd f runders kning t.ex. d rf r att den person som miss-tankarna riktar sig mot har l mnat Sverige.

N r det har beg tts brott av det slag som S kerhetspolisen b r ett prim rt ansvar f r att bek mpa, bitr der S kerhetspolisen  klagaren med genomf randet av f runders kningen. Inom ramen f r den verksamheten har S kerhetspolisen i princip samma behov av att kunna behandla personuppgifter som den  vriga polisen.  ndam lsbest mmelsen b r utformas s  att den knyter an till de typer av brott som S kerhetspolisen ansvarar f r.

I ett enskilt fall kan S kerhetspolisen fatta beslut om att f runders kningen betr ffande n gon annan typ av brott  n de nyss



nämnda antingen ska bedrivas hos Säkerhetspolisen eller under medverkan av Säkerhetspolisen. Vid vissa typer av brott ska Säkerhetspolisen alltid underrättas (se RPSFS 1999:10, FAP 403–3). Syftet med det är att Säkerhetspolisen ska kunna överväga att ta över utredningen eller att medverka i utredningen med sin expertis. Om åklagare är förundersökningsledare föregås normalt sådana beslut av samråd, eftersom åklagaren kan ha synpunkter på vilken polisenhet som bör biträda honom eller henne med förundersökningsarbetet. Säkerhetspolisen måste naturligtvis kunna behandla personuppgifter i sådana förundersökningar i samma utsträckning som i andra fall. Detta bör framgå direkt av lagen.

#### *Bevaknings- och säkerhetsarbete avseende personskydd*

Säkerhetspolisens personskyddsverksamhet syftar ytterst till att förhindra att den person som skyddas utsätts för brott riktade mot dennes person. Den får därför anses utgöra en del av Säkerhetspolisens brottsbekämpande verksamhet. Inom ramen för detta förebyggande arbete har Säkerhetspolisen behov av att kunna samla in, bearbeta och bevara personuppgifter inte bara rörande den person som skyddas utan också om andra personer, exempelvis sådana som kan utgöra ett potentiellt hot, även om det inte finns någon konkret misstanke om brott eller brottslig verksamhet. Beträffande personer som ständigt har personskydd är behovet av att systematiskt hantera uppgifter större än när det gäller personer som tillfälligt har sådant skydd.

Vi föreslår mot denna bakgrund att det i den nya lagen uttryckligen anges att Säkerhetspolisen får behandla personuppgifter för att fullgöra bevaknings- och säkerhetsarbete avseende den del av personskyddet som Säkerhetspolisen ansvarar för enligt sin instruktion eller som Rikspolisstyrelsen har överlämnat till Säkerhetspolisen. När det gäller polisen i övrigt – som också bedriver viss personskyddsverksamhet – har vi inte föreslagit någon motsvarande ändamålsbestämmelse. Skälet till att detta

 ndam l b r n mnas s rskilt i lagen, s vitt g ller S kerhetspolisen,  r att man inte kan f ruts tta att de brott som kan komma att riktas mot en person som har personskydd ryms under det f tal brottstyper som det ing r i S kerhetspolisens uppdrag att bek mpa.

#### * tg rder enligt viss utl nningslagstiftning*

S kerhetspolisen genomf r ocks  vissa  tg rder med st d av best mmelser som reglerar utl nningars r tt att vistas h r i landet. Enligt 2   lagen (1991:572) om s rskild utl nningskontroll kan S kerhetspolisen initiera ett  rende om utvisning av en utl nning som inte kan avvisas eller utvisas enligt utl nningslagen, om det beh vs av h nsyn till rikets s kerhet eller om det kan befaras att utl nningen kommer att beg  eller medverka till terroristbrott. Om utvisning beslutas men beslutet inte kan verkst llas, kan S kerhetspolisen beg ra att utl nningen  l ggs anm lningsplikt eller att vissa tv ngsmedel i r tteg ngsbalken f r anv ndas. Vid handl ggning av s dana  renden m ste S kerhetspolisen kunna behandla personuppgifter. N gon s rskild reglering i detta avseende  r inte n dv ndig, eftersom s dan behandling t cks av  ndam len att f rebygga och f rhindra brott mot rikets s kerhet eller terroristbrott.

#### *Uppgifter enligt s kerhetsskyddslagen*

S kerhetspolisen ska enligt 3   1 sin instruktion fullg ra de uppgifter som Rikspolisstyrelsen ska utf ra enligt s kerhetsskyddslagen (1996:627) och s kerhetsskyddsf rordningen (1996:633), bl.a. registerkontroll och s rskild personutredning. Detta s kerhetsskyddsarbete f r anses utg ra en del av S kerhetspolisens brottsbek mpande verksamhet, eftersom det yttersta syftet med kontrollen  r att f rebygga att personer som kan inneb ra ett s kerhetshot f r viktiga uppdrag. F r att fullg ra uppgifterna

enligt n mnda f rfattningar m ste S kerhetspolisen kunna bearbeta uppgifter som finns i dess egna datasystem samt samla in och bearbeta uppgifter som h rr r fr n s rskilda register hos den  vriga polisen och andra uppgifter som den behandlar. Detta  ndam l b r s ledes anges s rskilt i lagen.

#### *Internationellt arbete*

F r S kerhetspolisens verksamhet g ller, i  n st rre utstr ckning  n f r polisen i  vrigt, att arbetet  r ett resultat av internationellt samarbete. Ett viktigt sk l till detta  r att terrorismen numera  r transnationell. Det inneb r att S kerhetspolisen bl.a. arbetar f r att f rhindra att Sverige anv nds som bas f r rekrytering, finansiering eller planering av terrord d, oavsett mot vilket land dessa riktar sig, och f r att f rebygga att personer med anknytning till terroristn tverk bes ker Sverige eller f rs ker bos tta sig h r. En stor del av informationsutbytet sker inom den informella s marbetsorganisationen Bernklubben, som best r av s kerhetstj ns-terna fr n ett flertal medlemsstater inom EU.

Det internationella samarbetet f ruts tter ett  msesidigt och v l fungerande informationsutbyte. Vad som har sagts i avsnitt 7.4 om informationsutbyte vid internationellt samarbete  r i allt v sentligt giltigt ocks  f r S kerhetspolisens del.  ven S kerhetspolisen b r s ledes f  behandla personuppgifter f r att fullg ra internationella  taganden.

#### *Tekniskt bitr de*

Enligt 3   f rsta stycket 3 f rordningen (2002:1050) med instruktion f r S kerhetspolisen ing r det i S kerhetspolisens uppgifter att l mna tekniskt bitr de  t polisv sendet i den utstr ckning som det  r l mpligt med h nsyn till verksamhetens art. S kerhetspolisen har s ledes en m jlighet att bist  med bl.a. teknisk utrustning som den  vriga polisen inte har. Det tekniska

biträdet sker framför allt vid verkställighet av vissa tvångsmedel. Säkerhetspolisen har nämligen en specialuppgift som består i hanteringen av de datasystem som används för att samla in uppgifter från hemlig teleavlyssning och hemlig teleövervakning. Säkerhetspolisen ansvarar för kontakter med operatörerna, när det finns ett domstolsbeslut om hemlig teleavlyssning eller hemlig teleövervakning, och tar emot och lagrar den information som operatörerna levererar i enlighet med domstolsbesluten. Detta gäller inte enbart Säkerhetspolisens egna ärenden utan samtliga ärenden av detta slag i landet, oberoende av om förundersökningen bedrivs hos Säkerhetspolisen, inom den övriga polisen, hos Tullverket eller hos Ekobrottsmyndigheten. Behöriga tjänstemän vid polismyndigheterna, och i förekommande fall Tullverket, hämtar in informationen från Säkerhetspolisen och behandlar den vidare. Säkerhetspolisens uppgift är främst en administrativ hantering, men den kräver personuppgiftsbehandling som faller under ändamålet brottsbekämpning. Av det skälet bör denna behandling nämnas särskilt i lagen.

Inom systemet hanteras också material från hemlig teleavlyssning och hemlig teleövervakning i ärenden som handläggs av Säkerhetspolisen. Personuppgiftsbehandlingen i denna del faller under Säkerhetspolisens brottsutredande verksamhet eller, såvitt gäller hemlig teleavlyssning enligt lagen om särskild utlänningskontroll, uppgiften att förebygga, förhindra eller upptäcka brott.

Säkerhetspolisen lämnar också visst biträde med verkställigheten av hemlig kameraövervakning. Om riksdagen godkänner den tidigare nämnda propositionen om hemlig rumsavlyssning, är det antagligt att Säkerhetspolisen kommer att biträda polismyndigheterna även med verkställighet av det tvångsmedlet. Mot den bakgrunden bör den nu aktuella bestämmelsen utformas så att den täcker även personuppgiftsbehandling som kan aktualiseras vid sådant biträde.

### 18.4.3 Behandling av uppgifter f r att tillhandah lla information till andra

**Promemorians f rslag:** Om S kerhetspolisen behandlar personuppgifter med st d av n got av de prim ra  ndam len, f r uppgifterna  ven behandlas n r det  r n dv ndigt f r att tillhandah lla information som beh vs i

1. brottsbek mpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten,  klagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,

2. F rsvarmaktens f rsvarsunderr ttelseverksamhet och milit ra s kerhetstj nst, om det finns s rskilda sk l att tillhandah lla informationen, eller

3. brottsbek mpande verksamhet hos utl ndsk myndighet eller mellanfolklig organisation.

Personuppgifter som behandlas med st d av n got av de prim ra  ndam len f r  ven behandlas om det  r n dv ndigt f r att tillhandah lla information till riksdagen och regeringen samt, i den utstr ckning uppgiftsskyldighet f ljer av lag eller f rordning, andra.

Regeringen f r meddela f reskrifter om att personuppgifter som behandlas enligt de prim ra  ndam len och som avser efterlysta personer och avl gsnanden ur landet f r behandlas f r att tillhandah lla information till vissa s rskilt angivna myndigheter.

Personuppgifter ska alltid f a behandlas om behandlingen  r n dv ndig f r diarief ring eller om uppgifterna har l mnats i en anm lan eller liknande och behandlingen  r n dv ndig f r handl ggningen.

**Utredningens f rslag:** Utredningen har inte f rslagit n gra s rskilda best mmelser f r behandling av uppgifter f r att tillhandah lla information till andra.

**Remissinstanserna** har inte yttrat sig i fr gan.

**Skälen för promemorians förslag:** I likhet med polisen i övrigt måste Säkerhetspolisen kunna behandla den information som finns lagrad i digital form för att i viss utsträckning tillhandahålla den till andra brottsbekämpande enheter inom polisen eller till andra brottsbekämpande myndigheter. Vad som har sagts i avsnitt 7.6 om sekundära ändamål för behandling av personuppgifter har därför giltighet även för Säkerhetspolisens del.

Allmänt sett är dock behovet av informationsutbyte mellan Säkerhetspolisen och andra enheter inom polisväsendet inte lika framträdande som behovet av informationsutbyte mellan olika enheter inom den övriga polisen. Detta beror på att den information som Säkerhetspolisen behandlar ofta är av den arten att den varken kan eller bör vidarebefordras. Motsvarande gäller behovet av informationsutbyte mellan Säkerhetspolisen och andra brottsbekämpande myndigheter. Det finns emellertid situationer där Säkerhetspolisen kan behöva vidarebefordra information som den har samlat in, exempelvis för att kunna förhindra allvarliga brott som ligger utanför Säkerhetspolisens behörighet. Som exempel kan nämnas att det vid hemlig teleavlyssning som rör spioneri avslöjas konkreta planer på ett förestående bankrån. Den typen av information vidarebefordras normalt till den öppna polisen, i syfte att rånbrottet ska kunna förhindras. Det rör sig här om s.k. överskottsinformation, vars användning regleras i 27 kap. 23 a § rättegångsbalken. Likaså måste Säkerhetspolisen kunna vidarebefordra uppgifter om planerade eller begångna brott riktade mot någon som omfattas av Säkerhetspolisens personskydd, om det är fråga om ett brott som ligger utanför Säkerhetspolisens ansvarsområde.

Frågan är om bestämmelsen om de sekundära ändamål för vilka Säkerhetspolisen får behandla personuppgifter ska utformas på exakt samma sätt som för polisen i övrigt. Som framgått ovan kan det från brottsbekämpningssynpunkt finnas ett påtagligt behov av att Säkerhetspolisen kan lämna uppgifter till andra brottsbekämpande organ. Likaså har Säkerhetspolisen samma behov av att kunna lämna uppgifter till åklagare som andra brottsutredande polisenheter, om åklagaren behöver uppgiften

f r sin verksamhet. S kerhetspolisens behov av att kunna l mna uppgifter till exempelvis Tullverket  r mindre tydligt. Ibland kan det emellertid finnas ett samband mellan den brottslighet som Tullverket bek mpar och den brottslighet som h r till S kerhetspolisens ansvarsomr de. Det f rekommer t.ex. att narkotikabrottslighet anv nds f r att finansiera terroristbrott. Det medf r att S kerhetspolisen kan komma att f  del av uppgifter om t.ex. grova smugglingsbrott. Tullverket har ocks  en viktig roll n r det g ller gr nskontrollen. I den verksamheten kan S kerhetspolisen och Tullverket beh va utbyta information t.ex. om personer som anses inneb ra s kerhetsrisker eller som av annat sk l b r hindras att komma in i landet. Kustbevakningens uppdrag n r det g ller gr nskontrollen inneb r att det kan finnas behov f r S kerhetspolisen att kunna tillhandah lla information ocks  till den myndigheten. Det  r d rf r inte rimligt att avsk ra myndigheten fr n all m jlighet att l mna viktig information vidare till en annan brottsbek mpande myndighet, om informationen beh vs hos den mottagande myndigheten och S kerhetspolisen anser att det finns sk l f r att f ra den vidare. S kerhetspolisen m ste sj lvfallet ocks  kunna besvara f rfr gningar fr n polisen i  vrigt, eller fr n en annan brottsbek mpande myndighet, om inte sekretess hindrar det.

Eftersom Skatteverket enbart bedriver f runders kning ang ende ett f tal brottstyper som r knas upp i 1 § f rsta stycket lagen (1997:1024) om Skatteverkets medverkan i brottsutredningar kan det f refalla som om behovet av att kunna l mna uppgifter till den verksamheten inte  r s  stort. I S kerhetspolisens uppgift att utreda finansiering av allvarlig brottslig verksamhet kan det emellertid finnas behov av att utbyta uppgifter  ven med Skattemyndighetens brottsbek mpande del.

Mot den nu angivna bakgrunden b r det sekund ra  ndamålet att kunna tillhandah lla information till andra brottsbek mpande myndigheter utformas p  samma s tt f r S kerhetspolisen som f r polisen i  vrigt.

Likas  b r det sekund ra  ndamålet att kunna tillhandah lla information till en utl ndsk myndighet som bedriver brottsbe-

k ampande verksamhet eller till en mellanfolklig organisation med s adana uppgifter utformas p  samma s att f r S akerhetspolisen som f r polisen i  vrigt.

S akerhetspolisen har ocks , p  grund av sina speciella uppgifter, behov av att i vissa s arskilda fall kunna tillhandah lla information till F rsvarsmaktens underr ttelseverksamhet och s akerhetstj nst. Som exempel p  en s adan situation kan n mnas att det i S akerhetspolisens brottsbek ampande verksamhet kommer fram uppgifter som samtidigt har betydelse f r F rsvarsmaktens verksamhet. Det kan t.ex. r ra sig om f r landets s akerhet viktiga uppgifter om en f rsvarsanst lld eller n gon i dennes n rmaste krets eller om svagheter i skyddet hos n gon av F rsvarsmaktens anl ggningar. P  samma s att som brottsbek mpningen i vissa avseenden  r en f r flera myndigheter gemensam verksamhet  r ocks  den underr ttelseverksamhet som r r rikets s akerhet en f r S akerhetspolisen och F rsvarsmakten gemensam angel genhet. Mot den bakgrunden m ste det finnas ett utrymme f r att utbyta information mellan myndigheterna.

F rutom att det ska vara fr ga om en uppgift som beh vs i F rsvarsmaktens verksamhet b r det kr vas s arskilda sk l f r att uppgifter ska f  l mnas ut. H rigenom markeras att best mmelsen ska till mpas restriktivt.

Som p pekats i avsnitt 7.6 inneb r en  ndam lsbest mmelse av det slag som vi nu f resl r inte n gon reglering av vad som f r utl mnas eller hur detta ska ske. Best mmelsen m jligg r enbart den behandling som kr vs f r att uppgifterna  ver huvud taget ska kunna tillhandah llas, t.ex. en datak rning eller en utskrift av en handling.

Vi har ovan, s vitt avser den  vriga polisen, f rslagit en best mmelse om behandling av uppgifter f r att tillhandah lla information till riksdagen eller regeringen; jfr 14 kap. 1   sekretesslagen. En motsvarande best mmelse b r inf ras f r S akerhetspolisen. Detsamma b r g lla om S akerhetspolisen har uppgiftsskyldighet gentemot n gon annan enligt lag eller f rfattning; S akerhetspolisen m ste d  kunna genomf ra den behandling som kr vs f r att fullg ra uppgiftsskyldigheten. Som exem-



pel kan nämnas den lagfästa skyldigheten att underrätta bl.a. anhöriga till en person som har berövats friheten.

I avsnitt 7.6 har vi föreslagit en informationsbestämmelse om att regeringen meddelar föreskrifter om att personuppgifter rörande efterlysta personer och avlägsnanden ur landet får lämnas till vissa myndigheter. Det är naturligt med en motsvarande bestämmelse för personuppgiftsbehandlingen hos Säkerhetspolisen, eftersom Säkerhetspolisen bl.a. har vissa uppgifter enligt lagen (1991:572) om särskild utlänningskontroll.

Även för Säkerhetspolisens del bör det införas bestämmelser som gör det möjligt att utan hinder av vad som gäller i övrigt behandla uppgifter om det är nödvändigt för diarieföring eller för handläggningen av en anmälan eller liknande som kommit in till Säkerhetspolisen (se avsnitt 7.5).

## 18.5 Vissa allmänna bestämmelser som bör gälla även för Säkerhetspolisen

**Promemorians förslag:** Flera av de bestämmelser som ovan har föreslagits gälla i polisens brottsbekämpande verksamhet i övrigt ska gälla även i Säkerhetspolisens verksamhet, däribland bestämmelserna om

- förhållandet till personuppgiftslagen,
- tillsyn,
- behandlingen av känsliga personuppgifter,
- behandling av uppgifter om resultatet av DNA-analyser,
- tillgången till uppgifter och
- utlämnande av uppgifter till bl.a. utländsk myndighet.

Vidare ska bestämmelser med i huvudsak samma innebörd som motsvarande bestämmelser för polisen i övrigt gälla i fråga om behandling av uppgifter om juridiska personer, personuppgiftsansvar och gallring av uppgifter som inte har gjorts gemensamt tillgängliga.

**Utredningens f orslag:** Utredningen har valt en annan lagteknisk l osning. I sak  overensst ammer dock utredningens f orslag i allt v asentligt med promemorians f orslag.

**Remissinstanserna** har inte yttrat sig s arskilt i fr agan.

**Sk alen f or promemorians f orslag:** Vi har ovan konstaterat att S akerhetspolisens verksamhet i vissa delar avviker fr an den  ovriga polisens verksamhet och att det d arf or  ar befogat med speciella best ammelser.  atskilliga av de best ammelser som vi har f oreslagit ska g alla vid den  ovriga polisens behandling av personuppgifter b or emellertid g alla  aven f or S akerhetspolisen.

S a b or exempelvis de f oreslagna best ammelserna om lagens till ampningsomr ade g alla ocks a vid behandling av uppgifter inom S akerhetspolisen (se avsnitt 6.3). Detsamma g aller vad vi har f oreslagit om f orh allandet till personuppgiftslagen och till ampliga best ammelser i personuppgiftslagen (se avsnitt 6.5). Vidare b or – som vi  aterkommer till i avsnitt 19 – g alla samma best ammelser om tillsyn som f or polisen i  ovrigt. I avsnitt 8 har vi f oreslagit best ammelser som begr ansar m ojligheten att behandla k ansliga personuppgifter och uppgifter om resultatet av DNA-analyser. Ocks a dessa b or g alla vid personuppgiftsbehandling i S akerhetspolisens verksamhet. Detsamma g aller den principiellt viktiga och grundl aggande best ammelsen som vi har f oreslagit i avsnitt 6.7, att endast de personer i verksamheten som beh over ha tillg ang till uppgifter f or att kunna utf ora sina arbetsuppgifter ska ha det.

N ar det g aller utl amnande av uppgifter till bl.a. utl andska myndigheter har vi i avsnitt 13 f oreslagit att den nya lagen ges ett inneh all som motsvarar vad som g aller i dag. Detta b or g alla  aven i fr aga om S akerhetspolisen. De sekretessbrytande best ammelser om utl amnande som vi har f oreslagit f or polisen i  ovrigt, och som ytterst syftar till att m ojligg ora direkt atkomst mellan de brottsbek ampande myndigheterna, b or d aremot inte g alla f or S akerhetspolisen. Med h ansyn till arten av de uppgifter som kan f orekomma i S akerhetspolisens verksamhet utg or direkt atkomst inte n agon l amplig form f or informationsutbyte mellan S akerhetspolisen och andra myndigheter. Varje enskilt utl amnande av

uppgifter fr n S kerhetspolisen b r s ledes  ven forts ttningsvis f reg s av en s rskild sekretesspr vning och S kerhetspolisen b r inte kunna medge n gon annan myndighet direkt tkomst till uppgifter som behandlas inom myndigheten.

I f reg ende avsnitt har vi  cks  f reslagit best mmelser om personuppgiftsansvar och gallring av uppgifter som inte har gjorts gemensamt tillg ngliga. Det  r naturligt att dessa best mmelser g ller  ven f r S kerhetspolisen,  ven om en viss anpassning av best mmelserna kr vs. S kerhetspolisen b r naturligtvis vara personuppgiftsansvarig f r den behandling av personuppgifter som sker i dess egen verksamhet (se avsnitt 6.6). Vidare b r, p  samma s tt som vi har f reslagit i fr ga om polisen i  vrigt, best mmelserna om S kerhetspolisens personuppgiftsbehandling i till mpliga delar g lla  ven f r uppgifter om juridiska personer (se avsnitt 6.3).

## 18.6 Gemensamt tillg ngliga uppgifter

### 18.6.1 Allm nna utg ngpunkter

**Promemorians f rslag:** S rskilda best mmelser ska g lla f r behandling av uppgifter som g rs eller har gjorts gemensamt tillg ngliga i S kerhetspolisens verksamhet. Personuppgifter ska f  g ras gemensamt tillg ngliga i S kerhetspolisens verksamhet, om det beh vs f r n got av de  ndam l f r vilka behandling f r ske inom S kerhetspolisen. Uppgifter om resultatet av DNA-analyser f r dock inte g ras gemensamt tillg ngliga.

**Utredningens f rslag:** Utredningen har inte n got motsvarande f rslag.

**Remissinstanserna** har inte yttrat sig i fr gan.

**Sk len f r promemorians f rslag:** Som ovan har framg tt sker mycket av S kerhetspolisens personuppgiftsbehandling i

gemensamma register, analysdatabaser och ärendehanteringssystem. Oftast innebär en sådan behandling att ett flertal personer har tillgång till de behandlade uppgifterna. Vi har i avsnitt 9 konstaterat att ju fler personer som har åtkomst till personuppgifter, desto större är risken för otillbörliga intrång i den personliga integriteten. Av samma skäl som vi har angett där bör det i den nya lagen tas in särskilda bestämmelser för den behandling av uppgifter som ”görs eller har gjorts gemensamt tillgängliga” i Säkerhetspolisens verksamhet. Vad vi menar med ”görs eller har gjorts gemensamt tillgängliga” har vi utvecklat i avsnitt 9.1. De särskilda bestämmelserna bör – liksom för polisen i övrigt – innehålla bl.a. särskilda upplysningskrav, sökbegränsningar och särskilda krav på gallring.

Vi har för polisen i övrigt föreslagit en bestämmelse som begränsar och preciserar vilka personuppgifter som får göras gemensamt tillgängliga. Frågan är om någon motsvarande bestämmelse bör införas för Säkerhetspolisen.

I 33 och 34 §§ polisdatalagen anges vilka uppgifter som får behandlas i SÄPO-registret. Enligt 33 § får uppgifter som kan hänföras till en person behandlas endast om (1) den uppgifternas gällande kan misstänkas för att ha utövat eller kan komma att utöva brottslig verksamhet, (2) den uppgifternas gällande har undergått registerkontroll enligt säkerhetsskyddslagen, eller (3) det med hänsyn till registrets ändamål annars finns särskilda skäl till det. I förarbetena till lagen behandlas de tre olika registreringsgrunderna, se prop. 1997/98:97 s. 152. I fråga om den sistnämnda konstaterade regeringen att en sådan bestämmelse ger Säkerhetspolisen tämligen vida ramar att registrera uppgifter. Regeringen ansåg emellertid att detta var befogat och kunde försvaras bland annat med hänsyn till Registernämndens särskilda tillsyn, som medger insyn i och kontroll av registret. I 34 § polisdatalagen preciseras närmare vilka uppgifter som registret får innehålla. Säkerhetspolisen har tolkat denna bestämmelse som en bestämmelse som anger vad som får göras sökbart i registret. Vi återkommer till frågan om sökbegränsningar nedan i avsnitt 18.6.4.

Som nämnts ovan tillämpar Säkerhetspolisen bestämmelserna i polisdatalagen om SÄPO-registret på det centralregister som myndigheten för. En övervägande majoritet av de anteckningar som görs i registret sker på den grunden att det finns särskilda skäl för registreringen med hänsyn till registrets ändamål (33 § första stycket 3 polisdatalagen). Att särskilda skäl används som registreringsgrund i flertalet fall återspeglar att man i gällande lagstiftning inte har lyckats att precisera de olika kategorier av personuppgifter som Säkerhetspolisen behöver behandla. Den nuvarande lagstiftningen speglar alltså inte det verkliga behovet av behandling av personuppgifter.

Vi delar den tidigare utredningens uppfattning att de intressen som Säkerhetspolisen har till uppgift att skydda motiverar att Säkerhetspolisen ges en större handlingsfrihet än den övriga polisen i fråga om vilka uppgifter som bör få behandlas (se bl.a. SOU 1997:65 s. 243). Skälet till detta är bl.a. att Säkerhetspolisens verksamhet är inriktad mot brottslighet som till sin natur är svår att upptäcka och att tyngdpunkten i dess brottsbekämpande arbete ligger i underrättelsearbete och renodlat förebyggande arbete.

Det nu sagda talar för att de begränsningar som vi har föreslagit för polisen i övrigt för att göra uppgifter gemensamt tillgängliga inte bör gälla för Säkerhetspolisen. I samma riktning talar svårigheten att förutse och i lag uttrycka de olika kategorier av personuppgifter som bör få göras gemensamt tillgängliga hos Säkerhetspolisen. Vi föreslår därför att Säkerhetspolisen bör få göra personuppgifter gemensamt tillgängliga så snart det behövs för något av de primära ändamål för vilka Säkerhetspolisen får behandla personuppgifter. Ett undantag bör dock gälla för uppgifter om resultatet av DNA-analyser. Något behov av att göra sådana uppgifter gemensamt tillgängliga torde inte finnas, eftersom behandlingen av sådana uppgifter utförs av Statens kriminaltekniska laboratorium på uppdrag av Säkerhetspolisen.

Som exempel på behov av att göra uppgifter gemensamt tillgängliga kan nämnas att uppgifter som har betydelse för personskyddet kan behöva spridas till en vidare krets för att skyddet

ska fungera som avsett eller att uppgifter fr n n gon annan verksamhetsgren kan ha betydelse f r registerkontrollen och av det sk let b r g ras gemensamt tillg ngliga. Det torde d remot normalt inte finnas n got behov av att g ra uppgifter som behandlas i mindre projekt inom de olika verksamhetsgrenarna gemensamt tillg ngliga.

#### **18.6.2 Utl mnande av uppgifter p  medium f r automatisk behandling**

**Promemorians f rslag:** I S kerhetspolisens verksamhet ska g lla samma best mmelser som i den  vriga polisens verksamhet om utl mnande av uppgifter p  medium f r automatiserad behandling.

**Utredningens f rslag:** Utredningen har inte n got motsvarande f rslag.

**Remissinstanserna** har inte yttrat sig i fr gan.

**Sk len f r promemorians f rslag:** I avsnitt 12.3.5 har vi f reslagit att det inte ska vara m jligt att medge andra myndigheter direkt tkomst till de uppgifter som S kerhetspolisen behandlar. Av samma sk l som redovisats d r b r det inte heller vara m jligt f r S kerhetspolisen att l mna ut stora informationsm ngder p  medium f r automatiserad behandling (jfr avsnitt 14).

### 18.6.3 S rskilda upplysningar

**Promemorians f rslag:** Personuppgifter som g rs eller har gjorts gemensamt tillg ngliga ska f rses med en upplysning om  ndamålet med behandlingen, om detta inte  ndå tydligt framg r av omst ndigheterna.

Uppgifter som direkt kan h nf ras till en person som inte  r misst nkt vare sig f r visst brott eller f r att ha ut vat eller komma att ut va brottslig verksamhet ska f rses med en s rskild upplysning om detta f rh llande. Upplysning beh ver dock inte l mnas om f rh llande som  ndå framg r tydligt av omst ndigheterna.

Uppgifter, som avser en person som kan antas ha samband med brottslig verksamhet, ska f rses med upplysning om uppgiftsl mnarens trov rdighet och uppgifternas riktighet i sak, om inte detta p  grund av s rskilda omst ndigheter  r on digt. En s dan upplysning beh ver inte heller l mnas om

1. uppgifterna ing r i en uppgiftssamling som har skapats f r att bearbeta och analysera information och som enbart s rskilt angivna t janstem n har  tkomst till, och
2. bearbetningen och analysen befinner sig i ett inledande skede.

**Utredningens f rslag:** Utredningen har inte n got motsvarande f rslag.

**Remissinstanserna** har inte yttrat sig i fr gan.

**Sk len f r promemorians f rslag:** Enligt g llande best mmelser (33   andra stycket polisdatalagen) ska det av S APO-registret framg  p  vilken grund varje registrering har skett. S kerhetspolisen har inte n gon skyldighet att f rse personuppgifter med s rskilda upplysningar om huruvida en person som behandlas  r misst nkt eller inte eller om trov rdigheten hos en uppgiftsl mnare. De behandlade uppgifterna f rses dock  nd  regelm ssigt med s dana upplysningar.

Syftet med s dana s rskilda upplysningar  r dels att st rka skyddet f r den enskildes integritet, dels att f rhindra att uppgifter vilkas tillf rlitlighet och trov rdighet  r begr nsad l ggs till grund f r bed mningar och  tg rder som inte  r sakligt motiverade. Vi har d rf r, i avsnitt 10, f r polisen i  vrigt f reslagit lagbest mmelser om att gemensamt tillg ngliga uppgifter ska f renas med s rskilda upplysningar av det angivna slaget. De sk l som motiverar att s dana upplysningar l mnas har giltighet  ven f r den behandling som sker hos S kerhetspolisen. Best mmelser med denna inneb rd b r d rf r inf ras i den nya lagen. Best mmelserna b r dock ges en n got annorlunda utformning  n motsvarande best mmelser f r polisen i  vrigt. N r uppgifter tas in i en analysdatabas f r bearbetning och analys, kan det i ett inledande skede vara sv rt att l mna en s rskild upplysning om uppgiftsl mnarens trov rdighet och uppgifternas riktighet i sak. Kravet p  s dana upplysningar b r d rf r inte g lla upplysningar som har tillf rts en analysdatabas, s  l nge bearbetningen och analysen befinner sig i ett inledande skede. N r arbetet har n tt l ngre, exempelvis n r ett underr ttelseprojekt inriktat p  viss brottslighet har p b rjats, m ste dock kravet uppfyllas.



#### 18.6.4 S kbegr nsningar

**Promemorians f rslag:** K nsliga personuppgifter f r anv ndas som s kbegrepp endast om det  r absolut n dv ndigt f r de  ndam l som g ller f r S kerhetspolisens behandling av personuppgifter.

Vid s kning som sker i gemensamt tillg ngliga uppgifter f r endast vissa kategorier av uppgifter tas fram. Detta g ller dock inte vid s kning som sker i en viss handling eller i ett visst  rende. S kbegr nsningen g ller inte heller vid s kning i en s rskild uppgiftssamling som har skapats f r att bearbeta och analysera information och som enbart s rskilt angivna t janstem n hos S kerhetspolisen har  tkomst till.

Regeringen eller den myndighet som regeringen best mer meddelar n rmare f reskrifter om undantagen fr n s kbegr nsningen.

**Utredningens f rslag:** Utredningen har inte l mnat n got motsvarande f rslag.

**Remissinstanserna:** *Registern mnden* har ifr gasatt om det kommer att vara m jligt att undvika att k nsliga personuppgifter kommer att behandlas p  ett otill tet s tt, bl.a. i de s.k. analysdatabaserna.

#### Sk len f r promemorians f rslag

##### *K nsliga personuppgifter*

Polisdatalagen inneh ller inte n gra best mmelser om s kbegr nsningar. Det inneb r att det i dag inte finns n gra begr nsningar i fr ga om anv ndning av vissa uppgifter som s kbegrepp. Det enda undantaget kan s gas vara best mmelsen i 5   polisdatalagen om behandling av k nsliga uppgifter, men den best mmelsen g ller behandlingen generellt. I avsnitt 11.1 har f reslagits att k nsliga personuppgifter inte ska f  anv ndas som s kbe-

grepp inom den övriga polisverksamheten. Det innebär exempelvis att uppgifter som avslöjar ras, politisk åsikt, religiös övertygelse eller som rör hälsa eller sexualliv inte får utgöra sökbegrepp. Frågan är om detsamma bör gälla för Säkerhetspolisen.

I Säkerhetspolisens verksamhet kan uppgifter av de angivna slagen ha betydelse för verksamheten. I arbetet med att förebygga och upptäcka terroristbrott kan t.ex. uppgifter om en persons politiska åsikt eller religiösa övertygelse vara av avgörande betydelse. Vid brott mot rikets säkerhet kan uppgifter av det slaget bidra till att utröna om det finns något motiv för gärningen. Ett totalt förbud mot att använda sådana uppgifter som sökbegrepp skulle därför innebära en risk för att nödvändig analys och bearbetning av information inte kan ske. Verksamhetsskäl talar alltså för att man för Säkerhetspolisens del inte helt bör förbjuda användningen av känsliga personuppgifter som sökbegrepp. Verksamhetsintresset måste emellertid vägas mot intresset av att skydda de personer, vilkas uppgifter behandlas, mot intrång i den personliga integriteten. En lämplig avvägning mellan dessa var för sig mycket starka intressen är enligt vår mening följande. Huvudregeln bör vara att det är förbjudet att använda känsliga personuppgifter som sökbegrepp. Om en sådan användning är absolut nödvändig för något av de ändamål som Säkerhetspolisen får behandla personuppgifter för, bör den dock vara tillåten. Med en sådan regel kan känsliga personuppgifter inte rutinmässigt användas som sökbegrepp utan först sedan det vid en prövning av behovet i det enskilda fallet konstateras att det finns ett mycket påtagligt behov.

#### *Andra sökbegränsningar*

Hos Säkerhetspolisen behandlas ett stort antal olika kategorier av personuppgifter. I avsnitt 18.6.1 har vi gjort bedömningen att det inte är möjligt eller lämpligt att, på samma sätt som för den övriga polisverksamheten, ange vilka olika kategorier av personuppgifter som får göras gemensamt tillgängliga. Av samma skäl

 r det inte m jligt att f r S kerhetspolisen inf ra det slag av s kbegr nsningar som vi har f reslagit f r polisen i  vrigt i fr ga om s kning p  namn och personnummer. N gra s dana s kbegr nsningar finns inte heller i dag.

I 34   polisdatalagen anges vilka kategorier av uppgifter som f r behandlas i S PO-registret. Enligt den paragrafen f r S PO-registret endast inneh lla (1) identifieringsuppgifter, (2) uppgifter om grunden f r registreringen och (3) h nvisning till de  renden d r uppgifter om den registrerade behandlas. I f rarbetena preciserades inte inneb rden av dessa kriterier n rmare (prop. 1997/98:97 s. 154). S kerhetspolisen tolkar dock, som redan n mnts, best mmelsen som en s kbegr nsning och till mpar den p  det centralregister d r merparten av myndighetens personuppgiftsbehandling sker.

Med st d av best mmelsen registreras och g rs bl.a. f ljande uppgifter s kbara i S kerhetspolisens centralregister. *Punkten 1:* uppgifter om namn, personnummer, adress, telefonnummer, yrke, civilst nd, make/maka, signalement, passnummer, och registreringsnummer p  innehavd bil. *Punkten 2:* grunden f r registreringen enligt 33   1–3, ber rt verksamhetsomr de inom S kerhetspolisen, t.ex. personskydd, och kortfattad beskrivning av den h ndelse som f ranlett registreringen. *Punkten 3:* h nvisning till de handlingar och  renden d r uppgifter om den registrerade behandlas.

Vid s kning i centralregistret visas endast s dana uppgiftskategorier som n mns i paragrafen. Via registret n s emellertid de handlingar och  renden som ligger till grund f r registreringen. Dessa lagras i en databas som  r kopplad till registret. Uppgifterna i dessa handlingar och  renden  r dock inte s kbara.

Enligt v r mening talar integritetsintressen mot att till ta att samtliga personuppgifter som behandlas hos S kerhetspolisen g rs  tkomliga genom fritexts kning. Det relativt stora handlingsutrymme som S kerhetspolisen m ste ges i fr ga om vilka uppgifter som f r g ras gemensamt tillg ngliga b r s ledes balanseras av best mmelser om s kbegr nsningar som begr nsar  tkomsten till uppgifterna. Samma slag av s kbegr nsningar som

till mpas i dag b r d rf r g lla  ven i forts ttningen. En best mmelse med denna inneb rd b r tas in i den nya lagen.

Fr gan  r d  om dessa s kbegr nsningar ska g lla f r all personuppgiftsbehandling hos S kerhetspolisen. Vi anser att det av samma sk l som har redovisats i fr ga om den  ppna polisen inte finns sk l att ha n gra begr nsningar vid s kning i ett enskilt  rende eller i en viss handling (se avsnitt 11.2). De integritetssk l som g r sig g llande i fr ga om s kningar i ett stort material g r sig n mligen inte lika starkt g llande vid s kning i ett visst  rende eller i en handling. Den befattningshavare som har s kt fram ett visst  rende, har  tkomst till det och bed mer att han eller hon beh ver titta i  rendet f r att kunna utf ra sina arbetsuppgifter, b r allts  till tas att s ka fritt i detta. P  samma s tt som f r den  vriga polisen b r n gra s kbegr nsningar, f rutom de som avser k nsliga personuppgifter, inte heller g lla f r s kning i vissa mindre uppgiftssamlingar som f rs f r vissa n rmare angivna  ndam l. F r S kerhetspolisens del b r undantaget g lla f r uppgiftssamlingar som har skapats f r att bearbeta och analysera information och som enbart s rskilt angivna t janstem n har tillg ng till, dvs. de s.k. analysdatabaserna. Regeringen b r kunna meddela n rmare f reskrifter om under vilka f ruts ttningar s kning f r  ga rum.

### 18.6.5 Gallring

**Promemorians förslag:** Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Personuppgifter som behandlas i en s.k. analysdatabas ska dock gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Säkerhetspolisen får besluta att personuppgifter får behandlas längre tid än vad som nu har sagts, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas. Om uppgifter bevaras med stöd av ett sådant beslut, ska de gallras, eller frågan om bevarande prövas på nytt, senast vid utgången av det tionde året efter beslutet eller, i fråga om uppgifter i analysdatabaser, senast vid utgången av det tredje året efter beslutet.

Bestämmelserna om gallring ska inte tillämpas på uppgifter i brottsanmälningar, förundersökningar eller andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken. För behandling av uppgifter i avslutade förundersökningar bör samma bestämmelser gälla som i den övriga polisens verksamhet.

Bestämmelserna om gallring ska inte heller tillämpas om regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter om att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

**Utredningens förslag:** Utredningen har inte föreslagit några särskilda regler om gallring för Säkerhetspolisens verksamhet. Den allmänna bestämmelsen i förslaget, att personuppgifter inte ska bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen, har föreslagits gälla.

**Remissinstanserna** har inte yttrat sig i frågan.

**Skälen för promemorians förslag:** Vi har i avsnitt 16.3 föreslagit att den nya lagen inte ska innehålla några bestämmelser om gallring av uppgifter i brottsanmälningar, förundersökningar och andra utredningar som görs med stöd av bestämmelser i 23 kap. rättegångsbalken. Några sådana bestämmelser bör inte heller införas för Säkerhetspolisen. I avsnitt 16.3 har vi i stället, såvitt gäller polisen i övrigt, föreslagit vissa begränsningar i möjligheterna att behandla uppgifter i avslutade förundersökningar m.m. Dessa begränsningar bör gälla även för Säkerhetspolisen. Beträffande innebörden av begränsningarna hänvisas till avsnitt 16.3.

När det gäller övriga slag av uppgifter bör dessa – på samma sätt som motsvarande uppgifter hos den övriga polisen – omfattas av särskilda gallringsbestämmelser. Utgångspunkten för dessa gallringsbestämmelser bör vara att samma regler ska tillämpas, oavsett var i Säkerhetspolisens verksamhet som uppgiften behandlas. Det bör alltså, som huvudregel, inte gälla olika gallringsfrister beroende på i vilken uppgiftssamling uppgiften förekommer.

Med hänsyn till de betydande skillnader som finns mellan Säkerhetspolisens och den övriga polisens verksamhet är det inte givet att gallringsbestämmelserna bör utformas med de ovan föreslagna gallringsbestämmelser som ska gälla för den övriga polisen som förebild. Tvärtom finns det anledning att vid utformningen av de nya bestämmelserna ta de nuvarande bestämmelserna om gallring av uppgifter i SÄPO-registret som utgångspunkt. De nya bestämmelserna bör dock omfatta även andra uppgifter än de som förekommer i ett visst register. Vidare bör den nuvarande gallringsfristen om tio år från den senaste registreringen kunna förkortas för vissa fall. Av integritetsskyddsskäl finns det dessutom anledning att överväga om inte den nuvarande möjligheten att förlänga gallringsfristen bör snävas in något.

Flera omständigheter talar för att gallringsfristerna i den nya lagen bör vara förhållandevis snäva. Uppgifter som behandlas av Säkerhetspolisen är till sin natur ofta särskilt känsliga ur integritetssynpunkt. Mängden av s.k. känsliga uppgifter torde också,

allm nt sett, vara f rh llandevis st rre hos S kerhetspolisen  n hos polisen i  vrigt.

Andra omst ndigheter talar i motsatt riktning. I den speciella verksamhet som S kerhetspolisen bedriver kan det ofta vara n dv ndigt att bevara uppgifter under l ngre tid  n inom polisen i  vrigt. Som exempel kan n mnas att fr mmande agenter kan befinna sig l nge i ett land innan de p b rjar verksamhet som  r brottslig. Det kan s ledes vara n dv ndigt att kontrollera och f lja personer under en betydligt l ngre tid n r misstanken avser brottslig verksamhet riktad mot rikets s kerhet  n vad som  r sakligt motiverat n r det g ller brottslig verksamhet av det slag som den  vriga polisen bek mpar. Vidare har flertalet av de brott som S kerhetspolisen bek mpar en straffskala som inneb r att brotten preskriberas f rst efter l ng tid.

V r slutsats  r att huvudregeln, liksom i dag, b r vara att uppgifter i S kerhetspolisens verksamhet ska gallras inom tio  r efter utg ngen av det kalender r d  den senaste registreringen avseende personen gjordes.

I fr ga om vissa personuppgifter b r det dock g lla en avsev rt kortare gallringsfrist. Personuppgifter som f rekommer i en analysdatabas b r s lunda gallras tidigare, l mpligen inom tre  r efter det kalender r d  den senaste registreringen avseende personen gjordes.

Det b r framh llas att de gallringsbest mmelser som vi f resl r avser den senaste tidpunkt n r uppgifterna m ste gallras. Om det redan f re gallringstidens utg ng st r klart att uppgifterna saknar betydelse f r den brottsbek mpande verksamheten b r de naturligtvis gallras redan d .

Den nuvarande gallringsregeln f r S APO-registret medger att uppgifter bevaras  ven sedan tio rsfristen har l pt ut, om det finns s rskilda sk l. Vad som  r s rskilda sk l utvecklas inte n rmare i f rarbetena. Det finns inte heller n gon regel som anger vid vilken tidpunkt uppgifterna d  ska gallras.

En allm n gallringsfrist om, som l ngst, tio  r utg r enligt v r mening en rimlig avv gning mellan verksamhetens behov och den enskildes krav p  att uppgifter inte ska bevaras alltf r l ng

tid. Någon gång kan emellertid tio år vara en alltför kort tid. Det bör därför även i fortsättningen finnas möjlighet att i enskilda fall bevara uppgifterna längre tid. Varje sådant avsteg från den normala gallringsfristen bör dock kräva ett särskilt beslut, där behovet av längre tids bevarande motiveras. Vidare bör beslut av detta slag vara tidsbegränsade. En särskild regel som innebär att Säkerhetspolisen ska kunna fatta beslut om bevarande under viss ytterligare tid bör därför införas. Den tiden bör inte kunna vara längre än den ursprungliga tiden för bevarande.

Liksom i dag bör regeringen eller den myndighet som regeringen bestämmer få meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.



**Promemorians förslag:** Datainspektionen, som är tillsynsmyndighet enligt personuppgiftslagen, ska utöva tillsyn över polisens behandling av personuppgifter inom den brottsbekämpande verksamheten. Personuppgiftsbehandlingen ska också granskas av Säkerhets- och integritetsskyddsnämnden.

**Utredningens förslag** överensstämmer i huvudsak med förslaget. Utredningen har dock inte lämnat något förslag om granskning genom Säkerhets- och integritetsskyddsnämnden.

**Remissinstanserna** har inte haft någon invändning mot utredningens förslag eller har inte kommenterat saken närmare.

**Bakgrund:** Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen med uppgift att bl.a. verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter (se 1 och 2 §§ förordningen [1998:1192] med instruktion för Datainspektionen och 2 § personuppgiftsförordningen [1998:1191]). Denna tillsyn omfattar även den behandling av personuppgifter som sker med stöd av polisdatalagen. Därutöver har Registernämnden till uppgift att granska Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen, särskilt med avseende på behandlingen av känsliga personuppgifter (se 1 § förordningen [2006:1076] med instruktion för Registernämnden). Utredningen om rättssäkerhet vid hemliga tvångsmedel har i betänkandet Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. (SOU 2006:98) föreslagit att Registernämndens uppgift på detta

område ska överföras till en ny nämnd, Säkerhets- och integritetsskyddsnämnden. Regeringen har den 6 september 2007 lagt fram ett motsvarande förslag i propositionen Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. (prop. 2006/07:133).

**Skälen för promemorians förslag:** Det måste antas att såväl Säkerhetspolisen som polisen i övrigt kommer att skapa interna funktioner för kontroll av att myndighetens tjänstemän följer de regler för personuppgiftsbehandling som vi nu har föreslagit. Det kan emellertid ibland vara svårt för en brottsbekämpande myndighet – för vilken det brottsbekämpande arbetet står i fokus – att göra de många gånger grannliga avvägningar mellan brottsbekämpningsintresset och integritetsintresset som blir nödvändiga. Det är mot den bakgrunden angeläget att personuppgiftsbehandlingen i polisens brottsbekämpande verksamhet blir föremål för tillsyn från ett i förhållande till polisen fristående organ. Av särskild betydelse i detta sammanhang är att mycket av den polisverksamhet där personuppgifter behandlas omfattas av sekretess. Detta får till följd att den enskilde i många fall inte kommer att kunna ges information om pågående personuppgiftsbehandling som rör honom eller henne och därmed inte heller kommer att ha några praktiska möjligheter att själv åberopa rätten till exempelvis rättelse eller skadestånd. De brister i skyddet för den enskilde som detta medför kan kompenseras genom ett fristående tillsynsorgan, som har tillgång till sekretesskyddad information. Genom tillsyn av ett fristående organ kan också risken för onödiga integritetsintrång minimeras. Här kan tilläggas att Europarådets rekommendation No. R (87) 15 om användning av personuppgifter (se avsnitt 4.2.3) förutsätter att det finns ett fristående tillsynsorgan.

Hur bör då denna tillsyn anordnas?

En möjlighet är att anförtro tillsynen i dess helhet åt Datainspektionen. Det skulle i så fall innebära en förändring vad gäller tillsynen över Säkerhetspolisens personuppgiftsbehandling. En annan möjlighet är att överlåta hela tillsynen till ett fristående organ som är särskilt inriktat på att granska brottsbekämpande

verksamhet. En tredje möjlighet är att – med viss förebild i vad som gäller i dag i fråga om personuppgiftsbehandling inom Säkerhetspolisen – anförtro tillsynsuppgifterna åt två olika myndigheter som båda har den nödvändiga fristående rollen, i detta fall dels Datainspektionen, dels en myndighet vars verksamhet är inriktad på granskning av brottsbekämpande verksamhet.

Det finns skäl som talar för att all tillsyn över myndigheternas personuppgiftsbehandling bör ligga på en enda myndighet. Framför allt blir det då alldeles klart vilken myndighet som bär ansvaret för att tillsynen blir effektiv. Samtidigt finns det fördelar med en ordning där två myndigheter, var och en från sitt perspektiv, utövar tillsyn över personuppgiftsbehandlingen i den brottsbekämpande verksamheten. Inom Datainspektionen finns det en väl utarbetad kompetens och erfarenhet vad gäller personuppgifts- och integritetsfrågor, varför en tillsyn genom Datainspektionen ger goda förutsättningar framför allt att kontrollera att allmänna principer för behandling av personuppgifter tillämpas också inom den brottsbekämpande verksamheten. Samtidigt måste det antas att ju mera insikt i och erfarenhet av den granskade verksamheten som tillsynsmyndigheten har, desto lättare kan tillsynen inriktas på de områden som kan ge upphov till särskilda risker ut integritetssynpunkt. I sammanhanget måste också beaktas att Datainspektionens tillsynsområde är mycket omfattande och att den tillsyn som inspektionen kan utöva över polisens brottsbekämpande verksamhet därmed riskerar att bli begränsad. I det perspektivet skulle det uppenbarligen vara av värde om Datainspektionens tillsyn kan kompletteras med tillsyn genom en myndighet som har till särskild uppgift att utöva tillsyn över brottsbekämpande verksamhet. En sådan ”dubbel” tillsyn förekommer, som nyss har nämnts, redan i dag, såvitt gäller behandling av personuppgifter i Säkerhetspolisens verksamhet. På försvarsunderrättelseområdet gäller också sedan länge en liknande ordning (se propositionen Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt, prop. 2006/07:46). Tillsynen över Försvarsmaktens och Försvarets

radioanstalts personuppgiftsbehandling utövas således dels av Datainspektionen, dels av Försvarets underrättelsenämnd.

Enligt vår mening talar därför övervägande skäl för att man bör välja den sist diskuterade lösningen. Den personuppgiftsbehandling som förekommer i polisens brottsbekämpande verksamhet bör således stå under tillsyn av både Datainspektionen och en annan fristående myndighet, inriktad på tillsyn över brottsbekämpande verksamhet. Det finns redan en sådan myndighet i form av Registernämnden, men dess tillsyn är begränsad till personuppgiftsbehandling på Säkerhetspolisens område. Vi anser att den kompletterande tillsynen bör avse personuppgiftsbehandlingen inom hela polisväsendet, inklusive Säkerhetspolisen och den polisiära verksamheten vid Ekobrottsmyndigheten.

Som ovan har nämnts har regeringen nyligen föreslagit att Registernämndens uppgifter, däribland uppgiften att granska Säkerhetspolisens behandling av personuppgifter enligt polisdatlagen, överförs till en ny myndighet, Säkerhets- och integritetsskyddsnämnden. Nämndens huvuduppgift ska vara att utöva tillsyn över brottsbekämpande verksamhet där det förekommer användning av hemliga tvångsmedel. Tillsynen ska utövas genom inspektioner och andra undersökningar och syfta till att säkerställa att verksamheten sker författningsenligt. Ledamöterna i nämnden ska utses av regeringen och flertalet av dem ska utses bland sådana personer som har föreslagits av riksdagsgrupperna i riksdagen. Vi bedömer att den föreslagna nämnden kommer att vara väl ägnad att granska behandlingen av personuppgifter hos polisen.

Det kan tillfogas att regeringen även har föreslagit att, såvitt gäller Säkerhetspolisens personuppgiftsbehandling, det ska ingå i Säkerhets- och integritetsskyddsnämndens uppgifter att på begäran av en enskild kontrollera bl.a. om han eller hon har varit föremål för otillåten personuppgiftsbehandling hos Säkerhetspolisen (prop. 2006/07:133 s. 66). Nämnden är skyldig att utföra kontrollen och att underrätta den enskilde som begärt kontrollen om att den har utförts. En motsvarande ordning finns i ett flertal andra länder.

Vi föreslår alltså att både Datainspektionen och Säkerhets- och integritetsskyddsmyndigheten ska ha tillsyn över det nu aktuella området.

Vilka uppgifter bör då de båda tillsynsmyndigheterna ha? Det kan då först konstateras att personuppgiftslagen tillägger tillsynsmyndigheten, dvs. Datainspektionen, vissa särskilda befogenheter, avsedda att möjliggöra en granskning av om förekommande personuppgiftsbehandling är laglig. Myndigheten har sålunda rätt att på begäran få tillgång till de personuppgifter som behandlas, upplysning om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter (se 43 § personuppgiftslagen). Om tillsynsmyndigheten efter en sådan begäran inte kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får myndigheten vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem (se 44 §). Konstaterar myndigheten att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, ska myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Går det inte att få rättelse på annat sätt, eller är saken brådskande, får myndigheten vid vite förbjuda den personuppgiftsansvarige att fortsätta behandlingen på annat sätt än genom lagring av uppgifterna (se 45 §). Vidare får myndigheten hos länsrätten ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt ska förstöras. Beslut om utplånande ska dock inte meddelas om det är oskäligt.

Enligt vår mening är det naturligt att Datainspektionen har motsvarande uppgifter och befogenheter när den utövar tillsyn över polisens personuppgiftsbehandling. Den nya lagen bör därför innehålla bestämmelser som i allt väsentligt motsvarar de nyss angivna bestämmelserna i personuppgiftslagen. Därmed kommer innehållet i inspektionens tillsyn att bli i stort sett densamma, oavsett om tillsynen avser personuppgiftsbehandling i polisens brottsbekämpande verksamhet eller personuppgiftsbehandling i annan polisiär verksamhet. Dock bör, av de skäl som

vi angett i avsnitt 6.5.2, inspektionen inte ha möjlighet att förena ett förbud mot personuppgiftsbehandling med vite.

När det sedan gäller Säkerhets- och integritetsskyddsnämndens tillsyn föreslår vi att denna, liksom Datainspektionens tillsyn, ska avse frågan om personuppgiftsbehandlingen i polisens brottsbekämpande verksamhet står i överensstämmelse med lag och annan författning och att människor skyddas mot att deras integritet kränks genom behandlingen. Nämnden bör lämpligen tillämpa samma arbetssätt som i sin övriga tillsynsverksamhet. Det innebär att den på eget initiativ eller på enskildas begäran bör kunna genomföra olika slag av inspektioner och utredningar och därvid uttala sig om huruvida det har förekommit felaktigheter vid personuppgiftsbehandlingen. Vid sådana inspektioner och utredningar bör nämnden ha rätt att få tillgång till de upplysningar och det biträde som den begär. Vi kan dock inte se något behov av att tillägga nämnden några särskilda möjligheter att meddela förelägganden eller förbud eller att ge nämnden möjlighet att föra talan i domstol. Enligt vår mening är det lämpligare om nämnden, när den uppmärksammar att det har förekommit felaktig personuppgiftsbehandling, samråder med Datainspektionen och, vid behov, anmäler den felaktiga behandlingen dit. En sådan anmälan är självfallet inte bindande för inspektionen, som självständigt bedömer vilka åtgärder som kan behöva vidtas.

En annan fråga, som hör samman med tillsynen, är om det bör införas en samrådsskyldighet för polisen gentemot Datainspektionen. I dag finns det en bestämmelse om förhandskontroll i 2 § polisdataförordningen. Den innebär att vissa typer av behandling alltid ska anmälas tre veckor i förväg. Fördelen med en bestämmelse om förhandskontroll eller samrådsskyldighet är att tillsynsmyndigheten är informerad om nya behandlingar och kan reagera om det behövs med hänsyn till den planerade behandlingen. Den nuvarande bestämmelsen om förhandskontroll har dock den svagheten att det i praktiken är svårt för Datainspektionen att påverka framtida behandlingar, eftersom anmälan inte behöver göras förrän omedelbart inför igångsättandet av en ny

behandling. Vi gör bedömningen att det i stället bör finnas en skyldighet för polisen att i vissa situationer samråda med Datainspektionen, exempelvis när polisen planerar att ta nya större system i bruk, förbereder omfattande förändringar i befintliga system eller genomför förändringar som påverkar hanteringen av särskilt känsliga uppgifter. Detta är emellertid en fråga som inte bör regleras i lag utan som regeringen kan meddela föreskrifter om.

Det kan tillfogas att utöver den tillsyn som enligt vårt förslag ska utövas av Datainspektionen och Säkerhets- och integritetsskyddsnämnden har både Justitiekanslern och Riksdagens ombudsmän rätt att i enlighet med sina instruktioner utöva tillsyn över polisverksamheten och kan då givetvis även kontrollera personuppgiftsbehandlingen.





## 20 En ny lag om polisens spaningsregister

### 20.1 Behovet av det allmänna spaningsregistret

**Promemorians bedömning:** Polisen har behov av att även fortsättningsvis kunna anteckna sådana uppgifter som i dag finns i det allmänna spaningsregistret. Den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet bör på sikt, med de förändringar av nuvarande registerhantering som Rikspolisstyrelsen planerar, i allt väsentligt utgöra ett tillräckligt stöd för att anteckna nödvändiga uppgifter. Under en övergångstid bör dock det allmänna spaningsregistret bibehållas med stöd av en särskild författningsreglering. Behovet av en reglering av ett allmänt spaningsregister bör utvärderas i samband med en kommande utvärdering av den nya lagstiftningen om personuppgiftsbehandling i polisens brottsbekämpande verksamhet.

**Utredningens bedömning:** Också utredningen har bedömt att det allmänna spaningsregistret bör författningsregleras.

**Remissinstanserna:** Både *Riksskatteverket* och *Ekobrottsmyndigheten* har instämt i att det finns ett stort behov av det allmänna spaningsregistret. Övriga remissinstanser har inte yttrat sig.

**Skälen för promemorians bedömning:** Polisen för sedan år 1979, med stöd av Datainspektionens tillstånd och numera också övergångsbestämmelserna till polisdatalagen, ett allmänt spa-

ningsregister. En närmare redogörelse för registret och dess innehåll finns i *bilaga 6*.

En grundläggande fråga är om det finns behov av det allmänna spaningsregistret i polisens nya datamiljö, eller om detta åtminstone på sikt kan ersättas med de nya möjligheter till registrering som öppnas genom den föreslagna lagstiftningen. Rikspolisstyrelsen har under arbetets gång hävdats att registret måste få finnas kvar, i vart fall tills vidare.

Polisdatautredningen, som också hänvisade till starka krav från Rikspolisstyrelsen, ansåg att utredningens förslag till polisdatalag inte skulle täcka alla de behov som det allmänna spaningsregistret avser att fylla. Utredningen påpekade att misstankeregistret förutsätter att någon är skäligen misstänkt men att det finns behov av att kunna behandla uppgifter om personer mot vilka misstanken ligger på en lägre nivå. Utredningen fann att kriminalunderrättsregister inte heller kan fylla samma behov som det allmänna spaningsregistret, eftersom underrättsregistren är inriktade på brottslig verksamhet, inte på konkreta brott. Utredningen menade därför att det alltjämt finns behov av ett allmänt spaningsregister och föreslog en särskild reglering av detta.

Det ursprungliga tillståndet att föra det allmänna spaningsregistret har ändrats genom en rad nya beslut, där registreringsgrunder har tillkommit och tagits bort. Någon sammanhållen reglering av registret finns alltså inte. Detta gör det svårt att överblicka vilka uppgifter som registret får innehålla. Tillståndet speglar också att det är fråga om ett register uppbyggt efter dåtidens teknik med begränsade sökmöjligheter. Oavsett behovet av registrering av vissa typer av uppgifter är det troligt att registret på sikt behöver moderniseras och anpassas till den nya teknik som är under uppbyggnad inom polisen.

Vår reglering av polisens möjligheter att behandla personuppgifter i den brottsbekämpande verksamheten medför en något större frihet för polisen att registrera uppgifter än den som föreslogs av Polisdatautredningen. Det innebär att många av de uppgifter som i dag registreras i det allmänna spaningsregistret på

sikt kommer att kunna göras gemensamt tillgängliga i andra former. Det kommer emellertid att ta tid för polisen att bygga upp sin nya datastruktur. Under mellantiden kommer det alltså att finnas behov av att spara de uppgifter som nu är aktuella i en särskild registermiljö. Vi föreslår därför att registret tills vidare får finnas kvar som ett särskilt register och att registret författningsregleras men att denna reglering i så stor utsträckning som möjligt bör anpassas till vad som gäller för polisens personuppgiftsbehandling i övrigt.

Den nya lagstiftningen om polisens personuppgiftsbehandling innebär så stora förändringar på ett från integritetssynpunkt särskilt känsligt område att man, på samma sätt som med den nuvarande polisdatalagen, bör utvärdera den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet så snart som möjligt efter ikraftträdandet. I denna utvärdering bör bl.a. ingå att ta ställning till om regleringen tillgodoser polisens verksamhetsbehov, bl.a. när det gäller uppgifter som i dag finns i det allmänna spaningsregistret.

## 20.2 En ny lagreglering

**Promemorians förslag:** Polisens allmänna spaningsregister ska regleras i en särskild lag. Den ska ge polisen möjlighet att registrera i huvudsak samma uppgifter som i dag. Lagen bör ha begränsad giltighetstid. Registret ska föras av Rikspolisstyrelsen som också ska vara personuppgiftsansvarig för detta.

**Utredningens förslag** innebär i huvudsak detsamma som promemorians förslag men utgår från att registret permanentas. Utredningen har föreslagit att registret ska särregleras i den nya polisdatalagen och att denna reglering i allt väsentligt ska ge polisen rätt att fortsätta den behandling av personuppgifter som redan förekommer.

**Remissinstanserna:** *Kustbevakningen* har ställt sig bakom en lagreglering. Övriga remissinstanser har inte yttrat sig.

**Skälen för promemorians förslag:** Den reglering som vi föreslagit av personuppgiftsbehandlingen i polisens brottsbekämpande verksamhet innebär att registerbegreppet i största möjliga utsträckning slopas. Vi föreslår dock att det ska behållas dels för de register som redan i dag regleras i särskilda lagar (bl.a. misstankeregistret och belastningsregistret), dels för några få andra register som av olika skäl ansetts behöva särregleras (se avsnitt 17).

