Lagrådsremiss

Hemlig dataavläsning mot allvarliga brott

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 10 oktober 2024

Pål Jonson

Emma Pleiner
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Sedan 2020 har de brottsbekämpande myndigheterna, genom en tidsbegränsad lagstiftning, möjlighet att använda tvångsmedlet hemlig dataavläsning vid misstankar om allvarlig brottslighet. Det innebär att de med hjälp av tekniska hjälpmedel kan hämta in och ta del av information från till exempel en dator, en mobiltelefon eller ett användarkonto till en kommunikationstjänst. Hemlig dataavläsning är ett viktigt verktyg som ger myndigheterna tillgång till information som annars inte är tillgänglig. Regeringen föreslår att lagen om hemlig dataavläsning ska gälla utan tidsbegränsning med bland annat följande justeringar:

- Hemlig dataavläsning ska få användas i fler fall i syfte att utreda vem som skäligen kan misstänkas för ett brott.
- Reglerna för vilka typer av uppgifter som får hämtas in och för utformningen av ett tillstånd till hemlig dataavläsning ska förtydligas.
- Överskottsinformation som har kommit fram vid hemlig dataavläsning ska få användas för andra ändamål.
- Rättssäkerheten för den enskilde ska stärkas, bland annat genom förbättrade möjligheter till insyn och tillsyn.

Lagändringarna föreslås träda i kraft den 1 april 2025.

Innehållsförteckning

1 Beslut 4

2 Lagtext 5
- 2.1 Förslag till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål 5
- 2.2 Förslag till lag om dels fortsatt giltighet av lagen (2020:62) om hemlig dataavläsning, dels ändring i samma lag 6
- 2.3 Förslag till lag om ändring i lagen (2020:62) om hemlig dataavläsning 16
- 2.4 Förslag till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder 19
- 2.5 Förslag till lag om ändring i lagen (2024:332) om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder 21

3 Ärendet och dess beredning 22

4 Hemlig dataavläsning – ett verktyg i brottsbekämpningen 22
- 4.1 Ett tidsbegränsat tvångsmedel 22
- 4.2 Skyddsmekanismer och rättssäkerhetsgarantier 23

5 Regleringen ska gälla utan tidsbegränsning 25

6 Tydligare regler om hemlig dataavläsning 32
- 6.1 Innebörden av hemlig dataavläsning 32
- 6.2 Regleringen av vilka uppgiftstyper som får hämtas in 33

7 Bättre möjligheter att utreda vem som skäligen kan misstänkas för ett brott 36

8 Förbättrade rättssäkerhetsgarantier 48
- 8.1 Nuvarande rättssäkerhetsgarantier och behovet av kompletterande regler 48
- 8.2 Tydligare regler för tillståndets utformning 49
- 8.3 Regleringen av villkor bör förtydligas 52
- 8.4 Teknikanpassning och otillåten tilläggsinformation 56
- 8.5 Användningen av överskottsinformation 59
- 8.6 Krav på bevarande av material 62
- 8.7 Skyldighet att dokumentera 64
- 8.8 Rättssäkerhetsgarantierna är tillräckliga 65

9 Ikraftträdande- och övergångsbestämmelser 67

10 Konsekvenser 68
- 10.1 Konsekvenser för det brottsbekämpande arbetet och för enskilda 68
- 10.2 Ekonomiska konsekvenser 72

11 Författningskommentar 75
- 11.1 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål 75

11.2 Förslaget till lag om dels fortsatt giltighet av lagen (2020:62) om hemlig dataavläsning, dels ändring i samma lag ... 76
11.3 Förslaget till lag om ändring i lagen (2020:62) om hemlig dataavläsning ... 87
11.4 Förslaget till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder ... 89
Bilaga 1 Sammanfattning av betänkandet Hemlig dataavläsning – utvärdering och permanent lagstiftning (SOU 2023:78) ... 91
Bilaga 2 Betänkandets lagförslag ... 101
Bilaga 3 Förteckning över remissinstanserna ... 110

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål,
2. lag om dels fortsatt giltighet av lagen (2020:62) om hemlig dataavläsning, dels ändring i samma lag,
3. lag om ändring i lagen (2020:62) om hemlig dataavläsning,
4. lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder,
5. lag om ändring i lagen (2024:332) om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.

2 Lagtext

Regeringen har följande förslag till lagtext.

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

Härigenom föreskrivs att 4 kap. 28 e § lagen (2000:562) om internationell rättslig hjälp i brottmål ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
28 e §[1]	
Tekniskt bistånd med hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning i form av omedelbar överföring av meddelanden eller uppgifter om meddelanden får lämnas i Sverige enligt de förutsättningar som gäller enligt 25 b § andra, tredje och femte styckena. Vid hemlig dataavläsning i en annan stat än den som ansökt om tekniskt bistånd ska ett tillstånd enligt 28 f § ha lämnats.	
Ansökan ska prövas av åklagare. För beslutet om tekniskt bistånd tillämpas 1 §, 18 § första stycket 1–*3* och *tredje* stycket och 20 § andra stycket lagen om hemlig dataavläsning.	Ansökan ska prövas av åklagare. För beslutet om tekniskt bistånd tillämpas 1 §, 18 § första stycket 1 *och 2* och *andra* stycket och 20 § andra stycket lagen om hemlig dataavläsning.

Denna lag träder i kraft den 1 april 2025.

[1] Senaste lydelse 2020:65.

2.2 Förslag till lag om dels fortsatt giltighet av lagen (2020:62) om hemlig dataavläsning, dels ändring i samma lag

Härigenom föreskrivs i fråga om lagen (2020:62) om hemlig dataavläsning

dels att lagen, som gäller till utgången av mars 2025, ska fortsätta att gälla,

dels att nuvarande 4 b och 5 §§ ska betecknas 5 och 5 a §§,

dels att 1, 2, 4 a, den nya 5, 8, 9, 14, 17, 18, 23, 27–29 och 31 §§ och rubrikerna närmast före 2 och 27 §§ ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 18 a och 34 §§, och närmast före 34 § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet *och* med ett tekniskt hjälpmedel *läses av eller tas upp i ett avläsningsbart informationssystem*.	Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling *och åtkomliga i ett avläsningsbart informationssystem, hämtas in* i hemlighet med ett tekniskt hjälpmedel.
I lagen avses med	
avläsningsbart informationssystem: en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst,	
kommunikationsavlyssningsuppgifter: uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *någon* annan adress,	*kommunikationsavlyssningsuppgifter:* uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,
kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *någon* annan adress,	*kommunikationsövervakningsuppgifter:* uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,
platsuppgifter: uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,	
kameraövervakningsuppgifter: uppgifter som framkommer genom optisk personövervakning,	
rumsavlyssningsuppgifter: uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.	

Typer av uppgifter* som får *läsas av eller tas upp	***Uppgiftstyper* som får *hämtas in***
2 §	
Tillstånd till hemlig dataavläsning får *beviljas för att läsa av eller ta upp*	*Ett tillstånd* till hemlig dataavläsning får *gälla*
1. kommunikationsavlyssningsuppgifter,	
2. kommunikationsövervakningsuppgifter,	
3. platsuppgifter,	
4. kameraövervakningsuppgifter,	
5. rumsavlyssningsuppgifter,	5. rumsavlyssningsuppgifter, *eller*
6. uppgifter som *finns lagrade* i ett avläsningsbart informationssystem *men som inte* avses i 1–5*, eller*	6. *andra* uppgifter som *är åtkomliga* i ett avläsningsbart informationssystem.
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.	

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

4 a §[1]

Ett tillstånd enligt 4 § får endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av den misstänkte.

Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.	Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta.

Ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Trots tredje stycket får ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter avse den skäligen misstänkte i stället för en viss plats, om det finns särskilda skäl för det. Den hemliga dataavläsningen får då endast användas på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

[1] Senaste lydelse 2023:540.

4 b §

Ett tillstånd till hemlig dataavläsning som gäller *kommunikationsavlyssningsuppgifter* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får endast avse ett avläsningsbart informationssystem som

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten *under den tid som tillståndet avser* har använt eller kommer att använda, eller

2. det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.

5 §[2]

Ett tillstånd till hemlig dataavläsning som *inte* gäller *rumsavlyssningsuppgifter* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.

Ett tillstånd enligt första stycket får endast avse ett avläsningsbart informationssystem som

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda, eller

2. det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

Ett tillstånd enligt andra stycket 2 får inte gälla kameraövervakningsuppgifter.

Ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter får verkställas på en plats som är någons stadigvarande bostad, endast om det finns synnerlig anledning att anta att den person som åtgärden riktas mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser.

8 §[3]

Ett tillstånd till hemlig dataavläsning enligt 7 § får endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av den person som åtgärden riktas mot.

[2] Senaste lydelse av tidigare 4 b § 2023:540.
[3] Senaste lydelse 2024:566.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den person som åtgärden riktas mot *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.	Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den person som åtgärden riktas mot har kontaktat eller kommer att kontakta.

9 §[4]

Ett tillstånd till hemlig dataavläsning får beviljas för att *läsa av eller ta upp* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av	Ett tillstånd till hemlig dataavläsning får beviljas för att *hämta in* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

1. ett utvisningsbeslut enligt 2 kap. 1 § lagen (2022:700) om särskild kontroll av vissa utlänningar, eller

2. ett avvisnings- eller utvisningsbeslut enligt 8 kap. eller 8 a kap. utlänningslagen (2005:716) om det finns sådana omständigheter i fråga om utlänningen som avses i 2 kap. 1 § lagen om särskild kontroll av vissa utlänningar.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får också beviljas för att *läsa av eller ta upp* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.	Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får också beviljas för att *hämta in* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar ska tillämpas i fråga om utlänningen gäller också för ett beslut i fråga om hemlig dataavläsning.

Ett tillstånd får beviljas endast om det finns synnerliga skäl och det är av betydelse för att

[4] Senaste lydelse 2024:329.

1. klarlägga om utlänningen tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen (2022:666) eller om det finns en risk för att utlänningen kan komma att engagera sig i en sådan organisation eller grupp,

2. klarlägga om det finns risk för att utlänningen själv planlägger eller förbereder brott som avses i 1,

3. klarlägga om det finns risk för att utlänningen själv eller tillsammans med andra medverkar i eller på annat sätt främjar ett allvarligt brott som rör Sveriges säkerhet, eller

4. kunna lokalisera en utlänning som inte har fullgjort sin anmälningsskyldighet enligt lagen (2022:700) om särskild kontroll av vissa utlänningar.

Ett tillstånd får inte *avse* rumsavlyssningsuppgifter. Ett tillstånd enligt fjärde stycket 4 får endast *avse* kommunikationsövervakningsoch platsuppgifter.

Ett tillstånd får inte *gälla* rumsavlyssningsuppgifter. Ett tillstånd enligt fjärde stycket 4 får endast *gälla* kommunikationsövervakningsoch platsuppgifter.

14 §[5]

Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen.

Om en ansökan som gäller kameraövervaknings- eller rumsavlyssningsuppgifter avser en viss person i stället för en viss plats, ska åklagaren i samband med ansökan föreslå sådana villkor som avses i 18 § *första* stycket *4.*

I samband med ansökan *ska åklagaren eller Säkerhetspolisen* föreslå sådana villkor som avses i 18 § *tredje* stycket*, om villkor inte framstår som obehövligt. Sådana villkor ska dock alltid föreslås om en ansökan som gäller kameraövervaknings- eller rumsavlyssningsuppgifter avser en viss person i stället för en viss plats.*

17 §[6]

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att *inhämta* rättens tillstånd i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att *hämta in* rättens tillstånd i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

[5] Senaste lydelse 2024:566.
[6] Senaste lydelse 2023:540.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren snarast möjligt skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *lästs av eller tagits upp* inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *hämtats in* inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

18 §[7]

I ett tillstånd till hemlig dataavläsning ska följande anges:

1. vilken tid tillståndet avser,

2. vilket avläsningsbart informationssystem tillståndet avser,

3. vilken *typ av uppgift* enligt 2 § första stycket som får *läsas av eller tas upp*,

4. villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, och

5. vem som är skäligen misstänkt för brottet eller brotten, *vid en åtgärd enligt 6 §*, eller vem en åtgärd enligt 7 § riktas mot.

I ett tillstånd som gäller kameraövervaknings- eller rumsavlyssningsuppgifter ska det även anges vilken plats tillståndet avser. Om tillståndet avser en viss person i stället för en viss plats ska det anges i beslutet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska även det anges i beslutet.

Tiden för tillståndet får inte bestämmas längre än nödvändigt. *När det gäller tid som infaller efter beslutet* får *tiden* inte överstiga en månad från dagen för beslutet.

1. vilket avläsningsbart informationssystem tillståndet avser,

2. vilken *uppgiftstyp* enligt 2 § första stycket som får *hämtas in*, *och*

3. vem som är skäligen misstänkt för brottet eller brotten, *om sådan uppgift finns*, eller vem en åtgärd enligt 7 § riktas mot.

I tillståndet *ska det även anges under vilken tid som verkställighet får ske. Tiden för verkställighet* får inte bestämmas längre än nödvändigt *och* får inte överstiga en månad från dagen för beslutet.

[7] Senaste lydelse 2024:566.

I tillståndet ska det även anges vilka uppgifter som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Villkor behöver inte anges om det framstår som obehövligt. Om ett tillstånd som gäller kamera-övervaknings- eller rumsavlyssningsuppgifter avser en viss person i stället för en viss plats ska villkor dock alltid anges.

Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska även det anges i beslutet.

18 a §

I ett tillstånd som gäller kamera-övervaknings- eller rumsavlyssningsuppgifter ska det, förutom de uppgifter som framgår av 18 §, anges vilken plats tillståndet avser. Om tillståndet avser en viss person i stället för en viss plats ska det anges i beslutet.

23 §

Den teknik som används i samband med hemlig dataavläsning ska anpassas efter *det tillstånd som beviljats. Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet. Om sådana uppgifter har lästs av eller tagits upp ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas.*

Vid verkställighet av hemlig dataavläsning ska *tekniken och tillvägagångssättet* anpassas efter *tillståndet*.

Om uppgifter av någon annan uppgiftstyp än de som anges i tillståndet har hämtats in ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. Upptagningar och uppteckningar av uppgifter som inte får hämtas in eller granskas enligt

	villkor i tillståndet ska förstöras i de delar de innehåller sådana uppgifter så snart det står klart att uppgifterna har hämtats in.
Uppgifter som anges i *första* stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.	Uppgifter som anges i *andra* stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.
Förbud att *läsa av eller ta upp* vissa uppgifter	**Förbud att *hämta in* vissa uppgifter**
27 §[8]	
Hemlig dataavläsning enligt 2 § första stycket 6 *eller 7* får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.	Hemlig dataavläsning enligt 2 § första stycket 6 får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.
Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram.	
Om det under verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *verkställigheten* omedelbart avbrytas *och upptagningar* och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.	Om det under *eller efter* verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *granskningen av dessa uppgifter* omedelbart avbrytas. *Upptagningar* och uppteckningar *ska* omedelbart förstöras i de delar som de omfattas av förbudet.
28 §[9]	
När hemlig dataavläsning används eller har använts under en förundersökning ska *det som gäller för hemlig avlyssning av elektronisk kommunikation enligt* 27 kap. 23 a och 24 §§ rättegångsbalken *i lydelsen före den 1 oktober 2023* tillämpas för åtgärden. *Det som gäller för hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning*	När hemlig dataavläsning används eller har använts under en förundersökning ska 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden.

[8] Senaste lydelse 2023:540.
[9] Senaste lydelse 2023:540.

som gäller rumsavlyssnings-uppgifter.

För underrättelse till en enskild vid hemlig dataavläsning under förundersökning gäller 27 kap. 31–33 §§ rättegångsbalken. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

29 §[10]

När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 *och 13* §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott *i lydelsen före den 1 oktober 2023* tillämpas.	När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12–*14* §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

31 §[11]

När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och *8* §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *i lydelsen före den 1 september 2024* tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.	När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och *7* §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.

[10] Senaste lydelse 2024:566.

[11] Senaste lydelse 2024:566. Ändringen innebär bl.a. att andra stycket tas bort.

Uppgifter som har kommit fram vid hemlig dataavläsning enligt 10 § får användas i en förundersökning endast efter tillstånd till hemlig dataavläsning enligt 4 eller 5 § som gäller kommunikationsövervaknings- eller platsuppgifter. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för beslut om att inleda en förundersökning.

Dokumentation

34 §
Beslut och åtgärder som rör hemlig dataavläsning ska dokumenteras.

---

1. Denna lag träder i kraft den 1 april 2025.
2. Äldre föreskrifter gäller fortfarande för tillstånd som har beviljats före ikraftträdandet.
3. För uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet gäller 28, 29 och 31 §§ i den äldre lydelsen.

2.3 Förslag till lag om ändring i lagen (2020:62) om hemlig dataavläsning

Härigenom föreskrivs i fråga om lagen (2020:62) om hemlig dataavläsning[1]

dels att 8 b § ska upphöra att gälla,

dels att 7, 8 a, 10, 15 och 29 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	7 §[2]
Ett tillstånd till hemlig dataavläsning som inte gäller rumsavlyssningsuppgifter får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för	Ett tillstånd till hemlig dataavläsning som inte gäller rumsavlyssningsuppgifter får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för
1. att en person kommer att utöva brottslig verksamhet som innefattar brott som anges i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, eller	
2. att brottslig verksamhet som innefattar brott som anges i 1 *eller 1 a* § den lagen kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.	2. att brottslig verksamhet som innefattar brott som anges i 1 § den lagen kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.
Ett tillstånd till hemlig dataavläsning som gäller rumsavlyssningsuppgifter får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för	
1. att en person kommer att utöva brottslig verksamhet som innefattar brott som anges i 1 b § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott, eller	
2. att brottslig verksamhet som anges i 1 b eller 1 c § den lagen kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.	

[1] Senaste lydelse av 8 b § 2024:566.

[2] Senaste lydelse 2024:566. Ändringen innebär bl.a. att andra stycket tas bort.

Ett tillstånd enligt första *eller andra* stycket får beviljas endast om åtgärden är av synnerlig vikt för att förhindra den brottsliga verksamheten.	Ett tillstånd enligt första stycket får beviljas endast om åtgärden är av synnerlig vikt för att förhindra den brottsliga verksamheten.

8 a §[3]

Ett tillstånd till hemlig dataavläsning enligt 7 § som gäller kameraövervakningsuppgifter får endast avse en plats där den person som åtgärden riktas mot kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Trots första stycket får tillståndet avse den person som åtgärden riktas mot i stället för en viss plats, om det finns särskilda skäl för det. Den hemliga dataavläsningen får då endast användas på en plats där den personen kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

10 §[4]

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 *eller 2 a* § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Vid hemlig dataavläsning enligt första stycket får meddelanden inte hindras att nå fram enligt 2 § andra stycket.

15 §[5]

Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser ett brott som anges i 27 kap. 34 § rättegångsbalken, får frågan även prövas av Stockholms tingsrätt.

Frågor om hemlig dataavläsning enligt 7 *och 8* §§ prövas av *den domstol som är behörig enligt 6 §*	Frågor om hemlig dataavläsning enligt 7–*10* §§ prövas av *Stockholms tingsrätt*.

[3] Senaste lydelse 2024:566. Ändringen innebär att andra stycket tas bort.
[4] Senaste lydelse 2024:566.
[5] Senaste lydelse 2023:540.

lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Frågor om hemlig dataavläsning enligt 9 eller 10 § prövas av Stockholms tingsrätt.

Lydelse enligt 2.2 *Föreslagen lydelse*

29 §[6]

När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12–14 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– *hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter*

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

Denna lag träder i kraft den 1 oktober 2028.

[6] Senaste lydelse 2025:000.

2.4 Förslag till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

Härigenom föreskrivs att 9 och 10 §§ lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 §	
I fråga om hemlig dataavläsning ska följande bestämmelser i lagen (2020:62) om hemlig dataavläsning tillämpas*:*	
– 11 § om förbud mot hemlig dataavläsning,	
– 12 och 13 §§ om tillträdestillstånd,	
– 16 § om offentligt ombud och sammanträde,	
– 18 § om tillståndets innehåll,	
– 20 § om verkställbarhet och upphävande av beslutet,	
– 21 § om underrättelse till Säkerhets- och integritetsskyddsnämnden,	
– 22–26 §§ om genomförande av hemlig dataavläsning, *och*	– 22–26 §§ om genomförande av hemlig dataavläsning,
– 32 § om tystnadsplikt.	– 32 § om tystnadsplikt*, och*
	– 34 § om dokumentation.
Det som i bestämmelserna sägs om den misstänkte ska i stället avse den eftersökte.	
10 §[1]	
Åklagare får besluta att uppgifter som har kommit fram vid användning av hemlig övervakning av elektronisk kommunikation enligt 3 § får användas för ett annat ändamål än det som har legat till grund för åtgärden.	Åklagare får besluta att uppgifter som har kommit fram vid användning av hemlig övervakning av elektronisk kommunikation enligt 3 § *och hemlig dataavläsning enligt 4 §* får användas för ett annat ändamål än det som har legat till grund för åtgärden.
Uppgifter som har kommit fram vid användning av hemlig dataavläsning enligt 4 § får användas i en förundersökning endast efter tillstånd till hemlig dataavläsning enligt bestämmelserna i lagen (2020:62) om hemlig dataavläsning. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för beslut om att inleda en förundersökning eller, om det har kommit fram uppgifter om före-	

[1] Ändringen innebär bl.a. att andra stycket tas bort.

stående brott, för att förhindra brott.

---

1. Denna lag träder i kraft den 1 april 2025.
2. Äldre föreskrifter gäller fortfarande för tillstånd som har beviljats före ikraftträdandet.
3. För uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet gäller 10 § i den äldre lydelsen.

2.5 Förslag till lag om ändring i lagen (2024:332) om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

Härigenom föreskrivs att lagen (2024:332) om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder ska utgå.

3 Ärendet och dess beredning

En särskild utredare fick den 22 juni 2022 i uppdrag att utvärdera lagen (2020:62) om hemlig dataavläsning inför ett ställningstagande till om lagen bör permanentas och om den i så fall bör ändras i något avseende (dir. 2022:82).

Utredningen, som antog namnet Utredningen om utvärdering av hemlig dataavläsning, överlämnade den 29 november 2023 betänkandet Hemlig dataavläsning – utvärdering och permanent lagstiftning (SOU 2023:78). Betänkandet har remissbehandlats.

En sammanfattning av betänkandet finns i *bilaga 1*. Betänkandets lagförslag finns i *bilaga 2*. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2023/02690).

I denna lagrådsremiss behandlar regeringen utredningens förslag.

4 Hemlig dataavläsning – ett verktyg i brottsbekämpningen

4.1 Ett tidsbegränsat tvångsmedel

Genom lagen (2020:62) om hemlig dataavläsning, som trädde i kraft den 1 april 2020, infördes ett nytt hemligt tvångsmedel: hemlig dataavläsning. Genom hemlig dataavläsning har de brottsbekämpande myndigheterna fått större möjligheter att avlyssna och övervaka personer som är misstänkta för eller förväntas begå allvarliga brott. Lagstiftningen är tidsbegränsad till och med utgången av mars 2025.

Hemlig dataavläsning innebär att de brottsbekämpande myndigheterna med någon form av tekniskt hjälpmedel i hemlighet bereder sig tillgång till exempelvis en mobiltelefon, en dator eller ett användarkonto till en kommunikationstjänst. På så sätt kan myndigheten bl.a. få kännedom om hur utrustningen används eller har använts och vilken information som finns i den. Metoden innebär att myndigheten dels bereder sig tillgång till utrustningen, dels tar del av uppgifterna, se propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 55).

Hemlig dataavläsning är ett komplement till andra tvångsmedel. Den hemliga dataavläsningen kan avse flera olika uppgifter, bl.a. uppgifter om innehåll i meddelanden eller platsuppgifter (1 och 2 §§ lagen om hemlig dataavläsning). Många av de uppgifter som kan hämtas in genom hemlig dataavläsning kan de brottsbekämpande myndigheterna, efter tillstånd, hämta in också genom andra tvångsmedel. I vissa fall är det emellertid inte praktiskt möjligt att hämta in uppgifterna med hjälp av andra tvångsmedel trots att myndigheterna har fått tillstånd att göra det. Det beror till stor del på att internetbaserad kommunikation ofta har krypterat innehåll som inte kan fångas upp i ett läs- eller avlyssningsbart skick genom övriga tvångsmedel. Lagen om hemlig dataavläsning infördes i syfte att återställa de brottsbekämpande myndigheternas förmåga att hämta in och ta del av

information (prop. 2019/20:64 s. 56, 93 och 125). Genom bestämmelserna om hemlig dataavläsning kan de brottsbekämpande myndigheterna genom en ny metod få tillgång till samma typ av information som genom andra hemliga tvångsmedel. Dessutom har myndigheterna fått möjlighet att i hemlighet komma åt uppgifter som finns lagrade i en kommunikationsutrustning eller som visar hur utrustningen används. Sådana uppgifter var inte åtkomliga genom hemliga tvångsmedel innan möjligheten till hemlig dataavläsning infördes.

Hemlig dataavläsning kan användas under en förundersökning om viss allvarlig brottslighet. Utanför en förundersökning kan hemlig dataavläsning användas i underrättelseverksamhet enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Utöver det kan hemlig dataavläsning användas vid särskild utlänningskontroll enligt lagen (2022:700) om särskild kontroll av vissa utlänningar.

Under de senaste åren har tillämpningsområdet för hemlig dataavläsning successivt utvidgats. Det innebär bl.a. att hemlig dataavläsning kan användas vid fler typer av brott än tidigare och vid flera brott som sammantaget har ett högt straffvärde. Det har även införts en möjlighet att använda hemlig dataavläsning i syfte att förhindra särskilt allvarlig brottslighet som förekommer inom kriminella nätverk, se propositionen Hemliga tvångsmedel – effektiva verktyg för att förhindra och utreda allvarliga brott (prop. 2022/23:126) och propositionen Preventiva tvångsmedel för att förebygga och förhindra allvarliga brott (prop. 2023/24:117). Sedan den 1 juli 2024 kan hemlig dataavläsning dessutom användas för att lokalisera personer enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, se propositionen Bättre möjligheter att verkställa frihetsberövanden (prop. 2023/24:108).

4.2 Skyddsmekanismer och rättssäkerhetsgarantier

Lagen om hemlig dataavläsning innehåller ett flertal skyddsmekanismer som syftar till att säkra att tillämpningen är rättssäker och inte innebär obefogade intrång i enskildas integritet. Som utgångspunkt prövas frågor om hemlig dataavläsning av en domstol efter ansökan av en åklagare. Det finns även en möjlighet för åklagare att under särskilda omständigheter besluta om tillstånd till hemlig dataavläsning interimistiskt, dvs. i avvaktan på rättens beslut. Beslutet om tillstånd ska i så fall, anmälas till rätten som därefter skyndsamt ska pröva ärendet. I ett tillstånd till hemlig dataavläsning ska det i regel anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

I alla ärenden om hemlig dataavläsning ska offentliga ombud medverka. Ombuden har till uppgift att bevaka enskildas integritetsintressen. Det finns också en skyldighet att i efterhand underrätta den enskilde om att hemlig dataavläsning har använts så snart det inte längre hindras av sekretess. Om underrättelsen inte har kunnat lämnas inom ett år och sex

månader från det att tvångsmedelsanvändningen avslutades ska i stället Säkerhets- och integritetsskyddsnämnden underrättas. För preventivlagen gäller motsvarande om en underrättelse inte har kunnat lämnas inom ett år från det att ärendet avslutades.

Hemlig dataavläsning får inte riktas mot vissa verksamheter, dels sådana där tystnadsplikt gäller enligt bestämmelser i tryckfrihetsförordningen och yttrandefrihetsgrundlagen, dels sådana som bedrivs av vissa särskilt utpekade yrkeskategorier som omfattas av tystnadsplikt, däribland advokater, viss sjukvårdspersonal och präster. Lagstiftningen innehåller också ett förbud mot att hämta in vissa uppgifter som omfattas av tystnadsplikt, t.ex. om de rör advokaters eller läkares verksamhet eller uppgifter som en präst fått under bikt eller enskild själavård. För användning av hemlig dataavläsning ställs det höga kvalifikationskrav som tar sikte på behovet av åtgärden i det enskilda fallet. Exempelvis får ett tillstånd till hemlig dataavläsning under en förundersökning eller i preventivt syfte för att förhindra viss allvarlig brottslighet bara beviljas om åtgärden är av synnerlig vikt. På samma sätt som för all användning av tvångsmedel gäller ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Enligt ändamålsprincipen får ett tvångsmedel användas endast för det ändamål som framgår av lagstiftningen. Behovsprincipen innebär att en myndighet får använda ett tvångsmedel bara när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig. Proportionalitetsprincipen kommer till uttryck i 3 § lagen om hemlig dataavläsning och innebär att ett tillstånd till hemlig dataavläsning endast får beviljas om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse. För att hemlig dataavläsning ska vara en proportionerlig åtgärd måste den som ansöker om hemlig dataavläsning först utreda eller uttömma möjligheterna till andra åtgärder. Hemlig dataavläsning är aktuellt först när andra åtgärder för att komma åt uppgifterna i fråga inte bedöms vara tillräckliga, skulle vara väsentligt svårare att genomföra eller kan förväntas leda till större integritetsintrång (prop. 2019/20:64 s. 214 och 215).

Säkerhets- och integritetsskyddsnämnden har till uppgift att utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel. Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps. Nämnden är också skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel och om användningen har skett i enlighet med lag.

Regeringen lämnar årligen en skrivelse om användningen av hemliga tvångsmedel, inklusive hemlig dataavläsning, till riksdagen. Skrivelsen baseras på den redovisning som Åklagarmyndigheten varje år sammanställer tillsammans med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket. Redovisningen innehåller bl.a. uppgifter om antalet meddelade tillstånd, hur många personer som varit föremål för åtgärderna och om uppgifterna som har kommit fram gjort nytta. Den parlamentariska kontrollen av hemlig dataavläsning är avsedd att vid sidan av andra rättssäkerhetsgarantier fylla en viktig funktion och bidra till allmänhetens insyn i myndigheternas tvångsmedelsanvändning. Granskningen är även avsedd att bidra till att det finns tillgång till nödvändiga

data för utvärderingen av lagen om hemlig dataavläsning inför ställningstagandet till om den ska permanentas (prop. 2019/20:64 s. 173).

5 Regleringen ska gälla utan tidsbegränsning

Regeringens förslag: Lagen om hemlig dataavläsning ska gälla utan tidsbegränsning.

Bestämmelserna som innebär att hemlig dataavläsning som gäller rumsavlyssningsuppgifter får användas i preventivt syfte för att förhindra brottslig verksamhet ska tidsbegränsas att gälla till utgången av september 2028. Även bestämmelserna som innebär att ett tillstånd till hemlig dataavläsning som gäller kameraövervaknings- eller rumsavlyssningsuppgifter i preventivt syfte kan knytas till en person ska tidsbegränsas på samma sätt.

Möjligheten till hemlig dataavläsning enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder ska gälla utan tidsbegränsning.

Regeringens bedömning: Bestämmelserna om hemlig dataavläsning ska även i fortsättningen finnas i en särskild lag.

Utredningens förslag och bedömning överensstämmer i huvudsak med regeringens. Utredningen uttalar sig dock inte om de bestämmelser om hemlig dataavläsning som är tidsbegränsade till utgången av september 2028 och lämnar inte något förslag när det gäller lagen om hemliga tvångsmedel för att verkställa frihetsberövande påföljder.

Remissinstanserna: En majoritet av remissinstanserna tillstyrker eller har inte några synpunkter på förslaget att lagen ska gälla utan tidsbegränsning, däribland *Brottsoffermyndigheten*, *Ekobrottsmyndigheten*, *Göta hovrätt*, *Integritetsskyddsmyndigheten*, *Malmö tingsrätt*, *Polismyndigheten* och *Åklagarmyndigheten*. *Justitiekanslern (JK)* och *Riksdagens ombudsmän (JO)* anser att utredningen har gjort en grundlig utvärdering och noggranna avvägningar mellan de brottsbekämpande myndigheternas behov och de integritetsrisker som utredningens förslag kan innebära för enskilda. Flera remissinstanser, bl.a. *ECPAT Sverige (ECPAT)*, Malmö tingsrätt, Integritetsskyddsmyndigheten och Polismyndigheten, framhåller att det finns ett mycket stort behov av hemlig dataavläsning för att effektivt kunna utreda, lagföra och bekämpa allvarlig brottslighet. *Brottsofferjouren Sverige* och Brottsoffermyndigheten uppmärksammar särskilt vikten av effektiva utredningsmetoder ur ett brottsofferperspektiv.

Bahnhof, *Sveriges advokatsamfund*, *Solna tingsrätt* och *Journalistförbundet* avstyrker att hemlig dataavläsning permanentas. Det gör också *Brottsförebyggande rådet* och *Civil Rights Defenders*, även om de anser att det finns ett behov av hemlig dataavläsning. Brottsförebyggande rådet och Solna tingsrätt menar, i likhet med *Lunds universitet,* att det underlag som har använts inte är tillräckligt robust för att kunna analysera nyttan av

tvångsmedlet och att det därför inte är möjligt att ta ställning till behovet av en lagstiftning utan tidsbegränsning. Brottsförebyggande rådet och Solna tingsrätt föreslår att den tillfälliga lagen i stället förlängs. Sveriges advokatsamfund anser att den analys som gjorts talar emot att permanenta hemlig dataavläsning eftersom den visar att nyttan och effektiviteten av tvångsmedlet har varit begränsad. Advokatsamfundet anser att tillämpningsområdet i vart fall bör avgränsas till allvarligare brottslighet med högre straffvärden än vad som gäller för användningen av de övriga tvångsmedlen. *Föreningen för digitala fri- och rättigheter* avråder från att permanenta tvångsmedlet utifrån försiktighetsprincipen och mot bakgrund av komplexiteten på området. Civil Rights Defenders anser att hemlig dataavläsning inte bör permanentas innan tillräckliga garantier har införts till skydd för den personliga integriteten. Bahnhof anser att Säkerhets- och integritetsskyddsnämnden behöver tillföras en betydande resursförstärkning och befogenheter i sin tillsyn för att lagen ska uppfylla befogade krav på rättssäkerhet, och att tvångsmedlet inte bör permanentas om så inte görs.

Säkerhets- och integritetsskyddsnämnden varken tillstyrker eller avstyrker förslaget att permanenta hemlig dataavläsning men framhåller att användningen av tvångsmedlet har inneburit en tydligt ökad risk för den personliga integriteten. Många remissinstanser, däribland *Centrum för rättvisa*, *Integritetsskyddsmyndigheten*, *Stockholms tingsrätt* och *Svea hovrätt*, anser att det behövs en samlad översyn av regleringen om hemliga tvångsmedel. *Föreningen för digitala fri- och rättigheter* och *Civil Rights Defenders* anser att en sådan översyn bör göras innan möjligheten att använda hemlig dataavläsning permanentas.

Polismyndigheten och *Åklagarmyndigheten* efterfrågar utökade möjligheter att använda hemlig dataavläsning i det internationella rättsliga samarbetet. Polismyndigheten ser också ett ökat behov av att kunna använda hemlig dataavläsning i underrättelseverksamhet utan krav på personidentifiering. *Säkerhetspolisen* anser att behovet av följdändringar i regelverket för det internationella rättsliga samarbetet bör övervägas ytterligare.

Av de remissinstanser som uttalar sig särskilt om bestämmelsernas placering instämmer *Stockholms tingsrätt* och *Svea hovrätt* i utredningens bedömning medan *Göta hovrätt* och *Helsingborgs tingsrätt* förordar att bestämmelserna inarbetas bland reglerna om hemliga tvångsmedel i rättegångsbalken.

Skälen för regeringens förslag och bedömning

Behovet av hemlig dataavläsning är fortsatt stort

Hemlig dataavläsning infördes som ett sätt att behålla de brottsbekämpande myndigheternas förmåga att i den digitala miljön hämta in information när de befintliga tvångsmedlen inte längre kunde täcka behovet. Utöver att teknik- och samhällsutvecklingen har lett till att de hemliga tvångsmedlen förlorat i effektivitet konstaterades att beslag av elektronisk utrustning ger allt mindre information. Det beror dels på att kommunikation med krypterad information har blivit allt vanligare, dels på att vissa uppgifter som överförs digitalt över huvud taget inte lagras. Regeringen konstaterade att det finns ett påtagligt behov av hemlig

dataavläsning och bedömde att det kunde förväntas vara ett effektivt tvångsmedel (prop. 2019/20:64 s. 74–83).

Den förväntan som fanns om att hemlig dataavläsning skulle vara ett effektivt tvångsmedel i den brottsbekämpande verksamheten ansågs tala för att åtgärden skulle göras permanent redan vid införandet. Mot bakgrund av att det var fråga om en ny utredningsmetod som dessutom innebär vissa risker för den personliga integriteten bedömdes dock att lagen om hemlig dataavläsning inledningsvis skulle tidsbegränsas, i likhet med många andra lagar och bestämmelser om hemliga tvångsmedel. För att minimera risken för att lagen görs permanent utan ett fullgott underlag bestämdes lagens giltighetstid till fem år. Regeringen uttalade att nyttan, behovet och proportionaliteten av hemlig dataavläsning återigen skulle analyseras och bedömas vid en framtida utvärdering och beredning (prop. 2019/20:64 s. 99–101).

Mot bakgrund av de tidigare förarbetsuttalandena har utredningen analyserat om nyttan av hemlig dataavläsning har motsvarat de förväntningar som fanns då tvångsmedlet infördes. *Brottsförebyggande rådet*, *Lunds universitet* och *Solna tingsrätt* framför synpunkter på det underlag som utredningen har använt som de menar inte är tillräckligt robust för att möjliggöra en analys av nyttan. De anser därför att hemlig dataavläsning inte bör permanentas. Även *Sveriges advokatsamfund* avstyrker förslaget och framhåller att utredningens analys visar att nyttan och effektiviteten av tvångsmedlet hittills har varit begränsad.

Regeringen anser att utredningen har genomfört en samlad och gedigen kartläggning av användningen av hemlig dataavläsning. Som utredningen framhåller är det en komplicerad uppgift att bedöma nyttan och effektiviteten i hemliga tvångsmedel eftersom de är svåra att mäta i siffror och andelstal. Utvärderingen kompliceras också av att flera andra hemliga tvångsmedel ofta används parallellt med hemlig dataavläsning och att resultatet av tvångsmedlen samverkar med varandra. Det kan då vara svårt att med säkerhet avgöra vilken effekt en viss åtgärd har haft. Det jämförelsematerial som finns att tillgå utgörs, på grund av beslutens natur, av de brottsbekämpande myndigheternas och regeringens årliga redovisningar om användningen av hemliga tvångsmedel. Utredningen har använt dessa uppgifter som utgångspunkt för en fortsatt och mer resonerande analys. Utredningen har också tagit del av de brottsbekämpande myndigheternas beskrivningar av tillämpningen, liksom exempel i form av anonymiserade ärenden där hemlig dataavläsning har använts och varit till nytta. I likhet med bl.a. *JK* och *JO* anser regeringen att utredningen har gjort en grundlig utvärdering av lagstiftningen. Det underlag som utredningen har grundat utvärderingen på bedöms vara tillräckligt omfattande och robust för att på nytt kunna ta ställning till nyttan av hemlig dataavläsning.

Som *Sveriges advokatsamfund* påpekar har den kvantitativt uppskattade nyttan av hemlig dataavläsning, enligt de brottsbekämpande myndigheternas redovisningar, generellt sett varit något lägre än för de övriga hemliga tvångsmedlen, se regeringens skrivelse Redovisning av användningen av hemliga tvångsmedel under 2022 (skr. 2023/24:47). Samtidigt finns det, som utredningen redogör för, förhållandevis stora variationer mellan vilken typ av effekt som avses och vilken uppgiftstyp som jämförs i fråga om nyttobedömningen. Hemlig dataavläsning kan också vara

svårare att verkställa än andra tvångsmedel, bl.a. på grund av att det krävs ett omfattande förberedelsearbete och på grund av de tekniska svårigheter som kan uppstå inför och under verkställigheten. Som utredningen framhåller motsvarar därför inte antalet redovisade tillstånd antalet verkställda tillstånd.

Det kan dock konstateras att hemlig dataavläsning, såväl under förundersökning som i underrättelseverksamhet, har använts i större utsträckning än vad som uppskattades vid lagens införande. I likhet med andra hemliga tvångsmedel har hemlig dataavläsning framför allt använts i ärenden om narkotikabrottslighet och våldsbrott. Antalet tillstånd till hemlig dataavläsning har också ökat för varje år, vilket enligt utredningen kan antas bero på de senaste årens stegrande brottsutveckling och på att de brottsbekämpande myndigheterna har fått en ökande förmåga att överbrygga de tekniska svårigheter för verkställande av hemlig dataavläsning som förutspåddes då tvångsmedlet infördes. Att hemlig dataavläsning har tillämpats i ökande omfattning talar både för att åtgärden har medfört nytta i brottsbekämpningen och för att det finns ett fortsatt behov av tvångsmedlet. Den bilden förstärks av de beskrivningar och praktiska exempel som de brottsbekämpande myndigheterna har redovisat till utredningen. Av dem framgår att hemlig dataavläsning i många fall har varit ett helt avgörande verktyg i den brottsbekämpande verksamheten. Den hemliga dataavläsningen har lett till både konkreta uppgifter om begångna brott och uppgifter som har kunnat användas för att förhindra allvarlig brottslighet.

Behovet och nyttan av hemlig dataavläsning bekräftas också av flera remissinstanser. *Polismyndigheten* framhåller att hemlig dataavläsning har inneburit ett genombrott i kampen mot den allvarliga och organiserade brottsligheten. *Tullverket* konstaterar att den organiserade brottsligheten har ökat i omfattning och blivit mer samhällshotande under de senaste åren, vilket medför ett behov av effektiva hemliga tvångsmedel för att kunna utreda och lagföra brott såsom storskalig narkotikasmuggling. *ECPAT* anför att hemlig dataavläsning kan ha avgörande betydelse i förundersökningar om sexualbrott mot barn och barnpornografibrott, särskilt med beaktande av att det blir alltmer vanligt att kommunikationen mellan förövare sker med krypterad information. *Brottsofferjouren Sverige* och *Brottsoffermyndigheten* framhåller betydelsen av hemlig dataavläsning ur ett brottsofferperspektiv eftersom en fällande dom kan vara ett nödvändigt steg i upprättelsen för brottsoffer.

Sammanfattningsvis anser regeringen, i likhet med utredningen och flertalet remissinstanser, att det fortfarande finns ett påtagligt behov av hemlig dataavläsning för att möta den brottsutveckling som skett parallellt med den snabba tekniska utvecklingen och de förändrade kommunikationsvanorna. Om något har detta behov endast accentuerats ytterligare, jämfört med när hemlig dataavläsning först infördes. Det råder enligt regeringen heller ingen tvekan om att åtgärden kommer till avsevärd nytta i de brottsbekämpande myndigheternas verksamhet.

Det finns övervägande skäl för att lagstiftningen ska gälla utan tidsbegränsning

Utifrån utvärderingen har utredningen på nytt vägt nyttan och behovet av hemlig dataavläsning mot de integritetsrisker som tvångsmedlet kan innebära för enskilda. Utredningens slutsats är att det är proportionerligt att de brottsbekämpande myndigheterna får använda hemlig dataavläsning som tvångsmedel, såväl under en förundersökning som i underrättelseverksamhet. Enligt utredningen finns det inget som tyder på att behovet av hemlig dataavläsning skulle vara av tillfällig natur eller att reglerna av andra skäl bör vara tidsbegränsade. Utredningen föreslår att lagen om hemlig dataavläsning ska gälla utan begränsning i tid.

Integritetsskyddsmyndigheten och *Säkerhets- och integritetsskyddsnämnden* påpekar att hemlig dataavläsning kan ge de brottsbekämpande myndigheterna tillgång till en stor mängd information om enskilda och därmed innebära särskilda risker för intrång i enskildas personliga integritet. Säkerhets- och integritetsskyddsnämnden är kritisk till att skyddet för den personliga integriteten anses väga så lätt.

Det är av grundläggande betydelse i en rättsstat att rätten till skydd för privat- och familjeliv respekteras. För en effektiv brottsbekämpning är det samtidigt nödvändigt att det finns tillräckliga befogenheter för de brottsbekämpande myndigheterna att i vissa väl avgränsade fall kunna använda hemliga tvångsmedel som ett yttersta hjälpmedel. När det gäller hemlig dataavläsning avgränsas tillämpningsområdet på ett ändamålsenligt och tydligt sätt och riskerna för den personliga integriteten balanseras med kontrollmekanismer och andra rättssäkerhetsgarantier. Till exempel prövas frågor om tillstånd till hemlig dataavläsning av domstol och ett offentligt ombud, med uppgift att bevaka enskildas integritetsintressen, ska alltid delta i tillståndsprövningen i domstol (se avsnitt 4.2). Utredningen lämnar dessutom flera förslag som syftar till att säkerställa att lagstiftningen står i ännu bättre överensstämmelse med de högt ställda krav på rättssäkerhet och de krav på skydd för enskildas personliga integritet som följer av regeringsformen, den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga), se mer om dessa förslag i avsnitt 8. Ur integritetshänseende är också Säkerhets- och integritetsskyddsnämndens tillsyn över användningen av hemlig dataavläsning en viktig del av den externa kontroll som görs av tvångsmedelsanvändningen. För att den tillsynen ska kunna bedrivas effektivt är det, som både *JO* och *Bahnhof* betonar, avgörande att nämnden har tillräckliga resurser till sitt förfogande, se mer om det i avsnitt 10.

Utredningens förslag att lagen om hemlig dataavläsning ska gälla utan tidsbegränsning har föregåtts av noggranna avvägningar. I likhet med flertalet remissinstanser instämmer regeringen i utredningens slutsats att de brottsbekämpande myndigheternas behov av hemlig dataavläsning som verktyg för att bekämpa allvarlig brottslighet väger så tungt att det motiverar det intrång som åtgärden innebär för den personliga integriteten.

Flera remissinstanser framhåller att de ser ett behov av en samlad översyn på tvångsmedelsområdet i syfte att förenkla och harmonisera reglerna. *Föreningen för digitala fri- och rättigheter* och *Civil Rights*

Defenders anser att en sådan översyn bör genomföras innan tidsbegränsningen av lagen om hemlig dataavläsning tas bort. *Brottsförebyggande rådet* och *Solna tingsrätt* anser att lagen om hemlig dataavläsning bör förlängas för att möjliggöra en ny och mer ingående utvärdering vid ett senare tillfälle.

Regeringen kan konstatera att flera åtgärder har vidtagits på senare år för att genom hemliga tvångsmedel ge de brottsbekämpande myndigheterna bättre förutsättningar att utreda allvarlig brottslighet och förbättrade möjligheter att förhindra brott och avbryta pågående brottslighet (prop. 2022/23:126 och prop. 2023/24:117). Lagändringar om utökade möjligheter att använda hemliga tvångsmedel, även hemlig dataavläsning, trädde i kraft den 1 oktober 2023 och den 1 september 2024. Av hänsyn till den ökade risken för integritetsintrång och för att kunna möjliggöra en samlad utvärdering har vissa av ändringarna tidsbegränsats till utgången av september 2028.

Även med beaktande av de förändringar som nyligen skett på området anser regeringen att underlaget är tillräckligt för att nu – innan en översyn har gjorts på området – bedöma om lagen om hemlig dataavläsning bör gälla utan tidsbegränsning. Med hänsyn till brottsutvecklingen och den tekniska utvecklingen är det tydligt att behovet av hemlig dataavläsning inte kommer att minska inom överskådlig tid. Det finns därför inte skäl för att, så som *Brottsförebyggande rådet* och *Solna tingsrätt* föreslår, förlänga lagstiftningen utan den bör nu permanentas.

Regeringen delar utredningens bedömning att de grundläggande förutsättningarna för användning av hemlig dataavläsning enligt lagen om hemlig dataavläsning även fortsättningsvis ska vara desamma som i dag. Eftersom hemlig dataavläsning redan i dag endast får användas vid allvarlig brottslighet finns det inte skäl för att begränsa tillämpningsområdet till ännu allvarligare brottslighet, på det sätt som *Sveriges advokatsamfund* föreslår.

Hemlig dataavläsning kan även användas i det internationella rättsliga samarbetet enligt lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk utredningsorder. Utredningen bedömer att det regelverket är ändamålsenligt och proportionerligt utformat och att några författningsändringar inte är nödvändiga. *Polismyndigheten* och *Åklagarmyndigheten* är av motsatt uppfattning och anser att det finns anledning att utvidga tillämpningsområdet för hemlig dataavläsning enligt de nämnda lagarna. *Polismyndigheten* efterfrågar även utökade möjligheter att i underrättelseverksamheten använda hemlig dataavläsning utan krav på personidentifiering, vilket inte har analyserats av utredningen. Inom ramen för detta lagstiftningsärende saknas det beredningsunderlag för att utvidga tillämpningsområdet på det sätt som Polismyndigheten och Åklagarmyndigheten efterfrågar.

Bestämmelsernas placering

När hemlig dataavläsning infördes bedömde regeringen, mot bakgrund av att reglerna gäller både under och utom förundersökning, att det skulle vara svårt att införa reglerna i befintliga lagar utan att behöva upprepa många bestämmelser (prop. 2019/20:64 s. 100). Bestämmelserna om hemlig dataavläsning är därför placerade i en särskild lag. Lagrådet uttalade att

detta var acceptabelt eftersom det var fråga om en tillfällig lagstiftning, men ansåg att lagstiftningstekniken borde övervägas på nytt om det blir fråga om att förlänga eller permanenta hemlig dataavläsning (Lagrådets yttrande över bl.a. förslag till lag om hemlig dataavläsning, utdrag ur protokoll vid sammanträde 2019-11-18).

Utredningen har övervägt alternativet att arbeta in bestämmelserna i lagstiftningen om de övriga hemliga tvångsmedlen. Utredningen bedömer att det för närvarande framstår som ett sämre och mer svåröverskådligt alternativ än att även fortsatt låta hemlig dataavläsning regleras i en egen lag. Regeringen har förståelse för *Göta hovrätts* och *Helsingborgs tingsrätts* synpunkt om att regleringen skulle bli mer lättöverskådlig om det gick att samla bestämmelserna i regleringen av hemliga tvångsmedel i rättegångsbalken. I 27 kap. rättegångsbalken regleras dock endast tvångsmedel under förundersökning. Att föra in alla bestämmelser om hemlig dataavläsning i det kapitlet skulle innebära ett tydligt avsteg från systematiken. Det skulle heller inte vara ändamålsenligt eller underlätta för förståelsen om bestämmelserna om hemlig dataavläsning skulle delas upp i flera olika lagar. Av det skälet instämmer regeringen, i likhet med *Stockholms tingsrätt* och *Svea hovrätt*, i utredningens bedömning att nuvarande placering av bestämmelserna i en egen lag för närvarande är det lämpligaste alternativet.

Behov av följdändringar

Genom de lagändringar som trädde i kraft den 1 oktober 2023 och den 1 september 2024 har de brottsbekämpande myndigheterna fått utökade möjligheter att använda hemliga tvångsmedel, även hemlig dataavläsning. Vissa av ändringarna är tidsbegränsade till utgången av september 2028. I preventivlagen handlar det om det utvidgade tillämpningsområdet som möjliggör användning av hemliga tvångsmedel i syfte att förhindra särskilt allvarlig brottslighet som förekommer inom kriminella nätverk (prop. 2022/23:126 s. 84 och 85). Det handlar även om möjligheterna att använda hemlig rumsavlyssning i preventivt syfte och att knyta ett tillstånd till preventiv hemlig kameraövervakning eller hemlig rumsavlyssning till en person i stället för en plats (prop. 2023/24:117 s. 134 och 135). I och med att lagen om hemlig dataavläsning nu föreslås gälla utan tidsbegränsning bör, i enlighet med tidigare uttalanden i förarbetena, även möjligheten att använda hemlig dataavläsning som gäller rumsavlyssningsuppgifter i preventivt syfte tidsbegränsas till utgången av september 2028. Detsamma bör gälla för möjligheten att, i preventivt syfte, knyta ett tillstånd till hemlig dataavläsning som gäller kameraövervaknings- eller rumsavlyssningsuppgifter till en person i stället för en plats. Detta bör ske genom att det införs en ändringslag, med ikraftträdande den 1 oktober 2028, där de nämnda möjligheterna att använda hemlig dataavläsning tas bort (se avsnitt 9). I ändringslagen bör det även göras vissa lagtekniska justeringar med anledning av att regleringen om ett utvidgat tillämpningsområdet i preventivlagen och om en utvidgad brottskatalog i inhämtningslagen upphör att gälla vid utgången av september 2028.