Vi anser att det allmänna spaningsregistret utgör ett viktigt arbetsinstrument i polisens spaningsverksamhet och att den behandling som förekommer i registret i många avseenden bör kunna tillåtas även i fortsättningen. Enligt vår mening faller all den spaning som är knuten till ett konkret brott eller till preciserad brottslig verksamhet av visst slag in under ändamålen i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Det bedrivs emellertid även spaning som inte har en tydlig anknytning till visst brott eller viss brottslig verksamhet utan snarare till en viss person och dennes förehavanden. Sådan spaning utgör ett viktigt inslag framför allt i den mer allmänt inriktade verksamheten att förebygga och upptäcka brott. Vi anser att polisen även i fortsättningen bör kunna behandla personuppgifter för denna typ av spaning.

Det allmänna spaningsregistret omfattar i dag cirka 100 000 registrerade personer och innehåller känsliga uppgifter. Det är således en typ av register som det finns starka skäl att reglera i lag. Vi delar därför utredningens uppfattning att det allmänna spaningsregistret, med hänsyn till dess omfattning och innehåll, bör regleras i lag. Registrets nuvarande utformning låter sig emellertid svårligen förenas med den systematik som vi föreslagit ska gälla i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Detta gäller oavsett om man skulle begränsa behandlingen i registret eller inte. Enligt vår mening bör därför registret regleras i en särskild lag. Ytterligare

ett skäl för en sådan ordning är att regleringen av den aktuella behandlingen av uppgifter på sikt bör anpassas till och arbetas in i den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Lagen bör därför ha begränsad giltighetstid.

Registret bör liksom i dag föras av Rikspolisstyrelsen som också bör vara personuppgiftsansvarig för registret.

## 20.3 Utformningen av regleringen

### 20.3.1 Förhållandet till annan lagstiftning om polisregister och till personuppgiftslagen

**Promemorians förslag:** Lagen ska uttömmande reglera vad som gäller för det allmänna spaningsregistret. Lagen ska gälla vid sidan av personuppgiftslagen.

**Utredningens förslag** innebär att nära nog samtliga regler i den föreslagna polisdatalagen ska gälla även för det allmänna spaningsregistret och att den lagen ska ersätta regleringen i personuppgiftslagen.

**Remissinstanserna:** De remissinstanser som har uttalat sig om det allmänna spaningsregistret har tillstyrkt att registret regleras i lag.

**Skälen för promemorians förslag:** Vi har i avsnitt 6.5 konstaterat att personuppgiftslagens bestämmelser i väsentliga delar bör gälla vid personuppgiftsbehandling i polisens brottsbekämpande verksamhet. I vårt förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet har vi valt en lagstiftningsteknik som innebär att lagen innehåller *dels* en uttömmande uppräkningslista av de bestämmelser i personuppgiftslagen som ska tillämpas, *dels* ett antal bestämmelser som avviker från personuppgiftslagen. I bl.a. lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister används

en annan lagstiftningsmodell. Den innebär att lagen innehåller enbart de särbestämmelser som ska gälla i förhållande till personuppgiftslagen. Detta innebär att personuppgiftslagen blir tillämplig i övrigt. Enligt vår mening är det en bättre lösning när man särreglerar ett enskilt register. Den omständigheten att lagen föreslås ha en begränsad giltighetstid talar också för att regleringen bör vara så lagtekniskt enkel som möjligt. Den lösningen bör därför väljas i detta fall.

### 20.3.2 Ändamålet med registret

**Promemorians förslag:** Ändamålet med det allmänna spaningsregistret ska vara att underlätta tillgången till personuppgifter som behövs för spaning i polisens brottsbekämpande verksamhet.

**Utredningens förslag** överensstämmer delvis med promemorians förslag. Utredningen har föreslagit att registret ska få föras i syfte att underlätta tillgången till uppgifter med anknytning till polisverksamhet som består i att förebygga, upptäcka och utreda brott.

**Remissinstanserna:** Endast *Rikspolisstyrelsen* har kommenterat ändamålet med registret. Styrelsen har framhållit att polisen behöver kunna använda uppgifterna i registret även för den hjälpande verksamheten samt för handläggning av polismyndighetsärenden (t.ex. ärenden om vapenlicens). Styrelsen har föreslagit att spaningsregistret ska få användas för alla polisens uppgifter enligt 2 § polislagen (1984:387).

**Skälen för promemorians förslag:** Med hänsyn till det allmänna spaningsregistrets särdrag bör ändamålet med registret utformas på ett lite annorlunda sätt än ändamålen för polisens personuppgiftsbehandling i den brottsbekämpande verksamheten i övrigt. Vi anser att ändamålet med registret bör vara att underlätta tillgången till personuppgifter i polisens spaningsverk-

samhet. Vid spaning är det framför allt uppgifter om personer, både direkta och indirekta personuppgifter, som är mest intressanta. Det rör sig om behandling av personuppgifter som syftar till

- att finna gärningsmannen som har begått ett eller flera konkreta brott, om denne är okänd,
- att spåra en okänd person som visserligen är misstänkt därför att denne har setts på eller i närheten av en brottsplats men vars identitet inte är känd,
- att knyta en känd misstänkt person till viss brottslig verksamhet eller till ett konkret brott,
- att hitta samband mellan kriminella personer, eller
- att hitta en misstänkt person som håller sig undan polisen.

Spaning kan emellertid också ta sikte på misstänkta företeelser där man ännu inte nått den nivå att anmälan om ett konkret brott kan upprättas och där det inte heller finns tillräckligt underlag för att hävda att det förekommer brottslig verksamhet. Som exempel kan nämnas att polisen bedriver spaning mot en lokal eller en bostad där man misstänker att det pågår koppleri, narkotikaförsäljning eller olovlig försäljning av alkohol. Ofta grundar sig sådan spaning enbart på tips och iakttagelser om att det förekommer onormal trafik av personer till lokalen eller bostaden, vilket ger anledning att förmoda att någon form av olaglig verksamhet äger rum, även om man inte vet exakt vilken. Om det har förekommit en rad brott i ett visst område, t.ex. upprepade bostadsinbrott, kan spaning vara en arbetsmetod som används i förhoppning om att polisen ska påträffa den eller de skyldiga på bar gärning om de begår nya brott.

Behandling av personuppgifter med anledning av spaning som riktar sig mot personer och företeelser torde i stor utsträckning kunna ske med stöd av de nya generella bestämmelserna om personuppgiftsbehandling enligt den nya lagen. Den mera allmänt inriktade spaning som tar sikte på brottsligheten i allmänhet på en viss ort eller i en viss stadsdel torde dock sällan täckas av den regleringen. Det är framför allt för att täcka behovet hos närpolisen och den ordningshållande delen av polisen av ett arbetsred-

skap som knyter samman deras iakttagelser av personer och händelser, som kan ha samband med begångna brott eller misstänkt brottslig verksamhet, som ett separat spaningsregister kan behövas.

Vi anser att det direkt av ändamålet med registret bör framgå att uppgifterna behövs för spaning. Det innebär att uppgifter som enbart berör tidigare uppklarade brott i många fall faller utanför ändamålet med registret. Syftet är inte heller att registret ska innehålla uppgifter som skapar ett parallellt belastningsregister.

Vår avsikt med rekvisitet ”behövs för spaning” är att det ska finnas ett konkret behov av att registrera uppgifter som en större krets av personer inom polisen måste kunna ha tillgång till i sitt spaningsarbete. Behovsrekvisitet är således avsett att begränsa möjligheten att registrera uppgifter. Endast sådana uppgifter som har faktisk betydelse för spaningsarbetet, brottsuppleringen eller för spaningen i pågående brottsutredningar ska få registreras. Uppgifter som inte har relevans för den brottsbekämpande verksamheten ska således inte få registreras, även om de skulle ha ett allmänt intresse för polisen. Det ligger emellertid i sakens natur att det inte alltid går att på förhand avgöra om en viss uppgift har relevans för kommande spaningsverksamhet. Det bör därför räcka att det framstår som sannolikt att det finns ett behov av uppgiften i spaningsverksamheten. Avsikten är dock inte att registret ska kunna användas för att systematiskt kartlägga enskilda personer, vilkas kriminalitet inte är så allvarlig att personuppgifter om dem får behandlas med stöd av bestämmelserna om övervakning av brottsbelastade eller potentiellt farliga personer i den nya lagen om personuppgiftsbehandling i polisens brottsbekämpande verksamhet. Vi återkommer i nästa avsnitt till det närmare innehållet i registret.

*Rikspolisstyrelsen* har ifrågasatt om inte registret även ska föras för andra än brottsbekämpande ändamål. Det skulle enligt vår mening föra för långt om det allmänna spaningsregistret skulle få användas exempelvis i polisens hjälpande verksamhet. En annan sak är att uppgifter ur registret i vissa fall bör kunna



lämnas ut för viss annan polisverksamhet än den brottsbekämpande. Vi återkommer till frågan om möjligheten att lämna ut uppgifter ur registret i avsnitt 20.3.6.

### 20.3.3 Innehållet i registret

**Promemorians förslag:** Lagen om polisens allmänna spaningsregister ska innehålla bestämmelser om vilka kategorier av uppgifter som får behandlas.

Uppgifter som kan hänföras till en enskild person ska som huvudregel få behandlas endast om

1. den som uppgiften avser kan misstänkas ha begått ett brott, som inte enbart har böter i straffskalan, och
2. behandlingen är av särskild betydelse för brottsbekämpningen.

Även uppgifter som kan hänföras till personer som inte kan misstänkas för brott ska dock få behandlas om uppgiften har samband med en misstänkt person och uppgiften har särskild betydelse för polisens spaningsverksamhet.

Därutöver ska uppgifter om en juridisk person, ett transportmedel eller annat föremål som kan antas ha samband med ett brott få behandlas, om behandlingen är av särskild betydelse för brottsbekämpningen. Detta gäller dock inte om brottet enbart har böter i straffskalan.

Registret ska alltid innehålla uppgifter om

1. grunden för att en person antecknas som misstänkt eller att en juridisk person, ett transportmedel eller föremål införs i registret och omständigheterna i samband med detta,
2. de omständigheter och händelser som ger upphov till att andra uppgifter än de som anges i 1 tillförs registret,
3. den behandlade uppgiftens ursprung, och
4. uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Därutöver får registret innehålla bl.a. följande uppgifter om en registrerad person:

- uppgift som är ägnad att identifiera personen,
- uppgift om vistelseadress,
- uppgift om verkställighet av påföljd för brott,
- uppgift om att personen är eftersökt i samband med brott,
- uppgift om att personen tidigare har varit beväpnad, våldsam eller flyktbenägen,
- uppgift om att personen är föremål för särskild övervakning.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om de uppgifter som får behandlas i registret och om förfarandet vid registreringen.

**Utredningens förslag:** Utredningen har föreslagit att uppgifter om en enskild person får registreras endast om den som avses med uppgiften kan misstänkas för att ha begått ett brott och registreringen är av särskild betydelse för brottsbekämpningen. Vidare ska uppgifter om transportmedel eller varor som kan antas ha samband med brott samt hjälpmedel som kan ha använts i samband med brott få registreras, även om uppgifterna kan hänföras till en person mot vilken det inte finns någon misstanke.

**Remissinstanserna:** Endast *Rikspolisstyrelsen* har yttrat sig angående innehållet i registret. Styrelsen har tolkat förslaget så att man även i fortsättningen ska kunna i registret markera om en person tillhör landets allra grävsta brottslingar (s.k. A-markering) eller om vederbörande anses vara yrkeskriminell (s.k. Y-markering). Rikspolisstyrelsen anser att detta bör framgå direkt av lagtexten.

## Skälen för promemorians förslag

### *Allmänna utgångspunkter*

En utgångspunkt i vårt förslag är att den nya regleringen av det allmänna spaningsregistret, så långt det kan motiveras av ett behov i den polisiära verksamheten, bör motsvara den registrering som sker i dag. Samtidigt är det givetvis angeläget att man inte tillåter en registrering som inte är acceptabel med hänsyn till skyddet för den personliga integriteten. Den enskilde bör således i så stor utsträckning som möjligt ges samma skydd vid behandling av uppgifter i det allmänna spaningsregistret som vid behandling av uppgifter i polisens brottsbekämpande verksamhet i övrigt.

Vi anser därför att lagen bör innehålla regler inte bara om vad som krävs för att en person ska bli registrerad utan också om vilka andra uppgifter som får behandlas. Dessutom bör det införas begränsningar i fråga om vilka uppgifter som får vara sökbara i registret. Detta är begränsningar som i större eller mindre utsträckning har sin motsvarighet i det nuvarande tillståndet att föra det allmänna spaningsregistret.

### *Uppgifter om misstänkta personer*

För att en person ska få registreras bör det enligt vår mening för det första krävas att han eller hon är misstänkt för ett brott. Det bör räcka med en låg grad av misstanke, men det ska vara fråga om ett brott som ännu inte har lagförts. Eftersom registret syftar till att underlätta spaningsarbetet, kan lagförda brott inte läggas till grund för registreringen; dessa brott är ju uppklarade och kräver således ingen spaning.

Rikspolisstyrelsens föreskrifter om det allmänna spaningsregistret (RPS FS 2003:4, FAP 448–1) innehåller en uppräkningslista av ett stort antal brottsbalksbrott (brott mot 3–4, 6, 8–14, 16 och 17 kap. brottsbalken) och vissa brott mot specialstraffrättsliga

bestämmelser som utgör grund för behandling. En sådan uppräkningslista har bl.a. den nackdelen att den inte fångar in nya brottstyper. Som exempel kan nämnas att uppräkningslistan innehåller brott mot ransoneringslagen och valutabrott, som knappast förekommer, medan brott mot kreditupplysningslagen (1973:1173) inte täcks in, trots att det är en brottstyp som förknippas med brottslighet av organiserat slag.

Vi anser att man bör välja en mera generell lösning. Det får till följd att å ena sidan några av de brottstyper som i dag kan läggas till grund för registrering faller bort. Å andra sidan kan då vissa nya brottstyper ligga till grund för registrering. En enligt vår mening lämplig lösning är att avgränsa registreringen till personer som är misstänkta för brott som inte endast har böter i straffskalan. Det kan däremot inte anses motiverat att låta registret omfatta uppgifter om personer som enbart är misstänkta för bagatellobrott.

Förutom misstanke om brott av visst slag bör det krävas att behandlingen av personuppgifter är av särskild betydelse för brottsbekämpningen. I tillståndet till det nuvarande registret finns en likartad formulering. Kravet innebär att uppgifter som visserligen skulle ha allmänt värde för spaningsverksamheten, men där värdet inte är så stort, inte får behandlas. För att en uppgift ska anses ha särskild betydelse bör det krävas att den kan bidra till att brott, som är av sådan svårhetsgrad som krävs för behandling i registret, kan beivras. Det krävs en kvalificerad bedömning av om uppgifterna faktiskt har sådan betydelse. I dag är det endast ett fåtal tjänstemän som får göra den bedömningen.

#### *Uppgifter om andra personer och om föremål*

Vi anser vidare att det, på samma sätt som i dag, bör vara möjligt att i registret behandla även uppgifter som avser personer som inte är misstänkta för brott. Sådana uppgifter bör dock få behandlas endast om uppgiften har anknytning till en misstänkt person. Vidare bör det krävas att uppgiften är av särskild betydelse.

delse för polisens spaningsverksamhet. Bestämmelserna om vilka kategorier av uppgifter som får behandlas begränsar möjligheten att behandla uppgifter om icke-misstänkta personer ytterligare. I dag behandlas sådana uppgifter i löpande text och är inte sökbara. Det rör sig t.ex. om uppgifter om att en viss namngiven person har setts i en misstänkt persons sällskap eller att den misstänkte brukar bo hos en namngiven anhörig. Vi återkommer i det följande till vilka sökbegränsningar som ska gälla, se avsnitt 20.3.5.

Polisen har vidare ett behov av att kunna behandla uppgifter om fordon och andra föremål som *kan antas ha samband* med ett brott. Det rör sig här om indirekta personuppgifter, t.ex. om vem som är ägare till ett registrerat fordon som uppges ha lämnat en brottsplats i hög fart i nära anslutning till brottet. I många fall tillhör sådana fordon helt oskyldiga personer, eftersom stulna bilar ofta används som flyktfordon. I andra fall kan uppgifter om fordonet leda till att gärningsmannen kan spåras. Vi anser att uppgifter av detta slag bör kunna behandlas även i fortsättningen. En allmän förutsättning för detta bör dock vara att uppgifterna är av särskild betydelse för brottsbekämpningen.

Likaså har polisen behov av att i vissa fall, där det inte finns någon misstanke mot någon fysisk person, kunna registrera uppgifter om en juridisk person som kan antas ha samband med ett misstänkt brott. Det kan t.ex. röra sig om ett aktiebolag som äger eller disponerar en lokal där smuggelgods förvaras eller någon annan typ av juridisk person som äger eller hyr en lokal där alkohol eller narkotika tillverkas. Det kan även vara fråga om en juridisk person som har utfärdat vissa handlingar som utnyttjas för brottslig verksamhet. Samma förutsättningar som har föreslagits gälla för registrering av transportmedel bör gälla för registrering av juridiska personer.

*Registrets närmare innehåll*

Lagen om polisens allmänna spaningsregister bör reglera både vilka uppgifter som alltid måste finnas i registret och vilka uppgifter som därutöver får behandlas.

Vissa uppgifter i registret bör vara obligatoriska. Vi anser för det första att det alltid ska kunna utläsas vad som har motiverat att en person eller uppgifter om ett transportmedel eller annat föremål första gången har förts in i registret. Det måste således finnas uppgifter om det brott som har föranlett att en viss person har antecknats såsom misstänkt. Även omständigheterna kring brottet bör redovisas. Dessutom bör andra uppgifter om brottet, t.ex. att det fanns flera gärningsmän, kunna noteras, om uppgiften har betydelse för polisens spaningsarbete. Motsvarande krav bör ställas om det beträffande en registrerad person införs uppgifter om nya brottsmisstankar eller beträffande en juridisk person, ett transportmedel eller annat föremål införs nya uppgifter om samband med brott.

För det andra bör det framgå vad som har legat bakom att nya uppgifter av annat slag om en registrerad person tillförs registret. Här är det närmast fråga om vilka omständigheter eller händelser som gett upphov till den nya anteckningen. Det är nämligen vanligt att en registrering så småningom följs av nya noteringar om den registrerade personen, om uppgifterna är av värde från spaningssynpunkt. Det kan t.ex. röra sig om uppgifter om vilka personer en misstänkt narkotikabrottsling träffar, vilka fordon en misstänkt inbrottstjuv disponerar osv. Det är framför allt i dessa noteringar som det kan finnas uppgifter om personer, som inte själva är misstänkta för brott.

Vidare bör det vara obligatoriskt att ange källan till uppgiften och att, på samma sätt som nu, göra en bedömning av källans trovärdighet och tillförlitlighet. En sådan bedömning görs för närvarande av den person som avgör om uppgifterna har sådant värde från spaningssynpunkt att de över huvud taget bör tillföras registret.

Av lagen bör också framgå vilka ytterligare uppgifter om den registrerade som får behandlas. Uppräkningen bör vara uttömmande. Det bör vara fråga om uppgifter som typiskt sett är viktiga för polisens spaningsverksamhet och som i huvudsak motsvarar vad som får registreras i det allmänna spaningsregistret i dag. Eftersom spaning kan äga rum antingen med anledning av ett begånget brott eller i underrättelsesyfte, bör det finnas utrymme för uppgifter som underlättar båda typerna av spaning, framför allt uppgifter som underlättar personrelaterad spaning. Det rör sig exempelvis om uppgifter om var personen vistas, uppgifter som kan bidra till identifieringen av denne, uppgifter om anknytningen till juridiska personer och uppgifter som underlättar vid direkta ingripanden mot personen i fråga.

För att så långt som möjligt anpassa systemet till de behov som finns i verksamheten bör regeringen, eller den myndighet som regeringen bestämmer, få meddela närmare föreskrifter om de uppgifter som får behandlas i registret och om förfarandet vid registrering. Liksom i dag bör endast särskilt utpekade tjänstemän få besluta om när uppgifter ska tillföras registret.

#### 20.3.4 Behandling av känsliga personuppgifter

**Promemorians förslag:** Uppgifter om en person får inte behandlas på grund av vad som är känt om personens ras, etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Uppgifter som behandlas på annan grund får dock kompletteras med sådana uppgifter, om det är absolut nödvändigt för syftet med behandlingen.

Uppgifter om en persons utseende ska alltid utformas på ett objektiva sätt med respekt för människovärdet.

**Utredningens förslag** överensstämmer i sak med promemorians förslag. Utredningen har dock inte föreslagit någon begränsning när det gäller uppgifter om personers utseende.

**Remissinstanserna** har tillstyrkt utredningens förslag eller inte haft någon invändning mot det.

**Skälen för promemorians förslag:** Det finns särskilda regler om behandling av känsliga personuppgifter både i den nuvarande polisdatalagen (5 §) och i vårt förslag till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet (se avsnitt 8). En sådan bestämmelse – som också uppfyller kraven i artikel 2.5 i Europarådets rekommendation om polisens användning av personuppgifter – bör enligt vår mening också införas i lagen om polisens allmänna spaningsregister.

Bestämmelsen bör utformas efter mönster av den bestämmelse som vi har föreslagit ska tas in i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Det innebär att känsliga personuppgifter inte ska få behandlas ensamma. Däremot bör, om personuppgifter behandlas på annan grund, dessa få kompletteras med känsliga personuppgifter men endast om detta är absolut nödvändigt för syftet med behandlingen. Vidare bör det införas en bestämmelse om att uppgifter om en persons utseende alltid ska utformas på ett objektivt sätt och med respekt för människovärdet.



### 20.3.5 Särskilda uppgifter och sökbegränsningar

**Promemorians förslag:** Uppgifter, som direkt kan hänföras till en person som inte misstänks för brott, ska föras med en särskild upplysning om detta. Detsamma gäller uppgifter om en juridisk person eller ett transportmedel som indirekt kan hänföras till en sådan person. Någon upplysning behöver dock inte lämnas om det ändå framgår tydligt av omständigheterna att personen inte är misstänkt. Uppgifter som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara i registret.

**Utredningens förslag** överensstämmer med promemorians förslag vad gäller särskilda uppgifter. Utredningen har dock inte föreslagit att det ska gälla någon sökbegränsning för uppgifter om icke misstänkta personer.

**Remissinstanserna** har inte yttrat sig i saken.

**Skälen för promemorians förslag:** Som har framgått ovan anser vi att det allmänna spaningsregistret också bör få innehålla uppgifter om personer som inte är misstänkta för brott. Frågan är nu i vilken utsträckning sådana uppgifter bör föras med särskilda uppgifter och vilka sökbegränsningar som bör gälla.

Vi har föreslagit att lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet ska innehålla bestämmelser om att uppgifter som rör icke misstänkta personer, och som har gjorts gemensamt tillgängliga, som huvudregel ska föras med en upplysning om att personen i fråga inte är misstänkt (3 kap. 4 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet). Vi anser att motsvarande bestämmelser bör gälla för behandling av uppgifter i det allmänna spaningsregistret. Det innebär också att någon särskild upplysning inte ska behöva lämnas om det ändå tydligt av omständigheterna framgår att personen i fråga inte är misstänkt.

Vi anser också att uppgifter som direkt hänför sig till personer som inte själva är misstänkta inte bör få vara sökbara. Detta

motsvarar vad vi föreslår ska gälla enligt lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. I den lagen föreslås emellertid vissa undantag gälla.

Däremot bör indirekta personuppgifter som rör transportmedel och andra föremål kunna vara sökbara, på samma sätt som är fallet i dag. Uppgifter av det slaget är viktiga från spaningssynpunkt, samtidigt som det integritetsintrång som en behandling kan medföra är begränsat. Uppgifter om fordon är redan tillgängliga för gemene man och polisens behandling av dessa uppgifter kan – även om behandlingen innebär att uppgifterna sätts i samband med brott – inte sägas vara särskilt integritetskänslig. Detsamma gäller uppgifter om andra transportmedel. När det gäller andra föremål kan man inte dra lika generella slutsatser om risken för integritetsintrång, men eftersom uppgifterna kan ha stor betydelse för spaningsverksamheten, t.ex. en uppgift om var ett visst skjutvapen hör hemma, bör en behandling som innebär att uppgiften är sökbar ändå kunna godtas.

Även uppgifter om juridiska personer bör, liksom i dag, vara sökbara i registret. Sådana uppgifter har också ofta ett stort spaningsvärde. I detta fall finns uppgifterna normalt också tillgängliga i offentliga register och det eventuella integritetsintrånget är därför begränsat.

### 20.3.6 Utlämnande av uppgifter ur registret

**Promemorians förslag:** Personuppgifter som behövs för framställning av rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) ska uppgifter lämnas till

1. polismyndighet, Ekobrottsmyndigheten, Skatteverket, Tullverket och Kustbevakningen, om myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet, eller

2. polismyndighet om myndigheten har behov av uppgiften i annan verksamhet än den brottsbekämpande verksamheten och det finns särskilda skäl för att lämna ut den.

Regeringen får meddela föreskrifter om utlämnande i andra fall.

Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Polismyndigheter, Ekobrottsmyndigheten, Tullverket och Kustbevakningen ska kunna medges direktåtkomst till det allmänna spaningsregistret. Som huvudregel ska endast enstaka uppgifter få lämnas ut på medium för automatiserad behandling.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter som rör direktåtkomsten.

**Utredningens förslag:** Utredningen har föreslagit att uppgifter ur det allmänna spaningsregistret ska få lämnas ut till Ekobrottsmyndigheten, Kustbevakningen, en tullmyndighet eller en skattemyndighet, men endast om uppgifterna kan antas ha särskild betydelse för en pågående undersökning eller för andra brottsbekämpande åtgärder. Utredningen har vidare föreslagit att endast polismyndigheterna ska kunna få direktåtkomst till registret.

**Remissinstanserna:** Flera remissinstanser, däribland *Sveriges domareförbund* och *Kammarrätten i Jönköping*, har ifrågasatt

varför möjligheten att bevilja direktåtkomst generellt är så begränsad i utredningens förslag. *Riksskatteverket* har noterat att förslaget inte förfaller innebära någon förändring för skattebrottsenheternas del och framhållit behovet av samverkan mellan de brottsbekämpande myndigheterna.

### Skälen för promemorians förslag

#### *Utlämnande av uppgifter ur registret*

I avsnitt 12 har vi ingående diskuterat behovet av informationsutbyte för en effektivare brottsbekämpning. Vad som har sagts där har giltighet även för det allmänna spaningsregistret. Detsamma gäller behovet av tillgång till uppgifter genom direktåtkomst (avsnitt 12.3). För att möjliggöra informationsutbyte krävs det att särskilda regler om utlämnande tas in i den föreslagna lagen om polisens allmänna spaningsregister. Dessa regler bör utformas efter mönster av reglerna i förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

En regel om utlämnande av uppgifter bör enligt vår mening först och främst tillgodose behovet av att kunna lämna uppgifter från en polismyndighet till en annan. Vidare måste uppgifter kunna lämnas till andra brottsbekämpande myndigheter, eftersom brottsbekämpningen är en gemensam uppgift för flera myndigheter. De myndigheter som idag har möjlighet att få uppgifter ur det allmänna spaningsregistret bör kunna få det även när registret lagregleras. Vi föreslår därför att polismyndigheter, Ekobrottsmyndigheten, Skatteverket, Tullverket och Kustbevakningen ska kunna få tillgång till uppgifter ur registret.

Enligt vår mening bör en grundläggande förutsättning för att uppgifter ska kunna lämnas ut vara att den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet. Här kan anmärkas att åtkomsten till uppgifter i det allmänna spaningsregistret, för andra myndigheter än polismyn-

digheter, hittills har begränsats till sådana brottstyper som den mottagande myndigheten ska bekämpa. Som exempel kan nämnas Tullverket, vars åtkomst är begränsad till i huvudsak uppgifter om smuggling och om narkotikabrott. Vi anser att man inte bör ställa upp begränsningar av det slaget i lag. Däremot bör man ha samma generella begränsning som i den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, nämligen att tillgången till personuppgifter alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Vi anser vidare att uppgifter bör kunna lämnas ut till en polismyndighet, om myndigheten har behov av uppgiften i annan verksamhet än den brottsbekämpande och det finns särskilda skäl för att lämna ut uppgiften. Det bör således vara möjligt att lämna uppgifter ur registret i särskilda fall, även om utrymmet för detta bör vara mycket begränsat. Det kan t.ex. vara av stort värde för bedömningen av vissa tillståndsärenden att få kännedom om att en viss person har nära anknytning till exempelvis personer som misstänks för s.k. mc-kriminalitet. Vidare kan det, för polismännens personliga säkerhet, vara av stor betydelse att få veta om en person tidigare har uppträtt våldsamt vid polisinsgripanden.

Uppgifter som behövs för att framställa rättsstatistiken bör alltid få lämnas ut till den statistikansvariga myndigheten. Motsvarande bestämmelser finns i de andra registerlagar som reglerar polisens brottsbekämpande verksamhet.

Slutligen bör lagen också innehålla en bestämmelse om utlämnande av uppgifter ur registret till utländska myndigheter och mellanfolkliga organisationer. Bestämmelsen bör utformas efter mönster av den bestämmelse vi föreslagit i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Uppgifter ska således alltid kunna lämnas ut, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Vidare bör, på samma sätt som i dag, uppgifter kunna lämnas till en utländsk polis- eller åklagarmyndighet, eller till Interpol eller Europol. Förut-

sättningarna för detta bör vara dels att utlämnandet är förenligt med svenska intressen, dels att uppgiften behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott. Den som överväger att lämna ut en uppgift måste dessutom alltid försäkra sig om att den mottagande staten eller organisationen har en adekvat nivå för skydd av personuppgifter, se 33 och 34 §§ personuppgiftslagen. De nu föreslagna bestämmelserna om utlämnande till utländsk myndighet överensstämmer i huvudsak med vad som gäller i dag enligt polisdatlagen och polisdataförordningen.

#### *Sekretess*

I avsnitt 13 har vi ingående redovisat behovet av sekretessbrytande bestämmelser. Vad vi sagt där har giltighet även för utlämnande av uppgifter ur det allmänna spaningsregistret. För att det ska vara möjligt att bevilja direktåtkomst till uppgifter i registret dels till polismyndigheterna, dels till andra brottsbekämpande myndigheter, krävs det en särskild sekretessbrytande regel i den nya lagen. Denna regel kan utformas efter mönster av de motsvarande bestämmelser som vi föreslår ska tas in i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

#### *Direktåtkomst m.m.*

I dag har fler myndigheter än vad utredningen föreslog möjlighet att få direktåtkomst till det allmänna spaningsregistret. De myndigheter som för närvarande har direktåtkomst bör därför kunna få det även fortsättningsvis. Det finns enligt vår mening inget skäl att reglera direktåtkomsten till detta register på något i avgörande avseenden annat sätt än direktåtkomsten till belastningsregistret eller misstankeregistret (eller den föreslagna lagen om personuppgiftsbehandling i polisens brottsbekämpande verksamhet). De uppgifter som kan behandlas i dessa register

och uppgiftssamlingar kan vara lika integritetskänsliga som uppgifter i det nu aktuella registret. Huvudregeln bör alltså vara att de myndigheter som har rätt till uppgifter ur registret också ska kunna beredas direktåtkomst till detta. I ett mindre avseende finns det emellertid skäl att avvika från huvudregeln. Det allmänna spaningsregistret har sådant innehåll att endast myndigheter som själva bedriver spaningsverksamhet bör kunna medges direktåtkomst. Dessutom bör spaningsverksamheten i fråga röra brott med fängelse i straffskalan. Detta innebär att Skatteverket inte bör kunna medges direktåtkomst.

Det bör ankomma på Rikspolisstyrelsen att avgöra dels om myndigheternas behov av uppgifter är så stort att direktåtkomst är motiverad, dels om det är möjligt att bevilja direktåtkomst med hänsyn till mottagarens datasäkerhet m.m. Rikspolisstyrelsen kan givetvis, på samma sätt som nu, begränsa åtkomsten till vissa typer av uppgifter eller till uppgift om huruvida någon förekommer i registret eller inte. Det bör vidare ankomma på regeringen, eller den myndighet regeringen bestämmer att meddela närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Liksom för övrig personuppgiftsbehandling inom polisen bör huvudregeln vara att endast enstaka uppgifter ur det allmänna spaningsregistret ska få lämnas ut på medium för automatiserad behandling (se avsnitt 14).

### 20.3.7 Gallring

**Promemorians förslag:** Uppgifter om en misstänkt person ska gallras senast tre år efter det att en uppgift om att han eller hon kan misstänkas för att ha begått ett brott senast infördes. Avser den senast införda uppgiften misstanke om ett brott med lägst två års fängelse i straffskalan, behöver dock uppgifterna inte gallras förrän efter fem år.

Om en ny uppgift om den misstänkte införs före utgången av den tid som anges i första stycket kan gallringstiden förlängas. Uppgifter om en person som inte är misstänkt för brott ska gallras senast samtidigt som uppgifterna om den misstänkte som registreringen anknyter till gallras.

Uppgifter om en juridisk person, ett transportmedel eller annat föremål som har registrerats utan anknytning till någon misstänkt person ska gallras senast tre år efter den senaste registreringen. Om den senast införda uppgiften avser ett brott med lägst två års fängelse i straffskalan, behöver dock uppgifterna inte gallras förrän fem år efter att den senaste uppgiften infördes.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar ytterligare föreskrifter om gallring i vissa fall.

**Utredningens förslag:** Utredningen har föreslagit att personuppgifter ska gallras ur det allmänna spaningsregistret senast tre år efter det att uppgifter om den registrerade kan misstänkas ha begått brott senast infördes. Om den senaste händelsen avser misstanke om ett brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, ska dock uppgifterna få stå kvar i fem år efter den senaste registreringen.

**Remissinstanserna:** *Rikspolisstyrelsen*, *Riksåklagaren* och *Kriminalvårdsstyrelsen* har alla kritiserat utredningens förslag om gallringsfrister och hävdade att vissa uppgifter bör få behandlas under längre tid.



**Skälen för promemorians förslag:** Gallringsreglerna för det allmänna spaningsregistret är i dag komplicerade. Fristerna knyter an dels till brottets svårhetsgrad med tre olika frister (fem år, tre år och 18 månader), dels till typen av uppgift som registrerats (t.ex. 6 månaders gallringsfrist för transportmedel), dels till förekomsten av nya uppgifter om den registrerade. I det sistnämnda fallet innebär gallringsreglerna att vissa typer av noteringar innebär en något längre och andra en något kortare gallringstid. Något förenklat kan man säga att uppgifter av mer begränsat spaningsvärde (t.ex. uppgifter om fordon) gallras tidigare än uppgifter som generellt sett anses ha större spaningsvärde (t.ex. uppgifter om samröre med andra personer). Om det införs nya uppgifter i registret om den registrerade personen eller objektet, förlängs gallringsfristen, i vissa fall 18 månader och i andra fall kortare tid. Uppgifter om en person gallras omedelbart i vissa fall där det står klart att det inte längre finns någon brottsmisstänke. Slutligen finns det även en bestämmelse som hindrar gallring i vissa fall.

Remisskritiken visar enligt vår mening att en enhetlig gallringsregel av det slag som utredningen föreslog inte i tillräcklig utsträckning tillgodoser verksamhetens behov. Det är å andra sidan inte lämpligt att i en lag skapa så svåröverskådliga gallringsregler som tillämpas för det allmänna spaningsregistret för närvarande. Behovet av en effektiv verksamhet talar för att uppgifter som är viktiga för spaningsverksamheten ska kunna bevaras. Mot det står att uppgifterna i det allmänna spaningsregistret dels rör ett stort antal personer, dels bygger på misstankar som inte är så fast underbyggda att de kan registreras i misstankeregistret. Att bevara sådana uppgifter under en längre tid innebär en påtaglig risk för integritetsintrång.

En rimlig avvägning mellan intresset av att bekämpa brott och integritetsskyddsintresset är enligt vår mening att utgå från vad som föreslogs av utredningen och som i stor utsträckning tillämpas i dag, nämligen gallringsfrister på tre respektive fem år, beroende på vilket brott misstanken avser. Om det tillkommer nya brottsmisstankar, bör gallringsfristen kunna förlängas med

tre respektive fem år. Om registret tillförs andra uppgifter som är av särskilt värde för spaningsverksamheten, bör tiden för gallring också flyttas fram, men då bara med ett år.

På motsvarande sätt bör gallringsfristen för uppgifter om en juridisk person, ett transportmedel eller annat föremål som har införts i registret utan samband med en registrerad person konstrueras med utgångspunkt i det misstänkta brottet. Uppgifterna bör således gallras senast efter tre respektive fem år, med möjlighet till förlängning av gallringsfristen om en ny uppgift som kan antas ha samband med ett brott antecknas.

I de fall där registret har tillförts uppgifter om en person som inte själv kan misstänkas för brott men som har samband med en registrerad person, bör uppgifterna gallras senast samtidigt som uppgifterna om den registrerade personen gallras.

De nu angivna gallringsfristerna utgör en ram, varför mer detaljerade regler bör meddelas av regeringen eller av den myndighet som regeringen bestämmer. Det kan t.ex. finnas behov av regler om bevarande för historiska, statistiska eller vetenskapliga ändamål. Det kan också finnas skäl att överväga kortare gallringsfrister för vissa typer av uppgifter, t.ex. för uppgifter om fordon. Regeringen, eller den myndighet som regeringen bestämmer, bör också ha möjlighet att i ett enskilt fall besluta att uppgifter får bevaras om det finns synnerliga skäl för det. De närmare detaljerna angående gallringen utvecklas i författningskommentaren.

### 20.3.8 Övriga frågor

**Promemorians förslag:** Bestämmelserna i personuppgiftslagen om rättelse och skadestånd ska gälla för behandling enligt lagen.

**Utredningens förslag** motsvarar i sak promemorians förslag.

**Remissinstanserna** har tillstyrkt förslaget eller inte haft några synpunkter på det.

**Skälen för promemorians förslag:** På motsvarande sätt som inom andra områden kan det inte uteslutas att personuppgifter som behandlas med stöd av de nya bestämmelserna vid en kontroll i efterhand visar sig vara behäftade med felaktigheter. För sådana fall bör den registrerade vara berättigad till skadestånd under samma förutsättningar som gäller för behandling som omfattas av personuppgiftslagen (28 och 48 §§). Med hänsyn till hur dessa regler är utformade måste en särskild hänvisning göras till dem för att de ska gälla för behandling som sker enligt den nya lagen (jfr prop. 1997/98:97 s. 90).



## 21 Följändringar

**Promemorians förslag:** Följändringar görs i rättegångsbalken, sekretesslagen, säkerhetsskyddslagen och lagen om Schengens informationssystem.

**Utredningens förslag:** Överensstämmer i huvudsak med promemorians förslag.

**Remissinstanserna** har inte yttrat sig i saken.

**Skälen för promemorians förslag:** I ett antal lagar förekommer det hänvisningar till polisdatalagen eller till vissa register som förs med stöd av den lagen. Dessa hänvisningar bör nu ersättas med hänvisningar till den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet och, i vissa fall, den föreslagna lagen om polisens allmänna spaningsregister. Ändringar av detta slag bör göras i rättegångsbalken, sekretesslagen (1980:100) och lagen (2000:344) om Schengens informationssystem och kommer inte att innebära några förändringar i sak.

Liknande ändringar bör göras i säkerhetsskyddslagen (1996:627). Bestämmelsen om registerkontroll i 12 § säkerhetsskyddslagen bör dock utformas på ett sådant sätt att det medför en viss ändring i sak i förhållande till gällande rätt. I paragrafen behandlas sådan registerkontroll som görs inom ramen för en säkerhetsprövning. Enligt paragrafen avses med registerkontroll dels att uppgifter hämtas från register som omfattas av lagen om belastningsregister, lagen om misstankeregister eller polisdatalagen, dels att uppgifter hämtas som Rikspolisstyrelsen eller

Säkerhetspolisen annars behandlar. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller särskild utredning. Bestämmelsen fick sin nuvarande lydelse efter förslag i propositionen Polisens register som ledde fram till bl.a. polisdatalagen (prop. 1997/98:97, bet. 1997/98:JuU20). Dessförinnan avsågs med registerkontroll ”att uppgifter hämtas från polisregister”. I författningskommentaren i den nämnda propositionen angavs att ändringen var en följd av att polisregisterbegreppet inte längre används i den betydelse det tidigare haft men att någon ändring i sak i förhållande till gällande rätt inte var avsedd.

Registerkontrollen utgör en del av den säkerhetsprövning som syftar till att pröva en persons pålitlighet från säkerhetssynpunkt, för att förebygga att personer som inte är pålitliga deltar i verksamhet som har betydelse för rikets säkerhet. Registerkontrollens omfattning är olika beroende på om personen i fråga är placerad i säkerhetsklass 1, 2 eller 3. Den nuvarande registerkontrollen omfattar alltid kontroll av uppgifter i belastningsregistret och misstankeregistret och av uppgifter som behandlas hos Säkerhetspolisen. För kontroll av personer placerade i säkerhetsklass 1 och 2 görs ytterligare kontroller, dels inom ramen för registerkontrollen, dels inom ramen för en särskild personutredning enligt 18 § säkerhetsskyddslagen.

Att i en bestämmelse om registerkontroll uttömmande ange vilken kontroll som ska utföras låter sig knappast göras. Ett av skälen till detta är att man inte längre kan använda tekniken att hänvisa till vissa register, eftersom behandling av uppgifter som kan vara av betydelse för kontrollen inte längre sker enbart i traditionella register. Med hänsyn bl.a. till syftet med kontrollen är det enligt vår mening inte heller lämpligt att i lag uttömmande reglera omfattningen av registerkontrollen, eftersom behovet av kontroll kan variera. Bestämmelser om den närmare omfattningen av registerkontrollen bör i stället meddelas på lägre normgivningsnivå. I syfte att garantera en grundläggande nivå på kontrollen, som inte får underskridas, bör det dock i lag anges

vilken kontroll som alltid *ska* utföras. Därutöver bör det anges vilken kontroll som *får* utföras.





## 22 Kustbevakningens åtkomst till vissa register

**Promemorians förslag:** I lagen om misstankeregister och lagen om belastningsregister införs bestämmelser om att Kustbevakningen ska ha rätt att i sin brottsbekämpande verksamhet få ut uppgifter ur misstankeregistret och belastningsregistret.

**Promemorians bedömning:** Kustbevakningen bör kunna medges direktåtkomst till misstankeregistret och belastningsregistret.

**Kustbevakningens förslag** överensstämmer i sak med promemorians förslag.

**Remissinstanserna** har tillstyrkt eller inte haft något att invända mot att Kustbevakningen får direktåtkomst till misstankeregistret och belastningsregistret.

**Bakgrund:** Frågan om Kustbevakningens tillgång till uppgifter ur misstanke- och belastningsregistren uppmärksammades vid redovisningen i juni 2004 av Riksåklagarens, Ekobrottsmyndighetens, Rikspolisstyrelsens, Tullverkets och Skatteverkets gemensamma uppdrag att identifiera eventuella hinder mot ett rationellt informationsutbyte mellan myndigheterna (RIF-samarbetet). I januari 2005 begärde Kustbevakningen att förordningen (1999:1134) om belastningsregister och förordningen (1999:1135) om misstankeregister ska ändras så att Kustbevakningen får direktåtkomst till de båda registren. Kustbevakningen

förordade också att lagen om belastningsregister och lagen om misstankeregister på sikt ändras så att det av dessa lagar framgår dels att registren förs också för Kustbevakningens behov, dels att Kustbevakningen har rätt att få ut uppgifter ur registren.

**Skälen för promemorians förslag och bedömning:** När Kustbevakningen utgjorde en del av Tullverket, hade kustbevakningstjänstemän med brottsbekämpande uppgifter samma tillgång till polisens register som tulltjänstemän. Detta ändrades i och med att Kustbevakningen blev en egen myndighet, eftersom myndighetens rätt att få uppgifter ur dessa register inte togs upp när myndigheterna skildes åt. Kustbevakningen har därför – i motsats till övriga brottsbekämpande myndigheter – inte någon generell rätt att få uppgifter ur misstankeregistret eller belastningsregistret för sin brottsbekämpande verksamhet. Däremot kan myndigheten få sådana uppgifter efter en sedvanlig sekretessprövning. När Kustbevakningen utövar gränskontroll och en fråga om frihetsberövande med stöd av utlänningslagen (2005:716) aktualiseras, har myndigheten också rätt att få uppgifter ur belastningsregistret med stöd av 10 § 8 förordningen om belastningsregister.

Kustbevakningen har under senare år successivt fått en allt större roll när det gäller att förebygga, upptäcka och utreda brott. Myndigheten har bl.a. fått rätt att inleda förundersökning beträffande vissa brott och att utfärda föreläggande av ordningsbot. Ett skäl till denna utveckling är att det har ansetts viktigt att kunna utnyttja myndighetens kompetens och närvaro vid tillfällen och på platser där polisen inte finns till hands. Det finns också flera förslag om att Kustbevakningens brottsbekämpande roll ska utökas ytterligare, bl.a. vad gäller gränskontroll och kontroll av trafiknykterhet.

Kustbevakningen har i sin brottsbekämpande verksamhet samma behov av att snabbt få tillgång till uppgifter ur misstankeregistret och belastningsregistret som övriga brottsbekämpande myndigheter – som samtliga kan medges direktåtkomst till de båda registren. För Kustbevakningens verksamhet gäller i allt väsentligt samma sekretess för den brottsbekämpande verksam-

heten som hos de övriga brottsbekämpande myndigheterna. Eftersom Kustbevakningen bedriver verksamhet dygnet runt, är det särskilt angeläget att myndigheten kan få tillgång till uppgifter ur registren i fråga genom direktåtkomst.

Enligt vår bedömning bör därför Kustbevakningen ges rätt att i sin brottsbekämpande verksamhet få ut uppgifter ur misstankeregistret och belastningsregistret. Eftersom övriga brottsbekämpande myndigheters behov av och tillgång till uppgifter ur registren regleras i lagen om misstankeregister respektive lagen om belastningsregister med tillhörande förordningar, bör också Kustbevakningens rätt att få del av uppgifter från registren regleras i dessa lagar.

Det bör finnas möjlighet att medge Kustbevakningens tjänstemän direktåtkomst till de båda registren. Denna fråga bör dock på motsvarande sätt som för övriga myndigheter regleras i förordning.



## 23 Ikraftträdande och övergångsbestämmelser

### 23.1 Ikraftträdande

**Promemorians förslag:** Den nya lagstiftningen om behandling av personuppgifter i polisens brottsbekämpande verksamhet ska träda i kraft den 1 januari 2009, då polisdatalagen ska upphöra att gälla.

**Utredningen** har ansett det vara viktigt att övergångstiden till dess att den nya regleringen börjar gälla inte blir längre än nödvändigt.

**Remissinstanserna** har inte haft några synpunkter.

**Skälen för promemorians förslag:** Det är angeläget att den nya lagstiftningen träder i kraft så snart som möjligt, eftersom den är en förutsättning för att polisen ska kunna utveckla sin nya plattform för personuppgiftsbehandling. Vi bedömer att lagstiftningen bör kunna träda i kraft den 1 januari 2009, då polisdatalagen ska upphöra att gälla.

## 23.2 Övergångsbestämmelser

**Promemorians förslag:** Behandlingen av personuppgifter i särskilda undersökningar som har beslutats före ikraftträdandet ska under en tvåårig övergångsperiod omfattas av äldre bestämmelser.

Bestämmelserna om gallring och om behandling av uppgifter i brottsanmälningar och avslutade förundersökningar ska under en motsvarande övergångsperiod inte tillämpas på uppgifter som har samlats in före ikraftträdandet. I stället ska motsvarande äldre bestämmelser tillämpas. Vidare ska lagens bestämmelser om särskilda upplysningar inte behöva tillämpas på sådana uppgifter under övergångsperioden.

De register som enligt övergångsbestämmelserna till polisdatlagen förs med stöd av datalagen ska under en tvåårig övergångsperiod få fortsätta att föras på samma sätt. Detta ska dock inte gälla det allmänna spaningsregistret, fingeravtrycksregistret eller signalements- och känneteckensregistret. Ett tillstånd kan upphöra att gälla innan övergångsperioden har löpt ut genom att registret avanmäls hos Datainspektionen

**Promemorians bedömning:** Övriga lagförslag kräver inte några särskilda övergångsbestämmelser.

**Utredningens förslag:** Överensstämmer delvis med förslaget.

**Remissinstanserna** har inte framfört några synpunkter.

**Skälen för promemorians förslag och bedömning:** Polisdatlagen trädde i kraft den 1 april 1999. För de personregister som den 24 oktober 1998 fördes med Datainspektionens tillstånd gäller dock, enligt punkten 2 i övergångsbestämmelserna till polisdatlagen, bestämmelserna i datalagen till och med den 31 december 2007. Reglerna i 6–8 §§ polisdatlagen om utlämnande av uppgifter gäller dock även beträffande nämnda personregister. Regeringen har den 27 september 2007 i propositionen Övergångsbestämmelserna till polisdatlagen (prop. 2007/08:6) före-

slagit att nämnda övergångsbestämmelser ska förlängas till den 31 december 2008.

Utredningen har övervägt om det behövs några övergångsbestämmelser till de författningar som föreslagits men funnit att det inte behövs några sådana annat än i sekretesslagen. Den nya regleringen bör alltså enligt utredningen gälla fullt ut från dagen för ikraftträdandet. När det gäller sekretesslagen har utredningen ansett att det behövs en övergångsbestämmelse som anger att äldre bestämmelser om sekretess fortfarande ska gälla i fråga om uppgifter som hänför sig till tiden före ikraftträdandet.

Enligt vår bedömning krävs det inte några övergångsregler till sekretesslagen, eftersom de ändringar vi föreslår i den lagen inte innebär några ändringar i fråga om sekretessens omfattning. Vad sedan gäller behovet av övergångsbestämmelser till den nya lagen om personuppgiftsbehandling i polisens brottsbekämpande verksamhet gör vi följande bedömning.

En av utgångspunkterna för den nya lagen är att den ska vara teknikneutral, se avsnitt 6.1. Lagen bör alltså inte i detalj reglera hur polisens datasystem för informationshantering ska utformas. Den bör i stället utgöra ramen för polisens personuppgiftsbehandling och möjliggöra för polisen att modernisera sina datasystem. Arbetet med att modernisera systemen har redan påbörjats och kommer att fortsätta efter lagens ikraftträdande. Vi vet inte vilka av de nuvarande systemen och registren som polisen kommer att välja att behålla. Det är dock sannolikt att ett flertal av dessa fortfarande kommer att finnas kvar vid lagens ikraftträdande. Det står vidare klart att den nya lagen kommer att kräva viss anpassning av systemen. En stor del av detta arbete bör polisen kunna hantera fram till ikraftträdandet. I fråga om vissa system kan det dock förutsättas att mer omfattande förändringar kan komma att behövas. Det finns därför skäl att införa övergångsbestämmelser till lagen.

Vid utformningen av övergångsbestämmelserna är det nödvändigt att ta hänsyn till de bestämmelser av olika slag som för närvarande reglerar polisens personuppgiftsbehandling. I dag sker således behandlingen av personuppgifter dels med stöd av

särskilda bestämmelser i polisdatalagen, dels med stöd av datalagen och tillstånd från Datainspektionen enligt övergångsbestämmelserna till polisdatalagen, dels med stöd av de allmänna bestämmelserna i polisdatalagen och personuppgiftslagen (se avsnitt 5).

I fråga om den behandling som sker med stöd av särskilda bestämmelser i polisdatalagen bedömer vi att det bör införas övergångsbestämmelser för den behandling som i dag sker inom ramen för särskilda undersökningar. Vissa av dessa undersökningar kommer att omfattas av de föreslagna bestämmelserna om behandling av gemensamt tillgängliga uppgifter, bl.a. bestämmelserna om särskilda upplysningar. För att undvika att belasta underrättelseverksamheten med ett tidskrävande arbete med märkning av uppgifter i redan pågående undersökningar, anser vi att äldre bestämmelser bör fortsätta att tillämpas på de särskilda undersökningar som har beslutats före lagens ikraftträdande. De äldre bestämmelserna bör dock gälla endast under en övergångsperiod. Enligt vår bedömning bör denna tid bestämmas till två år. En särskild undersökning pågår normalt högst ett år (se 16 § polisdatalagen), med möjlighet att fortsätta behandlingen under längre tid om det finns särskilda skäl. Vårt förslag innebär således att de allra flesta särskilda undersökningar bör hinna avvecklas under övergångsperioden.

För övrig behandling av uppgifter som i dag sker med stöd av polisdatalagen bedömer vi att det framför allt är några särskilda bestämmelser i den nya lagen som polisen kan ha svårigheter att tillämpa redan vid ikraftträdandet. Det rör sig om de föreslagna bestämmelserna för gemensamt tillgängliga uppgifter om gallring, om särskilda upplysningar samt om behandling av uppgifter i brottsanmälningar och i avslutade förundersökningar. Under en övergångsperiod bör därför dessa bestämmelser inte tillämpas på redan insamlade uppgifter. I den mån det finns motsvarande bestämmelser i gällande författningar bör alltså dessa bestämmelser fortsätta att tillämpas. Om polisen vill börja tillämpa bestämmelserna om särskilda upplysningar före övergångsperioden, bör dock detta vara möjligt. Även i fråga om ikraftträdandet av nu



aktuella bestämmelser anser vi att en tvåårig övergångsperiod är tillräcklig.

De register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av den upphävda datalagen skiljer sig i flera avseenden åt sinsemellan. I fråga om vissa register är det dessutom svårt att överblicka vilka bestämmelser som gäller för registret. Detta beror bl.a. på att Datainspektionen med stöd av datalagen kan ha meddelat ett stort antal föreskrifter för registren. Med hänsyn till detta är det svårt att utforma detaljerade övergångsbestämmelser för behandlingen av personuppgifter i dessa register. Flera av registren synes dock behöva anpassas till den nya lagens bestämmelser i väsentliga delar. I Rationell anmälningsrutin (RAR) måste det exempelvis skapas rapporteringsrutiner från åklagare och domstol för att polisen ska kunna tillämpa de föreslagna bestämmelserna om behandling av uppgifter i brottsanmälningar och i avslutade förundersökningar. Sammantaget anser vi att det bör införas generella övergångsbestämmelser för de aktuella registren som innebär att registren får fortsätta att föras under en övergångsperiod om två år efter lagens ikraftträdande. Det får antas ge polisen tillräckligt utrymme att anpassa den personuppgiftsbehandling som sker i de aktuella registren till den nya lagens bestämmelser.

Den personuppgiftsansvarige bör, liksom i dag, kunna avanmäla ett register hos Datainspektionen. Genom en sådan avanmälan kommer polisen att kunna göra den nya lagen tillämplig på behandlingen redan innan den föreslagna övergångsperioden har löpt ut. Detta bör framgå av övergångsbestämmelserna.

Vi föreslår också att några av de register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av datalagen ska regleras särskilt, nämligen fingeravtrycksregistret, signalements- och känneteckenregistret samt det allmänna spaningsregistret (se avsnitt 17 och 20). De bestämmelser som föreslås gälla för dessa register överensstämmer i huvudsak med vad som gäller i dag. Därför bedömer vi att det inte behövs några övergångsbestämmelser för just dessa register.



## 24 Kustbevakningens personuppgiftsbehandling

### 24.1 Bakgrund

Den 21 oktober 2004 tillkallades en särskild utredare med uppdrag att göra en översyn av regleringen av behandlingen av personuppgifter i Kustbevakningens verksamhet. Utredningen antog namnet Utredningen om Kustbevakningens personuppgiftsbehandling. Den 28 februari 2006 överlämnade utredningen betänkandet Kustbevakningens personuppgiftsbehandling Integritet – Effektivitet (SOU 2006:18). Sedan betänkandet remissbehandlats bedömdes att den fortsatta beredningen av förslaget skulle samordnas med beredningen av Polisdatautredningens förslag, i syfte att åstadkomma en mer enhetlig reglering av personuppgiftsbehandlingen hos de brottsbekämpande myndigheterna. Utöver regleringen av polisens personuppgiftsbehandling tas därför också upp vilka principiella överväganden som bör läggas till grund för den fortsatta beredningen av förslaget till ny reglering av personuppgiftsbehandlingen i Kustbevakningens brottsbekämpande verksamhet.

### 24.2 Kustbevakningens verksamhet

#### 24.2.1 Allmänt

Kustbevakningens närmare uppgifter följer i huvudsak av förordningen (2005:742) med instruktion för Kustbevakningen.

Enligt instruktionen har myndigheten till uppgift att bedriva sjöövervakning i Sveriges sjöterritorium och ekonomiska zon samt på land i anslutning till dessa vatten (1 §).

Uppdraget att bedriva sjöövervakning preciseras så att detta omfattar

- övervakning för att förebygga och ingripa mot störningar av ordningen i sjötrafiken,
- att i enlighet med särskilda föreskrifter förhindra och upptäcka brottslig verksamhet,
- att ingripa vid misstanke om brott, samt
- utreda och beivra eller bistå med utredningen av brott (2 §).

Kustbevakningens uppgift att bedriva sjöövervakning inrymmer därutöver att utreda och besluta i ärenden om vattenföroreningsavgift (3 §) och att i den utsträckning det följer av föreskrifter och i förekommande fall efter överenskommelse med annan myndighet, bedriva tillsyns- och kontrollverksamhet inom ett flertal områden (4 §).

Inom ramen för uppdraget att bedriva sjöövervakning ska Kustbevakningen vidare vara kontaktpunkt för sjötrafiken i fråga om förhandsanmälningar enligt föreskrifter om gränskontroll avseende personer och enligt överenskommelse med annan myndighet (5 §).

Beträffande fiske ansvarar Kustbevakningen också för Sveriges del av de kontrollåtgärder som EU genomför till sjöss med stöd av de bestämmelser som Nordostatlantiska fiskerikommisionen (NEAFC) utfärdat (7 §).

Inom ramen för myndighetens räddningstjänstupdrag och med stöd av särskilda föreskrifter har Kustbevakningen vidare ett självständigt ansvar för miljöräddningstjänsten till sjöss. Myndigheten deltar också på begäran av räddningsledare i sjöräddningstjänst och annan räddningstjänst (8 §). Vid räddningstjänstinsatser får Kustbevakningen begära bistånd från och lämna bistånd till utländsk myndighet eller en medlemsstat i EU (9 §). Sådant bistånd kan också begäras från eller lämnas till de nor-

diska länderna eller andra stater enligt ingångna överenskommelser.

Kustbevakningen har även till uppgift att samordna civila behov av sjöövervakning och förmedla civil sjöinformation till berörda myndigheter (10 §).

I myndighetens uppdrag ingår också internationell samverkan. Kustbevakningen ska följa den internationella utvecklingen inom sitt verksamhetsområde och medverka i internationellt samarbete för att utveckla gränskontroll, brottsbekämpning till sjöss, miljöskydd till sjöss och annan sjöövervakning. Kustbevakningen ska vidare samverka med andra myndigheter för att främja svenskt deltagande i internationellt samarbete inom sitt verksamhetsområde (11 §).

Kustbevakningen har möjlighet att, mot avgift, bedriva uppdragsverksamhet inom sitt verksamhetsområde (12 §).

#### **24.2.2 Brottsbekämpande verksamhet**

Som framgår av myndighetens instruktion har Kustbevakningen en självständig, övergripande uppgift att bedriva sjöövervakning för att förebygga och förhindra brott samt att ingripa vid misstanke om brott. Eftersom Kustbevakningen numera enligt 48 kap. 20 § rättegångsbalken och 2 § ordningsbetskungörelsen (1968:199) har möjlighet att utfärda föreläggande om ordningsbot för vissa brott innebär uppgiften också att Kustbevakningen har ett självständigt ansvar att beivra brott.

Kustbevakningens övervakning till havs innefattar ansvar och uppgifter inom det svenska sjöterritoriet, längs kusterna och i Väneren och Mälaren samt därutöver också på internationellt vatten i svensk ekonomisk zon. När Kustbevakningen bedriver sjöövervakning, ligger tyngdpunkten på olika former av förebyggande insatser. Kustbevakningen arbetar brottsförebyggande genom att under hela året patrullera med såväl fartyg och flygplan som bilar längs hela den svenska kusten och genom att bedriva en kontinuerlig övervakning till sjöss. Inte minst när det

gäller utsläppsbrott, fiskebrott och brott mot sjötrafikregler är den kontinuerliga övervakningen viktig. Inhämtning, bearbetning och riktad spridning av information från olika samverkansmyndigheter och samverkansorgan är också ett grundläggande moment i det brottsförebyggande arbetet. Sådana uppgifter bidrar till att inrikta insatserna på de viktigaste platserna och objekten.

Uppgiften att ingripa vid misstanke om brott och att utreda eller bistå med utredning av brott – uppgifter som alltså rymms inom ramen för myndighetens uppdrag att utföra sjöövervakning – preciseras indirekt genom de författningar som innehåller bestämmelser om Kustbevakningens uppgifter och en kustbevakningstjänstemans befogenheter. Den centrala regleringen i detta hänseende är lagen (1982:395) om Kustbevakningens medverkan vid polisiär övervakning (LKP).

De grundläggande bestämmelserna om befogenheter vid brottsbekämpning finns framför allt i rättegångsbalken och förundersökningskungörelsen (1947:948). Dessa bestämmelser kompletteras av befogenhetsregler för de tjänstemän som genomför brottsutredningar. I polislagen (1984:387) finns regler om bl.a. våldsanvändning som också är tillämpliga på kustbevakningstjänstemän. För Kustbevakningens del är, som nyss nämnts, LKP den centrala regleringen.

Befogenhetsreglerna i LKP avgränsas genom en uppräkningslista av de rättsområden inom vilka Kustbevakningen har polisiära befogenheter. Vid överträdelser på något av de områden som anges i LKP har en kustbevakningstjänsteman skyldighet att ingripa.

Enligt lagen (1980:424) om åtgärder mot förorening från fartyg (vattenföroreningsslagen) har en kustbevakningstjänsteman rätt att inleda och bedriva förundersökning. Befogenheterna gäller för brott avseende olagliga utsläpp av olja och andra skadliga ämnen från fartyg (2 a § LKP).

Vid förundersökning rörande brott mot de föreskrifter som avses i 1 § LKP och vid brott mot vattenföroreningsslagen får åklagaren, eller polismyndigheten om denna bedriver undersök-

ningen, anlita biträde av Kustbevakningen samt uppdra åt en kustbevakningstjänsteman att vidta de särskilda åtgärder som behövs för undersökningen, om det är lämpligt med hänsyn till omständigheterna (7 § LKP och 11 kap. 3 § vattenföreningsslagen).

En kustbevakningstjänsteman har också befogenheter enligt bl.a. lagen (2000:1225) om straff för smuggling (smugglingslagen), tullagen (2000:1281) och narkotikastrafflagen (1968:64).

Kustbevakningen har sedan den 1 april 2006 rätt att utfärda föreläggande av ordningsbot avseende brott enligt 5 kap. 1 § sjötrafikförordningen (1986:300) samt sedan den 1 juli 2006 också för brott enligt 16 § tredje stycket lagen (2006:263) om transport av farligt gods.

Rattfylliutredningen har föreslagit att en kustbevakningstjänsteman ska ges befogenhet att genomföra rutinmässiga alkoholutandningsprov enligt 2 § lagen (1976:1090) om alkoholutandningsprov och att Kustbevakningen ska få fatta beslut om att inleda förundersökning avseende misstanke om rattfylleribrott samt inleda förundersökning avseende misstanke om sjöfylleri (SOU 2006:12 och SOU 2006:47).