Med hänsyn till att lagen om hemlig dataavläsning är tidsbegränsad beslutades att möjligheterna att använda hemlig dataavläsning enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande

påföljder också skulle tidsbegränsas (prop. 2023/24:108 s. 81, bet. 2023/24:JuU26, rskr. 2023/24:216). Det infördes en ändringslag där möjligheten att använda hemlig dataavläsning togs bort, med ikraftträdande den 1 april 2025, se lagen (2024:332) om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder. Eftersom lagen om hemlig dataavläsning nu föreslås gälla utan tidsbegränsning finns det inte längre något skäl att tidsbegränsa regleringen av hemlig dataavläsning i lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder. Ändringslagen bör därför utgå.

6 Tydligare regler om hemlig dataavläsning

6.1 Innebörden av hemlig dataavläsning

Regeringens förslag: Definitionen av hemlig dataavläsning förtydligas på så sätt att det anges att hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling och åtkomliga i ett avläsningsbart informationssystem, hämtas in i hemlighet med ett tekniskt hjälpmedel.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* tillstyrker förslaget. *Journalistförbundet* instämmer i att definitionen hellre bör utgå från att uppgifter hämtas in än att de läses av och tas upp men anser att det är otydligt att tvångsmedlet kallas hemlig dataavläsning. Ingen annan remissinstans uttalar sig särskilt i frågan.

Skälen för regeringens förslag: Eftersom hemlig dataavläsning innebär inskränkningar i den enskildes fri- och rättigheter är det av största vikt att tvångsmedlet avgränsas på ett tydligt sätt. Det är därför angeläget att definitionen av hemlig dataavläsning i lagtext är korrekt och fullständig.

Enligt den nuvarande definitionen innebär hemlig dataavläsning att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem (1 § första stycket lagen om hemlig dataavläsning). Att uppgifter läses av syftar både på den tekniska process som utförs av en dator eller annat tekniskt hjälpmedel, för att exempelvis göra viss information läsbar, och på den process som äger rum när en person som ansvarar för hemlig dataavläsning tar del av innehållet i informationen. Att uppgifter tas upp innebär att de kan sparas för att granskas i efterhand (prop. 2019/20:64 s. 210).

Utredningen anser att det finns goda skäl att på nytt överväga definitionen av hemlig dataavläsning i syfte att skapa en tydligare och därmed mer förutsebar reglering. Utredningen föreslår att definitionen ändras på så sätt att det i bestämmelsen anges att uppgifter hämtas in i stället för att de läses av eller tas upp. Någon ändring i sak är däremot inte

avsedd. *Säkerhets- och integritetsskyddsnämnden* anser att utredningens förslag medför en tydligare reglering som i större utsträckning återspeglar sättet som tvångsmedlet verkställs på.

Utredningens förslag ska ses mot bakgrund av hur hemlig dataavläsning utförs. Verkställigheten består av dels en inhämtningsfas, dels en bearbetningsfas. Inhämtningsfasen innebär att informationen läses av och förs över från det avläsningsbara informationssystemet till den brottsbekämpande myndigheten. Under bearbetningsfasen bearbetas informationen, t.ex. genom förädling, sortering och filtrering, för att därefter granskas. I den nuvarande definitionen av hemlig dataavläsning anges inte uttryckligen att de verkställande myndigheterna hämtar in uppgifterna för att ta del av dem efter att de tagits upp. Enligt utredningen har företrädare för de brottsbekämpande myndigheterna och domstolarna framfört att det innebär att definitionen av hemlig dataavläsning i vissa avseenden kan vara missvisande och orsaka tillämpningssvårigheter. Uttrycket ”läses av eller tas upp” återkommer nämligen i flera bestämmelser i lagen om hemlig dataavläsning som både tar sikte på själva inhämtningen och på hur uppgifter som har hämtats in ska hanteras. Mot bakgrund av hur hemlig dataavläsning utförs och hur övriga bestämmelser i lagen är uppbyggda anser utredningen att definitionen av hemlig dataavläsning bör begränsas till själva inhämtningen av uppgifter.

Regeringen instämmer i utredningens bedömning att innebörden av hemlig dataavläsning bör kunna utläsas i lagtexten och att definitionen bör begränsas till själva inhämtningen. Att inhämtade uppgifter får bearbetas och granskas följer både direkt och indirekt av andra bestämmelser i lagen. Som utredningen föreslår framstår det lämpligt att använda samma uttryck som återfinns i rättegångsbalkens bestämmelse om övervakning av elektronisk kommunikation (27 kap. 19 §) och genomgående i inhämtningslagen. Regeringen anser däremot inte att det finns skäl att, som *Journalistförbundet* föreslår, byta namn på tvångsmedlet hemlig dataavläsning.

6.2 Regleringen av vilka uppgiftstyper som får hämtas in

Regeringens förslag: Uppdelningen mellan lagrade uppgifter och uppgifter som visar hur viss teknisk utrustning används tas bort. I stället samlas regleringen av uppgifter som är åtkomliga i ett informationssystem utan att vara kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter, platsuppgifter, kameraövervakningsuppgifter och rumsavlyssningsuppgifter i en uppgiftstyp.

Regeringens bedömning: Det bör inte införas någon huvudregel för vilka typer av uppgifter som ska omfattas av ett tillstånd.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår också att det ska införas en huvudregel för vilka uppgiftstyper som ska omfattas av ett tillstånd.

Remissinstanserna: *Civil Rights Defenders* tillstyrker förslaget om att ta bort uppdelningen mellan lagrade uppgifter och uppgifter som visar hur

viss teknisk utrustning används. *Säkerhets- och integritetsskyddsnämnden* anser att förslaget försämrar möjligheterna att genom olika uppgiftstyper differentiera åtgärderna men anser att förslaget är godtagbart med hänsyn till möjligheten att begränsa ett tillstånd genom villkor.

Göta hovrätt, *Helsingborgs tingsrätt*, *Malmö tingsrätt*, *Skatteverket*, *Solna tingsrätt* och *Stockholms tingsrätt* avstyrker eller ifrågasätter behovet av den huvudregel som utredningen föreslår om vilka uppgiftstyper som ett tillstånd ska omfatta. Göta hovrätt, Stockholms tingsrätt och Skatteverket anför att en sådan bestämmelse riskerar att medföra att kravet på differentiering i tillståndsgivningen åsidosätts och att prövningen blir slentrianmässig i den delen. *Säkerhets- och integritetsskyddsnämnden* anser att förslaget riskerar att medföra att uppgifterna inte differentieras på det sätt som avsågs när lagstiftningen infördes.

Skälen för regeringens förslag och bedömning

En uppgiftstyp för övriga uppgifter som är åtkomliga i ett informationssystem

Hemlig dataavläsning kan avse en stor mängd olika information som har delats upp i sju olika uppgiftstyper. När ett tillstånd till hemlig dataavläsning beslutas ska en bedömning göras i det enskilda fallet av vilka uppgiftstyper som ska få hämtas in. Tillståndet omfattar alltså inte per automatik alla uppgiftstyper. Att det på så sätt görs en differentiering av uppgifterna har ansetts öka graden av rättssäkerhet (prop. 2019/20:64 s. 107).

De sju uppgiftstyperna preciseras i 2 § lagen om hemlig dataavläsning som

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,
6. övriga lagrade uppgifter, och
7. övriga uppgifter som visar hur viss teknisk utrustning används.

Uppgiftstyperna har, med undantag för uppgifterna i punkterna 6 och 7, sin motsvarighet i de andra hemliga tvångsmedlen.

I punkten 6 ingår uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte omfattas av de tidigare uppgiftstyperna (s.k. lagrade uppgifter). Av tidigare förarbeten framgår att uppgifterna kan vara lagrade varaktigt eller temporärt. Det saknar betydelse i vilket format uppgifterna har lagrats så länge de är lagrade i informationssystemet när avläsningen eller upptagningen genomförs. Det kan t.ex. handla om datafiler, såsom text-, bild- och ljudfiler, men också om program- eller systemfiler. Vidare kan en lagrad uppgift vara ett meddelande som sparats som utkast i ett program för meddelanden eller e-post. Eftersom begreppet avläsningsbart informationssystem innefattar utrustning som anslutits till ett sådant system kan även uppgifter som finns lagrade på ett externt lagringsmedium som kopplats in i en dator läsas av eller tas upp. När det är fråga om uppgifter som är lagrade i ett avläsningsbart informations-

system, t.ex. på ett användarkonto för en internetbaserad lagringstjänst, anses uppgifterna lagrade i informationssystemet om de kan tillgängliggöras med det (prop. 2019/20:64 s. 213).

Med uppgifter som visar hur ett avläsningsbart informationssystem används, s.k. användningsuppgifter, avses uppgifter om vad en användare använder ett informationssystem till. Det kan exempelvis handla om användning som inte leder till att information lagras, t.ex. vilka program eller applikationer som körs, anteckningar som görs och utkast till meddelanden som inte sparas (prop. 2019/20:64 s. 214). Även punkten 7 är sekundär till de övriga punkterna. Den avser endast realtidsuppgifter. Om en uppgift lagras på informationssystemet faller den alltså inte in under punkten.

Utredningen föreslår att de uppgifter som är åtkomliga i ett informationssystem men som inte ingår i någon av punkterna 1–5 ska samlas i en gemensam punkt. Syftet är att göra lagstiftningen tydligare och mer förutsebar. Eftersom de flesta uppgifter som finns i ett informationssystem lagras, i vart fall tillfälligt, är det endast en begränsad mängd uppgifter som faller in under punkten 7. Även realtidsuppgifter som uppstår när en dator används, t.ex. information om att en fil öppnas, uppstart eller stängning av program och anslutning av externa lagringsmedier, sparas ibland i internminnet eller tillfälligt i processorn. Om sådana uppgifter hämtas in i realtid kan de falla under punkten 7, men om uppgifterna finns lagrade, även om det bara är tillfälligt, kan de i stället sortera under punkten 6.

Som utredningen konstaterar är differentieringen av uppgifter ett viktigt led i den proportionalitetsbedömning som alltid ska göras. Uppdelningen av den information som faller under 2 § första stycket 6 respektive 7 är dock inte tydlig. Det förefaller i många fall vara slumpmässigt om användningsuppgifter lagras eller inte. I praktiken kan uppgiftstyperna sällan särskiljas. Enligt utredningen beviljas vanligtvis tillstånd till hemlig dataavläsning även för uppgifter enligt punkten 6 om det är aktuellt med uppgifter enligt punkten 7. De gränsdragningssvårigheter som finns talar för att uppgiftstyperna inte bör vara uppdelade i två olika punkter. Om regleringen av de uppgiftstyper som faller in under punkterna 6 och 7 samlas skulle lagstiftningen bli tydligare, mer förutsebar och i större utsträckning teknikneutral. Som *Säkerhets- och integritetsskyddsnämnden* framhåller kan ett tillstånd till hemlig dataavläsning dessutom begränsas genom villkor, t.ex. om att endast användningsuppgifter får hämtas in, om det bedöms ändamålsenligt i det enskilda fallet. Eftersom förslaget inte innebär att myndigheterna får ökade möjligheter att hämta in information utan enbart syftar till att göra användningen av hemlig dataavläsning tydligare och mer förutsebar, bedömer regeringen att förslaget inte kommer att få någon påverkan på enskildas personliga integritet. Sammanfattningsvis bör förslaget därför genomföras.

Det bör inte införas någon huvudregel för vilka uppgifter som ett tillstånd ska omfatta

I ett tillstånd till hemlig dataavläsning ska det anges vilken typ av uppgift som får hämtas in (18 § första stycket lagen om hemlig dataavläsning). Utredningen föreslår att det ska införas en huvudregel om att ett tillstånd till hemlig dataavläsning ska omfatta alla uppgiftstyper förutom kamera-

övervaknings- och rumsavlyssningsuppgifter, om inget annat beslutas eller framgår av andra bestämmelser. Utredningens förslag bör läsas i ljuset av vissa uttalanden som Säkerhets- och integritetsskyddsnämnden gjort i sin granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts. Säkerhets- och integritetsskyddsnämnden har särskilt uppmärksammat att majoriteten av de granskade tillstånden har omfattat alla uppgiftstyper med undantag för kameraövervaknings- och rumsavlyssningsuppgifter. Enlig Säkerhets- och integritetsskyddsnämnden väcker det frågan om behovet av uppgifter i varje enskilt fall har varit styrande på det sätt som lagstiftaren ansett (Säkerhets- och integritetsskyddsnämndens uttalande med beslut den 15 december 2021, dnr 92-2020).

Utredningen framhåller att det kan vara svårt att på förhand förutse var i informationssystemet som den eftersökta informationen kommer att hittas, vilket försvårar bedömningen av vilka uppgiftstyper som bör ingå i ett tillstånd. De uppgiftstyper som, enligt den huvudregel som utredningen föreslår, ska ingå i ett tillstånd motsvarar enligt utredningen det behov som de brottsbekämpande myndigheterna vanligtvis har och de omfattas också ofta i praktiken av ett tillstånd. Av samma skäl ger ett tillstånd till hemlig avlyssning av elektronisk kommunikation även rätt att vidta åtgärder enligt reglerna om hemlig övervakning av elektronisk kommunikation (27 kap. 18 § andra stycket rättegångsbalken). Syftet med utredningens förslag om en huvudregel är att lagstiftningen bättre ska spegla verkligheten och att den ska vara tydligare.

Av rättssäkerhetsskäl är det dock viktigt att det görs en differentiering av vilka uppgifter som ska ingå i ett tillstånd till hemlig dataavläsning och en proportionalitetsbedömning utifrån myndigheternas behov och risken för intrång i enskildas personliga integritet. Som *Göta hovrätt*, *Skatteverket* och *Stockholms tingsrätt* framhåller finns en risk att en sådan huvudregel som utredningen föreslår uppfattas som en presumtion för vilka uppgiftstyper ett tillstånd ska omfatta. En sådan ordning skulle, i linje med vad *Säkerhets- och integritetsskyddsnämnden* anför, minska betydelsen av kravet på att differentiera uppgifterna. Utifrån hur uppdelningen av uppgiftstyper ser ut och med hänsyn till det behov som de brottsbekämpande myndigheterna vanligtvis har framstår det i och för sig som naturligt att ett tillstånd till hemlig dataavläsning ofta omfattar alla uppgiftstyper förutom kameraövervaknings- och rumsavlyssningsuppgifter. Den nuvarande regleringen hindrar inte heller en sådan tillämpning. Att införa en huvudregel enligt utredningens förslag riskerar emellertid att skapa en osäkerhet vid tillståndsprövningen. Förslaget i denna del bör därför inte genomföras.

7 Bättre möjligheter att utreda vem som skäligen kan misstänkas för ett brott

Regeringens förslag: Hemlig dataavläsning ska kunna användas i fler fall för att utreda vem som skäligen kan misstänkas för ett brott eller för

delaktighet i brottslighet. När det gäller samtliga uppgiftstyper förutom rumsavlyssningsuppgifter ska detta kunna ske under förutsättning att åtgärden är av synnerlig vikt för utredningen och det är fråga om viss allvarlig brottslighet.

Åtgärden ska få avse ett avläsningsbart informationssystem som det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda. Om åtgärden inte avser kameraövervakningsuppgifter ska den också kunna avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.

Kameraövervakningsuppgifter ska som utgångspunkt inte kunna hämtas in i någons stadigvarande bostad. Endast om det finns synnerliga skäl att anta att den person som åtgärden riktas mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystemet ska åtgärden kunna verkställas i någons stadigvarande bostad.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser tillstyrker eller har inte några synpunkter på förslagen, däribland *Brottsoffermyndigheten*, *ECPAT Sverige (ECPAT)*, *Polismyndigheten* och *Åklagarmyndigheten. Brottsförebyggande rådet* anser att det är rimligt att hemlig dataavläsning får användas till att identifiera misstänkta personer då just den typ av kommunikation som lagstiftningen syftar till att kunna samla in och läsa, i många fall görs anonymt. Brottsoffermyndigheten pekar på betydelsen av att det finns tvångsmedel som möjliggör utredning av sexualbrott på internet och betonar vikten av att gärningspersoner identifieras och lagförs så att brottsoffer får möjlighet till rehabilitering. ECPAT framhåller särskilt att möjligheten att hämta in kameraövervakningsuppgifter i någons stadigvarande bostad är av avgörande betydelse eftersom de internetrelaterade sexualbrotten som begås mot barn nästan uteslutande sker från förövarens bostad. ECPAT anser att säkerhetsventilerna är tillräckliga för att förslaget ska anses stå i proportion till den inskränkning som åtgärden innebär.

Flera remissinstanser, däribland *Integritetsskyddsmyndigheten*, *JK* och *JO*, framför att förslaget om en möjlighet att hämta in kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott innebär en ökad risk för integritetsintrång, särskilt eftersom det riktas mot en mer obestämbar krets av personer. Integritetsskyddsmyndigheten ifrågasätter om behovet av den föreslagna regleringen står i rimlig proportion till det intrång i den personliga integriteten som det innebär och anser därför att förslaget behöver analyseras vidare. *Centrum för rättvisa*, *Civil Rights Defenders* och *Sveriges advokatsamfund* avstyrker förslaget då de anser att risken för oproportionerliga ingrepp i skyddet för enskildas privat- och familjeliv är för stort. Förslaget innebär, enligt Centrum för rättvisa, betydligt större risker för integritetsintrång än vid hemlig kameraövervakning eftersom myndigheterna inte vet var den tekniska utrustningen finns och möjligheten att kartlägga individer då blir betydligt större. Centrum för rättvisa framhåller också att det är relativt

enkelt att värja sig mot åtgärden, vilket underminerar effektiviteten i övervakningen.

Civil Rights Defenders befarar att undantaget om att tillåta inhämtning av kameraövervakningsuppgifter i någons stadigvarande bostad kan leda till omfattande övervakning, både av den person som åtgärden riktas mot och mot utomstående, i mycket integritetskänsliga situationer. *Säkerhets- och integritetsskyddsnämnden* anser att kravet på koppling mellan gärningsperson och informationssystem, i de fall som avser kameraövervakningsuppgifter i någons stadigvarande bostad, bör utformas på ett snävare sätt. *Stockholms tingsrätt* anser att det föreslagna rekvisitet ”synnerliga skäl att anta” inte motsvarar det krav som utredningen beskriver och att ett alternativt uttryckssätt därför bör övervägas.

Säkerhets- och integritetsskyddsnämnden anser att förslaget om lagrade uppgifter och användningsuppgifter framstår som acceptabelt i fråga om ett avläsningsbart informationssystem som gärningsmannen använder. Nämnden ifrågasätter dock att hemlig dataavläsning som gäller platsuppgifter, lagrade uppgifter och användningsuppgifter ska kunna avse ett avläsningsbart informationssystem som gärningsmannen kontaktar. Enligt nämnden lever förslaget inte upp till de krav som regeringsformen ställer på lagstiftning som begränsar skyddet mot betydande intrång i den personliga integriteten.

Skälen för regeringens förslag

I vissa situationer behöver hemlig dataavläsning kunna användas även om ingen är skäligen misstänkt för ett brott

Hemlig dataavläsning får som utgångspunkt användas endast om någon är skäligen misstänkt för brott. Om det är av synnerlig vikt för utredningen får dock tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter respektive kommunikationsavlyssningsuppgifter beviljas för att utreda vem som är skäligen misstänkt. Det kan handla om situationer där det inte gått att hitta någon misstänkt eller för att identifiera ytterligare personer som skälig misstanke kan riktas mot (prop. 2019/20:64 s. 124 och prop. 2022/23:126 s. 241).

När det gäller kommunikationsövervaknings- eller platsuppgifter kan ett sådant tillstånd i syfte att utreda vem som skäligen kan misstänkas för brott beviljas i en förundersökning om brott som avses i 27 kap. 19 b § andra stycket rättegångsbalken. Det motsvarar vad som gäller för hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken. Den hemliga dataavläsningen kan endast avse ett avläsningsbart informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten eller som av någon annan anledning är av synnerlig vikt för utredningen (5 § lagen om hemlig dataavläsning).

Hemlig dataavläsning som avser kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brott kan användas i förundersökningar om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken. Åtgärden får då avse ett avläsningsbart informationssystem som gärningsmannen eller någon annan som har medverkat till brottet använder eller kontaktar (4 b § lagen om hemlig dataavläsning).

Reglerna för när kommunikationsövervaknings- och platsuppgifter får hämtas in i syfte att utreda vem som är skäligen misstänkt för ett brott och

när kommunikationsavlyssningsuppgifter får hämtas in i motsvarande syfte skiljer sig alltså åt, främst i fråga om vilket informationssystem som åtgärden får avse. Regleringen innebär också att det i dag inte finns någon möjlighet att använda hemlig dataavläsning som gäller kameraövervakningsuppgifter eller lagrade uppgifter och användningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott. Detta kan jämföras med rättegångsbalkens regler som tillåter att såväl hemlig avlyssning och övervakning av elektronisk kommunikation som hemlig kameraövervakning används för att utreda vem som är skäligen misstänkt (27 kap. 18 b, 19 b och 20 c §§). Däremot finns det enligt rättegångsbalken inte någon möjlighet att använda hemlig rumsavlyssning i detta syfte.

När hemlig dataavläsning infördes bedömde regeringen att en möjlighet att använda åtgärden i syfte att utreda vem som kan misstänkas för ett brott kan ge viktiga upplysningar när det inte går att hitta någon misstänkt genom andra åtgärder. Utan en sådan möjlighet ansågs det finnas en risk för att brottsbekämpande myndigheter inte skulle kunna komma vidare i utredningar om allvarliga brott. Eftersom utgångspunkten var att hemlig dataavläsning skulle återställa de brottsbekämpande myndigheternas förmåga, begränsades möjligheten att använda hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för ett brott till att avse kommunikationsövervaknings- och platsuppgifter, vilket då motsvarade vad som gällde för de bakomliggande hemliga tvångsmedlen enligt rättegångsbalken (prop. 2019/20:64 s. 124 och 125).

Möjligheterna att använda hemliga tvångsmedel för att utreda vem som skäligen kan misstänkas för ett visst brott eller för delaktighet i viss brottslighet har därefter utökats. Den 1 oktober 2023 infördes möjligheten att använda hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att identifiera en skäligen misstänkt. Regeringen konstaterade att det i vissa fall inte finns någon tillgänglig och reell möjlighet att komma framåt i en utredning och identifiera en skäligen misstänkt. Som exempel nämndes situationer där brottsbekämpande myndigheter har kännedom om att en viss ip-adress kan knytas till brott, men där adressen inte är möjlig att koppla till en viss person. En möjlighet att använda hemlig avlyssning av elektronisk kommunikation och motsvarande hemlig dataavläsning i det angivna syftet ansågs innebära en stor förbättring när det gäller möjligheterna att utreda allvarliga brott såsom mord, människorov och sexualbrott mot barn (prop. 2022/23:126 s. 118–120).

Utredningen föreslår att möjligheterna att använda hemlig dataavläsning i syfte att utreda vem som kan misstänkas för brott ska utökas ytterligare. Som utredningen redogör för används ofta en komplex digital infrastruktur vid brott som helt eller delvis genomförs över internet, t.ex. vid narkotikahandel, internetrelaterade sexuella övergrepp mot barn och grova dataintrång. Det kan handla om att gärningsmän använder Darknet – en anonymiserad och krypterad del av internet – eller skadlig programvara i form av t.ex. virus, trojaner eller spionprogram. I takt med den digitala utvecklingen har det också blivit vanligare att digital kommunikation sker med information i krypterad form, t.ex. genom applikationer som möjliggör kryptering. Anonymiseringen och krypteringen innebär att det många gånger är omöjligt att ta reda på vem eller vilka som ligger bakom ett brott. Ofta känner de brottsbekämpande myndigheterna till att ett visst

informationssystem används för att begå allvarlig brottslighet, men saknar verktyg för att identifiera den misstänkte, exempelvis vem eller vilka som är involverade i ett pågående terroristbrott.

Regeringen anser i likhet med utredningen att det är ett oacceptabelt hinder i den brottsbekämpande verksamheten att myndigheterna, på grund av att anonyma tjänster eller krypterad information används, inte kan komma vidare i utredningar om fullt synlig, allvarlig brottslighet. En möjlighet att använda hemlig dataavläsning i fler fall i syfte att identifiera en skäligen misstänkt skulle kunna medföra avsevärd nytta i den brottsutredande verksamheten. Av det skälet och för att åstadkomma en tydligare och mer enhetlig reglering bör tillämpningsområdet för hemlig dataavläsning utvidgas genom att utöka möjligheterna att använda tvångsmedlet för att utreda vem som skäligen kan misstänkas för ett brott eller för delaktighet i brottslighet.

Utgångspunkten bör, så som utredningen konstaterar, vara att hemlig dataavläsning ska kunna användas på motsvarande sätt som övriga hemliga tvångsmedel. Eftersom det enligt rättegångsbalken inte är tillåtet med hemlig rumsavlyssning för att identifiera en skäligen misstänkt bör någon sådan möjlighet inte införas för hemlig dataavläsning (jfr 27 kap. 20 e § rättegångsbalken).

Kommunikationsövervaknings- och platsuppgifter

Möjligheten att använda hemlig dataavläsning som avser kommunikationsövervaknings- och platsuppgifter i syfte att utreda vem som är skäligen misstänkt för ett brott är, som framgår ovan, i dag begränsad till informationssystem med en koppling till brottet eller till uppgifter som av något annat skäl är av synnerlig vikt för utredningen. Utredningen föreslår att den möjligheten ska utvidgas så att regleringen motsvarar förutsättningarna för att hämta in kommunikationsavlyssningsuppgifter i motsvarande syfte. Det skulle innebära att kommunikationsövervaknings- och platsuppgifter kan hämtas in genom hemlig dataavläsning även från informationssystem utan lika tydlig koppling till brottet eller brottsplatsen.

De grundläggande förutsättningarna för regleringen av kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott knyter an till motsvarande regler om hemlig avlyssning av elektronisk kommunikation i 27 kap. 18 b § rättegångsbalken (4 b § lagen om hemlig dataavläsning). En första förutsättning för att kunna använda de aktuella tvångsmedlen i syfte att utreda vem som skäligen kan misstänkas för ett brott är att åtgärden är av synnerlig vikt för utredningen.

Därutöver förutsätts att det finns en misstanke om särskilt allvarlig brottslighet. Det ska som regel röra sig om brott där det lägsta föreskrivna straffet är fängelse i fyra år, eller brott som omfattas av en särskild brottskatalog (27 kap. 18 b § andra stycket rättegångsbalken). Det ska jämföras med den brottslighet som i dag kan aktualisera hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter i syfte att utreda vem som är skäligen misstänkt för ett brott där utgångspunkten är att det lägsta föreskrivna straffet ska vara fängelse i två år eller att brottet omfattas av en särskild brottskatalog.

Det finns också ett krav på samband mellan det informationssystem som åtgärden riktas mot och gärningspersonen. Som utgångspunkt ska det finnas särskild anledning att anta att informationssystemet har använts eller kommer att användas av gärningsmannen eller någon annan som har medverkat till brottet eller brotten. Kravet innebär att det ska finnas någon faktisk omständighet som med viss styrka talar för att gärningsmannen har använt eller kommer att använda informationssystemet. Ett allmänt antagande om att så är fallet är inte tillräckligt (prop. 2022/23:126 s. 210 och 241). Om det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta ett visst informationssystem kan åtgärden också avse ett sådant informationssystem. Det betyder att det på grund av tillförlitliga uppgifter ska vara så gott som säkert att gärningsmannen har kontaktat eller kommer att kontakta informationssystemet (prop. 2022/23:126 s. 211 och 241).

Enligt systematiken i rättegångsbalken innebär ett tillstånd till hemlig avlyssning av elektronisk kommunikation också en rätt att vidta åtgärder för att hämta in uppgifter om elektronisk kommunikation i hemlighet (27 kap. 18 § andra stycket och 27 kap. 19 § rättegångsbalken). Det beror på att det i de flesta fall är nödvändigt för de brottsbekämpande myndigheterna att få tillgång till övervakningsuppgifter även vid hemlig avlyssning, se propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55 s. 69). Som utredningen framhåller talar systematiska skäl för att också ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter ska kunna beviljas under samma förutsättningar som ett tillstånd som gäller kommunikationsavlyssningsuppgifter i motsvarande syfte.

Enligt rättegångsbalkens regler kan motsvarande information redan i dag hämtas in genom hemlig övervakning av elektronisk kommunikation utan något krav på samband mellan det misstänkta brottet och den person som åtgärden riktas mot (27 kap. 19 b § rättegångsbalken). När det gäller platsuppgifter är det dock, som *Säkerhets- och integritetsskyddsnämnden* anför, möjligt att hämta in mer precisa uppgifter genom hemlig dataavläsning än genom hemlig kommunikationsövervakning. Ytterligare en skillnad är att anonymisering och kryptering inte på samma sätt innebär ett hinder för de brottsbekämpande myndigheterna när hemlig dataavläsning tillämpas.

Säkerhets- och integritetsskyddsnämnden ifrågasätter behovet av att kunna rikta en åtgärd som gäller platsuppgifter mot ett informationssystem som gärningsmannen eller någon annan som har medverkat till brottet kontaktar. I många av de situationer där det finns ett påtagligt behov av att hämta in platsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott kan det förväntas vara tillräckligt att rikta åtgärden mot ett informationssystem som gärningsmannen eller någon annan som medverkar till brottet använder. Det kan dock finnas situationer då den enda reella möjligheten att identifiera en gärningsman är att rikta åtgärden mot ett annat informationssystem, trots att det saknar en tydlig koppling till gärningsmannen. Det kan t.ex. handla om en telefon som tillhör en målsägande som befinner sig på samma plats eller som har stämt möte med gärningsmannen. Genom att få tillgång till platsuppgifter i samband med

kommunikation med gärningsmannen kan det på så sätt vara möjligt att få reda på vem han eller hon är. Det bör inte överlämnas till målsäganden eller någon annan att avgöra om ett allvarligt brott ska utredas eller inte. Syftet är dock inte att i något annat avseende kartlägga eller utreda målsägandens eller någon annan än gärningsmannens förehavanden.

Det kan också konstateras att ett tillstånd till hemlig dataavläsning alltid ska avse ett visst utpekat avläsningsbart informationssystem. Det innebär att rätten vid tillståndsprövningen måste ta ställning till om det finns skäl att rikta åtgärden mot ett visst informationssystem som det finns synnerlig anledning att anta att gärningsmannen eller någon som har medverkat till brottet har kontaktat eller kommer att kontakta. Den grundläggande förutsättningen att en åtgärd ska vara av synnerlig vikt för utredningen innebär att ett tillstånd till en viss åtgärd inte kan beviljas utan noga övervägande.

Som utredningen framhåller utgör de höga kvalifikationskraven en kraftig begränsning av möjligheten att hämta in kommunikationsövervaknings- och platsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott. Det innebär att åtgärden enbart kommer att kunna användas i de situationer då den är nödvändig för att komma vidare i utredningar om allvarlig brottslighet. Det kan också tilläggas att ett tillstånd till hemlig dataavläsning kan begränsas genom villkor om att endast vissa uppgifter får hämtas in, om det bedöms ändamålsenligt i det enskilda fallet. Att kategorin av informationssystem som åtgärden kan riktas mot är något bredare talar för att fler uppgifter kommer att kunna hämtas in. Samtidigt ställs det högre krav på brottets allvar än enligt den befintliga regeln om inhämtning av kommunikationsövervaknings- och platsuppgifter i syfte att utreda vem som kan misstänkas för ett brott, vilket i någon mån kan sägas kompensera den högre risk för integritetsintrång som det innebär. Sammantaget bedömer regeringen att förslaget är proportionerligt. Förslaget bör därför genomföras.

Kameraövervakningsuppgifter

Genom reglerna om hemlig dataavläsning finns en möjlighet för de brottsbekämpande myndigheterna att i hemlighet hämta in kameraövervakningsuppgifter, t.ex. genom att aktivera en befintlig kamera på en dator eller en telefon. Enligt nuvarande reglering förutsätter åtgärden att någon skäligen kan misstänkas för det aktuella brottet. Utredningen föreslår att det ska införas en möjlighet att hämta in kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott. Enligt utredningen talar den omständigheten att de aktuella uppgifterna kan hämtas in genom hemlig kameraövervakning för att motsvarande åtgärd bör vara möjlig genom hemlig dataavläsning.

Frågan om möjligheten att hämta in kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott övervägdes när lagen om hemlig dataavläsning infördes. Då bedömdes dock behovet av att använda hemlig dataavläsning för att övervaka den plats där ett brott har begåtts eller en nära omgivning till denna plats, på det sätt som är möjligt genom hemlig kameraövervakning, inte vara särskilt stort. Regeringen ifrågasatte inte att det fanns fall där det skulle vara verksamhetsmässigt värdefullt att kunna ta upp kameraövervakningsuppgifter för att kunna identifiera en person. En möjlighet att ta upp sådana uppgifter

ansågs dock som en inte obetydlig utvidgning av vad som var rättsligt möjligt med tanke på att hemlig kameraövervakning vid den tidpunkten inte kunde användas i syfte att identifiera en person (prop. 2019/20:64 s. 125). Någon sådan möjlighet infördes därför inte.

Sedan hemlig dataavläsning infördes har såväl brottsutvecklingen som den tekniska utvecklingen visat att en möjlighet att hämta in kameraövervakningsuppgifter genom hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för ett brott skulle kunna vara till stor nytta i brottsutredningar i flera fall. En vanlig situation är att de brottsbekämpande myndigheterna känner till att ett visst informationssystem används i samband med allvarlig brottslighet, men saknar verktyg för att identifiera vem som använder det. Andra tvångsmedel kan sällan ge sådan information och därför kommer de brottsbekämpande myndigheterna ofta inte vidare i utredningarna. Med den snabba utvecklingen av både brottslighet och teknik följer ett behov av mer effektiva verktyg. En möjlighet att använda hemlig dataavläsning som gäller kameraövervakningsuppgifter för att utreda vem som skäligen kan misstänkas för brott skulle kunna ge avgörande upplysningar om vem som ligger bakom en viss brottslighet. Genom att vid ett givet tillfälle aktivera kamerafunktionen på den informationsutrustning som används som brottsverktyg skulle myndigheten enkelt kunna identifiera den misstänkte. På så sätt skulle det också vara möjligt att tidigt pröva en invändning från en misstänkt om att han eller hon har lånat ut sin dator eller telefon vid tidpunkten då t.ex. ett sexualbrott mot ett barn eller ett narkotikabrott har begåtts på datorn eller telefonen.

I likhet med flera remissinstanser, bl.a. *Polismyndigheten* och *Åklagarmyndigheten*, instämmer regeringen i utredningens bedömning att det i dag finns ett påtagligt behov av att kunna använda hemlig dataavläsning för att kunna ta del av kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett visst brott eller för delaktighet i viss brottslighet. En sådan möjlighet bedöms kunna leda till avsevärd nytta för de brottsbekämpande myndigheterna. Att det, som *Centrum för rättvisa* påpekar, är möjligt att täcka för en kamera och på så sätt försvåra inhämtning av kameraövervakningsuppgifter påverkar inte regeringens bedömning i det avseendet.

De ökade risker som en utvidgning av tillämpningsområdet för med sig förutsätter att det ställs upp särskilda kvalifikationskrav för att använda åtgärden. På samma sätt som gäller för inhämtning av kommunikationsavlyssningsuppgifter bör det krävas att åtgärden är av synnerlig vikt för utredningen. Det innebär att först när andra åtgärder för att komma åt uppgifterna i fråga inte bedöms vara tillräckliga, skulle vara väsentligt svårare att genomföra eller kan förväntas leda till större integritetsintrång kan det bli aktuellt att besluta om åtgärden. Kravet på synnerlig vikt för utredningen innefattar på så sätt både ett kvalitetskrav på de uppgifter som kan förväntas erhållas med åtgärden och ett krav på att syftet med åtgärden i princip inte är möjligt att uppnå på något annat sätt (prop. 2022/23:126 s. 208, 240 och 241). Därmed kan det förväntas att åtgärden kommer att tillämpas restriktivt. På samma sätt som vid inhämtning av kommunikationsavlyssningsuppgifter i syfte att utreda vem som är skäligen misstänkt bör det också krävas att det är fråga om allvarlig brottslighet. Som

utgångspunkt bör det även för inhämtning av kameraövervakningsuppgifter handla om brott där det lägsta föreskrivna straffet är fängelse i fyra år, eller brott som omfattas av en särskild brottskatalog.

Frågan är då om behovet och nyttan med åtgärden väger så tungt att en sådan reglering framstår som proportionerlig i förhållande till riskerna för intrång i enskildas personliga integritet. Som *JK* och *JO* påpekar innebär förslaget en ökad risk för integritetsintrång och en ökad risk för att åtgärden riktas mot en bredare krets av personer. Det ligger i sakens natur att en åtgärd som kan användas innan en misstänkt har kunnat identifieras riskerar att riktas mot någon som inte har någon koppling till brottsligheten. Eftersom kameraövervakningsuppgifter redan i dag kan hämtas in genom hemlig kameraövervakning i syfte att identifiera en gärningsman ska dock den ökade risken för intrång i enskildas personliga integritet som förslaget innebär inte överdrivas. Sammantaget får införandet av en möjlighet att hämta in kameraövervakningsuppgifter i detta syfte anses innebära en godtagbar avvägning mellan å ena sidan intresset av att effektivt kunna bekämpa allvarlig brottslighet och å andra sidan intresset av att skydda enskildas personliga integritet.

Enligt utredningens förslag ska kameraövervakningsuppgifter i undantagsfall kunna hämtas in i någons stadigvarande bostad. Några remissinstanser, bl.a. *JK* och *Integritetsskyddsmyndigheten*, efterfrågar ytterligare analys av frågan om det alls ska vara möjligt att hämta in sådana uppgifter i någons stadigvarande bostad.

Varken hemlig dataavläsning som avser kameraövervakningsuppgifter eller hemlig kameraövervakning får i dag verkställas i någons stadigvarande bostad (4 a § tredje stycket lagen om hemlig dataavläsning och 27 kap. 25 a § andra stycket rättegångsbalken). Utgångspunkten bör också vara, i enlighet med utredningens förslag, att inte heller kameraövervakningsuppgifter i syfte att utreda vem som kan misstänkas för ett brott ska kunna verkställas i någons stadigvarande bostad. Som *ECPAT* framhåller kan det emellertid finnas ett stort behov av att hämta in kameraövervakningsuppgifter i någons bostad exempelvis vid internetrelaterade sexualbrott mot barn som nästan uteslutande sker från förövarens hem. Även annan allvarlig brottslighet kan begås i eller från en bostad. En situation som kan uppstå är att de brottsbekämpande myndigheterna har kunnat ta reda på vilket informationssystem som används som brottsverktyg och i vilket bostadsområde det finns, men att det inte har varit möjligt att närmare ringa in var informationssystemet finns. I den situationen kan information från kamerafunktionen i ett informationssystem ha avgörande betydelse för möjligheten att utreda vem eller vilka som ligger bakom den i övrigt fullt synliga brottsligheten. Ett förbud mot att verkställa åtgärden på en plats som är någons stadigvarande bostad skulle riskera att motverka syftet med att införa en möjlighet att hämta in kameraövervakningsuppgifter.

En möjlighet att hämta in kameraövervakningsuppgifter i någons bostad innebär visserligen ett större ingrepp i skyddet för enskildas privat- och familjeliv än befintliga möjligheter till hemlig kameraövervakning, vilket påpekas av bl.a. *Civil Rights Defenders*. Som utredningen framhåller innebär verkställighetsmetoden för hemlig kameraövervakning i sig dock ett större ingrepp. Hemlig kameraövervakning genomförs nämligen genom att den verkställande myndigheten i hemlighet skaffar sig tillträde

till och installerar tekniska hjälpmedel på en plats som annars skyddas mot intrång. Installationsmomentet består av montering av kameror som övervakar den misstänkte eller, om någon skäligen misstänkt inte finns, den plats där brottet har begåtts eller en nära omgivning till denna plats. Vid hemlig dataavläsning som avser kameraövervakningsuppgifter krävs däremot inget installationsmoment eller tillträdestillstånd eftersom verkställighet sker genom aktivering av kamerafunktionen i det informationssystem som tillståndet avser. Det kan också finnas större möjligheter att avgränsa åtgärden på ett sådant sätt att integritetsintrånget blir mer begränsat än genom hemlig kameraövervakning. För att minska den risk som bl.a. *Centrum för rättvisa* framhåller för att den person som åtgärden riktar sig mot befinner sig i en särskilt integritetskänslig situation bör regleringen utformas restriktivt.

Utredningen föreslår att åtgärden ska kunna verkställas i någons stadigvarande bostad endast om det finns synnerliga skäl att anta att den person som åtgärden riktas mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser. *Säkerhets- och integritetsskyddsnämnden* invänder mot utformningen och anser att kravet på koppling mellan gärningsperson och informationssystem bör formuleras på ett snävare sätt. Även *Stockholms tingsrätt* har synpunkter på utformningen och framför att det föreslagna rekvisitet ”synnerliga skäl att anta” inte motsvarar det högt ställda krav som utredningen eftersträvar och att ett alternativt uttryckssätt därför bör övervägas. Motsvarande beviskrav förekommer emellertid i flera bestämmelser i lagen om hemlig dataavläsning (se t.ex. 4 a och 4 b §§ lagen om hemlig dataavläsning). Det föreslagna beviskravet innebär att bestämmelsen ska tillämpas restriktivt och endast i situationer då det på grund av tillförlitliga uppgifter är så gott som säkert att det förhåller sig på ett visst sätt (jfr prop. 2019/20:64 s. 217 och prop. 2022/23:126 s. 211 och 241). Det innebär ett krav på att myndigheten vid verkställighet kan säkerställa t.ex. att den person som åtgärden riktar sig mot använder sig av informationssystemet. Det kravet minskar väsentligt den risk som *Centrum för rättvisa* gör gällande för att uppgifterna hämtas in när någon befinner sig i en särskilt integritetskänslig situation.

Användningen av åtgärden begränsas också av ändamålet att utreda vem som skäligen kan misstänkas för ett brott. När syftet är uppnått, dvs. som regel när den person som åtgärden riktas mot kan identifieras som skäligen misstänkt, ska åtgärden avbrytas.

Därutöver ska hänsyn tas till integritetsintresset, både hos den som åtgärden riktas mot och hos utomstående personer, vid tillståndsprövningen. En förutsättning för ett tillstånd är att det av underlaget tydligt framgår hur informationssystemet i fråga har ringats in. Tillståndet kan utifrån detta förenas med särskilda villkor för åtgärdens användande, anpassade efter omständigheterna i den enskilda situationen. Eftersom hemlig dataavläsning som gäller kameraövervakningsuppgifter endast avser inhämtning av realtidsuppgifter bör villkoren tydligt ta sikte på verkställigheten. Som utredningen framhåller kan det i många fall vara nödvändigt med villkor om åtgärder som exempelvis spaning i samband med verkställigheten, för att kunna säkerställa att integritetsintrånget för den enskilde och risken för att utomstående drabbas blir så begränsade som möjligt. Genom villkor kan rätten också begränsa bl.a. under hur lång tid

kameraövervakningsuppgifter får hämtas in. Mot den sammantagna bakgrunden delar regeringen inte *Civil Rights Defenders* farhåga att möjligheten att hämta in kameraövervakningsuppgifter i någons stadigvarande bostad kan leda till omfattande övervakning.

När det gäller vilka informationssystem som åtgärden ska kunna avse instämmer regeringen i utredningens bedömning att åtgärden bör vara begränsad till sådana informationssystem som kan antas användas av den person som åtgärden riktas mot. På det sättet blir tillämpningsområdet mer begränsat för kameraövervakningsuppgifter än för övriga uppgiftstyper som får hämtas in i syfte att utreda vem som misstänks för brott.

Sammanfattningsvis konstaterar regeringen att det stora behovet och nyttan av en möjlighet att i undantagsfall kunna hämta in kameraövervakningsuppgifter i någons stadigvarande bostad väger tyngre än den risk för ingrepp i enskildas personliga integritet som det innebär. Att införa en sådan möjlighet bedöms därför proportionerligt. Till skillnad från bl.a. *Centrum för rättvisa* och *Civil Rights Defender*s bedömer regeringen att den föreslagna regleringen är förenlig med regeringsformen och Europakonventionen. Det bör därför införas en möjlighet att hämta in kameraövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för ett brott, i enlighet med utredningens förslag.

Övriga uppgifter som är åtkomliga i ett avläsningsbart informationssystem

De övriga åtkomliga uppgifterna, s.k. lagrade uppgifter och användningsuppgifter, kan t.ex. bestå av text-, bild- och ljudfiler eller ett utkast till ett meddelande, men det kan också vara uppgifter om hur ett informationssystem används. Enligt nuvarande reglering är det, till skillnad från vad som gäller för kommunikationsavlyssningsuppgifter, inte möjligt att hämta in lagrade uppgifter och användningsuppgifter i syfte att utreda vem som kan misstänkas för brott. Utredningen föreslår att en sådan möjlighet ska införas.

Ett skäl till att ändra reglerna är att det kan vara svårt att på förhand skilja kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter från lagrade uppgifter och användningsuppgifter. När en viss uppgiftstyp hämtas in, t.ex. kommunikationsavlyssningsuppgifter, kommer ofta annan lagrad information som tillhör en annan uppgiftstyp med i inhämtningen. De uppgifterna utgör då otillåten tilläggsinformation (23 § lagen om hemlig dataavläsning).

Som utredningen konstaterar kan både behovet och nyttan av att kunna ta del av lagrade uppgifter och användningsuppgifter i ett tidigt skede av en brottsutredning, innan det finns någon skäligen misstänkt, förväntas vara stort. Det kan t.ex. handla om uppgifter som är åtkomliga på en server och som ger de brottsbekämpande myndigheterna en möjlighet att analysera bl.a. källkoder, loggfiler, noder och andra uppgifter som inte har kommunicerats. Vid en sådan analys kan digitala spår från olika håll kombineras och utredas parallellt för att upptäcka eventuella samband, vilket många gånger är en förutsättning för att kunna identifiera personerna bakom brottsligheten. Med nuvarande reglering får myndigheterna inte alltid del av centrala delar av informationen vilket gör det svårare att dra korrekta slutsatser.

Polismyndigheten har lämnat exempel till utredningen på när det kan finnas ett stort behov av att ta del av information som kategoriseras som övriga åtkomliga uppgifter. Vid internetrelaterade sexuella övergrepp mot barn, då en stor del av kommunikationen i form av text- och fildelning sker via olika Darknetforum, kan en misstanke om brott uppstå då en fil som föreställer sexuella övergrepp mot barn påträffas. Filen kan ha skickats från ett alias till ett annat via ett Darknetforum. I vissa fall kan ett fåtal intressanta personer identifieras, men i detta skede kan ingen av dessa personer anses vara skäligen misstänkt för brottet. En möjlighet att i en sådan situation hämta in uppgifter genom hemlig dataavläsning skulle öka förutsättningarna för att komma vidare i utredningen. Den här typen av brottslighet sker ofta över nationsgränser med gärningsmän utspridda i olika länder. En förutsättning för att de brottsbekämpande myndigheterna ska kunna upptäcka, avbryta och utreda den kriminella verksamheten är att de kan använda effektiva hemliga tvångsmedel mot exempelvis informationssystem med krypterad information. Att de svenska brottsbekämpande myndigheterna inte har möjlighet att komma åt övriga lagrade uppgifter innebär både att myndigheterna inte kommer vidare i vissa utredningar och att de inte kan biträda andra länder i deras utredningar om allvarlig brottslighet. Det medför också en risk för att det blir attraktivt att i Sverige placera digital infrastruktur som används för illegala syften.

Utredningen föreslår att de grundläggande förutsättningarna för att hämta in lagrade uppgifter och användningsuppgifter i syfte att utreda vem som kan misstänkas för ett brott ska vara desamma som för att hämta in kommunikationsavlyssningsuppgifter i motsvarande syfte. Det innebär ett krav på att åtgärden är av synnerlig vikt för utredningen och att misstanken gäller särskilt allvarlig brottslighet. Åtgärden ska som utgångspunkt avse ett avläsningsbart informationssystem som gärningsmannen använder. Om det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta ett annat informationssystem, kan åtgärden avse det informationssystemet.

Säkerhets- och integritetsskyddsnämnden ifrågasätter att ett tillstånd att hämta in lagrade uppgifter ska kunna avse ett avläsningsbart informationssystem som gärningsmannen kontaktar. Nämnden anser att den föreslagna regleringen skulle utgöra en oacceptabel utvidgning av möjligheterna att använda hemliga tvångsmedel mot utomstående personer. Regeringen delar inte den uppfattningen. Genom att hämta in övriga åtkomliga uppgifter kan de brottsbekämpande myndigheterna ta del av t.ex. bilder eller olika former av meddelanden som inte har skickats eller anteckningar med kontaktuppgifter till en gärningsperson. En möjlighet att ta del av sådana uppgifter från t.ex. en målsägande eller en person som gärningsmannen är i kontakt med angående brottsligheten kan göra att de brottsbekämpande myndigheterna kan komma vidare i utredningar där det annars inte är möjligt. Även om det är fråga om en viss utvidgning kommer de föreslagna kvalifikationskraven att utgöra en kraftig begränsning av möjligheten att använda åtgärden. Utöver att åtgärden ska vara av synnerlig vikt för utredningen krävs att det är så gott som säkert att gärningsmannen eller någon som har medverkat till brottet kan komma att kontakta eller har kontaktat det informationssystem som åtgärden avser.

Endast när det är nödvändigt kommer åtgärden kunna riktas mot ett avläsningsbart informationssystem som gärningsmannen kontaktar. Eftersom lagrade uppgifter och användningsuppgifter kan vara svåra att skilja från kommunikationsavlyssningsuppgifter bör samma grundläggande förutsättningar gälla för åtgärderna. Sammantaget finns det skäl för att åtgärden också ska kunna avse ett informationssystem som gärningsmannen kontaktar.

Att utöka tillämpningsområdet för hemlig dataavläsning genom att göra det möjligt att hämta in övriga åtkomliga uppgifter i syfte att utröna vem som kan misstänkas för ett brott innebär att de brottsbekämpande myndigheterna får möjlighet att hämta in mer information än tidigare. Eftersom syftet med åtgärden är att utreda vem som skäligen kan misstänkas är det ofrånkomligt att tvångsmedlet kan komma att riktas mot en mer obestämbar krets av personer. Förslaget innebär därmed ökade risker för enskildas personliga integritet och för att utomstående drabbas av åtgärden. Hur stort integritetsintrånget är beror dock på hur tillståndet utformas och vilket informationssystem som åtgärden riktar sig mot. Som utredningen redogör för finns det tillfällen då integritetsintrånget är begränsat, t.ex. då åtgärden riktar sig mot en s.k. proxyserver där den enda användaren av servern är den person som utför det aktuella brottet. Vidare saknas det enligt regeringens bedömning lämpligare eller mindre ingripande alternativ för att få ta del av uppgifterna. Utifrån de grundläggande högt ställda kvalifikationskraven för hemlig dataavläsning i allmänhet och för åtgärder i syfte att utreda vem som skäligen kan misstänkas för brott i synnerhet bedömer regeringen att förslaget är proportionerligt och att det bör genomföras.