Genom beslut den 25 januari 2007 tillkallades en särskild utredare med uppdrag att göra en översyn av regleringen av Kustbevakningens befogenheter i den brottsbekämpande och ordningshållande verksamheten (dir. 2007:5). Utredningen har den 4 oktober 2007 genom tilläggsdirektiv också fått i uppdrag att utreda möjligheten att ge Kustbevakningen förundersökningsrätt i fråga om vissa fiskebrott (dir. 2007:139).

### **24.3 Regleringen av Kustbevakningens personuppgiftsbehandling**

Kustbevakningens behandling av personuppgifter regleras av personuppgiftslagen och förordningen (2003:188) om behandling av personuppgifter inom Kustbevakningen. Förordningen gäller utöver personuppgiftslagen och innehåller ingen hänvis-

ning till tillämpliga bestämmelser i denna. Utöver den brottsbekämpande verksamheten gäller förordningen också för Kustbevakningens kontroll- och tillsynsverksamhet samt verksamhet som rör ärenden om vattenföroreningsavgift.

När det gäller den brottsbekämpande verksamheten anges att personuppgifter får behandlas om det är nödvändigt för att förhindra eller upptäcka brottslig verksamhet som innefattar brott mot vilka Kustbevakningen har att ingripa, eller för att utreda sådana brott. Förordningen reglerar inte uttömmande för vilka sekundära ändamål personuppgifter får behandlas, utan i den delen gäller personuppgiftslagens bestämmelser.

I förordningen skiljs på sådana uppgifter som används gemensamt i verksamheten (kustbevakningsdatabasen) och sådana där tillgången är begränsad till enskilda eller begränsade grupper av tjänstemän. Behandlingen av uppgifter i kustbevakningsdatabasen omgärdas av särskilda regler när det gäller de personer om vilka uppgifter får behandlas, vilka uppgifter som får förekomma och sökbegränsningar.

I förordningen regleras vidare vilka övriga myndigheter som kan få åtkomst till kustbevakningsdatabasen. Det finns också bl.a. bestämmelser om behandling av känsliga personuppgifter och gallring.

## **24.4 Samverkan och informationsutbyte med andra brottsbekämpande myndigheter**

### *Polisen*

Inom Kustbevakningens underrättelseverksamhet överlämnar myndigheten tips och underrättelser avseende brottslig verksamhet till polisen och får i viss utsträckning samma typ av information tillbaka.

Vid genomförande av övervakning till sjöss ingriper Kustbevakningen mot upptäckta brott och ordningsstörningar i sjötrafiken, vilket föranleder uppgiftslämnande eller avrapportering till



polisen. När fråga är om utsläppsbrott lämnas informationen till Åklagarmyndigheten.

Till polisen rapporteras vidare brott som upptäcks i samband med Kustbevakningens miljöövervakning och tillsyn avseende djur- och naturskyddsområden, jakt, maritima fornminnen och sjöfynd m.m. Rapporteringen till polisen avser i ökad utsträckning sjöfylleri.

#### *Tullverket*

Kustbevakningen övervakar och kontrollerar trafiken till och från utlandet så att bestämmelserna om in- och utförsel av varor efterlevs. Kustbevakningen informerar härvid alltid Tullverket om tullkontroller som resulterar i en anmälan om brott eller att brister annars noterats. Konkreta tull- och smugglingsbrott rapporteras till Tullverket, vilket även kan inkludera vissa förundersökningsdokument och uppgifter om beslag eller andra tvångsmedel.

Kustbevakningen lämnar även information om andra iakttagelser i samband med den genomförda kontrollen som bedöms vara av intresse för Tullverket. Kustbevakningen vidarebefordrar även tips, från t.ex. allmänheten, om misstänkt brottslig verksamhet och annan underrättelseinformation till Tullverket. Också från Tullverket till Kustbevakningen vidarebefordras tips angående misstänkt brottslig verksamhet och andra underrättelser.

#### *Åklagarmyndigheten*

Förundersökning i anledning av brott mot vattenföroreningslagen genomförs av Kustbevakningen, med all förundersökningsdokumentation, och leds av Kustbevakningen eller åklagare. Sådan förundersökning föranleder informationsutbyte med

ansvarig åklagare eller Åklagarmyndigheten och i viss utsträckning med berörd polismyndighet.

Vid utsläppsbrott genomför Kustbevakningen även vissa brottsutredningar som kräver ett nationellt informationsutbyte med såväl polisväsendet och tullväsendet som åklagare, samt ett internationellt informationsutbyte som bl.a. sker i gemensamma utredningsgrupper.

Det förekommer att Kustbevakningen genomför utredningar avseende brott med stöd av lagen (1982:395) om Kustbevakningens medverkan vid polisiär övervakning (LKP) efter begäran, främst vad gäller fiskebrott, brott mot utlänningslagen och mot lagen om sjöfartsskydd.

## 24.5 Enhetlig reglering av grundläggande principer för personuppgiftsbehandling i brottsbekämpande verksamhet

**Promemorians bedömning:** De grundläggande principer som föreslås gälla för polisens behandling av personuppgifter i den brottsbekämpande verksamheten bör i flera avseenden gälla också för Kustbevakningens behandling av personuppgifter i sådan verksamhet.

**Skälen för promemorians bedömning:** I Kustbevakningens brottsbekämpande verksamhet aktualiseras en rad frågeställningar som är gemensamma för den verksamheten och motsvarande verksamhet hos andra myndigheter. Det gäller inte minst i fråga om förutsättningarna för behandlingen av personuppgifter. Kustbevakningens brottsbekämpande verksamhet är visserligen av mindre omfattning och delvis annan karaktär än polisens, men när det gäller frågor om hur den enskildes integritet ska skyddas och hur avvägningen ska ske i förhållande till verksamhetens effektivitet, är det angeläget att samma grundläggande principer gäller. Detta kan bli än mer viktigt som en följd av den översyn

som pågår av Kustbevakningens befogenheter och de förslag som har lämnats bl.a. när det gäller myndighetens roll i samband med bekämpning av rattfylleri- och sjöfylleri-brott. Beroende på hur förslagen slutligen utformas kan de innebära att Kustbevakningens roll i brottsbekämpningen betonas ytterligare.

En samordning av regleringen av personuppgiftsbehandlingen i den brottsbekämpande verksamheten hos polisen och Kustbevakningen skulle skapa bättre förutsättningar för samarbete mellan myndigheterna och underlätta informationsutbytet mellan dem. Det skulle också innebära att den enskilde lättare kan få överblick över vilka förutsättningar som gäller för behandling av uppgifter om honom eller henne i respektive verksamhet.

Som beskrivits närmare i avsnittets inledning pågår för närvarande ett arbete med att se över regleringen av Kustbevakningens personuppgiftsbehandling, med utgångspunkt från det betänkande som lämnats av Utredningen om Kustbevakningens personuppgiftsbehandling (SOU 2006:18). Under arbetet med en ny lag om polisens behandling av personuppgifter i den brottsbekämpande verksamheten har det identifierats att det på flera områden finns anledning att överväga delvis andra lösningar än de som har föreslagits i betänkandet och som närmare ansluter till de regler som föreslagits för polisen.

Nedan anges vilka av de övergripande principer som har föreslagits för polisen som också bör gälla för Kustbevakningen. Hur den närmare utformningen av dessa bör ske får övervägas i det fortsatta arbetet, med beaktande av de speciella förutsättningar som gäller för Kustbevakningen.

De överväganden som bör gälla också för Kustbevakningens del är, utöver de grundläggande utgångspunkterna i avsnitt 6.4, följande.

På samma sätt som föreslås för polisens del bör insamling av vissa typer av uppgifter, vilka regleras i andra lagar, falla utanför tillämpningsområdet för den nya lagstiftningen för Kustbevakningens brottsbekämpande verksamhet. Likaså bör den framtida regleringen för denna verksamhet, av de skäl som anges i avsnitt 6.3, innehålla bestämmelser om behandling av uppgifter om juri-

diska personer, eftersom sådana uppgifter inte alltid kan skiljas från uppgifter om fysiska personer.

Vidare bör samma lösning i frågan om förhållandet mellan personuppgiftslagen och den nya lagstiftningen som valts för polisens del tillämpas på den framtida lagstiftningen för Kustbevakningen (se avsnitt 6.5). Det innebär att den nya lagen ska gälla i stället för personuppgiftslagen och att det i en ny lag om Kustbevakningens personuppgiftsbehandling bör hänvisas till de bestämmelser i personuppgiftslagen som föreslås gälla.

Kustbevakningens reglering bör likaså innehålla en bestämmelse som begränsar varje tjänstemans tillgång till personuppgifter i den brottsbekämpande verksamheten till vad denne behöver för att kunna fullgöra sina arbetsuppgifter (se avsnitt 6.7).

På samma sätt som föreslagits för polisens del bör självfallet den framtida lagstiftningen för Kustbevakningen ange tydliga ändamål för personuppgiftsbehandlingen i den brottsbekämpande verksamheten. I Kustbevakningens reglering bör följaktligen på motsvarande sätt uttömmande anges för vilka primära och sekundära ändamål som personuppgifter får behandlas. Att ändamålen anges uttömmande innebär att personuppgiftslagens finalitetsprincip, dvs. att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in, inte tillämpas i denna del av myndighetens verksamhet.

Som primära ändamål bör också för Kustbevakningens del anges att förebygga, förhindra och upptäcka brottslig verksamhet (jfr avsnitt 7.2), även om myndighetens verksamhet i dessa hänseenden är mera begränsad. Det ingår likaså i Kustbevakningens uppgifter att i viss utsträckning utreda och beivra brott. Detta bör således också vara ett grundläggande ändamål för personuppgiftsbehandling i den brottsbekämpande verksamheten (jfr avsnitt 7.3).

I de fall där Kustbevakningen utför polisiära uppgifter har myndigheten i princip samma behov som polisen av att kunna behandla personuppgifter för att fullgöra internationella åtaganden. Vad som anges i avsnitt 7.4 om behandling av personuppgif-

ter inom ramen för internationellt samarbete har därför relevans även för den framtida regleringen av personuppgiftsbehandlingen i Kustbevakningens brottsbekämpande verksamhet.

Kustbevakningen har också samma behov som polisen – och många andra myndigheter – av att kunna behandla personuppgifter i den utsträckning det är nödvändigt för diarieföring eller för handläggningen av en anmälan eller liknande i vilken uppgifterna återfinns (se avsnitt 7.5).

Kustbevakningen har i princip samma behov som polisen att kunna utbyta information med andra brottsbekämpande myndigheter. Sådant informationsutbyte underlättas väsentligt om myndigheterna har en likartad lagstiftning. Vad som anges i avsnitt 7.6 angående behovet av behandling för att kunna tillhandahålla information till andra brottsbekämpande myndigheter har därför relevans också för Kustbevakningens del.

På motsvarande sätt behöver Kustbevakningen kunna behandla personuppgifter för att tillhandahålla information till utländska brottsbekämpande myndigheter eller organisationer för att fullgöra internationella åtaganden. Behovet av informationsutbyte kan komma att öka dels om Kustbevakningen får nya arbetsuppgifter, dels om det internationella samarbetet utvecklas. Kustbevakningen bör vidare också få behandla uppgifter när det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt till andra när uppgiftsskyldighet följer av lag eller förordning.

En annan principiellt viktig fråga är behandlingen av det som brukar kallas känsliga personuppgifter. Vad som anges i avsnitt 8 om begränsningar i polisens rätt att behandla sådana uppgifter bör kunna ligga till grund för regleringen även för Kustbevakningens del.

För polisens del föreslås att det ska göras åtskillnad i den brottsbekämpande verksamheten mellan gemensamt tillgängliga uppgifter och andra uppgifter (avsnitt 9). För uppgifter av förstnämnda slag ska strängare regler gälla. Denna princip bör gälla även för Kustbevakningens personuppgiftsbehandling. Vid den närmare utformningen av bestämmelserna om vilka personupp-

gifter som ska få behandlas måste dock särskild hänsyn tas till att Kustbevakningens brottsbekämpande verksamhet är av annan karaktär och omfattning än polisens. Det gäller särskilt i fråga om de närmare förutsättningarna för att göra personuppgifter tillgängliga i verksamhet för att förebygga, förhindra och upptäcka brottslig verksamhet. Det finns naturligtvis även för Kustbevakningens del ett behov av att förse gemensamt tillgängliga personuppgifter med särskilda upplysningar (avsnitt 10).

För polisens del har föreslagits att det ska införas sökbe-gränsningar av olika slag när det gäller gemensamt tillgängliga uppgifter. Vad som anges i avsnitt 11.1 om känsliga personuppgifter som sökbegrepp bör tillämpas även för Kustbevakningen. I allt väsentligt bör också de föreslagna principerna för vilka sökbe-gränsningar i övrigt som ska gälla (avsnitt 11.2) kunna tillämpas också i Kustbevakningens brottsbekämpande verksamhet.

Bedömningarna och förslagen i avsnitt 12 angående informationsutbyte mellan de brottsbekämpande myndigheterna och förutsättningarna för direktåtkomst är, som framgått av det tidigare sagda, relevanta också för Kustbevakningens del. Detsamma gäller behovet av sekretessbrytande regler och bestämmelser om uppgiftsskyldighet i enlighet med vad som närmare utvecklas i avsnitt 13. De sekretessbrytande reglerna måste dock utformas något annorlunda för Kustbevakningen med hänsyn till att verksamheterna i vissa avseenden skiljer sig åt.

På samma sätt som föreslagits för polisen (avsnitt 14) bör utlämnande av personuppgifter på medium för automatiserad behandling begränsas i den framtida regleringen av Kustbevakningens brottsbekämpande verksamhet.

## 25 Ekonomiska konsekvenser

**Promemorians bedömning:** De framlagda förslagen ger inte upphov till kostnader som inte kan täckas av myndigheternas befintliga anslag.

**Utredningen** gör samma bedömning.

**Remissinstanserna** har inte haft några synpunkter.

**Skälen för promemorians bedömning:** De förslag till nya författningar som läggs fram i denna promemoria ger polisen de rättsliga förutsättningarna för att kunna bygga upp en modernare informationshantering och att avveckla vissa register. Förslagen innebär jämfört med den nuvarande regleringen att polisen ges bättre förutsättningar att behandla personuppgifter i den brottsbekämpande verksamheten, bl.a. när det gäller uppgifter som behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet. Detta, i förening med den ökade möjligheten till utlämnande av uppgifter mellan de brottsbekämpande myndigheterna, skapar förutsättningar för en effektivare brottsbekämpande verksamhet. Detta bör kunna leda till såväl en ökad brottsupplärning som ekonomiska besparingar, även om den nya regleringen initialt kan medföra vissa ökade kostnader för en ändring av de nuvarande systemen. Kostnaderna för inrättandet av nya system för informationshantering ingår i den normala verksamheten inom polisväsendet och bör således täckas av de berörda myndigheternas vanliga anslag. Rikspolisstyrelsen har för övrigt, oberoende av den nya lagen, beslutat om en översyn av den nuvarande registerstrukturen.

Det vidgade tillsynsansvar som vi föreslår för Säkerhets- och integritetsskyddsnämnden kommer att medföra ökade kostnader för nämnden. Dessa bör finansieras från anslaget 4:1 polisorganisationen.



## 26 Författningskommentar

### **26.1 Förslaget till lag om behandling av personuppgifter i polisens brottsbekämpande verksamhet**

#### **1 kap. Lagens syfte och tillämpningsområde**

##### **Lagens syfte**

1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i polisens brottsbekämpande verksamhet.

I paragrafen anges att syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagens övergripande syfte är därmed detsamma som syftet med personuppgiftslagen (1998:204). Motiven till bestämmelsen har redovisats i avsnitt 6.5.1.

##### **Lagens tillämpningsområde m.m.**

2 § Denna lag gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet vid Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten, om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 2 kap. 4 § andra stycket och 10 § gäller även vid andra myndigheters behandling av uppgifter som har lämnats ut genom direktåtkomst med stöd av denna lag.

Lagen gäller inte vid sådan behandling av personuppgifter som sker enligt lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister eller lagen (2008:000) om polisens allmänna spaningsregister. Den gäller inte heller vid insamling av personuppgifter genom allmän kameraövervakning, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning.

Paragrafen anger lagens tillämpningsområde. Frågan har behandlats i avsnitt 6.3.

I *första stycket* anges inledningsvis att lagen gäller vid "behandling av personuppgifter". Med personuppgifter avses det samma som i 3 § personuppgiftslagen (1998:204), dvs. alla typer av uppgifter som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Också "behandling" har samma innebörd som i den bestämmelsen, dvs. varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, t.ex. insamling, registrering, organisering, lagring, bearbetning, användning, spridning eller annat tillhandahållande, sammanställning och samkörning.

Ytterligare en förutsättning för att lagen ska vara tillämplig är att behandlingen är helt eller delvis automatiserad eller att personuppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier (jfr 5 § personuppgiftslagen som innehåller samma rekvisit). Utanför lagens tillämpningsområde faller således helt manuell behandling av personuppgifter som inte ingår i någon samling som är tillgänglig för sökning.

Av första stycket följer vidare att lagen endast är tillämplig i polisens brottsbekämpande verksamhet. Med brottsbekämpande verksamhet avses i detta sammanhang all den verksamhet för vilken personuppgifter får behandlas enligt 2 kap. 5 § eller 5 kap. 2 §. För en närmare beskrivning av vilka verksamheter som omfattas hänvisas till kommentaren till dessa bestämmelser. Lagen är däremot inte tillämplig i fråga om annan verksamhet som polisen bedriver, t.ex. hjälpande verksamhet eller verksamhet för

upprätthållande av ordning och säkerhet utan anknytning till brottsbekämpning. För behandling av personuppgifter i sådan verksamhet gäller i stället personuppgiftslagen. Därmed faller också en del av de register som polisen för i dag utanför den nya lagens tillämpningsområde, t.ex. polisens adressdatabas, fastighetsfråga och folkbokföringsdatabas samt passregistret. I vilken utsträckning uppgifter från dessa register får föras in i den brottsbekämpande verksamheten får alltså bedömas enligt personuppgiftslagen. Det är däremot bestämmelserna i denna lag (främst 2 kap. 6 § första stycket 3) som avgör om personuppgifter som har samlats in i den brottsbekämpande verksamheten får användas även i polisens övriga verksamhet.

Polisverksamhet utövas vid Rikspolisstyrelsen och polismyndigheterna samt, i viss utsträckning, vid Ekobrottsmyndigheten. I lagtexten har klargjorts att lagen gäller oavsett vid vilken av dessa myndigheter som personuppgiftsbehandlingen sker. Sådan personuppgiftsbehandling vid Ekobrottsmyndigheten som inte tillhör polisverksamheten faller utanför lagens tillämpningsområde.

I ett avseende gäller lagens bestämmelser även för andra myndigheter än de som anges i första stycket. I *andra stycket* anges att bestämmelserna om personuppgiftsansvar i 2 kap. 4 § andra stycket och om begränsning av tillgång till uppgifterna i 2 kap. 10 § även gäller hos annan myndighet, om myndigheten har fått uppgifter från polisen genom direktåtkomst.

Av *tredje stycket* framgår att lagen inte gäller vid sådan personuppgiftsbehandling som sker med stöd av bestämmelserna i lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister, lagen (2000:344) om Schengens informationssystem, lagen (2006:444) om passagerarregister eller lagen (2008:000) om polisens allmänna spaningsregister. Detta överensstämmer, förutom såvitt avser sistnämnda lag, med vad som gäller enligt 1 § tredje stycket polisdatalagen.

I tredje stycket undantas också ett särskilt slag av personuppgiftsbehandling från lagens tillämpningsområde, nämligen insamling av personuppgifter genom allmän kameraövervakning,

hemlig teleavlyssning, hemlig teleövervakning eller hemlig kameraövervakning. För sådan personuppgiftsbehandling gäller i stället bestämmelserna i 27 kap. rättegångsbalken, lagen (1998:150) om allmän kameraövervakning, lagen (1995:1506) om hemlig kameraövervakning, lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål, lagen (1991:572) om särskild utlänningskontroll och lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Sedan uppgifterna har samlats in gäller dock denna lag för den fortsatta behandlingen av uppgifterna. I den mån rättegångsbalken eller de angivna lagarna innehåller särskilda begränsningar i fråga om användningen av den insamlade informationen gäller dock givetvis dessa (se särskilt 27 kap. 23 a § rättegångsbalken och andra bestämmelser om användning av överskottsinformation).

I tredje stycket undantas också insamling av uppgifter genom hemlig rumsavlyssning, dvs. det hemliga tvångsmedel som föreslås i prop. 2005/06:178.

**3 §** Följande bestämmelser gäller även vid behandling av uppgifter om juridiska personer:

1. 2 kap. 4 § om personuppgiftsansvar,
2. 2 kap. 5–7 §§ om ändamålen för behandlingen,
3. 2 kap. 11 § om gallring,
4. 3 kap. 1–18 §§ om gemensamt tillgängliga uppgifter,
5. 4 kap. 20–22 §§ om behandling av uppgifter i penningtvättsregister,
6. 5 kap. 2–4 §§ om ändamålen för behandlingen hos Säkerhetspolisen,
7. 5 kap. 6 § om Säkerhetspolisens personuppgiftsansvar,
8. 5 kap. 7 § om gallring hos Säkerhetspolisen, och
9. 5 kap. 8–17 §§ om gemensamt tillgängliga uppgifter hos Säkerhetspolisen.

Vad som sägs i de angivna paragraferna om personuppgifter ska därvid avse uppgifter om juridiska personer.

Paragrafen innehåller bestämmelser om behandling av uppgifter om juridiska personer. Frågan har behandlats i avsnitt 6.3.

Det kan många gånger vara svårt att dra gränsen mellan personuppgifter – dvs. uppgifter som direkt eller indirekt anknyter till fysiska personer – och uppgifter om juridiska personer. För att undvika gränsdragningsvårigheter har i denna paragraf föreskrivits att vissa av lagens bestämmelser ska tillämpas också vid behandling av uppgifter om juridiska personer. Det gäller bestämmelserna om personuppgiftsansvar (2 kap. 4 §), om ändamålen med behandlingen (2 kap. 5–7 §§) och om gallring (2 kap. 11 §). Det gäller vidare samtliga bestämmelser som avser gemensamt tillgängliga uppgifter (3 kap.) och uppgifter som behandlas i penningtvätsregister (4 kap. 20–22 §§) samt vissa bestämmelser avseende Säkerhetspolisens personuppgiftsbehandling (5 kap. 2–4, 6, 7 och 8–17 §§).

**4 §** I 2 kap. finns allmänna bestämmelser om sådan behandling av personuppgifter som omfattas av lagen. För behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga gäller även bestämmelserna i 3 kap. För behandling i register med uppgifter om resultat av DNA-analyser, fingeravtrycksregister, signalementsregister eller penningtvätsregister gäller dock särskilda bestämmelser i 4 kap. i stället för bestämmelserna i 3 kap.

Bestämmelserna i 5 kap. gäller för behandling av personuppgifter i Säkerhetspolisens verksamhet. Vid sådan behandling ska bestämmelserna i 2–4 kap. tillämpas endast i den utsträckning som framgår av 5 kap.

Paragrafen anger hur lagen är disponerad.

*Första stycket* erinrar om att 2 kap. innehåller allmänna bestämmelser om sådan behandling av personuppgifter som lagen reglerar. Bestämmelserna i 2 kap. gäller alltså i princip för all personuppgiftsbehandling som omfattas av lagen (jfr dock andra stycket angående behandling i Säkerhetspolisens verksamhet).

I 3 kap. finns bestämmelser som är tillämpliga vid behandling av personuppgifter ”som görs eller har gjorts gemensamt tillgängliga”. Med detta uttryck avses såväl sådan behandling som innebär att personuppgifterna blir gemensamt tillgängliga som behandling av sådana uppgifter som har blivit gemensamt till-

gängliga genom tidigare behandling. Vad som avses med ”gemensamt tillgängliga” kommenteras närmare i anslutning till 3 kap. 1 §. Vid behandling av personuppgifter som omfattas av bestämmelserna i 3 kap. gäller även bestämmelserna i 2 kap.

Vid behandling i register med uppgifter om resultat av DNA-analyser, fingeravtrycksregister, signalementsregister eller penningtvättsregister gäller, utöver bestämmelserna i 2 kap., även vissa bestämmelser i 4 kap. Bestämmelserna i 3 kap. ska inte tillämpas vid sådan behandling.

I *andra stycket* anges att bestämmelserna i 5 kap. gäller för behandling av personuppgifter i Säkerhetspolisens verksamhet. I 5 kap. utpekas de bestämmelser i 2–4 kap. som gäller i Säkerhetspolisens verksamhet. Övriga bestämmelser i 2–4 kap. gäller däremot inte i den verksamheten.

## **2 kap. Allmänna bestämmelser om personuppgiftsbehandling i polisens brottsbekämpande verksamhet**

### **Förhållandet till personuppgiftslagen**

1 § Om inte annat anges i 2 §, gäller denna lag i stället för personuppgiftslagen (1998:204).

Av paragrafen framgår att lagen, om något annat inte anges i 2 §, gäller *i stället för* personuppgiftslagen. Vid sådan personuppgiftsbehandling som omfattas av lagen ska alltså bestämmelser i personuppgiftslagen tillämpas endast om det finns en hänvisning till dem i 2 §. Utformningen av den nya lagen skiljer sig i detta avseende från polisdatalagen, som gäller *utöver* personuppgiftslagen. Skälen till att den nya lagen har getts denna utformning har utvecklats i avsnitt 6.5.1.

Personuppgifter som har samlats in i polisens brottsbekämpande verksamhet kan i vissa fall komma att användas i annan polisiär verksamhet (om förutsättningarna för det, se kommentaren till 6 §). Vid behandlingen av uppgifterna i sådan annan

verksamhet gäller personuppgiftslagens bestämmelser. Finns det en särskild registerlag för den andra verksamheten, gäller den.

2 § När personuppgifter behandlas enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen, gäller följande bestämmelser i personuppgiftslagen (1998:204):

1. 3 § om definitioner,
2. 8 § om förhållandet till offentlighetsprincipen,
3. 9 § första stycket a), b) och e)–h) om grundläggande krav på behandling,
4. 22 § om behandling av personnummer,
5. 23 § och 25–27 §§ om information till den registrerade,
6. 28 § om rättelse,
7. 30–32 §§ om säkerheten vid behandling,
8. 33–35 §§ om överföring av personuppgifter till tredjeland,
9. 36 § andra stycket och 38–41 §§ om personuppgiftsombud m.m.,
10. 42 § om upplysningar till allmänheten om vissa behandlingar,
11. 43 och 44 §§, 45 § första stycket och 47 § om tillsynsmyndighetens befogenheter,
12. 48 § om skadestånd, och
13. 51 § första stycket, 52 § första stycket och 53 § om överklagande.

Var och en av de myndigheter som avses i 1 kap. 2 § ska utse ett eller flera personuppgiftsombud.

Information enligt 23 § personuppgiftslagen behöver inte lämnas om uppgifterna samlas in i samband med larm och det med hänsyn till omständigheterna inte finns tid att lämna informationen.

Förbud enligt 44 eller 45 § personuppgiftslagen får inte förenas med vite.

Paragrafen kommenteras närmare i avsnitt 6.5.2.

Som framgår av 1 § är utgångspunkten i den nya lagen att bestämmelserna i personuppgiftslagen inte ska tillämpas vid sådan behandling av personuppgifter som omfattas av lagen. Vissa utpekade paragrafer i personuppgiftslagen ska dock tillämpas. Dessa anges i förevarande paragrafs *första stycke*. Uppräkningen är avsedd att vara uttömmande.

Först anges 3 § personuppgiftslagen. De definitioner som anges i den paragrafen ska alltså tillämpas även vid behandling av personuppgifter som omfattas av den nya lagen.

Genom hänvisningen till 8 § personuppgiftslagen klargörs att bestämmelserna i den nya lagen – eller de bestämmelser till vilka lagen hänvisar – inte ska tillämpas om det skulle inskränka en myndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter. Det innebär t.ex. att en myndighet inte kan vägra att ta fram och lämna ut uppgifter i enlighet med tryckfrihetsordningens bestämmelser enbart med hänvisning till att utlämnandet inte ryms inom de i 5–7 §§ angivna ändamålen för behandling. I sammanhanget bör dock understrykas att offentlighetsprincipen inte innebär någon skyldighet att lämna ut uppgifter i elektronisk form. Vid bedömningen av om en uppgift som omfattas av den nya lagen kan lämnas ut i elektronisk form måste alltså lagens regler beaktas fullt ut.

Av hänvisningen till 8 § personuppgiftslagen följer också att den nya lagen inte hindrar att en myndighet arkiverar eller bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet (jfr 8 § andra stycket personuppgiftslagen). Bestämmelserna i den nya lagen ska tillämpas också när arkiverade uppgifter används på nytt i polisens brottsbekämpande verksamhet.

Vidare hänvisas till 9 § första stycket a), b) och e) – h) personuppgiftslagen. Hänvisningen innebär att den personuppgiftsansvarige (jfr 4 §) ska se till att uppgifterna behandlas enbart om det är lagligt och att de behandlas på ett korrekt sätt och i enlighet med god sed (om innebörden i ”god sed”, se prop. 1997/98:44 s. 143). Den personuppgiftsansvarige ska också se till *dels* att de behandlade personuppgifterna är adekvata och relevanta i förhållande till ändamålen för behandlingen, *dels* att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen för behandlingen, *dels* att de behandlade personuppgifterna är riktiga och, om det är nödvändigt, aktuella, *dels* att alla rimliga åtgärder vidtas för att rätta, blockera och utplåna sådana personuppgifter som är felaktiga eller ofullständiga



med hänsyn till ändamålen med behandlingen. De ändamål som det härvid måste relateras till får i detta sammanhang anses vara de ändamål som anges i 5–7 §§. Det är givet att man vid tillämpningen av de aktuella bestämmelserna måste ta hänsyn till den särskilda karaktären hos de uppgifter som förekommer i brottsbekämpande verksamhet. Exempelvis kan kravet på att de behandlade uppgifterna är riktiga inte anses innebära något hinder mot att samla in osäkra underrättelseuppgifter, under förutsättning att uppgifterna har relevans för underrättelsearbetet (jfr även 3 kap. 4 § andra stycket).

Paragrafen hänvisar inte till 9 § första stycket c) och d) personuppgiftslagen. Skälen till det har behandlats i avsnitt 6.5.2. Av den nya lagen följer i stället att personuppgifterna får behandlas enbart för de i 5–7 §§ angivna ändamålen.

Vidare hänvisas till 22 § personuppgiftslagen. Innebörden är att uppgifter om personnummer eller samordningsnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

Av hänvisningen till 23 § personuppgiftslagen följer att den myndighet som samlar in uppgifter om en enskild person från personen själv själv ska informera honom eller henne om behandlingen. Det innebär t.ex. att en polismyndighet i samband med att den tar emot och behandlar en uppgift från en person om att denne har utsatts för brott ska underrätta honom eller henne om behandlingen. Vad informationen ska omfatta anges i 25 § personuppgiftslagen; uppgift om den personuppgiftsansvariges identitet, uppgift om ändamålen med behandlingen samt övrig information som den aktuella personen behöver för att ta tillvara sina rättigheter i samband med behandlingen.

Bestämmelserna om informationsplikt i 23 och 25 §§ personuppgiftslagen modifieras emellertid av andra bestämmelser. Som framgår av hänvisningen till 27 § personuppgiftslagen gäller bestämmelserna inte i den utsträckning det gäller sekretess eller tystnadsplikt för informationen. Som en följd av detta gäller ingen informationsplikt när en polis som arbetar under skydds-

identitet samlar in uppgifter från misstänkta, eftersom det i den situationen måste antas att informationsinhämtandet skyddas av sekretess enligt 5 kap. 1 § sekretesslagen. Dessutom begränsas informationsskyldigheten av den särskilda bestämmelsen i tredje stycket (se nedan).

Såsom framgår av hänvisningen till 26 § personuppgiftslagen är den personuppgiftsansvarige också skyldig att på begäran lämna information till en sökande om huruvida personuppgifter som rör denne behandlas. Om sådan behandling sker, ska upplysning också lämnas om bl.a. ändamålet med behandlingen. Också denna informationsskyldighet modifieras genom bestämmelserna i 27 § personuppgiftslagen. Om det gäller sekretess för uppgiften behöver någon information inte lämnas. Det innebär t.ex. att information inte behöver lämnas om sådant som polisen har inhämtat i sin underrättelseverksamhet, om det kan antas att syftet med beslutade eller förutsedda åtgärder skulle motverkas av att information lämnas (jfr 5 kap. 1 § första stycket sekretesslagen).

Såsom följer av hänvisningen till 28 § personuppgiftslagen ska också den lagens bestämmelser om rättelse tillämpas. Den personuppgiftsansvarige är alltså skyldig att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med förevarande lag – däribland de bestämmelser i personuppgiftslagen till vilka lagen hänvisar – eller föreskrifter som har utfärdats med stöd av lagen. Rättelse ska dock inte ske enbart därför att uppgifter som framstod som riktiga eller rimliga när de samlades in, t.ex. brottsmisstankar, senare har visat sig vara oriktiga.

En hänvisning görs också till 30–32 §§ personuppgiftslagen. Enligt 30 § första stycket får ett personuppgiftsbiträde (dvs. den som behandlar personuppgifter för den personuppgiftsansvariges räkning) och den eller de personer som arbetar under biträdets eller den personuppgiftsansvariges ledning behandla personuppgifter enbart i enlighet med instruktioner från den personuppgiftsansvarige. Om det i lag eller annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i det

allmännas verksamhet, gäller dock – enligt 30 § tredje stycket – dessa i stället. Den sistnämnda bestämmelsen syftar särskilt på bestämmelser om tystnadsplikt och sekretess. Av 31 § följer bl.a. att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de behandlade personuppgifterna. Enligt 32 § får tillsynsmyndigheten i enskilda fall besluta om vilka åtgärder som den personuppgiftsansvarige ska vidta enligt 31 §. Med tillsynsmyndigheten avses här tillsynsmyndigheten enligt personuppgiftslagen, dvs. Datainspektionen (2 § personuppgiftsförordningen [1998:1191]).

En hänvisning görs också till 33–35 §§ personuppgiftslagen. Enligt 33 § är det förbjudet att överföra personuppgifter till tredjeland om landet inte har en adekvat nivå för skyddet av personuppgifter. Frågan om en skyddsnivå är adekvat ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska fästas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredjelandet. I 34 och 35 §§ föreskrivs undantag från förbudet. Enligt 34 § får således överföring trots förbudet ske dels om den registrerade har lämnat sitt samtycke till behandlingen, dels om behandlingen är nödvändig med hänsyn till vissa uppräknade omständigheter. Det är också enligt den paragrafen tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen (se avsnitt 4.2.2). Enligt 35 § får regeringen – och för vissa fall även den myndighet som regeringen bestämmer – meddela föreskrifter om undantag från förbudet i 33 §.

Hänvisningen till 36 § andra stycket personuppgiftslagen innebär att den personuppgiftsansvarige ska anmäla till tillsynsmyndigheten när ett personuppgiftsombud utses eller entledigas. Med personuppgiftsombud avses en fysisk person som självständigt ser till att personuppgifter behandlas på ett korrekt och lagligt sätt. Vilka närmare uppgifter som personuppgiftsombudet har framgår av 38–40 §§ personuppgiftslagen. Skyldigheten att utse personuppgiftsombud framgår av andra stycket.

En hänvisning görs också till 41 § personuppgiftslagen. Enligt bestämmelsen har regeringen möjlighet att föreskriva att vissa särskilt känsliga behandlingar ska anmälas till Datainspektionen för förhandskontroll.

Av hänvisningen till 42 § personuppgiftslagen följer att den personuppgiftsansvarige ska till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om sådana behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten, dvs. Datainspektionen. Sekretessbelagda uppgifter och uppgifter om vidtagna säkerhetsåtgärder behöver dock inte lämnas ut.

Tillsynsmyndigheten, dvs. Datainspektionen, har rätt att för sin tillsyn på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter (43 § personuppgiftslagen). Om tillsynsmyndigheten inte har tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får den förbjuda behandlingen (44 §). Konstaterar tillsynsmyndigheten att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, ska den genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Om det inte går att få till stånd rättelse, eller om saken är brådskande, får tillsynsmyndigheten förbjuda behandlingen (45 § första stycket personuppgiftslagen). Tillsynsmyndigheten har också möjlighet att hos länsrätten ansöka om att personuppgifter som har behandlats på ett olagligt sätt ska utplånas (47 § personuppgiftslagen).

Av hänvisningen till 48 § personuppgiftslagen följer att den personuppgiftsansvarige ska ersätta den registrerade för sådan skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag – och de bestämmelser i personuppgiftslagen till vilken denna lag hänvisar – har orsakat.

Av 51 § första stycket personuppgiftslagen följer att tillsynsmyndighetens beslut får överklagas till allmän förvaltningsdom-

stol. Såsom framgår av hänvisningen till 52 § första stycket personuppgiftslagen kan den personuppgiftsansvariga myndighetens beslut om information enligt 26 §, om rättelse och om underrättelse till tredje man enligt 28 § och om upplysningar enligt 42 § personuppgiftslagen överklagas hos allmän förvaltningsdomstol. Av hänvisningen till 53 § personuppgiftslagen följer att andra slag av beslut inte får överklagas.

*Andra stycket* innehåller en föreskrift om att de myndigheter som omfattas av lagens tillämpningsområde ska utse ett eller flera personuppgiftsombud. Genom hänvisningarna till 38–40 §§ personuppgiftslagen görs lagens bestämmelser om personuppgiftsombudets uppgifter tillämpliga.

Det *tredje stycket* innehåller ett undantag från informations-skyldigheten i 23 § personuppgiftslagen. Information enligt 23 § behöver inte lämnas om uppgifterna samlas in i samband med ett larm och det med hänsyn till omständigheterna inte finns tid att lämna information. Med larm avses en brådskande begäran om att polisen omedelbart ska vidta en åtgärd av något slag. Larm görs vanligtvis till polisens kommunikationscentraler, men bestämmelsen tar sikte även på de situationer när en person vänder sig till en enskild polisman eller till en telefonist i polisens allmänna växel. I sådan verksamhet som uteslutande består i att ta emot larm, t.ex. vid en kommunikationscentral, torde information enligt 23 § aldrig behöva lämnas, eftersom det i den verksamheten typiskt sett inte finns tid att lämna information. När larm görs i andra sammanhang, måste det avgöras från fall till fall om det finns tid att lämna informationen. Avgörande för denna bedömning bör främst vara om det skulle medföra en försening av den efterfrågade åtgärden eller om denna åtgärd på annat sätt skulle påverkas negativt av att informationen lämnades. Om undantaget från informationsplikten är tillämpligt, behöver polisen inte heller lämna informationen i efterhand.

Förbud enligt 44 och 45 § personuppgiftslagen får normalt förenas med vite. I *fjärde stycket* föreskrivs att vite inte får användas vid tillsynen enligt denna lag.

## Tillsyn

3 § Utöver de bestämmelser om tillsyn som avses i 2 § första stycket 11 finns bestämmelser om tillsyn i 1 § lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet.

Paragrafen innehåller en erinran om den tillsyn som Säkerhets- och Integritetsskyddsmyndigheten ska utöva över polisens personuppgiftsbehandling. Frågan har behandlats i avsnitt 19.

## Personuppgiftsansvar m.m.

4 § Rikspolisstyrelsen eller polismyndigheterna är personuppgiftsansvariga för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra.

En myndighet som har direktåtkomst till uppgifter enligt denna lag ansvarar för att åtkomsten begränsas enligt 10 §.

Paragrafen innehåller bestämmelser om personuppgiftsansvar. Frågan har behandlats i avsnitt 6.6.

I *första stycket* anges att Rikspolisstyrelsen eller polismyndigheterna är personuppgiftsansvariga för den behandling av personuppgifter enligt 1–4 kap. som myndigheten utför eller som det åligger myndigheten att utföra. Av 5 kap. 6 § framgår att Säkerhetspolisen på motsvarande sätt är personuppgiftsansvarig för den behandling av personuppgifter som Säkerhetspolisen utför eller ska utföra.

Uttrycket personuppgiftsansvarig definieras i 3 § personuppgiftslagen; personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Flera bestämmelser i personuppgiftslagen, till vilka det hänvisas i 2 § i detta kapitel, ålägger den personuppgiftsansvarige särskilda skyldigheter. Så är det t.ex. enligt 9 § första stycket personuppgiftslagen den personuppgiftsansvariges skyldighet att se till att de behandlade personuppgifterna är adekvata och relevanta i förhållande till ända-

målen för behandlingen och att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen för behandlingen. Det ankommer också på den personuppgiftsansvarige att se till att information lämnas till den registrerade och att uppgifter gallras i rätt tid.

Eftersom 1 kap. 3 § hänvisar till denna paragraf, har den personuppgiftsansvarige också ett motsvarande ansvar för uppgifter om juridiska personer.

Den myndighet som samlar in och lagrar en personuppgift är givetvis personuppgiftsansvarig för den behandlingen. Om samma uppgift lämnas ut till en annan myndighet, genom direktåtkomst eller på annat sätt, blir den mottagande myndigheten personuppgiftsansvarig för den fortsatta behandlingen av uppgiften hos den myndigheten. När uppgifter lämnas ut till olika myndigheter kan alltså personuppgiftsansvaret för en och samma uppgift komma att ligga hos flera myndigheter. Var och en ansvarar för den egna behandlingen.

Av *andra stycket* framgår att en myndighet som har direktåtkomst till personuppgifter som behandlas enligt lagen också är ansvarig för att tillgången till uppgifterna inom den egna myndigheten begränsas i enlighet med bestämmelsen i 10 §. Myndigheten är alltså skyldig att se till att endast den som behöver en uppgift för att fullgöra sina arbetsuppgifter har rätt eller möjlighet att få del av uppgiften. Bestämmelsen gäller inte enbart Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten utan också övriga myndigheter som har direktåtkomst till personuppgifter hos polisen.

## Ändamål med behandlingen av personuppgifter

5 § Personuppgifter får, om inte annat följer av 6 eller 7 §, behandlas endast om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet,
2. utreda eller beivra brott, eller
3. fullgöra de förpliktelser som följer av internationella åtaganden.

Paragrafen anger de primära ändamål för vilka personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Avgränsningen av dessa ändamål har behandlats i avsnitt 7. Paragrafen kompletteras av bestämmelserna i 6 § som anger att personuppgifter som behandlas enligt 5 § också får behandlas för ett antal ytterligare ("sekundära") ändamål (se vidare kommentaren till den paragrafen). Av 7 § framgår att personuppgiftsbehandling dessutom får ske för diarieföring och inom ramen för viss ärendehantering. Såsom framgår av hänvisningen i 2 § till 8 § personuppgiftslagen får behandling också ske i den mån den är nödvändig för att en myndighet ska kunna fullgöra sina skyldigheter enligt 2 kap. tryckfrihetsförordningen. Tillsammans anger de nu nämnda paragraferna uttömmande de tillåtna ändamålen för behandling av personuppgifter inom polisens brottsbekämpande verksamhet. Lagen gör härvid ingen skillnad mellan insamling av personuppgifter och efterföljande behandling av insamlade uppgifter. Den s.k. finalitetsprincipen i 9 § första stycket d) personuppgiftslagen har alltså ingen motsvarighet i den nya lagen.

En grundläggande förutsättning för att behandlingen ska vara tillåten är att den behövs för viss polisiär verksamhet. Med detta avses att det ska finnas ett konkret behov av att genomföra behandlingen och att detta behov svarar mot ändamålet med denna. Som exempel kan nämnas att det i en förundersökning kan vara nödvändigt att sammanställa uppgifter om vilka personer som har befunnit sig på platsen för brottet för att säkerställa att alla presumtiva vittnen har hörts i saken, att sammanställa en förteckning över alla målsägande och deras ersättningskrav eller att redovisa vilka personer som har haft kontakt med ett mordoffer i tidsmässigt nära samband med brottet. Likaså måste självfallet många personuppgifter om den eller de misstänkta behandlas för att tillgodose dels åklagarens behov av underlag för sitt ställningstagande i åtalsfrågan, dels domstolens behov av personutredning i brottmål (jfr bestämmelserna i 20 och 21 §§ förundersökningskungörelsen [1947:948] om vad ett förundersökningsprotokoll ska innehålla). Om ändamålet är att förebygga eller förhindra brott, kan det t.ex. vara nödvändigt att sammanställa



uppgifter om vem som hyr vissa lokaler eller vem som äger eller disponerar fordon som man misstänker används i den brottsliga verksamheten. Det kan också handla om att kartlägga vilka personer som regelbundet besöker en viss plats där man misstänker att allvarlig brottslig verksamhet förekommer. Som exempel på att en viss behandling *inte* behövs kan nämnas att det i en förundersökning om ekonomisk brottslighet rimligen inte behövs behandling av uppgifter om att den misstänkte tidigare har varit misstänkt för eller dömts för sexualbrott. I underrättelseprojekt som rör en viss typ av allvarlig brottslighet bör inte underrättelseuppgifter som helt saknar samband med just det projektet kunna behandlas. Är uppgifterna av annat skäl av intresse för brottsbekämpningen, får de i stället behandlas inom ramen för en annan förundersökning eller ett annat underrättelseprojekt.

En stor mängd av den information som polisen samlar in och bearbetar för ett specifikt ändamål, exempelvis för att utreda ett visst brott, måste kunna vidarebehandlas för andra ändamål som antingen anknyter till det ursprungliga ändamålet eller ligger vid sidan av detta. Sådan vidarebehandling är tillåten, under förutsättning att den efterföljande behandlingen faller in under något av ändamålen i 5–7 §§ eller har stöd i någon annan författning, t.ex. lagen om misstankeregister eller lagen om belastningsregister.

I *punkten 1* anges att personuppgifter får behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet (avsnitt 7.2). Det polisarbete som åsyftas är framför allt det som normalt kallas underrättelseverksamhet, dvs. arbete med insamling, bearbetning och analys av information för att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att ett visst brott redan har begåtts. Även behandling av överskottsinformation med stöd av 27 kap. 23 a § andra stycket rättegångsbalken faller in under denna punkt. Polisarbete som är inriktat på en redan begången individualiserad brottslig gärning faller i stället in under punkten 2.

Av *punkten 2* framgår att personuppgifter får behandlas för att utreda och beivra brott (avsnitt 7.3). Med brott avses ett

konkret brott. Det kan vara fråga om såväl brott som bevisligen har begåtts som brott som det enbart finns misstankar om. Misstankarna behöver inte vara riktade mot någon bestämd person. Om misstankarna enbart gäller icke-preciserad brottslig verksamhet, är det dock i stället fråga om sådan ”brottslig verksamhet” som avses i punkten 1. Rör misstanken ett visst brott som kan komma att begås i framtiden är det normalt något som hör hemma under punkten 1. Har den förväntade gärningen nått den punkt där den är straffbar såsom försök, förberedelse, stämpling eller anstiftan – dvs. om det finns grund för att inleda förundersökning – är det däremot fråga om något som faller in under punkten 2.

Under punkten 2 faller all behandling som sker inom ramen för en förundersökning (även spaning). Detsamma gäller behandling som sker med stöd av 23 kap. 3 och 8 §§ rättegångsbalken innan en förundersökning har inletts och behandling inom ramen för en s.k. förenklad utredning enligt 23 kap. 22 § rättegångsbalken. Handläggningen av en brottsanmälan hör också hit, även om denna inte leder till något beslut om att inleda förundersökning.

Punkten 2 är också tillämplig vid sådan utredning som inte utgör förundersökning men som polisen utför, för egen räkning eller åt åklagare, med stöd av lag eller annan författning enligt reglerna om förundersökning. Exempel på sådana bestämmelser finns i 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, 16 § lagen (1957:668) om utlämning för brott, 10 § lagen (1959:254) om utlämning för brott till Danmark, Finland, Island och Norge, 9 § lagen (1988:688) om besöksförbud, 3 § lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder och 8 § lagen (2005:321) om tillträdesförbud vid idrottsarrangemang.

Både punkten 1 och punkten 2 avser endast brottsbekämpande verksamhet som bedrivs av svensk polis. Av *punkten 3* följer att behandling av personuppgifter i viss utsträckning också får ske om syftet är att gagna utländsk brottsbekämpande verksamhet (jfr avsnitt 7.4). Personuppgifter får behandlas med stöd

av denna punkt om det behövs för att fullgöra de förpliktelser som följer av internationella åtaganden. Detta gäller oavsett om den brottslighet som den utländska brottsbekämpande verksamheten avser faller in under svensk jurisdiktion eller inte. Sådana förpliktelser följer dels av vissa lagar som grundar sig på internationella överenskommelser och som reglerar viss polisverksamhet, dels direkt av vissa andra internationella överenskommelser.

Till de lagar som innehåller förpliktelser av detta slag hör lagen (2003:1174) om vissa former av internationellt samarbete i brottsutredningar. Den reglerar polisiärt samarbete mellan EU:s medlemsstater samt samarbete med Island och Norge och innehåller bl.a. bestämmelser om gemensamma utredningsgrupper och om uppgifter och bevisning som lämnas till en sådan grupp. En annan sådan lag är lagen (2000:343) om internationellt polisiärt samarbete som reglerar gränsöverskridande övervakning med stöd av Schengenavtalet. Såsom framgår av 1 kap. 2 § faller däremot behandling av personuppgifter som sker med stöd av lagen om Schengens informationssystem utanför lagens tillämpningsområde. Sådan brottsutredning som sker inom ramen för rättslig hjälp till en annan stat hör också hemma under punkten 3, om den inte faller under punkten 2.

I den mån en internationell överenskommelse innebär att svensk polis är skyldig att överlämna information till en polismyndighet i en annan stat eller till någon annan kan personuppgifter behandlas enligt denna punkt. Som exempel kan nämnas skyldigheten att underrätta en främmande stats konsulat eller beskickning om att någon av statens medborgare har berövats friheten i Sverige, som delvis följer av internationella överenskommelser.

Det förekommer också internationella överenskommelser som innebär att svenska myndigheter *får* lämna information till utländska myndigheter. Eftersom det i sådana fall inte är fråga om någon förpliktelse att tillhandahålla information, faller ett sådant tillhandahållande inte in under denna punkt. Däremot kan det rymmas under 6 § första stycket 2.

Paragrafen är också avsedd att ge utrymme för sådan behandling av personuppgifter som sker i syfte att planera, följa upp och utvärdera verksamhet som anges i paragrafen (se prop. 2004/05:164 s. 179).

**6 §** Om personuppgifter behandlas enligt 5 §, får de även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,

2. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation,

3. annan verksamhet som polisen ansvarar för, om det finns särskilda skäl att tillhandahålla informationen, eller

4. annan myndighets verksamhet, om det enligt lag eller förordning åligger polisen att bistå myndigheten med viss uppgift.

Personuppgifter som behandlas enligt 5 § får även behandlas om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, till andra.

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 5 § och som avser efterlysta personer och avlägsnanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter och att uppgifter som behandlas i en förundersökning får tillhandahållas konkursförvaltare.

I paragrafen anges de ”sekundära” ändamål för vilka personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Frågan har behandlats i avsnitt 7.6. Behandling enligt denna paragraf förutsätter att uppgifterna redan är föremål för behandling enligt 5 §. Det är alltså inte tillåtet att samla in personuppgifter enbart i syfte att behandla dem enligt förevarande paragraf.

Inom ramen för de primära ändamålen kan de myndigheter vars brottsbekämpande verksamhet omfattas av lagen – Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten – utbyta den information som behövs i det brottsbekämpande arbetet. Med brottsbekämpande verksamhet avses detsamma som i 5 § 1–3.

Av *första stycket* 1 framgår att personuppgifter som behandlas med stöd av 5 § även får behandlas för att tillhandahålla information som är nödvändig i brottsbekämpande verksamhet hos vissa andra myndigheter, nämligen Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket. I detta sammanhang nämns även Ekobrottsmyndigheten; därmed klargörs att uppgifterna kan tillhandahållas även åklagare vid myndigheten. Vidare nämns Säkerhetspolisen eftersom denna myndighets verksamhet inte generellt omfattas av regleringen i andra kapitlet. Det förhållandet att uppgifter får behandlas påverkar inte de bestämmelser som gäller om sekretess. Bestämmelserna i sekretesslagen om sekretess mellan och inom myndigheter ska således beaktas på vanligt sätt.

Första stycket 2 ger möjlighet att behandla information som behandlas enligt 5 § för att tillhandahålla information som är nödvändig för brottsbekämpande verksamhet vid en utländsk myndighet eller mellanfolklig organisation. Denna bestämmelse ger stöd för själva behandlingen – utlämnandet – av uppgifterna. Hur stort utrymme är för sådan behandling bestäms även av reglerna om sekretess. Såsom kommer att beröras närmare i anslutning till 13 § kan personuppgifterna inte tillhandahållas utländska myndigheter om de omfattas av sekretess. De utländska myndigheter som avses är främst polis- och åklagarmyndigheter. I den mån brottsbekämpande verksamhet handhas av någon annan myndighet ger dock paragrafen utrymme för att tillhandahålla personuppgifter även till den myndigheten. Det kan t.ex. vara fråga om specialmyndigheter med brottsbekämpande uppgifter på det finansiella området. Möjligheten att behandla uppgifterna genom att lämna ut dem kan begränsas av reglerna i 33–35 §§ personuppgiftslagen som inskränker möjligheten att överföra uppgifter till tredjeland (se kommentaren till 2 §).

Enligt första stycket 3 får personuppgifter som behandlas enligt 5 § även behandlas om det är nödvändigt för att tillhandahålla information som behövs i sådan verksamhet hos polisen som inte är av brottsbekämpande natur. Bestämmelsen ger polisen ett visst utrymme för att använda personuppgifter som har

samlats in med stöd av 5 § i olika förvaltningsärenden hos polisen, t.ex. vapenärenden, eller inför verkställighet av handräckningsuppgifter som polisen ansvarar för. En förutsättning för behandling av detta slag är dock att det finns särskilda skäl att tillhandahålla informationen. Informationen får alltså inte rutinmässigt tillhandahållas för annan polisiär verksamhet, utan det måste i det enskilda fallet föreligga särskilda omständigheter som gör det nödvändigt att använda informationen. I ett passärende har passmyndigheten, normalt polismyndigheten, anledning att undersöka om sökanden är skäligen misstänkt för brott. Enligt 8 § passlagen (1978:302) ska passmyndigheten nämligen, om det framkommer att sökanden är skäligen misstänkt för brott för vilket inte är föreskrivet lindrigare straff än fängelse sex månader, underrätta förundersökningsledaren om passansökan. För att fullgöra denna skyldighet räcker det emellertid med en kontroll i misstankeregistret. Det kan därför inte anses föreligga särskilda skäl att använda personuppgifter som behandlas med stöd av förevarande lag i ett passärende. I sådana förvaltningsärenden där det är fråga om att bedöma en persons lämplighet och laglydnad torde det också som regel vara tillräckligt med de uppgifter som kan inhämtas från belastnings- och misstankeregistren. I enstaka fall, t.ex. när det framstår som nödvändigt att få innebörden av en uppgift i belastnings- eller misstankeregistret närmare belyst, kan det emellertid finnas ett särskilt behov av att få tillgång till uppgifter som omfattas av den nya lagen, t.ex. uppgifter ur en förundersökning. Detsamma gäller inför ett handräckningsuppdrag som polisen ska utföra. När anteckningar i belastnings- eller misstankeregistren ger anledning att anta att uppdraget kan innebära särskilda risker som polisen måste förbereda sig inför, kan det således vara motiverat att utnyttja uppgifter ur andra uppgiftssamlingar som polisen har tillgång till. I ärenden om tillstånd till offentlig tillställning och liknande ärenden kan det någon enstaka gång vara befogat att tillföra ärendet uppgifter av underrättelsekaraktär, särskilt när det kan antas att det kommer att begås allvarlig brottslighet i

samband med tillställningen. I samtliga fall rör det sig dock om undantagssituationer.

Medan punkten 3 täcker polisens behov av att kunna behandla uppgifter i den brottsbekämpande verksamheten för att fullgöra andra polisiära uppgifter, bl.a. handräckningsuppdrag, är punkten 4 avsedd att tillgodose polisens behov av att fullgöra författningenliga förpliktelser att direkt biträda en annan svensk myndighet i dess verksamhet. Denna punkt täcker bl.a. den behandling som kan krävas för att polisen ska kunna bistå Riksdagens ombudsmän och Justitiekanslern med uppgifter när de uppträder som förundersökningsledare och åklagare, i den mån det inte är en behandling som faller in under 5 § 2. Enligt 6 kap. 20 § tullagen (2000:1281) har polisen även rätt att vidta olika åtgärder som normalt utförs av tulltjänstemän (bl.a. att inom ramen för en tullkontroll anbringa lås eller omhändertaga handlingar). Förevarande punkt ger polisen rätt att behandla personuppgifter inom ramen för sådant biträde i en annan myndighets verksamhet.

I *andra stycket* anges att uppgifter även får behandlas om det är nödvändigt för att tillhandahålla information till riksdagen eller regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, till annan (jfr 14 kap. 1 § sekretesslagen som innehåller en motsvarande sekretessbrytande regel). Med annan avses såväl myndighet som enskild. Motsvarande bestämmelser finns i 9 § lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Exempel på uppgiftsskyldighet gentemot annan myndighet finns i 14 kap. 1 § socialtjänstlagen (2001:453) som föreskriver skyldighet att göra anmälan till socialnämnden när nämnden behöver ingripa till barns skydd. I en del fall är polisen skyldig att avge yttrande till annan myndighet med skyldighet att därvid redovisa viss information eller grunden för sitt ställningstagande. Också detta utgör en sådan uppgiftsskyldighet som omfattas av den aktuella bestämmelsen. Som exempel kan nämnas polisens yttrande till en kommun i ärenden om tillstånd till alkoholutskänkning (se 7 kap. 14 § alkohollagen, 1994:1738).

Andra exempel på uppgiftsskyldighet som kan omfatta även polisen finns i 12 kap. 6 § regeringsformen och 6 § lagen (2002:1022) om revision av statlig verksamhet (skyldighet att tillhandahålla Riksdagens ombudsmän respektive Riksrevisionen begärda upplysningar).

Det finns i detta sammanhang anledning att peka på 15 kap. 5 § sekretesslagen. I den paragrafen anges att en myndighet på begäran av en annan myndighet ska lämna uppgift som den förfogar över i den mån hinder inte möter på grund av bestämmelse om sekretess eller av hänsyn till arbetets behöriga gång. Den bestämmelsen innefattar inte en sådan uppgiftsskyldighet som avses i förevarande paragraf.

I övrigt har polisen – om det inte är fråga om utlämnande enligt 2 kap. tryckfrihetsförordningen – inte någon möjlighet att använda personuppgifter som behandlas enligt 5 § för att tillhandahålla information till annan. Uppgifterna kan då varken lämnas ut i elektronisk form eller tas fram med något slag av sökfunktion för utskrift i pappersform eller ges muntligen. Detta gäller även när polisen involveras i ett ärende som en annan myndighet ansvarar för, t.ex. genom att polisen ges möjlighet att yttra sig över en ansökan till den andra myndigheten. Även om det finns skäl som kan synas tala för att den information som polisen har tillgång till skulle vara av värde vid den andra myndighetens prövning, får uppgifterna inte lämnas ut, om det kräver behandling.

Enligt 17 § polisdataförordningen (1999:81) får uppgifter om efterlysta personer och om avlägsnanden ur riket lämnas till vissa myndigheter. Vidare får enligt 17 a § samma förordning förundersökningsuppgifter som kan antas ha betydelse för en konkursutredning lämnas till konkursförvaltaren. Av *tredje stycket* följer att regeringen kan meddela föreskrifter om motsvarande tillhandahållande av uppgifter. Jfr även kommentaren till 2 kap. 17 §.



7 § Personuppgifter får alltid behandlas om

1. behandlingen är nödvändig för diarieföring, eller
2. uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Paragrafen ger möjlighet att behandla personuppgifter i två speciella fall, oavsett om förutsättningarna för behandling enligt 5 eller 6 § är förhanden. Frågan har berörts i avsnitt 7.5.

I *punkten 1* anges att personuppgifter alltid får behandlas om behandlingen är nödvändig för diarieföring. Vilka uppgifter som måste noteras i samband med diarieföring av en handling framgår av 15 kap. 2 § sekretesslagen (1980:100). Vid diarieföring av inkomna handlingar får således alltid anges vem handlingen har kommit från och i korthet vad handlingen rör.

Vidare får, enligt *punkten 2*, personuppgifter alltid behandlas om de har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen. Begreppet ”anmälan eller liknande” innefattar alla slag av framställningar till polisen. Ofta ryms framställningar av detta slag inom de i 5 § angivna ändamålen, men någon gång kan innehållet i framställan vara av sådan art att behovskriteriet i 5 § inte är uppfyllt. Eftersom framställan normalt påfordrar något slag av handläggning hos myndigheten, har det ansetts nödvändigt med en särskild bestämmelse för personuppgiftsbehandling i dessa fall. Behandlingen måste vara ”nödvändig för handläggningen”. Det kan i ett enskilt fall innebära att personuppgifter i ett e-postmeddelande inte får behandlas på annat sätt än genom att uppgifterna tas emot och därefter omedelbart arkiveras eller gallras. I ett annat fall kan bestämmelsen få till följd att personuppgifterna också får behandlas i samband med besvarandet av framställan.

## Behandling av känsliga personuppgifter

8 § Uppgifter om en person får inte behandlas på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Trots bestämmelsen i första stycket får uppgifter om en person som behandlas på annan grund kompletteras med uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen. Uppgifter som avses i första stycket får också behandlas om

1. behandlingen är nödvändig för diarieföring, eller
2. uppgifterna har lämnats i en anmälan eller liknande och behandlingen är nödvändig för handläggningen.

Uppgifter som beskriver en persons utseende ska alltid utformas på ett objektivet sätt med respekt för människovärdet.

Paragrafen anger i vilken utsträckning känsliga personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Frågan har behandlats i avsnitt 8.

Enligt *första stycket* får personuppgifter inte behandlas på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Bestämmelsen överensstämmer nära med 5 § polisdatalagen. Uttrycket sexuell läggning i den lagen har dock ersatts med uttrycket sexualliv, vilket motsvarar ordalydelsen i personuppgiftslagen. Som en följd av bestämmelsen är det inte tillåtet att föra register över eller på annat sätt göra anteckningar om enskilda enbart på den grunden att de utifrån ras, etniskt ursprung eller något annat i paragrafen angivet kriterium kan hänföras till en viss kategori av människor.

En uppgift om utseende utgör normalt inte en sådan personuppgift som avses i första stycket och den får alltså behandlas, med den begränsning som följer av tredje stycket. Om en sådan uppgift samtidigt innefattar uppgift om ras eller etniskt ursprung, omfattas den dock av bestämmelsen.

Bestämmelsen i första stycket hindrar inte heller att uppgifter om en persons nationalitet behandlas, eftersom en sådan uppgift normalt inte ger upplysning om ras eller etniskt ursprung. Likaså faller som regel uppgifter om att en viss person närmast kommer från en viss världsdel eller ett visst land utanför förbudet mot behandling av känsliga personuppgifter. Uppgifter om att N.N. är spansk medborgare, född i Spanien eller inrest från Spanien omfattas alltså inte av förbudet. Skulle emellertid en sådan uppgift i det enskilda fallet avslöja ras eller etniskt ursprung faller den in under paragrafen.