8 Förbättrade rättssäkerhetsgarantier

8.1 Nuvarande rättssäkerhetsgarantier och behovet av kompletterande regler

Användning av hemlig dataavläsning ställer höga krav på att regelverket omges av rättssäkerhetsgarantier och kontrollmekanismer för att garantera en rättssäker tillståndsgivning och att intrången i den personliga integriteten inte blir större än vad som kan godtas enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga.

Som beskrivs i avsnitt 4 innehåller reglerna om hemlig dataavläsning flera skyddsmekanismer för att säkerställa att tillämpningen är rättssäker och inte innebär obefogade intrång i enskildas integritet. Reglerna omfattar bl.a. krav på domstolsprövning, medverkan av offentliga ombud vid tillståndsprövningen och efterföljande tillsyn och kontroll av Säkerhets- och integritetsskyddsnämnden.

I avsnitt 5 föreslås att möjligheten till hemlig dataavläsning ska gälla utan tidsbegränsning och i avsnitt 7 föreslås en viss utvidgning av tillämpningsområdet för hemlig dataavläsning. Förslagen förutsätter att det finns fungerande kontrollmekanismer och andra rättssäkerhetsgarantier.

Regleringen om hemlig dataavläsning är utformad med bestämmelserna om de övriga hemliga tvångsmedlen i rättegångsbalken som förebild. De rättssäkerhetsgarantier som gäller för de sistnämnda tvångsmedlen har tidigare utvärderats och i huvudsak ansetts tillräckliga och väl fungerande, se betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel (SOU 2018:61). De nuvarande rättssäkerhetsgarantierna för hemlig dataavläsning är dessutom i vissa avseenden förstärkta i förhållande till övriga hemliga tvångsmedel. Reglerna innebär att det ställs höga krav på rättssäkerhet vid användning av hemlig dataavläsning. Tillämpningen har dock visat att det trots detta finns skäl att göra vissa förändringar och förtydliganden i lagstiftningen i syfte att ytterligare stärka rättssäkerheten, bl.a. genom tydligare regler för tillståndsbeslutens innehåll och för användning av information från hemlig dataavläsning samt stärkta förutsättningar för att kontrollera verkställigheten i efterhand.

8.2 Tydligare regler för tillståndets utformning

Regeringens förslag: Reglerna för vad som ska anges i ett tillstånd till hemlig dataavläsning förtydligas.

I tillståndet ska rätten ange vem som är skäligen misstänkt för brottet eller brotten, om sådan uppgift finns.

Rätten ska också ange under vilken tid tillståndet får verkställas, i stället för vilken tid tillståndet avser. Tiden för verkställighet får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet.

Kravet på samband mellan den person som den hemliga dataavläsningen riktas mot och det informationssystem som den hemliga dataavläsningen avser justeras på så sätt att det inte längre ska krävas att kontakten sker under den tid som tillståndet avser.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser, däribland *Civil Rights Defenders* och *Riksdagens ombudsmän (JO)*, tillstyrker eller har inga invändningar mot förslaget att tiden för verkställighet ska anges i tillståndet. *Sveriges advokatsamfund* ifrågasätter om förslaget innebär att rättssäkerheten stärks eftersom myndigheterna får tillgång till en utökad mängd information och anser att förslaget behöver analyseras ytterligare. *Säkerhets- och integritetsskyddsnämnden* är positiv till att det blir tydligt att verkställighetsförsök får göras under som längst en månad från beslutet men anser att förslaget enbart kan godtas om det införs ett krav på att ett beslut om tillstånd som gäller andra uppgiftstyper än kameraövervaknings- och rumsavlyssningsuppgifter alltid ska förenas med villkor som tar sikte på tidsmässiga avgränsningar.

Skälen för regeringens förslag

Uppgift om vem som är skäligen misstänkt bör anges

I ett tillstånd till hemlig dataavläsning ska det anges vem som är skäligen misstänkt för brottet eller brotten vid en åtgärd som gäller rums-

avlyssningsuppgifter eller vem en åtgärd i preventivt syfte enligt preventivlagen riktas mot. Som utredningen konstaterar bör detta anges även i övriga fall då tillstånd till hemlig dataavläsning beviljas. I enlighet med utredningens förslag bör det förtydligas att det i ett tillstånd till hemlig dataavläsning ska anges vem som är skäligen misstänkt, om en sådan uppgift finns.

Tiden för verkställighet bör anges

I ett tillstånd till hemlig dataavläsning ska det bl.a. anges vilken tid tillståndet avser. Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet (18 § första stycket 1 och fjärde stycket lagen om hemlig dataavläsning).

Vid verkställighet av hemlig dataavläsning kan inte bara realtidsuppgifter utan även lagrade filer, t.ex. textdokument, som är åtkomliga i det avläsningsbara informationssystemet hämtas in. Av lagtexten framgår inte någon begränsning i fråga om hur gamla uppgifter som får hämtas in med stöd av ett tillstånd. I förarbetena anges emellertid att rätten bör begränsa de uppgifter som får tas upp, även när det gäller tiden före beslutet, eftersom tiden inte får vara längre än vad som är nödvändigt i det enskilda fallet. En tidsgräns för meddelanden kan sättas t.ex. genom att inskränka tillståndet till att avse meddelanden som skickats eller tagits emot endast efter en viss tidpunkt. När det däremot gäller lagrade filer kan det vara svårare att sätta någon sådan gräns. En fil kan vara skapad vid en viss tidpunkt och ändrad vid en eller flera andra tidpunkter. Ett tillstånd bör då enligt förarbetena uttryckas som att det avser filer som skapats eller ändrats efter en viss given tidpunkt. Avläsningen får då avse uppgifter i filer som ändrats efter den givna tidpunkten, även om de skapats före (prop. 2019/20:64 s. 234).

I lagstiftningen anges inte heller när ett tillstånd om hemlig dataavläsning senast bör verkställas. Som allmän princip för tvångsmedelsanvändning gäller dock att verkställighet bör ske så nära ett beslut som möjligt.

Enligt utredningen visar den hittillsvarande tillämpningen att regleringen har orsakat vissa verkställighetsproblem. Av Säkerhets- och integritetsskyddsnämndens granskning av användningen av hemlig dataavläsning framgår att det har uppstått osäkerhet om hur länge nya verkställighetsförsök kan göras efter misslyckade försök att verkställa ett tillstånd. Nämnden har uttalat att det vore lämpligt att låta den i lag angivna tidsbegränsningen på en månad utgöra den bortre gränsen också för möjligheten till fortsatta verkställighetsförsök avseende historiska uppgifter (Säkerhets- och integritetsskyddsnämndens uttalande med beslut den 15 december 2001, dnr 92-2020).

För att öka tydligheten och förutsebarheten i regleringen föreslår utredningen att det i ett tillstånd till hemlig dataavläsning ska anges under vilken tid som verkställighet får äga rum, i stället för vilken tid som tillståndet avser. Tiden för verkställighet får enligt förslaget inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet. Förslaget syftar till att förtydliga att ett tillstånd till hemlig dataavläsning som gäller lagrade uppgifter omfattar inhämtning av

alla uppgifter som under verkställighetstiden är åtkomliga i informationssystemet, om inte något annat framgår av tillståndets villkor. Det innebär att själva inhämtningen inte längre skulle behöva begränsas tidsmässigt.

Som utredningen framhåller är bestämmelsens nuvarande utformning otydlig när det gäller vad den i lag angivna tiden avser. Den riskerar också att skapa onödiga hinder i den brottsbekämpande verksamheten. Regleringen utgår från att det ska anges en ram för vilken tid som informationen härrör ifrån. I det avseendet skiljer den sig från regleringen av öppna tvångsmedel såsom husrannsakan, beslag och genomsökning på distans. För dessa tvångsmedel saknas det tidsgräns i förhållande till vilken information som de brottsbekämpande myndigheterna får ta del av.

Uppgifter i en elektronisk kommunikationsutrustning är som regel svårare att överblicka än uppgifter i fysiska dokument. Exempelvis kan mobiltelefoner, surfplattor och datorer innehålla en stor mängd information av vitt skilda slag. Det kan handla om realtidsuppgifter eller information som finns lagrad i komplexa mappstrukturer och olika applikationer eller är samlad på annat sätt. Vissa uppgifter blir synliga först när en fil eller applikation öppnas. Det innebär att det kan vara svårt för den brottsbekämpande myndigheten att på förhand göra tydliga tidsmässiga avgränsningar av den information som de har ett behov av att hämta in. Därutöver kan det vara svårt att avgöra inom vilken tid som uppgifterna är skapade. Utöver att en fil kan ändras efter att den skapats kan de tidsmarkörer som anges för filen enkelt manipuleras genom att tidsinställningarna i ett informationssystem ändras. Det innebär att ett tillstånd som innehåller en begränsning bakåt i tiden kan medföra att viss information oavsiktligt inte går att hämta in. På så sätt kan de brottsbekämpande myndigheterna missa information som de söker.

Regeringen instämmer i utredningens bedömning att det finns skäl att förtydliga regleringen och att den bör utformas på ett sätt som bättre motsvarar de öppna tvångsmedlen. Som *Säkerhets- och integritetsskyddsnämnden* framhåller är det viktigt att det tydliggörs att verkställighetsförsök får göras under en viss tid efter beslutet. I ett tillstånd bör det därför anges under vilken tid som verkställighet får ske. Utredningens förslag om en månad som bortre gräns framstår som lämpligt.

Förslaget innebär att det inte kommer att finnas ett obligatoriskt krav att ange en tidsmässig begränsning för den information som kan hämtas in. Eftersom det som utgångspunkt innebär att de brottsbekämpande myndigheterna får tillgång till mer information än tidigare är det viktigt att integritetsintrånget begränsas genom villkor i det enskilda fallet för att den sammantagna effekten ska vara proportionerlig. Bland annat mot den bakgrunden finns det skäl att överväga ändringar i regleringen av villkor. Till skillnad från *Säkerhets- och integritetsskyddsnämnden* anser regeringen däremot inte att förslaget förutsätter att det ställs ett krav på att det alltid ska anges villkor som tar sikte på tidsmässiga avgränsningar.

Som en följd av förslaget att ta bort kravet på att i ett tillstånd till hemlig dataavläsning ange vilken tid tillståndet avser bör också vissa andra bestämmelser i lagen om hemlig dataavläsning justeras. Det handlar om reglerna som innebär att det ska finnas en koppling mellan en enskild och det informationssystem som den hemliga dataavläsningen avser. För att ett tillstånd till hemlig dataavläsning under en förundersökning ska beviljas krävs som huvudregel att det avläsningsbara informationssystemet

används av den misstänkte. Under vissa förutsättningar får ett tillstånd beviljas för att ta del av uppgifter i ett annat avläsningsbart informationssystem än det som den misstänkte använder. Detta uttrycks genom att det anges att det ska finnas synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta det andra informationssystemet (4 § lagen om hemlig dataavläsning). Motsvarande krav på samband mellan den person som den hemliga dataavläsningen riktas mot och det informationssystem som åtgärden avser gäller vid användning av hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brott och när hemlig dataavläsning används vid särskild utlänningskontroll (4 b och 9 §§). I enlighet med utredningens förslag bör det i lagtexten inte längre ställas upp något krav på att kontakten med informationssystemet ska ha skett under en viss tid. Det kravet bör därför utgå i de aktuella bestämmelserna. Ett sådant krav kan dock även fortsättningsvis ställas upp i villkor om det i ett enskilt fall behövs för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

Med anledning av förändringar i den lagtekniska utformningen av 18 § lagen om hemlig dataavläsning bör följdändringar göras i lagen (2000:562) om internationell rättslig hjälp i brottmål.

8.3 Regleringen av villkor bör förtydligas

Regeringens förslag: Utöver det befintliga kravet på att rätten ska ange villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, införs ett krav på att ange vilka uppgifter som inte får granskas.

Om det framstår som obehövligt behöver villkor inte anges. Det ska dock alltid anges villkor i ett tillstånd som gäller kameraövervaknings- eller rumsavlyssningsuppgifter och som avser en viss person i stället för en viss plats.

Åklagaren, eller Säkerhetspolisen, ska i samband med en ansökan om hemlig dataavläsning föreslå de villkor som tillståndet bör förenas med. Ett sådant förslag behöver dock inte lämnas om villkor framstår som obehövligt.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår dock inte att villkor alltid ska anges om ett tillstånd som gäller kameraövervaknings- eller rumsavlyssningsuppgifter avser en viss person i stället för en viss plats.

Remissinstanserna: *Civil Rights Defenders* tillstyrker förslaget att det genom villkor ska anges vilka uppgifter som inte får granskas och att åklagaren eller Säkerhetspolisen ska föreslå villkor men avstyrker att det införs en ventil för när villkor inte behöver anges. *Helsingborgs tingsrätt* tillstyrker förslaget om en ventil men anser att en motsvarande bestämmelse som gäller för övriga hemliga tvångsmedel enligt rättegångsbalken hade varit att föredra. *Sveriges advokatsamfund* och *Göta hovrätt* är i huvudsak positiva till förslaget om tydligare regler för villkor men anser att tillstånd utan villkor endast bör förekomma i mycket begränsad utsträckning och att det därför bör framgå att villkor ska anges om det inte

är uppenbart obehövligt. *Säkerhets- och integritetsskyddsnämnden* avstyrker förslaget om att villkor inte behöver anges och framhåller att förslaget riskerar att medföra att villkor i flera fall inte ställs upp. Nämnden anser att det alltid finns ett behov av tidsmässigt begränsande villkor. Även *Integritetskyddsmyndigheten* är tveksam till förslaget om en ventil och menar att en stor mängd överskottsinformation kan genereras om ventilen används i större utsträckning än avsett eller om de villkor som anges inte får den begränsande effekt som avsetts. *Stockholms tingsrätt* anser att det bör framgå av lagtexten att sökanden ska ange om det är obehövligt med villkor.

Skälen för regeringens förslag: För att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan ska rätten i samband med att ett tillstånd till hemlig dataavläsning beslutas ange villkor (18 § första stycket 4 lagen om hemlig dataavläsning). Sådana villkor kan ta sikte på i stort sett vilka omständigheter som helst som kan gagna skyddet för den personliga integriteten. Exempelvis kan det anges att användningen av hemlig dataavläsning bör begränsas när det finns risk att utomstående, som inte alls har med utredningen att göra, riskerar att figurera i tal eller på film vid aktivering av en mikrofon eller kamera på en mobiltelefon (prop. 2019/20:64 s. 156). Villkorsbestämmelsen motsvarar vad som gäller för övriga hemliga tvångsmedel, med den skillnaden att det vid ett tillstånd till hemlig dataavläsning är obligatoriskt med villkor. Vid användning av de övriga hemliga tvångsmedlen gäller som huvudregel att villkor endast ska anges när det finns skäl för det. I tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning som avser en viss person i stället för en viss plats ska det dock alltid anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Åklagaren är skyldig att föreslå sådana villkor i samband med ansökan (27 kap. 21 § rättegångsbalken, 6 § preventivlagen och 14 § lagen om hemlig dataavläsning).

I Säkerhets- och integritetsskyddsnämndens granskning av användningen av hemlig dataavläsning har det framkommit att kravet på att ange villkor inte alltid följs i praktiken. Nämnden noterade i sin första granskning av hemlig dataavläsning 2021 att det i stor utsträckning förekommit tillstånd som saknade villkor (Säkerhets- och integritetsskyddsnämndens uttalande med beslut den 15 december 2021, dnr 92-2020). I en granskning av tillstånd med villkor som nämnden gjorde 2023 konstaterade nämnden att 90 procent av de granskade tillstånden innehöll standardiserade villkor. Nämndens slutsats var då att användningen av villkor inte har utgjort den rättssäkerhetsgaranti som var avsikten när lagen om hemlig dataavläsning infördes (Säkerhets- och integritetsskyddsnämndens uttalande med beslut den 20 juni 2023, dnr 80-2022).

Utöver förekomsten av standardiserade villkor har utredningen kunnat konstatera att det har förekommit villkor som har varit alltför begränsande och därmed hindrat att tillstånden har kunnat verkställas. Det kan, som utredningen redogör för, handla om att villkoren tar sikte på specifika filtreringar som ska göras redan vid inhämtningen. Eftersom det i många fall är okänt vilka de tillgängliga uppgifterna är innan inhämtningen påbörjas, innebär villkor som tar sikte på inhämtningsfasen typiskt sett att verkställigheten försvåras. Det är t.ex. svårt att på förhand veta när ett samtal kommer att äga rum, vilka som kommer att delta och vad som då

kommer att avhandlas. Det gör att ett tillstånd med villkor om att endast samtal med en viss person får hämtas in är svårt att verkställa.

För att komma till rätta med de problem som framkommit anser utredningen att det i regleringen bör tydliggöras vad villkoren ska avse. Utredningen föreslår att det nuvarande kravet på att ange villkor till skydd för enskildas personliga integritet ska kompletteras med ett krav på att ange vilka uppgifter som inte får granskas.

Regeringen delar utredningens bedömning att regleringen bör ändras. Förekomsten av standardiserade villkor som i princip återger någon av de grundläggande principer som gäller för tillämpningen av hemlig data-avläsning är problematisk, eftersom sådana villkor inte medför något starkare skydd för enskildas integritet. Det är också viktigt att villkoren inte formuleras på ett sätt som begränsar möjligheterna att verkställa tvångsmedlet på ett sätt som inte varit avsett. Villkoren bör i stället utformas med tillräcklig precision och tydlighet så att de kan utgöra den rättssäkerhetsgaranti som de är tänkta att vara. Eftersom det som regel är omöjligt att filtrera uppgifter i inhämtningsfasen bör villkoren i normalfallet i stället vara utformade för att begränsa vilka uppgifter som granskas. Att på så sätt ställa krav på att uppgifterna filtreras i samband med granskningen skulle inte vålla samma problem som villkor som tar sikte på inhämtningen. Även sådana villkor innebär att den information som de brottsbekämpande myndigheterna kan använda begränsas. Som utredningen föreslår bör därför det befintliga kravet på att rätten ska ange villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan kompletteras med ett krav på att ange vilka uppgifter som inte får granskas.

Att det ska anges villkor som tar sikte på granskningen hindrar inte att villkor som tar sikte på inhämtningsfasen anges om det framstår som ändamålsenligt i ett enskilt fall. Som *Säkerhets- och integritetsskydds-nämnden* framför kan det t.ex. finnas starka skäl att begränsa tillgången till uppgifter utifrån uppgifternas ålder. Om det är möjligt och ändamålsenligt bör alltså tidsmässiga villkor som tar sikte på inhämtningsfasen ställas upp. I de fall det inte är möjligt att ange sådana villkor bör det i de allra flesta fall vara möjligt att ange tidsmässiga villkor som begränsar vilka uppgifter som får granskas. Vilka uppgifter som får hämtas in eller granskas eller vilka övriga villkor som bör ställas upp får bedömas utifrån omständigheterna i det enskilda fallet. Avgörande är att villkoren är tydligt utformade och syftar till att se till att verkställigheten är rättssäker med så begränsade intrång i den enskildes personliga integritet som möjligt utifrån ändamålet med åtgärden.

Utredningen föreslår dessutom att det nuvarande obligatoriska kravet på villkor ska förses med en ventil för fall där villkor framstår som obehövligt. Förslaget ifrågasätts av *Civil Rights Defenders* och *Säkerhets- och integritetsskyddsnämnden*. *Sveriges advokatsamfund* och *Göta hovrätt* anför att det i stället bör regleras att villkor ska anges om det inte är uppenbart obehövligt, för att tydliggöra att tillstånd utan villkor endast bör förekomma i mycket begränsad utsträckning.

Förekomsten av villkor är av stor betydelse vid proportionalitets-bedömningen eftersom villkor begränsar intrånget i enskildas integritet. Att det finns villkor underlättar också tillsynsmyndighetens efterhands-kontroll. Regeringen anser därför att det är viktigt att villkor anges i de

situationer det är möjligt och ändamålsenligt. I likhet med utredningen bedömer regeringen att villkor som begränsar risken för onödiga integritetsintrång i de allra flesta fall är nödvändiga för att skapa tillräckliga garantier för att den hemliga dataavläsningen blir proportionerlig och rättssäker i det enskilda fallet. Som utredningen anför kan det dock finnas situationer där villkor för tillståndet framstår som överflödigt. Det kan t.ex. handla om en åtgärd som riktas mot ett informationssystem som endast används i kriminellt syfte. Det kan också finnas situationer där det framstår som tillräckligt att antingen ange vilka uppgifter som inte får granskas eller andra villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Som *Säkerhets- och integritetsskyddsnämnden* påpekar kan villkor som tar sikte på tidsmässiga avgränsningar vara en förutsättning för att en åtgärd ska kunna bedömas vara proportionerlig. Även när det gäller sådana villkor kan det dock förekomma situationer där de framstår som överflödiga.

Till skillnad från bl.a. Säkerhets- och integritetsskyddsnämnden anser regeringen därför, i likhet med utredningen, att det bör införas en ventil från kravet på att ange villkor. Som utredningen anger bör villkor anges om inte risken för onödiga kränkningar av den personliga integriteten redan är omhändertagen utan särskilda villkor. Så snart det finns anledning att tro att ett villkor kan vara av betydelse för att begränsa integritetsintrånget bör tillståndet alltså förenas med villkor. Mot den bakgrunden bör risken för att ventilen används i för stor utsträckning, som *Integritetsskyddsmyndigheten* befarar, vara ytterst begränsad. Till skillnad från *Sveriges advokatsamfund* och *Göta hovrätt* anser regeringen att den av utredningen föreslagna utformningen av ventilen framstår som väl avvägd. En förutsättning för att rätten inte ska behöva ange vilka uppgifter som inte får granskas eller övriga villkor till skydd för enskildas integritet bör därför vara att sådana villkor framstår som obehövligt. Däremot bör den ordning som enligt rättegångsbalken och preventivlagen gäller för hemlig rumsavlyssning och hemlig kameraövervakning som avser en viss person i stället för en viss plats även gälla när sådana uppgifter hämtas in genom hemlig dataavläsning (jfr prop. 2022/23:126 s. 153–155). I tillägg till utredningens förslag bör det därför framgå också i lagen om hemlig dataavläsning att villkor alltid ska anges i tillstånd som gäller rumsavlyssnings- eller kameraövervakningsuppgifter som avser en viss person i stället för en viss plats.

Utredningen föreslår vidare att åklagaren eller i förekommande fall Säkerhetspolisen, i samband med en ansökan om hemlig dataavläsning, ska vara skyldig att föreslå de villkor som tillståndet bör förenas med. När lagen om hemlig dataavläsning infördes uttalade regeringen att den inte såg något behov av en bestämmelse om att sökanden ska ange villkor, men att det vid sammanträdet kan finnas anledning för den som ansöker om tillstånd att motivera sin ansökan genom att på ett övergripande plan beskriva hur tvångsmedlet ska verkställas (prop. 2019/20:64 s. 156 och 157).

Det kan vara svårt för rätten att genom frågor se till att underlaget är tillräckligt för att kunna utforma villkoren på ett ändamålsenligt sätt eller bedöma om ett villkor hindrar verkställigheten på ett sätt som inte är avsett. Det beror bl.a. på att hemlig dataavläsning är en tekniskt komplicerad metod och att förutsättningarna för både verkställighet och

utformningen av villkor varierar mellan olika ärenden. Det är åklagaren som, tillsammans med de tekniker som ska genomföra verkställigheten, har bäst insyn i utredningen. Redan i samband med ansökan bör åklagaren också ha övervägt de närmare förutsättningarna för verkställighet och hur integritetsintrånget kan begränsas. En skyldighet för åklagaren, eller i förekommande fall Säkerhetspolisen, att lämna förslag på villkor bör kunna bidra till att villkoren får högre kvalitet och samtidigt minska risken för att tillstånd meddelas helt utan villkor trots att det finns behov av det eller med standardiserade eller verkställighetshindrande villkor. En sådan skyldighet bör därför införas. På samma sätt som i dag bör det därefter vara upp till rätten att göra en bedömning av om de föreslagna villkoren är tillräckliga för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan eller om andra eller ytterligare villkor behövs. Om åklagaren eller Säkerhetspolisen anser att det är obehövligt att förena ett tillstånd med villkor bör det anges med en motivering varför så är fallet. Till skillnad från *Stockholms tingsrätt* anser regeringen att det inte behöver framgå uttryckligen av lagtexten.

8.4 Teknikanpassning och otillåten tilläggsinformation

Regeringens förslag: Det nuvarande kravet på att tekniken inte får möjliggöra inhämtning av någon annan uppgiftstyp än vad som anges i tillståndet tas bort. I stället ska det, vid verkställighet av hemlig dataavläsning, krävas att både tekniken och tillvägagångssättet anpassas efter tillståndet.

Om det har hämtats in uppgifter som enligt villkor i tillståndet inte får hämtas in eller granskas ska uppgifterna omedelbart förstöras. Sådana uppgifter får inte användas till nackdel för någon i en brottsutredning.

Skyldigheten att avbryta verkställigheten av hemlig dataavläsning om det kommer fram otillåten tilläggsinformation justeras. Om det under eller efter verkställigheten kommer fram sådan information ska granskningen av uppgifter i den delen omedelbart avbrytas. Upptagningarna och uppteckningarna ska då förstöras i de delar som de omfattas av förbuden.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Säkerhets- och integritetsskyddsnämnden* anser att det är positivt att förslaget bidrar till att det inte bevaras fler inhämtade uppgifter än vad som är nödvändigt men menar att det bör analyseras hur den föreslagna regleringen förhåller sig till Europadomstolens praxis. *Tidningsutgivarna* är tveksamma till förslaget om att granskningen och inte verkställigheten ska avbrytas om det kommer fram otillåten tilläggsinformation och understryker att ändringen inte får medföra att hanteringen fördröjs.