*Andra stycket* innerhåller två undantag från huvudregeln, varav det ena motsvarar 5 § polisdatalagen. För det första får uppgifter om en person som behandlas på annan grund kompletteras med sådana uppgifter som avses i första stycket, om det är absolut nödvändigt för syftet med behandlingen. Bestämmelsen innebär att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får dessa kompletteras med uppgifter om ras eller etniskt ursprung om det är av avgörande betydelse för utredningen. Under utredning av ett sexualbrott kan det t.ex. någon gång vara befogat att anteckna uppgifter om någon av de misstänkta sexualliv. Med hänsyn till den restriktivitet som ligger i begreppet "absolut nödvändigt" måste dock givetvis behovet av att göra sådana kompletteringar prövas noga i det enskilda ärendet.

För det andra får känsliga personuppgifter alltid behandlas i de fall som avses i 7 §, dvs. om det är nödvändigt för diarieföring eller, i fråga om uppgifter i ansökan eller liknande, om det är nödvändigt för handläggningen. Det innebär bl.a. att det är möjligt för polisen att ta emot och besvara anmälningar och liknande skrifter som lämnas i elektronisk form även om dessa innehåller känsliga personuppgifter.

I *tredje stycket*, som saknar motsvarighet i polisdatalagen, föreskrivs att uppgifter som beskriver en persons utseende ska utformas på ett objektiva sätt med respekt för människovärdet. Syftet med bestämmelsen är att förhindra att personer beskrivs i nedsättande ordalag som kan vara kränkande för individen.

Exempel på signalementsbeteckningar som anses acceptabla finns bl.a. i Rikspolisstyrelsens föreskrifter och allmänna råd om fingeravtryck och fotografering (RPSFS 2000:16, FAP 473-1).

Som bestämmelserna i paragrafen har utformats är polisen alltid oförhindrad att, när den får ett tips från allmänheten om att en person kan misstänkas för brottslig verksamhet, göra de anteckningar som är nödvändiga för att underlätta identifieringen av personen, t.ex. anteckningar om fysiska kännetecken. Anteckningarna måste dock – i enlighet med tredje stycket – utformas på ett objektivt sätt. I anslutning till dessa anteckningar får även sådana känsliga personuppgifter som avses i första stycket antecknas, under förutsättning att det är absolut nödvändigt för det polisarbete som tipset bör föranleda.

### Behandling av uppgifter om resultat av DNA-analyser

- 9 § Uppgifter om resultat av DNA-analyser får endast behandlas
1. i en förundersökning, eller
  2. enligt bestämmelserna i 4 kap. om behandling i DNA-register, utredningsregister och spårregister.

I paragrafen regleras uttömmande vad som gäller i fråga om behandling av resultat av DNA-analyser. Härmed avses behandlingen av en DNA-profil. Behandlingen av det utlåtande över vad som förekommit vid analysarbetet och vilken identifiering som i förekommande fall har gjorts, regleras således inte här. Motiven till bestämmelsen har behandlats i avsnitt 8.

Av paragrafen framgår att resultatet av en DNA-analys, d.v.s. DNA-profilen, endast får behandlas inom ramen för en förundersökning eller i särskilda register. Förstnämnda fall tar sikte på den behandling som sker hos Statens kriminaltekniska laboratorium; såväl analysen av ett enskilt prov som de jämförelser med annat DNA-material och med uppgifter ur DNA-register som utförs som ett led i arbetet med att spåra DNA och att fastslå identiteten på den person från vilken DNA-materialet härrör. I de fall där Statens kriminaltekniska laboratorium begär hjälp med

analysen av ett utländskt laboratorium eller någon annan sakkunnig utanför polisväsendet har behandlingen också stöd i paragrafen, så länge den utgör ett led i en förundersökning.

Behandlingen av resultat från DNA-analyser i särskilda register regleras i 4 kap. 1–13 §§.

### Tillgången till personuppgifter

**10 §** Tillgången till personuppgifter ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

I paragrafen anges att tillgången till personuppgifter alltid ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter. Skälen till bestämmelsen har behandlats i avsnitt 6.7. Bestämmelsen ska ses mot bakgrund av att det totala antalet uppgifter som förekommer i polisens brottsbekämpande verksamhet är betydande och att många av dessa uppgifter kan vara av integritetskänsligt slag. Med tillgång avses inte bara tillgång genom direktåtkomst utan även tillgång i skriftlig och muntlig form. Bestämmelsen riktar sig därmed såväl till dem som beslutar om nödvändiga system för personuppgiftsbehandling som till alla tjänstemän som i sin dagliga verksamhet kommer i kontakt med personuppgifter. För den förra gruppen av tjänstemän handlar det om att skapa system som gör att uppgifterna inte sprids på ett omotiverat sätt. För den andra gruppen handlar det om att inte lämna uppgifterna vidare till andra än de tjänstemän som behöver uppgifterna i sitt arbete.

### Gallring

**11 §** Personuppgifter som behandlas automatiserat i ett ärende ska gallras senast ett år efter det att ärendet avslutades. Personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Bestämmelserna i första stycket gäller inte

1. uppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken,
2. uppgifter som har gjorts gemensamt tillgängliga, och
3. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

Paragrafen reglerar gallring av personuppgifter som behandlas automatiserat och som inte har gjorts gemensamt tillgängliga. Frågan om gallring av detta slag av uppgifter har behandlats i avsnitt 16.1. För gallring av gemensamt tillgängliga personuppgifter finns särskilda bestämmelser i 3 kap. 16–18 §§.

Såsom framgår av *första stycket* ska personuppgifter som behandlas i ett ärende gallras senast ett år efter det att ärendet avslutades, medan personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången. Gallringsfristens längd beror alltså på om personuppgifterna behandlas inom ett ärende eller inte. Begreppet ärende har här en särskild innebörd som kan avvika från den innebörd som begreppet har i förvaltningslagen (1986:223). Med ärende avses en serie åtgärder som är avsedd att leda fram till ett bestämt slut. Ett exempel på detta är ett särskilt underrättelseprojekt. Också åtgärder som vidtas med anledning av att någon enskild har påkallat att polisen agerar får anses som ett ärende. Det är däremot inte fråga om något särskilt ärende när en polisman vidtar en tillfällig åtgärd inom ramen för polisens fortlöpande verksamhet, t.ex. tar emot ett tips från allmänheten som inte har samband med en pågående brottsutredning eller ett underrättelseprojekt.

Traditionellt har gallring inneburit utsortering och förstöring av dokument. I samband med gallringen har alltså såväl informationen som informationsbäraren försvunnit. I fråga om information på ADB-medium anses dock att gallring sker även då den elektroniskt lagrade informationen överförs till en pappersutskrift och sedan raderas från ADB-mediet. Avgörande för om gallring ska anses ha skett anses vara om olika möjligheter att

söka i eller göra sammanställningar av materialet har gått förlo-  
rade (se SOU 2002:97 s. 73). Också överföring till andra data-  
bärare kan vara att anse som gallring, nämligen om överföringen  
innebär informationsförlust, förlust av möjliga informations-  
sammanställningar, förlust av sökmöjligheter eller förlust av  
möjligheter att fastställa informationens autenticitet (se Riksar-  
kivets föreskrifter RA-FS 1991:1 och 1994:2).

Som framgår av *andra stycket* gäller andra bestämmelser för  
vissa typer av uppgifter. Enligt *punkten 1* gäller inte gallringsbe-  
stämmelserna i första stycket i fråga om personuppgifter i en  
brottsanmälan eller förundersökning. I fråga om sådana person-  
uppgifter gäller i stället bestämmelserna om gallring i arkivlagen.  
Detsamma gäller personuppgifter i ”annan utredning som hand-  
läggs enligt bestämmelser i 23 kap. rättegångsbalken”. Med detta  
uttryck avses *dels* s.k. primärutredningar som görs med stöd av  
23 kap. 3 § tredje stycket rättegångsbalken innan förundersök-  
ning har inletts, *dels* s.k. förenklade utredningar som görs i så-  
dana fall där det enligt 23 kap. 22 § rättegångsbalken inte krävs  
någon förundersökning, *dels* utredningar som enligt bestämmel-  
ser i annan författning ska handläggas enligt 23 kap. rättegångs-  
balken. Bestämmelser av det sistnämnda slaget finns bl.a. i 16 §  
lagen (1957:668) om utlämning för brott, 10 § lagen (1959:254)  
om utlämning för brott till Danmark, Finland, Island och Norge,  
31 § lagen (1964:167) med särskilda bestämmelser om unga lag-  
överträdare, 9 § lagen (1988:688) om besöksförbud, 3 § lagen  
(2003:1156) om överlämnande från Sverige enligt en europeisk  
arresteringsorder och 8 § lagen (2005:321) om tillträdesförbud  
vid idrottsarrangemang. Många brottsanmälningar och allmänna  
påståenden om brottsliga gärningar föranleder ingen annan åtgärd  
än ett beslut att förundersökning inte ska inledas. Det-  
samma gäller sådana skrivelser från enskilda där det är oklart om  
den ska uppfattas som en anmälan eller inte. För att dessa inte  
ska falla under regleringen i första stycket omnämns de särskilt.

Enligt *punkten 2* ska gallringsbestämmelsen i första stycket  
inte tillämpas på uppgifter som har gjorts gemensamt tillgäng-

liga. För sådana uppgifter gäller särskilda gallringsregler i 3 kap. 16–18 §§.

Av *punkten 3* framgår att regeringen eller den myndighet regeringen bestämmer kan meddela föreskrifter om att personuppgifter, trots vad som sägs i första stycket, får bevaras för historiska, statistiska eller vetenskapliga ändamål. En motsvarande bestämmelse finns i 13 § andra stycket polisdatalagen.

### Utlämnande av uppgifter och uppgiftsskyldighet

**12 §** Personuppgifter som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Enligt paragrafen, som motsvarar 6 § polisdatalagen, ska personuppgifter som är nödvändiga för att framställa rättsstatistik lämnas till den myndighet som ansvarar för framställandet av sådan statistik. Bestämmelsen, vars bakgrund har beskrivits i avsnitt 13.2, bryter den sekretess som kan råda för personuppgifterna.

Av förordningen (2001:100) om den officiella statistiken framgår att Brottsförebyggande rådet är statistikansvarig myndighet på rättsväsendets område, med undantag för domstolarnas verksamhet.

**13 §** Personuppgifter får lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Om det är förenligt med svenska intressen, får uppgifter vidare lämnas

1. till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott, eller

2. till utländsk underrättelse- eller säkerhetstjänst.

Av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) följer att uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation även i vissa andra fall.



Paragrafen innehåller bestämmelser om utlämnande till utländsk myndighet eller mellanfolklig organisation. Frågan har behandlats i avsnitt 13.3.

Inom ramen för de allmänna ändamålen för personuppgiftsbehandling i 5 § 1 och 2 kan det i vissa fall finnas anledning att föra över uppgifter till en utländsk myndighet. Så blir fallet när en svensk myndighet vid en svensk brottsutredning begär rättsligt bistånd från en utländsk myndighet eller när en svensk myndighet aktualiserar en fråga om överföring av verkställighet till utlandet. Av 5 § 3 framgår att personuppgifter får behandlas för att fullgöra de förpliktelser som följer av internationella åtaganden (se kommentaren till den paragrafen); också i sådana fall blir det ofta aktuellt att lämna information till en utländsk myndighet. Vidare innehåller 6 § en allmän bestämmelse om att personuppgifter som behandlas enligt 5 § också får behandlas för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos utländsk myndighet. De nu angivna bestämmelserna sätter gränserna för när behandling som har till ändamål att överföra information till utländsk myndighet över huvud taget får förekomma.

För att sådant utlämnande ska få ske krävs emellertid därutöver att det inte på grund av sekretess finns hinder mot att lämna över uppgifterna till en utländsk myndighet. För många av de personuppgifter som förekommer hos polisen gäller sekretess, såväl sekretess till skydd för intresset av att förebygga och beivra brott som sekretess till skydd för enskilds ekonomiska eller personliga förhållanden. Enligt 1 kap. 3 § tredje stycket sekretesslagen får en sekretessbelagd uppgift inte röjas för en utländsk myndighet eller en mellanfolklig organisation annat än om utlämnandet sker i enlighet med en särskild föreskrift om detta i lag eller förordning eller om uppgiften i motsvarande fall skulle få utlämnas till en svensk myndighet och det enligt den utlämnande myndigheten står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Det har ansetts att 1 kap. 3 § sekretesslagen bör tillämpas även i fråga om personuppgifter i brottsbekämpande verksamhet. En erinran om den paragrafen har därför tagits in i *tredje stycket* av förevarande paragraf. I vissa fall kan emellertid en utlämnandeprövning enligt 1 kap. 3 § sekretesslagen vara komplicerad. I den nya regleringen anges därför vissa mera preciserade fall där utlämnande av en uppgift till utländsk myndighet får ske, trots att det gäller sekretess för uppgiften. Bestämmelsen om detta i paragrafens första stycke överensstämmer i huvudsak med 7 § första stycket polisdatalagen. Bestämmelserna i paragrafens andra stycke punkterna överensstämmer i huvudsak med 18 § polisdataförordningen.

I *första stycket* anges sålunda att personuppgifter får lämnas ut till en utländsk myndighet eller en mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Bestämmelsen är tillämplig när den internationella överenskommelsen ålägger Sverige att lämna ut vissa slag av uppgifter. Däremot gäller den inte för överenskommelser där det enbart sägs att utlämnande *får* ske.

Enligt *andra stycket* får uppgifter, om det är förenligt med svenska intressen, även lämnas till en polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, till Interpol och Euro-pol (*punkten 1*) samt till utländsk underrättelse- eller säkerhetstjänst (*punkten 2*). Utlämnande av uppgifter till polis- eller åklagarmyndighet samt till Interpol eller Europol får ske endast om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott. Bestämmelsen ger liksom i dag utrymme för svenska myndigheter att lämna ut uppgifter utan föregående begäran från en utländsk myndighet.

Såsom har utvecklats närmare i avsnitt 13.3 måste den utlämnande myndigheten alltid försäkra sig om att den mottagande staten har en adekvat nivå för skyddet av personuppgifter innan uppgifter lämnas ut, se 33 § personuppgiftslagen.

14 § Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) ska personuppgifter som har gjorts gemensamt tillgängliga hos polisen lämnas till Rikspolisstyrelsen, polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet.

Första stycket gäller inte uppgifter som behandlas i särskilda register med stöd av 4 kap.

Paragrafen innehåller en bestämmelse som i viss utsträckning bryter den sekretess som annars skulle ha gällt gentemot andra myndigheter. Frågan har behandlats i avsnitt 13.2.

I *första stycket* regleras andra brottsbekämpande myndigheters rätt att, utan hinder av viss i paragrafen angiven sekretess till skydd för enskild, i den brottsbekämpande verksamheten få del av personuppgifter som har gjorts gemensamt tillgängliga inom polisen. Eftersom sekretess kan hindra att uppgifter lämnas ut, har undantag gjorts för vissa typer av sekretess, där sekretessen är lika stark hos den mottagande myndigheten som hos den utlämnande. Paragrafen har utformats som en uppgiftsskyldighet. En förutsättning för att uppgifterna ska lämnas ut är dock att det finns ett behov av uppgifterna hos den mottagande myndigheten. Det är den utlämnande myndigheten, dvs. i detta fall polisen, som ytterst avgör om den andra myndigheten har behov av uppgiften för sin brottsbekämpande verksamhet. Det förutsätts emellertid att den myndighet som vill ha tillgång till en sådan uppgift lämnar polisen det underlag som kan krävas för en korrekt bedömning av behovet. Uppgifter kan lämnas ut antingen på begäran av den andra myndigheten eller på polisens eget initiativ.

Endast uppgifter i polisens brottsbekämpande verksamhet omfattas. Det innebär att uppgifter i polisens övriga verksamhet faller utanför tillämpningsområdet.

Med polismyndighet avses även Säkerhetspolisen när myndigheten för Rikspolisstyrelsens räkning leder och bedriver polisverksamhet (se 7 § andra stycket polislagen [1984:387] jämförd

med 2 § förordningen [2002:1050] med instruktion för Säkerhetspolisen). När Säkerhetspolisen utför andra uppgifter (3 § samma förordning) är myndigheten en del av Rikspolisstyrelsen. Uppgifter som behandlas hos den övriga polisen kan således utan hinder av i paragrafen angiven sekretess i vissa fall lämnas till Säkerhetspolisen.

I *andra stycket* görs undantag för uppgifter som behandlas i de register som regleras särskilt i 4 kap. Om sådana uppgifter kan lämnas ut får, som huvudregel, avgöras efter en sekretessbedömning i det enskilda fallet. Som framgår av 15 och 16 §§ gäller dock särskilda bestämmelser om utlämnande av uppgifter från register med uppgifter om resultat av DNA-analyser och fingeravtrycks- eller signalementsregister.

**15 §** Uppgift om huruvida en person förekommer i register med uppgifter om resultat av DNA-analyser ska utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) lämnas till polismyndighet, Åklagarmyndigheten och Ekobrottsmyndigheten, om den mottagande myndigheten har behov av uppgiften i sin brottsbekämpande verksamhet.

I paragrafen regleras vissa myndigheters rätt att, utan hinder av viss i paragrafen angiven sekretess till skydd för enskild, i den brottsbekämpande verksamheten få del av uppgift ur register om resultat av DNA-analyser (avsnitt 13.2). Endast uppgift om huruvida någon förekommer i registret omfattas av bestämmelsen. Den krets av myndigheter som anges i bestämmelsen är snävare än kretsen i 14 § och består av de myndigheter som kan medges direktåtkomst enligt 4 kap. 12 §. En förutsättning för att uppgifterna ska lämnas ut är att de behövs för den brottsbekämpande verksamheten hos den mottagande myndigheten. Vad som har sagts i anslutning till 14 § angående behovet av uppgifter och om paragrafens tillämplighet på Säkerhetspolisen gäller även i fråga om denna bestämmelse.

16 § Personuppgifter som behandlas i fingeravtrycks- eller signalementsregister med stöd av 4 kap. 14–19 §§ ska utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) lämnas till polismyndighet, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om den mottagande myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet.

Paragrafen innehåller, på motsvarande sätt som 14 och 15 §§, en bestämmelse om att uppgifter ur fingeravtrycks- och signalementsregister får lämnas ut till en annan i paragrafen angiven brottsbekämpande myndighet även om det råder viss sekretess till skydd för enskild för uppgiften i fråga (avsnitt 13.2). Den krets av myndigheter som har rätt att få del av sådana uppgifter motsvarar vad som enligt 4 kap. 18 § gäller för direktåtkomst till vissa uppgifter i registren i fråga.

En förutsättning för att uppgifterna ska lämnas ut är att de behövs för den brottsbekämpande verksamheten hos den mottagande myndigheten. Vad som har sagts i anslutning till 14 § angående behovet av uppgifter och om paragrafens tillämplighet på Säkerhetspolisen gäller även i fråga om denna bestämmelse.

17 § Regeringen meddelar föreskrifter om att personuppgifter får lämnas ut även i andra fall än som sägs i 12–16 §§.

Av paragrafen följer att regeringen har möjlighet att meddela föreskrifter om att personuppgifter får lämnas ut även i andra fall än som anges i 12–16 §§ (jfr 1 kap. 3 § första och tredje styckena sekretesslagen). Det kan vara aktuellt med föreskrifter som motsvarar 17 och 17 a §§ polisdataförordningen (1999:81). Vidare kan det behövas föreskrifter som möjliggör för finanspolisen att lämna ut uppgifter till utländska myndigheter som har motsvarande uppdrag att ta emot och lämna ut information om misstänkt penningtvätt eller finansiering av särskilt allvarlig brottslighet (se kommentaren till 4 kap. 20 §). Undantagsvis kan det nämligen vara en annan utländsk myndighet än en polis- eller

åklagarmyndighet som utför detta arbete. Möjligheten att lämna ut uppgifter omfattas därmed inte av 13 § andra stycket 1.

### 3 kap. Gemensamt tillgängliga uppgifter

1 § Detta kapitel innehåller särskilda bestämmelser för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet. Uppgifter som endast ett fåtal bestämda personer har rätt att ta del av anses inte som gemensamt tillgängliga.

Såsom närmare har utvecklats i avsnitt 9.1 bygger den föreslagna lagen på en uppdelning mellan *å ena sidan* behandling av ”gemensamt tillgängliga uppgifter” eller behandling som innebär att uppgifter blir gemensamt tillgängliga och *å andra sidan* annan behandling. Bestämmelserna i 3 kap. gäller vid behandling av det förra slaget.

Om avsikten är att uppgifterna ska vara åtkomliga för en i förväg obestämd krets av anställda inom polisen, får uppgifterna alltid anses vara gemensamt tillgängliga. Som exempel på detta kan nämnas uppgifter i polisens nationella uppgiftssamlingar men även lokala register där det inte på förhand har bestämts exakt vilka personer som får ha tillgång till uppgifterna. Det samma gäller uppgiftssamlingar som endast en bestämd krets av personer har tillgång till om det är förutsatt att denna krets komma att ändras längre fram. Att olika personalkategorier kan ha olika behörighet, och att en uppgift därför i praktiken vid en viss tidpunkt är åtkomlig enbart för ett begränsat antal personer eller enbart för handläggare inom en viss polismyndighet, innebär alltså inte att uppgiften inte kan anses vara gemensamt tillgänglig. Uppgifter som en annan brottsbekämpande myndighet har tillgång till genom direktåtkomst är alltid gemensamt tillgängliga, se kommentaren till 3 kap. 9 §.

Om uppgifterna å andra sidan lagras på ett sådant sätt att endast en viss person har tillgång till dem, kan uppgifterna normalt inte anses gemensamt tillgängliga. En uppgift som lagras elek-

troniskt på hårddisken i en dator eller en server i samband med att en enskild tjänsteman arbetar med ordbehandling och som är åtkomlig endast för tjänstemannen själv (och för systemadministratören) kan alltså inte anses vara gemensamt tillgänglig. Detta gäller även om syftet är att uppgiften senare ska lagras så att andra får tillgång till den. I sådana fall är därför bestämmelserna i 3 kap. inte tillämpliga. Härav följer också att insamling av personuppgifter genom upptagning av bild eller ljud med digital teknik inte omfattas av 3 kap., utom i de fall där de görs gemensamt tillgängliga samtidigt som insamlingen görs, exempelvis genom en direktsändning av upptagningen till ett större antal mottagare. Det är alltså först när insamlade uppgifter av detta slag görs gemensamt tillgängliga i den brottsbekämpande verksamheten som bestämmelserna i 3 kap. måste tillämpas. En annan sak är att den som samlar in uppgifter, som kan antas bli gemensamt tillgängliga vid en senare tidpunkt, givetvis bör beakta de regler som gäller för behandling av gemensamt tillgängliga uppgifter för att inte försvåra den fortsatta behandlingen.

I vad mån uppgifter som är tillgängliga enbart för en bestämd krets av personer är att anse som gemensamt tillgängliga får bedömas med hänsyn till främst hur många personer som ingår i kretsen. Enbart det förhållandet att kretsen består av flera personer innebär inte att uppgifterna ska anses gemensamt tillgängliga. Behandlingar som sker exempelvis inom ramen för särskilda underrättelseprojekt i vilka endast vissa utpekade tjänstemän deltar, kan alltså mycket väl falla utanför bestämmelserna i 3 kap. Om antalet tjänstemän i en sådan grupp uppgår till mer än ett fåtal, måste dock de personuppgifter som behandlas inom gruppen, trots att den är avgränsad, anses vara gemensamt tillgängliga. Var gränsen går får bedömas med hänsyn till samtliga omständigheter i ett enskilt fall, men en tumregel kan vara att uppgifterna är att anse som gemensamt tillgängliga om antalet deltagare i gruppen överstiger ett tiotal.

Även den tid under vilken uppgifter avses bli behandlade kan ha betydelse för frågan om uppgifterna ska anses vara gemensamt tillgängliga eller inte. I projekt med längre varaktighet

måste man således räkna med att de personer som sysslar med projektet med tiden kommer att bytas ut. Som en följd av detta kommer de uppgifter som behandlas med tiden att bli tillgängliga för ett större antal personer än vad som motsvarar det normala antalet deltagare i projektet. Mot den bakgrunden får uppgifter som behandlas i långsiktiga projekt ofta anses vara gemensamt tillgängliga, trots att antalet deltagare vid varje givet tillfälle är begränsat. Störst betydelse torde detta ha för underrättelseverksamheten.

När det gäller frågan om huruvida en uppgift är gemensamt tillgänglig eller inte är det viktigt att framhålla att karaktären av en uppgift kan förändras under den tid som den behandlas. Uppgifter som från början har betraktats som icke gemensamt tillgängliga kan göras gemensamt tillgängliga. Det kan t.ex. bli nödvändigt att göra viss underrättelseinformation tillgänglig för tjänstemän utanför det aktuella underrättelseprojektet. När så har skett ska de strängare bestämmelserna om behandling av sådana uppgifter tillämpas.

Som exempel på existerande uppgiftssamlingar där uppgifterna måste anses gemensamt tillgängliga kan nämnas det centrala kriminalunderrättelseregistret, det allmänna spaningsregistret, det centrala brottspaningsregistret och beslags- och analysregistren. Som nyss nämnts bör även uppgifter i större särskilda undersökningar anses vara gemensamt tillgängliga.

### Personuppgifter som får göras gemensamt tillgängliga

2 § Endast följande personuppgifter får göras gemensamt tillgängliga.

1. Uppgifter som kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten
  - a) innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller
  - b) sker systematiskt.
2. Uppgifter som behövs för övervakningen av en person, om han eller hon



a) kan antas komma att begå brott för vilket är föreskrivet fängelse i två år eller däröver, och

b) är allvarligt kriminellt belastad eller kan antas vara farlig för annans personliga säkerhet.

3. Uppgifter som förekommer i ett ärende om utredning eller beivrande av brott.

4. Uppgifter som behövs för att fullgöra de förpliktelser som följer av internationella åtaganden.

5. Uppgifter som har rapporterats till polisens kommunikationscentraler.

Uppgifter om resultat av DNA-analyser får inte göras gemensamt tillgängliga. Att sådana uppgifter får behandlas i särskilda register följer av 4 kap.

Uppgifter som avses i första stycket 4 får göras gemensamt tillgängliga endast om det behövs för att fullgöra den aktuella förpliktelsen.

Tillgången till uppgifter som görs gemensamt tillgängliga med stöd av första stycket 2 ska begränsas till särskilt angivna tjänstemän som har till uppgift att arbeta med övervakningen. Information om huruvida en person är föremål för övervakning får dock göras tillgänglig för flera.

När personuppgifter görs gemensamt tillgängliga (se kommentaren till 1 § om innebörden av uttrycket "gemensamt tillgängliga") innebär det, typiskt sett, ökade risker för intrång i den personliga integriteten. Paragrafens *första stycke* innehåller därför en uppräkningslista av de typer av personuppgifter som får göras gemensamt tillgängliga. Uppräkningslistan är avsedd att vara uttömmande och det är alltså inte tillåtet att göra personuppgifter gemensamt tillgängliga i andra fall.

I *punkten 1*, som har behandlats närmare i avsnitt 9.2, nämns personuppgifter "som kan antas ha samband med misstänkt brottslig verksamhet". Rekviritet innebär att det måste finnas en misstanke om att sådan brottslig verksamhet som avses 2 kap. 5 § 1 har begåtts eller kommer att begås. Den brottsliga verksamheten måste vara på visst sätt kvalificerad. Huvudregeln är att den ska innefatta brott som kan ge fängelse i ett år eller däröver. Detta innebär att alla brott som enligt huvudregeln i 24 kap. 1 § rättegångsbalken kan föranleda häktning omfattas. Även om den

brottsliga verksamheten inte innefattar brott med en sådan straffskala – såsom exempelvis är fallet om verksamheten innefattar enbart bedrägligt beteende i form av s.k. snyltning, dvs. att inte göra rätt för sig på hotell och liknande – får personuppgifter som kan antas ha samband med den brottsliga verksamheten göras gemensamt tillgängliga om det kan antas att verksamheten sker systematiskt. Att personuppgifterna ”kan antas ha samband” med den brottsliga verksamheten innebär att de ska kunna antas ha någon direkt eller indirekt koppling till den brottsliga verksamheten. Det kan vara fråga om uppgifter om en misstänkt, en målsägande, ett vittne eller någon annan person som har en direkt anknytning till brottsligheten. Även en affärspartner till den misstänkte kan ibland ha en sådan anknytning, exempelvis om man misstänker att den brottsliga verksamheten helt eller delvis bedrivs i samma lokal som affärsverksamheten. Det kan också vara fråga om indirekta personuppgifter, t.ex. adressuppgifter eller uppgifter om transportmedel eller andra föremål som har eller kan antas ha anknytning till fysiska personer. Det följer av 2 kap. 5 § 1 att uppgifterna alltid ska vara behövliga i arbetet med att förebygga, förhindra eller upptäcka den aktuella brottsliga verksamheten.

*Punkten 2*, som har behandlats närmare i avsnitt 9.2, avser personuppgifter som behövs för övervakningen av vissa personer som kan antas komma att begå brott med två års fängelse eller däröver i straffskalan. Bestämmelsen anknyter till den särskilda bevakning av yrkeskriminella som polisen redan i dag bedriver. Den torde därför få sin främsta betydelse ifråga om personer som bedöms mer eller mindre livnära sig på allvarlig brottslig verksamhet, t.ex. organiserad brottslighet i form av grov narkotikasmuggling eller grov människohandel. Bedömningen av om en person kan antas komma att begå brott får i första hand göras på grund av tidigare domar. Även pågående brottsutredningar och trovärdiga underrättelseuppgifter bör dock kunna beaktas. Enbart det faktum att en person kan antas vara brottsbenägen räcker dock inte för att uppgifter om honom eller henne ska få göras gemensamt tillgängliga. Därutöver krävs att personens ti-

digare brottslighet är av allvarligt slag – varvid ett riktmärke kan vara att den bedöms ha ett straffvärde på minst två års fängelse – eller att personen kan antas vara farlig för annans personliga säkerhet, t.ex. därför att han eller hon har hotat att döda eller misshandla någon annan.

Med stöd av punkten 2 får också mera allmänna uppgifter om den övervakade personen göras gemensamt tillgängliga. Det behöver alltså inte – till skillnad från vad som gäller enligt punkten 1 – finnas något antaget samband mellan personuppgiften och viss brottslig verksamhet. Det finns därför ett visst utrymme för att i ett register över övervakade yrkeskriminella personer föra in uppgifter om anhöriga, bekanta m.m. Uppgifterna måste dock alltid vara relevanta för övervakningen och – som följer av 2 kap. 5 § – nödvändiga för att förebygga, förhindra och upptäcka brottslig verksamhet.

Av *punkten 3*, som har behandlats närmare i avsnitt 9.3, framgår att personuppgifter som ingår i ett ärende om utredning och beivrande av brott alltid får göras gemensamt tillgängliga. Det handlar här om personuppgifter som behandlas enligt 2 kap. 5 § 2, t.ex. uppgifter i en brottsanmälan eller uppgifter som behandlas inom ramen för en förundersökning.

*Punkten 4*, som har behandlats i avsnitt 9.5, innebär att det är tillåtet att göra uppgifter gemensamt tillgängliga för att fullgöra internationella förpliktelser. Det handlar bl.a. om sådana internationella efterlysningar av personer eller föremål som kommer från andra länder. Dessa är avsedda att spridas inom polisorganisationen. När brottsbekämpande myndigheter i Sverige bedriver brottsutredningar tillsammans med sina motsvarigheter i andra länder eller när man i flera länder bedriver parallella brottsutredningar eller samlar underrättelseinformation om samma brottslighet (exempelvis narkotikabrottslighet eller människohandel), kan det också finnas ett behov av göra uppgifterna gemensamt tillgängliga. Om utländska uppgifter föranleder en svensk brottsutredning eller ett svenskt underrättelseprojekt, behandlas uppgifterna med stöd av de grundläggande ändamålen i 2 kap. 5 §

1 eller 2 och kan då göras gemensamt tillgängliga på samma sätt som andra uppgifter som förekommer i ett sådant ärende.

Vid rättslig hjälp förekommer ofta direktkommunikation mellan myndigheterna i olika länder. I dessa fall, där samarbetet rör en viss bestämd fråga i ett enskilt ärende, torde det normalt inte finnas något behov av att göra de personuppgifter som behandlas inom ramen för ärendet gemensamt tillgängliga.

Ett annat exempel är arbetet vid en nationell kontaktpunkt. Det internationella samarbetet bygger i allt större utsträckning på att länderna har nationella kontaktpunkter för vissa typer av brådskande ärenden. En sådan kontaktpunkt ska vara tillgänglig dygnet runt året om för att besvara förfrågningar, förmedla kontakter till polis och åklagare, vidarebefordra ärenden m.m. De uppgifter som lämnas till en nationell kontaktpunkt ska kunna vara gemensamt tillgängliga. Såsom framgår av tredje stycket får dock uppgifterna för dessa fall göras gemensamt tillgängliga enbart i den utsträckning det är nödvändigt för att fullgöra den internationella förpliktelsen.

Enligt *punkten 5* får även uppgifter som har rapporterats till kommunikationscentraler behandlas gemensamt. Motiven för denna bestämmelse har redovisats i avsnitt 9.4. Eftersom lagen enbart gäller för den brottsbekämpande verksamheten hos polisen, är det enbart rapporter som har relevans för sådan verksamhet, dvs. som omfattas av 2 kap. 5 § 1 och 2, som får göras gemensamt tillgängliga enligt denna punkt. För övrig verksamhet vid kommunikationscentralerna tillämpas personuppgiftslagen (se avsnitt 6.3).

Enligt *andra stycket* får uppgifter om resultat av DNA-analyser inte göras gemensamt tillgängliga. Däremot får sådana uppgifter behandlas i särskilda register enligt 4 kap., om förutsättningarna i övrigt för en sådan behandling är uppfyllda. Med ”resultat av DNA-analyser” avses DNA-profiler (se kommentaren till 2 kap. 9 §). Bestämmelsen hindrar därmed inte att ett utlåtande över den eventuella identifiering som har gjorts och vad som har förekommit vid analysarbetet görs gemensamt tillgängligt med stöd av första stycket punkten 3.

I *tredje stycket*, som har behandlats i avsnitt 9.5, anges att uppgifter som behandlas för att fullgöra internationella förpliktelser får göras gemensamt tillgängliga endast om detta är nödvändigt för att fullgöra den aktuella förpliktelsen. Inom ramen för Euro-polsamarbetet tar Sverige emot ett stort antal uppgifter. Uppgifterna torde i de allra flesta fall vara sådana som får göras gemensamt tillgängliga med stöd av någon annan punkt än punkten 4. Om så inte är fallet blir dock tredje stycket tillämpligt. En tillämpning av stycket kan bl.a. aktualiseras för uppgifter som behöver föras in i efterlysningsregister och för sådan behandling av ärenden vid en nationell kontaktpunkt som har redogjorts för under punkten 4 ovan.

I *fjärde stycket* kompletteras den allmänna bestämmelsen i 2 kap. 10 § om att tillgången till uppgifter ska begränsas med en bestämmelse som begränsar åtkomsten till uppgifter som behandlas för att underlätta övervakningen av yrkeskriminella personer. Endast de tjänstemän som arbetar med denna övervakning får ha tillgång till uppgifterna. Tillgången till uppgifter behöver däremot inte begränsas till tjänstemän vid en viss myndighet. Vid varje myndighet ska det dock i förväg bestämmas vilka tjänstemän som ska ha tillgång till uppgifterna och ha möjlighet att behandla dem, bl.a. i analysdatabaser. I andra meningen görs ett undantag från åtkomstbegränsningsregeln. Information om huruvida en person är övervakad med stöd av aktuell bestämmelse får spridas till andra. Även här gäller dock som en allmän begränsning att mottagaren måste ha behov av uppgiften för sitt arbete (jfr 2 kap. 10 §).

### Särskilda upplysningar

**3 §** Vid behandling enligt 1 § ska personuppgifterna förses med en särskild upplysning om det närmare ändamålet med behandlingen. Har uppgifterna gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, ska det också lämnas upplysning om detta. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

I paragrafen uppställs krav på särskilda upplysningar om ändamålen med behandlingen m.m. Skälen till regleringen har utvecklats i avsnitt 10.

Enligt första meningen ska personuppgifter som görs eller har gjorts gemensamt tillgängliga förses med upplysning om det närmare ändamålet med behandlingen. Upplysningen måste till att börja med ge information om huruvida uppgiften behandlas enligt 1, 2 eller 3 i 2 kap. 5 § eller om det finns någon annan grund för behandlingen. Härutöver ska upplysning lämnas om för vilket närmare slag av brott eller brottslig verksamhet etc. som behandlingen sker, exempelvis ett underrättelseprojekt om vapensmuggling från Y-land.

Har uppgiften samlats in för visst ändamål och kommer den senare att användas för något nytt ändamål, måste vid den senare behandlingen upplysning om det nya ändamålet lämnas. Om uppgifter från en förundersökning avseende visst brott senare används i kriminalunderrättelseverksamhet avseende annan brottslig verksamhet, måste det således till uppgiften fogas en ny upplysning om ändamålet med denna behandling.

I andra meningen föreskrivs att om uppgifter har gjorts gemensamt tillgängliga med stöd av 2 § första stycket 2 eller 5, så ska upplysning lämnas också om detta. En personuppgift som har gjorts gemensamt tillgänglig enbart som ett led i övervakningen av en yrkeskriminell person ska alltså kompletteras med en upplysning om detta.

Såsom framgår av tredje meningen behöver upplysningar inte lämnas i fall det förhållande, som det ska lämnas upplysning om, redan framgår klart av omständigheterna. En personuppgift som t.ex. behandlas enbart i ett register över övervakade yrkeskriminella personer (jfr 2 § första stycket 2) behöver därför vanligen inte kompletteras med någon särskild upplysning enligt denna paragraf. Om uppgiften förekommer i en förundersökning (jfr 2 § första stycket 3), behövs inte heller någon särskild upplysning.

4 § Om uppgifter, som behandlas enligt 1 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva sådan brottslig verksamhet som avses i 2 § första stycket 1, ska uppgifterna föras med en särskild upplysning om att personen inte är misstänkt. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

Uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska föras med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om inte detta på grund av särskilda omständigheter är onödigt. Detsamma gäller uppgifter om personer som avses i 2 § första stycket 2.

Paragrafen innehåller bestämmelser om att uppgifter som görs eller har gjorts gemensamt tillgängliga i vissa fall ska kompletteras med särskilda upplysningar. Frågan har behandlats i avsnitt 10.

Bestämmelserna avser endast direkta personuppgifter ("om uppgifter..... direkt kan hänföras till en person"). Om den person som en sådan uppgift gäller inte är misstänkt vare sig för något brott eller för sådan brottslig verksamhet som avses i 2 § första stycket 1, följer av *första stycket* att uppgiften ska kompletteras med en särskild upplysning om detta. Upplysningsplikten inträder först om det inte finns några som helst misstankar mot den aktuella personen. Förekommer det misstankar – vare sig det handlar om "skäligen misstanke" eller om någon annan misstankegrad – behöver någon tilläggsupplysning inte lämnas. Upplysning behöver inte heller lämnas, om det av sammanhanget framgår tydligt att det inte är fråga om en misstänkt person. Om en person har hörts under en förundersökning men det av sammanhanget klart framgår att han eller hon har hörts endast som målsägande eller vittne, behöver således uppgifterna inte föras med någon tilläggsupplysning.

Av *andra stycket* följer att uppgifter om personer som kan antas ha samband med misstänkt brottslig verksamhet ska föras med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Kravet på en sådan upplysning avser uppgifter som behandlas utan att det finns misstanke om något

konkret brott, dvs. uppgifter som behandlas för ändamålet förebygga, förhindra eller upptäcka brottslig verksamhet. Bestämningen är således inte tillämplig på uppgifter som behandlas i brottsutredande verksamhet.

Upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak behöver inte lämnas om detta på grund av särskilda omständigheter skulle vara onödigt. Så kan exempelvis vara fallet om uppgifter om en viss person hämtas från offentliga register, t.ex. adress- och telefonuppgifter. Framgår det att en uppgift har lämnats av en polisman, krävs det normalt inte någon värdering av trovärdigheten, eftersom det följer av en polismanns tjänsteplikt att lämna korrekta uppgifter. Däremot ska en bedömning av riktigheten i sak alltid göras, eftersom en iakttagelse eller bedömning kan vara osäker oberoende av från vem den kommer. Det kan t.ex. vara fråga om en iakttagelse som har gjorts under ogynnsamma yttre omständigheter (regn, dimma, långt avstånd eller liknande) och som därför är osäker.

## Sökning

5 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp.

Vad som sägs i första stycket hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

Paragrafen innehåller i *första stycket* ett förbud mot att använda känsliga personuppgifter (dvs. uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv) som sökbegrepp vid sökning i gemensamt tillgängliga uppgifter. Frågan har behandlats i avsnitt 11.1. Av *andra stycket* följer att förbudet inte hindrar att man använder uppgifter som beskriver en persons utseende som sökbegrepp även om sådana uppgifter,



t.ex. uppgift om hudfärg, kan ge indikationer om personens ras eller etniska ursprung.

6 § Vid sökning i gemensamt tillgängliga uppgifter på namn, firma, personnummer, samordningsnummer, organisationsnummer eller andra liknande identitetsbeteckningar får endast sådana uppgifter tas fram som anger att den sökta personen

1. är anmäld för brott,
2. är misstänkt för brott eller för brottslig verksamhet som avses i 2 § första stycket 1,
3. övervakas enligt 2 § första stycket 2,
4. har anmält ett brott eller är målsägande i ett ärende som rör ansvar för brott,
5. är vittne eller annars ska höras eller avge yttrande i ett ärende,
6. har gett in eller tillhandahållits en handling, eller
7. är anmäld försvunnen.

Paragrafen innehåller en särskild sökbegränsning vid sökning i gemensamt tillgängliga uppgifter på namn, personnummer eller liknande identitetsbeteckningar. Frågan har berörts i avsnitt 11.2.

Mot bakgrund av att de informationsmängder som kan göras gemensamt tillgängliga i polisens brottsbekämpande verksamhet sammantaget kan bli mycket betydande har det inte ansetts lämpligt att tillåta alla slag av sökningar i informationen. Visserligen innebär den nya lagen att namn alltid kan användas som sökbegrepp. En sökning på namn eller personnummer får emellertid inte innebära att all information i polisens brottsbekämpande verksamhet som rör den sökta personen tas fram. Av paragrafen framgår att man vid sökning på namn endast får ta fram sådana uppgifter om den sökta som anger att han eller hon (1) är anmäld för brott, (2) är misstänkt, (3) övervakas, (4) har gjort en brottsanmälan eller är målsägande, (5) är vittne eller annars ska höras eller avge yttrande (6) har gett in en handling eller fått en handling i ett ärende expedierad till sig eller (7) är anmäld försvunnen. Vid sökningen får det alltså inte tas fram uppgifter av annat slag, t.ex. uppgifter från underrättelsearbete som visar att den sökta är släkt med eller inneboende hos en

övervakad person. För sökning på personnummer, samordningsnummer eller organisationsnummer gäller detsamma som för sökning på namn. Med namn avses även delar av namn och med personnummer, samordningsnummer och organisationsnummer även de sifferkombinationer som ingår i numren. Också sökning med hjälp av födelsedatum eller de sista fyra kontrollsiffrorna i ett personnummer omfattas alltså av bestämmelsen. Bestämmelsen är avsedd att omfatta motsvarande nummer i andra länder även om de är uppbyggda på annat sätt.

Bestämmelsen ställer krav på viss anpassning av de tekniska system som används vid sökning. Vid sökning på ett visst namn, N.N., ska det inte komma upp andra uppgifter om N.N. än sådana som anges i paragrafen. Bestämmelsen är dock inte avsedd att förhindra att det vid en sökning, som visar att N.N. är misstänkt för visst brott, också går att ta del av annan, i anslutning till brottsmisstanken angiven information, t.ex. att N.N. är inneboende hos eller släkt med S.S. Vid en sökning på en person som visserligen förekommer i de gemensamt tillgängliga personuppgifterna men inte på något av de sätt som anges i första stycket 1–7 ska det däremot inte komma fram någon information. Om det inte finns några andra uppgifter om S.S. än att han har N.N. som inneboende, ska alltså en sökning på S.S. inte ge någon träff.

I sammanhanget är det viktigt att betona att de föreslagna sökbegränsningarna naturligtvis även gäller för en myndighet som har medgetts direktåtkomst till uppgifter som behandlas inom polisen.

I 7 § finns undantag från sökbegränsningen i paragrafen.

7 § Bestämmelsen i 6 § gäller inte vid

1. sökning i en viss handling eller i ett visst ärende, eller
2. sökning i en uppgiftssamling som har skapats för att undersöka vissa preciserade slag av brottslighet eller vissa preciserade kriminella grupperingar och som enbart de som arbetar i undersökningen eller som omfattas av andra stycket 2 har åtkomst till.

Bestämmelsen i 6 § gäller inte heller vid sökning som

1. sker för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i fyra

år eller däröver eller för sådant ändamål som avses i 2 § första stycket 2, och

2. utförs av särskilt angivna tjänstemän med uppgift att undersöka den brottsliga verksamheten eller övervaka personer enligt 2 § första stycket 2.

Om det finns särskilda skäl får, trots bestämmelsen i 6 §, sökning även ske för att utreda brott för vilket är föreskrivet fängelse i fyra år eller däröver, om sökningen utförs av särskilt angivna tjänstemän.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om och under vilka förutsättningar sökning får äga rum med stöd av andra eller tredje stycket.

Paragrafen innehåller fyra undantag från sökbegränsningsregeln i 6 §. Motiven till dessa undantag har redovisats i avsnitt 11.2.

Enligt *första stycket 1* gäller 6 § inte vid sökning som sker i ett visst ärende eller en viss handling. Det handlar här om sökning i så begränsade informationsmängder att några egentliga integritetsrisker inte kan anses föreligga.

Av *första stycket 2* framgår att 6 § inte heller gäller vid sökning i uppgiftssamlingar som har skapats för att utreda vissa preciserade slag av brottslighet (t.ex. narkotikabrottslighet i viss region) eller vissa preciserade kriminella grupperingar (t.ex. ett visst kriminellt mc-gäng) och som enbart de som arbetar i undersökningen har åtkomst till och andra särskilt angivna tjänstemän (se kommentaren till andra stycket). Uppgifter som ingår i sådana uppgiftssamlingar kan inte alltid anses vara gemensamt tillgängliga (se kommentaren till 1 §). Om så inte är fallet, är bestämmelserna i 2 kap. överhuvudtaget inte tillämpliga på dem.

Av *andra stycket* framgår att 6 § inte heller gäller vid underrättelseverksamhet som rör den allra grövsta brottsligheten. Undantaget aktualiseras bl.a. vid underrättelseverksamhet som rör grovt narkotikabrott, grov narkotikasmuggling, terroristbrott, människohandel, brott mot rikets säkerhet och vissa andra typer av brott. Undantag görs också för behandling i samband med särskild övervakning av kriminella personer (jfr 2 § 2).

Undantagen gäller endast om underrättelseverksamheten eller övervakningen bedrivs av polispersonal som har detta som särskild uppgift. För polismän som inte är utpekade för sådana uppgifter gäller sökbegränsningen i 6 §.

I *tredje stycket* öppnas en möjlighet att, utan hinder av 6 §, göra mera omfattande sökningar även inom ramen för en förundersökning. För att en generell sökning ska vara tillåten i ett sådant fall krävs dock att det finns särskilda skäl. Med särskilda skäl avses för det första att det är fråga om ett allvarligt brott med mycket högt straffvärde, som mord, eller att det är fråga om seriebrott av allvarlig karaktär, t.ex. upprepade våldtäkter eller mordbränder. För det andra ska sökningen syfta till att spåra gärningsmannen, eller eventuella medgärningsmän. Avsikten är således att sökmöjligheten ska utnyttjas enbart under förundersökningens spaningskedje, innan det finns någon som är misstänkt för brottet. En sökning av detta slag ska endast få utföras av på förhand särskilt utpekade tjänstemän.

Med stöd av *fjärde stycket* kan t.ex. meddelas föreskrifter om att det ska framgå av en förteckning eller liknande vilka personer som har anförtrotts den utökade möjligheten att söka på de uppgifter som behandlas inom polisen.

### Utlämnande av uppgifter på medium för automatiserad behandling

8 § Endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall.

Paragrafen reglerar under vilka förutsättningar uppgifter får lämnas ut i elektronisk form, t.ex. i ett e-postmeddelande eller på diskett. Bestämmelsen har inte någon sekretessbrytande verkan. Skälen för bestämmelsen har redovisats i avsnitt 14.

Bestämmelsen innebär att en större mängd personuppgifter, t.ex. ett helt register eller delar av ett register, inte får lämnas ut på medium för automatiserad behandling såvida inte regeringen har meddelat föreskrifter om detta eller i ett enskilt fall beslutat att sådant utlämnande får ske. Däremot kan enstaka uppgifter lämnas ut. Uttrycket enstaka används här med en något annan innebörd än i vanligt språkbruk. När personuppgifter förekommer i en eller ett fåtal handlingar är bestämmelsen således inte avsedd att utgöra ett hinder mot att handlingarna lämnas ut genom t.ex. ett e-postmeddelande. Bestämmelsen är också avsedd att ge stöd för utlämnande av ett ärende eller delar av ett ärende där personuppgifter förekommer (jfr prop. 2006/07:46 s. 124).

### Direktåtkomst

9 § Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får i den brottsbekämpande verksamheten medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Paragrafen innehåller bestämmelser om direktåtkomst. Frågan om direktåtkomst har behandlats i avsnitt 12.3.5.

Den grundläggande innebörden av begreppet direktåtkomst är att någon har direkt tillgång till register, databaser eller andra samlingar av uppgifter som behandlas automatiserat och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i uppgiftssamlingen. I begreppet direktåtkomst ligger också att den som är ansvarig för uppgiftssamlingen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle tar del av. Om en enskild har direktåtkomst till samtliga

uppgifter i en myndighets register, kan den enskilde alltså själv välja vilka uppgifter han eller hon vill ta del av vid ett visst tillfälle, utan att myndigheten först fattar ett beslut om att just dessa uppgifter ska lämnas ut.

I *första stycket* anges att Rikspolisstyrelsen, polismyndigheterna, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket i den brottsbekämpande verksamheten får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. På motsvarande sätt som har angetts i kommentaren till 2 kap. 14 § ger bestämmelsen möjlighet att medge även Säkerhetspolisen direktåtkomst.

Bestämmelsen innebär inte att myndigheterna har en absolut rätt till direktåtkomst.

Såsom framgår av *andra stycket* ska regeringen, eller den myndighet som regeringen bestämmer, kunna meddela föreskrifter om bl.a. begränsningar i direktåtkomsten och om behörighet och säkerhet. På grundval av dessa föreskrifter får varje myndighet avgöra om den kan medge en annan myndighet direktåtkomst.

Det bör understrykas att en bestämmelse om direktåtkomst anger endast i vilken form uppgifter får lämnas ut. Möjligheten att lämna ut vissa uppgifter genom direktåtkomst kan vara begränsad genom att uppgifterna är skyddade av sekretess. Något utlämnande genom direktåtkomst får inte ske om utlämnandet förutsätter en sekretessprövning. I och med att Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheterna enligt 2 kap. 14 § åläggs en sekretessbrytande uppgiftsskyldighet i förhållande till varandra och andra brottsbekämpande myndigheter kan dock uppgifter som omfattas av den bestämmelsen utlämnas genom direktåtkomst.

**10 §** Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet, i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Direktåtkomsten får endast avse personuppgifter som har gjorts gemensamt tillgängliga.

Paragrafen reglerar möjligheten att ge utländska myndigheter direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet. För närvarande finns det inte några bindande åtaganden av det slag som avses i paragrafen, utöver regleringen av Schengens informationssystem, som dock faller utanför lagens tillämpningsområde. Såsom har framgått av avsnitt 4.4 pågår emellertid förhandlingar inom EU om internationella instrument med sådana åtaganden.

### Behandling av uppgifter i brottsanmälningar

**11 §** Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i polisens brottsbekämpande verksamhet. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får uppgifterna inte behandlas i polisens brottsbekämpande verksamhet efter det att det påstådda brottet har preskriberats.

Paragrafen, som behandlas i avsnitt 16.3, reglerar hur länge och för vilket ändamål uppgifter i en brottsanmälan får behandlas, i de fall där en anmälan inte har lett till en förundersökning eller annan motsvarande utredning. För anmälningar som resulterat i förundersökning eller annan utredning gäller i stället bestämmelserna i 12–15 §§.

Huvudregeln är att uppgifter i en avskriven brottsanmälan ska kunna behandlas fram till den tidpunkt när brottet preskriberas, eftersom förundersökning kan inledas om det kommer fram omständigheter som gör att brottet kan klaras upp. När brottet har preskriberats, får uppgifterna däremot inte behandlas längre i den brottsbekämpande verksamheten.

Från huvudregeln om att behandling får ske fram till dess att brottet har preskriberats görs dock undantag för uppgifter i sådana anmälningar som har avskrivits på den grunden att det inte förelåg något brott, exempelvis helt ogrundade anmälningar. Uppgifter i sådana anmälningar får, när beslut om avskrivning

har meddelats, över huvud taget inte behandlas i den brottsbekämpande verksamheten.

### Behandling av uppgifter i avslutade förundersökningar

12 § Om en förundersökning har lett till åtal eller annan domstolsprövning, får uppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år sedan domen, eller det beslut som meddelades med anledning av talan, vann laga kraft.

Om en förundersökning har lagts ned eller avslutats på annat sätt än genom åtal får uppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter åklagarens eller förundersökningsledarens beslut. Om det i samband med beslutet anges att brottet, trots nedläggningsbeslutet, kan komma att bli föremål för lagföring, får dock behandling ske även senare fram till dess att brottet har preskriberats.

Vad som sägs i första och andra styckena gäller även personuppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken.

Bakgrunden till paragrafen har redovisats i avsnitt 16.3.

Paragrafen reglerar möjligheten att behandla uppgifter i förundersökningar efter det att de har avslutats.

Ibland kan de personuppgifter som finns i en nedlagd förundersökning eller i en förundersökning som har lett till en frikännande dom vara av betydelse för annan brottsbekämpande verksamhet. Inhämtade vittnesuppgifter kan t.ex. ge vid handen att någon annan person har begått det brott som förundersökningen gällde eller något annat brott. Uppgifter som har framkommit under en sedermera nedlagd förundersökning kan också tyda på att den tidigare misstänkte har tagit del i brottslig verksamhet av helt annat slag. Utgångspunkten är att sådana uppgifter måste kunna behandlas.

Sådana personuppgifter i en förundersökning som har lett till domstolsprövning får enligt *första stycket* bli föremål för fortsatt behandling även under viss tid efter det att saken har avslutats.



Eftersom det kan vara fråga om betydande mängder information, har det av integritetshänsyn ansetts att tiden för fortsatt sådan behandling bör begränsas till fem år. Tiden räknas från det att domstolens dom eller slutliga beslut vann laga kraft.

En motsvarande regel om fortsatt behandling av uppgifter i en förundersökning som inte har lett till domstolsprövning finns i *andra stycket*. Även i de fallen är huvudregeln att tiden för fortsatt behandling är fem år. I dessa fall räknas tiden från det att förundersökningen avslutades. Det finns emellertid ett undantag från huvudregeln. Om åklagaren eller förundersökningsledaren vid nedläggningsbeslutet anger att brottet, trots nedläggningsbeslutet, kan komma att lagföras, får fortsatt behandling ske. Det krävs således ett aktivt beslut för att avsteg från huvudregeln ska vara möjligt. Eftersom avsteget beror på att förundersökningen ska kunna tas upp på nytt, ska initiativet komma från den som är behörig att besluta i den frågan, dvs. åklagaren eller annan förundersökningsledare. Om han eller hon gör bedömningen att det inte finns några förutsättningar för att brottet någonsin kommer att lagföras, t.ex. därför att gärningsmannen har avlidit eller att brottet har begåtts av någon som var under 15 år, kommer uppgifterna inte att kunna behandlas längre än vad som gäller för förundersökningar i allmänhet. Detta gäller oavsett vilket brott det är fråga om. I andra fall kan åklagaren göra bedömningen att förundersökningen kommer att tas upp på nytt om det inträffar någon ny omständighet. Den nya omständigheten kan t.ex. vara att det framkommer ny bevisning. Det är inte heller ovanligt att en förundersökning läggs ned därför att gärningsmannen befinner sig utomlands och inte förväntas återvända och åklagaren därför förutser att en rättegång aldrig kommer att kunna hållas. Skulle den misstänkte återkomma till landet, kommer saken i ett nytt läge och det finns då anledning att överväga om förundersökningen ska tas upp på nytt. Har den som är ansvarig för förundersökningen meddelat att brottet trots nedläggningsbeslutet kan bli föremål för lagföring får dock fortsatt behandling efter femårsfristens utgång inte pågå längre än till dess att brottet har preskriberats. Om ett nedläggningsbeslut meddelas mycket

snabbt kommer preskriptionstiden och femårsfristen att löpa parallellt. I många fall kan emellertid femårsfristen utgöra den yttersta gränsen för behandling även vid brott som har en längre preskriptionstid än fem år. Detta kan bero t.ex. på att brottet inte anmäldes omedelbart eller att förundersökningen drog ut på tiden. Efter fristens utgång får personuppgifterna inte vara tillgängliga för behandling i polisen brottsbekämpande verksamhet. Bestämmelserna hindrar dock inte att uppgifter från en förundersökning fram till fristens utgång inhämtas till annan brottsbekämpande verksamhet (t.ex. ett särskilt underrättelseprojekt), under förutsättning att de behövs där (jfr 2 kap. 5 §). I så fall får uppgifterna bli föremål för fortsatt behandling för sitt nya ändamål även sedan den ursprungliga fristen har gått ut. En sådan fortsatt behandling får dock bara ske i den utsträckning behandlingen behövs för det nya ändamålet. Vidare förutsätts att uppgifterna gallras enligt bestämmelserna i 16 §.

Bestämmelserna i paragrafen gäller – såsom framgår av *tredje stycket* – också uppgifter i andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken. Vad som avses med ”annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken” har berörts i kommentaren till 2 kap. 5 §.

**13 §** Trots bestämmelserna i 12 § får personuppgifter i en förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken behandlas i polisens brottsbekämpande verksamhet, om det behövs för att återuppta förundersökningen eller utredningen eller för en prövning enligt 58 eller 59 kap. rättegångsbalken. Om det finns särskilda skäl, får uppgifterna även behandlas, om det behövs för en utredning som avser brott, för vilket är föreskrivet fängelse i fyra år eller däröver, eller för en undersökning av brottslig verksamhet som innefattar sådant brott.

I paragrafen anges att uppgifter i en förundersökning eller annan utredning i några undantagsfall får behandlas efter det att tidsfristerna i 12 § har löpt ut. Frågan har behandlats i avsnitt 16.3.

Utgångspunkten i 12 § är att uppgifter i förundersökningar och andra liknande utredningar får behandlas under en viss tid

efter det att saken har avgjorts. När den tiden har löpt ut, får de över huvud taget inte vara tillgängliga i den brottsbekämpande verksamheten, om de inte behandlas för något nytt ändamål. Den nu aktuella paragrafen skapar en möjlighet för polisen att i vissa fall, trots förbudet mot fortsatt behandling i 12 §, kunna använda uppgifter som finns i sådana förundersökningar.

Bestämmelsen innehåller inledningsvis två viktiga undantag från huvudregeln i 12 §. Det ena undantaget är om förundersökningen ska tas upp på nytt och uppgifterna behövs för det ändamålet. Bestämmelsen i 12 § andra stycket andra meningen innebär en möjlighet att fortsätta att behandla förundersökningar fram till preskriptionstidpunkten, om man kan förutse ett behov av fortsatt behandling. Det kan emellertid finnas situationer där behovet av att återuppta förundersökningen inte har kunnat förutses. Som exempel kan nämnas att åklagarens ställningstagande har grundat sig på felaktiga uppgifter och det visar sig att den misstänkte faktiskt var straffmyndig vid brottet eller att det framkommer nya uppgifter som på annat sätt kullkastar den tidigare bedömningen. Av det skälet har undantag gjorts för de fall där förundersökningen ska återupptas. Vidare har undantag gjorts för de fall där frågan om prövning av extraordinära rättsmedel aktualiseras. Den frågan kan väckas av såväl den misstänkte själv som av målsäganden eller åklagaren. Det måste då finnas möjlighet att ta upp saken på nytt och att inom ramen för den utredning som görs i resningsfrågan behandla uppgifterna i förundersökningen.

Slutligen har det öppnats en möjlighet för polisen att trots bestämmelserna i 12 § kunna behandla uppgifter i brottsutredningar, om det finns särskilda skäl till det. Syftet med bestämmelsen är att polisen vid utredning av allvarliga brott, eller undersökning av allvarlig brottslighet, undantagsvis ska kunna använda uppgifter ur avslutade brottsutredningar, trots att utredningsmaterialet, enligt huvudregeln, inte längre får användas i den brottsbekämpande verksamheten.

Bestämmelsen förutsätter för det första att uppgifterna *behövs* för det nya ändamålet. Behovet ska kunna konkretiseras.

Polisen ska veta vilken förundersökning eller vilket slag av uppgifter som eftersöks och som bedöms vara nödvändig för undersökningen eller utredningen. Dessutom ska det föreligga särskilda skäl. Med särskilda skäl avses framför allt att det i det enskilda fallet är av stor vikt för en ny brottsutredning eller undersökning att ha tillgång till uppgifterna ur den aktuella förundersökningen. Så kan vara fallet om det är fråga om återfall i brott av en person som en längre tid har avtjänat fängelsestraff eller varit intagen för rättspsykiatrisk vård för ett grovt brott. Om personen i fråga har frigetts och sedan på nytt misstänks för det slag av brottslighet som han eller hon tidigare har dömts för, exempelvis mordbrand, kan uppgifter från tidigare brottsutredningar vara av stort värde i den nya brottsutredningen. Det är däremot inte tillåtet att använda uppgifterna för att söka efter spaningsuppslag. Detta skulle innebära ett kringgående av de föreslagna bestämmelserna om tidsbegränsning av tillgången till uppgifter i en förundersökning.

**14 §** Om en förundersökning mot en person har lagts ned på grund av bristande bevisning, om åtal har lagts ned eller om frikännande dom, som har vunnit laga kraft, har meddelats, får en uppgift om att personen är misstänkt för brott inte längre vara sökbar, om inte förundersökningsledaren har beslutat att återuppta förundersökningen eller fråga är om prövning enligt 58 eller 59 kap. rättegångsbalken.

Paragrafen innehåller en bestämmelse om behandling av personuppgifter som rör brottsmisstankar efter det att en förundersökning har lagts ned på grund av bristande bevisning, ett åtal har lagts ned eller en åtalad person har frikänts genom en lagakraftvunnen dom. Bestämmelsen, som har motiverats i avsnitt 16.3, omfattar all behandling enligt lagen.

Enligt bestämmelsen får en uppgift om att en person är misstänkt för brott som regel inte vara sökbar efter det att förundersökningen mot personen har lagts ned på grund av bristande bevisning. Om förundersökningen har lett till åtal, men detta har

lagts ned eller lett till en frikännande dom, får den åtalade personen inte längre vara sökbar såsom misstänkt för brottet.