Skälen för regeringens förslag

Tekniken och tillvägagångssättet ska anpassas efter tillståndet

Enligt nuvarande reglering ska den teknik som används i samband med hemlig dataavläsning anpassas efter det tillstånd som beviljats. Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet (23 § lagen om hemlig dataavläsning). Enligt förarbetena innebär det att det inte ska vara möjligt att med den teknik som används t.ex. läsa av eller ta upp kameraövervakningsuppgifter om tillståndet avser kommunikationsavlyssningsuppgifter. Om ett tekniskt hjälpmedel är konstruerat på så sätt att det i och för sig är möjligt att använda det för att läsa av eller ta upp olika uppgiftstyper krävs det att hjälpmedlet är inställt på ett sådant sätt att det inte är möjligt att utan ändringar av inställningarna i hjälpmedlet komma åt andra uppgiftstyper än de som tillståndet avser (prop. 2019/20:64 s. 236 och 237).

Utifrån hur hemlig dataavläsning har visat sig användas i praktiken konstaterar utredningen att regleringen kan framstå som missvisande. Det har framkommit att det i princip alltid är tekniskt möjligt att hämta in andra uppgiftstyper än de som anges i tillståndet. Dessutom går den information som ingår i de olika uppgiftstyperna inte alltid att dela upp under inhämtningsfasen. Även om det är möjligt att särskilja t.ex. kommunikationsavlyssningsuppgifter från kameraövervakningsuppgifter kan det vara svårt att särskilja övriga lagrade uppgifter från de andra uppgiftstyperna. Mot denna bakgrund framstår det inte som ändamålsenligt med ett krav på att den tekniska utrustningen inte får möjliggöra inhämtning av vissa uppgiftstyper. Som utredningen föreslår bör det kravet tas bort och i stället bör den skyldighet som finns att anpassa tekniken efter tillståndet även omfatta myndigheternas tillvägagångssätt vid genomförandet. I praktiken handlar verkställigheten av hemlig dataavläsning nämligen lika mycket om det tillvägagångssätt som används som hur tekniken anpassas. Ett anpassningskrav som tar sikte på hela verkställigheten skulle utöver inhämtningen av uppgifter även omfatta bearbetningen av uppgifterna i form av förädling, sortering och filtrering av inhämtade uppgifter. Den myndighet som verkställer ett beslut om hemlig dataavläsning ansvarar för att kraven på anpassning är uppfyllda.

Tydligare regler om vad som utgör otillåten tilläggsinformation

Om en typ av uppgift som inte omfattas av tillståndet till hemlig dataavläsning har hämtats in så utgör den uppgiften otillåten tilläggsinformation. Sådana uppgifter ska omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden ska underrättas. Uppgifterna får inte heller användas till nackdel för någon i en brottsutredning (23 § lagen om hemlig dataavläsning). Utredningen föreslår att det ska förtydligas att även uppgifter som har hämtats in i strid med villkor i tillståndet utgör otillåten tilläggsinformation. Eftersom ett villkor i ett tillstånd kan begränsa vilka uppgifter som får hämtas in eller granskas kan även inhämtande av en viss uppgift vara oförenlig med tillståndet. Regeringen instämmer i utredningens bedömning att även sådana uppgifter bör hanteras som otillåten tilläggsinformation. Det finns därför skäl att förtydliga att upptagningar och uppteckningar av uppgifter som inte får hämtas in eller granskas enligt villkor i ett tillstånd ska förstöras i de delar de innehåller sådana uppgifter. Det bör

göras så snart det står klart att sådana uppgifter har hämtats in eller granskats. Det innebär att de uppgifter som enligt villkoren får hämtas in men inte granskas ska förstöras när de påträffas, dvs. i regel direkt efter att de sorterats och filtrerats bort i en initial bearbetningsfas. Som utredningen framhåller bör det, ur ett integritetsskyddsperspektiv, undvikas att information som aldrig har efterfrågats bevaras.

En risk med att information inte bevaras är att det kan försvåra kontroll i efterhand. *Säkerhets- och integritetsskyddsnämnden* framför att det kan finnas skäl att ytterligare analysera hur den föreslagna regleringen förhåller sig till Europadomstolens praxis. Europadomstolen har i ett par avgöranden fällt Finland för att material från hemliga tvångsmedel förstörts under utredningsstadiet (Europadomstolens domar den 8 december 2009 i målet Janatuinen mot Finland, nr 28552/05, och den 30 juni 2009 i målet Natunen mot Finland, nr 21022/04). Europadomstolen fann att agerandet hade inneburit en kränkning av den misstänktes rätt till en rättvis rättegång, eftersom besluten att förstöra materialet medfört att varken domstolen eller den misstänkte fått möjlighet att bedöma om materialet varit relevant eller inte.

Som utredningen konstaterar skiljer sig dock den situation som det här är fråga om från en situation där de brottsbekämpande myndigheterna har gjort ett urval av utredningsmaterialet. I den nu aktuella situationen handlar det om material som myndigheterna, om det varit tekniskt möjligt, inte skulle ha hämtat in. Informationen bör sorteras bort i ett tidigt skede och varken granskas närmare eller användas. Av det skälet instämmer regeringen i utredningens bedömning att informationen bör förstöras på samma sätt som annan information som har hämtats in av misstag.

Enligt nuvarande ordning får uppgiftstyper som inte omfattas av tillståndet inte användas till nackdel för någon. Regleringen har motiverats med att tydliga och uttryckliga bestämmelser till skydd för rättssäkerheten är nödvändigt med hänsyn till lagens ingripande karaktär (prop. 2019/20:64 s. 163). På motsvarande sätt bör det vara tydligt att inte heller uppgifter som inte får hämtas in eller granskas enligt ett tillstånd får användas till nackdel för någon.

Ett tydligare förbud mot granskning av vissa uppgifter

I rättegångsbalken finns regler om förbud mot beslag av skriftliga handlingar och mot hemlig avlyssning av elektronisk kommunikation i vissa fall (27 kap. 2 och 22 §§ rättegångsbalken). Förbuden syftar till att skapa ett skydd för information som motsvarar det skydd som undantagen från vittnesplikten ger (det s.k. frågeförbudet i 36 kap. 5 § rättegångsbalken). Frågeförbudet innebär att det inte är tillåtet att höra företrädare för vissa yrkeskategorier, bl.a. advokater, sjukvårdspersonal och präster, som vittne om vissa förhållanden som de har anförtrotts eller erfarit i sin yrkesutövning. Enligt beslags- och avlyssningsförbuden får handlingar inte tas i beslag och samtal eller andra meddelanden får inte avlyssnas om det förekommer uppgifter som skyddas av frågeförbudet.

Motsvarande regler finns för hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter, rumsavlyssningsuppgifter och övriga åtkomliga uppgifter. Om det kommer fram uppgifter som omfattas av beslags- eller avlyssningsförbuden under verkställigheten av hemlig

dataavläsning ska den omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbuden (27 § lagen om hemlig dataavläsning). Som utredningen anger kan bestämmelsen dock ge en missvisande bild av de brottsbekämpande myndigheternas möjligheter att avbryta inhämtning av sådana uppgifter som förbuden tar sikte på. Under inhämtningsfasen av andra uppgifter än realtidsuppgifter har myndigheterna begränsad kännedom om materialets innehåll. Vid inhämtning av sådana uppgifter är det därför svårt och ofta omöjligt för de brottsbekämpande myndigheterna att göra en bedömning av om uppgifterna omfattas av beslags- eller avlyssningsförbuden. Enligt utredningen har företrädare för de brottsbekämpande myndigheterna framhållit att särskilt uppgifter som omfattas av avlyssningsförbudet i princip bara är möjliga att upptäcka först vid själva granskningen av de inhämtade uppgifterna.

Som utredningen föreslår bör det i lagtexten anges att granskningen ska avbrytas i stället för att verkställigheten ska avbrytas. På så sätt tar regleringen tydligare sikte på sådana uppgifter som den verkställande myndigheten får kännedom om efter verkställigheten, dvs. i granskningsfasen. I fråga om hur verkställigheten går till kan hemlig dataavläsning jämföras med en husrannsakan snarare än med hemlig avlyssning av elektronisk kommunikation. Det innebär att den verkställande myndigheten som regel först hämtar in materialet och därefter tar del av innehållet. Det saknas därför skäl att avbryta verkställigheten stället bör granskningen av uppgifterna i den delen avbrytas om det under eller efter verkställigheten kommer fram uppgifter som omfattas av förbudsbestämmelserna. Som *Tidningsutgivarna* framhåller bör avbrytandet dock inte göras senare än vad som är möjligt.

På samma sätt som i dag bör upptagningarna och uppteckningarna omedelbart förstöras i de delar som de omfattas av förbuden.

8.5 Användningen av överskottsinformation

Regeringens förslag: Åklagare ska, utan några begränsningar, få besluta att uppgifter som har kommit fram vid användning av hemlig dataavläsning får användas för ett annat ändamål än det som har legat till grund för åtgärden.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser tillstyrker eller har inga invändningar mot förslaget. *Centrum för rättvisa*, *Civil Rights Defenders* och *Journalistförbundet* avstyrker förslaget. Civil Rights Defenders anser att en användning av överskottsinformation som har tillkommit genom hemliga tvångsmedel måste föregås av lagregler samt mekanismer som säkerställer en rättssäker och proportionerlig användning av informationen med hänsyn till åtgärdens integritetskränkande karaktär. *Centrum för rättvisa* anser att förslaget kommer att medföra betydande risker för enskildas rättigheter och att möjligheten till ansvarsutkrävande och kontroll kommer vara mycket begränsad. Centrum för rättvisa föreslår att det tydliggörs i lag vilka typer av uppgifter som får respektive inte får användas, till vilka myndigheter uppgifterna får lämnas och för vilka

syften. *Journalistförbundet* menar att möjligheten att använda överskottsinformation ökar risken för att uppgifter som omfattas av källskydd röjs. *JO* framhåller att förslaget innebär särskilda risker, bl.a. en risk för att gränsen mellan hemliga tvångsmedel inom ramen för en förundersökning och preventiva tvångsmedel suddas ut. JO poängterar även vikten av en rättssäker reglering.

Skälen för regeringens förslag

En tydligare regel med ett utökat användningsområde

De uppgifter som kommer fram vid användningen av hemliga tvångsmedel och som handlar om något annat än det brott eller den brottslighet som legat till grund för åtgärden kallas överskottsinformation. För enskilda innebär användningen av hemliga tvångsmedel ett betydande intrång i den personliga integriteten, och att använda den information som tvångsmedlen ger tillgång till för andra ändamål kan innebära ett ytterligare intrång. Utifrån Europadomstolens praxis finns inget förbud mot att använda sådan information, men bestämmelser om användningen ska vara tydliga och huvudsakligen finnas i lag. Av rättssäkerhetsskäl är det därför viktigt att det finns en proportionerlig, heltäckande och uttömmande reglering om när överskottsinformation från hemliga tvångsmedel får användas.

Enligt nuvarande regler får överskottsinformation från hemlig dataavläsning alltid användas för att förhindra förestående brott. Om de uppgifter som kommer fram under förundersökning eller i underrättelseverksamhet enligt preventivlagen rör viss allvarlig brottslighet får de också användas för att utreda brottet (28 och 29 §§ lagen om hemlig dataavläsning). Vid hemlig dataavläsning i underrättelseverksamhet enligt inhämtningslagen får uppgifter som har kommit fram användas i en förundersökning endast efter tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för beslut om att inleda en förundersökning (31 § andra stycket lagen om hemlig dataavläsning).

När reglerna om användning av överskottsinformation från hemlig dataavläsning under förundersökning och i underrättelseverksamhet infördes motsvarade de vad som då gällde för de bakomliggande tvångsmedlen. De reglerna har dock kritiserats för att vara otydliga, oförutsebara och alltför begränsande i förhållande till i vilken utsträckning överskottsinformation får användas. Mot den bakgrunden infördes ändrade regler om användning av överskottsinformation för hemliga tvångsmedel enligt rättegångsbalken och preventivlagen den 1 oktober 2023. De nya reglerna innebär att åklagare, utan andra begränsningar än de som följer av proportionalitetsprincipen, ska få besluta att uppgifter som kommit fram vid användning av hemliga tvångsmedel ska få användas för ett annat ändamål än det som har legat till grund för åtgärden (27 kap. 23 a § rättegångsbalken och 12 § preventivlagen). Motsvarande möjlighet att använda överskottsinformation finns sedan den 1 september 2024 även enligt inhämtningslagen, dock med den skillnaden att det är den verkställande myndigheten som beslutar om användningen (6 § inhämtningslagen). Lagändringarna har inte omfattat hemlig dataavläsning.

Som skäl för förändringarna anfördes bl.a. att de brottsbekämpande myndigheterna behöver ha goda möjligheter att hämta in och bearbeta information för att kunna förebygga, förhindra, upptäcka, utreda och lagföra brott. Ett problem som uppmärksammades var att bestämmelserna om överskottsinformation i syfte att förhindra brott inte var tillämpliga när ett brott väl har påbörjats. Det ansågs vara en otillfredsställande ordning att de brottsbekämpande myndigheterna inte alltid kunde använda sig av konkreta uppgifter för att ingripa och avbryta pågående brottslighet eller för att utreda brott som redan begåtts. Vidare ansåg regeringen att det kan finnas ett tydligt behov av att kunna överlämna överskottsinformation till en annan myndighet i vissa fall, t.ex. vid uppgifter om att ett barn far illa. Det konstaterades att begränsningar i hur information får användas för att utreda brott är ovanliga i det processrättsliga regelverket som genomsyras av principerna om fri bevisföring och fri bevisprövning. För att förenkla tillämpningen infördes därför en enhetlig regel för all användning av informationen, såväl inom som utanför de brottsbekämpande myndigheternas verksamhet. Det innebär att användning av överskottsinformation numera bedöms utifrån samma faktorer som annan information och på samma sätt som för hemliga tvångsmedel enligt rättegångsbalken, preventivlagen och inhämtningslagen. Detta har ansetts förenkla handläggningen för de brottsbekämpande myndigheterna och minska riskerna för att fel begås (prop. 2022/23:126 s. 173–177 och prop. 2023/24:117 s. 77–80).

När lagen om hemlig dataavläsning infördes bedömdes att reglerna om överskottsinformation skulle följa de regler som gäller för de övriga hemliga tvångsmedlen (prop. 2019/20:64 s. 168). Som utredningen konstaterar talar systematiska skäl för att regleringen om överskottsinformation från hemlig dataavläsning nu bör ändras på motsvarande sätt som för övriga hemliga tvångsmedel. Ett argument, som *JO* lyfter, som kan tala mot en sådan utvidgning av användningsområdet för överskottsinformation är att hemlig dataavläsning i förhållande till övriga hemliga tvångsmedel kan generera stora mängder information inklusive överskottsinformation, vilket kan innebära ökade risker för enskildas personliga integritet. Det ska dock beaktas att det är fråga om information som de brottsbekämpande myndigheterna redan har tillgång till. Det framstår också som en svårförklarlig ordning att uppgifter som hämtats in genom hemlig dataavläsning inte skulle kunna överlämnas till andra myndigheter för användning i ett annat befogat syfte enbart på grund av att de kommit fram genom hemlig dataavläsning, när det hade varit möjligt att överlämna dem om de framkommit på annat sätt. Med hänsyn till de positiva effekter som ett utvidgat användningsområde kan antas få anser regeringen, i likhet med utredningen och flertalet remissinstanser, att övervägande skäl talar för att ändra reglerna om överskottsinformation på motsvarande sätt som redan gjorts i rättegångsbalken, preventivlagen och inhämtningslagen. Regeringen instämmer således inte i de synpunkter som förs fram av *Centrum för rättvisa* och *Civil Rights Defenders* om att det krävs ytterligare förtydliganden i lagtexten för hur överskottsinformation ska få användas. Mot bakgrund av att hemlig dataavläsning inte får avse vissa informationssystem till skydd för journalistisk verksamhet, delar regeringen inte heller *Journalistförbundets* farhåga att ändrade regler för

användningen av överskottsinformation innebär en risk för att källskyddet inte respekteras.

Utvidgningen innebär emellertid inte att det alltid ska vara tillåtet att använda överskottsinformation. Innan tillstånd till användning av överskottsinformation ges ska en prövning göras av om användningen är förenlig med proportionalitetsprincipen. Det innebär att överskottsinformationen endast får användas i de fall det är rimligt i förhållande till syftet med åtgärden, vägt mot bl.a. det intrång som användningen kan innebära för den som informationen avser. När det gäller vem som ska få fatta beslut om hur överskottsinformation ska användas bör motsvarande ordning gälla som för de bakomliggande hemliga tvångsmedlen. Det innebär att åklagare beslutar om användning av överskottsinformation i en förundersökning och enligt preventivlagen och att den verkställande myndigheten beslutar om användningen enligt inhämtningslagen.

Behov av följdändringar

I lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder, som trädde i kraft den 1 juli 2024, stämmer bestämmelsen om överskottsinformation från övervakning av elektronisk kommunikation överens med de nya reglerna om överskottsinformation i rättegångsbalken och preventivlagen. En åklagare får alltså besluta att uppgifter som har kommit fram vid användning av hemlig övervakning av elektronisk kommunikation får användas för ett annat ändamål än det som legat till grund för åtgärden.

Regleringen av överskottsinformation från hemlig dataavläsning utformades dock annorlunda (se 10 § andra stycket lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder).

De skäl som ligger bakom den nu föreslagna ändringen av hanteringen av överskottsinformation i lagen om hemlig dataavläsning gör sig lika starkt gällande när hemlig dataavläsning används enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder. Det är också fortsatt viktigt att reglerna om hantering av överskottsinformation från hemlig dataavläsning är tydliga och enhetliga. Motsvarande ändringar bör därför göras i reglerna om överskottsinformation från hemlig dataavläsning i lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.

8.6 Krav på bevarande av material

Regeringens förslag: Upptagningar och uppteckningar från hemlig dataavläsning ska bevaras utan begränsning till att de ska vara av betydelse från brottsutredningssynpunkt. Om den misstänkte medger det ska upptagningar och uppteckningar från en förundersökning få förstöras innan förundersökningen har avslutats eller ett mål har avgjorts slutligt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser, däribland *JO*, är positiva eller har inte några invändningar mot förslaget. *Säkerhets- och integritets-*

skyddsnämnden anser att förslaget inte bör genomföras utan att bestämmelsen om bevarande och förstöring av material i rättegångsbalken justeras. Enligt nämnden innebär den bestämmelsens ordalydelse att förstöringsskyldigheten även omfattar sådana uppgifter som har överlämnats för att användas i underrättelseverksamhet, även om så inte varit avsikten.

Skälen för regeringens förslag: I de delar upptagningar och uppteckningar från användningen av hemlig dataavläsning under en förundersökning är av betydelse ur brottsutredningssynpunkt ska de bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal har beslutats, målet har avgjorts slutligt. De ska därefter förstöras (28 § lagen om hemlig dataavläsning och 27 kap. 24 § andra stycket rättegångsbalken i dess lydelse före den 1 oktober 2023). Regeln om bevarande gäller både sådant material som är av betydelse för utredningen av det brott som legat till grund för beslutet om hemliga tvångsmedel och, i förekommande fall, de delar som är av betydelse för att utreda andra brott, se propositionen Överskottsinformation vid användning av hemliga tvångsmedel m.m. (prop. 2004/05:143 s. 52). I de delar som upptagningarna och uppteckningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. När materialet inte längre behövs för detta ändamål ska det förstöras. I de delar upptagningar och uppteckningar från användningen av hemlig dataavläsning i underrättelseverksamhet är av betydelse för att förebygga, förhindra eller upptäcka brott får de bevaras så länge de behövs för sitt syfte. Om uppgifter i upptagningarna och uppteckningarna från åtgärder enligt preventivlagen får användas för att utreda brott ska de bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal har beslutats, målet har avgjorts slutligt. De ska därefter förstöras (29 § lagen om hemlig dataavläsning och 13 § preventivlagen i lydelsen före den 1 oktober 2023 samt 31 § lagen om hemlig dataavläsning och 8 § inhämtningslagen i lydelsen före den 1 september 2024).

Fram till den 1 oktober 2023, då nya regler om bevarande infördes i rättegångsbalken, gällde samma regelverk för bevarande av material från de hemliga tvångsmedlen enligt rättegångsbalken som för bevarande av material från hemlig dataavläsning. De nya reglerna innebär att allt material från hemliga tvångsmedel under en förundersökning ska bevaras till dess förundersökningen läggs ned eller, om åtal väcks, till dess målet avgjorts slutligt. Endast om den misstänkte medger det får materialet förstöras innan dess. Det är alltså inte längre en förutsättning för bevarande att upptagningarna och uppteckningarna är av betydelse ur brottsutredningssynpunkt. I förarbetena motiveras förändringen bl.a. med att det under en pågående utredning kan vara svårt att göra en bedömning av vilket material som har betydelse för utredningen. En felaktig bedömning kan gå ut över både möjligheterna att utreda och lagföra brottet och den misstänktes möjlighet att förbereda sitt försvar. Det kan i sin tur leda till att den misstänktes rätt till en rättvis rättegång åsidosätts. I praktiken var utgångspunkten visserligen redan innan lagändringen att material från hemliga tvångsmedel ska bevaras så länge förundersökning och lagföring pågår, om materialet inte omfattas av avlyssningsförbudet. För att förenkla tillämpningen och få en bättre överensstämmelse med Europadomstolens praxis och det sätt som regleringen tillämpas i praktiken togs dock

begränsningen bort om att upptagningarna och uppteckningarna ska vara av betydelse från brottsutredningssynpunkt för att bevaras. I och med att lagen om hemlig dataavläsning infördes efter att den utredning som föreslagit ändringarna i rättegångsbalken redovisat sitt uppdrag, omfattades hemlig dataavläsning inte av de överväganden som gjordes då (prop. 2022/23:126 s. 182–185).

I preventivlagen ändrades bestämmelsen om bevarande som en följd av att en begränsning av användningen av överskottsinformation togs bort. Av samma skäl har även bestämmelsen om bevarande i inhämtningslagen nyligen ändrats (prop. 2022/23:126 s. 233 och prop. 2023/24:117 s. 81).

När hemlig dataavläsning infördes bedömdes att reglerna om bl.a. bevarande av material skulle följa vad som gäller för de bakomliggande tvångsmedlen (prop. 2019/20:64 s. 171). Som utredningen konstaterar gäller de argument som låg till grund för att justera bestämmelsen om bevarande i rättegångsbalken även för hemlig dataavläsning. Utredningen föreslår därför att reglerna ska ändras så att de återigen motsvarar vad som gäller enligt rättegångsbalken, preventivlagen och inhämtningslagen. Lagtekniskt innebär förslaget att hänvisningarna i lagen om hemlig dataavläsning justeras så att de inte längre avser äldre lydelser av de aktuella bestämmelserna i rättegångsbalken, preventivlagen och inhämtningslagen.

Säkerhets- och integritetsskyddsnämnden framhåller att den bestämmelse i rättegångsbalken (27 kap. 24 §) som lagen om hemlig dataavläsning föreslås hänvisa till, anger att det är uppgifter – och inte, som tidigare, upptagningar och uppteckningar – som ska förstöras när de inte längre ska bevaras. Nämnden anser att bestämmelsen har fått en otydlig utformning eftersom det kan uppfattas som att förstöringsskyldigheten även omfattar överskottsinformation, t.ex. uppgifter som överlämnats till Polismyndighetens underrättelseverksamhet. Nämnden anser att det därför kan ifrågasättas om det är lämpligt att låta rättegångsbalkens bestämmelse gälla även för hemlig dataavläsning.

Genom de ändringar i 27 kap. 24 § rättegångsbalken som trädde i kraft den 1 oktober 2023 utgick den tidigare regleringen om hantering av material inom ramen för användandet av överskottsinformation. Av förarbetena till bestämmelsen framgår att överskottsinformation får behandlas med stöd av bestämmelsen i 27 kap. 23 a § rättegångsbalken utan särskilda begränsningar (prop. 2022/23:126 s. 222). Mot den bakgrunden finns det inte skäl att frångå utredningens förslag, utan till skillnad från *Säkerhets- och integritetsskyddsnämnden* anser regeringen att förslaget bör genomföras.

8.7 Skyldighet att dokumentera

Regeringens förslag: Beslut och åtgärder som rör hemlig dataavläsning ska dokumenteras.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *JO* och *Tidningsutgivarna* tillstyrker förslaget. *Riksarkivet* tillstyrker dokumentationskravet men anser att det bör övervägas om regeringen eller den myndighet som regeringen bestämmer

bör bemyndigas att meddela närmare föreskrifter om dokumentationens innehåll. *Malmö tingsrätt* anser att det bör förtydligas vilken myndighet som ska vara skyldig att dokumentera beslut och åtgärder som rör hemlig dataavläsning. *Bahnhof* anser att det av dokumentationskravet bör framgå vilken metod som de brottsbekämpande myndigheterna avser använda för hemlig dataavläsning.

Skälen för regeringens förslag: Det finns inte någon lagstadgad skyldighet att dokumentera användningen av hemlig dataavläsning. För hemliga tvångsmedel enligt rättegångsbalken, preventivlagen och inhämtningslagen gäller däremot en skyldighet att dokumentera beslut och åtgärder sedan den 1 oktober 2023 respektive den 1 september 2024 (27 kap. 35 § rättegångsbalken, 19 § preventivlagen och 8 § inhämtningslagen). Syftet med reglerna är att stärka den enskildes möjlighet till efterhandskontroll och förbättra förutsättningarna för Säkerhets- och integritetsskyddsnämndens tillsyn. Reglerna innehåller inga närmare bestämmelser om vilka uppgifter och åtgärder som ska dokumenteras. I förarbetena har det dock inte uteslutits att det framöver kan finnas ett behov av särskilda föreskrifter om vad dokumentationsskyldigheten bör omfatta (prop. 2022/23:126 s. 181 och 182).

De argument som framhållits för att införa ett dokumentationskrav i rättegångsbalken, preventivlagen och inhämtningslagen gör sig gällande även i fråga om hemlig dataavläsning. Regeringen instämmer därför i utredningens bedömning att det bör införas en skyldighet att dokumentera beslut och åtgärder som rör hemlig dataavläsning. Inte heller denna reglering bör vara alltför detaljerad utan bör utformas på motsvarande sätt som gäller för övriga hemliga tvångsmedel. Av det skälet bedömer regeringen inte att det bör preciseras i lagtexten att de brottsbekämpande myndigheternas metod ska dokumenteras, något som *Bahnhof* föreslår. Som *Riksarkivet* framhåller kan det även när det gäller hemlig dataavläsning finnas skäl att förtydliga dokumentationsskyldigheten genom ytterligare föreskrifter. Någon ytterligare reglering i lag behövs däremot inte. Regeringen delar inte *Malmö tingsrätts* uppfattning att det i lagtexten bör förtydligas hos vilken myndighet dokumentationen ska ske. En naturlig utgångspunkt är dock att åtgärderna dokumenteras vid den myndighet de vidtas.