För de fall där ett åtal har lagts ned eller en person har frikänts genom en dom som har vunnit laga kraft gäller bestämmelsen oberoende av grunden för att åtalet har lagts ned eller att personen har frikänts. När en förundersökning har lagts ned, gäller dock bestämmelsen endast för de fall där nedläggningsbeslutet har grundats på att bevisningen inte är tillräcklig.

Bestämmelsen ska givetvis inte tolkas så att alla handlingar där det förekommer uppgifter om att en viss person har pekats ut eller hörts som misstänkt måste förstöras. Däremot ska det inte längre vara möjligt att vid sökning i elektroniskt lagrat material återfinna den utpekade personen om man söker efter misstänkta personer.

Bestämmelsen hindrar inte heller fortsatt behandling av andra personuppgifter rörande den tidigare misstänkta personen än själva brottsmisstanken. Om förundersökningen om brottet fortsätter, är det givetvis också tillåtet att behandla misstankar mot andra personer. Det är även tillåtet att – endera inom ramen för förundersökningen eller senare – behandla uppgifter om andra icke misstänkta personer, t.ex. uppgifter om målsägande och vittnen (med den begränsning som följer av 12 §).

### **Användning av arkiverade uppgifter m.m.**

15 § Bestämmelserna i 11–14 §§ hindrar inte att personuppgifter i brottsanmälningar, förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken arkiveras och gallras enligt bestämmelserna i arkivlagen (1990:782). För användningen av arkiverade uppgifter i polisens brottsbekämpande verksamhet gäller dock de begränsningar som anges i 11–14 §§.

I paragrafen klargörs att bestämmelserna i 11–14 §§ – som på olika sätt begränsar möjligheten att behandla uppgifter i brottsutredningar, förundersökningar och andra utredningar – inte hindrar att uppgifterna arkiveras och gallras. Bestämmelsen be-

hövs, eftersom definitionen av *behandling* inrymmer arkivering och gallring (avsnitt 16.3).

I paragrafen klargörs vidare att arkiverade uppgifter får behandlas endast under de förutsättningar som anges i 11–14 §§. Om t.ex. tidsfristerna i 12 § har löpt ut, får uppgifterna således behandlas endast om något av undantagen i 13 § är tillämpligt.

## Gallring

**16 §** Personuppgifter som har gjorts gemensamt tillgängliga ska gallras enligt bestämmelserna i andra-sjätte styckena.

Uppgifter som kan antas ha samband med sådan brottslig verksamhet som anges i 2 § första stycket 1 ska gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om den person som uppgiften avser inte är eller varit misstänkt, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats i samband med sådan övervakning som avses i 2 § första stycket 2 ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende den övervakade personen gjordes. Om en uppgift inte avser den övervakade personen, ska uppgiften gallras senast tre år efter det att den behandlades automatiserat första gången.

Uppgifter som har behandlats med stöd av 2 § första stycket 4 ska gallras senast ett år efter det att ärendet i vilket uppgifterna behandlades avslutades.

Uppgifter som har behandlats med stöd av 2 § första stycket 5 ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Den tid under vilken en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i andra och tredje styckena.

Paragrafen innehåller bestämmelser som, tillsammans med 17 och 18 §§, reglerar gallring av gemensamt tillgängliga uppgifter. Vid gallring av gemensamt tillgängliga uppgifter ska alltså 16–18 §§ tillämpas i stället för bestämmelserna i 2 kap. 11 §. Bak-

grunden till bestämmelserna har behandlats närmare i avsnitt 16.2.

I kommentaren till 2 kap. 11 § har berörts vad som avses med gallring. Som har konstaterats där behöver gallring av elektroniskt lagrad information inte innebära att själva informationen förstörs. Gallring kan också ske genom att den elektroniskt lagrade informationen överförs till en pappersutskrift och sedan raderas från ADB-mediet. Också överföring till andra databärare är att anse som gallring, om överföringen innebär informationsförlust, förlust av möjliga informationssammanställningar, förlust av sökmöjligheter eller förlust av möjligheter att fastställa informationens autenticitet. En sådan överföring bör dock, för att anses som gallring, vara i princip oåterkallelig. Enbart det förhållandet att informationen på grund av författning eller myndighets beslut inte längre får behandlas (jfr 11–15 §§) utgör därför inte gallring.

Det gäller olika gallringsfrister beroende på vilket slag av uppgifter det är fråga om.

Personuppgifter som kan antas ha samband med brottslig verksamhet (2 § första stycket 1) ska – såsom framgår av *andra stycket* – gallras inom en treårsfrist. Denna treårsfrist ska, om uppgiften avser en person som är eller varit misstänkt för den brottsliga verksamheten, räknas från utgången av det kalenderår då den senaste registreringen avseende honom eller henne gjordes. Om ytterligare uppgifter om personen samlas in – vare sig de har samband med den aktuella brottsliga verksamheten eller samlas in av annat skäl – förlängs alltså gallringsfristen. Om uppgiften i stället avser en person som varken är eller har varit misstänkt för den brottsliga verksamheten, ska treårsfristen alltid löpa från det att uppgiften behandlades automatiserat första gången. Ytterligare registreringar avseende den personen medför inte att gallringsfristen förlängs. Skulle uppgiften komma att behandlas för något nytt ändamål – t.ex. därför att den visar sig ha betydelse i ett annat underrättelseprojekt – börjar dock en ny gallringsfrist löpa. Med personuppgifter avses i båda fallen såväl direkta som indirekta personuppgifter, dvs. inte bara uppgifter

som direkt tar sikte på en person, t.ex. namn och utseende, utan också uppgifter om fordon, adresser m.m. som kan knytas till en person.

*Tredje stycket* innehåller bestämmelser om gallring av uppgifter som behandlas i samband med övervakning av brottsbelastade eller potentiellt farliga personer (2 § första stycket 2). Sådana uppgifter ska, om de avser den övervakade personen, gallras inom tio år från utgången av det kalenderår då den senaste registreringen avseende honom eller henne gjordes. Avser uppgifterna någon annan person, t.ex. en bekant till den övervakade, ska de i stället gallras inom tre år från det att de behandlades automatiserat första gången. Om det – innan gallring har skett – uppkommer behov av uppgifterna i något annat brottsbekämpande projekt, t.ex. underrättelseverksamhet, får dock uppgifterna hämtas in till den verksamheten. I så fall gäller en ny, yttersta gallringsfrist.

Som framgår av *sjätte stycket* ska den tid som en person avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning inte räknas med vid beräkningen av gallringsfristerna i andra och tredje styckena. Bestämmelserna tar endast sikte på misstänkta eller övervakade personer.

I *fjärde stycket* anges att uppgifter som har behandlats med stöd av 2 § första stycket 4, dvs. uppgifter som behövs för att fullgöra internationella åtaganden, ska gallras senast ett år efter att det ärende i vilket uppgifterna behandlades avslutades. Bestämmelsen ska tillämpas t.ex. när en svensk brottsbekämpande myndighet har lämnat rättslig hjälp åt en utländsk brottsbekämpande myndighet.

Enligt *femte stycket* ska uppgifter som har behandlats med stöd av 2 § första stycket 5, dvs. uppgifter som har rapporterats till polisens kommunikationscentraler, gallras inom ett år från det att uppgifterna behandlades automatiserat första gången. Också här gäller att uppgifterna kan hämtas till annan brottsbekämpande verksamhet. I så fall ska den längre gallringstid som gäller i den verksamheten tillämpas.



Gallringsfristerna i andra–femte styckena utgör maximitider. I den mån det redan vid en tidigare tidpunkt står klart att uppgifterna saknar betydelse från brottsbekämpningssynpunkt ska de gallras redan då. Detta följer av de allmänna bestämmelserna i 2 kap.

17 § Bestämmelserna i 16 § gäller inte

1. personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken, och

2. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

I fråga om behandling av sådana personuppgifter som anges i första stycket 1 gäller vad som sägs i 11–15 §§.

Av första stycket *punkten 1* framgår att personuppgifter i brottsanmälningar, förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken inte omfattas av gallringsbestämmelserna i 16 §. I stället gäller, som framgår av *andra stycket*, de begränsningar i möjligheten till behandling av uppgifterna som uppställs i 11–15 §§. Vad som avses med "annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken" har berörts i kommentaren till 2 kap. 5 §.

I vilken utsträckning brottsanmälningar, förundersökningar och de övriga utredningar som omfattas av paragrafen kan gallras får avgöras enligt bestämmelserna i arkivlagstiftningen.

Av första stycket *punkten 2* framgår att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål. En motsvarande bestämmelse, såvitt gäller kriminalunderrättelseregister, finns i 21 § andra stycket polisdatalagen.

18 § Vad som föreskrivs i 11–16 §§ hindrar inte att regeringen meddelar föreskrifter om att uppgifter i vissa särskilda fall får behandlas och bevaras under längre tid än vad som anges där.

Av paragrafen framgår att regeringen kan meddela föreskrifter om att uppgifter i vissa särskilda fall får behandlas och bevaras längre än vad som följer av 11–16 §§. Bemyndigandet ger regeringen möjlighet att föreskriva att speciella slag av uppgiftssamlingar ska gallras först efter längre tid. En sådan längre gallringsfrist kan t.ex. behövas för de uppgifter som i dag behandlas i det barnpornografiregister som Rikspolisstyrelsen för.

#### 4 kap. Register

##### Register med uppgifter om resultat av DNA-analyser

###### Ändamål m.m.

1 § Med DNA-analys förstås varje förfarande som kan användas för analys av deoxyribonukleinsyra.

Paragrafen innehåller en definition av begreppet DNA-analys. Den motsvarar definitionen i 3 § polisdatalagen.

2 § Rikspolisstyrelsen får föra register över uppgifter om resultat av DNA-analyser i enlighet med 3–13 §§ (DNA-register, utredningsregister och spårregister). Utöver för de ändamål som anges i 2 kap. får sådana register föras för att underlätta identifiering av avlidna personer.

Paragrafen reglerar, tillsammans med 2 kap. 9 §, uttömmande vilken behandling av DNA-profiler som är tillåten. Frågan har behandlats i avsnitt 17.2. Här regleras enbart behandlingen av DNA-profiler i register. Endast Rikspolisstyrelsen får föra sådana register – DNA-register, utredningsregister och spårregister – vilket överensstämmer med nuvarande reglering. Registren får föras dels för de ändamål som anges i 2 kap., dels för att under-

lätta identifiering av avlidna personer. Registrens närmare innehåll regleras i 3–6 §§.

### DNA-register

3 § Ett DNA-register får innehålla uppgifter om resultatet av DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som

1. genom lagakraftvunnen dom har dömts till annan påföljd än böter, eller
2. har godkänt ett strafföreläggande som avser villkorlig dom.

Paragrafen, som tillsammans med 4 § reglerar ett DNA-registers innehåll, överensstämmer med 23 § polisdatalagen.

4 § Registreringen av resultatet av en DNA-analys ska begränsas till uppgifter som ger information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får inte registreras.

Utöver vad som sägs i första stycket får DNA-registret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts och vem analysen avser.

Paragrafen, som tillsammans med 3 § reglerar ett DNA-registers innehåll, överensstämmer i sak med 24 § polisdatalagen.

### Utredningsregister

5 § Ett utredningsregister får innehålla uppgifter om resultatet av DNA-analyser som har gjorts med stöd av bestämmelserna i 28 kap. rättegångsbalken och som avser personer som är skäligen misstänkta för brott på vilket fängelse kan följa.

Vad som anges i 4 § gäller också vid registrering i utredningsregistret.

Paragrafen, som reglerar innehållet i ett utredningsregister, överensstämmer med 24 a § polisdatalagen.

## Spårregister

6 § Ett spårregister får innehålla uppgifter om resultatet av DNA-analyser som har gjorts under utredning av brott och som inte kan hänföras till en identifierbar person. Utöver uppgifter om analysresultat får spårregistret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts.

Paragrafen, som innehåller bestämmelser om vad ett spårregister får innehålla, överensstämmer med 25 § polisdatalagen.

7 § Uppgifter i ett spårregister får endast jämföras med analysresultat

1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller
3. som kan hänföras till en person som är skäligen misstänkt för brott.

Paragrafen innehåller bestämmelser som begränsar användningen av uppgifter i spårregister. Den överensstämmer med 26 § polisdatalagen.

## Gallring

8 § Uppgifter i DNA-registret ska gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter i utredningsregistret ska gallras senast när uppgifterna om den registrerade får föras in i DNA-registret eller när förundersökning eller åtal läggs ned, åtal ogillas, åtal bifalls men påföljden bestäms till enbart böter eller när den registrerade har godkänt ett strafföreläggande som avser enbart böter.

Uppgifter i spårregistret ska gallras senast trettio år efter registreringen.

Paragrafen, som innehåller bestämmelser om gallring av uppgifter i de olika typerna av register, överensstämmer med 27 § polisdatalagen.

## Särskilda bestämmelser om prov för DNA-analys

9 § Om det i samband med utredning av ett brott har tagits ett prov för DNA-analys, får provet inte användas för något annat ändamål än det för vilket det togs.

Paragrafen överensstämmer med 28 § polisdatalagen.

10 § Ett prov för DNA-analys som har tagits med stöd av bestämmelserna i 28 kap. 12–12 b §§ rättegångsbalken ska förstöras senast sex månader efter det att provet togs.

Om uppgifterna i utredningsregistret ska gallras vid en tidigare tidpunkt enligt 8 §, ska även det prov som avser den registrerade förstöras senast vid samma tidpunkt.

Om provet har tagits från någon som inte är skäligen misstänkt för brott, ska provet förstöras så snart målet eller ärendet slutligt har avgjorts.

Paragrafen överensstämmer med 27 a § polisdatalagen.

## Utlämnande av uppgifter på medium för automatiserad behandling

11 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för utlämnande av uppgifter om resultat av DNA-analyser.

Paragrafen hänvisar till bestämmelsen i 3 kap. 8 §. Innebörden av bestämmelsen behandlas i kommentaren till den paragrafen.

## Direktåtkomst

12 § Statens kriminaltekniska laboratorium, polismyndigheter, Ekobrottsmyndigheten och Åklagarmyndigheten får medges direktåtkomst till register med uppgifter om resultat av DNA-analyser.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Skälen för den valda lösningen har redovisats i avsnitt 12.3.5.

Enligt *första stycket* får Statens kriminaltekniska laboratorium, polismyndigheter, Åklagarmyndigheten och Ekobrottsmyndigheten medges direktåtkomst till register med uppgifter om DNA-analyser. På motsvarande sätt som har angetts i kommentaren till 2 kap. 14 § ger bestämmelsen möjlighet att medge även Säkerhetspolisen direktåtkomst.

Regleringen överensstämmer med vad som gäller i dag enligt 11 § polisdataförordningen (1999:81). I den bestämmelsen anges dock att annan myndighet än Statens kriminaltekniska laboratorium endast ska ha åtkomst till uppgifter om huruvida någon förekommer i ett register eller inte. Med stöd av paragrafens *andra stycke* kan regeringen meddela föreskrifter om motsvarande begränsning.

**13 §** Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till register med uppgifter om resultat av DNA-analyser i den utsträckning detta är nödvändigt för fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Åtkomsten ska begränsas till uppgift om huruvida någon förekommer i registret.

Paragrafen innebär att regeringen får meddela föreskrifter om att utländska myndigheter får medges direktåtkomst till register med uppgifter om DNA-analyser om det följer av internationella åtaganden att sådan åtkomst ska kunna beviljas. Frågan har behandlats i avsnitt 12.3.6. En viktig begränsning är att åtkomsten endast får avse uppgift om huruvida någon förekommer i registret eller inte. Som framgår av avsnitt 4.4. har det träffats en politisk överenskommelse om ett rambeslut som bygger på det s.k. Prümfördraget. Enligt detta ska utländsk polismyndighet kunna få tillgång till uppgifter om huruvida en person förekommer i ett svenskt DNA-register och vice versa.

## Fingeravtrycks- eller signalementsregister

### Ändamål

14 § Rikspolisstyrelsen får föra fingeravtrycks- eller signalementsregister i enlighet med 15–19 §§. Utöver för de ändamål som anges i 2 kap. får sådana register föras för att underlätta identifiering av okända personer.

I paragrafen anges för vilka ändamål fingeravtrycks- eller signalementsregister får föras samt att endast Rikspolisstyrelsen får föra sådana register. Förutom för de ändamål som anges i 2 kap. får fingeravtrycks- eller signalementsregister föras för att underlätta identifiering av okända personer. Fingeravtrycks- eller signalementsregister utgör ett stöd framför allt i den brottsutredande verksamheten men kan användas även för att underlätta arbetet med att förebygga och förhindra brott. Registrets närmare innehåll regleras i 15 §.

### Innehåll

15 § Ett fingeravtrycks- eller signalementsregister får endast innehålla uppgifter om den som är misstänkt eller dömd för brott eller som har fått lämna fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll. I ett sådant register får endast antecknas uppgifter om

1. fingeravtryck,
2. signalement,
3. identifieringsuppgifter,
4. ärendenummer, och
5. brottskoder.

Fingeravtrycks- eller signalementsregister får inte innehålla uppgifter som har lämnats av en person under femton år enligt 36 § första stycket 2 lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

Skälen för paragrafens bestämmelser har behandlats i avsnitt 17.3. Bestämmelserna motsvarar 30 § polisdatalagen. Ett tillägg

har dock gjorts i *första stycket* genom punkten 5 som innebär att uppgifter om brottskoder får antecknas i registret. Med brottskod avses den kod som används för att framställa brottsstatistik och som anger vilket brott som den aktuella personen är misstänkt eller dömd för.

Det *andra stycket* har oförändrat förts över från 30 § polisdatlagen.

## Gallring

**16 §** Uppgifter i ett fingeravtrycks- eller signalementsregister om en misstänkt person ska gallras senast

1. tio år efter registreringen, om denna skett på grund av misstanke om brott för vilket det inte föreskrivs strängare straff än fängelse i två år,

2. femton år efter registreringen, om denna skett på grund av misstanke om brott för vilket det föreskrivs strängare straff än fängelse i två år men inte strängare straff än fängelse i åtta år,

3. tjugofem år efter registreringen, om denna skett på grund av misstanke om brott för vilket det föreskrivs strängare straff än fängelse i åtta år,

4. tre månader efter det att åtal mot personen har lagts ned eller efter att personen genom lagakraftvunnen dom har frikänts, eller

5. tre månader efter det att en förundersökning mot personen har lagts ned.

Om en person blir misstänkt för ett nytt brott före utgången av den tid som anges i första stycket 1, 2 eller 3 får de uppgifter som finns registrerade om personen bevaras till dess att den senare registreringen avseende personen ska gallras enligt första stycket.

Uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll ska gallras när uppgifterna inte längre behövs för ändamålet med behandlingen eller enligt föreskrifter som regeringen meddelar.

Av *första stycket* 1–3 följer att gallringstidens längd har gjorts beroende av straffvärdet på det brott som personen misstänks för. Enligt bestämmelserna ska uppgifter om personer som misstänks för mindre allvarliga brott gallras tidigare än uppgifter om perso-



ner som misstänkts för grövre brott. Punkterna 4 och 5 uttrycker den viktiga principen att uppgifter om personer som inte längre är misstänkta ska gallras. Det är fråga om uppgifter om personer mot vilka en förundersökning har lagts ned eller ett åtal har lagts ned och uppgifter om personer som har frikänts. Enligt punkterna 4 och 5 ska uppgifterna gallras senast tre månader efter det att en förundersökning eller ett åtal lades ned eller en frikännande dom vann laga kraft.

I paragrafens *andra stycke* anges att om nya registreringar avseende en person tillkommer innan gallringstiden för den tidigare registreringen har löpt ut får tidigare uppgifter bevaras till dess att de senast registrerade uppgifterna ska gallras.

För uppgifter om personer som har lämnat fingeravtryck med stöd av lagen (1991:572) om särskild utlänningskontroll föreskrivs i *tredje stycket* att uppgifterna ska gallras när de inte längre behövs för ändamålet med behandlingen eller enligt föreskrifter som regeringen meddelar. Motsvarande gäller enligt 13 och 31 §§ polisdatalagen.

### Utlämnande av uppgifter på medium för automatiserad behandling

17 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för utlämnande av uppgifter i ett fingeravtrycks- eller signalementsregister.

Paragrafen hänvisar till bestämmelsen i 3 kap. 8 §. Innebörden av bestämmelsen behandlas i kommentaren till den paragrafen.

### Direktåtkomst

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket får i den brottsbekämpande verksamheten medges direktåtkomst till personuppgifter i ett fingeravtrycks- eller signalementsregister.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Enligt *första stycket* får övriga brottsbekämpande myndigheter medges direktåtkomst till fingeravtrycks- och signalementsregister. Frågan har behandlats i avsnitt 12.3.5. På motsvarande sätt som har angetts i kommentaren till 2 kap. 14 § ger bestämmelsen möjlighet att medge även Säkerhetspolisen direktåtkomst. Åklagare har inte bedömts ha behov av annat än enstaka uppgifter ur aktuella register och finns därför inte med i uppräkningslistan.

Med stöd av *andra stycket* kan regeringen bl.a. föreskriva att endast polispersonal vid Ekobrottsmyndigheten ska medges åtkomst till uppgifter ur registret. Vidare kan regeringen meddela föreskrifter om andra begränsningar i fråga om åtkomst och om behörighet och säkerhet.

**19 §** Regeringen meddelar föreskrifter om att utländsk myndighet får medges direktåtkomst till ett fingeravtrycks- eller signalementsregister i den utsträckning detta är nödvändigt fullgörandet av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt. Åtkomsten ska begränsas till uppgift om huruvida någon förekommer i registret.

Paragrafen innebär att regeringen får meddela föreskrifter om att utländska myndigheter får medges direktåtkomst till fingeravtrycks- och signalementsregister om det följer av internationella åtaganden att sådan åtkomst ska kunna beviljas. Frågan har behandlats i avsnitt 12.3.6. En viktig begränsning är att åtkomsten endast får avse uppgift om huruvida någon förekommer i registret eller inte. Som framgår av avsnitt 4.4 har det träffats en politisk överenskommelse om ett rambeslut som bygger på det s.k. Prümfördraget. Enligt detta ska polismyndigheterna i olika länder kunna få uppgift om huruvida en person förekommer i ett fingeravtrycksregister i ett annat land.

## Penningtvätsregister

### Ändamål m.m.

20 § Rikspolisstyrelsen får behandla uppgifter i penningtvätsregister om det behövs för att förebygga, förhindra eller upptäcka

1. brottslig verksamhet där penningtvätt är ett led för att dölja vinning av brott eller brottslig verksamhet, eller

2. brottslig verksamhet som innefattar brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m.

I ett sådant register får endast behandlas uppgifter som kan antas ha samband med sådan misstänkt brottslig verksamhet som avses i första stycket 1 och 2, uppgifter som har rapporterats till myndigheten med stöd av bestämmelser i lag eller annan författning och uppgifter som har lämnats av en utländsk myndighet som ansvarar för arbetet med att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses i första stycket 1 och 2 i det landet.

Enligt paragrafen får Rikspolisstyrelsen behandla uppgifter i särskilda penningtvätsregister inom ramen för arbetet med att bekämpa penningtvätt och finansiering av särskilt allvarlig brottslig verksamhet. I dag förs ett sådant register av Finanspolisen, som är en enhet vid Rikspolisstyrelsen. Frågan har behandlats i avsnitt 17.4.

Enligt *första stycket* får uppgifter behandlas i sådana register om det behövs för att förebygga, förhindra eller upptäcka vissa slag av brottslig verksamhet. För det första avses sådan brottslig verksamhet där penningtvätt utgör ett led för att dölja vinning av brott eller brottslig verksamhet. Med penningtvätt avses enkelt uttryckt åtgärder som syftar till att dölja illegalt åtkomna tillgångars ursprung. Den närmare innebörden av begreppet anges i 1 § lagen (1993:768) om åtgärder mot penningtvätt (penningtvättslagen). För det andra avses brottslig verksamhet som innefattar brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m. (terrorismfinansieringslagen). I 2 § nämnda lag finns en uppräkningslista av de brott som avses med uttrycket särskilt allvarlig brottslig verksamhet.

Enligt båda dessa lagar är fysiska och juridiska personer som driver finansiell verksamhet skyldiga att bl.a. granska misstänkta penningtransaktioner och lämna uppgifter om dem till Finanspolisen. Anmälningar av detta slag som ger underlag för misstanke om brott eller brottslig verksamhet får behandlas med stöd av reglerna i första stycket. Om det vid Finanspolisens egen verksamhet kommer fram uppgifter som tyder på sådan misstanke, får uppgifterna givetvis också behandlas.

Uppgifter som har rapporterats till Finanspolisen med stöd av penningtvättslagen eller terrorismfinansieringslagen, eller med stöd av annan författning, får enligt *andra stycket* behandlas i penningtvätsregister. Detta gäller även om anmälan då ännu inte ger tillräckligt underlag för misstanke om brott eller brottslig verksamhet. Vidare får sådana uppgifter behandlas som har rapporterats av utländska myndigheter med motsvarande uppgifter som Finanspolisen. Slutligen får även andra uppgifter som *kan antas ha samband* med misstänkt brottslig verksamhet som anges i paragrafens första stycke behandlas. För innebörden av uttrycken "brottslig verksamhet" och "kan antas ha samband med", se kommentaren till 3 kap. 2 § första stycket 1.

## Gallring

21 § Personuppgifter i ett penningtvätsregister ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Första stycket gäller inte om regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter om att uppgifter ska bevaras för historiska, statistiska eller vetenskapliga ändamål.

I *första stycket* anges att personuppgifter ska gallras senast fem år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Bestämmelsen knyter an till regler om bevarande av uppgifter som finns i lagen (1993:768) om åtgärder mot penningtvätt. Gallringsfristen om fem år är en maxi-

mitid. Om det redan tidigare står klart att uppgifterna saknar betydelse från brottsbekämpningssynpunkt ska de gallras redan då. Av *andra stycket* följer att uppgifter inte ska gallras om regeringen eller den myndighet som regeringen bestämmer har meddelat föreskrifter om att uppgifterna ska bevaras.

### **Utlämnande av uppgifter på medium för automatiserad behandling**

22 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling gäller även för uppgifter i ett penningtvättsregister.

Paragrafen hänvisar till bestämmelsen i 3 kap. 8 §. Innebörden av bestämmelsen behandlas i kommentaren till den paragrafen.

## **5 kap. Behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet**

### **Allmänna bestämmelser**

1 § Detta kapitel innehåller bestämmelser om behandling av personuppgifter hos Säkerhetspolisen i dess brottsbekämpande verksamhet.

Av paragrafen framgår att kapitlet innehåller särskilda bestämmelser för den personuppgiftsbehandling som sker hos Säkerhetspolisen. Att sådana bestämmelser finns framgår även av lagens inledande kapitel (1 kap. 4 § andra stycket). Frågor kring Säkerhetspolisens behandling av personuppgifter har behandlats i avsnitt 18.

Att de bestämmelser som gäller för behandlingen av personuppgifter hos Säkerhetspolisen har samlats i ett särskilt kapitel innebär inte att de i alla avseenden avviker från vad som gäller för den övriga polisen. I många avseenden ska således Säkerhetspoli-

sen tillämpa samma regler som gäller för polisverksamheten i övrigt. Detta framgår av hänvisningar i detta kapitel till vissa av lagens övriga bestämmelser.

Liksom lagen i övrigt gäller bestämmelserna i detta kapitel behandling av personuppgifter såsom begreppet definieras i 3 § personuppgiftslagen.

## Ändamål

2 § I Säkerhetspolisens brottsbekämpande verksamhet får, om inte annat följer av 3 eller 4 §, personuppgifter behandlas endast om det behövs för att

1. förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

a) brott mot rikets säkerhet,

b) terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott,

c) brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m., eller

d) tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv,

2. utreda eller beivra sådana brott som avses i 1, eller, efter särskilt beslut, annat brott,

3. fullgöra bevaknings- och säkerhetsarbete avseende personskydd,

4. fullgöra de uppgifter som följer av säkerhetsskyddslagen (1996:627),

5. fullgöra de förpliktelser som följer av internationella åtaganden, eller

6. lämna tekniskt biträde till Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten eller Tullverket.

Paragrafen anger, tillsammans med 3 och 4 §§, uttömmande de ändamål för vilka personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet. Skälen till den valda lösningen har redovisats i avsnitt 18.4.2. En grundläggande förutsättning för att behandling ska vara tillåten är att behandlingen behövs för den verksamhet som anges i paragrafen. Det innebär

att det ska finnas ett konkret behov av att genomföra behandlingen och att detta behov svarar mot något av de ändamål som anges i paragrafen.

I *punkten 1 a* nämns en av Säkerhetspolisens huvuduppgifter, att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som rör brott mot rikets säkerhet. Vidare räknas vissa andra typer av brott upp som Säkerhetspolisen har huvudansvar för, nämligen terroristbrott och brott som avser finansiering av terrorism (*punkterna 1 b och c*). Med brott mot rikets säkerhet brukar främst avses brott mot bestämmelserna i 18 och 19 kap. brottsbalken samt brott mot vissa bestämmelser i 13 kap. brottsbalken (bl.a. 13 kap. 1, 2, 3, 5 a och 5 b §§), beroende på syftet med brottet. Med terroristbrott avses framför allt brott mot lagen (2003:148) om straff för terroristbrott och lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall, m.m., den s.k. terrorismfinansieringslagen. Enligt föreskrifter som Rikspolisstyrelsen har meddelat ska Säkerhetspolisen vidare leda eller vara delaktig i förundersökningar avseende yttrandefrihetsbrott och tryckfrihetsbrott med rasistiskt eller främlingsfientligt motiv i de fall där Justitiekanslern är ensam åklagare (RPSFS 1999:10, FAP 403-3). Säkerhetspolisen får enligt *punkten 1 d* behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka sådana brott.

Under ändamålet förebygga, förhindra eller upptäcka brottslig verksamhet faller bl.a. Säkerhetspolisens kartläggning och kontroll av personer, företeelser och annat som kan belysa riskerna för brott av nu aktuellt slag. Insamling av uppgifter rörande verksamheter, sammanslutningar och annat som kan utvecklas till konkreta hot mot det svenska samhällsskicket eller mot enskilda personer i statsledningen är ett annat exempel. Vidare hör spaning i syfte att uppdaga sådan brottslig verksamhet som Säkerhetspolisen bekämpar hit. När uttrycket brottslig verksamhet används i lagen i övrigt syftar det på verksamhet av viss konkretion. Detsamma gäller i detta sammanhang, även om det här rör sig om helt andra typer av företeelser och verksam-

heter där anknytningen till urskiljbara brott ofta inte är lika tydlig. Säkerhetspolisens underrättelseverksamhet har således en bredare inriktning än motsvarande verksamhet hos den övriga polisen, eftersom den senare är tydligare inriktad på vissa brottstyper eller brottsliga företeelser. Även i Säkerhetspolisens underrättelseverksamhet krävs det emellertid att ändamålet med insamlingen eller bearbetningen av personuppgifter kan preciseras. Det kan t.ex. vara fråga om att en främmande stat misstänks bedriva underrättelseverksamhet av visst slag, utan att några konkreta brott kan urskiljas. Det kan också röra sig om företeelser i det svenska samhället som kan komma att utvecklas till brott enligt 18 eller 19 kap. brottsbalken.

Under det nu aktuella ändamålet faller också viss behandling av överskottsinformation med stöd av 27 kap. 23 a § rättegångsbalken, om syftet är att använda överskottsinformationen för att förhindra brott. Övrig användning av överskottsinformation faller, på samma sätt som för polisen i övrigt, under punkten 2.

*Punkten 2* behandlar utredning och beivrande av brott som ligger inom Säkerhetspolisens primära verksamhetsområde, dvs. sådana brott som anges i punkten 1. Vidare omfattas utredning och beivrande av brott i de fall där Säkerhetspolisen har hand om eller är delaktig i utredningen efter särskilt beslut. Vad som avses med uttrycket ”utreda och beivra brott” utvecklas närmare i kommentaren till 2 kap. 5 §. Som framhållits där ska det vara fråga om konkreta brott. Under denna punkt faller bl.a. det biträde Säkerhetspolisen ger åklagare i förundersökningar inkluderande hanteringen av hemliga tvångsmedel. Även spaning under förundersökning hör hit, liksom användning av överskottsinformation för att utreda brott.

Det ändamål som anges i *punkten 3* täcker den personuppgiftsbehandling som behövs för att Säkerhetspolisen ska kunna fullgöra sina uppgifter att skydda bl.a. den centrala statsledningen. Det innefattar exempelvis behandling av uppgifter rörande den skyddade personen själv, personer i hans eller hennes närmaste krets och andra personer som han eller hon kommer i beröring med samt uppgifter rörande personer som kan



utgöra hot mot den skyddade personen. Det är dock enbart uppgifter som behövs för att skyddsuppgiften ska kunna fullgöras som får behandlas. Punkten täcker dessutom behandlingen av personuppgifter för själva bevaknings- och säkerhetsarbetet, exempelvis uppgifter om vem som fullgör bevakningsuppgiften vid ett visst tillfälle.

Eftersom personskydd ytterst syftar till att förebygga brott mot den skyddade personen, kan personuppgiftsbehandling för detta syfte till viss del falla under punkten 1. Säkerhetspolisens uppgift att förebygga brott omfattar emellertid bara vissa typer av brott. Dessutom är långt ifrån alla brott mot person straffbara på planeringsstadiet. Punkten 3 ger tillsammans med punkten 1 stöd för den personuppgiftsbehandling som behövs för Säkerhetspolisens personskydd.

Säkerhetspolisens personuppgiftsbehandling för att fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627) täcks av *punkten 4*. I dessa uppgifter ingår bl.a. registerkontroll och utlämnande av uppgifter på grund av sådan kontroll.

I *punkten 5* regleras den personuppgiftsbehandling som krävs för att Säkerhetspolisen ska kunna fullgöra internationella åtaganden. Till dessa hör bl.a. att skydda vissa företrädare för utländska stater som besöker Sverige, bl.a. statsöverhuvuden och regeringsföreträdare. I den mån skyddet av dessa inte faller in under punkten 3, t.ex. därför att skyddet i huvudsak fullgörs av utländsk säkerhetspersonal, regleras det i denna punkt.

Säkerhetspolisen lämnar, i likhet med den öppna polisen, i viss utsträckning rättslig hjälp i brottsutredningar. Det kan exempelvis gälla hjälp med att hålla förhör med en viss person eller att verkställa en tvångsåtgärd. Denna punkt omfattar även den behandling av personuppgifter som behövs i sådana sammanhang.

Under denna punkt faller också Säkerhetspolisens regelbundna informations- och erfarenhetsutbyte med motsvarande myndigheter i andra länder, i den mån detta utbyte grundar sig på ett internationellt åtagande. Om informationsutbytet äger rum enbart i svenskt intresse faller det normalt under någon av

de tidigare punkterna. Däremot hör sådant informationsutbyte som enbart gagnar den utländska myndigheten, t.ex. uppgift om brott i en annan stat, hemma under denna punkt.

*Punkten 6* tar sikte på Säkerhetspolisens personuppgiftsbehandling när myndigheten lämnar tekniskt biträde till andra brottsbekämpande myndigheter. Sådant biträde kan t.ex. bestå i hjälp med användning av särskild spaningsutrustning. Den vanligaste formen av biträde är dock vid verkställighet av beslut om hemliga tvångsmedel, t.ex. beslut om hemlig teleavlyssning eller hemlig teleövervakning. Punkten täcker dels den behandling av personuppgifter som krävs för att Säkerhetspolisen ska kunna vidarebefordra beslut av domstol eller åklagare i frågor angående dessa tvångsmedel till vederbörande operatör, dels den behandling i form av lagring som sker hos Säkerhetspolisen när operatörerna överför uppgifter dit i enlighet med beslutet. Vidare täcks Säkerhetspolisens biträde vid verkställighet av andra hemliga tvångsmedel, i den mån sådant biträde kräver personuppgiftsbehandling. Så kan t.ex. vara fallet om biträdet rör hemlig kameraövervakning och Säkerhetspolisen tar hand om det upptagna bildmaterialet.

**3 §** Om personuppgifter behandlas enligt 2 §, får de även behandlas när det är nödvändigt för att tillhandahålla information som behövs i

1. brottsbekämpande verksamhet hos Rikspolisstyrelsen, polismyndigheter, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket,

2. Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om det finns särskilda skäl att tillhandahålla informationen, eller

3. brottsbekämpande verksamhet hos utländsk myndighet eller mellanfolklig organisation.

Personuppgifter som behandlas enligt 2 § får även behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning uppgiftsskyldighet följer av lag eller förordning, andra.

Regeringen meddelar föreskrifter om att personuppgifter som behandlas enligt 2 § och som avser efterlysta personer och avlägs-

nanden ur landet får behandlas för att tillhandahålla information till vissa särskilt angivna myndigheter.

Paragrafen reglerar de sekundära ändamål för vilka Säkerhetspolisen får behandla personuppgifter. Skälen för den valda regleringen har redovisats i 18.4.3. Behandlingen enligt denna paragraf förutsätter att uppgifterna redan är föremål för behandling enligt 2 §. Det är således inte tillåtet att samla in personuppgifter enbart i syfte att behandla dem med stöd av denna paragraf.

Det förhållandet att uppgifterna får behandlas påverkar inte heller de bestämmelser som gäller om sekretess. Bestämmelserna i sekretesslagen om sekretess mellan myndigheter och inom verksamhetsgrenar av samma myndighet ska därför beaktas på vanligt sätt i den utsträckning det inte finns särskilda sekretessbrytande regler (se 5 § 6).

Paragrafen motsvarar i stora delar den reglering som har föreslagits för polisen i övrigt (2 kap. 6 §). Det finns dock några viktiga skillnader. En sådan är att Säkerhetspolisen inte får behandla uppgifter för att lämna information till den övriga polisen i syfte att denna ska användas för annat ändamål än brottsbekämpning. Däremot öppnas möjlighet till informationsutbyte med Försvarsmaktens underrättelseverksamhet, vilket inte har någon motsvarighet i polisverksamheten i övrigt. Ytterligare en skillnad är att uppgifter inte får lämnas till konkursförvaltare.

*Första stycket* reglerar Säkerhetspolisens möjlighet att behandla uppgifter för att kunna lämna dem till en annan brottsbekämpande myndighet eller till Försvarsmaktens underrättelseverksamhet. Enligt *punkten 1* får Säkerhetspolisen, vars brottsbekämpning rör ett relativt avgränsat område, utföra den behandling som krävs för att vidarebefordra bl.a. uppgifter om brott eller brottslig verksamhet som upptäcks i den brottsbekämpande verksamheten och som Säkerhetspolisen saknar behörighet att handlägga. Som exempel kan nämnas att det vid hemlig teleavlyssning visar sig att någon av de avlyssnade personerna planerar att begå ett rån eller att det kommer fram uppgifter om

en leverans av narkotika. Sådana uppgifter måste kunna bli föremål för den behandling som krävs för att Säkerhetspolisens ska kunna lämna över dem till den enhet inom polisen, eller en annan brottsbekämpande myndighet (Tullverket i exemplet med narkotikan om det rör sig om smuggling) som har till uppgift att ingripa mot brottet. Säkerhetspolisen kan också ha behov av att till en annan enhet inom polisen lämna sådana uppgifter som har samband med personskyddet, t.ex. uppgifter om planerade eller begångna brott som inte är av den arten att de utreds av Säkerhetspolisen.

Enligt *punkten 2* får Säkerhetspolisen även behandla uppgifter för att kunna lämna dem till Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Möjligheterna till sådan behandling begränsas genom kravet på att det ska finnas särskilda skäl att tillhandahålla informationen. Som exempel på särskilda skäl kan nämnas att det under en förundersökning som Säkerhetspolisen genomför kommer fram information om en försvarsanställd, eller någon anhörig till honom eller henne, som inte föranleder misstanke om brott men som kan ha stor betydelse för Försvarmakten. Ett annat exempel kan vara att Säkerhetspolisen i sin brottsbekämpning noterar svagheter eller brister i skyddet för Försvarmaktens anläggningar.

I *punkten 3* regleras möjligheten att lämna uppgifter till en utländsk myndighet eller mellanfolklig organisation. Enligt denna punkt kan information, som ändå behandlas enligt 2 §, också behandlas för att tillhandahålla information som är nödvändig för den brottsbekämpande verksamheten vid en utländsk myndighet eller en mellanfolklig organisation. Exempel på uppgifter som kan lämnas ut med stöd av denna punkt är uppgifter om brott, brottsmisstankar och misstänkt brottslig verksamhet men också uppgifter som härrör från personskyddet, t.ex. aktuella hotbilder, om det behövs för att den utländska myndigheten ska kunna skydda en svensk företrädare för den centrala statsledningen som gör ett officiellt besök i det andra landet. I 2 kap. 13 §, som enligt 5 § 6 ska tillämpas även av Säkerhetspolisen, finns en regel om utlämnande av uppgifter till utländsk myndig-

het eller mellanfolklig organisation. Denna regel är sekretessbrytande.

*Andra och tredje styckena* motsvarar 2 kap. 6 § andra och tredje styckena. I fråga om innebörden hänvisas till kommentaren till den paragrafen.

4 § Bestämmelserna i 2 kap. 7 § om diarieföring av personuppgifter m.m. gäller även för behandling av personuppgifter hos Säkerhetspolisen.

I 2 kap. 7 § finns särskilda bestämmelser som innebär att personuppgifter alltid får behandlas om behandlingen är nödvändig för diarieföring eller, om uppgifterna har lämnats i en anmälan eller liknande, för handläggningen. I förevarande paragraf anges att dessa bestämmelser ska gälla även för Säkerhetspolisen. För en närmare beskrivning av innebörden av bestämmelserna hänvisas till kommentaren till 2 kap. 7 §.

### **Tillämpliga bestämmelser i 2 kap.**

5 § Följande bestämmelser i 2 kap. ska tillämpas vid behandling av personuppgifter hos Säkerhetspolisen:

1. 1 och 2 §§ om förhållandet till personuppgiftslagen,
2. 3 § om tillsyn,
3. 8 § om behandling av känsliga personuppgifter,
4. 9 § behandling av uppgifter om resultatet av DNA-analyser,
5. 10 § om tillgången till uppgifter, och
6. 12, 13 och 17 §§ om utlämnande av uppgifter.

I paragrafen anges vilka av bestämmelserna i 2 kap. som, utöver bestämmelsen om behandling för diarieföring m.m. (2 kap. 7 §), ska tillämpas på den behandling som utförs av Säkerhetspolisen. Frågan har behandlats i avsnitt 18.5.

Av *punkten 1* följer att lagen ska tillämpas i stället för personuppgiftslagen (1998:204), om inte annat framgår av 2 kap. 2 §. I sistnämnda paragraf räknas upp vilka regler i personuppgiftsla-

gen som ska tillämpas. Urvalet av bestämmelser beskrivs närmare i kommentaren till 2 kap. 2 §.

Genom hänvisningen i *punkten 2* till 2 kap. 3 § tydliggörs att vad som där sägs om tillsyn gäller även för Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten.

Hänvisningen i *punkten 3* till 2 kap. 8 § innebär att Säkerhetspolisen ska tillämpa samma grundläggande regler vid behandling av känsliga personuppgifter som polisen i övrigt.

Av *punkten 4* följer att även Säkerhetspolisen får behandla uppgifter om resultatet av DNA-analyser endast inom ramen för en förundersökning. Med uppgifter om resultatet av DNA-analyser avses som framgår av kommentaren till 2 kap. 9 § den DNA-profil som blir resultatet av en analys. I praktiken är det endast Statens kriminaltekniska laboratorium som har behov av att behandla DNA-profiler, vilket myndigheten gör när de inom ramen för en förundersökning biträder Säkerhetspolisen med att utföra DNA-analyser.

Vidare ska enligt *punkten 5* bestämmelsen i 2 kap. 10 § tillämpas på Säkerhetspolisen. Den innebär att varje persons tillgång till personuppgifter ska begränsas till vad han eller hon behöver för att fullgöra sin arbetsuppgifter. Som framgår av kommentaren till 2 kap. 10 § avses inte bara tillgång genom direktåtkomst utan även annan muntlig eller skriftlig tillgång till uppgifterna.

Slutligen ska enligt *punkten 6* bestämmelserna i 2 kap. 12 § (om utlämnande av statistikuppgifter), 13 § (om utlämnande av uppgifter till utländska myndigheter och mellanfolkliga organisationer) och 17 § (om viss föreskriftsrätt för regeringen) tillämpas också på Säkerhetspolisens brottsbekämpande verksamhet.

## Personuppgiftsansvar

**6 §** Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller som det åligger myndigheten att utföra.

Paragrafen innehåller en bestämmelse om personuppgiftsansvar. Bestämmelsen innebär att Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför eller är skyldig att utföra. En motsvarande bestämmelse för polisens övriga brottsbekämpande verksamhet finns i 2 kap. 4 §.

## Gallring

7 § Personuppgifter som behandlas automatiserat i ett ärende ska gallras senast ett år efter det att ärendet avslutades. Personuppgifter som inte kan hänföras till ett ärende ska gallras senast ett år efter det att de behandlades automatiserat första gången.

Bestämmelserna i första stycket gäller inte

1. uppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken,
2. uppgifter som har gjorts gemensamt tillgängliga, och
3. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

Paragrafen innehåller gallringsregler för sådana personuppgifter som helt eller delvis behandlas automatiskt och som inte har gjorts gemensamt tillgängliga. För gemensamt tillgängliga uppgifter gäller andra gallringsregler (se 16 och 17 §§). Skälen för den valda lösningen har redovisats i avsnitt 18.6.5.

Enligt *första stycket* ska personuppgifter som behandlas automatiserat i ett ärende gallras senast ett år efter det att ärendet avslutades, medan uppgifter som inte hör till något ärende ska gallras ett år efter det att de behandlades automatiserat första gången. En motsvarande bestämmelse för polisens övriga brottsbekämpande verksamhet finns i 2 kap. 11 §. Vad som avses med ett ärende och med gallring utvecklas närmare i kommentaren till den paragrafen.

I *andra stycket* görs undantag för uppgifter i brottsanmälningar, förundersökningar och andra utredningar som handläggs enligt bestämmelser i 23 kap. rättegångsbalken. Detta motsvarar

regleringen i 2 kap. 11 §. Bestämmelsen ska inte heller tillämpas om personuppgifterna har gjorts gemensamt tillgängliga; i så fall ska i stället de särskilda gallringsbestämmelserna i 16 och 17 §§ tillämpas. Det tredje undantaget gäller om regeringen, eller den myndighet som regeringen bestämmer, meddelat föreskrifter om att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

### Gemensamt tillgängliga uppgifter

**8 §** Om det behövs för de ändamål som anges i 2 §, får personuppgifter göras gemensamt tillgängliga i Säkerhetspolisens verksamhet. Uppgifter om resultat av DNA-analyser får dock inte göras gemensamt tillgängliga. Uppgifter som endast ett fåtal bestämda personer hos Säkerhetspolisen har rätt att ta del av anses inte som gemensamt tillgängliga.

Bestämmelserna i 9–17 §§ gäller för behandling av personuppgifter som görs eller har gjorts gemensamt tillgängliga.

Paragrafen innehåller en bestämmelse om vilka uppgifter som får göras gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet. Frågan har berörts i avsnitt 18.6.1. Vad som avses med gemensamt tillgängliga uppgifter har behandlats ingående i avsnitt 9 och i kommentaren till 3 kap. 1 §.

I *första stycket* fastslås att personuppgifter får göras gemensamt tillgängliga om det behövs för de primära ändamål för vilka Säkerhetspolisen får behandla uppgifter. Uppgifter om resultat av DNA-analyser – varmed avses DNA-profiler (se kommentaren till 2 kap. 9 §) – får dock aldrig göras gemensamt tillgängliga.

Av *andra stycket* framgår att bestämmelserna i 9–17 §§ ska tillämpas i de fall där personuppgifter har gjorts gemensamt tillgängliga. Dessa strängare bestämmelser innebär bl.a. att andra gallringsfrister gäller, att uppgifterna ska förses med särskilda upplysningar och att det finns begränsningar i fråga om vilka sökningar som får göras.



## Särskilda upplysningar

9 § Vid behandling enligt 8 § ska personuppgifterna föras med en särskild upplysning om det närmare ändamålet med behandlingen. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

I paragrafen, som delvis motsvarar 3 kap. 3 §, ställs det krav på att uppgifter som görs gemensamt tillgängliga ska föras med särskild upplysning om det närmare ändamålet med behandlingen. Frågan har behandlats i avsnitt 18.6.3. Bestämmelsen innebär till att börja med att det ska framgå med stöd av vilket ändamål i 2 § som uppgiften i fråga behandlas. Om ändamålet är att förebygga eller förhindra brottslig verksamhet, ska det dessutom t.ex. framgå vilken typ av brottslig verksamhet det är fråga om.

Om uppgifter samlas in för ett visst ändamål men senare kommer att användas för ett annat ändamål, måste en upplysning om det nya ändamålet lämnas vid den senare behandlingen. Så blir t.ex. fallet om uppgifter, som har framkommit i ett under rättelseprojekt, senare utnyttjas i personskyddet eller om uppgifter från en förundersökning tillförs ett underrättelseprojekt.

I de fall där det tydligt framgår av omständigheterna för vilket ändamål uppgiften behandlas krävs dock inte någon särskild upplysning. Uppgifter i en förundersökning eller annan utredning enligt 23 kap. rättegångsbalken behöver därför normalt inte föras med någon särskild upplysning.

10 § Om uppgifter, som behandlas enligt 8 §, direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet, ska de föras med en särskild upplysning om att personen inte är misstänkt. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

Uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska föras med upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Upplysning

behöver dock inte lämnas, om det på grund av särskilda omständigheter är onödigt. Upplysning behöver inte heller lämnas om

1. uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till, och
2. bearbetningen och analysen befinner sig i ett inledande skede.

Paragrafen innehåller bestämmelser om att uppgifter som görs gemensamt tillgängliga i Säkerhetspolisens verksamhet i vissa fall ska kompletteras med särskilda upplysningar. Skälen för detta har angetts i avsnitt 18.6.3. Bestämmelserna motsvarar i allt väsentligt vad som gäller för polisens övriga brottsbekämpande verksamhet enligt 3 kap. 4 §. Uttrycket ”uppgifter som direkt kan hänföras till en person” innebär att paragrafen bara är tillämplig på direkta personuppgifter.

Enligt *första stycket* ska sådana personuppgifter som avser personer som varken är misstänkta för brott eller kan antas ha samband med brottslig verksamhet förses med en tilläggsupplysning om att personen i fråga inte är misstänkt. Som framgår av kommentaren till 3 kap. 4 § inträder skyldigheten bara om det inte alls finns någon misstanke. Vidare görs undantag från upplysningsskyldigheten i de fall där det ändå av omständigheterna klart framgår att vederbörande inte är misstänkt. Det innebär t.ex. att det inte behövs någon tilläggsupplysning om en person enbart har hörts som målsägande eller vittne.

Av *andra stycket* följer att uppgifter om personer som kan antas ha samband med brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Motsvarande bestämmelse gäller för övriga polisen. För en närmare beskrivning av innebörden av bestämmelsen hänvisas till kommentaren till 3 kap. 4 § andra stycket.

Uppgift om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak behöver – på samma vis som enligt 3 kap. 4 § – inte lämnas om det på grund av särskilda omständigheter är onödigt. Vidare har undantag gjorts för uppgifter i analysdatabaser som enbart särskilt utpekade tjänstemän har tillgång till och där

analysen befinner sig i ett första, inledande skede. Detta undantag saknar motsvarighet i 3 kap. 4 §. Med inledande skede avses här den tid efter det att en uppgift har tillförts en analysdatabas och under vilken det inte är möjligt att bedöma om uppgiften har betydelse för analysarbetet eller kan avföras som ointressant. Undantaget innebär att personuppgifterna under detta skede, som ska vara en kortare tid, inte behöver kompletteras med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Om analysarbetet däremot leder vidare t.ex. till en fördjupad analys av vissa personers kontakter eller förehanden eller till en förundersökning, måste personuppgifterna så snart som möjligt kompletteras med särskilda upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

## Sökning

11 § Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv användas som sökbegrepp endast om det är absolut nödvändigt för de ändamål som anges i 2 §.

Första stycket hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

Paragrafen reglerar möjligheterna att använda känsliga personuppgifter som sökbegrepp vid sökning i gemensamt tillgängliga uppgifter. Skälen för den valda lösningen har redovisats i avsnitt 18.6.4. Om uppgifterna inte har gjorts gemensamt tillgängliga, gäller inte bestämmelsen.

I motsats till vad som gäller för polisen i övrigt får Säkerhetspolisen, enligt *första stycket*, i begränsad utsträckning använda känsliga personuppgifter vid sökningar. Så kan t.ex. uppgifter som rör politiska åsikter ibland vara av intresse, eftersom det ingår i Säkerhetspolisens uppgifter att kartlägga sådan politisk verksamhet som kan komma att hota vitala samhällsfunktioner. Vid underrättelseverksamhet eller utredning av terroristbrott

kan andra känsliga uppgifter vara väsentliga. Kravet på att det ska vara *absolut nödvändigt* från verksamhetssynpunkt att använda ett sådant sökbegrepp gör dock att utrymmet för sådana sökningar är starkt begränsat och att rutinmässiga sökningar på känsliga uppgifter över huvud taget inte är tillåtna.

I *andra stycket* görs klart att uppgifter som beskriver en persons utseende får användas som sökbegrepp.

12 § Vid sökning i gemensamt tillgängliga uppgifter får endast följande uppgifter tas fram:

1. identifieringsuppgifter,
2. uppgifter om grunden för registreringen, och
3. hänvisning till de ärenden där uppgifter om personen behandlas.

Paragrafen innehåller de övriga begränsningar som gäller för sökning i gemensamt tillgängliga uppgifter hos Säkerhetspolisen. Eftersom det kan vara fråga om en stor informationsmängd, har det inte ansetts rimligt att tillåta alla slags sökningar i denna. I likhet med vad som gäller för den övriga polisen får därför Säkerhetspolisen endast söka efter vissa typer av uppgifter. Regleringen har emellertid utformats på ett annat sätt, eftersom arbetsuppgifterna inte är desamma. Den nu aktuella bestämmelsen har också utformats för att motsvara de särskilda krav som gäller i Säkerhetspolisens verksamhet på att uppgifter inte sprids till fler personer än vad som är absolut nödvändigt. Skälen för den valda lösningen har redovisats i avsnitt 18.6.4.

Det är enligt paragrafen endast tre typer av uppgifter som får sökas, förutom de fall som anges i 13 § första stycket. Den första typen är enligt *punkten 1* uppgifter som är ägnade att identifiera en person som söks. Det kan vara fråga både om direkta personuppgifter, t.ex. ett personnummer eller annat identifikationsnummer, och indirekta personuppgifter, t.ex. uppgift om en viss bil, en adress, ett bolag eller något annat genom vilken man kan identifiera en enskild person.

Enligt *punkten 2* kan man också söka efter uppgifter som anger grunden för registreringen. Med detta avses uppgift om varför den aktuella personen är registrerad, t.ex. om det rör sig om en förundersökning eller om vederbörande är föremål för personskydd. Det bör i förekommande fall också kortfattat framgå vilken händelse eller företeelse som har föranlett registreringen.

Den tredje typen av uppgifter som enligt *punkten 3* får sökas är uppgifter som hänvisar till det eller de ärenden där uppgifter om personen behandlas. Det kan röra sig om diarienummer, aktbeteckning eller någon annan liknande typ av uppgifter.

**13 §** Bestämmelsen i 12 § gäller inte vid sökning

1. i en viss handling eller i ett visst ärende, eller
2. i en uppgiftssamling som har skapats för att bearbeta och analysera information och som enbart särskilt angivna tjänstemän har åtkomst till.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om och under vilka förutsättningar sökning får ske enligt första stycket.

Paragrafen, som behandlas i avsnitt 18.6.4, innehåller i *första stycket* två generella undantag från reglerna om vilka typer av uppgifter som får eftersökas bland uppgifter som är gemensamt tillgängliga. Den har i huvudsak sin motsvarighet i 3 kap. 7 §, som gäller för polisens övriga brottsbekämpande verksamhet. Det första undantaget innebär att sökbegränsningarna i 12 § inte gäller vid sökning i en viss handling eller inom ramen för ett visst ärende. Det rör sig i dessa fall om mera begränsade informationsmängder. Det andra undantaget gäller vid sökning i de särskilda analysdatabaser som förekommer hos Säkerhetspolisen och som enbart vissa utpekade tjänstemän har tillgång till.

Enligt *andra stycket* kan regeringen, eller den myndighet som regeringen bestämmer, meddela närmare föreskrifter angående sökning enligt första stycket.

## Utlämnande av uppgifter på medium för automatiserad behandling

14 § Bestämmelsen i 3 kap. 8 § om utlämnande av uppgifter på medium för automatiserad behandling ska tillämpas även vid utlämnande av uppgifter som behandlas hos Säkerhetspolisen.

Paragrafen reglerar förutsättningarna för att lämna ut uppgifter i elektronisk form, exempelvis via e-post eller på diskett eller CD-rom. Samma begränsningar gäller för Säkerhetspolisen som för polisens övriga brottsbekämpande verksamhet. I fråga om den närmare innebörden av bestämmelsen hänvisas till kommentaren till 3 kap. 8 §.

## Behandling av uppgifter i avslutade förundersökningar m.m.

15 § Bestämmelserna i 3 kap. 11–15 §§ om behandling av uppgifter i avslutade förundersökningar m.m. ska tillämpas även vid behandling av personuppgifter hos Säkerhetspolisen.

Enligt paragrafen ska Säkerhetspolisen tillämpa samma regler som polisen i övrigt vid behandlingen av uppgifter i brottsanmälningar, avslutade förundersökningar och andra utredningar enligt 23 kap. rättegångsbalken.

## Gallring

16 § Personuppgifter som har gjorts gemensamt tillgängliga ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Personuppgifter som behandlas i en sådan uppgiftssamling som avses i 10 § andra stycket 1 ska dock gallras senast tre år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes.

Säkerhetspolisen får besluta att personuppgifter får behandlas längre tid än vad som sägs i första och andra styckena, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas.

Om uppgifter bevaras med stöd av ett sådant beslut, ska de gallras, eller frågan om bevarande prövas på nytt, senast vid utgången av det tionde kalenderåret efter beslutet eller, om det är fråga om uppgifter som avses i andra stycket, senast vid utgången av det tredje kalenderåret efter beslutet.

Paragrafen innehåller bestämmelser som, tillsammans med 17 §, reglerar gallring av gemensamt tillgängliga uppgifter. I fråga om gallring av uppgifter som inte har gjorts gemensamt tillgängliga tillämpas 7 §. Vad som avses med gallring har redovisats närmare i kommentaren till 2 kap. 11 § och 3 kap. 16 §. Frågor om gallring vid Säkerhetspolisens personuppgiftsbehandling har behandlats i avsnitt 18.6.5.

Skilda gallringsfrister gäller för olika typer av uppgifter. Huvudregeln, som anges i *första stycket*, är att personuppgifter som har gjorts gemensamt tillgängliga inom Säkerhetspolisen ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen beträffande den aktuella personen gjordes. Detta motsvarar vad som för närvarande gäller för gallring av personuppgifter i SÄPO-registret.

Enligt *andra stycket* ska dock uppgifter i sådana särskilda analysdatabaser som avses i 10 § andra stycket 1 gallras senast tre år efter utgången av det kalenderår när den senaste registreringen avseende personen gjordes. Om nya uppgifter om personen samlas in, förlängs alltså gallringsfristen. Detta gäller oavsett om uppgifterna har samband med den först aktuella brottsliga verksamheten eller samlas in av annat skäl.

I *tredje stycket* öppnas en möjlighet för Säkerhetspolisen att genom ett särskilt beslut i det enskilda fallet förlänga gallringsfristen. Detta förutsätter att personuppgifterna fortfarande behövs för de ändamål för vilket de behandlas. Ett beslut av detta slag ska fattas innan gallringsfristen har löpt ut. Har Säkerhetspolisen meddelat ett beslut om fortsatt bevarande, ska uppgifterna som huvudregel gallras – eller frågan om bevarande prövas på nytt – senast vid utgången av det tionde året efter beslutet. Uppgifter som avses i andra stycket ska dock gallras – eller be-

slutet omprövas – senast vid utgången av det tredje året efter beslutet.

17 § Bestämmelserna i 16 § gäller inte

1. personuppgifter i en brottsanmälan, förundersökning eller annan utredning som handläggs enligt bestämmelser i 23 kap. rättegångsbalken, och

2. uppgifter som ska bevaras för historiska, statistiska eller vetenskapliga ändamål enligt föreskrifter som har meddelats av regeringen eller den myndighet som regeringen har bestämt.

I fråga om behandling av sådana personuppgifter som anges i första stycket 1 ska i stället 3 kap. 11–15 §§ tillämpas.

Bakgrunden till paragrafen har behandlats i avsnitt 18.6.5.

I *första stycket punkten 1* görs undantag från gallringsbestämmelserna i 16 § för personuppgifter i brottsanmälningar, förundersökningar och andra utredningar som handläggs enligt 23 kap. rättegångsbalken. I stället ska, som framgår av *andra stycket*, bestämmelserna i 3 kap. 11–15 §§ tillämpas, dvs. de bestämmelser som gäller även för polisens övriga brottsbekämpande verksamhet. Liksom för polisen i övrigt gäller också att uppgifter som har hämtats från en förundersökning för att behandlas för ett nytt ändamål ska gallras enligt de frister som gäller för det nya ändamålet. Uppgifter från en förundersökning kan t.ex. behöva behandlas även efter det att tidsfristerna i 3 kap. 11–15 §§ har löpt ut, om det krävs för att förebygga, förhindra eller upptäcka brottslig verksamhet. I så fall gäller gallringsfristerna i 16 §.

Enligt *punkten 2* ska gallringsbestämmelserna inte heller tillämpas om regeringen, eller den myndighet som regeringen bestämmer, har meddelat föreskrifter om att uppgifterna får bevaras för historiska, statistiska eller vetenskapliga ändamål. En motsvarande bestämmelse om möjlighet att meddela föreskrifter finns för polisens övriga brottsbekämpande verksamhet i 3 kap. 17 §.

I *andra stycket* erinras om att 3 kap. 11–15 §§ ska tillämpas i stället för första stycket 1.



## Övergångsbestämmelser

Övergångsbestämmelserna har behandlats ingående i avsnitt 23.2.

## 26.2 Förslaget till lag om polisens allmänna spaningsregister

Lagen innehåller en reglering av ett register som i stora delar motsvarar polisens nuvarande allmänna spaningsregister. Den allmänna motiveringen till att denna särlösning har valts finns i avsnitt 20.1. Lagen, som delvis har utformats efter mönster av lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister, reglerar uttömmande vad som gäller för det allmänna spaningsregistret.

### Allmänt spaningsregister

1 § Rikspolisstyrelsen får med hjälp av automatiserad behandling föra ett allmänt spaningsregister.

Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret. En myndighet som har direktåtkomst enligt denna lag ansvarar för att åtkomsten begränsas enligt 11 §.

Enligt paragrafens *första stycke* får Rikspolisstyrelsen föra ett allmänt spaningsregister. Registret, som ska vara nationellt, får föras med hjälp av automatiserad behandling. Lagen tillåter däremot inte att det förs lokala sådana spaningsregister. Vilken behandling av personuppgifter som är tillåten i övrigt i polisens brottsbekämpande verksamhet styrs framför allt av lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet. I *andra stycket* fastslås att Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av uppgifter i registret. Frågan har behandlats i avsnitt 20.2. På samma vis som i 2 kap. 4 § andra stycket lagen om behandling av personuppgif-

ter i polisens brottsbekämpande verksamhet fastslås också att myndigheter som har medgetts direktåtkomst till registret ansvarar för att åtkomsten begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

### Ändamål

2 § Det allmänna spaningsregistret ska ha till ändamål att underlätta tillgången till personuppgifter som behövs för spaning i polisens brottsbekämpande verksamhet.

I paragrafen anges ändamålet med registret, vilket är att underlätta tillgången till personuppgifter som behövs i spaning i polisens brottsbekämpande verksamhet. Frågan har behandlats i avsnitt 20.3.2.

Det är meningen att registret ska utgöra ett verksamhetsstöd särskilt anpassat för spaningsverksamheten. Detta återspeglas i 6–8 §§, som reglerar innehållet i registret.

Med spaning avses såväl den spaning som äger rum under en förundersökning (jfr 23 kap. 2 § rättegångsbalken) som den allmänna spaning som polisen bedriver inom ramen för arbetet med att förebygga, förhindra och upptäcka brottslig verksamhet. Däremot faller sådan spaning som inte hör till den brottsbekämpande verksamheten utanför paragrafens tillämpningsområde. Som exempel på sådan verksamhet kan nämnas spaning efter personer som rymt från kriminalvårdsanstalt under straffverkställighet eller från vissa sjukvårdsenheter. För dessa fall gäller i stället reglerna i personuppgiftslagen. Att uppgifter ur registret under vissa förutsättningar får lämnas ut för att tillgodose andra ändamål återkommer vi till i kommentaren till 15 §.

Behovsrekvisitet innebär att endast sådana uppgifter som det finns ett konkret behov av i spaningsverksamheten får behandlas. Uppgifter som härrör från andra register eller från uppgiftssamlingar som redan är tillgängliga för en bred krets finns det i allmänhet inget behov av att föra in i registret. Som exempel kan

nämnas att det sällan torde finnas något behov av att föra över uppgifter från belastningsregistret eller misstänkeregistret till det allmänna spaningsregistret, eftersom hela polisväsendet ändå har tillgång till dessa uppgifter.

### Vilka personuppgifter som får behandlas

3 § I det allmänna spaningsregistret får behandlas uppgifter som kan hänföras till en enskild person, om

1. den som uppgiften avser kan misstänkas för att ha begått ett brott, som inte enbart har böter i straffskalan, och
2. behandlingen är av särskild betydelse för brottsbekämpningen.

Bakgrunden till paragrafen har behandlats i avsnitt 20.3.3.

Paragrafen reglerar, tillsammans med 4 och 5 §§, uttömmande vilka personuppgifter som får behandlas i registret.

För att uppgifter som avser en viss person ska få föras in i registret krävs det enligt huvudregeln i förevarande paragraf att personen är misstänkt för att ha begått ett brott som inte endast har böter i straffskalan. I stället för en uppräkningslista av de brott som får leda till registrering har valts en generell lösning som bygger på brottets straffskala. Det är emellertid inget som hindrar att Rikspolisstyrelsen på samma sätt som nu inskränker tillämpningsområdet till vissa angivna brott. Det är tillräckligt med en misstanke på låg nivå, vilket markeras genom uttrycket ”kan misstänkas”.

Förutom misstanke om ett visst konkret brott krävs det också att behandlingen i registret är av särskild betydelse för brottsbekämpningen. Detta rekvisit motsvarar i princip vad som gäller enligt tillståndet för det allmänna spaningsregistret. Med brottsbekämpningen avses, liksom i 2 §, all polisens brottsbekämpande verksamhet. Att en uppgift ska ha särskild betydelse för brottsbekämpningen innebär att uppgiften måste vara värdefull antingen i strävandena att förebygga, upptäcka eller förhindra brott eller i verksamheten att utreda eller beivra brott.

Det får med andra ord inte vara en uppgift som man både kan ha och mista.

Om en person uppfyller kraven i första stycket får uppgifter om denne behandlas. Det gäller både direkta och indirekta personuppgifter. Till direkta personuppgifter hör bl.a. uppgifter som identifierar denne, t.ex. personnummer och födelsetid. Exempel på en indirekt personuppgift är uppgift om fordon med visst registreringsnummer.

4 § I registret får behandlas uppgifter som kan hänföras till en enskild person som inte kan misstänkas för brott, om uppgiften

1. har samband med en person som har registrerats enligt 3 §, och
2. är av särskild betydelse för polisens spaningsverksamhet.

I paragrafen regleras i vilken utsträckning uppgifter om andra personer än misstänkta (jfr 3 §) får behandlas i registret. Frågan har behandlats i avsnitt 20.3.3.

För att detta ska vara tillåtet krävs det dels att uppgiften har samband med en misstänkt som registrerats i registret, dels att uppgiften har särskild betydelse för polisens spaningsverksamhet. Alla typer av personuppgifter som på något sätt har anknytning till den misstänkte personen i fråga kan behandlas. Det kan t.ex. vara uppgifter om hans eller hennes anhöriga, såsom uppgifter om deras innehav av bostad eller transportmedel. Vidare kan uppgifter om andra personer som står den misstänkte nära, eller som den misstänkte tillbringar en stor del av sin tid hos, behandlas. Uppgifter om en person som har funnits i den misstänktes omedelbara närhet när han eller hon har ertappats med brott eller en person hos vilken brottet har begåtts eller mot vilken brott har begåtts kan också falla in under bestämmelsen. Detsamma gäller uppgifter om personer som har setts i den misstänktes sällskap under oklara omständigheter. Även uppgifter om någon som tidigare har straffats för brott med direkt anknytning till den misstänktes egen brottslighet, t.ex. namnet på

en hälare som en viss inbrottstjuv ofta vänder sig till, kan vara aktuella.

Förutom att det krävs att uppgiften ska ha samband med en misstänkt person som är registrerad i det allmänna spaningsregistret krävs det också att uppgiften ska ha särskild betydelse för spaningsverksamheten. Innebörden av det är för det första att uppgiften som sådan måste ha relevans för spaningsverksamheten. Det kan uppgiften ha t.ex. om den underlättar eftersökning av den misstänkte, bidrar till upptäckten av brott som han eller hon har begått eller leder till att han eller hon kan knytas som gärningsman till ett visst brott. Uppgifter som *enbart* har betydelse för utredningen av ett brott faller därmed utanför tillämpningsområdet, t.ex. insamlandet av bevisning.

Det räcker emellertid inte med att en uppgift har relevans för polisens spaningsverksamhet; det krävs också att den är av *särskild betydelse* för denna verksamhet. För att exempelvis en uppgift om att två personer sammanträffar med varandra eller att en misstänkt använder en annan persons bil ska anses ha särskild betydelse för spaningsverksamheten krävs det att uppgiften belyser något som – i ett längre perspektiv – kan utnyttjas antingen vid ett ingripande mot den misstänkta personen eller vid utredningen av brott som han eller hon misstänks för. Registreringen får således inte användas för att kringgå bestämmelserna i 2 kap. 2 § första stycket 2 lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Möjligheten att behandla uppgifter om icke misstänkta personer begränsas också av bestämmelserna om vilka kategorier av uppgifter som registret får innehålla, se kommentaren till 6 och 7 §§.

**5 §** Utöver de uppgifter som får behandlas enligt 3 och 4 §§ får uppgifter behandlas om en juridisk person, ett transportmedel eller annat föremål som kan hänföras till en enskild person, om

1. uppgiften kan antas ha samband med ett brott som inte enbart har böter i straffskalan, och
2. behandlingen är av särskild betydelse för brottsbekämpningen.

I paragrafen regleras behandling i vissa fall av uppgifter som kan hänföras till en enskild person och som har samband med ett brott, men där det inte finns någon person som är misstänkt för brottet. Bakgrunden till paragrafen har tecknats i avsnitt 20.3.3.

Bestämmelsen gör det möjligt att bl.a. registrera uppgifter om juridiska personer och vilka företag de bedriver. Som exempel på vad som kan registreras kan vidare nämnas bilar och andra registreringspliktiga fordon. Båtar och fartyg som kan hänföras till viss person genom fartygsregister eller liknande hör också hit, liksom mindre flygplan. Ett namn på en båt som är registrerad på en viss person utgör således en sådan personuppgift som kan behandlas.

Paragrafen täcker också behandling av uppgifter om andra typer av föremål, under förutsättning att dessa kan knytas till en person på sådant sätt att de utgör personuppgifter. Det kan vara fråga om föremål som kräver tillstånd och som kan identifieras genom bl.a. tillverkningsnummer, exempelvis ett skjutvapen.

I paragrafen ställs det upp två krav som ska vara uppfyllda för att den juridiska personen, transportmedlet, eller föremålet, ska få införas i registret. Det ena kravet är att det som ska registreras kan antas ha samband med ett brott som inte har enbart böter i straffskalan. Uttrycket ”kan antas ha samband med” täcker givetvis även fall där det finns ett påvisat samband. Exempel på uppgifter som kan behandlas enligt paragrafen – om förutsättningarna i övrigt är uppfyllda – är uppgifter om att det förekommer brottslig verksamhet, t.ex. omlastning av smuggelgods eller tillverkning av narkotika, i en lokal som ägs eller disponeras av en juridisk person. Ett annat exempel är en vittnesuppgift som knyter ett visst fordon till en brottsplats. Ytterligare ett exempel är en uppgift om ett fordon som sätts i samband med ett brott därför att fordonet har iakttagits en stund efter brottet på en väg som kan vara en naturlig flyktväg.

Det andra kravet för registrering är att behandlingen är av särskild betydelse för brottsbekämpningen. Det är samma krav som ställs i 3 § för registrering av en misstänkt person. I fråga om

tolkningen av begreppet hänvisas till kommentaren till den bestämmelsen.

## Innehåll

6 § Det allmänna spaningsregistret ska innehålla uppgifter om

1. grunden för att en person registreras enligt 3 § eller att en juridisk person, ett transportmedel eller föremål enligt 5 § förs in i registret och omständigheterna i samband med registreringen,

2. de omständigheter och händelser som ger upphov till att andra uppgifter än sådana som avses i 1 tillförs registret,

3. den behandlade uppgiftens ursprung, och

4. uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

I paragrafen slås i fyra punkter fast vilka uppgifter som alltid ska antecknas när det allmänna spaningsregistret tillförs nya uppgifter. Frågan har berörts i avsnitt 20.3.3. Bestämmelserna är tillämpliga både när en fysisk eller juridisk person eller ett transportmedel eller annat föremål registreras första gången och varje gång det tillförs nya uppgifter om personen i fråga eller om transportmedlet eller föremålet. De två första punkterna är alternativa. En av dessa måste således alltid tillämpas, tillsammans med uppgifterna i punkterna 3 och 4.

*Punkten 1* är avsedd att användas när uppgifter om en fysisk person registreras på grund av misstanke om brott. Den gäller oavsett om det är fråga om den första registreringen eller att registret tillförs uppgift om en ny brottsmisstanke. Då ska dels grunden för att uppgifterna registreras anges, dels de närmare omständigheterna. Det innebär normalt att det ska anges vilket brott misstanken avser och omständigheterna kring brottet, exempelvis tidpunkten, eventuella medgärningsmän, uppgifter som har betydelse för spaningen etc. Om det uppstår en ny brottsmisstanke ska motsvarande uppgifter anges.

När en juridisk person, ett transportmedel eller annat föremål registreras med stöd av 5 § ska det på motsvarande sätt framgå

vilket brott som den juridiska personen, transportmedlet eller föremålet har samband med, skälen för registreringen samt andra uppgifter som är viktiga från spaningssynpunkt.

*Punkten 2* reglerar vilka uppgifter som är obligatoriska när man tillför nya uppgifter till de befintliga uppgifterna om en registrerad person eller om en juridisk person, ett transportmedel eller föremål som anges i 5 §. Då ska anges vilka omständigheter eller vilken händelse som gett upphov till att nya uppgifter tillfördes. Om en ny uppgift består i exempelvis en iakttagelse av personen på en viss plats eller i visst sällskap, eller en notering om att en registrerad person disponerar ett fordon som ägs av någon annan, ska således detta antecknas.

Enligt *punkten 3* ska den registrerade uppgiftens ursprung alltid anges. Med detta avses från vilken källa uppgiften kommer. Om uppgiften exempelvis utgörs av en polismans iakttagelser, information från en informatör eller tips från allmänheten ska alltså detta framgå. Hur ingående uppgifter som krävs beror till stor del på ursprunget. I fråga om en uppgift ur en brottsutredning bör det exempelvis framgå om uppgiften har lämnats av ett vittne, en medmisstänkt eller någon annan.

Slutligen ska enligt *punkten 4* uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak anges. Uppgiften ska, som framgår av punkten 3, normalt kunna härledas till en person vars trovärdighet ska värderas. I fråga om uppgifter som lämnas av polismän krävs i detta sammanhang ingen värdering av trovärdigheten, eftersom det följer av en polismans tjänsteplikt att lämna korrekta uppgifter. Däremot ska en bedömning av riktigheten i sak alltid göras eftersom en iakttagelse eller bedömning kan vara osäker oberoende av från vem den kommer. Om det exempelvis är fråga om en iakttagelse som har gjorts på stort avstånd eller i mörker är den allmänt sett inte lika tillförlitlig som en motsvarande iakttagelse gjord i dagsljus på nära håll. När det gäller uppgifternas riktighet i sak får det avgöras av omständigheterna vilka uppgifter som ska anges. Om det är fråga om uppgifter i andra eller tredje hand kan det behövas en mera ingående analys av om uppgifterna har något värde. Uppgifter från en mer



eller mindre tillförlitlig uppgiftslämnare kan värderas med utgångspunkt i vad man känner till om personen etc. Det viktiga är att den som får del av uppgiften har möjlighet att med utgångspunkt i upplysningen kunna bedöma hur tillförlitlig uppgiften är.

7 § Det allmänna spaningsregistret får, utöver vad som anges i 6 §, endast innehålla följande uppgifter om en person som har registrerats enligt 3 §:

1. uppgift som är ägnad att identifiera personen, dock inte uppgifter om resultat av DNA-analyser eller fingeravtryck,
2. uppgift om vistelseadress,
3. uppgift om verkställighet av påföljd för brott,
4. uppgift om att personen är eftersökt i samband med brott,
5. uppgift om att personen tidigare har varit beväpnad, våldsam eller flyktbenägen,
6. uppgift om att personen är föremål för sådan övervakning som avses i 3 kap. 2 § första stycket 2 lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet,
7. uppgift om anknytning till juridisk person,
8. uppgift om anknytning till andra personer som har registrerats enligt 3 § och som kan antas tillhöra samma gruppering som den registrerade,
9. uppgift om att personen har något speciellt tillvägagångssätt, och
10. ärendenummer.

Paragrafen behandlas i avsnitt 20.3.3.

Paragrafen innehåller närmare bestämmelser om vilka uppgifter som får behandlas beträffande den som har antecknats i registret såsom misstänkt. Den tar enbart sikte på uppgifter som rör den registrerade själv. Den allmänna utgångspunkten är att uppgifterna i fråga ska ha betydelse för spaningsverksamheten, eftersom det är det grundläggande ändamålet med behandlingen.

Enligt *punkten 1* får uppgifter som är ägnade att identifiera personen antecknas. Med detta avses bl.a. uppgifter om namn, födelsetid, personnummer eller annat liknande identitetsnummer, adress, arbetsplats, öknamn, nationalitet, signalementsuppgifter och särskilda fysiska kännetecken samt andra uppgifter som kan bidra till att underlätta identifieringen. Det är dock inte

tillåtet att registrera fingeravtryck eller uppgifter om resultat av DNA-analyser, d.v.s. DNA-profiler (se kommentaren till 2 kap. 9 § i den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet).

Med *punkten 2*, vistelseadress, avses inte den fasta adress där en person är skriven utan andra adresser där han eller hon vistas. Det kan röra sig om en adress till en anhörig, t.ex. föräldrar, make/maka eller sambo. Det kan också vara fråga om adressen till en eller flera flickvänner eller pojkvänner. En adress där den misstänkte vistas enbart tillfälligt, t.ex. om denne vid något enstaka tillfälle övernattar hos en bekant, kan inte ses som en vistelseadress. Det krävs således en fastare anknytning till adressen i fråga. Uppgifter av det här slaget kan snabbt bli inaktuella. Det är därför viktigt att uppgifterna kontrolleras innan de läggs till grund för exempelvis beslut om straffprocessuella tvångsmedel.

Enligt *punkten 3* får uppgifter om verkställighet av påföljd antecknas i registret. Sådana uppgifter kan t.ex. vara att den misstänkte avtjänar fängelsestraff och en uppgift om på vilken kriminalvårdsanstalt denne är intagen. Uppgifter av det slaget har betydelse vid spaningen bl.a. på det sättet att det snabbt går att kontrollera var den misstänkte har befunnit sig vid ett visst tillfälle.

*Punkten 4* tar sikte på uppgifter om att personen är eftersökt i samband brott. Det kan t.ex. vara fråga om ett hämtningsbeslut som inte har verkställts eller om att personen ska delges stämning eller kallelse till domstol. Om sådana uppgifter förekommer i ett register, förbättras möjligheterna att snabbt få kontakt med den misstänkte, eftersom uppgifterna kan vara tillgängliga exempelvis för patruller som gör rutinkontroller av fordon och förare.

Uppgifter om att en person tidigare har agerat på sådant sätt att man bör närma sig honom eller henne med försiktighet regleras i *punkten 5*. Enligt den punkten får registret innehålla uppgifter om att personen vid tidigare ingripanden varit beväpnad, våldsam eller visat flyktbenägenhet. Uppgifter av det slaget kan ha stor betydelse för planeringen av ingripanden.

Registret får enligt *punkten 6* också innehålla uppgift om att en person är föremål för särskild övervakning med stöd av 3 kap. 2 § första stycket 2 lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Sådana uppgifter har stor betydelse för att fånga upp iakttagelser om den övervakade personen som görs av andra polismän än de som hanterar övervakningen.

Vidare får enligt *punkten 7* uppgifter om den misstänktes anknytning till en juridisk person behandlas. Det kan t.ex. vara fråga om organisationsnumret till en juridisk person som han eller hon äger eller företräder. Det kan också vara fråga om namnet på ett aktie- eller handelsbolag som den misstänkte driver verksamhet i eller någon annan liknande uppgift.

*Punkten 8* tar sikte på uppgifter om särskilda grupperingar. Det kan exempelvis vara fråga om vissa större ligor som specialiserar sig på en särskild brottstyp, begår brott tillsammans i olika konstellationer eller på annat sätt har nära samband med varandra. Som exempel på sådana grupperingar kan nämnas vissa mc-gäng, bl.a. Hells Angels och Bandidos. Ett annat exempel är brottsbelastade personer som tar sig särskilda namn för att markera gemenskap och som utnyttjar samhörigheten till gruppen för att skrämja eller hota andra. Vid behandling av uppgifter om grupper måste alltid bestämmelserna i 10 §, som förbjuder behandling av känsliga uppgifter, beaktas.

Enligt *punkten 9* får uppgifter om en misstänkts tillvägagångsätt också behandlas. Det kan t.ex. röra sig om en misstänkts sätt att maskera sig, att närma sig ett brottsoffer, att använda en viss typ av tillhygge eller vapen eller att använda visst brännbart material vid mordbränder. Uppgifter av det slaget kan användas bl.a. för att kontrollera om samme misstänkt kan ha gjort sig skyldig till andra brott än de som han eller hon misstänks för.

Slutligen får enligt *punkten 10* registret innehålla uppgifter om nummer på det eller de ärenden där det finns uppgifter om den misstänkte personen. Det kan t.ex. vara fråga om ett diarie-nummer, referensnummer till ett underrättelseprojekt eller liknande.

8 § Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om de uppgifter som får registreras i det allmänna spaningsregistret och om förfarandet vid registreringen.

Enligt paragrafen kan regeringen, eller den myndighet som regeringen bestämmer, meddela närmare föreskrifter om de uppgifter som får behandlas i registret (jfr avsnitt 20.3.3). Tillståndet till det nuvarande registret innehåller detaljerade bestämmelser i olika frågor. Vissa av dessa bestämmelser bör gälla även när registret lagregleras. Eftersom detaljregler av det slaget bör meddelas i förordning eller genom föreskrifter på lägre nivå innehåller paragrafen en erinran om att närmare föreskrifter kan meddelas.

### Särskilda upplysningar

9 § Uppgifter i det allmänna spaningsregistret som direkt kan hänföras till en person som inte misstänks för brott ska förses med en särskild upplysning om detta. Detsamma gäller uppgifter om en juridisk person eller ett transportmedel som indirekt kan hänföras till en sådan person. Upplysning behöver dock inte lämnas om förhållande som ändå framgår tydligt av omständigheterna.

I paragrafen uppställs ett krav på att personuppgifter som direkt kan hänföras till en person som inte själv är misstänkt för brott ska förses med en särskild upplysning om detta förhållande. Detta gäller dock bara i de fall där det inte finns någon misstanke alls. Upplysning behöver inte lämnas om det ändå tydligt framgår av omständigheterna att personen i fråga inte är misstänkt. Så är exempelvis fallet om personuppgiften rör ett brottsoffer. Bestämmelsen motsvarar i denna del vad som föreslås gälla enligt 3 kap. 4 § och 5 kap. 10 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Även indirekta personuppgifter som avser en juridisk person eller ett transportmedel ska på samma sätt förses med sådana upplysningar, om per-

sonen som uppgifterna kan hänföras till inte är misstänkt för brott.

Frågan har behandlats i avsnitt 20.3.5.

### Registrering av känsliga personuppgifter

10 § Uppgifter om en person får inte registreras i det allmänna spaningsregistret på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv.

Trots bestämmelsen i första stycket får uppgifter om en person som registreras på annan grund kompletteras med sådana uppgifter som avses i första stycket om det är absolut nödvändigt för syftet med registreringen.

Uppgifter som beskriver en persons utseende ska alltid utformas på ett objektivt sätt med respekt för människovärdet.

Paragrafen anger i vilken utsträckning känsliga personuppgifter får behandlas. Bestämmelsen motsvarar i allt väsentligt 2 kap. 8 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. För det närmare innehållet hänvisas till kommentaren till den bestämmelsen.

Frågan har behandlats i avsnitt 20.3.4.

### Tillgången till personuppgifter

11 § Tillgången till personuppgifter i det allmänna spaningsregistret ska alltid begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

I paragrafen föreskrivs att tillgången till uppgifter alltid ska begränsas till vad var och en behöver för att fullgöra sina arbetsuppgifter. En motsvarande bestämmelse finns i 2 kap. 10 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Med tillgång avses både direktåtkomst och annan tillgång till uppgifter i skriftlig eller muntlig form. Bestämmelsen

riktar sig därigenom inte bara till de tjänstemän som beslutar om systemen för personuppgiftsbehandling och till dem som beslutar om behörighet att ta del av uppgifter utan även till de enskilda tjänstemän som har tillgång till uppgifterna. För de sistnämnda innebär bestämmelsen att de inte får lämna uppgifter vidare till andra tjänstemän än de som behöver uppgifterna i sitt arbete.

## Sökning

**12 §** Uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv får inte användas som sökbegrepp vid sökning i det allmänna spaningsregistret. Detta hindrar inte att uppgifter som beskriver en persons utseende används som sökbegrepp.

Paragrafen innehåller ett förbud mot att använda känsliga personuppgifter som grund för sökning i det allmänna spaningsregistret. Begränsningar av likartat slag har föreslagits i 3 kap. 5 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Frågan har behandlats i avsnitt 20.3.5.

**13 §** Uppgifter i det allmänna spaningsregistret som direkt kan hänföras till en person som inte är misstänkt för brott får inte vara sökbara.

I paragrafen regleras vilka personuppgifter om icke misstänkta personer som får vara sökbara. Sådana uppgifter som direkt kan hänföras till en person, som inte misstänks för brott, får inte vara sökbara. Begränsningen omfattar som framgår av lydelsen endast direkta personuppgifter. Däremot får uppgifter som indirekt rör en icke misstänkt person behandlas, t.ex. uppgifter om ett fordon som han eller hon är ägare till.

Skälen till bestämmelsen har behandlats i avsnitt 20.3.5.

## Utlämnande av uppgifter och uppgiftsskyldighet

14 § Personuppgifter i det allmänna spaningsregistret som är nödvändiga för att framställa rättsstatistik ska lämnas till den myndighet som ansvarar för att framställa sådan statistik.

Paragrafen har samma innehåll som 6 § polisdatalagen. En motsvarande regel har föreslagits i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet (2 kap. 12 §). Enligt bestämmelsen ska personuppgifter som är nödvändiga för att framställa rättsstatistik lämnas till den myndighet som ansvarar för att framställa statistiken. Enligt bilagan till förordningen (2001:100) om den officiella statistiken är Brottsförebyggande rådet statistikansvarig på rättsväsendets område (utom såvitt avser domstolarnas verksamhet).

15 § Personuppgifter får lämnas till en utländsk myndighet eller mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Om det är förenligt med svenska intressen, får uppgifter vidare lämnas till en polismyndighet eller åklagarmyndighet i en stat som är ansluten till Interpol, eller till Interpol eller Europol, om det behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott.

Av 1 kap. 3 § tredje stycket sekretesslagen (1980:100) följer att uppgifter får lämnas till en utländsk myndighet eller en mellanfolklig organisation även i vissa andra fall.

Paragrafen innehåller bestämmelser om utlämnande av personuppgifter till utländska myndigheter och mellanfolkliga organisationer. Skälen för bestämmelsen har behandlats i avsnitt 20.3.6. Bestämmelsen motsvarar i sina huvuddrag 2 kap. 13 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Enligt *första stycket* får personuppgifter lämnas till en utländsk myndighet eller mellanfolklig organisation om utlämnandet följer av en internationell överenskommelse som Sverige efter riks-

dagens godkännande har tillträtt. Bestämmelsen är tillämplig om överenskommelsen ålägger Sverige att lämna vissa typer av uppgifter. Däremot gäller den inte för överenskommelser där det enbart sägs att utlämnande *får* ske.

Enligt *andra stycket* får uppgifter lämnas ut till en utländsk polis- eller åklagarmyndighet, eller till Interpol eller Europol. Uppgifter kan lämnas utan föregående begäran. Förutsättningarna är dels att utlämnandet ska vara förenligt med svenska intressen, dels att uppgiften behövs för att myndigheten eller organisationen ska kunna förebygga, upptäcka, utreda eller beivra brott. Vidare måste den som överväger att lämna ut en uppgift med stöd av paragrafen alltid försäkra sig om att den mottagande staten eller organisationen har en adekvat nivå på skyddet för personuppgifter.

Det *tredje stycket* innehåller en erinran om att det också finns bestämmelser om utlämnande av uppgifter till utländska myndigheter i sekretesslagen.

16 § Utan hinder av sekretess enligt 7 kap. 1 a § och 9 kap. 17 § sekretesslagen (1980:100) ska personuppgifter i det allmänna spåringsregistret lämnas till

1. polismyndighet, Ekobrottsmyndigheten, Tullverket, Kustbevakningen och Skatteverket, om myndigheten har behov av uppgifterna i sin brottsbekämpande verksamhet, eller

2. polismyndighet, om myndigheten har behov av uppgifterna i annan verksamhet än den brottsbekämpande verksamheten och det finns särskilda skäl för att lämna ut dem.

Regeringen meddelar föreskrifter om att uppgifter får lämnas ut till andra myndigheter än de som anges i första stycket.

Paragrafen innehåller sekretessbrytande bestämmelser om utlämnande. Skälen för bestämmelserna har behandlats i avsnitt 20.3.6.

I *första stycket* regleras i vilken utsträckning uppgifter ur registret, utan hinder av sekretess, får lämnas ut till andra myndigheter, om de begär det. Den sekretessbrytande regeln omfattar dels viss sekretess enligt 7 kap. sekretesslagen, dels sekretess en-



ligt 9 kap. 17 §. Den sistnämnda paragrafen reglerar sekretess till skydd för enskilda personliga eller ekonomiska förhållanden i bl.a. förundersökningar och andra brottsutredningar. Regeln har utformats efter mönster av bestämmelserna i 2 kap. 14–16 §§ lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Direktåtkomst till registret regleras inte i denna paragraf utan i 18 §.

Enligt *punkten 1* får uppgifter ur registret lämnas till övriga brottsbekämpande myndigheter, men endast om de har behov av uppgifterna i sin brottsbekämpande verksamhet. Behovet får i första hand bedömas med utgångspunkt i de uppgifter som den andra myndigheten har att sköta. Eftersom registret i huvudsak är personrelaterat, torde en begäran normalt avse en person som är föremål för misstanke, eller som av annat skäl är intressant i en förundersökning eller ett underrättelseprojekt som bedrivs vid den andra myndigheten.

*Punkten 2* reglerar möjligheten att lämna uppgifter ur registret till en polismyndighet om myndigheten behöver uppgiften för annan verksamhet än brottsbekämpning. I sådana fall krävs det särskilda skäl för att lämna uppgiften. Exempel på när särskilda skäl kan anses föreligga är att en uppgift om en persons farlighet kan ha betydelse för polisens insats i ett visst handräckningsärende.

Med stöd av *andra stycket* kan regeringen meddela föreskrifter om att uppgifter får lämnas ut till en annan myndighet än de som anges i paragrafen.

### **Utlämnande av uppgifter på medium för automatiserad behandling**

**17 §** Endast enstaka personuppgifter i det allmänna spaningsregistret får lämnas ut på medium för automatiserad behandling, om inte regeringen har meddelat föreskrifter eller i ett enskilt fall har beslutat om att uppgifter får lämnas ut på sådant medium även i andra fall.

Paragrafen reglerar under vilka förutsättningar uppgifter får lämnas ut i elektronisk form, t.ex. på diskett, CD-rom eller i ett e-postmeddelande. Den motsvarar 3 kap. 8 § lagen om behandlingen av personuppgifter i polisens brottsbekämpande verksamhet. Innebörden är att en större mängd personuppgifter inte får lämnas ut på medium för automatiserad behandling, såvida inte regeringen har meddelat föreskrifter om det eller i ett enskilt fall beslutat om detta. Däremot kan enstaka uppgifter lämnas ut. I fråga om vad som avses med enstaka uppgifter hänvisas till kommentaren till 3 kap. 8 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet

Frågan har behandlats i avsnitt 20.3.6.

### Direktåtkomst

18 § Polismyndigheter, Ekobrottsmyndigheten, Tullverket och Kustbevakningen får medges direktåtkomst till det allmänna spningsregistret.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet.

Paragrafen innehåller bestämmelser om direktåtkomst. Frågan har behandlats i avsnitt 20.3.6.

*Första stycket* innebär att Rikspolisstyrelsen har möjlighet att besluta att vissa myndigheter får ha direktåtkomst till registret. De uppräknade myndigheterna har alltså inte en absolut rätt att få sådan tillgång till registret. Bestämmelsen motsvarar 3 kap. 9 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. För en närmare beskrivning av innebörden av bestämmelsen hänvisas till kommentaren till den bestämmelsen.

Enligt *andra stycket* kan regeringen, eller den myndighet som regeringen bestämmer, meddela närmare föreskrifter om direktåtkomsten samt om behörighet och säkerhet.

## Gallring

19 § Uppgifter i det allmänna spaningsregistret om en person som har registrerats enligt 3 § ska gallras senast tre år efter det att uppgiften om misstanke om brott registrerades. Om uppgiften avser misstanke om brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver dock uppgifterna inte gallras förrän fem år efter registreringen.

Om en ytterligare uppgift om personen förs in i registret, behöver uppgifterna om den registrerade personen inte gallras förrän

1. fem år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,

2. tre år från det att den nya uppgiften fördes in i registret, om uppgiften avser misstanke om annat brott än i 1, eller

3. ett år från det att den nya uppgiften fördes in i registret, om uppgiften inte avser misstanke om brott.

Den tid under vilken en person som har registrerats enligt 3 § avtjänar ett fängelsestraff eller genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning ska inte räknas med vid beräkningen av de frister som anges i första och andra styckena.

Uppgifter om en person som avses i 4 § ska gallras senast när uppgifterna om den person som har registrerats enligt 3 § och som uppgifterna har samband med gallras.

Paragrafen, vars bakgrund har kommenterats i avsnitt 20.3.7, innehåller bestämmelser om gallring av uppgifter som har registrerats med stöd av 3 eller 4 §. Bestämmelserna anger när en uppgift senast ska gallras, vilket innebär att uppgifterna kan gallras tidigare. Den frågan aktualiseras bl.a. om personen avlider eller om det av något annat skäl inte längre finns grund för att behandla uppgifter om personen i det allmänna spaningsregistret. Gallring kan också aktualiseras om det med stöd av 21 § har utfärdats föreskrifter om kortare gallringstid än vad som anges i paragrafen.

I *första stycket* föreskrivs att uppgifter om en person som avses i 3 §, dvs. en person som är misstänkt för brott, enligt huvudregeln ska gallras efter tre år. Är det fråga om ett mycket allvar-

ligt brott, dvs. brott med lägst två års fängelse i straffskalan, får uppgifterna bevaras i fem år.

I *andra stycket* behandlas den situationen att nya uppgifter om en registrerad person tillförs registret. I sådana fall kan gallringsfristen komma att förskjutas framåt. Om uppgifterna består i nya brottsmisstankar förlängs gallringsfristen med tre respektive fem år, beroende på brottets svårhetsgrad. Om den nya uppgiften inte avser en ny brottsmisstanke, utan exempelvis uppgifter om den misstänktes kontakter med andra brottsmisstänkta personer, förlängs gallringsfristen med ett år. Det innebär att om registret beträffande en person, som misstänks för ett brott som medför att uppgifterna ska gallras efter tre år, tillförs uppgift om ett nytt brott av samma svårhetsgrad ett år efter den ursprungliga registreringen så kommer uppgifterna om honom eller henne att kunna bevaras i sammanlagt fyra år, under förutsättning att inga nya brottsmisstankar eller andra noteringar tillkommer som kan förlänga tiden ytterligare. En registrering av en ny uppgift kan endast förlänga den ursprungliga gallringsfristen, inte förkorta den. Om t.ex. en notering enligt *andra stycket 3* görs i början av en tre- eller femårsfrist kommer den således inte att påverka den totala bevarandetiden. Den nya uppgiften får bevaras lika länge som övriga uppgifter.

Det *tredje stycket* innehåller en bestämmelse som innebär att tidpunkten för gallring skjuts fram i de fall där den registrerade avtjänar fängelsestraff, genomgår sluten ungdomsvård eller rättspsykiatrisk vård med särskild utskrivningsprövning. En motsvarande bestämmelse finns i 3 kap. 16 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

I *fjärde stycket* regleras när uppgifter om personer som behandlas i registret med stöd av 4 §, dvs. personer som inte själva är misstänkta för brott, ska gallras. Sådana uppgifter ska gallras senast när uppgifterna om den misstänkte, som registreringen har samband med, gallras.

20 § Uppgifter om en juridisk person, ett transportmedel eller annat föremål som har registrerats enligt 5 § ska gallras senast tre år efter den senaste registreringen. Om den senast införda uppgiften avser ett brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet, behöver dock uppgifterna inte gallras förrän fem år efter det att den senaste uppgiften infördes.

Bakgrunden till paragrafen har tecknats i avsnitt 20.3.7. Den reglerar när uppgifter som har registrerats med stöd av 5 § ska gallras. Det rör sig här om uppgifter om juridiska personer, transportmedel och andra föremål som kan antas ha samband med brott men där det inte finns någon person som är misstänkt för brottet. Sådana uppgifter gallras enligt huvudregeln tre år efter den senaste registreringen. Är det fråga om ett allvarigare brott, dvs. brott med lägst två års fängelse i straffskalan, får uppgifterna bevaras i fem år.

Gallringstiden förlängs om registret, innan tiden har löpt ut, tillförs en ny uppgift som kan antas ha samband med brott, eftersom gallringstiden enligt denna bestämmelse löper från den senaste registreringen.

21 § Vad som föreskrivs i 19 och 20 §§ hindrar inte att regeringen eller den myndighet som regeringen bestämmer

1. meddelar föreskrifter om att uppgifter gallras vid en tidigare tidpunkt, eller bevaras för historiska, statistiska eller vetenskapliga ändamål, eller

2. i ett enskilt fall beslutar att en uppgift ska bevaras om det finns synnerliga skäl för det.

Ett beslut enligt första stycket 2 ska omprövas varje år.

Bakgrunden till paragrafen har behandlats i avsnitt 20.3.7.

Enligt *första stycket* får regeringen, eller den myndighet regeringen bestämmer meddela föreskrifter om andra gallringsfrister än de som anges i 19 och 20 §§.

Enligt *punkten 1* kan sådana föreskrifter avse dels att uppgifter i registret ska gallras vid en tidigare tidpunkt, dels att uppgifter ska bevaras för historiska, statistiska eller vetenskapliga ändamål.

I *punkten 2* öppnas en möjlighet att i ett enskilt fall besluta att uppgifter, som annars skulle ha gallrats, får bevaras. För ett sådant beslut krävs synnerliga skäl, vilket innebär att skälen ska vara mycket starka. Som exempel kan nämnas att det ibland kan finnas skäl att bevara uppgifter som rör vissa typer av brottslingar under längre tid än vad som annars är tillåtet, om risken för återfall i brott bedöms vara särskilt stor. Det kan t.ex. gälla en sexualförbrytare som periodvis vårdas för psykisk sjukdom, och som av det skälet inte vistas ute i samhället och har möjlighet att begå nya brott, men där risken för att vederbörande senare begår nya brott är markant.

Ett beslut om att uppgifter ska bevaras trots att den normala gallringsfristen har löpt ut bör dokumenteras, eftersom beslutet ska kunna omprövas årligen enligt *andra stycket*.

### Rättelse och skadestånd

22 § Bestämmelserna i 28 och 48 §§ personuppgiftslagen (1998:204) om rättelse och skadestånd gäller vid behandling av personuppgifter enligt denna lag eller enligt föreskrifter som har meddelats med stöd av lagen.

Paragrafen, vars bakgrund har tecknats i avsnitt 20.3.8, reglerar en registrerad persons rätt till rättelse och skadestånd, om dennes personuppgifter har behandlats på ett felaktigt sätt. Genom hänvisningen till personuppgiftslagen regleras felaktig personuppgiftsbehandling på samma sätt som i bl.a. lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister och den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet (se 2 kap. 2 §).

## 26.3 Förslaget till lag om ändring i rättegångsbalken

### 28 kap.

**12 a §** Kroppsbesiktning genom tagande av salivprov får ske på den som skäligen kan misstänkas för ett brott på vilket fängelse kan följa, om syftet är att göra en DNA-analys av provet och registrera uppgifter om resultatet av analysen i det DNA-register eller det utredningsregister som förs enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet*.

En tidigare hänvisning till polisdatalagen har ersatts med en hänvisning till den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Någon ändring i sak är inte avsedd.

**12 b §** Kroppsbesiktning genom tagande av salivprov får ske på annan än den som skäligen kan misstänkas för ett brott, om

1. syftet är att genom en DNA-analys av provet underlätta identifiering vid utredning av ett brott på vilket fängelse kan följa, och
2. det finns synnerlig anledning att anta att det är av betydelse för utredningen av brottet.

Analysresultatet får inte jämföras med de uppgifter som finns registrerade i register som förs enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller i övrigt användas för annat ändamål än det för vilket provet har tagits.

Första stycket gäller inte den som är under 15 år.

En tidigare hänvisning i *andra stycket* till polisdatalagen har ersatts med en hänvisning till den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Någon ändring i sak är inte avsedd.

## 26.4 Förslaget till lag om ändring i sekretesslagen (1980:100)

### 5 kap.

1 § Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,
2. angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,
3. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde,
4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott, eller
5. Finansinspektionens verksamhet som rör övervakning enligt lagen (2005:377) om straff för marknadsmissbruk vid handel med finansiella instrument,  
om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till *verksamhet hos polisen enligt 2 kap. 5 § 1 lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller till verksamhet hos Säkerhetspolisen enligt 5 kap. 2 § 1 samma lag* gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Detsamma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott samt hos tillsynsmyndigheten i konkurs och hos Kronofogdemyndigheten för uppgift som angår misstanke om brott.

Utän hinder av sekretessen enligt andra stycket kan enskild få uppgift om huruvida han eller hon förekommer i Säkerhetspolisens register med anledning av den verksamhet som bedrevs med stöd av



1. personalkontrollkungörelsen (1969:446) och de tilläggsföreskrifter som utfärdats med stöd av den,

2. förordningen den 3 december 1981 med vissa bestämmelser om verksamheten vid Rikspolisstyrelsens säkerhetsavdelning, eller

3. motsvarande äldre bestämmelser.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i andra stycket om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling som hänför sig till sådan verksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

Eftersom underrättelseverksamhet inte särregleras på samma sätt i den nya lagen som i polisdatalagen har omfattningen av sekretessen enligt *andra stycket* formulerats om. Någon ändring i sak är dock inte avsedd.

7 § Sekretess gäller i verksamhet som avser rättsligt samarbete på begäran av annan stat eller mellanfolklig domstol för uppgift som hänför sig till

1. utredning enligt bestämmelserna om förundersökning i brottmål, eller

2. angelägenhet som angår tvångsmedel,

om det kan antas att det varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* och lagen om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst fyrtio år.

Hänvisningen till polisdatalagen har ersatts med en hänvisning till den nya lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Sekretessen i nu aktuella delar

rör uppgifter som hänför sig till angelägenheter som regleras i Schengens informationssystem. Behandlingen av sådana uppgifter regleras i huvudsak i den särskilda lagstiftningen som rör Schengens informationssystem och faller enligt 1 kap. 2 § tredje stycket lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet utanför den lagens tillämpningsområde. Ett svenskt polisiärt ingripande, t.ex. omhändertagande av en person som har efterlysts för senare utlämning eller överlämnande enligt lagstiftningen om den europeiska arresteringsordern, leder emellertid till viss nödvändig personuppgiftsbehandling därutöver, vilken hittills har reglerats i polisdatalagen, t.ex. behandling av uppgifter rörande frihetsberövandet. Hänvisningen till den nya lagen avser enbart sådan behandling.

## 7 kap.

**41 §** Sekretess gäller hos polismyndighet och åklagarmyndighet, samt hos Rikspolisstyrelsen, Tullverket, Kustbevakningen och Migrationsverket, för uppgift om enskilda personliga förhållanden i en angelägenhet som avser en framställning enligt 3 § lagen (2000:344) om Schengens informationssystem

1. om omhändertagande av en person som har efterlysts för överlämnande eller utlämning,

2. om att en person *ska* nekas tillträde till eller uppehållstillstånd i Schengenstaterna (spärlista),

3. om tillfälligt omhändertagande av en person med hänsyn till dennes eller någon annans säkerhet, samt

4. om dold övervakning eller särskilda kontrollåtgärder, om det inte står klart att uppgiften kan lämnas ut utan att den enskilde eller någon honom närstående lider men.

Sekretess gäller hos myndighet som prövar ansökningar om visering och uppehållstillstånd för uppgift om enskilda personliga förhållanden i en angelägenhet som avser en sådan framställning som avses i första stycket 2 under samma förutsättningar som anges i första stycket.

Utän hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i *lagen (2008:000) om behandling av personuppgifter i*

*polisens brottsbekämpande verksamhet* och lagen (2000:344) om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

Ändringen är av samma slag och har samma bakgrund som ändringen i 5 kap. 7 §.

## 9 kap.

17 § Sekretess gäller för uppgift om enskilda personliga och ekonomiska förhållanden, om inte annat följer av 18 §

1. i utredning enligt bestämmelserna om förundersökning i brottmål,

2. i angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,

3. i angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),

4. i åklagarmyndighets, polismyndighets, Skatteverkets, Statens kriminaltekniska laboratoriums, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,

5. i Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller polismyndighet i brottmål,

6. i register som förs av Rikspolisstyrelsen enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller som annars behandlas där med stöd av samma lag,

7. i register som förs enligt *lagen (1998:621) om misstankeregister*,

8. i det register som förs enligt *lagen (2008:000) om polisens allmänna spaningsregister*,

9. i register som förs av Skatteverket enligt *lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar* eller som annars behandlas där med stöd av samma lag,

10. i särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänförs till registrering som avses i 15 kap. 1 §,

11. i register som förs av Tullverket enligt lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas med stöd av samma lag,

om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till den enskilde lider skada eller men.

Sekretess enligt första stycket 2 gäller hos domstol i dess rättskipande eller rättsvårdande verksamhet endast om det kan antas att den enskilde eller någon närstående till den enskilde 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 annat allvarligt men om uppgiften röjs. Av 12 kap. 2 § andra stycket framgår att även sekretessen enligt första stycket 1 är begränsad hos domstol.

Sekretess enligt första stycket gäller hos tillsynsmyndigheten i konkurs för uppgift som angår misstanke om brott.

Sekretess gäller i verksamhet, som avses i första stycket, för anmälan eller utsaga från enskild, om det kan antas att fara uppkommer för att någon utsätts för våld eller annat allvarligt men om uppgiften röjs.

Utan hinder av sekretessen får en skadelidande, eller den som den skadelidande överlätit sin rätt till, ta del av en uppgift

1. i en nedlagd förundersökning eller i en förundersökning som avslutats med ett beslut om att åtal inte ska väckas,

2. i en annan brottsutredning som utförts enligt bestämmelserna i 23 kap. rättegångsbalken och som avslutats på annat sätt än med beslut att väcka åtal, med strafföreläggande eller med föreläggande av ordningsbot, eller

3. i en avslutad utredning enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,

om den skadelidande, eller den som den skadelidande överlätit sin rätt till, behöver uppgiften för att kunna få ett anspråk på skadestånd eller på bättre rätt till viss egendom tillgodosett och det inte bedöms vara av synnerlig vikt för den som uppgiften rör eller någon närstående till honom eller henne att den inte lämnas ut.

Utan hinder av sekretessen får en uppgift också lämnas ut

1. till enskild enligt vad som föreskrivs i den särskilda lagstiftningen om unga lagöverträdare,

2. till enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) samt i förordning som har stöd i den lagen,

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar, lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* samt i förordningar som har stöd i dessa lagar,

4. till enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

Utän hinder av sekretessen får polisen på begäran av den som lidit person- eller sakskada vid en trafikolycka lämna uppgift om identiteten hos en trafikant som haft del i olyckan.

Utän hinder av sekretessen enligt första stycket 1 får uppgift lämnas till konkursförvaltare, om uppgiften kan antas ha betydelse för konkursutredningen.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i första stycket 1–4 eller 6 eller motsvarande verksamhet enligt äldre bestämmelser, om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling gäller sekretessen i högst sjuttio år.

I *första stycket punkten 6* har hänvisningen till polisdatalagen ersatts med en hänvisning till lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Enligt *punkten 8* gäller sekretess för uppgifter i register som förs enligt den föreslagna lagen om polisens allmänna spaningsregister. Registret bör på motsvarande sätt som misstankeregistret regleras i en särskild punkt i paragrafen.

Övrig ändring i paragrafen är endast av språklig natur.

## **26.5 Förslaget till lag om ändring i säkerhetskyddslagen (1996:627)**

12 § Med registerkontroll avses *kontroll av om det förekommer uppgifter om en person i register som förs av polisen eller om sådana uppgifter annars behandlas där i den brottsbekämpande verksamheten.*

*Vid en registerkontroll ska uppgifter hämtas från register som omfattas av lagen (1998:620) om belastningsregister och lagen (1998:621) om misstankeregister. Vidare ska uppgifter hämtas som Säkerhetspoli-*

sen behandlar med stöd av 5 kap. lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

Uppgifter får också hämtas från register som omfattas av 4 kap. lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet eller lagen (2008:000) om polisens allmänna spaningsregister. Vidare får uppgifter hämtas som polisen i övrigt behandlar med stöd av 2 kap. 5 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, om uppgifterna har gjorts gemensamt tillgängliga.

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om omfattningen av registerkontrollen.

I paragrafen regleras vad en registerkontroll omfattar. Bestämelsen har kommenterats i avsnitt 21.

I första stycket definieras vad som avses med registerkontroll, nämligen kontroll av om en viss person förekommer antingen i register som förs av polisen eller om det annars förekommer uppgifter om personen som behandlas i polisens brottsbekämpande verksamhet.

I andra stycket anges i de två första meningarna vilken kontroll som är obligatorisk. Registerkontrollen ska alltid omfatta åtminstone kontroll av misstankeregistret och belastningsregistret samt av uppgifter som Säkerhetspolisen behandlar i sin brottsbekämpande verksamhet.

I tredje stycket anges att kontrollen därutöver även får omfatta uppgifter ur register som förs med stöd av 4 kap. lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet, dvs. uppgifter ur bl.a. DNA-register och fingeravtrycksregister, samt uppgifter som behandlas med stöd av 2 kap. 5 § samma lag om uppgifterna har gjorts gemensamt tillgängliga. Slutligen får kontrollen också omfatta uppgifter i polisens allmänna spaningsregister.

Av fjärde stycket följer att regeringen, eller den myndighet regeringen bestämmer, kan meddela närmare föreskrifter om omfattningen av registerkontrollen.

21 § Utlämnande av uppgifter vid registerkontroll får omfatta

1. för säkerhetsklass 1 eller 2: varje uppgift som finns tillgänglig om den kontrollerade och, om det är oundgängligen nödvändigt, om make eller sambo, och

2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret *och* misstankeregistret *samt* uppgifter som behandlas hos Säkerhetspolisen.

Hänvisningen till SÄPO-registret i punkten 2 har tagits bort. Någon ändring i sak är inte avsedd.

22 § Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som finns i belastningsregistret *och* misstankeregistret *samt* uppgifter som behandlas hos Säkerhetspolisen.

Hänvisningen till SÄPO-registret har tagits bort och ersatts med en hänvisning till Säkerhetspolisens personuppgiftsbehandling i lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet. Någon ändring i sak är inte avsedd.

## 26.6 Förslaget till lag om ändring i lagen (1998:620) om belastningsregister

2 § Belastningsregistret *ska* föras för att ge information om sådana belastningsuppgifter som behövs i verksamhet hos

1. *polismyndigheter, Skatteverket, Tullverket och Kustbevakningen* för att förebygga, upptäcka och utreda brott,

2. åklagarmyndigheter för beslut om förundersökning och åtal samt för utfärdande av strafföreläggande,

3. allmänna domstolar för straffmätning och val av påföljd och

4. polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.

Registret får användas också för att till enskild lämna uppgifter som är av särskild betydelse i dennes verksamhet.

Ändringen i *första stycket* 1 innebär att ändamålet med belastningsregistret utökas så att det kommer att föras för samtliga brottsbekämpande myndigheters behov, således även Kustbevakningens. Ändringen kommenteras i avsnitt 22. Vidare har, utöver en språklig justering, benämningarna på myndigheterna inom skatteförvaltningen och tullväsendet anpassats till gjorda organisationsförändringar.

**6 §** Personuppgifter ur belastningsregistret *ska* lämnas ut om det begärs av

1. Riksdagens ombudsmän, Justitiekanslern eller Datainspektionen för deras tillsynsverksamhet,

2. *polismyndighet, Skatteverket, Tullverket, Kustbevakningen, åklagarmyndighet* eller allmän domstol för verksamhet som avses i 2 § första stycket 1–3,

3. förvaltningsdomstol för prövning enligt 2 § första stycket 4 eller

4. myndighet i övrigt i den utsträckning regeringen för vissa slag av ärenden föreskriver det eller för ett särskilt fall ger tillstånd till det.

Regeringen får föreskriva att en myndighet som avses i första stycket får ha direktåtkomst till registret.

Ändringen i *första stycket* 2 innebär att Kustbevakningen får rätt till uppgifter ur belastningsregistret för sin brottsbekämpande verksamhet. Ändringen kommenteras i avsnitt 22. Vidare har, på samma sätt som i 2 §, myndighetsbenämningarna anpassats till gjorda organisationsförändringar samt en språklig justering gjorts. Genom att Kustbevakningen omnämns i paragrafens första stycke kan regeringen med stöd av andra stycket meddela föreskrifter om att Kustbevakningen får ha direktåtkomst till registret. Det *andra stycket* är oförändrat.



## 26.7 Förslaget till lag om ändring i lagen (1998:621) om misstankeregister

2 § Misstankeregistret *ska* föras för att underlätta tillgången till sådana uppgifter om skäligen misstanke om brott som behövs i verksamhet hos

1. *polismyndigheter, Skatteverket, Tullverket och Kustbevakningen* för att samordna förundersökningar mot en person och för att förebygga, upptäcka och utreda brott,

2. åklagarmyndigheter för beslut om förundersökning och åtal och

3. polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning.

Registret får användas också för att till enskild lämna uppgifter som är av särskild betydelse i dennes verksamhet.

Ändringen är av samma slag och har samma bakgrund som ändringen i 2 § lagen om belastningsregister.

5 § Uppgifter ur misstankeregistret *ska* lämnas ut om det begärs av

1. *polismyndighet, Skatteverket, Tullverket, Kustbevakningen, åklagarmyndighet eller allmän domstol* för verksamhet som avses i 2 § första stycket 1–3,

2. myndighet i övrigt i den utsträckning regeringen för vissa slag av ärenden föreskriver det eller för ett särskilt fall ger tillstånd till det.

Regeringen får föreskriva att en myndighet som avses i första stycket får ha direktåtkomst till registret.

Att uppgifter får lämnas ut i vissa andra fall framgår av 14 kap. sekretesslagen (1980:100).

Ändringarna är av samma slag och har samma bakgrund som ändringarna i 6 § lagen om belastningsregister.

## 26.8 Förslaget till lag om ändring i lagen (2000:344) om Schengens informations-system

5 § Registret *ska* endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.

Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* eller annan svensk författning.

Ändringen i *andra stycket* består enbart i att tidigare hänvisning till polisdatalagen har ersatts med en hänvisning till den föreslagna lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet.

## 26.9 Förslaget till lag om ändring i lagen (2007:000) om tillsyn över viss brottsbekämpande verksamhet

1 § Säkerhets- och integritetsskyddsnämnden (nämnden) *ska* utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet.

Nämnden *ska* även utöva tillsyn över *polisens* behandling av uppgifter enligt *lagen (2008:000) om behandling av personuppgifter i polisens brottsbekämpande verksamhet* och *lagen (2008:000) om polisens allmänna spaningsregister*. Tillsynen *ska* särskilt *avse* *behandlingen av sådana känsliga personuppgifter som avses i 2 kap. 8 § lagen om behandling av personuppgifter i polisens brottsbekämpande verksamhet* och *10 § lagen om polisens allmänna spaningsregister*.

Tillsynen *ska* särskilt syfta till att säkerställa att verksamhet enligt första och andra styckena bedrivs i enlighet med lag eller annan författning.

Paragrafen innebär att det i Säkerhets- och integritetsskyddsnämndens uppgifter ska ingå att utöva tillsyn över såväl den öppna polisens som Säkerhetspolisens personuppgiftsbehandling i den brottsbekämpande verksamheten. Tillsynen ska särskilt avse behandlingen av känsliga personuppgifter. Som utvecklas närmare i avsnitt 19 ska tillsynen syfta till att säkerställa att personuppgiftsbehandlingen är lagenlig.



# Sammanfattning av SOU 2001:92

## Behandling av personuppgifter i polisens verksamhet

### Några utgångspunkter

Utredningens direktiv innebär ett uppdrag att följa genomförandet av den nya polisregisterlagstiftningen och att påtala eventuella brister särskilt från integritetssynpunkt. Utredningen skall överväga om det behöver vidtas några åtgärder, t.ex. i form av författningsändringar eller genom ökade möjligheter till insyn eller kontroll, för att lagstiftningen skall uppnå sitt syfte att öka möjligheten till effektiv brottsbekämpning och samtidigt värna om den enskildes personliga integritet.

Sedan den 1 april 1999 gäller en ny lag om behandling av personuppgifter hos polisen, polisdatalagen (1988:622). Den nya lagen bygger på personuppgiftslagen (1998:204) och innehåller bara de särregler som ansetts nödvändiga i polisens verksamhet. Polisdatalagen utgör en del av den nya lagstiftningen om behandling av personuppgifter i polisens verksamhet. Övriga lagar inom detta område utgörs av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister och lagen (2000:344) om Schengens informationssystem.

Nämnda lagar har utgjort utgångspunkten för vårt arbete. Bland övriga rättskällor av betydelse bör särskilt nämnas Europakonventionen, Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna samt

Europarådets rekommendation om användningen av personuppgifter inom polissektorn m.m.

Målsättningen med våra förslag är att de skall utgöra en lämplig avvägning mellan polisens rätt att använda modern teknik och den enskildes integritet. En utgångspunkt för oss i arbetet har varit att hinder för ett rationellt utnyttjande av datorstöd inte bör ställas upp i större utsträckning än vad som är nödvändigt med hänsyn till intresset av skydd för den personliga integriteten.

Vi har i enlighet med direktiven inventerat de register som förs inom polisen. Den befintliga registerstrukturen har uppkommit främst som följd av Datainspektionens tillstånd för polisen att föra olika enskilda register och är således inte resultatet av någon övergripande planering.

Ett stort antal register förs, såväl centralt som lokalt. Registeren kan indelas i tre grupper beroende på vilka bestämmelser som styr behandlingen, nämligen

- register som förs med stöd av särskilda regler i lagstiftningen,
- register som förs med stöd av personuppgiftslagen och de allmänna bestämmelserna i polisdatalagen, och
- register som enligt övergångsbestämmelserna till polisdatalagen förs med stöd av tillstånd från Datainspektionen.

Det traditionella registerbegreppet har vid flera tillfällen kritiserats. Dagens system inom polisen byggs företrädesvis som ärendehanteringssystem och inte som traditionella register. I ärendehanteringssystem lagras hela aktmaterial. Systemen är anpassade för fritextsökning. Vi finner dock inte anledning att i lagstiftningen ersätta begreppet register som beteckning för vissa fastställda informationsmängder med något annat begrepp.

### **Nya arbetsmetoder och ny teknik**

Inom en mycket snar framtid lär praktiskt taget allt skrivarbete komma att utföras med hjälp av datorer. En realistisk lagstiftning

måste ta hänsyn till de nya förhållandena. Manuell behandling av information, däribland personuppgifter, är inte längre ett realistiskt alternativ till automatiserad behandling av information. Den omständigheten att mängden automatiserat behandlade personuppgifter kraftigt ökat gör det ännu viktigare att en lagstiftning om behandling av personuppgifter i polisens verksamhet ger ett tillfredsställande skydd för den enskildes personliga integritet.

Polisen skall enligt nyare uttalanden från statsmakterna arbeta problemorienterat och verka brottsförebyggande. Arbetet skall vara proaktivt och inte reaktivt inriktat. För att kunna verka brottsförebyggande måste dock polisen inhämta och bearbeta information om enskilda personer i större utsträckning än som skedde vid ett traditionellt reaktivt arbetssätt. Det ligger därför i sakens natur att en brottsförebyggande arbetsmetod innebär ett ökat intrång i den enskildes personliga integritet i förhållande till ett reaktivt arbetssätt.

Användningen av digital teknik för behandling av ljud och bild är i hög grad ägnad att höja kvaliteten på polisens brottsutredningar. Detta gäller framför allt beträffande digitala bilder. Eftersom den digitala tekniken får anses utgöra automatiserad behandling blir dock bestämmelserna i personuppgiftslagen tillämpliga i den utsträckning behandlingen avser digitala bilder eller ljud som innehåller personuppgifter.

Polisens intranät används i första hand för att sprida verksamhetsrelaterad information inom polismyndigheterna.

### **Informationsutbytet med Europol**

Sverige har anslutit sig till Europolkonventionen. Europols främsta uppgift är att vara ett kriminalunderrättelseorgan för de brottsbekämpande myndigheterna i medlemsländerna inom EU. Som sådant är Europol en knutpunkt för utbyte av information och underrättelser mellan medlemsländerna. Europol fungerar så att medlemsländerna tillhandahåller Europol uppgifter främst ur sina nationella polisregister. Dessa uppgifter bearbetas och ana-

lyseras sedan hos Europol. Resultatet av bearbetningen och analyserna delges därefter medlemsländerna.

Polisdatalagen medger inte att personuppgifter som härrör från kriminalunderrättelseverksamhet behandlas automatiserat annat än i särskilda undersökningar eller kriminalunderrättelseregister. Härigenom har informationsutbytet med Europol kommit att allvarligt försvåras.

### **En nordisk jämförelse**

Som underlag för våra överväganden har vi inhämtat upplysningar om vilka regler som gäller i Danmark, Finland och Norge beträffande automatiserad behandling av personuppgifter i polisens verksamhet. Jämförelsen visar att den svenska lagstiftningen är mer restriktiv för polisen än de regleringar som gäller i de övriga nordiska länderna.

### **En ny polisdatlag**

I enlighet med direktiven för utredningen har vi analyserat konsekvenserna av den nya regleringen om polisens rätt att behandla personuppgifter automatiserat. Vi har vid vår analys av lagstiftningen kommit fram till att det behöver göras ändringar av regleringen i polisdatalagen. Ändringarna som vi anser erfordras är relativt omfattande. Vi anser därför att en ny lag om behandling av personuppgifter i polisens verksamhet som ersätter den nuvarande polisdatalagen bör införas. Även den nya lagen bör ges namnet polisdatalagen.

De särskilda lagarna om belastningsregister, om misstankeregister och om Schengens informationssystem bör vara kvar oförändrade.

Den nya polisdatalagen bör vara heltäckande och upprepa de bestämmelser i personuppgiftslagen som skall vara tillämpliga i polisens verksamhet.



Den nya lagens syfte bör liksom personuppgiftslagen vara att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

Den nya lagen bör gälla vid behandling av personuppgifter i sådan polisverksamhet som avses i 2 § 1–3 polislagen (1984:387), dvs. i den egentliga polisverksamheten.

Lagen bör gälla vid behandling av personuppgifter i form av bilder eller ljud, dock ej vid sådan behandling som består i insamling av personuppgifter genom upptagning av bilder eller ljud. Lagen bör inte gälla vid insamling av personuppgifter genom teleavlyssning, teleövervakning eller kameraövervakning.

Det digitala referensbiblioteket över barnpornografiska framställningar som förs av Rikskriminalpolisen behöver inte regleras särskilt i lagstiftningen.

Den nya polisdatalagen bör gälla enbart i polisens verksamhet. Lagen bör därför inte omfatta Ekobrottsmyndigheten.

### **Grundläggande bestämmelser om behandling av personuppgifter i den nya polisdatalagen**

Personuppgiftslagens *definitioner* av begreppen behandling av personuppgifter, blockering av personuppgifter, mottagare, personuppgifter, personuppgiftsansvarig, personuppgiftsbiträde, personuppgiftsombud, tillsynsmyndigheten och tredje man samt polisdatalagens definition av begreppet DNA-analys bör finnas med även i en ny lag för polisen.

Bestämmelsen i 9 § personuppgiftslagen om *grundläggande krav på behandling av personuppgifter* bör även i fortsättningen gälla i polisens verksamhet. Även särbestämmelsen om *gallring* i 13 § polisdatalagen bör vara kvar.

Rikspolisstyrelsen bör även i fortsättningen vara ensam personuppgiftsansvarig för de centrala registren i polisens verksamhet. En bestämmelse som ger Rikspolisstyrelsen möjlighet att besluta verkställighetsföreskrifter bör ingå i en ny polisdataförordning.