Även när hemlig dataavläsning sker enligt lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder bör beslut och åtgärder dokumenteras på motsvarande sätt. En bestämmelse om detta bör därför införas även i den lagen.

8.8 Rättssäkerhetsgarantierna är tillräckliga

Regeringens bedömning: De nuvarande rättssäkerhetsgarantierna i lagen om hemlig dataavläsning innebär tillsammans med de kompletterande regler som föreslås i denna lagrådsremiss ett tillräckligt skydd för enskildas integritet och är förenliga med regeringsformens och Europakonventionens krav.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser uttalar sig inte särskilt över utredningens bedömning. *Bahnhof* anser att de brottsbekämpande myndigheterna bör ha ett strikt skadeståndsansvar i förhållande till telekomoperatörer och tredje man när operatörerna tvingas medverka vid verkställighet av hemlig dataavläsning. Bahnhof menar också att Säkerhets- och Integritetsskyddsnämnden bör få möjlighet att utöva tillsyn under verkställighet och avbryta en verkställighet som man anser är felaktig. *Tidningsutgivarna* förordar att beslut om hemlig dataavläsning endast ska kunna fattas av rätten, bl.a. eftersom behovet av att åklagare fattar interimistiska beslut är begränsat. *Civil Rights Defenders* delar inte utredningens bedömning att kontrollmekanismerna och rättssäkerhetsgarantierna är tillräckliga och föreslår att det bör utredas hur Säkerhets- och integritetsskyddsnämnden ska få bättre insyn och om rätten till effektiva rättsmedel för den enskilde vars integritet har kränkts är tillräcklig. *Säkerhets- och integritetsskyddsnämnden* anser att skyldigheten att underrätta nämnden bör ligga på den ansökande myndigheten och inte på rätten som beslutar om ett tillstånd om hemlig dataavläsning. *Diskrimineringsombudsmannen* påtalar nödvändigheten av att diskrimineringslagens tillämpningsområde utvidgas så att offentlig verksamhet, inklusive Polismyndighetens och andra rättsvårdande myndigheters verksamheter, fullt ut omfattas av lagens förbud mot diskriminering.

Skälen för regeringens bedömning: Hemlig dataavläsning medför som utgångspunkt risker för intrång i enskildas personliga integritet. Om det ska vara möjligt att använda hemlig dataavläsning måste reglerna utformas på ett sätt som innebär en rimlig balans mellan integritetsintressena och de syften som tvångsmedlet ska användas för.

Utredningen har utvärderat nuvarande kontrollmekanismer och andra rättssäkerhetsgarantier och konstaterar att regelverket i stor utsträckning lever upp till de krav som regeringsformen och Europakonventionen ställer på lagstiftningen, även med beaktande av de ändringar som nyligen har genomförts för att utöka möjligheterna att använda hemliga tvångsmedel. Tillsammans med de föreslagna kompletterande och förtydligande reglerna för att stärka rättssäkerheten bedömer regeringen att enskilda har ett robust och ändamålsenligt integritetsskydd och att lagstiftningen uppfyller befogade krav på rättssäkerhet.

I likhet med utredningen som har haft kontakt med bl.a. företrädare för de största operatörerna i frågan, men till skillnad från *Bahnhof*, görs bedömningen att reglerna om medverkansskyldighet i 24 § lagen om hemlig dataavläsning uppfyller de rättssäkerhetskrav som ställs på lagstiftningen.

Sammanfattningsvis anser regeringen, till skillnad från *Bahnhof* och *Civil Rights Defenders*, att de nuvarande rättssäkerhetsgarantierna i lagen om hemlig dataavläsning ger ett tillräckligt skydd för enskildas integritet och är förenliga med regeringsformens och Europakonventionens krav. Regeringen bedömer att det inom ramen för detta lagstiftningsarbete inte finns beredningsunderlag att ta ställning till *Säkerhets- och integritetsskyddsnämndens* förslag att ändra rättens underrättelseskyldighet eller att överväga *Tidningsutgivarnas* förslag om att förändra möjligheten för åklagare att fatta interimistiska beslut.

9 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Lagändringarna ska träda i kraft den 1 april 2025.

Ändringarna i lagen om hemlig dataavläsning som upphäver de tidsbegränsade bestämmelserna som innebär att hemlig dataavläsning kan användas i syfte att förhindra brottslig verksamhet ska träda i kraft den 1 oktober 2028.

Äldre föreskrifter ska gälla för tillstånd som har beslutats före ikraftträdandet.

Äldre bestämmelser om möjligheter att använda överskottsinformation i rättegångsbalken, preventivlagen och lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder ska gälla för uppgifter från hemlig dataavläsning som verkställts före ikraftträdandet.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att lagändringarna ska träda i kraft den 1 mars 2025. Utredningen lämnar inte något förslag när det gäller de bestämmelser om hemlig dataavläsning som föreslås begränsas i tid eller någon övergångsbestämmelse i förhållande till lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder.

Remissinstanserna uttalar sig inte särskilt om förslaget.

Skälen för regeringens förslag: Den nuvarande lagen om hemlig dataavläsning upphör att gälla vid utgången av mars 2025. I avsnitt 5 föreslås att lagen ska fortsätta gälla. Det är därför lämpligt att lagändringarna träder i kraft den 1 april 2025. Bestämmelserna som innebär att hemlig dataavläsning som gäller rumsavlyssningsuppgifter får användas i preventivt syfte för att förhindra brottslig verksamhet föreslås dock tidsbegränsas till utgången av september 2028. Detsamma gäller bestämmelserna som innebär att ett tillstånd till hemlig dataavläsning som gäller kameraövervaknings- eller rumsavlyssningsuppgifter i preventivt syfte kan knytas till en person. Ändringarna i lagen om hemlig dataavläsning som upphäver de nyss nämnda bestämmelserna bör därför träda i kraft den 1 oktober 2028.

Utgångspunkten när det gäller processrättslig lagstiftning är att nya regler ska tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. För tydlighetens skull bör det dock regleras vad som gäller för ett tillstånd som har beslutats före ikraftträdandet, men som ännu inte har löpt ut. Äldre föreskrifter bör fortfarande gälla för tillstånd som har beviljats före ikraftträdandet.

Förslagen i avsnitt 8 innebär att möjligheterna att använda överskottsinformation från hemlig dataavläsning under förundersökning och i preventivt syfte samt enligt lagen om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder utökas. Av rättssäkerhetsskäl bör det inte vara tillåtet att använda sådan information i större utsträckning än vad som var tillåtet vid den tidpunkt då informationen samlades in. De äldre bestämmelserna bör därför gälla för överskottsinformation som samlats in innan de nya reglerna trätt i kraft. I övrigt behövs inte några övergångsbestämmelser.

10 Konsekvenser

10.1 Konsekvenser för det brottsbekämpande arbetet och för enskilda

Regeringens bedömning: Förslagen innebär sammantaget en viss ökad risk för intrång i den personliga integriteten men bidrar samtidigt till att förbättra möjligheterna för de brottsbekämpande myndigheterna att förhindra, utreda och lagföra allvarlig brottslighet. Därmed innebär förslagen en ökad rättstrygghet för enskilda. Vissa förslag leder också till en förbättrad rättssäkerhet. Förslagen ger sammantaget uttryck för en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Några remissinstanser, bl.a. *Integritetsskyddsmyndigheten*, anser att effekterna av de samlade lagstiftningsåtgärderna på tvångsmedelsområdet inte är möjliga att överblicka eftersom det nyligen genomförts stora förändringar. Flera remissinstanser, bl.a. *Justitiekanslern* och *Institutet för mänskliga rättigheter*, menar att det bör göras en översyn där det ingår att bedöma de sammantagna konsekvenserna för enskildas fri- och rättigheter av de åtgärder som genomförts. *Brottsoffermyndigheten* framhåller att möjligheten att i större utsträckning utreda brott genom hemlig dataavläsning ökar sannolikheten för brottsoffer att få skadestånd eller brottsskadeersättning och på så sätt upprättelse. *ECPAT Sverige (ECPAT)* anser att förslaget om att permanenta lagstiftningen kan göra stor skillnad i arbetet med att upptäcka och förhindra sexualbrott mot barn, och att särskilt möjligheten att hämta in kameraövervakningsuppgifter från en förövares bostad är avgörande för brottsbekämpningen.

Skälen för regeringens bedömning

Konsekvenser för det brottsbekämpande arbetet

Förslaget om att lagen om hemlig dataavläsning ska permanentas innebär att de brottsbekämpande myndigheterna även fortsättningsvis kommer att ha ett viktigt verktyg i arbetet med att förhindra, utreda och lagföra allvarlig brottslighet. Det är en nödvändig anpassning till de senaste årens brotts-, teknik- och samhällsutveckling och en förutsättning för en fortsatt effektiv brottsbekämpning. Förslaget får konsekvenser för det brottsbekämpande arbetet både under en förundersökning och i underrättelseverksamhet.

Med tydligare regler som är bättre anpassade till hur hemlig dataavläsning verkställs i praktiken, t.ex. genom förslagen om justerad reglering av uppgiftstyper och av tillståndens utformning, förbättras möjligheterna att verkställa tillstånd till hemlig dataavläsning. Fler verkställda tillstånd innebär förbättrade utredningsmöjligheter med en ökad upptäcktsrisk och bättre förutsättningar att förhindra allvarlig brottslighet.

Möjligheten att använda hemlig dataavläsning i större utsträckning för att utreda vem som skäligen kan misstänkas för ett brott kan förväntas ge bättre förutsättningar att utreda brott och därmed bidra till att fler brott

klaras upp. Det gäller särskilt i utredningar där det är svårt att genom andra tvångsmedel utreda vem eller vilka som ligger bakom en i övrigt fullt synlig brottslighet. Som exempel på brottslighet där den föreslagna möjligheten kan ha stor betydelse kan nämnas terroristbrott, spionerі, narkotikahandel på internet, grova dataintrång och barnpornografibrott.

Användning av överskottsinformation från hemlig dataavläsning kan förväntas leda till att fler allvarliga brott kan förhindras, utredas och lagföras.

Konsekvenser för enskilda

Att använda hemlig dataavläsning innebär som utgångspunkt ett intrång i någon enskilds personliga integritet. Genom tvångsmedlet kan integritetskänsliga uppgifter hämtas in och enskildas personliga förhållanden kan övervakas och kartläggas. I dess natur ligger dessutom att det görs i hemlighet och utan samtycke.

Enskilda tillförsäkras skydd mot godtyckliga ingrepp i sitt privat- och familjeliv från statens sida genom bl.a. 2 kap. 6 § regeringsformen, artikel 8 i Europakonventionen och artikel 7 i EU:s rättighetsstadga. I 2 kap. 6 § regeringsformen föreskrivs att var och en gentemot det allmänna är skyddad mot undersökning av brev och andra förtroliga försändelser samt mot hemlig avlyssning eller upptagning av telefonsamtal eller andra förtroliga meddelanden. Utöver detta är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Paragrafens skydd för den personliga integriteten är inte absolut utan kan begränsas genom lag om det görs för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle, aldrig går utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den, inte sträcker sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar och inte görs enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 20 § första stycket 2 och 21 § regeringsformen).

I artikel 8.1 i Europakonventionen anges att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i dessa rättigheter får endast göras med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt bl.a. med hänsyn till statens säkerhet och den allmänna säkerheten, till förebyggande av oordning och brott eller till skydd för andra personers fri- och rättigheter (artikel 8.2).

Av artikel 7 i EU:s rättighetsstadga följer att var och en har rätt till respekt för sitt privatliv och familjeliv och sina kommunikationer. Medlemsstaterna ska följa stadgan när de tillämpar och genomför unionsrätten. Varje inskränkning i de fri- och rättigheter som erkänns i stadgan måste vara föreskriven i lag och förenlig med det väsentliga innehållet i fri- och rättigheterna. Inskränkningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och svarar mot ett allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter (artikel 52.1).

Vid åtgärder som begränsar skyddet i 2 kap. 6 § regeringsformen, art. 8.1 i Europakonventionen och artikel 7 i EU:s rättighetsstadga ska det göras en proportionalitetsbedömning där riskerna med en åtgärd vägs mot

dess fördelar. Det innebär noggranna avvägningar mellan å ena sidan behovet av åtgärden samt åtgärdens förväntade effektivitet och nytta och å andra sidan vilka integritetsintrång som åtgärden kan förväntas medföra. Inom ramen för den utvidgning av tillämpningsområdet för hemlig dataavläsning som har gjorts under de senaste åren har den begränsning av skyddet som utvidgningen medfört, bedömts proportionerlig och förenligt med såväl regeringsformen som Europakonventionen och EU:s rättighetsstadga (se prop. 2022/23:126 s. 194–197 och prop. 2023/24:117 s. 167–170).

Förslaget om att lagen om hemlig dataavläsning ska gälla utan begränsning i tid och förslaget om att utöka möjligheterna att hämta in uppgifter för att utreda vem som skäligen kan misstänkas för ett brott innebär en viss ökad risk för den personliga integriteten och en inskränkning i skyddet enligt bl.a. 2 kap. 6 § regeringsformen.

Europadomstolen har vid flera tillfällen uttalat att det måste vara förutsebart för den enskilde när tvångsmedel får användas. Det krävs att det finns klara och detaljerade regler som beskriver när myndigheterna får använda tvångsmedel i hemlighet mot en person (se t.ex. Europadomstolens dom den 2 augusti 1984 i målet Malone mot Förenade kungariket, nr 8691/79). Europadomstolen har genom åren också utvecklat vissa minimigarantier som bör finnas i nationell rätt för att undvika att enskilda utsätts för godtycklig maktutövning (Europadomstolens dom den 4 december 2015 i målet Roman Zakharov mot Ryssland, nr 47143/06, punkt 231).

Regleringen av hemlig dataavläsning finns i lag. Flera av de förslag som lämnas syftar till att göra regelverket tydligare och mer transparent. Det innebär att det även i fortsättningen kommer att vara förutsebart för den enskilde när och hur hemlig dataavläsning får användas. Regleringen uppfyller även i övrigt de minimigarantier som har utvecklats i Europadomstolens praxis.

När det gäller nödvändigheten av åtgärderna kan det konstateras att tillgång till hemlig dataavläsning är avgörande för de brottsbekämpande myndigheternas möjlighet att ta del av information, inte minst i krypterad form, som kan leda till att allvarlig brottslighet kan förhindras eller utredas och lagföras. Såväl fortsatt tillgång till hemlig dataavläsning som den utvidgning av möjligheten att använda tvångsmedlet för att identifiera en gärningsperson bedöms nödvändigt för att kunna förebygga brott. Av artikel 8 i Europakonventionen följer inte bara ett förbud mot godtyckliga ingrepp i privatlivet, utan även en positiv förpliktelse för staten att skydda enskilda mot ingrepp i t.ex. privatlivet från andra (Europadomstolens dom den 12 november 2013 i målet Söderman mot Sverige, nr 5786/08). Ett sådant skydd kan tillgodoses genom både lagstiftning och andra åtgärder, t.ex. genom att säkerställa att brottsbekämpningen fungerar på ett tillfredsställande sätt. Flera av de förslag som lämnas bedöms ge de brottsbekämpande myndigheterna bättre förutsättningar att förhindra, utreda och lagföra brottslighet. Det kan alltså antas att förslagen kommer att leda till att färre personer blir utsatta för brott och, i förlängningen, att fler brott mot enskilda kan klaras upp. En sådan utveckling kan också, som *Brottsoffermyndigheten* framhåller, leda till att fler brottsoffer får upprättelse. Förslagen förväntas alltså leda till en ökad rättstrygghet för enskilda. Hemlig dataavläsning omgärdas också av ett väl utbyggt system

med rättssäkerhetsgarantier som syftar till att begränsa integritetsintrånget och göra det möjligt att utöva en effektiv tillsyn. Dessutom bedöms flera av förslagen innebära en förstärkt rättssäkerhet för den enskilde. Det handlar bl.a. om tydligare regler för tillståndsbeslutens innehåll och för hur information från hemlig dataavläsning får användas. Kravet på dokumentation och bevarande av material stärker den enskildes möjlighet till efterhandskontroll och förbättrar förutsättningarna för Säkerhets- och integritetsskyddsnämndens tillsyn.

Några remissinstanser framför att effekterna av de samlade lagstiftningsåtgärderna på tvångsmedelsområdet inte är möjliga att överblicka eftersom det nyligen har genomförts stora förändringar. Flera remissinstanser menar att det bör göras en översyn där det ingår att bedöma de sammantagna konsekvenserna för enskildas fri- och rättigheter av de åtgärder som genomförts. Regeringen har förståelse för synpunkterna. Den allvarliga utvecklingen av brottsligheten innebär dock att de brottsbekämpande myndigheterna här och nu behöver goda förutsättningar att förhindra, utreda och lagföra allvarlig brottslighet. Även med beaktande av de lagändringar som nyligen genomförts för att utöka möjligheterna att använda hemliga tvångsmedel (se avsnitt 4.1 och 5) anser regeringen sammantaget att de nu aktuella förslagen innebär en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet. Det är alltså regeringens samlade bedömning att förslagen är proportionerliga i fråga om enskildas personliga integritet.

Konsekvenser för barn

Bestämmelserna om hemlig dataavläsning berör barn på så sätt att hemlig dataavläsning kan komma att riktas mot barn under 18 år. Barn ingår också i den krets av utomstående som kan komma att drabbas av åtgärden.

Sedan den 1 januari 2020 gäller barnkonventionen som lag i Sverige. All lagstiftning som rör barn ska utformas i överensstämmelse med barnkonventionens bestämmelser, se propositionen Inkorporering av FN:s konvention om barnets rättigheter (prop. 2017/18:186 s. 94). För svenskt vidkommande räknas enligt artikel 1 varje människa under 18 år som barn. Av artikel 3 följer att vid alla åtgärder som rör barn, vare sig de vidtas av offentliga eller privata sociala välfärdsinstitutioner, domstolar, administrativa myndigheter eller lagstiftande organ, ska i första hand beaktas vad som bedöms vara barnets bästa. Vid en bedömning av vad som är barnets bästa ingår att ta hänsyn till samtliga grundläggande principer och barnkonventionen i sin helhet. Genom artikel 16 fastslås vidare att inget barn får utsättas för godtyckliga ingripanden i bl.a. sitt privatliv. Ett barns privatliv skyddas även genom artikel 8 i Europakonventionen och artikel 7 i EU:s rättighetsstadga. Rätten till skydd för privatliv är dock inte absolut utan får inskränkas (artikel 8.2 i Europakonventionen, artikel 52.1 i EU:s rättighetsstadga).

Som anförs i avsnittet om konsekvenser för enskilda ovan gör regeringen bedömningen att förslagen sammantaget innebär en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet. Det finns ingen anledning att göra någon annan bedömning i fråga om straffmyndiga barn.

Det ska dock framhållas att det vid användning av hemlig dataavläsning mot barn kan finnas skäl att vara återhållsam. Vid varje beslut om hemlig dataavläsning som rör ett barn ska också barnets bästa beaktas. Det följer av artikel 3 i barnkonventionen. Inom ramen för den proportionalitetsbedömning som ska göras vid varje enskilt beslut om hemlig dataavläsning bör det också beaktas särskilt om en åtgärd riktar sig mot ett barn.

Genom artikel 34 i barnkonventionen har konventionsstaterna åtagit sig att skydda barn från alla former av sexuellt utnyttjande och sexuella övergrepp. En liknande förpliktelse kan även utläsas ur artikel 8 i Europakonventionen (Europadomstolens dom den 12 november 2013 i målet Söderman mot Sverige, nr 5786/08). Möjligheten att använda hemlig dataavläsning kan ha stor betydelse vid t.ex. utredningar om sexualbrott mot barn, särskilt i de fall brottsligheten begås på nätet eller annars med hjälp av elektronisk kommunikation. Förslaget att permanenta lagen om hemlig dataavläsning medför därför förbättrade möjligheter för de brottsbekämpande myndigheterna att upptäcka, förhindra och utreda sådan allvarlig brottslighet. Även förslaget om utökade möjligheter att använda hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för ett brott kommer att kunna få betydelse vid utredningen av brott mot barn. Som *ECPAT* framhåller kommer möjligheten att hämta in kameraövervakningsuppgifter i den situationen att kunna ha stor betydelse för det brottsbekämpande arbetet i fråga om internetrelaterade sexualbrott mot barn.

Övriga konsekvenser

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

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

10.2 Ekonomiska konsekvenser

Regeringens bedömning: Förslagen leder till ökade kostnader för Säkerhets- och integritetsskyddsnämnden. I enlighet med budgetpropositionen för 2025 tillförs Säkerhets- och integritetsskyddsnämnden medel fr.o.m. 2025 för att finansiera dessa kostnader. De kostnadsökningar som förslagen kan medföra i övrigt bedöms inte vara större än att de kan hanteras inom berörda myndigheters befintliga ekonomiska ramar.

Utredningens bedömning stämmer i huvudsak överens med regeringens. Utredningen bedömer att förslagen också leder till ökade kostnader för Tullverket och Säkerhetspolisen som inte kan hanteras inom befintliga anslag.

Remissinstanserna: Majoriteten av remissinstanserna instämmer i eller har inte några invändningar mot utredningens bedömning. *Kriminalvården*

påpekar att en ökad lagföring när det gäller allvarlig brottslighet kommer att innebära en ökad belastning för Kriminalvården. *Tullverket* menar att myndigheten behöver tillföras ytterligare medel för att inte behöva prioritera ner sin förmåga när det gäller hemlig dataavläsning eller prioritera om, så att andra delar av Tullverkets verksamhet får stå tillbaka. *Bahnhof* och *Riksdagens ombudsmän (JO)* betonar vikten av att Säkerhets- och integritetsskyddsnämnden har tillräckliga resurser för att kunna bedriva en effektiv tillsyn över användning av hemliga tvångsmedel. *Bahnhof* anser att *Säkerhets- och integritetsskyddsnämnden* bör få en betydande resursförstärkning så att de har möjlighet att granska minst tio procent av de hemliga dataavläsningar som görs. *Justitiekanslern* anför att en tänkbar konsekvens av att Säkerhets- och integritetsskyddsnämndens tillsynsuppdrag ökar är att nämnden anmäler fler ärenden till Justitiekanslern än vad som görs i dag. *Domarnämnden* framhåller att det kan innebära en ökad arbetsbörda för nämnden om behovet av fler offentliga ombud ökar med anledning av att fler ärenden prövas i domstol. *Domstolsverket* anser att förslagen måste ses i ett större sammanhang där utvecklingen av antalet ärenden i domstol av samtliga typer av hemliga tvångsmedel och preventiva tvångsmedel beaktas. *Helsingborgs tingsrätt* och *Göta hovrätt* framhåller att den ökade användningen av hemliga tvångsmedel och de förslag som nu lämnas medför ökad arbetsbelastning för domstolarna. Enligt *Göta hovrätt* behöver ytterligare medel tillföras Sveriges Domstolar eftersom hemliga tvångsmedel tar alltmer av domstolarnas resurser i anspråk och för att kunna utveckla ett verksamhetsstöd för ärendetypen.

Skälen för regeringens bedömning

Konsekvenser för Polismyndigheten, Säkerhetspolisen, Tullverket, Åklagarmyndigheten och Ekobrottsmyndigheten

Att använda hemlig dataavläsning är resurskrävande för de brottsbekämpande myndigheterna. Förutom att tillståndsförfarandet tar resurser i anspråk kräver verkställigheten ofta omfattande förberedelser. Dessutom ska myndigheterna hantera och bearbeta all den information som samlas in. Hemlig dataavläsning har hittills använts i endast ett begränsat antal fall, både i absoluta tal och jämfört med andra hemliga tvångsmedel. Genom förslaget att göra lagstiftningen permanent kan de brottsbekämpande myndigheterna fortsätta använda hemlig dataavläsning. Mot bakgrund av att antalet redovisade tillstånd till hemlig dataavläsning har ökat varje år sedan lagens ikraftträdande kan en fortsatt ökning av antalet tillstånd de närmsta åren förutspås. Vissa förslag som lämnas kan dessutom förväntas få till följd att fler tillstånd kan verkställas. Det handlar t.ex. om förslaget om förändrade uppgiftstyper och förslagen om tydligare regler för villkor.

Utredningen bedömer att förslagen kommer att leda till ett ökat resursbehov för Säkerhetspolisen och Tullverket och att dessa myndigheter därför bör tillföras ytterligare medel. De ökade kostnaderna avser huvudsakligen teknikkostnader och personalkostnader för att bibehålla och utveckla egen nödvändig teknisk förmåga på området.

Även för Polismyndigheten kan förslagen innebära ett ökat behov av teknisk utrustning och personal. För Åklagarmyndigheten och Ekobrotts-

myndigheten kan förslaget om utökade möjligheter att använda hemlig dataavläsning för att identifiera en skäligen misstänkt och förslaget om ökade möjligheter att använda överskottsinformation komma att innebära fler ärenden för myndigheterna. Enligt utredningens bedömning bör eventuella kostnadsökningar dock inte vara större än att de ryms inom Polismyndighetens, Åklagarmyndighetens och Ekobrottsmyndighetens befintliga anslagsramar.

Att med kraft trycka tillbaka den organiserade brottsligheten är en av regeringens mest prioriterade uppgifter. Regeringen har därför i budgetpropositionerna för 2024 och 2025 gått fram med stora satsningar på de brottsbekämpande myndigheterna för att de ska kunna utföra sina uppgifter. Med anledning av de lagändringar som trädde i kraft den 1 oktober 2023 har regeringen dessutom tillskjutit resurser till Ekobrottsmyndigheten, Polismyndigheten och Tullverket för att bl.a. hantera den ärendeökning som beräknas uppstå med anledning av de utökade möjligheterna att använda hemliga tvångsmedel. Mot den bakgrunden anser regeringen att eventuella kostnadsökningar på grund av de förslag som nu lämnas inte kommer att vara större än att de kan hanteras inom Polismyndighetens, Säkerhetspolisens, Tullverkets, Åklagarmyndighetens och Ekobrottsmyndighetens befintliga anslagsramar.