Personuppgifter bör få behandlas endast om *behandlingen är nödvändig* för att polisen skall kunna utföra polisverksamhet som består i att

1. förebygga brott och andra störningar av den allmänna ordningen och säkerheten,
2. övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när sådana inträffat eller
3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

Den nya lagen bör inte hindra att personuppgifter *diarieförs* eller *behandlas i löpande text* om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det.

Bestämmelsen i 5 § polisdatalagen om behandling av *känsliga personuppgifter* bör gälla även i fortsättningen.

Bestämmelsen i 22 § personuppgiftslagen om behandling av *personnummer och samordningsnummer* bör gälla på polisområdet. Dock bör samtycke inte kunna åberopas som grund för behandling.

I 10 och 11 §§ polisdatalagen finns bestämmelser om *behandling av uppgifter om kvarstående misstankar*. Dessa bestämmelser bör oförändrat gälla även i fortsättningen.

Någon bestämmelse om förbud mot överföring av personuppgifter till tredjeland motsvarande 33 § personuppgiftslagen bör inte gälla i den egentliga polisverksamheten. En följd av detta blir att offentliga personuppgifter kan spridas på *Internet*. Av integritetsskäl bör dock en efterlysning av en person med anledning av att han eller hon avvikit från verkställande av påföljd för brott eller med anledning av att han eller hon misstänks för brott, få ske på *Internet* endast om

1. domen eller misstanken avser ett brott för vilket inte lindrigare straff än fängelse i två år är föreskrivet, eller
2. personen kan antas vara farlig för annans personliga säkerhet.

Reglerna i 23–27 §§ personuppgiftslagen om *information till registrerade* bör även i fortsättningen gälla i polisens verksamhet. Det behövs dock därutöver ytterligare två undantag från polisens

informationsplikt. I fall uppgifter om en enskild person samlas in från personen själv, bör information heller inte behöva lämnas, om

- det finns bestämmelser om antecknandet eller utlämnandet av personuppgifter i författning, eller
- uppgifterna samlas in i samband med larm eller annan liknande underrättelse och larmet eller underrättelsen kräver omedelbara insatser från den personuppgiftsansvarige.

I stället för att som i dag avse registrerade bör bestämmelserna i den nya lagen om information avse enskilda.

Bestämmelserna i 28 § personuppgiftslagen om *rättelse* bör även i fortsättningen gälla på polisområdet. Bestämmelserna bör dock avse den enskilde i stället för den registrerade.

När det gäller *säkerheten vid behandling* bör liksom i dag bestämmelserna i 30–32 §§ personuppgiftslagen gälla i polisens verksamhet. Regeln i 32 § om tillsynsmyndighetens rätt att besluta om säkerhetsåtgärder bör dock meddelas genom förordning. Därutöver bör det i den nya lagen finnas en bestämmelse som föreskriver att *direkt åtkomst* till personuppgifter skall vara förbehållen de personer inom polisen som på grund av sina arbetsuppgifter behöver tillgång till information om uppgifterna.

Bestämmelsen i 8 § personuppgiftslagen om *förhållandet till offentlighetsprincipen* bör liksom i dag gälla för polisen.

I 6–8 §§ polisdatalagen och i 15–16 §§ polisdataförordningen finns bestämmelser om *utlämnande av uppgifter*. Bestämmelserna bör oförändrade föras över till en ny polisdatlag respektive en ny polisdataförordning.

Bestämmelserna i 36–41 §§ personuppgiftslagen och 3–7 §§ personuppgiftsförordningen om *anmälan till tillsynsmyndigheten* och personuppgiftsombudets uppgifter, i 13 § personuppgiftsförordningen om bemyndiganden, i 2 § polisdataförordningen om förhandskontroll, och i 14 § polisdataförordningen om underrättelseskyldighet bör gälla även i fortsättningen för polisen.

Om den personuppgiftsansvarige har utsett ett personuppgiftsombud och anmälan därför inte behöver göras, bör *anmälan*

i stället göras *till personuppgiftsombudet*. En ny polisdatalag bör innehålla en bestämmelse härom.

Bestämmelsen i 42 § personuppgiftslagen om upplysningar till allmänheten om behandlingar som inte anmälts bör gälla för polisen.

Personuppgiftslagens bestämmelser i 43–47 §§ personuppgiftslagen och i 2 § personuppgiftsförordningen om *Datainspektionens befogenheter* bör gälla på polisområdet. Bestämmelserna bör dock meddelas i förordning.

Bestämmelserna i 48 § personuppgiftslagen och i 9 § polisdatalagen om *skadestånd* bör gälla för polisen också i fortsättningen. Den nya regeln bör dock avse enskilda och inte registrerade. Någon *straffbestämmelse* motsvarande 49 § personuppgiftslagen behövs inte i den nya lagen.

Bestämmelserna i 51 § personuppgiftslagen om *överklagande* bör i sak gälla även i fortsättningen för polisen. Dessutom bör det i en ny lag föreskrivas att en myndighets beslut om rättelse och om information som skall lämnas efter ansökan skall överklagas hos kammarrätten.

### **Behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot**

Vid utformningen av en lag om behandling av personuppgifter i polisens verksamhet måste beaktas att polisens arbete skall vara inriktat främst på brottsförebyggande verksamhet.

Polisdatalagen innehåller en reglering om behandling av personuppgifter i kriminalunderrättelseverksamhet och i kriminalunderrättelseregister. Regleringen har kommit att försvåra polisens arbete med att verka problemorienterat och brottsförebyggande.

En lag om behandling av personuppgifter bör handla om just behandling av personuppgifter och inte vara inriktad på att reglera vissa verksamheter eller arbetsmetoder hos polisen. Bestämmelserna om kriminalunderrättelseverksamhet och krimi-

nalunderrättsregister bör bl.a. av det skälet inte vara kvar i en ny polisdata lag. Bestämmelserna härom bör i stället ersättas av bestämmelser om behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot.

De personuppgifter som kommer att omfattas av sistnämnda regler är först och främst sådana som avser personer som inte är misstänkta för något konkret brott, men väl för att ha utövat eller utöva brottslig verksamhet. Uppgifterna kan dock även avse andra personer, t.ex. personer som lämnat upplysningar om iakttagelser m.m. utan att själva vara misstänkta.

Uppgifter om en enskild person som det inte finns någon misstanke om brott mot bör få behandlas för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer.

Alla uppgifter som är nödvändiga för ändamålet med behandlingen bör få behandlas. Om uppgifter om en person som det över huvud taget inte finns någon misstanke mot behandlas, bör uppgiften förses med en anteckning om detta förhållande. Vid aktuell behandling av personuppgifter bör uppgifterna förses med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

Aktuell behandling av personuppgifter bör få ske för att underlätta övervakning av personer som kan antas komma att begå brott. Behandling i detta syfte bör dock endast få avse dömda personer som antingen är allvarligt kriminellt belastade eller som kan antas vara farliga för annans personliga säkerhet.

Den personuppgiftsansvarige bör särskilt besluta de ändamål och villkor i övrigt som behövs för att förebygga otillbörligt intrång i enskildas personliga integritet. När det gäller villkor i övrigt kan det t.ex. röra sig om hur information skall inhämtas, hur arbetet skall ske och avrapporteras samt säkerheten vid behandling m.m.

Personuppgifter som behandlas enligt här aktuella bestämmelser bör få bevaras högst tre år från det att uppgifterna om personen samlades in. Uppgifter som behandlas för att underlätta övervakning av personer som kan antas komma att begå

brott bör dock få bevaras till dess att uppgifterna gallras ur belastningsregistret.

Bestämmelserna om aktuell behandling av personuppgifter bör inte gälla personuppgifter

- i en förundersökning, eller
- i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

### **Det allmänna spaningsregistret**

Det föreligger ett mycket stort behov av det allmänna spaningsregistret (ASP) inom brottsbekämpningen. ASP är viktigt bl.a. för att närpolisverksamheten skall kunna fungera.

Det bör i den nya polisdatalagen införas särskilda regler om ASP. Lagregleringen bör i allt väsentligt ge polisen rätt att fortsätta den behandling av personuppgifter som i dag förekommer.

ASP bör få föras i syfte att underlätta tillgången till uppgifter med anknytning till polisverksamhet som består i att förebygga, upptäcka och utreda brott. Bestämmelserna i den nya polisdatalagen om behandling av uppgifter om kvarstående misstankar bör inte gälla vid behandling av personuppgifter i ASP.

I ASP bör uppgifter som kan hänföras till en enskild person få föras in endast om den som avses med uppgiften kan misstänkas för att ha begått ett brott och om registreringen är av särskild betydelse för brottsbekämpningen. Uppgifter om transportmedel eller andra varor som kan antas ha samband med brott bör få registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Uppgifterna skall därvid förses med en upplysning om att det inte finns någon misstanke mot denne. I lagen bör vidare anges vilka typer av personuppgifter som får eller skall registreras i ASP.

Personuppgifter i ASP bör som regel gallras senast tre år efter det att uppgifter om att den registrerade kan misstänkas för att ha begått brott senast infördes. Om den senaste händelsen avser

misstanke om ett brott för vilket inte lindrigare straff än fängelse i två år är föreskrivet bör dock uppgifterna få stå kvar i fem år efter den senaste registreringen.

Uppgifter ur ASP bör under vissa förutsättningar få lämnas ut till Ekobrottsmyndigheten, Kustbevakningen, en tullmyndighet eller en skattemyndighet. Polismyndigheterna bör få ha direkt åtkomst till uppgifter i ASP.

### **Ytterligare bestämmelser om vissa register m.m.**

Den nya polisdatalagen bör utöver regler om ASP innehålla särskilda regler om register med uppgifter om DNA-analyser i brottmål och om fingeravtrycks- och signalementsregister.

Bestämmelserna i 22–28 §§ polisdatalagen och i 11 § polisdataförordningen om register med uppgifter om DNA-analyser i brottmål bör gälla även i fortsättningen.

Särskilda författningsregler om den behandling av personuppgifter i Statens kriminaltekniska laboratoriums verksamhet som sker med anledning av laboratoriets DNA-analyser bör inte införas.

Bestämmelserna i 29–31 §§ polisdatalagen om fingeravtrycks- och signalementsregister bör gälla även i fortsättningen. Sådana register bör dock utöver vad som framgår av 30 § polisdatalagen även få innehålla uppgifter om brottskoder.

Det behövs inte någon särskild författningsreglering för eventuella centrala system motsvarande de lokala system som i dag används, t.ex. rationell anmälningsrutin (RAR), datoriserad utredningsrutin – tvångsmedel (DurTvå) och kommunikationscentralernas system (KC-systemen).

### **Säkerhetspolisen**

En ändring av Säkerhetspolisens organisation bestående i en sammanslagning mellan Säkerhetspolisen och Rikskriminalpoli-

sen övervägs för närvarande. Våra förslag utgår från den nuvarande organisationen av Säkerhetspolisen.

Bestämmelserna i den nya polisdatalagen om behandling av personuppgifter i Säkerhetspolisens verksamhet bör i huvudsak ha samma innebörd som i dag. Den särskilda lagregleringen om SÄPO-registret bör dock inte vara kvar i den nya lagen. Några särskilda registerbestämmelser för Säkerhetspolisen bör inte heller i övrigt införas.

Säkerhetspolisen bör få behandla personuppgifter för att underlätta

- spaning i syfte att förebygga och avslöja brott mot rikets säkerhet,
- spaning i syfte att bekämpa terrorism och
- registerkontroll enligt säkerhetsskyddslagen.

Bestämmelserna i den nya polisdatalagen om behandling av uppgifter om kvarstående misstankar och om behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot bör inte gälla för Säkerhetspolisen.

### **Ikraftträdande**

Den nya polisdatalagen bör kunna träda i kraft den 1 juli 2003, då polisdatalagen (1998:622) bör upphöra att gälla. Vi har bedömt att några övergångsbestämmelser till den nya lagen inte behövs.

### **Konsekvenser**

Vi har genomfört konsekvensanalyser enligt 14 och 15 §§ kommittéförordningen (1998:1474). Våra förslag bör ge polisen bättre förutsättningar att arbeta problemorienterat och verka brottsförebyggande.

Enligt vår bedömning ger de förslag som vi lämnar inte upphov till kostnader som inte ryms inom berörda myndigheters



anslag. Förslagen i övrigt får inte några sådana konsekvenser som motiverar en särskild redovisning.



# Polisdatautredningens lagförslag

## Förslag till polisdatalag

Härigenom föreskrivs följande.

### 1 kap. Lagens syfte och tillämpningsområde

#### Syftet med lagen

1 § Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter i polisens verksamhet.

#### Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter i polisens verksamhet för att

1. förebygga brott och andra störningar av den allmänna ordningen och säkerheten,
2. övervaka den allmänna ordningen och säkerheten, hindra störningar därav samt ingripa när sådana inträffat eller
3. bedriva spaning och utredning i fråga om brott som hör under allmänt åtal.

Lagen gäller också behandling av sådana uppgifter som avses i 5 kap. 10 och 11 §§.

**3 §** Lagen gäller inte för behandling av personuppgifter som företas med stöd av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller lagen (2000:344) om Schengens informationssystem.

Lagen gäller heller inte vid insamling av personuppgifter genom teleavlyssning, teleövervakning eller kameraövervakning. Lagen gäller vid övrig behandling av personuppgifter i form av bilder eller ljud, dock ej vid sådan behandling som består i insamling av personuppgifter genom upptagning av bilder eller ljud.

Vid behandling av personuppgifter i form av bilder eller ljud skall vad som i lagen sägs om insamling tillämpas när uppgifterna första gången behandlas efter det att insamlingen avslutats.

**4 §** Vid annan behandling av personuppgifter i polisens verksamhet än som avses i 2 eller 3 § gäller personuppgiftslagen (1998:204).

**5 §** Bestämmelserna i 1 och 2 kap., 3 kap. 1 och 2 §§, 4 kap. samt 6 och 7 kap. gäller för sådan behandling av personuppgifter som helt eller delvis är automatiserad samt även för annan behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier.

Bestämmelserna i 3 kap. 3–11 §§ och 5 kap. gäller endast automatiserad behandling av personuppgifter.

## Definitioner

6 § I denna lag används följande beteckningar med nedan angivna betydelse.

<i>Beteckning</i>	<i>Betydelse</i>
<i>Behandling (av personuppgifter)</i>	Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.
<i>Blockering (av personuppgifter)</i>	En åtgärd som vidtas för att personuppgifterna skall vara förknippade med information om att de är spärrade och om anledningen till spärren och för att personuppgifterna inte skall lämnas ut till tredje man annat än med stöd av 2 kap. tryckfrihetsförordningen.
<i>DNA-analys</i>	Varje förfarande som kan användas för analys av deoxyribonukleinsyra.

<i>Mottagare</i>	Den till vilken personuppgifter lämnas ut. När personuppgifter lämnas ut för att en myndighet skall kunna utföra sådan tillsyn, kontroll eller revision som den är skyldig att sköta, anses dock inte myndigheten som mottagare.
<i>Personuppgifter</i>	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
<i>Personuppgiftsansvarig</i>	Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
<i>Personuppgiftsbiträde</i>	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning.
<i>Personuppgiftsombud</i>	Den fysiska person som, efter förordnande av den personuppgiftsansvarige, självständigt skall se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

## 2 kap. Grundläggande principer vid behandling av personuppgifter

### Grundläggande krav på behandlingen av personuppgifter

1 § Den personuppgiftsansvarige skall se till att

1. personuppgifter behandlas bara om det är lagligt,
2. personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed,
3. personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål,
4. personuppgifter inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in,
5. de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen,
6. inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen,
7. de personuppgifter som behandlas är riktiga och, om det är nödvändigt, aktuella,
8. alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen, och
9. gallring sker av personuppgifter som inte längre behövs för ändamålet med behandlingen om inte annat anges i denna lag.

Vad som sagts i första stycket 9 gäller inte personuppgifter

1. i en förundersökning, eller
2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

2 § Vid tillämpning av 1 § första stycket 4 gäller att en behandling av personuppgifter för historiska, statistiska eller vetenskapliga ändamål inte skall anses som oförenlig med de ändamål för vilka uppgifterna samlades in.

Personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål under längre tid än som sagts i 1 § första

stycket 9. Personuppgifterna får dock i sådana fall inte bevaras under en längre tid än vad som behövs för dessa ändamål.

Personuppgifter som behandlas för historiska, statistiska eller vetenskapliga ändamål får användas för att vidta åtgärder i fråga om den enskilde bara om den enskilde har lämnat sitt samtycke eller det finns synnerliga skäl med hänsyn till den enskildes vitala intressen.

### När behandlingen av personuppgifter är tillåten

3 § Personuppgifter får behandlas bara om behandlingen är nödvändig för att sådan polisverksamhet som anges i 1 kap. 2 § första stycket skall kunna utföras.

Lagen hindrar inte att personuppgifter diarieförs eller behandlas i löpande text om uppgifterna har lämnats i ett ärende eller är nödvändiga för handläggningen av det.

## 3 kap. Vissa behandlingar av personuppgifter

### Behandling av känsliga personuppgifter

1 § Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexuella läggning.

Om uppgifter om en person behandlas på annan grund får uppgifterna kompletteras med sådana uppgifter som avses i första stycket, om det är oundgängligen nödvändigt för syftet med behandlingen.

### Behandling av personnummer

2 § Uppgifter om personnummer eller samordningsnummer får behandlas bara när det är klart motiverat med hänsyn till



1. ändamålet med behandlingen,
2. vikten av en säker identifiering, eller
3. något annat beaktansvärt skäl.

### Behandling av uppgifter om kvarstående misstankar

3 § Om en förundersökning mot en person har lagts ned på grund av bristande bevisning får uppgifter om brottsmisstanken behandlas för annat ändamål än arkivering endast under förutsättning att

1. den misstänkte enligt förundersökningsledarens bedömning fortfarande är skäligen misstänkt för brottet och
2. uppgifterna behövs för att förundersökningen skall kunna tas upp på nytt.

4 § Om åtal mot en person har lagts ned eller om denne genom lagakraftvunnen dom har frikänts får uppgifter om brottsmisstanken behandlas för annat ändamål än arkivering endast

1. om förundersökningen tas upp på nytt eller
2. för prövning av ett särskilt rättsmedel enligt 58 kap. rättegångsbalken.

### Behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot

#### *Syften med behandlingen*

5 § Uppgifter om en enskild person som det inte finns någon misstanke om brott mot får behandlas för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller mer.

Uppgifter om en enskild person som det inte finns någon misstanke mot skall föras med en upplysning om detta förhållande.

6 § Personuppgifter som behandlas enligt 5 § skall förses med upplysningar om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak.

7 § Personuppgifter som behandlas enligt 5 § för att underlätta övervakning av personer som kan antas komma att begå brott får endast avse dömda personer som är allvarligt kriminellt belastade eller som kan antas vara farliga för annans personliga säkerhet.

#### *Beslut om villkor för behandlingen*

8 § Den personuppgiftsansvarige skall särskilt besluta ändamål för behandlingen av personuppgifter och de villkor i övrigt som behövs för att förebygga otillbörligt intrång i enskildas personliga integritet.

#### *Gallring*

9 § Personuppgifter som behandlas enligt 5 § får inte bevaras längre tid än tre år från det att uppgifterna om personen samlades in. Sådana personuppgifter som avses i 7 § får dock bevaras senast till dess att uppgifterna om personen gallras ur belastningsregistret.

Regeringen, eller den myndighet regeringen bestämmer, får meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål.

#### *Behandling av personuppgifter som inte omfattas av bestämmelserna*

10 § Bestämmelserna i 5–9 §§ gäller inte behandling av personuppgifter

1. i en förundersökning eller

2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

### **Behandling av uppgifter på Internet om efterlysningar av enskilda personer**

11 § En efterlysning av en person med anledning av att han eller hon avvikit från verkställighet av påföljd för brott eller med anledning av att han eller hon misstänks för brott, får göras allmänt tillgänglig på Internet endast om

1. domen eller misstanken avser ett brott för vilket inte lindrigare straff än fängelse i två år är föreskrivet eller
2. personen kan antas vara farlig för annans personliga säkerhet.

### **4 kap. Särskilt om behandling av personuppgifter hos Säkerhetspolisen**

1 § Säkerhetspolisen får utan hinder av bestämmelserna i 3 kap. 3–10 §§ behandla personuppgifter för att underlätta

1. spaning i syfte att förebygga och avslöja brott mot rikets säkerhet,
2. spaning i syfte att bekämpa terrorism och
3. registerkontroll enligt säkerhetsskyddslagen (1996:627).

## 5 kap. Register

### Spaningsregister

#### *Ändamål*

1 § Rikspolisstyrelsen får föra ett allmänt spaningsregister för polisens spaningsverksamhet. Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

2 § Det allmänna spaningsregistret får föras i syfte att underlätta tillgången till uppgifter med anknytning till polisverksamhet som består i att förebygga, upptäcka och utreda brott.

#### *Innehåll*

3 § Det allmänna spaningsregistret får innehålla uppgifter som kan hänföras till en enskild person endast om den som avses med uppgiften kan misstänkas för att ha begått ett brott och om registreringen är av särskild betydelse för brottsbekämpningen.

Uppgifter om transportmedel eller andra varor som kan antas ha samband med ett brott eller om hjälpmedel som kan antas ha använts i samband med ett brott får registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Uppgifterna skall därvid föras med upplysning om att det inte finns någon misstanke mot denne.

4 § Det allmänna spaningsregistret får innehålla följande uppgifter om en enskild person:

1. upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet,
2. identifieringsuppgifter,
3. vistelseadress,
4. uppgifter om särskilda fysiska kännetecken,
5. uppgifter om verkställighet av påföljd för brott,
6. uppgifter om varor, brottshjälpmedel och transportmedel,

7. ärendenummer och

8. varning om att personen tidigare varit beväpnad, våldsam eller flyktbenägen.

Det allmänna spaningsregistret skall alltid innehålla uppgifter om de omständigheter och händelser som gett anledning att anta att den registrerade begått brott.

### *Gallring*

**5 §** Uppgifter i det allmänna spaningsregistret om en registrerad person skall gallras senast tre år efter det att uppgifter om att denne kan misstänkas för att ha begått ett brott senast infördes. Om den senast införda uppgiften avser misstanke om ett brott för vilket lindrigare straff än fängelse i två år inte är föreskrivet behöver dock uppgifterna inte gallras förrän fem år efter att den senaste uppgiften infördes.

Regeringen, eller den myndighet regeringen bestämmer, får meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska och vetenskapliga ändamål.

### *Bestämmelser som inte gäller*

**6 §** Bestämmelserna i 3 kap. 3 och 4 §§ gäller inte vid behandling av personuppgifter i det allmänna spaningsregistret.

## **Register med uppgifter om DNA-analyser i brottmål**

### *Ändamål*

**7 §** Uppgifter om resultat av DNA-analyser får behandlas endast för att underlätta identifiering av personer i samband med utredning av brott. Rikspolisstyrelsen får föra register (DNA-register och spårregister) i enlighet med 8–12 §§ över de uppgif-

ter som behandlas. Rikspolisstyrelsen är personuppgiftsansvarig för behandling av uppgifter i registren.

Sådana uppgifter som avses i första stycket får även behandlas i

1. i en förundersökning eller
2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

#### *DNA-register*

8 § Ett DNA-register får innehålla uppgifter om resultatet av DNA-analyser som har gjorts under utredning av ett brott och som avser personer som har dömts för

1. ett sådant brott mot en persons liv eller hälsa, personliga integritet eller säkerhet som avses i 3, 4, 6, 8, 12 eller 17 kap. brottsbalken, om brottet kan leda till fängelse i mer än två år,
2. ett allmänfarligt brott som avses i 13 kap. brottsbalken, om brottet kan leda till fängelse i mer än två år, eller
3. försök, förberedelse, stämpling, anstiftan eller medhjälp till ett sådant brott som avses i 1 eller 2.

9 § Registreringen av ett analysresultat skall begränsas till uppgifter som ger information om den registrerades identitet. Analysresultat som kan ge upplysning om den registrerades personliga egenskaper får inte registreras.

Utöver vad som sägs i första stycket får DNA-registret endast innehålla upplysningar som visar i vilket ärende analysen har gjorts och vem analysen avser.

#### *Spårregister*

10 § Ett spårregister får innehålla uppgifter om DNA-analyser som har gjorts under utredning av brott och som inte kan hänfö-

ras till en identifierbar person. Utöver uppgifter om analysresultat får ett spårregister endast innehålla upplysningar som visar i vilket ärende analysen har gjorts.

11 § Uppgifter i spårregister får endast jämföras med analysresultat

1. som inte kan hänföras till en identifierbar person,
2. som finns i DNA-registret, eller
3. som kan hänföras till en person som är misstänkt för brott.

### *Gallring*

12 § Uppgifter i DNA-registret skall gallras senast när uppgifterna om den registrerade gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.

Uppgifter i spårregister skall gallras senast trettio år efter registreringen.

### *Prover från personer som inte är misstänkta för brott*

13 § Om det i samband med utredning av ett brott har tagits ett prov för DNA-analys från någon som inte är misstänkt för brottet får provet inte användas för något annat ändamål än det för vilket det togs. Ett sådant prov får inte heller sparas efter det att målet slutligt har avgjorts.

## **Fingeravtrycks- och signalementsregister**

### *Ändamål*

14 § För att underlätta identifiering av personer i samband med brott får Rikspolisstyrelsen behandla uppgifter i fingeravtrycks- och signalementsregister. Ett sådant register får användas för identifiering av okända personer även i andra fall. Rikspolissty-

relsen är personuppgiftsansvarig för behandling av uppgifter i registren.

Sådana uppgifter som avses i första stycket får även behandlas i

1. i en förundersökning eller
2. i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.

#### *Uppgifter som får behandlas*

**15 §** Fingeravtrycks- och signalementsregister får endast innehålla uppgifter om den som är misstänkt eller dömd för brott eller som har fått lämna fingeravtryck enligt 19 § lagen (1991:572) om särskild utlänningskontroll. I ett sådant register får endast antecknas uppgifter om

1. fingeravtryck,
2. signalement,
3. identifieringsuppgifter,
4. ärendenummer och
5. brottskoder.

#### *Gallring*

**16 §** Uppgifter i fingeravtrycks- eller signalementsregister om en misstänkt person skall gallras när förundersökning eller åtal mot personen läggs ned eller när åtal ogillas. Uppgifterna får dock bevaras längre om andra uppgifter om den registrerade skall behandlas med stöd av 3 kap. 3 och 4 §. När dessa uppgifter gallras skall även uppgifter i fingeravtrycks- och signalementsregister gallras.

Om den registrerade döms skall uppgifterna i registret gallras senast vid den tidpunkt då uppgifterna gallras ur belastningsregistret enligt lagen (1998:620) om belastningsregister.



Regeringen får meddela föreskrifter om gallring av uppgifter om den som har lämnat fingeravtryck enligt lagen (1991:572) om särskild utlänningskontroll.

## **6 kap. Information till den enskilde, rättelse och säkerheten vid behandling**

### **Information till den enskilde**

#### *Information som skall lämnas självant*

**1 §** Om uppgifter om en enskild person samlas in från personen själv, skall den personuppgiftsansvarige i samband därmed självant lämna den enskilde information om behandlingen av uppgifterna.

Information enligt första stycket behöver inte lämnas, om det finns bestämmelser om antecknandet eller utlämnandet av personuppgifterna i författning.

Information enligt första stycket behöver heller inte lämnas om uppgifterna samlas in i samband med ett larm eller en annan liknande underrättelse och larmet eller underrättelsen kräver omedelbara insatser från den personuppgiftsansvarige.

**2 §** Om personuppgifterna har samlats in från någon annan källa än den enskilde, skall den personuppgiftsansvarige självant lämna den enskilde information om behandlingen av uppgifterna när de antecknas. Är uppgifterna avsedda att lämnas ut till tredje man, behöver informationen dock inte ges förrän uppgifterna lämnas ut för första gången.

Information enligt första stycket behöver inte lämnas, om det finns bestämmelser om antecknandet eller utlämnandet av personuppgifterna i författning.

Information behöver inte heller lämnas enligt första stycket, om detta visar sig vara omöjligt eller skulle innebära en opropor­tionerligt stor arbetsinsats. Om uppgifterna används för att vidta

åtgärder som rör den enskilde, skall dock information lämnas senast i samband med att så sker.

*Vad informationen skall omfatta*

3 § Information enligt 1 eller 2 § skall omfatta

1. uppgift om den personuppgiftsansvariges identitet,
2. uppgift om ändamålen med behandlingen, och
3. all övrig information som behövs för att den enskilde skall kunna ta till vara sina rättigheter i samband med behandlingen, såsom information om mottagarna av uppgifterna, skyldighet att lämna uppgifter och rätten att ansöka om information och få rättelse.

Information behöver dock inte lämnas om sådant som den enskilde redan känner till.

*Information som skall lämnas efter ansökan*

4 § Den personuppgiftsansvarige är skyldig att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om personuppgifter som rör den sökande behandlas eller ej. Behandlas sådana uppgifter skall skriftlig information lämnas också om

1. vilka uppgifter om den sökande som behandlas,
2. varifrån dessa uppgifter har hämtats,
3. ändamålen med behandlingen, och
4. till vilka mottagare eller kategorier av mottagare som uppgifterna lämnas ut.

En ansökan enligt första stycket skall göras skriftligen hos den personuppgiftsansvarige och vara undertecknad av den sökande själv. Information enligt första stycket skall lämnas inom en månad från det att ansökan gjordes. Om det finns särskilda skäl för det, får information dock lämnas senast fyra månader efter det att ansökan gjordes.

Information enligt första stycket behöver inte lämnas om personuppgifter i löpande text som inte fått sin slutliga utformning när ansökan gjordes eller som utgör minnesanteckning eller liknande. Vad som nu sagts gäller dock inte om uppgifterna har lämnats ut till tredje man eller om uppgifterna behandlas enbart för historiska, statistiska eller vetenskapliga ändamål eller, när det gäller löpande text som inte fått sin slutliga utformning, om uppgifterna har behandlats under längre tid än ett år.

*Undantag från informationskyldigheten vid sekretess och tystnadsplikt*

5 § I den utsträckning det är särskilt föreskrivet i författning eller i beslut som har meddelats med stöd av författning att uppgifter inte får lämnas ut till den enskilde gäller inte bestämmelserna i 1–4 §§.

### Rättelse

6 § Den personuppgiftsansvarige är skyldig att på begäran av den enskilde snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med denna lag eller föreskrifter som har utfärdats med stöd av lagen. Den personuppgiftsansvarige skall också underrätta tredje man till vilken uppgifterna har lämnats ut om åtgärden, om den enskilde begär det eller om mera betydande skada eller olägenhet för den enskilde skulle kunna undvikas genom en underrättelse. Någon sådan underrättelse behöver dock inte lämnas, om detta visar sig vara omöjligt eller skulle innebära en oproportionerligt stor arbetsinsats.

## Säkerheten vid behandling

7 § Ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige.

Det skall finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet skall det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige och att personuppgiftsbiträdet är skyldigt att vidta de åtgärder som avses i 8 § första stycket.

Om det i annan författning finns särskilda bestämmelser om behandlingen av personuppgifter i polisens verksamhet i frågor som avses i första stycket, skall dessa gälla i stället för vad som sägs i första stycket.

8 § Den personuppgiftsansvarige skall vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna skall åstadkomma en säkerhetsnivå som är lämplig med beaktande av

1. de tekniska möjligheter som finns,
2. vad det skulle kosta att genomföra åtgärderna,
3. de särskilda risker som finns med behandlingen av personuppgifterna och
4. hur pass känsliga de behandlade personuppgifterna är.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde, skall den personuppgiftsansvarige förvissa sig om att personuppgiftsbiträdet kan genomföra de säkerhetsåtgärder som måste vidtas och se till att personuppgiftsbiträdet verkligen vidtar åtgärderna.

9 § Direkt åtkomst till personuppgifter skall vara förbehållen de personer inom polisen som på grund av sina arbetsuppgifter behöver tillgång till uppgifterna.

## 7 kap. Övriga bestämmelser

### Förhållandet till offentlighetsprincipen

1 § Bestämmelserna i denna lag tillämpas inte i den utsträckning det skulle inskränka Rikspolisstyrelsens eller en polismyndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut personuppgifter.

Bestämmelserna hindrar inte heller att Rikspolisstyrelsen eller en polismyndighet arkiverar och bevarar allmänna handlingar eller att arkivmaterial tas om hand av en arkivmyndighet. Bestämmelserna i 2 kap. 2 § tredje stycket gäller inte för Rikspolisstyrelsens eller en polismyndighets användning av personuppgifter i allmänna handlingar.

### Utlämnande av uppgifter

2 § Uppgifter som är nödvändiga för att framställa rättsstatistiken skall lämnas till den myndighet som ansvarar för att framställa sådan statistik.

3 § Uppgifter får lämnas ut till en utländsk myndighet eller en mellanfolklig organisation, om utlämnandet följer av en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt.

Regeringen får meddela föreskrifter om att uppgifter på begäran får lämnas till polis- eller åklagarmyndighet i en stat som är ansluten till Interpol om det behövs för att myndigheten eller organisationen skall kunna förebygga, upptäcka, utreda eller beivra brott.

Uppgifter får vidare lämnas ut enligt vad som framgår av 1 kap. 3 § tredje stycket sekretesslagen (1980:100).

4 § Regeringen får meddela föreskrifter om att uppgifter får lämnas ut även i andra fall än som sägs i 2 och 3 §§.

## Anmälan till tillsynsmyndigheten

### *Anmälningsskyldighet*

5 § Behandling av personuppgifter som är helt eller delvis automatiserad omfattas av anmälningsskyldighet. Den personuppgiftsansvarige skall göra en skriftlig anmälan till tillsynsmyndigheten innan en sådan behandling eller en serie av sådana behandlingar med samma eller liknande ändamål genomförs.

Om den personuppgiftsansvarige utser ett personuppgiftsombud skall detta anmälas till tillsynsmyndigheten. Även ett entledigande av ett personuppgiftsombud skall anmälas till tillsynsmyndigheten.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om undantag från anmälningsskyldigheten enligt första stycket för sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörligt intrång i den personliga integriteten.

### *Om det finns ett personuppgiftsombud skall anmälan göras till personuppgiftsombudet*

6 § Om den personuppgiftsansvarige har anmält till tillsynsmyndigheten att ett personuppgiftsombud utsetts och vem det är, behöver anmälan enligt 5 § första stycket inte göras till tillsynsmyndigheten. Anmälan om sådan behandling av personuppgifter som avses i 5 § första stycket skall då i stället göras till personuppgiftsombudet.

### *Personuppgiftsombudets uppgifter*

7 § Personuppgiftsombudet skall ha till uppgift att självständigt se till att den personuppgiftsansvarige behandlar personuppgifter på ett lagligt och korrekt sätt och i enlighet med god sed samt påpeka eventuella brister för honom eller henne.

Har personuppgiftsombudet anledning att misstänka att den personuppgiftsansvarige bryter mot de bestämmelser som gäller för behandlingen av personuppgifter och vidtas inte rättelse så snart det kan ske efter påpekande, skall personuppgiftsombudet anmäla förhållandet till tillsynsmyndigheten.

Personuppgiftsombudet skall även i övrigt samråda med tillsynsmyndigheten vid tveksamhet om hur de bestämmelser som gäller för behandlingen av personuppgifter skall tillämpas.

**8 §** Personuppgiftsombudet skall föra en förteckning över de behandlingar som den personuppgiftsansvarige genomför och som omfattas av anmälningsskyldighet till tillsynsmyndigheten eller till personuppgiftsombudet. Förteckningen skall omfatta åtminstone de uppgifter som en anmälan enligt 5 § skulle ha innehållit.

**9 §** Personuppgiftsombudet skall hjälpa enskilda att få rättelse när det finns anledning att misstänka att behandlade personuppgifter är felaktiga eller ofullständiga.

#### *Förhandskontroll av särskilt integritetskänsliga behandlingar*

**10 §** Regeringen får meddela föreskrifter om att sådana behandlingar av personuppgifter som innebär särskilda risker för otillbörligt intrång i den personliga integriteten skall för förhandskontroll anmälas till tillsynsmyndigheten enligt 5 § tre veckor i förväg. Om regeringen har meddelat sådana föreskrifter, gäller inte undantaget från anmälningsskyldigheten till tillsynsmyndigheten enligt 6 §.

## Upplysningar till allmänheten om behandlingar som inte anmälts

11 § Den personuppgiftsansvarige skall till var och en som begär det skyndsamt och på lämpligt sätt lämna upplysningar om sådana automatiserade eller andra behandlingar av personuppgifter som inte har anmälts till tillsynsmyndigheten. Upplysningarna skall omfatta det som en anmälan enligt 5 § första stycket skulle ha omfattat. Den personuppgiftsansvarige är dock inte skyldig att lämna ut sekretessbelagda uppgifter eller uppgifter om vilka säkerhetsåtgärder som har vidtagits.

## Skadestånd

12 § Den personuppgiftsansvarige skall ersätta den enskilde för skada och kränkning av den personliga integriteten som en behandling av personuppgifter i strid med denna lag har orsakat.

Ersättningsskyldigheten kan i den utsträckning det är skäligt jämkas, om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne. Detta gäller dock inte vid behandling av personuppgifter enligt konventionen om tillämpning av Schengenavtalet av den 14 juni 1985.

## Överklagande

13 § Tillsynsmyndighetens beslut enligt förordning som har meddelats för verkställighet av denna lag om annat än föreskrifter får överklagas hos allmän förvaltningsdomstol.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Tillsynsmyndigheten får bestämma att dess beslut skall gälla även om det överklagas.



14 § Rikspolisstyrelsens eller en polismyndighets beslut om rättelse och om information som skall lämnas enligt 6 kap. 4 § överklagas till kammarrätten.

---

Denna lag träder i kraft den 1 juli 2003, då polisdatalagen (1998:622) upphör att gälla.

## Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 5 kap 1 och 7 §§, 7 kap. 41 § och 9 kap. 17 § sekretesslagen (1980:100) skall ha följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

### 5 kap.

#### 1 §

Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,
  2. angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,
  3. verksamhet som rör utredning i frågor om näringsförbud,
  4. åklagarmyndighets, polismyndighets, skattemyndighets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott, eller
  5. Finansinspektionens verksamhet som rör övervakning enligt insiderstrafflagen (2000:1086),
- om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till *sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller för-*

För uppgift som hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Det samma gäller uppgift som hänför sig till

utsedda åtgärder motverkas eller den framtida verksamheten skadas. Det samma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar samt sådan underrättelseverksamhet som avses i 2 § lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

sådan *underrättelseverksamhet som bedrivs av polisen*, sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar samt sådan underrättelseverksamhet som avses i 2 § lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, skattemyndighet, Tullverket eller Kustbevakningen med att uppdaga, utreda eller beivra brott samt hos tillsynsmyndighet i konkurs och inom exekutionsväsendet för uppgift som angår misstanke om att en gäldenär har begått brott som avses i 11 kap. brottsbalken eller annat brott som har samband med gäldenärens näringsverksamhet.

I fråga om uppgift i allmän handling som hänför sig till sådan underrättelseverksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

#### 7 §

Sekretess gäller i verksamhet som avser rättslig hjälp på begäran av annan stat för uppgift som hänför sig till

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som angår tvångsmedel,  
om det kan antas att den rättsliga hjälpen begärts under förutsättning att uppgiften inte röjs.

Motsvarande sekretess gäller hos polismyndighet och åklagarmyndighet samt hos Rikspolisstyrelsen, Tullverket och Kustbevakningen, för uppgift i en angelägenhet som avses i 3 § 1 och 6 lagen (2000:344) om Schengens informationssystem. Utan hinder av sekretessen enligt detta stycke får uppgift lämnas ut enligt vad som föreskrivs i *polisdatalagen* (1998:622) och lagen om Schengens informationssystem.

I fråga om uppgift i allmän handling gäller sekretessen i högst fyrtio år.

## 7 kap.

### 41 §

Sekretess gäller hos polismyndighet och åklagarmyndighet, samt hos Rikspolisstyrelsen, Tullverket, Kustbevakningen och Migrationsverket, för uppgift om enskilda personliga förhållanden i en angelägenhet som avser en framställning enligt 3 § lagen (2000:344) om Schengens informationssystem

1. om omhändertagande av en person som har efterlysts för utlämning,

2. om att en person skall nekas tillträde till eller uppehållstillstånd i Schengenstaterna (spärlista),

3. om tillfälligt omhändertagande av en person med hänsyn till dennes eller någon annans säkerhet, samt

4. om dold övervakning eller särskilda kontrollåtgärder, om det inte står klart att uppgiften kan lämnas ut utan att den enskilde eller någon honom närstående lider men.

Sekretess gäller hos myndighet som prövar ansökningar om visering och uppehållstillstånd för uppgift om enskilda personliga förhållanden i en angelägenhet som avser en sådan framställning som avses i första stycket 2 under samma förutsättningar som anges i första stycket.

Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i <i>polisdatalagen</i> (1998:622) och lagen (2000:344) om Schengens informationssystem.	Utan hinder av sekretessen får uppgift lämnas ut enligt vad som föreskrivs i <i>polisdatalagen</i> (0000:00) och lagen (2000:344) om Schengens informationssystem.
---	--

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

## 9 kap.

### 17 §

Sekretess gäller för uppgift om enskilda personliga och ekonomiska förhållanden, om inte annat följer av 18 §

1. i utredning enligt bestämmelserna om förundersökning i brottmål,

2. i angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,

3. i angelägenhet som avser registerkontroll och särskild personutredning enligt säkerhetsskyddslagen (1996:627),

4. i åklagarmyndighets, polismyndighets, skattemyndighets, Statens kriminaltekniska laboratoriums, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,

5. i Statens biografbyrås verksamhet att biträda Justitiekanslern, allmän åklagare eller polismyndighet i brottmål,

6. i register som förs av Rikspolisstyrelsen enligt <i>polisdatalagen</i> (1998:622) eller som annars behandlas där med stöd av samma lag,	6. i register som förs av Rikspolisstyrelsen enligt <i>polisdatalagen</i> (0000:00) eller som annars behandlas där med stöd av samma lag,
--	---

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

8. i register som förs av Riksskatteverket enligt lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar eller som annars behandlas där med stöd av samma lag,

9. i särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 15 kap. 1 §,

10. i register som förs av Tullverket enligt lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet eller som annars behandlas där med stöd av samma lag,

om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon honom närstående lider skada eller men.

Sekretess gäller i verksamhet, som avses i första stycket, för anmälan eller utsaga från enskild, om det kan antas att fara uppkommer för att någon utsätts för våld eller annat allvarligt men om uppgiften röjs.

Utan hinder av sekretessen får en skadelidande, eller den som den skadelidande överlåtits sin rätt till, ta del av en uppgift

1. i en nedlagd förundersökning eller i en förundersökning som avslutats med ett beslut om att åtal inte skall väckas,

2. i en annan brottsutredning som utförts enligt bestämmelserna i 23 kap. rättegångsbalken och som avslutats på annat sätt än med beslut att väcka åtal, med strafföreläggande eller med föreläggande av ordningsbot, eller

3. i en avslutad utredning enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, om den skadelidande, eller den som den skadelidande överlåtits sin rätt till, behöver uppgiften för att kunna få ett anspråk på skadestånd eller på bättre rätt till viss egendom tillgodosett och det inte bedöms vara av synnerlig vikt för den som uppgiften rör eller någon närstående till honom att den inte lämnas ut.

Utan hinder av sekretessen får en uppgift också lämnas ut

1. till enskild enligt vad som föreskrivs i den särskilda lagstiftningen om unga lagöverträdare,

2. till enskild enligt vad som föreskrivs i säkerhetsskyddslagen (1996:627) samt i förordning som har stöd i den lagen,

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, *polisdatalagen* (1998:622), lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar och i lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet samt i förordningar som har stöd i dessa lagar,

3. enligt vad som föreskrivs i lagen (1998:621) om misstankeregister, *polisdatalagen* (0000:00), lagen (1999:90) om behandling av personuppgifter vid skattemyndigheters medverkan i brottsutredningar och i lagen (2001:85) om behandling av personuppgifter i Tullverkets brottsbekämpande verksamhet samt i förordningar som har stöd i dessa lagar,

4. till enskild enligt vad som föreskrivs i 27 kap. 8 § rättegångsbalken.

Utan hinder av sekretessen får polisen på begäran av en enskild som lidit person- eller sakskada vid en trafikolycka lämna uppgift om identiteten hos en trafikant som haft del i olyckan.

I fråga om uppgift i allmän handling gäller sekretessen i högst sjuttio år.

---

1. Denna lag träder i kraft den 1 juli 2003.

2. Äldre bestämmelser om sekretess gäller fortfarande i fråga om uppgifter som hänför sig till tiden före ikraftträdandet.

## Förslag till lag om ändring i säkerhetsskyddslagen (1996:627)

Härigenom föreskrivs att 12, 21 och 22 §§ säkerhetsskyddslagen (1996:627) skall ha följande lydelse

### *Nuvarande lydelse*

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller *polisdatalagen* (1998:622). Med registerkontroll avses också att sådana personuppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller *särskild undersökning i kriminalunderrättelseverksamhet*.

### *Föreslagen lydelse*

#### 12 §

Med registerkontroll avses att uppgifter hämtas från ett register som omfattas av lagen (1998:620) om belastningsregister, lagen (1998:621) om misstankeregister eller *polisdatalagen* (0000.00). Med registerkontroll avses också att sådana personuppgifter hämtas som Rikspolisstyrelsen eller Säkerhetspolisen behandlar utan att det ingår i ett sådant register som avses i första stycket. Med registerkontroll avses dock inte att uppgifter hämtas från en förundersökning eller från en brottsutredning som *handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare*.



## 21 §

Utlämnande av uppgifter vid registerkontroll får omfatta

1. för säkerhetsklass 1 eller 2: varje uppgift som finns tillgänglig om den kontrollerade och, om det är oundgängligen nödvändigt, om make eller sambo, och

2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret, misstankeregistret, *SÄPO-registret* och uppgifter som *annars* behandlas hos Säkerhetspolisen.

2. för säkerhetsklass 3: uppgifter om den kontrollerade i belastningsregistret *och* misstankeregistret *samt* uppgifter om den kontrollerade som behandlas hos Säkerhetspolisen.

## 22 §

Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som *finns i SÄPO-registret* eller *annars* behandlas hos Säkerhetspolisen samt de uppgifter om den kontrollerade som finns i belastningsregistret och i misstankeregistret om dom eller misstanke om brott som avses i

- 3 kap. 1, 2, 5 och 6 §§ brottsbalken,
- 4 kap. 1–6 och 8–9 a §§ brottsbalken,
- 6 kap. 1 och 2 §§ brottsbalken,
- 8 kap. 4–6 §§ brottsbalken,
- 9 kap. 3 och 4 §§ brottsbalken,
- 12 kap. 3 § brottsbalken,
- 13 kap. 1–5 b och 7 §§ brottsbalken,
- 16 kap. 1–3, 5, 6 och 8 §§ brottsbalken,
- 17 kap. 1 § brottsbalken,
- 18 kap. 1 och 3–5 §§ brottsbalken,
- 19 kap. brottsbalken,
- 1 och 3 §§ narkotikastrafflagen (1968:64), och

Vid registerkontroll enligt 14 § får utlämnandet omfatta alla uppgifter om den kontrollerade som behandlas hos Säkerhetspolisen samt de uppgifter om den kontrollerade som finns i belastningsregistret och i misstankeregistret om dom eller misstanke om brott som avses i

– 9 kap. 1 § vapenlagen (1996:67).

Även uppgift om försök och förberedelse till dessa gärningar får lämnas ut.

---

Denna lag träder i kraft den 1 juli 2003.

## Förslag till lag om ändring i lagen (2000:344) om Schengens informationssystem

Härigenom föreskrivs att 5 § lagen (2000:344) om Schengens informationssystem skall ha följande lydelse.

*Nuvarande lydelse*

*Föreslagen lydelse*

### 5 §

Registret skall endast innehålla uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning.

Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *polisdatalagen* (1998:622) eller annan svensk författning.

Rikspolisstyrelsen får registrera uppgifter i SIS endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen (1998:204), *polisdatalagen* (0000:00) eller annan svensk författning.

---

Denna lag träder i kraft den 1 juli 2003.

## Förslag till polisdataförordning

Härigenom föreskrivs följande.

### Inledande bestämmelse

1 § I denna förordning ges kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av polisdatalagen (0000:00).

I förordningen (1970:517) om rättsväsendets informationssystem finns särskilda föreskrifter om automatiserad behandling av personuppgifter i rättsväsendets informationssystem.

### Undantag från gallring

2 § Riksarkivet får, efter samråd med Rikspolisstyrelsen, meddela föreskrifter om att uppgifter som skall gallras enligt 2 kap. 1 § 9, 3 kap. 9 § eller 5 kap. 5 § polisdatalagen (0000:00) får bevaras för historiska, statistiska och vetenskapliga ändamål.

### Behandling av uppgifter om enskilda personer som det inte finns någon misstanke om brott mot

3 § Uppgifter som behandlas enligt 3 kap. 5 § polisdatalagen (0000:00) får lämnas ut till Ekobrottsmyndigheten, Kustbevakningen, en tullmyndighet eller en skattemyndighet endast om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder.

## Spaningsregister

4 § Polismyndigheterna får ha direkt åtkomst till det allmänna spaningsregistret.

Uppgifter ur det allmänna spaningsregistret får lämnas ut till Ekobrottsmyndigheten, Kustbevakningen, en tullmyndighet eller en skattemyndighet endast om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder.

## Register med uppgifter om DNA-analyser i brottmål

5 § Statens kriminaltekniska laboratorium, polismyndigheter och åklagarmyndigheter får ha direkt åtkomst till register med uppgifter om DNA-analyser i brottmål. Polismyndigheterna och åklagarmyndigheternas åtkomst skall dock begränsas till uppgifter om huruvida någon förekommer i register med uppgifter om DNA-analyser i brottmål eller inte.

## Tillsynsmyndighet

6 § Datainspektionen är tillsynsmyndighet enligt polisdatalagen (0000:00).

## Datainspektionens befogenheter

7 § Datainspektionen får i enskilda fall besluta om vilka säkerhetsåtgärder som den personuppgiftsansvarige skall vidta enligt 6 kap. 8 § polisdatalagen (0000:00).

I 10 § finns det bestämmelser om Datainspektionens möjligheter att förena beslutet med vite.

8 § Datainspektionen har rätt att för sin tillsyn på begäran få

1. tillgång till de personuppgifter som behandlas,
2. upplysningar om och dokumentation av behandlingen av personuppgifter och säkerheten vid denna, och
3. tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter.

9 § Om Datainspektionen inte efter begäran enligt 8 § kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får myndigheten vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem.

10 § Om Datainspektionen konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, skall myndigheten genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Går det inte att få rättelse på något annat sätt eller är saken brådskande, får myndigheten vid vite förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på något annat sätt än genom att lagra dem.

Om den personuppgiftsansvarige inte frivilligt följer ett beslut om säkerhetsåtgärder enligt 7 § som vunnit laga kraft, får Datainspektionen föreskriva vite.

11 § Innan Datainspektionen beslutar om vite enligt 9 eller 10 §, skall den personuppgiftsansvarige ha fått tillfälle att yttra sig. Om saken är brådskande, får Datainspektionen dock i avvaktan på yttrandet meddela ett tillfälligt beslut om vite. Det tillfälliga beslutet skall omprövas, när yttrandetiden har gått ut.

Ett vitesföreläggande skall delges den personuppgiftsansvarige.

12 § Datainspektionen får hos Länsrätten i Stockholms län ansöka om att sådana personuppgifter som har behandlats på ett olagligt sätt skall utplånas.

Beslut om utplånande får inte meddelas om det är oskäligt.

## Anmälan till Datainspektionen

13 § Anmälningsskyldigheten enligt 7 kap. 5 § första stycket polisdatalagen (0000:00) gäller inte för behandling av personuppgifter som utförs till följd av Rikspolisstyrelsens eller en polismyndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut allmän handling.

14 § Anmälningsskyldigheten enligt 7 kap. 5 § första stycket polisdatalagen (0000:00) gäller inte för behandling av personuppgifter i löpande text.

15 § Datainspektionen får meddela föreskrifter om undantag från anmälningsskyldigheten enligt 7 kap. 5 § första stycket polisdatalagen (0000:00) för sådana typer av behandlingar som sannolikt inte kommer att leda till otillbörligt intrång i den personliga integriteten.

16 § Datainspektionen skall med automatiserad behandling registrera de behandlingar av personuppgifter som anmälts till inspektionen enligt 7 kap. 5 § första stycket polisdatalagen (0000:00).

## Förhandskontroll

17 § Automatiserad behandling av personuppgifter som ger upplysning om att en person är dömd eller misstänkt för brott skall anmälas för förhandskontroll till Datainspektionen tre veckor i förväg.

Första stycket gäller inte om behandlingen utförs

1. i en polismyndighets diarium över inkomna ärenden,
2. till följd av en polismyndighets skyldighet enligt 2 kap. tryckfrihetsförordningen att lämna ut en allmän handling,
3. till följd av bestämmelserna i arkivlagen (1990:782) eller arkivförordningen (1991:446),

4. enligt förordningen (1970:517) om rättsväsendets informationssystem,
5. enligt de särskilda föreskrifterna om register i 5 kap. polisdatalagen (0000:00),
6. i en förundersökning eller i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare,
7. i ett ärende som rör en enskild person hos en polismyndighet,
8. hos Säkerhetspolisen eller
9. i löpande text och endast avser enstaka personuppgifter.

### **Underrättelseskyldighet**

18 § Justitiekanslern och en domstol som förordnar om beslag på skrift på vilken tryckfrihetsförordningen skall tillämpas eller på en film eller annan upptagning av ljud eller bilder på vilken yttrandefrihetsgrundlagen skall tillämpas skall underrätta Rikspolisstyrelsen om beslutet. Detsamma gäller om beslaget hävs eller förfaller eller om domstolen förordnar om att konfiskering av en sådan skrift eller upptagning skall verkställas.

### **Utlämnande av uppgifter**

19 § Rikspolisstyrelsen får lämna ut uppgifter om efterlysta personer och avlägsnanden ur landet samt om beslut som har samband därmed till Regeringskansliet, Arbetsmarknadsstyrelsen, Migrationsverket, Utlänningsnämnden, länsstyrelserna, polis- och åklagarmyndigheterna, Kustbevakningen, tullmyndigheterna, de svenska beskickningarna och konsulaten samt de centrala utlänningsmyndigheterna i Danmark, Finland, Island och Norge.



20 § Uppgifter som behandlas enligt polisdatalagen (0000:00) får, om det är förenligt med svenska intressen, lämnas ut till

1. utländsk underrättelse- eller säkerhetstjänst och
2. polis- eller åklagarmyndighet i en stat som är ansluten till Interpol, om det behövs för att myndigheten eller organisationen skall kunna förebygga, upptäcka, utreda eller beivra brott.

### Bemyndiganden

21 § Datainspektionen får i fråga om automatiserad behandling av personuppgifter meddela närmare föreskrifter om

1. i vilka fall behandling av personuppgifter är tillåten,
2. vilka krav som ställs på den personuppgiftsansvarige,
3. i vilka fall användning av personnummer eller samordningsnummer är tillåten,
4. vad en anmälan eller ansökan till en personuppgiftsansvarig skall innehålla,
5. vilken information som skall lämnas till registrerade och hur informationen skall lämnas,
6. anmälan till inspektionen och förfarandet när anmälda uppgifter har ändrats.

22 § Rikspolisstyrelsen får efter samråd med Datainspektionen meddela de ytterligare föreskrifter som behövs för verkställighet av polisdatalagen (0000:00) och denna förordning.

---

Denna förordning träder i kraft den 1 juli 2003, då polisdataförordningen (1999:81) upphör att gälla.

## Förslag till förordning om ändring i sekretessförordningen (1980:657)

Härigenom föreskrivs att 5 § sekretessförordningen (1980:657) skall ha följande lydelse.

### *Nuvarande lydelse*

#### 5 §

Följande myndigheter är i den utsträckning som framgår nedan undantagna från registreringskyldigheten enligt 15 kap. 1 § första stycket sekretesslagen (1980:100).

---

### Myndigheter

---

Rikspolisstyrelsen	handlingar som utgör underlag för belastningsregistret, misstankeregistret, <i>kriminalundermåttelseregister</i> , DNA-register, fingeravtrycksregister, signalementsregister och andra register angående brott, <i>handlingar som utgör underlag för sådan särskild undersökning som avses i 14–16 §§ polisdatalagen (1998:622)</i> , framställningar om fingeravtrycksundersökning samt statistiskt primärmaterial
åklagarmyndigheterna	utdrag ur folkbokföringsdatabasen, utdrag ur belastningsregistret, misstankeregistret och

andra register som förs med stöd av *polisdatalagen* (1998:622), utdrag ur körkortsregistret samt rekvisitioner av sådana utdrag

*Föreslagen lydelse*

5 §

Följande myndigheter är i den utsträckning som framgår nedan undantagna från registreringskyldigheten enligt 15 kap. 1 § första stycket sekretesslagen (1980:100).

---

*Sekretessbelagda handlingar som inte behöver registreras*

Rikspolisstyrelsen

handlingar som utgör underlag för belastnings registret, misstankeregistret, DNA-register fingeravtrycksregister, signalementsregister och andra register angående brott, framställningar om fingeravtrycksundersökning samt statistiskt primärmaterial

---

åklagarmyndigheterna

utdrag ur folkbokföringsdatabasen, utdrag ur belastningsregistret, misstankeregistret och andra register som förs med stöd av *polisdatalagen* (0000:00), utdrag ur körkorts-

registret samt rekvisitioner av  
sådana utdrag

---

Denna förordning träder i kraft den 1 juli 2003.

## Förslag till förordning om ändring i förordningen (1989:773) med instruktion för Rikspolisstyrelsen

Härigenom föreskrivs att 5 b § förordningen (1989:773) med instruktion för Rikspolisstyrelsen skall ha följande lydelse.

### *Nuvarande lydelse*

Säkerhetspolisen skall i enlighet med 11 § förordningen (1996:730) med instruktion för Registernämnden lämna utdrag av eller upplysning om

1. *innehållet i SÄPO-registret och*

2. *de övriga uppgifter Säkerhetspolisen behandlar enligt polisdatalagen (1998:622).*

### *Föreslagen lydelse*

#### 5 b §

Säkerhetspolisen skall i enlighet med 11 § förordningen (1996:730) med instruktion för Registernämnden lämna utdrag av eller upplysning om de uppgifter Säkerhetspolisen behandlar enligt *polisdatalagen (0000:00)*.

---

Denna förordning träder i kraft den 1 juli 2003.

## Förslag till förordning om ändring i folkbokföringsförordningen (1991:749)

Härigenom föreskrivs att 5 § folkbokföringsförordningen (1991:749) skall ha följande lydelse.

### *Nuvarande lydelse*

#### 5 §

Samordningsnummer enligt 18 a § folkbokföringslagen (1991:481) får tilldelas för de ändamål och på begäran av de myndigheter som anges nedan.

### *Ändamål*

- |   |   |
|---|---|
| 1. Registrering i skatteregister  | Rikspolisstyrelsen, polismyndigheten, åklagarmyndigheten och allmänna domstolar |
| 2. Registrering i belastningsregister, misstankeregister, och register som förs enligt <i>polisdatalagen</i> (1998:622) eller i rättsväsendets informationssystem |   |
| 3. Utfärdande av pass och registrering i passregistret  | Passmyndigheten   |
| 4. Registrering i socialförsäkringsregister   | Allmänna försäkringskassan  |
| 5. Sjömansregistrering  | Sjöfartsverket  |
| 6. Registrering i körkorts- och bilregistret  | Länsstyrelsen och Vägverket   |
| 7. Registrering i register över totalförsvarspliktiga   | Totalförsvarets pliktverk   |

Samordningsnummer får på begäran av Regeringskansliet även tilldelas en person som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall.

Tilldelning enligt första stycket 1 och 2 får ske även om den enskildes identitet inte med säkerhet kunnat fastställas av den myndighet som begär tilldelningen.

Samordningsnummer tilldelas av den skattemyndighet som Riksskatteverket bestämmer.

### *Föreslagen lydelse*

#### 5 §

Samordningsnummer enligt 18 a § folkbokföringslagen (1991:481) får tilldelas för de ändamål och på begäran av de myndigheter som anges nedan.

### *Myndigheter*

- |  |   |
|--|---|
| 1. Registrering i skatteregister   | Skattemyndigheten   |
| 2. Registrering i belastningsregister, misstankeregister, och register som förs enligt <i>polisdatalagen</i> (0000:00) eller i rättsväsendets informationssystem | Rikspolisstyrelsen, polismyndigheten, åklagarmyndigheten och allmänna domstolar |
| 3. Utfärdande av pass och registrering i passregistret   | Passmyndigheten   |
| 4. Registrering i socialförsäkringsregister  | Allmänna försäkringskassan  |
| 5. Sjömansregistrering   | Sjöfartsverket  |
| 6. Registrering i körkort- och bilregistret  | Länsstyrelsen och Vägverket   |
| 7. Registrering i register över totalförsvarspliktiga  | Totalförsvarets pliktverk   |

Samordningsnummer får på begäran av Regeringskansliet även tilldelas en person som omfattas av lagen (1976:661) om immunitet och privilegier i vissa fall.

Tilldelning enligt första stycket 1 och 2 får ske även om den enskildes identitet inte med säkerhet kunnat fastställas av den myndighet som begär tilldelningen.

Samordningsnummer tilldelas av den skattemyndighet som Riksskatteverket bestämmer.

---

Denna förordning träder i kraft den 1 juli 2003.



## Förordning om ändring i förordningen (1996:730) med instruktion för Registernämnden

Härigenom föreskrivs att 1 och 11 §§ förordningen (1996:730) med instruktion för Registernämnden skall ha följande lydelse.

### *Nuvarande lydelse*

### *Föreslagen lydelse*

#### 1 §

Registernämnden har till uppgift att i ärenden om registerkontroll enligt säkerhetsskyddslagen (1996:627) pröva frågor om utlämnande av

1. uppgifter från register som omfattas av lagen (1998:620) om belastningsregister,

2. uppgifter från register som omfattas av lagen (1998:621) om misstankeregister,

3. uppgifter från register som omfattas av *polisdatalagen* (1998:622), eller

4. övriga uppgifter som Rikspolisstyrelsen eller Säkerhetspolisen behandlar enligt polisdatalagen om de inte ingår i en förundersökning *eller särskild undersökning i kriminalunderrättelseverksamhet.*

3. uppgifter från register som omfattas av *polisdatalagen* (0000:00), eller

4. övriga uppgifter som Rikspolisstyrelsen eller Säkerhetspolisen behandlar enligt polisdatalagen om de inte ingår i en förundersökning *eller i en brottsutredning som handläggs enligt 23 kap. 22 § rättegångsbalken eller enligt 31 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare.*

Nämnden skall pröva frågor om utlämnande av uppgifter även i sådana fall som avses i 10 § förordningen (1989:149) om bevakningsföretag m.m.

Nämnden skall vidare granska Säkerhetspolisens behandling av uppgifter enligt *polisdatalagen (1998:622)*, särskilt med avseende på 5 § *polisdatalagen*.

Nämnden skall vidare granska Säkerhetspolisens behandling av uppgifter enligt *polisdatalagen (0000:00)*, särskilt med avseende på 3 kap. 1 § *polisdatalagen*.

## 11 §

För fullgörandet av sin tillsynsuppgift enligt 1 § tredje stycket har nämnden rätt att få del av

1. *uppgifter ur SÄPO-registret och*

2. *de övriga uppgifter Säkerhetspolisen behandlar enligt polisdatalagen (1998:622).*

De uppgifter Säkerhetspolisen behandlar enligt *polisdatalagen (0000:00)*.

---

Denna förordning träder i kraft den 1 juli 2003.

## Förteckning över de remissinstanser som yttrat sig över Polisdatautred- ningens betänkande

1. Riksdagens ombudsmän
2. Justitiekanslern
3. Domstolsverket
4. Riksåklagaren
5. Ekobrottsmyndigheten
6. Rikspolisstyrelsen
7. Registernämnden
8. Statens kriminaltekniska laboratorium
9. Kriminalvårdsstyrelsen
10. Brottsförebyggande rådet
11. Brottsoffermyndigheten
12. Datainspektionen
13. Statskontoret
14. Statistiska centralbyrån
15. Försvarsmakten
16. Socialstyrelsen
17. Tullverket
18. Riksrevisionsverket
19. Riksarkivet
20. Svea hovrätt
21. Malmö tingsrätt
22. Umeå tingsrätt
23. Kammarrätten i Jönköping

24. Uppsala universitet, Juridiska fakulteten
25. Lunds universitet, Juridiska fakulteten
26. Länsstyrelsen i Stockholms län
27. Länsstyrelsen i Östergötlands län
28. Länsstyrelsen i Kronobergs län
29. Länsstyrelsen i Gotlands län
30. Länsstyrelsen i Skåne län
31. Länsstyrelsen i Västra Götalands län
32. Länsstyrelsen i Örebro län
33. Länsstyrelsen i Gävleborgs län
34. Länsstyrelsen i Jämtlands län
35. Länsstyrelsen i Västerbottens län
36. Sveriges advokatsamfund
37. Sveriges domareförbund

# Kustbevakningens framställan om åtkomst till belastningsregistret och misstankeregistret

-----

## **Förordningen (1999:1134) om belastningsregister**

10 § 18. *Kustbevakningen för verksamhet för att förebygga, upptäcka och utreda brott.*

19 § Polismyndigheter, Skatteverket, Tullverket, *Kustbevakningen*, åklagarmyndigheter, kriminalvårdsmyndigheter, Migrationsverket och allmänna domstolar får ha direktåtkomst till uppgifter ur belastningsregistret.

Direktåtkomsten skall begränsas till att endast gälla sådana uppgifter som myndigheterna har rätt att få ut enligt lagen (1998:620) om belastningsregister eller denna förordning.

-----

**Förordningen (1999:1135) om misstankeregister**

3 § 12. *Kustbevakningen för att samordna förundersökningar mot en person och för att förebygga, upptäcka och utreda brott.*

6 § Polismyndigheter, Skatteverket, Tullverket, *Kustbevakningen*, åklagarmyndigheter och Migrationsverket får ha direktåtkomst till uppgifter ur misstankeregister.

Direktåtkomsten skall begränsas till att endast gälla sådana uppgifter som myndigheterna har rätt att få ut enligt lagen (1998:621) om misstankeregister eller denna förordning.

## Förteckning över de remissinstanser som yttrat sig över Kustbevakningens framställan

1. Åklagarmyndigheten
2. Rikspolisstyrelsen
3. Säkerhetspolisen
4. Registernämnden
5. Datainspektionen





# Polisens register

## Register som regleras särskilt i polisdatalagen

### Kriminalunderrättelseregister

*Polisdatalagens och polisdataförordningens bestämmelser om kriminalunderrättelseregister*

Med underrättelseverksamhet förstås i polisdatalagen den polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap. rättegångsbalken. Med kriminalunderrättelseverksamhet avses annan underrättelseverksamhet än den som bedrivs av Säkerhetspolisen. För SÄPO-registret innehåller lagen särskilda bestämmelser (se nedan). Bestämmelser om kriminalunderrättelseverksamhet finns i 14–21 §§ polisdatalagen.

I kriminalunderrättelseverksamhet får för det första automatiserad behandling av personuppgifter förekomma i s.k. *särskilda undersökningar*. Sådana får inledas efter särskilt beslut om det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas. Undersökningarna sker med syfte att ge underlag för beslut om förundersökning eller för beslut om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. I särskilda undersökningar får även uppgifter om icke misstänkta personer behandlas, men uppgifterna måste förses med upplysning om att personen inte är misstänkt. Som exempel på en särskild undersökning kan nämnas den undersökning som gjordes

inför Europeiska rådets möte i Göteborg den 14–16 juni 2001 vid Polismyndigheten i Västra Götaland (SOU 2002:122 s. 258 f).

Personuppgifter får också behandlas inom ramen för *kriminalunderrättelseregister*. Ett kriminalunderrättelseregister får föras för att ge underlag för beslut om särskilda undersökningar avseende allvarlig brottslig verksamhet eller för att underlätta tillgången till allmänna uppgifter med anknytning till underrättelseverksamhet. Kriminalunderrättelseregister får föras av Rikspolisstyrelsen eller av en polismyndighet. Den myndighet som för registret är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Ett kriminalunderrättelseregister får innehålla uppgifter som kan hänföras till en enskild person endast om uppgifterna ger anledning att anta att allvarlig brottslig verksamhet har utövats eller kan komma att utövas. Med allvarlig brottslig verksamhet menas enligt 3 § polisdatalagen verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver. Det krävs vidare att den person som avses med uppgifterna skäligen kan misstänkas för att ha utövat eller komma att utöva den allvarliga brottsliga verksamheten. Uppgifter om transportmedel eller varor som kan antas ha samband med allvarlig brottslig verksamhet eller om hjälpmedel som kan ha använts i samband med sådan verksamhet får dock registreras, även om uppgifterna kan hänföras till en enskild person som det inte finns någon misstanke mot. Uppgifterna ska då föras med upplysning om att det inte finns några misstankar mot denne.

Lagen talar om vilka uppgifter som får finnas i ett kriminalunderrättelseregister. Ett sådant register får endast innehålla

- upplysningar om varifrån den registrerade uppgiften kommer och om uppgiftslämnarens trovärdighet,
- identifieringsuppgifter,
- uppgifter om särskilda bestående fysiska kännetecken,
- de omständigheter och händelser som ger anledning att anta att den registrerade utövat eller kan komma att utöva allvarlig brottslig verksamhet,
- uppgifter om varor, brottshjälpmedel och transportmedel,

- ärendenummer och
- hänvisning till en särskild undersökning där uppgifter om den registrerade behandlas och till register som förs av polis- och tullmyndighet i vilket uppgifter om den registrerade förekommer.

Uppgifter i ett kriminalunderrättelseregister om en registrerad person ska gallras senast tre år efter det att uppgifter om att denne skäligen kan misstänkas för att ha utövat eller komma att utöva allvarlig brottslig verksamhet senast infördes. Om det dessförinnan har inletts en särskild undersökning som rör den registrerade personen, får uppgifterna stå kvar tills undersökningen har avslutats. Regeringen, eller den myndighet som regeringen bestämmer, får vidare meddela föreskrifter om att uppgifter får bevaras för historiska, statistiska och vetenskapliga ändamål.

Rikspolisstyrelsen, polismyndigheterna och Ekobrottsmyndigheten får enligt polisdataförordningen ha direkt åtkomst till kriminalunderrättelseregistren. Åtkomsten till registren ska förbehållas de personer som på grund av sina arbetsuppgifter behöver tillgång till information om sådana uppgifter som behandlas i registren. Vid Ekobrottsmyndigheten får endast polisman och annan person som deltar i polisiärt arbete, med undantag för åklagare, ha direktåtkomst till kriminalunderrättelseregistren.

Uppgifter ur ett kriminalunderrättelseregister får lämnas ut till Kustbevakningen, Tullverket eller Skatteverket. Utlämnande får dock endast ske om uppgiften kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder.

### **Det centrala kriminalunderrättelseregistret**

Det centrala kriminalunderrättelseregistret utgör en nationell, gemensam databas som polismyndigheterna och Rikspolisstyrelsen har tillgång till. De enheter som bedriver kriminalunderrättelsetjänst har därigenom ett system för att lagra uppgifter för

att kunna återfinna handlingar. Endast sådana befattningshavare som är knutna till enheter eller rotlar som sysslar med kriminalunderrättelsetjänst har behörighet att behandla uppgifter i registret.

Innehållet i det centrala kriminalunderrättelseregistret består av underrättelseinformation som kommit in till en underrättelserotel eller Rikspolisstyrelsen från polismän, från allmänheten, andra myndigheter eller internationella organisationer. Informationen kan också ha kommit fram vid det interna arbetet på roteln eller genom underrättelser från något annat land.

I det centrala kriminalunderrättelseregistret finns personuppgifter som avser personer vilka skäligen kan misstänkas för att de kan komma att utöva, utövar eller har utövat allvarlig brottslig verksamhet. Misstankarna behöver inte avse konkreta brott. Registret innehåller även uppgifter om transportmedel och hjälpmedel som förekommer i allvarlig brottslig verksamhet. I de fall där dessa uppgifter kan hänföras till en person som det inte föreligger någon misstanke mot, förses uppgifterna med en upplysning om detta.

### **Register med uppgifter om DNA-analyser**

Resultatet av prov för DNA-analys som tagits med stöd av bestämmelserna om kroppsbesiktning i 28 kap. rättegångsbalken får under vissa förutsättningar registreras i register som förs med stöd av polisdatalagen. Bestämmelser om dessa register finns i 22–28 §§ polisdatalagen.

Med stöd av polisdatalagen för Rikspolisstyrelsen tre olika register; DNA-register, utredningsregister och spårregister. DNA-registret innehåller DNA-profiler från personer som dömts till annan påföljd än enbart böter. Utredningsregister innehåller DNA-profiler från personer som är skäligen misstänkta för brott på vilket fängelse kan följa. Spårregister innehåller uppgifter om DNA-analyser som har gjorts under utredning av ett brott och som inte kan hänföras till en identifierbar person.

Rikspolisstyrelsen är personuppgiftsansvarig för samtliga register. Registren förs hos Statens kriminaltekniska laboratorium.

Uppgifter om en person i DNA-registret ska gallras när de inte längre behövs och senast när uppgifterna om den registrerade har gallrats ur belastningsregistret. Uppgifterna i utredningsregister ska gallras när förundersökning eller åtal läggs ned, åtal ogillas eller åtal bifalls men påföljden bestäms till enbart böter. Uppgifter i spårregister ska gallras när de inte längre behövs och senast trettio år efter registreringen.

Statens kriminaltekniska laboratorium, polismyndigheter och Åklagarmyndigheten får ha direkt åtkomst till register med uppgifter om DNA-analyser i brottmål. Polismyndigheternas och Åklagarmyndighetens åtkomst är dock begränsad till uppgifter om huruvida någon förekommer i ett sådant register.

### **Fingeravtrycks- och signalementsregister**

Enligt 28 kap. 14 § rättegångsbalken samt förordningen (1992:824) om fingeravtryck m.m. ska fingeravtryck och fotografi alltid tas av den som häktats. I vissa uppräknade fall ska fingeravtryck och fotografi också tas av den som är anhållen. Fingeravtrycket och fotografiet ska enligt 7 § förordningen skyndsamt sändas till Rikspolisstyrelsen tillsammans med en beskrivning av personen.

Rikspolisstyrelsen för ett fingeravtrycksregister och ett signalements- och känneteckensregister med stöd av tillstånd från Datainspektionen från år 1976. Enligt övergångsbestämmelserna till polisdatalagen ska datalagen (1973:289) tillämpas på personregister som den 24 oktober 1998 fördes med stöd av Datainspektionens tillstånd. Övergångsbestämmelserna har förlängts flera gånger och föreslås i propositionen Övergångsbestämmelserna till polisdatalagen (prop. 2007/08:6) förlängas ytterligare till den 31 december 2008. Fingeravtrycksregistret och signalements- och känneteckensregistret förs således i dag med stöd av övergångsbestämmelserna till polisdatalagen.

Eftersom registren fortfarande förs med stöd av lagens övergångsbestämmelser tillämpas inte bestämmelserna i 29–31 §§ polisdatalagen om fingeravtrycks- och signalementsregister på de aktuella registren. Bestämmelserna behandlar bl.a. sådana registers ändamål och innehåll. Uppgifter får behandlas för att underlätta identifiering av personer i samband med brott. De får också användas för identifiering av okända personer i andra fall. De får vidare behandlas i förundersökningar och särskilda undersökningar. Bestämmelserna i polisdatalagen om ändamål och innehåll överensstämmer i stort med den hittillsvarande användningen av ifrågavarande register.

Polisdatalagen innehåller även en bestämmelse om gallring. Där föreskrivs att uppgifter i fingeravtrycks- och signalementsregister om en misstänkt person ska gallras när förundersökning eller åtal mot personen läggs ned eller när åtal mot personen ogillas. Uppgifterna får dock bevaras längre om andra uppgifter om den registrerade ska behandlas med stöd av polisdatalagens regler om behandling av uppgifter om kvarstående misstankar. Om den registrerade döms, ska uppgifterna gallras senast då uppgifterna gallras ur belastningsregistret. Datainspektionen har genom beslut den 1 december 2005 och den 20 juni 2006 meddelat gallringsbestämmelser för fingeravtrycksregistret respektive signalements- och känneteckensregistret. Bestämmelserna för fingeravtrycksregistret överensstämmer i sak med polisdatalagens bestämmelse om gallring medan bestämmelserna för signalements- och känneteckensregistret är något annorlunda utformade. I sistnämnda bestämmelser varierar gallringstiden beroende på det misstänkta brottets svårhetsgrad.

## **Andra centrala system**

### **Det allmänna spaningsregistret**

Det allmänna spaningsregistret förs av Rikspolisstyrelsen med tillstånd av Datainspektionen enligt beslut den 18 maj 1977. Re-

gistret förs i dag med stöd av övergångsbestämmelserna till polisdatalagen. Registret ska enligt sin ändamålsbeskrivning lagra och systematisera uppgifter med anknytning till misstänkt eller konstaterad brottslighet för att användas i polisens spanande och brottsutredande verksamhet. Uppdatering av registren ska ske dels av Rikspolisstyrelsen, dels av den lokala polisorganisationen. Enligt ändamålsbeskrivningen ska för uppdateringen företrädesvis användas terminaler. Terminalanvändarna ska kunna initiera systematiseringar och sammanställningar av registrerade uppgifter.

Det allmänna spaningsregistret syftar till att bygga upp kunskaper om och kring personer som misstänks för brott. Registret utgår från misstänkta gärningsmän. En person registreras i det allmänna spaningsregistret om det finns misstanke om att han eller hon begått ett brott. Uppgifterna i registret kommer från brottsanmälningar och förundersökningsprotokoll, men registrering kan också ske på grund av trovärdiga tips från t.ex. personal inom socialförvaltningen.

Det är ett krav för registrering att det alltid finns en grundhandling varifrån den registrerade uppgiften är hämtad. En referens till denna grundhandling ska antecknas i registret tillsammans med uppgiften. På grundhandlingen antecknas vem som fattat beslut om registreringen och vem som rent faktiskt utfört registreringen.

Olika uppgifter om den misstänkte får registreras. Det som bl.a. får registreras är namn och personnummer, alternativa förnamn och efternamn, adresser där personen brukar vistas, speciella fysiska kännetecken, intressenter (alla som bidrar med uppgifter om personen) och senaste händelse inom kriminalvården. Registret innehåller också andra uppgifter kopplade till personen. Det registreras brottstyper som personen ägnar sig åt (hans modus operandi), händelseanteckningar som rör tidigare brottsmisstankar, anknytning till andra personer och spaningsinformation rörande brottsmisstankar.

En speciell typ av noteringar i registret är de så kallade A-markeringarna och Y-markeringarna. En A-markering för en

misstänkt person betyder att personen är synnerligen allvarligt brottsbelastad. A-markeringar sätts enbart av Rikskriminalpolisen. En Y-markering talar om att den misstänkte bedöms vara yrkeskriminell. Denna markering sätts av de lokala polismyndigheterna.

Vid sökningar i registret kan man variera mellan ett eller flera sökbegrepp. Dessa sökbegrepp kan dock inte varieras helt fritt utan det finns begränsningar i sökmöjligheterna. Man kan t.ex. söka på ålder och något speciellt fysiskt kännetecken och på det viset få fram alla personer som svarar mot de sökbegreppen. Registret innehåller också uppgifter om personer med anknytning till den misstänkte. Dessa ”anknytningspersoner” behöver inte vara misstänkta för brott för att registrering ska få ske. Deras namn är dock inte sökbara i registret, om de inte själva är misstänkta för brott.

Det allmänna spaningsregistret innehåller omkring 100 000 sökbara personer. Antalet personer har sedan lång tid legat konstant på den nivån.

Uppgifter i registret gallras efter 18 månader, tre år eller fem år beroende på brottets svårighetsgrad. Uppgifter får bevaras längre om en ny uppgift om personen antecknas före gallringstidens utgång. A- eller Y-markering utgör hinder mot gallring. Gallringen sker automatiskt med hjälp av ett särskilt gallringsprogram.

All tillgång till uppgifter i registret för enskilda befattningshavare styrs av personligt tilldelad behörighet. Polismyndigheterna beslutar om vilka personer som ska ha denna behörighet. Ett ytterligare begränsat antal personer har behörighet att föra in uppgifter i registret. Enligt 14 § polisdataförordningen får polismyndigheter och Ekobrottsmyndigheter ha direktåtkomst till det allmänna spaningsregistret. Uppgifter ur registret får enligt 15 § lämnas till Tullverket, Kustbevakningen och Skatteverket, om uppgifterna kan antas ha särskild betydelse för en pågående undersökning i myndighetens brottsutredande verksamhet eller för andra brottsbekämpande åtgärder.



## Det centrala brottsspaningsregistret

Det centrala brottsspaningsregistret inrättades med stöd av kungörelsen (1970:517) om rättsväsendets informationssystem (RI-förordningen). Därefter har Datainspektionen beslutat föreskrifter den 21 december 1976, 25 januari 1978, 2 oktober 1984 och 15 juni 1994 angående behandlingen av uppgifter i registret. Bestämmelserna i polisdatalagen och personuppgiftslagen är i dag tillämpliga på registret.

Ändamålet med det centrala brottsregistret är att skapa ett särskilt brottsregister över anmälda allvarligare brott som kan utnyttjas i brottsspanings- och brottsutredningsverksamhet samt i annan därmed jämförlig polisiär verksamhet. Även mindre allvarliga brott får dock registreras.

Det centrala brottsspaningsregistret innehåller uppgifter om anmälda brott, tillvägagångssätt, signalement beträffande personer som setts på brottsplatsen, motsvarande uppgifter om fordon och spår från brottsplatsen m.m. Registret skiljer sig från det allmänna spaningsregistret genom att det förra utgår från brott och inte från misstänkta gärningsmän. Det kan sägas vara ett register över modus operandi. Uppgifter till registret kommer från systemet rationell anmälningsrutin (RAR, se nedan). Det är framför allt allvarliga brott som registreras. Rikspolisstyrelsen har föreskrivit vilka brott som ska antecknas i centrala brottsregistret. Personuppgifterna i registret utgörs av noteringar om misstänkta gärningsmän.

Registret innehåller noteringar om ungefär 129 000 brott. Det används inom polisen för att t.ex. söka liknande brott eller brott som har förövats av samma person. Ibland kan man finna att personer med samma signalement har syntts vid flera brott av samma typ.

All tillgång till uppgifter ur det centrala brottsspaningsregistret styrs av personligt tilldelad behörighet. Polismyndigheterna beslutar själva om vilka som ska ha denna behörighet. Ett mindre antal personer har behörighet att föra in uppgifter i registret.

### Beslags- och analysregister

Beslags- och analysregistren förs av Rikspolisstyrelsen och polismyndigheterna med tillstånd meddelat av Datainspektionen den 6 november 1987. Registren förs i dag med stöd av övergångsbestämmelserna till polisdatalagen.

Ändamålet med registren ska enligt tillståndet vara

- dels underlag för undersökning av modus operandi och profiler av strategisk och taktisk betydelse för den nationella och internationella narkotikabekämpningen,
- dels rapportering av analysresultat avseende beslagtagna narkotika samt framställning av statistik.

Syftet med systemet är att analysresultat snabbt ska kunna bli tillgängliga för Rikspolisstyrelsen och respektive narkotikarotet via bildskärm. Analysdelen av registren innehåller uppgift om det misstänkta preparatet och motsvarande beslagsnummer. Enligt Datainspektionen får delregistren anses förda för respektive myndighets verksamhet, vilket innebär att myndigheterna ska vara personuppgiftsansvariga för sina egna register.

I registret antecknas uppgifter om bl.a. modus operandi, transportmedel, eventuell beslagtagna valuta och eventuella vapen. Dessutom ska den beslagtagna narkotikan beskrivas samt var och när den anträffades.

### Finanspolisens analys- och spaningsregister

Finanspolisens analys- och spaningsregister inrättades under år 1994 med stöd av ett tillstånd från regeringen den 16 december 1993. Datainspektionen meddelade den 27 januari 1994 föreskrifter för registret. Registret omfattas inte av övergångsbestämmelserna i polisdatalagen eftersom det inte fördes med tillstånd från Datainspektionen utan med stöd av ett tillstånd från regeringen. Bestämmelserna i personuppgiftslagen och polisdatalagen är därmed ensamt tillämpliga på registret.

Registret består av två delregister, Finanspolisens analys- och förspaningsregister samt Finanspolisens diarium. Finanspolisens analys- och förspaningsregister utgör ett hjälpmedel i Rikspolisstyrelsens spanings- och analysverksamhet i ärenden hos Finanspolisen som avser sådana förfaranden som anges i lagen (1993:768) om åtgärder mot penningtvätt (penningtvättslagen). En del av uppgifterna i registret har underrättelsekaraktär. Registret används även för framställning av statistik. Ändamålet med Finanspolisens diarium är att utgöra ett diarium enligt 15 kap. sekretesslagen.

Registret får innehålla uppgifter som rapporteras till Rikspolisstyrelsen enligt penningtvättslagens bestämmelser eller från andra polismyndigheter eller motsvarande utländska samarbetspartners eller som framkommit i Finanspolisens spanings- och analysverksamhet, under förutsättning att det finns skäl att anta att transaktionen avser medel som härrör från ett brottsligt förvärv av allvarigare slag. Registret får även innehålla uppgifter som rapporteras till Rikspolisstyrelsen från Tullverket eller verkets utländska samarbetspartners i deras brottsbekämpande verksamhet, under förutsättning att det finns skäl att anta att transaktionen avser medel som härrör från ett brottsligt förvärv av allvarigare slag. Vidare får registret innehålla uppgifter som härrör från andra källor än vad som sägs ovan om de bedöms vara av betydelse för utredningen av det aktuella ärendet.

### **Digitalt referensbibliotek över barnpornografiska framställningar**

Barnpornografiutredningen föreslog i sitt betänkande Barnpornografifrågan (SOU 1997:29) att en internationellt tillgänglig databank med barnpornografiska framställningar skulle inrättas i Sverige med Rikspolisstyrelsen som huvudansvarig.

Efter en ansökan från Rikspolisstyrelsen beslutade regeringen den 18 september 1997 att det hos Rikspolisstyrelsen skulle inrättas och föras ett personregister med namnet Digitalt referens-

bibliotek över barnpornografiska framställningar. Ändamålet med registret är enligt regeringsbeslutet att utföra bildanalys i brottsutredningar samt att bistå utländska brottsutredande myndigheter med uppgifter om bildanalys i brottsutredningar. Innehållet i registret ska bestå av kopior av barnpornografiska framställningar som tagits i beslag. Registret får också innehålla barnpornografiska framställningar som överlämnats av en utländsk brottsutredande myndighet. Registret får även innehålla uppgifter om var framställningen tagits i beslag.

Registret omfattas inte av övergångsbestämmelserna i polisdatalagen eftersom det inte förs med tillstånd av Datainspektionen utan med stöd av ett regeringsbeslut. Bestämmelserna i personuppgiftslagen och polisdatalagen är därför numera ensamt tillämpliga på behandlingen av personuppgifter i registret. Till följd av detta har en särskild undersökning enligt polisdatalagens bestämmelser inletts som omfattar den behandling av personuppgifter som är nödvändig i arbetet med att förebygga och beivra brott relaterade till barnpornografi.

### **Personefterlysnings- och U-boksregistret**

Personefterlysnings- och U-boksregistret utgör det s.k. EPU-systemet (efterlysta personer och U-boken). Systemet förs med stöd av tillstånd från Datainspektionen den 11 oktober 1977. Registret förs i dag med stöd av övergångsbestämmelserna till polisdatalagen. Registret består av två delregister; EP-delen och U-boksdelen.

Ändamålet med registret är enligt tillståndet att

- dels i enlighet med efterlysningskungörelsen (1969:293) föra register över efterlysningar och utge förteckningar över gällande efterlysningar och över efterlysningar som har återkallats,
- dels i enlighet med 5 § andra stycket lagen (1965:94) om polisregister m.m. sammanställa och sända ut uppgifter

från polisregister om avlägsnanden ur riket och beslut som har samband därmed,

- dels använda de registrerade uppgifterna vid utredningar i passärenden enligt passkungörelsen (1941:836) och vid passkontroll enligt utlänningskungörelsen (1969:136) samt vid annan därmed jämförlig polisiär verksamhet.

Av 2 § efterlysningskungörelsen framgår att efterlysning verkställs genom att uppgifter införs i ett register över efterlysta personer som förs med ADB. Rikspolisstyrelsen, polismyndighet, åklagarmyndighet eller Kriminalvården beslutar om efterlysning. Annan myndighet kan göra framställning hos polisen om efterlysning. Uppgifter om personefterlysningar införs i EP-delen av registret.

För framställning av U-boken antecknar Rikspolisstyrelsen i ett centralt register uppgifter om den som utvisats ur Sverige på grund av brott samt uppgifter om den som avvisats eller utvisats enligt beslut av Migrationsverket, en migrationsdomstol, Migrationsöverdomstolen eller regeringen i de fall där beslutet är förordat med ett återreseförbud.

Personefterlysningsregistret innehåller känsliga personuppgifter i personuppgiftslagens mening, såvitt avser anledningen till efterlysningen. En sådan anledning till efterlysning kan t.ex. vara att personen avvikit från ett behandlingshem för vård av missbrukare.

### **Interpolregistret**

Registret förs av Rikspolisstyrelsen med tillstånd meddelat av Datainspektionen den 15 maj 1982. Det förs i dag med stöd av övergångsbestämmelserna till polisdatalagen. Registret består av två delregister. Det ena innehåller polisregisteruppgifter och det andra utgör ett diarium över ärenden inom Interpolsektionen.

Ändamålet med registret är enligt tillståndet att återfinna ärenden i en aktsamling vid styrelsens Interpolsektion.

Registret får förutom administrativa uppgifter innehålla uppgift om ärendetyp, land, personnummer, nationalitet, fordon, kontonummer, nummer på legitimationshandling, indikativ (begrepp för att ange förfalskningstyp) samt åtgärd.

Interpolregistret har ersatts av ett nytt ärendehanteringssystem, DAR II, i vilket behandlingen av personuppgifter sker i enlighet med personuppgiftslagen och polisdatalagen. Rikspolisstyrelsen avser att avanmäla Interpolregistret hos Datainspektionen.

### **Godsregister**

Godsregistret förs med stöd av Datainspektionens tillstånd den 23 juni 1977 och således med stöd av övergångsbestämmelserna till polisdatalagen. Ändamålet med registret är enligt tillståndet följande. I registret antecknas gods som stulits, förkommit eller omhändertagits, t.ex. såsom hittegods, eller som har beslagttagits vid husrannsakan. Registret används i polisens spanings- och utredningsverksamhet för att identifiera sådant gods. Registret används vidare för att kontrollera gods som pantsatts hos pantlånerörelser och liknande inrättningar. Det kan även – efter förfrågan från en enskild person till vederbörande polismyndighet – användas för kontroll av gods som utjudits till enskild person för försäljning. Registret utgör också underlag för viss statistik avseende arten och värdet av gods m.m. Godsregistret håller på att avvecklas.

### **Efterlysningssystem för fordon m.m.**

Efterlysningssystemet för fordon m.m. förs med stöd av Datainspektionens tillstånd den 23 juni 1986. Systemet förs i dag med stöd av övergångsbestämmelserna till polisdatalagen.

Ändamålet med registret är enligt tillståndet att utgöra underlag och hjälpmedel för den polisiära spaningsverksamheten

samt att sprida upplysning inom polisen och till vissa andra myndigheter m.fl. om fordon som efterlysts.

Registret får endast innehålla de uppgifter som framgår av ansökan. De personer som får registreras är ägare till fordon som ska efterlysas (omkring 40 000 per år), person som anträffar ett efterlyst fordon (omkring 10 000 per år) samt person som efterspanas och som kan misstänkas färdas med ett visst fordon som ägs av annan (omkring 400 per år). De uppgifter som får anges är bl.a. uppgifter om fordonet, ägarens personnummer eller organisationsnummer, ägarens namn, anledning till efterlysningen, handläggande polismyndighet och diarienummer samt var och när fordonet anträffades. Av Datainspektionens beslut framgår att fritext bara får innehålla uppgifter av den art som exemplifieras i ansökningen. I ansökningen sägs att fritext inte ska innehålla uppgift om brott eller brottsmisstanke.

### Passregistret

Registret förs av Rikspolisstyrelsen och de lokala polismyndigheterna. Sedan den 1 oktober 2001 förs registret med stöd av personuppgiftslagen. Ändamålet med registret är att tillhandahålla uppgifter som behövs för att utfärda pass, för att kontrollera vilka personer som innehar pass, för att hindra att någon innehar mer än ett pass, för att kontrollera om passtillstånd fordras, för identifieringskontroll i polisens verksamhet samt för kontroll och avstämning av passuppgifter, passböcker och avgifter.

Enligt 23 § passförordningen (1979:664) ska Rikspolisstyrelsen föra ett centralt passregister och ett centralt register över omständigheter som avses i 20 § 1 och 3 passlagen (1978:302).

Passregistret får innehålla uppgift om bl.a. passinnehavarens identitet, passnummer, passets giltighetstid och kod för särskilt passhinder.

Av 20 § passlagen följer att passtillstånd fordras bl.a. för den som är intagen för vård enligt lagen (1991:1128) om psykiatrisk

tvångsvård eller lagen (1991:1129) om rättspsykiatrisk vård, dock endast om chefsöverläkaren vid sjukvårdsinrättningen har gjort anmälan om att pass inte får utfärdas utan sådant tillstånd (första punkten) eller för att patienten tidigare utfärdat pass efter intagningen eller inskrivningen har återkallats på grund av framställning från Socialstyrelsen (tredje punkten).

### **Registret för identifiering av försvunna personer**

Registret för identifiering av försvunna personer förs med tillstånd av Datainspektionen den 16 juni 1988. Det förs i dag med stöd av övergångsbestämmelserna till polisdatalagen. Ändamålet med registret ska enligt tillståndet vara att underlätta framtagning av detaljerade signalementsuppgifter om personer som varit försvunna en längre tid och därvid underlätta identifieringen av okända och avlidna personer.

Till registret överförs uppgifter om personer som anmäls försvunna och som registrerats i personefterlysnings- och Uboksregistret (se ovan) samt inte återfunnits efter sextio dagar.

### **Disaster Victim Identification**

Registret Disaster Victim Identification (DVI-registret) förs med tillstånd av Datainspektionen den 15 oktober 1998. Det förs i dag med stöd av övergångsbestämmelserna till polisdatalagen.

DVI-registret består av blanketter som tagits fram inom Interpol för registrering av uppgifter om försvunna personer och om oidentifierade människokroppar. Registret innehåller mycket detaljerade uppgifter om de registrerade och många av uppgifterna i registret utgör känsliga personuppgifter i personuppgiftslagens mening. Detta gäller t.ex. uppgifter om religiös övertygelse, om smittsamma infektioner, om användning av läkemedel och annan information från läkarjournaler.



## Register med anknytning till det statliga person- och adressregistret

Polisens adressdatabas, polisens fastighetsfråga, polisens historikdatabas och polisens folkbokföringsdatabas är register av administrativ karaktär. De fyra registren har alla samband med det statliga person- och adressregistret (SPAR) som förs med stöd av lagen (1998:527) om det statliga personadressregistret.

Adressdatabasen förs med tillstånd av Datainspektionen meddelade den 3 mars och 16 april 1992. Ändamålet med registret är att ge polisen upplysning om vilka personer som är folkbokförda på en viss adress för att därmed utgöra ett stöd i sådan hjälpande verksamhet som avses i 2 § 4 polislagen. Dessutom ska registret utgöra ett stöd i polisens spaning och utredning i fråga om brott som hör under allmänt åtal. I ansökan om tillstånd anges att registret endast ska innehålla uppgifter om ”personer folkbokförda i Sverige med undantag för de som sekretessmärkt sina adresser i folkbokföringen”. De uppgifter som registreras är personnummer, gatuadress och ”markering om personens gatuadress är aktuell eller ej”. Registret bygger på information från SPAR.

Polisens fastighetsfråga förs med tillstånd av Datainspektionen meddelade den 24 september 1993 och 15 september 1997. Ändamålet med registret är enligt tillståndet att ge polisen upplysning om fastighet (fastighetsbeteckning) hörande till viss person. Registret får bara innehålla uppgifter om personer som är folkbokförda i Sverige. Inga andra uppgifter än personnummer och fastighetsbeteckning förs in i registret.

Polisens historikdatabas förs med tillstånd av Datainspektionen meddelade den 24 september 1993, 21 januari 1997 och 15 december 1997. Ändamålet med registret är att ge polisen upplysning om uppgifter som gallrats ur SPAR avseende personer under 90 år. Endast personer som är folkbokförda i Sverige ska registreras.

Polisens folkbokföringsdatabas förs med stöd av Datainspektionens tillstånd den 16 december 1997. Innehållet i registret be-

står av folkbokföringsuppgifter som ingår i Riksskatteverkets Aviseringsregister men som inte får ingå i SPAR.

## **Belastningsregistret, misstankeregistret och Schengens informationssystem**

### **En uppdelning av uppgifter på belastningsuppgifter och misstankesuppgifter**

I Europarådets rekommendation, No. R (87) 15, om användning av personuppgifter inom polissektorn anges att olika kategorier av uppgifter så långt det är möjligt ska hållas åtskilda efter graden av riktighet och tillförlitlighet. I propositionen Riktlinjer för registreringen av påföljder m.m. (prop. 1994/95:144) uttalade regeringen att det finns starka skäl att hålla uppgifter om påföljder och uppgifter om misstankar åtskilda och att en uppdelning skulle göras genom att person- och belastningsregistret skulle ersättas av ett belastningsregister, i vilket endast påföljder och liknande skulle tas in, och ett misstankeregister. Riksdagen, som vid flera tillfällen tidigare uttalat sig för en sådan uppdelning, godkände regeringens förslag (bet. 1994/95:JuU21, rskr. 1994/95:378).

Genom införandet av lagen (1998:620) om belastningsregister och av lagen (1998:621) om misstankeregister genomfördes en sådan uppdelning.

### **Belastningsregistret**

Enligt 1 § lagen om belastningsregister ska Rikspolisstyrelsen föra ett rikstäckande belastningsregister. Rikspolisstyrelsen är personuppgiftsansvarig för registret.

Ändamålet med belastningsregistret är att ge information om sådana belastningsuppgifter som behövs i verksamhet hos polis-, skatte- och tullmyndigheter för att förebygga, upptäcka och utreda brott, hos åklagarmyndigheter för beslut om förundersök-

ning och åtal och vid utfärdande av strafförelägganden samt hos allmänna domstolar för val av påföljd och straffmätning. Uppgifter i registret ska också få användas av polismyndigheter och andra myndigheter vid sådan lämplighetsprövning, tillståndsprövning och annan prövning som anges i lag eller förordning samt för att lämna uppgifter till enskilda om det är av särskild betydelse i den enskildes verksamhet. I lagen om belastningsregister bemyndigas regeringen att föreskriva att en myndighet får ha direktåtkomst till belastningsregistret.

Alla påföljder för brott ska registreras i belastningsregistret. Registret innehåller uppgifter om 800 000–1 000 000 personer och omkring 1 200 000 noteringar om påföljder. De allra flesta av dessa noteringar avser bötespåföljder som fastställts genom föreläggande av ordningsbot.

Belastningsregistret ska vidare innehålla uppgifter om den som har ålagts förvandlingsstraff för böter, den som med tillämpning av 30 kap. 6 § brottsbalken har förklarats fri från påföljd, den som ska utvisas eller utlämnas samt om den som har meddelats besöksförbud. Vissa uppgifter om den som är dömd i utlandet ska också registreras.

Respekten för den personliga integriteten kommer bl.a. till uttryck i begränsningar när det gäller utlämnande av uppgifter ur belastningsregistret. För registret gäller enligt 7 kap. 17 § sekretesslagen (1980:100) absolut sekretess, vilket innebär att uppgifter endast får lämnas ut enligt vad som är särskilt föreskrivet. Domstolarna och de övriga rättsvårdande myndigheterna har rätt att få ut de uppgifter som är nödvändiga för att de ska kunna bedriva sin verksamhet. Vidare har den registrerade alltid rätt att få ut de uppgifter som finns registrerade om honom eller henne. Andra enskilda har rätt att i den utsträckning som regeringen föreskriver få ut uppgifter om andra personer ur registret, om det behövs för att pröva en fråga om anställning eller uppdrag i en verksamhet som avser vård eller som är av betydelse för att förebygga eller beivra brott. Vidare får uppgifter i vissa fall lämnas till utländska myndigheter och till myndigheter som för statistik.

Uppgifter i belastningsregistret gallras när förutsättningarna för registrering inte längre föreligger, t.ex. om den registrerade blir frikänd efter överklagande eller om en ordningsbot undanröjs. Vid frikännande dom plockas den tidigare domen bort direkt. Uppgifter ur belastningsregistret gallras vidare när viss tid förflutit, i de flesta situationer efter tio år.

Personuppgiftslagens bestämmelser om rättelse och skadestånd gäller för behandlingen av personuppgifter i registret.

Regeringen bemyndigas i lagen om belastningsregister att utfärda föreskrifter om registrets närmare innehåll. Det kan bl.a. gälla uppgifter om utvisning, intagning i eller utskrivning från sjukvårdsinrättning av den som av domstol överlämnats till psykiatrisk vård samt uppgifter om resning.

### **Misstankeregistret**

Enligt 1 § lagen om misstankeregister ska Rikspolisstyrelsen föra ett rikstäckande register med uppgifter om dem som är skäligen misstänkta för brott. Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av personuppgifter i registret.

Misstankeregistret ska föras för att underlätta tillgången till sådana uppgifter om skäligen misstänkt om brott som behövs i verksamhet hos polis-, skatte- och tullmyndigheter för att samordna förundersökningar mot en misstänkt person och för att förebygga, upptäcka och utreda brott samt hos åklagarmyndigheter för beslut om förundersökning och åtal. Registret får även användas av polismyndigheter och andra myndigheter som ska utföra lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning. Slutligen får registret användas för att till enskild lämna uppgift som är av särskild betydelse i dennes verksamhet.

Misstankeregistret innehåller uppgifter om den som har fyllt 15 år och som är skäligen misstänkt antingen för något brott mot brottsbalken eller för något annat brott för vilket svårare straff än böter är föreskrivet. Uppgifter förs också in om den

som är skäligen misstänkt för ett motsvarande brott utomlands, om frågan om lagföring för brottet ska avgöras i Sverige. Registret innehåller vidare uppgifter om den mot vilken det har inletts utredning om förvandling av böter och om den som begärts överlämnad eller utlämnad för brott.

De myndigheter för vars räkning registret förs samt domstolarna ska oavsett sekretess ha rätt till uppgifter ur registret. Regeringen får föreskriva att andra myndigheter ska få uppgifter ur registret för vissa slag av ärenden eller för särskilt fall. Uppgifter ur registret ska vidare i viss utsträckning kunna lämnas till myndigheter och organisationer utomlands.

Det finns ungefär 100 000 personer registrerade i misstankeregistret, medan det finns omkring 225 000 uppgifter om brottsmisstankar i registret.

Uppgifter i misstankeregistret gallras om en förundersökning har avslutats utan att åtal har väckts med anledning av misstanken, om åtal har lagts ned eller om dom eller beslut angående misstanken har vunnit laga kraft.

Personuppgiftslagens bestämmelser om rättelse och skadestånd gäller för behandling av uppgifter i misstankeregistret.

### **Schengens informationssystem**

Sverige är anslutet till Schengensamarbetet (prop. 1997/98:42, bet. 1997/98:JuU15, rskr. 1997/98:121). Schengensamarbetet bygger på två grundtankar. Den första är den fria rörligheten för personer, i den betydelsen att någon personkontroll vid nationsgränserna mellan Schengenstaterna inte ska förekomma. Den andra är att kampen mot internationell kriminalitet och illegal invandring ska stärkas.

Ett hjälpmedel i detta sammanhang är dataregistret Schengens informationssystem (SIS). SIS består av ett nationellt register för varje Schengenstat och en central teknisk stödfunktion, som är gemensam för Schengenländerna. Lagen (2000:344) om Schengens informationssystem innehåller regler om behandling av per-

sonuppgifter i den nationella enheten. Det register som är den svenska nationella enheten i SIS förs av Rikspolisstyrelsen, som också är personuppgiftsansvarig. Registret är anslutet till den centrala enheten i SIS.

Varje Schengenstats nationella enhet innehåller uppgifter som är identiska med uppgifterna i de övriga ländernas nationella enheter.

Registret är ett hjälpmedel för Schengenstaterna att göra framställningar för att främja samarbete som avser polisiära och rättsliga frågor samt frågor om inresa och uppehållstillstånd. Det är uppbyggt som ett spanings- och efterlysningshjälpmedel. I SIS-registret kan varje Schengenstat föra in uppgifter om personer eller föremål som är efterlysta eller på annat sätt eftersökta med en begäran om att en viss åtgärd ska vidtas när en efterlyst person eller ett efterlyst fordon påträffas. Uppgifterna i SIS-registret består av identifieringsuppgifter angående registrerade personer. De kompletterande uppgifter som behövs, för att ett land som har påträffat en efterlyst person eller ett efterlyst föremål, ska kunna verkställa en begärd åtgärd lämnas över först när det blir aktuellt i varje enskilt fall genom direkt kontakt mellan de berörda länderna.

Lagen om SIS innehåller bestämmelser om vilka framställningar som får föras in i registret. I lagen regleras också vilka personuppgifter som får föras in i registret, vem som får använda uppgifter ur det och ett förbud mot att använda uppgifter för annat ändamål än det som uppgiften registrerats för. I registret finns uppgifter om namn, särskilda bestående fysiska kännetecken, födelsedatum och födelseort, kön, medborgarskap samt om personen är beväpnad eller kan tillgripa våld. Vidare registreras syftet med framställningen samt begärd åtgärd. Registret innehåller endast uppgifter som har behandlats av behöriga myndigheter i Schengenstaterna, i enlighet med respektive stats nationella lagstiftning. Uppgifter registreras av Rikspolisstyrelsen endast om behandling av motsvarande slag av uppgifter är tillåten enligt personuppgiftslagen, polisdatalagen eller annan svensk författning. Känsliga personuppgifter registreras inte.

Uppgifterna i registret gallras senast ett, tre, fem eller tio år efter registreringen. Det tillämpas olika gallringstider för olika slag av uppgifter.

I lagen med tillhörande förordning anges också vilka myndigheter som har rätt att ha direktåtkomst till registret.

### **Passagerarregister**

Enligt lagen (2006:444) om passagerarregister ska Rikspolisstyrelsen föra ett register över sådana passagerare som avses i 9 kap. 3 a § utlänningslagen (2005:716). Rikspolisstyrelsen är personuppgiftsansvarig för behandlingen av uppgifter i registret. Ändamålet med registret är att underlätta verkställandet av personkontroller vid Sveriges gräns mot stater som inte tillhör EU och inte heller har träffat avtal om samarbete enligt Schengenkonventionen med konventionsstaterna.

I registret får förekomma uppgifter om bl.a. namn, födelsedatum, medborgarskap, nummer på och typ av resehandling som används samt gränsövergångsställe för inresa.

Uppgifter ur registret ska lämnas ut på en begäran från en polismyndighet och Tullverket. Polismyndigheterna får ha direktåtkomst till registret. Regeringen får meddela föreskrift om att även annan myndighet får ha direktåtkomst till registret.

### **Säkerhetspolisens system**

#### **Allmänt**

I Säkerhetspolisens verksamhet används flera olika databaser som innehåller personuppgifter. Det rör sig om SÄPO-registret, centralregistret, systemet för hemlig teleavlyssning och hemlig teleövervakning samt analysdatabaser.

Utöver det i polisdatalagen särskilt reglerade SÄPO-registret styrs behandlingen av personuppgifter i Säkerhetspolisens verk-

samhet av bestämmelserna i personuppgiftslagen, polisdatalagens allmänna del och arbetsordningen för Säkerhetspolisen.

### SÄPO-registret

SÄPO-registret är ett register som är avsett för den särskilda polisverksamhet som Säkerhetspolisen bedriver. Bestämmelserna om SÄPO-registret finns i 32–35 §§ polisdatalagen. Polisdatalagen föreskriver att Säkerhetspolisen ska föra ett register (SÄPO-registret) som har till ändamål att

- underlätta spaning i syfte att förebygga och avslöja brott mot rikets säkerhet,
- underlätta spaning i syfte att bekämpa terrorism och
- utgöra underlag för registerkontroll enligt säkerhetsskyddslagen (1996:627).

SÄPO-registret får innehålla uppgifter som kan hänföras till en enskild person endast

- om den uppgifternas gäller kan misstänkas för att ha utövat eller komma att utöva brottslig verksamhet som innefattar hot mot rikets säkerhet eller terrorism,
- om personen har undergått registerkontroll enligt säkerhetsskyddslagen (1996:627) eller
- om det med hänsyn till registrets ändamål annars finns särskilda skäl till det.

Registrerade uppgifter ska gallras senast tio år efter det att en sådan uppgift om personen som kan föranleda registrering senast infördes. Om det finns särskilda skäl får dock uppgifterna stå kvar under längre tid.

Direkt åtkomst till uppgifter i SÄPO-registret eller till uppgifter som i annat fall behandlas automatiserat hos Säkerhetspolisen är enligt 13 § polisdataförordningen förbehållen de personer som på grund av sina arbetsuppgifter behöver informationen.

SÄPO-registret är avsett att vara ingången till Säkerhetspolisens hantering av personuppgifter (prop. 1997/98:97 s. 154). Detta innebär att registret endast får innehålla identifieringsupp-



gifter, uppgifter om grunden för registrering och hänvisning till de ärenden där uppgifter om den registrerade behandlas. Registret fyller inte någon operativ funktion i Säkerhetspolisens verksamhet. All behandling av personuppgifter av betydelse för verksamheten sker i andra system. Registret förs enbart för att uppfylla kravet i 32 § polisdatalagen om att Säkerhetspolisen ska föra ett sådant register.

### **Säkerhetspolisens centralregister**

Säkerhetspolisens centralregister är den databas som huvudsakligen används i Säkerhetspolisens verksamhet. Centralregistret kan sägas utgöra en ingång till den samlade personuppgiftshandlingen hos Säkerhetspolisen.

Det övergripande ändamålet med centralregistret är att det ska utgöra ett spaningsregister i Säkerhetspolisens verksamhet för att förebygga och avslöja brott mot rikets säkerhet och för att bekämpa terrorism. Vidare används uppgifter ur databasen som underlag för registerkontroller.

Databasen innehåller uppgifter om personer mot vilka det föreligger misstankar om brottslig verksamhet, som inte behöver vara preciserade till vissa konkreta brott. I databasen behandlas även uppgifter om personer som har samband med någon som antecknats på grund av en misstanke. Det behandlas också uppgifter om personer som kan bli utsatta för hot av olika slag eller som i känsliga verksamheter kan bli föremål för närmanden från utländska underrättelsetjänster.

Personuppgifter noteras i centralregistret i den utsträckning som uppgifterna behövs för databasens ändamål.

Känsliga personuppgifter antecknas som kompletterande uppgifter, om en viss persons uppträdande ger anledning anta att personen kan misstänkas för sådana brott som Säkerhetspolisen ska ingripa mot. Om det är oundgängligen nödvändigt att en känslig personuppgift noteras för att viss information i registret ska bli begriplig får notering ske. Det sistnämnda inne-

bär t.ex. att uppgifter om en hotad persons politiska tillhörighet kan komma att antecknas.

Uppgifterna i centralregistret är tillgängliga för Säkerhetspolisens operativa personal i enlighet med särskilda behörighetsregler.

### **Systemet för hemlig teleavlyssning och hemlig teleövervakning**

Systemet för hemlig teleavlyssning och hemlig teleövervakning utgör ett bearbetnings- och analysverktyg vid behandling av uppgifter som inhämtats genom hemlig teleavlyssning eller hemlig teleövervakning. Systemet innehåller personuppgifter i den utsträckning sådana uppgifter behövs för behandlingens ändamål.

De personuppgifter som antecknas i systemet utgörs av uppgifter om abonnent- och teleadresser som är kopplade till ett tillstånd till hemlig teleavlyssning eller hemlig teleövervakning. Vidare antecknas uppgifter om kontakter och teleadresser som uppmärksammas med anledning av en pågående teleavlyssning eller teleövervakning. Dessutom noteras innehållet i telefonsamtal och andra telemeddelanden samt utredningsanteckningar.

Uppgifterna i systemet utgörs till en början av obearbetade underrättelser som i en bestämd utredning inhämtats genom något av de nyss nämnda tvångsmedlen. De inhämtade uppgifterna bearbetas och analyseras. Efter bearbetning och analys tas de uppgifter bort som inte är relevanta för utredningen. Övriga uppgifter tillförs centralregistret. Uppgifterna i systemet är tillgängliga för de befattningshavare som har behörighet att arbeta med det aktuella ärendet.

### **Analysdatabaser**

Analysdatabaserna innehåller liksom systemet för hemlig teleavlyssning och hemlig teleövervakning underrättelser som är av-

sedda att bearbetas. Underrättelserna i analysdatabaserna inhämtas genom uppgifter från källor, genom spaning samt genom tvångsmedel som t.ex. hemlig teleavlyssning och hemlig teleövervakning. Personuppgifter antecknas om uppgifterna behövs för behandlingens ändamål.

Bearbetad och bedömd information förs över till centralregistret, medan uppgifter som inte behövs gallras under utredningens gång.

Uppgifter i en analysdatabas är tillgängliga endast för de befattningshavare som är behöriga att arbeta med det aktuella ärendet. En analysdatabas får inrättas efter beslut från chefen för dokumentationsenheten hos Säkerhetspolisen.

## **Lokala system med nationell spridning**

### **Allmänt**

De lokala polismyndigheterna har inrättat flera olika system för automatiserad behandling av uppgifter. Det gäller bl.a. s.k. tillhållsregister samt system för intern samordning av pågående utredningar. Att ett system är lokalt innebär att det i princip bara är den egna polismyndigheten som har tillgång till uppgifter ur systemet. Här redovisas fyra lokala system som har nationell spridning, nämligen rationell anmälningsrutin, datoriserad utredningsrutin – tvångsmedel, kommunikationscentralernas system och förundersökningsregister.

### **Rationell anmälningsrutin**

Rationell anmälningsrutin (RAR) förs av de lokala polismyndigheterna med tillstånd meddelade av Datainspektionen den 17 september 1993 och 17 december 1997. Registret förs i dag med stöd av övergångsbestämmelserna till polisdatalagen.

Ändamålet med registren är att tillhandahålla uppgifter om brottsanmälningar som behövs i den registeransvariges brottsutredande verksamhet och som behövs för att Rikspolisstyrelsen skall kunna fullgöra sin stödjande, samordnande och förstärkande verksamhet, för service åt allmänheten och för att i enlighet med lag eller förordning lämna uppgifter till annan myndighet. Ett annat ändamål med registret är att tillhandahålla uppgifter för polismyndighetens ärenden, lämna underlag för samordning, bevakning, planering och uppföljning av verksamheten, utgöra underlag för registrering av uppgifter i misstankeregistret och produktion av statistik samt tillika utgöra myndighetens kriminaldiarium.

RAR innehåller uppgifter direkt från polisens brottsanmälningsblanketter. Blanketterna för brottsanmälan är numera inlagda i datorsystem. Detta medför att när en blankett fylls i registreras samtidigt brottsanmälningens uppgifter i RAR. De flesta brottsbalksbrott registreras i RAR.

Samtliga uppgifter i brottsanmälningarna registreras i RAR. Förutom uppgifter om själva brottet finns personuppgifter avseende målsägande, anmälare, skäligen misstänkt gärningsman, vittne samt försvunna och avlidna personer.

### **Datoriserad utredningsrutin – Tvångsmedel**

Systemet datoriserad utredningsrutin – tvångsmedel (DurTvå) är ett lokalt datasystem med nationell spridning, vilket syftar till att effektivisera polisens och åklagarnas arbete med förundersökningar i brottmål. Systemet regleras av personuppgiftslagen och de allmänna bestämmelserna i polisdatalagen.

Genom DurTvå skapas ett system genom vilket förundersökningsprotokoll upprättas på elektronisk väg. Alla anmälningar ur RAR hämtas automatiskt till DurTvå. Därefter upprättas hela förundersökningsprotokollet i DurTvå. I dag saknas möjlighet att göra fritextsökningar i DurTvå, men den möjligheten kommer att finnas när systemet är fullt utbyggt.

Det finns ett behörighetssystem för sökning i DurTvå. Behörigheten att få del av uppgifter är uppdelad i tre nivåer.

### **Kommunikationscentralernas system**

För att effektivisera och samordna bl.a. alarmeringsåtgärder och viss tillfällig spaningsverksamhet ska det i varje län finnas en ort med kommunikationscentral. Uppgifterna för kommunikationscentralerna är att ta emot och vidarebefordra inkommande larm och andra meddelanden samt att inledningsvis vidta och samordna polisåtgärder med anledning av larmen och meddelandena.

Som stöd för denna verksamhet finns det ett systemstöd för kommunikationscentralerna, det s.k. KC-systemet. Behandlingen av personuppgifterna i systemet sker med stöd av bestämmelserna i personuppgiftslagen och i de allmänna bestämmelserna i polisdatalagen. Det finns motsvarigheter till KC-systemet i flera andra europeiska länder och även i USA. Systemet är ursprungligen framtaget i Kanada.

Huvudsyftet med behandlingen är att dokumentera, bevaka och följa upp händelser och iakttagelser som rapporteras till kommunikationscentralerna. Ett annat syfte är att på ett tidigt stadium erhålla signaler om pågående och återkommande brottslig verksamhet, exempelvis om familjevåld och mc-brottslighet. Vidare har behandlingen till ändamål att ge underlag för planering av polisens resurser och för uppföljning av verksamheten.

I KC-systemet registreras uppgifter om brotts- eller händelseplatser med besked om tid, plats, händelsetyp, brottskod och övrig information som kan vara till hjälp vid en kommande polisutredning. Systemet innehåller också personuppgifter. Registrering sker av anmälare, målsägande, vittne, misstänkta, utpekade och försvunna personer samt personer som på olika sätt kontaktar polisen i ärenden som registreras i KC-systemet. I Stockholm noteras 1 000–1 200 ärenden per dygn i KC-systemet.

Rikspolisstyrelsen har i enlighet med 2 § polisdataförordningen anmält KC-systemet till Datainspektionen för förhandskontroll. Inspektionen har i ett beslut den 21 december 1999 framfört synpunkter på rutinerna för gallring och för information till de registrerade.

Enligt anmälan ska de registrerade uppgifterna i händelserapporterna vara tillgängliga i KC-systemet under 13 månader. Datainspektionen har erinrat om att personuppgifter som behandlas automatiserat enligt huvudregeln i 13 § polisdatalagen ska gallras när uppgifterna inte längre behövs för sitt ändamål.

I fråga om information till registrerade sägs i anmälan att information om uppgiftsbehandling inte ska lämnas annat än till vissa särskilt angivna kategorier av personer. Rikspolisstyrelsen har därvid hänvisat till bestämmelsen i 24 § tredje stycket personuppgiftslagen, som föreskriver att information får underlåtas om lämnandet skulle visa sig vara omöjligt eller innebära en oproportionerligt stor arbetsinsats. Datainspektionen har anfört att denna undantagsbestämmelse inte kan anses vara generellt tillämplig i fråga om samtliga angivna kategorier av registrerade.

### **Förundersökningsregister**

Förundersökningsregister får enligt regeringens beslut den 28 november 1985 föras av de lokala polismyndigheterna. Datainspektionen meddelade föreskrifter för registren den 21 januari 1986.

Ändamålet med registren är att utgöra hjälpmedel för att lagra, systematisera och återvinna uppgifter i förundersökningar med komplicerat eller omfattande utredningsmaterial.

Förundersökningsregister får enligt Datainspektionens beslut endast innehålla uppgifter av den art som framgår av ansökningsen. Förutom administrativa uppgifter får sålunda registreras uppgifter om namn på uppgiftslämnare, uppgifter om en person som kan sättas i samband med något brott, beskrivning av for-

don och personer, uppgifter om brottsplats, uppgifter ur förhör samt uppgifter om adresser till kända "tillhåll" och "kvartar".

## **Intranät**

Polisens intranät används i första hand för att sprida verksamhetsrelaterad information inom polismyndigheterna.

## **IntraPolis**

IntraPolis är ett nationellt nätverk. Olika polismyndigheter har utvecklat intranät för respektive myndigheter och dessa intranät utgör delar av IntraPolis. Genom polismyndigheternas intranät förmedlas både öppen och skyddad information. Den öppna informationen är tillgänglig för alla inom polisen medan det erfordras särskild behörighet inom respektive polismyndighet för att få tillgång till den skyddade informationen.

På intranäten finns dock även information som omfattas av sekretess. För tillträde till den del av intranäten som innehåller sådan information krävs som nämnts särskild behörighet.

Ett exempel på skyddad information är s.k. KUT-Info.

## **KUT-Info**

I fråga om behandlingen av personuppgifter i KUT-Info gäller bestämmelserna i personuppgiftslagen och polisdatlagen. Konsekvenserna av dessa regelverk för behandling av personuppgifter på intranät belyses av ett beslut från Datainspektionen den 28 januari 2000. Beslutet föranleddes av att Polismyndigheten i Stockholms län enligt 2 § polisdataförordningen hade anmält att myndigheten i systemet KUT-Info avsåg att behandla personuppgifter som gav upplysning om att personer var dömda eller misstänkta för brott.

I förhandsanmälan till Datainspektionen anförde polismyndigheten beträffande en planerad behandling av personuppgifter i KUT-Info bl.a. följande.

Inom Stockholms län ska distribueras kriminalunderrättelseinformation, förkortat KUT-Info, från länskriminalens underrettelserotet ett par gånger i veckan. Informationen ska bestå av uppgifter om efterlysta personer, om oidentifierade gärningsmän, om framställningar från olika utredningsmän om hjälp, om permissioner, om brott av polisiärt intresse som uppgifter angående t.ex. dolda vapen och om tillvägagångssätt vid brott m.m. Uppgifterna ska spridas genom IntraPolis till omkring 400 användare, som i sin tur ska skicka uppgifterna vidare till ytterligare ett stort antal poliser och andra anställda inom myndigheten. KUT-Info ska skickas främst till anställda hos Polismyndigheten i Stockholms län men även till behöriga tjänstemän inom andra polismyndigheter i Sverige. Syftet med den planerade nya behandlingen är att utnyttja den moderna tekniken och använda IntraPolis för snabb publicering av kriminalunderrättelseinformation samt att snabbt sprida väsentlig information som polisanställda har behov av i sin tjänst.

Uppgifterna beträffande efterlysta personer ska omfatta namn, personnummer, foto, adressuppgifter samt fordon. Dessutom kommer uppgifter om vilka brott personen är efterlyst för samt uppgifter om farlighet att anges. Polisen avser även att sprida fotografier på oidentifierade personer som är misstänkta för brott. Även fotografier och uppgifter om värdefullt tillgripet gods ska spridas. Uppgifter beträffande personer som är dömda för grova brott samt tidpunkterna för dessa personers permissioner och frigivning från avtjänande av påföljder kommer att nämnas i KUT-Info.

Datainspektionen meddelade som nämnts ovan den 28 januari 2000 ett beslut rörande anmälingen om behandling av personuppgifter i KUT-Info. Enligt inspektionens uppfattning borde frågan om i vilken utsträckning den aktuella informationsförmedlingen ska kunna förekomma och vilka uppgifter som ska kunna presenteras bli föremål för central reglering, åtminstone



genom sådana föreskrifter som förutsätts i 17 § polisdataförordningen. Vidare uttalade Datainspektionen att enligt dess mening är behandling och registrering av personuppgifter i kriminalunderrättelseverksamhet uttömmande reglerad i polisdatalagen. Det är inte förenligt med polisdatalagen att i ett system som KUT-Info behandla personuppgifter som faller under begreppet kriminalunderrättelseverksamhet.

Med anledning av Datainspektionens beslut anpassade Polismyndigheten i Stockholms län behandlingen och driftsatte under våren 2000 ett KUT-infosystem. Även andra länspolismyndigheter har i likhet med polismyndigheten i Stockholms län infört system för KUT-info.

## DocPol

Inom EU tillhör samarbetet på polisområdet den s.k. tredje pelaren, dvs. samarbetet är mellanstatligt. Inom ramen för samarbetet på polisens område har det upprättats en europeisk polisbyrå, Europol. Europols främsta uppgift är att vara ett kriminalunderrättelseorgan för de brottsbekämpande myndigheterna i medlemsländerna inom EU. Som sådant är Europol en knutpunkt för utbyte av information och underrättelser mellan medlemsländerna. Europol fungerar så att medlemsländerna tillhandahåller Europol uppgifter främst ur sina nationella polisregister. Dessa uppgifter sammanställs och bearbetas samt kompletteras, i en del fall, med uppgifter från annat håll och analyseras sedan hos Europol. Dessa underlag delges sedan medlemsländerna.

Europols verksamhet regleras i Europolkonventionen. Riksdagen beslutade under hösten 1997 att Sverige skulle ansluta sig till konventionen (prop. 1996/97:164, bet. 1997/98:JuU2, rskr. 1997/98:22). Den 1 oktober 1998 trädde Europolkonventionen i kraft. Verksamheten inleddes den 1 juli 1999.

Nuvarande polisdatalag medger inte att personuppgifter som härrör från kriminalunderrättelseverksamhet behandlas automa-

tiserat annat än i så kallade särskilda undersökningar eller i kriminalunderrättelseregister.

För att kunna uppfylla de krav informationsutbytet med Europol ställer anmälde Rikspolisstyrelsen i februari 2000 till Datainspektionen för förhandskontroll att man avsåg att bygga ut dokument- och ärendehanteringssystemet DocPol, i vilket ärenden avseende bl.a. Europol registreras. Enligt Datainspektionens beslut från mars samma år omfattade den planerade behandlingen i vissa avseenden uppgifter i kriminalunderrättelseverksamhet. Den tänkta behandlingen ansågs inte stå i överensstämmelse med polisdatalagens regler om behandling av personuppgifter i sådan verksamhet och var därför inte tillåten. Rikspolisstyrelsen överklagade Datainspektionens beslut. Efter att frågan prövats i sak av länsrätten (överklagandet avslogs) fann kammarrätten att Datainspektionens beslut inte hade sådana rättsverkningar mot Rikspolisstyrelsen att det kunde anses överklagbart. Kammarrätten undanröjde länsrättens dom och avvisade överklagandet.