Konsekvenser för Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden utövar tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. Förslagen, särskilt förslaget om en utökad möjlighet att använda hemlig dataavläsning i syfte att utreda vem som kan misstänkas för brott, innebär att omfattningen av nämndens tillsynsuppdrag kommer att öka. Eftersom hemlig dataavläsning innebär en ökad risk för integritetsintrång jämfört med övriga hemliga tvångsmedel är det, som *JO* och *Bahnhof* framhåller, nödvändigt att denna risk vägs upp av en effektiv tillsyn. För att det ska vara möjligt behöver nämnden tillföras medel. I budgetpropositionen för 2025 föreslår regeringen att Säkerhets- och integritetsskyddsnämnden ska tillföras medel fr.o.m. 2025 med anledning av förslagen.

Konsekvenser för de allmänna domstolarna, Domarnämnden, Justitiekanslern och anslaget Rättsliga biträden m.m.

Ärenden om hemlig dataavläsning ska prövas av allmän domstol och ett offentligt ombud ska utses i alla ärenden. En möjlig följd av de förslag som nu lämnas kan vara att det kan komma att bli fråga om något fler ärenden om hemlig dataavläsning i allmän domstol och därmed också att offentliga ombud kan komma att behövas i fler ärenden än i dag. Som *Justitiekanslern* anför skulle det förändrade regelverket kunna innebära att något fler ärenden anmäls till Justitiekanslern än vad som görs i dag. Förslagen bedöms dock inte påverka resursbehovet för Sveriges Domstolar, Domarnämnden eller Justitiekanslern. i större omfattning än att ökningen bedöms rymmas inom befintliga anslagsramar. Eventuella kostnadsökningar för anslaget Rättsliga biträden m.m. bedöms inte heller vara större än att de ryms inom ramen för befintliga anslagsramar.

Konsekvenser för Skatteverket, Finansinspektionen, Kriminalvården och företag

Skatteverket biträder Ekobrottsmyndigheten i många utredningar om allvarlig brottslighet. Det förekommer även att Finansinspektionen biträder Ekobrottsmyndigheten i sådana utredningar. Förslagen kan komma att innebära vissa kostnadsökningar för Skatteverket och Finansinspektionen.

Som *Kriminalvården* framhåller bedöms förslagen leda till en ökad lagföring när det gäller allvarlig brottslighet, vilket kan komma att innebära en ökad belastning för Kriminalvården. De eventuella ökade kostnader som förslagen kan komma att innebära för Skatteverket, Finansinspektionen och Kriminalvården bedöms emellertid rymmas inom befintliga anslagsramar. För de företag som medverkar vid verkställighet bedöms förslagen inte medföra några ökade kostnader.

11 Författningskommentar

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

4 kap.

28 e § Tekniskt bistånd med hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2020:62) om hemlig dataavläsning i form av omedelbar överföring av meddelanden eller uppgifter om meddelanden får lämnas i Sverige enligt de förutsättningar som gäller enligt 25 b § andra, tredje och femte styckena. Vid hemlig dataavläsning i en annan stat än den som ansökt om tekniskt bistånd ska ett tillstånd enligt 28 f § ha lämnats.

Ansökan ska prövas av åklagare. För beslutet om tekniskt bistånd tillämpas 1 §, 18 § första stycket 1 *och 2* och *andra* stycket och 20 § andra stycket lagen om hemlig dataavläsning.

I paragrafen regleras frågan om tekniskt bistånd genom omedelbar överföring av meddelanden eller uppgifter om meddelanden när hemlig dataavläsning avser inhämtning av kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter. Övervägandena finns i avsnitt 8.2.

I *andra stycket* görs följdändringar med anledning av de redaktionella ändringar som görs i 18 § lagen (2020:62) om hemlig dataavläsning, se författningskommentaren till den paragrafen.

11.2 Förslaget till lag om dels fortsatt giltighet av lagen (2020:62) om hemlig dataavläsning, dels ändring i samma lag

1 § Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling *och åtkomliga i ett avläsningsbart informationssystem, hämtas in* i hemlighet med ett tekniskt hjälpmedel.

I lagen avses med

avläsningsbart informationssystem: en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst,

kommunikationsavlyssningsuppgifter: uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,

kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,

platsuppgifter: uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,

kameraövervakningsuppgifter: uppgifter som framkommer genom optisk personövervakning,

rumsavlyssningsuppgifter: uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.

Paragrafen innehåller en definition av hemlig dataavläsning och definitioner av andra begrepp i lagen. Övervägandena finns i avsnitt 6.1.

I *första stycket* ändras definitionen av hemlig dataavläsning genom att det i stället för ”läses av eller tas upp” anges att uppgifter ”hämtas in”. Inhämtningen kan genomföras på olika sätt, t.ex. genom avlyssning, upptagning eller övervakning med hjälp av ett tekniskt hjälpmedel. I stycket förtydligas också att inhämtningen kan avse alla de uppgifter som är åtkomliga i det avläsningsbara informationssystemet. Ingen ändring i sak är avsedd.

Övriga ändringar är språkliga.

Uppgiftstyper* som får *hämtas in

2 § *Ett tillstånd* till hemlig dataavläsning får *gälla*

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter, *eller*
6. *andra* uppgifter som *är åtkomliga* i ett avläsningsbart informationssystem.

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

Paragrafen anger vilka uppgiftstyper som får hämtas in med hemlig dataavläsning och att meddelanden i vissa fall får hindras från att nå fram. Övervägandena finns i avsnitt 6.2.

I *första stycket* görs en justering av punkten 6 på så sätt att det inte längre anges att uppgifter ska vara lagrade i ett avläsningsbart informationssystem, utan i stället att de ska vara åtkomliga i ett sådant system. Med uppgifter som är åtkomliga avses all information som under verkställighetstiden finns tillgänglig i det avläsningsbara informationssystemet. Ändringen innebär att även uppgifter som visar hur ett avläsningsbart informationssystem används, som i hittillsvarande lydelse regleras i punkten 7, nu omfattas av punkten 6. Punkten 7 tas därför bort. Punkten 6 är sekundär till övriga punkter, dvs. den omfattar bara sådana uppgifter som inte omfattas av punkterna 1–5.

Övriga ändringar är språkliga.

4 a § Ett tillstånd enligt 4 § får endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av den misstänkte.

Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta.

Ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Trots tredje stycket får ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter avse den skäligen misstänkte i stället för en viss plats, om det finns särskilda skäl för det. Den hemliga dataavläsningen får då endast användas på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Paragrafen innehåller bestämmelser om hemlig dataavläsning som inte gäller rumsavlyssningsuppgifter när det finns en skäligen misstänkt. Övervägandena finns i avsnitt 8.2.

Ändringen i *andra stycket* är en anpassning till att det inte längre krävs att det i ett tillstånd till hemlig dataavläsning anges vilken tid som tillståndet avser, se 18 §. Ändringen innebär att det av lagtexten inte längre följer något krav på att den misstänktes kontakt med informationssystemet ska ha skett under en viss tid. Ett sådant krav kan dock även fortsättningsvis ställas upp i villkor om det i ett enskilt fall behövs för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, se 18 § tredje stycket.

5 § Ett tillstånd till hemlig dataavläsning som *inte* gäller *rumsavlyssningsuppgifter* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.

Ett tillstånd enligt första stycket får endast avse ett avläsningsbart informationssystem som

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda, eller

2. det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakt.

Ett tillstånd enligt andra stycket 2 får inte gälla kameraövervakningsuppgifter.

Ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter får verkställas på en plats som är någons stadigvarande bostad, endast om det finns synnerlig anledning att anta att den person som åtgärden riktas mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser.

Paragrafen, som i hittillsvarande lydelse betecknas 4 b §, innehåller bestämmelser om användning av hemlig dataavläsning, som inte gäller rumsavlyssningsuppgifter, i syfte att utreda vem som skäligen kan misstänkas för brott. Övervägandena finns i avsnitt 7.

Enligt *första stycket* får hemlig dataavläsning som inte gäller rumsavlyssningsuppgifter, utöver i de fall som avses i 4 §, även användas för att utreda vem som skäligen kan misstänkas för brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken. I hittillsvarande lydelse gäller paragrafen endast kommunikationsavlyssningsuppgifter. Ändringen innebär alltså att ett tillstånd enligt paragrafen kan avse de uppgiftstyper som anges i 2 § punkterna 1–4 och 6. Kommunikationsövervaknings- och platsuppgifter kan enligt 5 a § också hämtas in för att utreda vem som skäligen kan misstänkas för ett eller flera brott.

Ändringen i *andra stycket* första punkten är en anpassning till att det inte längre krävs att det i ett tillstånd till hemlig dataavläsning anges vilken tid som tillståndet avser, se 18 §. Ändringen innebär att det av lagtexten inte längre följer något krav på att kontakten med det informationssystem som den hemliga dataavläsningen avser ska ha skett under en viss tid.

Bestämmelsen *i tredje stycket*, som är nytt, innebär att ett tillstånd som gäller kameraövervakningsuppgifter inte får avse ett avläsningsbart informationssystem som gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta. Om tillståndet gäller kameraövervakningsuppgifter får det alltså endast avse ett informationssystem som det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda.

I *fjärde stycket*, som är nytt, anges att ett tillstånd för att hämta in kameraövervakningsuppgifter endast under vissa omständigheter får verkställas på en plats som är någons stadigvarande bostad. Det är ett krav som ska beaktas vid verkställigheten och inte vid tillståndsprövningen. Som utgångspunkt får ett tillstånd som gäller kameraövervakningsuppgifter alltså inte verkställas på en sådan plats. För att det ska få ske krävs att det finns synnerlig anledning att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser. Kravet på att det ska finnas synnerlig anledning att anta är detsamma som i andra stycket. Det innebär att det på grund av tillförlitliga uppgifter ska vara så gott som säkert att den person som åtgärden riktar sig mot använder informationssystemet och befinner sig i direkt anslutning till det. Begreppet stadigvarande bostad förekommer i bl.a. 4 a och 6 §§ och har samma innebörd som i de paragraferna.

Övriga ändringar är språkliga.

8 § Ett tillstånd till hemlig dataavläsning enligt 7 § får endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av den person som åtgärden riktas mot.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den person som åtgärden riktas mot har kontaktat eller kommer att kontakta.

Paragrafen innehåller bestämmelser om krav på koppling mellan ett avläsningsbart informationssystem och den enskilde vid tillstånd som avses i 7 § (preventivlagsfallen). Övervägandena finns i avsnitt 8.2.

Ändringen i paragrafens *andra stycke* är en anpassning till att det inte längre krävs att det i ett tillstånd till hemlig dataavläsning anges vilken tid som tillståndet avser, se 18 §. Ändringen innebär att det av lagtexten inte längre följer något krav på att utlänningens kontakt med informationssystemet ska ha skett under en viss tid.

9 § Ett tillstånd till hemlig dataavläsning får beviljas för att *hämta in* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

1. ett utvisningsbeslut enligt 2 kap. 1 § lagen (2022:700) om särskild kontroll av vissa utlänningar, eller
2. ett avvisnings- eller utvisningsbeslut enligt 8 kap. eller 8 a kap. utlänningslagen (2005:716) om det finns sådana omständigheter i fråga om utlänningen som avses i 2 kap. 1 § lagen om särskild kontroll av vissa utlänningar.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får också beviljas för att *hämta in* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar ska tillämpas i fråga om utlänningen gäller också för ett beslut i fråga om hemlig dataavläsning.

Ett tillstånd får beviljas endast om det finns synnerliga skäl och det är av betydelse för att

1. klarlägga om utlänningen tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen (2022:666) eller om det finns en risk för att utlänningen kan komma att engagera sig i en sådan organisation eller grupp,
2. klarlägga om det finns risk för att utlänningen själv planlägger eller förbereder brott som avses i 1,
3. klarlägga om det finns risk för att utlänningen själv eller tillsammans med andra medverkar i eller på annat sätt främjar ett allvarligt brott som rör Sveriges säkerhet, eller
4. kunna lokalisera en utlänning som inte har fullgjort sin anmälningsskyldighet enligt lagen (2022:700) om särskild kontroll av vissa utlänningar.

Ett tillstånd får inte *gälla* rumsavlyssningsuppgifter. Ett tillstånd enligt fjärde stycket 4 får endast *gälla* kommunikationsövervaknings- och platsuppgifter.

I paragrafen regleras vad som gäller för tillståndsgivning till hemlig dataavläsning när det finns förhållanden som kan ligga till grund för beslut

om hemliga tvångsmedel enligt lagen (2022:700) om särskild kontroll av vissa utlänningar. Övervägandena finns i avsnitt 6.1 och 8.2.

I *första* och *andra styckena* ersätts ”läsa av eller ta upp” med ”hämta in” som en följd av motsvarande ändring i 1 §, se författningskommentaren till den paragrafen. Andra stycket ändras även på så sätt att kravet på att den misstänktes kontakt med informationssystemet ska ha skett under en viss tid utgår. Ändringen är en anpassning till att det inte längre krävs att det i ett tillstånd till hemlig dataavläsning anges vilken tid som tillståndet avser, se 18 §.

Övriga ändringar är språkliga.

14 § Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen.

I samband med ansökan *ska åklagaren eller Säkerhetspolisen* föreslå sådana villkor som avses i 18 § *tredje* stycket*, om villkor inte framstår som obehövligt. Sådana villkor ska dock alltid föreslås om en ansökan som gäller kameraövervaknings- eller rumsavlyssningsuppgifter avser en viss person i stället för en viss plats.*

I paragrafen finns regler om ansökan om hemlig dataavläsning. Övervägandena finns i avsnitt 8.3.

Enligt *andra stycket* ska åklagaren eller Säkerhetspolisen i samband med en ansökan föreslå vilka villkor som tillståndet enligt 18 § tredje stycket ska förenas med. Ändringen innebär att skyldigheten gäller vid alla tillståndsansökningar om villkor inte framstår som obehövligt och omfattar även Säkerhetspolisen när myndigheten är sökande. Om åklagaren eller Säkerhetspolisen bedömer att det är obehövligt med villkor bör det motiveras i samband med ansökan. För exempel på situationer där det kan framstå som obehövligt med villkor, se författningskommentaren till 18 §. Om en ansökan som gäller kameraövervaknings- eller rumsavlyssningsuppgifter avser en viss person i stället för en viss plats ska villkor, liksom tidigare, alltid föreslås.

17 § Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att *hämta in* rättens tillstånd i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren snarast möjligt skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *hämtats in* inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

I paragrafen finns bestämmelser om möjligheten för åklagaren att bevilja interimistiska beslut om hemlig dataavläsning och om rättens prövning av sådana beslut. Övervägandena finns i avsnitt 6.1.

I paragrafens *tredje stycke* ersätts ”lästs av eller tagit upp” med ”hämtats in” som en följd av motsvarande ändring i 1 §, se författningskommentaren till den paragrafen. I övrigt görs en språklig ändring.

18 § I ett tillstånd till hemlig dataavläsning ska följande anges:

1. vilket avläsningsbart informationssystem tillståndet avser,

2. vilken *uppgiftstyp* enligt 2 § första stycket som får *hämtas in*, *och*

3. vem som är skäligen misstänkt för brottet eller brotten, *om sådan uppgift finns*, eller vem en åtgärd enligt 7 § riktas mot.

I tillståndet *ska det även anges under vilken tid som verkställighet får ske. Tiden för verkställighet* får inte bestämmas längre än nödvändigt *och* får inte överstiga en månad från dagen för beslutet.

I tillståndet ska det även anges vilka uppgifter som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Villkor behöver inte anges om det framstår som obehövligt. Om ett tillstånd som gäller kameraövervaknings- eller rumsavlyssningsuppgifter avser en viss person i stället för en viss plats ska dock villkor alltid anges.

Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska även det anges i beslutet.

Paragrafen reglerar vad ett beslut om tillstånd till hemlig dataavläsning ska innehålla. Övervägandena finns i avsnitt 8.3.

I *första stycket* anges vad som ska framgå av ett tillstånd till hemlig dataavläsning. Punkterna motsvarar hittillsvarande 2, 3 och 5 i samma stycke med vissa justeringar. Kravet i den hittillsvarande första punkten på att ange vilken tid tillståndet avser utgår. Bestämmelsen i hittillsvarande andra punkten finns därför nu i första punkten. I andra (hittillsvarande tredje) punkten ersätts ”läsas av eller tas upp” med ”hämtas in” som en följd av ändringen i 1 §. I tredje (hittillsvarande femte) punkten ändras kravet på att i vissa fall ange vem som är skäligen misstänkt till att omfatta alla tillstånd, förutsatt att en sådan uppgift finns. Om det är fråga om en åtgärd enligt 7 § (preventivlagsfallen) ska det i stället anges vem åtgärden riktas mot.

Enligt *andra stycket*, som delvis motsvarar hittillsvarande tredje stycket, ska det i ett tillstånd anges under vilken tid som verkställighet får ske. Tiden för verkställighet får inte bestämmas längre än vad som är nödvändigt i det enskilda fallet och får inte vara längre än en månad från dagen för beslutet. Om det finns behov av hemlig dataavläsning under en längre period än en månad krävs ett nytt beslut. Regleringen hindrar inte att verkställighet äger rum flera gånger under verkställighetsperioden. Under verkställighetsperioden får alla uppgifter som omfattas av tillståndet och som är åtkomliga i informationssystemet hämtas in. Det följer alltså inte någon begränsning av lagtexten för hur gamla uppgifter som får inhämtas. En sådan begränsning bör dock som utgångspunkt ställas upp i de villkor som tillståndet förenas med.

Av *tredje stycket*, som är nytt, framgår att det i ett tillstånd ska anges vilka uppgifter som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan. Bestämmelsen

motsvarar det som i hittillsvarande lydelse anges i första stycket punkten 4, med tilläggen att villkoren också ska avse vilka uppgifter som inte får granskas och att villkor inte behöver anges om det framstår som obehövligt. Ett villkor om vilka uppgifter som inte får granskas innebär en begränsning av vilka inhämtade uppgifter som de behöriga personerna får gå igenom efter inhämtning och den initiala bearbetningen. Att det i villkoren ska anges vilka uppgifter som inte får granskas hindrar inte att villkoren i stället anger vilka uppgifter som faktiskt får granskas. Avgörande är att villkoren ur ett integritets- och rättssäkerhetsperspektiv är tydligt utformat. Om det är möjligt och ändamålsenligt bör villkoren ta sikte på tidsmässiga avgränsningar. Det kan t.ex. göras genom att det anges att endast uppgifter från ett visst datum eller före eller efter ett visst datum får granskas. En annan begränsning kan vara att bara kommunikation med en viss person får granskas. Ett villkor kan också ange att kommunikation från användarkonton som tillhör någon annan person, t.ex. en familjemedlem till den person som åtgärden mot, inte får granskas.

Med ”övriga villkor” avses andra villkor som kan gagna skyddet för den personliga integriteten men som inte tar sikte på själva granskningen. Om det är möjligt och ändamålsenligt bör sådana villkor ta sikte på inhämtningen. I de fall som det går att göra en åtskillnad mellan lagrade uppgifter och realtidsuppgifter redan i inhämtningsfasen bör detta göras. Om åtgärden exempelvis endast avser ett visst samtal eller möte kan behovet av inhämtning vara begränsat till realtidsuppgifter. I en sådan situation kan ett villkor begränsa inhämtningen till att avse uppgifter som tillkommer under verkställighetsperioden, dvs. utesluta inhämtning av lagrade uppgifter.

Om det framstår som obehövligt med villkor krävs inte att tillståndet förenas med villkor. Det kan exempelvis handla om situationer när myndigheterna på förhand känner till att informationssystemet endast används i kriminellt syfte. Så kan vara fallet när åtgärden riktas mot vissa chattkonton eller telefoner som enbart används för kommunikation mellan kriminella. I vissa fall kan den omständigheten att informationssystemet endast har använts under en begränsad tid göra att villkor framstår som obehövligt. Om det finns anledning att tro att villkor kan vara av betydelse bör sådana anges. En bedömning måste alltid göras i det enskilda fallet.

Av *fjärde stycket* framgår att det ska anges om ett tillstånd är förenat med ett tillträdestillstånd. I hittillsvarande lydelse framgår det av andra stycket.

Det som anges om tillstånd som gäller kameraövervaknings- eller rumsavlyssningsuppgifter i hittillsvarande andra stycket förs över till den nya 18 a §.

Övriga ändringar är språkliga.

18 a § *I ett tillstånd som gäller kameraövervaknings- eller rumsavlyssningsuppgifter ska det, förutom de uppgifter som framgår av 18 §, anges vilken plats tillståndet avser. Om tillståndet avser en viss person i stället för en viss plats ska det anges i beslutet.*

I paragrafen, som är ny, anges särskilda krav på vad som ska framgå av ett tillstånd som gäller kameraövervaknings- eller rumsavlyssningsuppgifter. Övervägandena finns i avsnitt 8.3.

Paragrafen motsvarar hittillsvarande 18 § andra stycket, förutom bestämmelsen om att det ska anges om beslutet är förenat med ett tillträdestillstånd, vilket i stället anges i 18 § fjärde stycket.

23 § *Vid verkställighet av* hemlig dataavläsning ska *tekniken och tillvägagångssättet* anpassas efter *tillståndet*.

Om uppgifter av någon annan uppgiftstyp än de som anges i tillståndet har hämtats in ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. Upptagningar och uppteckningar av uppgifter som inte får hämtas in eller granskas enligt villkor i tillståndet ska förstöras i de delar de innehåller sådana uppgifter så snart det står klart att uppgifterna har hämtats in.

Uppgifter som anges i *andra* stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.

I paragrafen finns bestämmelser om verkställighet av hemlig dataavläsning. Övervägandena finns i avsnitt 8.4.

I *första stycket* tas det hittillsvarande kravet på att tekniken inte får göra det möjligt att läsa av eller ta upp någon annan uppgiftstyp än vad som anges i tillståndet bort. I stället regleras att såväl tekniken som tillvägagångssättet ska anpassas efter tillståndet vid verkställigheten. Det innebär att verkställigheten av hemlig dataavläsning ska ske inom de ramar som satts i det enskilda tillståndet. Tillvägagångssättet kan anpassas bl.a. genom särskilda instruktioner eller riktlinjer om arbetssätt. Det är den verkställande myndigheten som ansvarar för att upprätta sådana instruktioner och riktlinjer till den särskilt utsedda personal som ska verkställa den hemliga dataavläsningen.

Av *andra stycket* framgår att uppgifter av någon annan uppgiftstyp än som anges i tillståndet utgör s.k. otillåten tilläggsinformation. Bestämmelsen ändras med anledning av att förbudet mot att tekniken gör det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet tas bort i första stycket. I andra meningen görs ett tillägg av innebörden att uppgifter som har hämtats in eller granskats i strid med villkor enligt 18 § tredje stycket ska förstöras. Så snart det står klart att sådana uppgifter har hämtats in eller granskats ska upptagningarna och uppteckningarna förstöras i de delar de innehåller sådana uppgifter. Det kan t.ex. handla om ett villkor om att endast meddelanden som har skickats eller tagits emot efter en viss tidpunkt får hämtas in. Om den verkställande myndigheten, trots villkoret, har hämtat in meddelanden som har skickats eller tagits emot före angiven tidpunkt, utgör dessa meddelanden otillåten tilläggsinformation och ska alltså förstöras. Att de otillåtna uppgifterna ska förstöras så snart det står klart att sådana uppgifter har hämtats in innebär i praktiken ett krav på förstöring så snart sådana uppgifter påträffas. I regel görs det direkt efter att de har sorterats och filtrerats bort i en initial bearbetningsfas. I vissa fall påträffas uppgifterna emellertid först vid granskningen och kan först då förstöras. Om myndigheten aldrig går igenom de otillåtna uppgifterna kommer de inte att identifieras. I dessa fall kommer de otillåtna uppgifterna att förstöras i enlighet med reglerna om förstörande som framgår av 28–31 §§ och där angivna hänvisningar. Till skillnad från vad som gäller för inhämtning av uppgifter av någon annan uppgiftstyp än

som följer av tillståndet ska Säkerhets- och integritetsskyddsnämnden inte underrättas särskilt vid inhämtning av uppgifter som inte får hämtas in eller granskas enligt villkor i tillståndet.

Tredje stycket motsvarar hittillsvarande andra stycket.

Förbud att *hämta in* vissa uppgifter

27 § Hemlig dataavläsning enligt 2 § första stycket 6 får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.

Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram.

Om det under *eller efter* verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *granskningen av dessa uppgifter* omedelbart avbrytas. *Upptagningar* och uppteckningar *ska* omedelbart förstöras i de delar som de omfattas av förbudet.

I paragrafen regleras förbud mot att i vissa fall hämta in vissa uppgifter. Övervägandena finns i avsnitt 8.4.

I *första stycket* tas hänvisningen till 2 § första stycket 7 bort som en följd av ändringen i den paragrafen som innebär att punkten 6 även omfattar uppgifter enligt hittillsvarande punkten 7.

I *tredje stycket* görs ett tillägg om att även uppgifter som kommer fram efter verkställighet ska leda till att den hemliga dataavläsningen avbryts om de omfattas av första eller andra stycket. Vidare ersätts begreppet ”verkställigheten” av ”granskningen av dessa uppgifter”. Om det kommer fram uppgifter som omfattas av de s.k. beslags- och avlyssningsförbuden i första och andra styckena ska granskningen av dessa uppgifter omedelbart avbrytas.

28 § När hemlig dataavläsning används eller har använts under en förundersökning ska 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden.

För underrättelse till en enskild vid hemlig dataavläsning under förundersökning gäller 27 kap. 31–33 §§ rättegångsbalken. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

I paragrafen anges vad som gäller bl.a. beträffande hur överskottsinformation får användas vid hemlig dataavläsning under en förundersökning. Övervägandena finns i avsnitt 8.5 och 8.6.

Genom ändringen i *första stycket* tas hänvisningen till rättegångsbalkens bestämmelser i dess lydelser före den 1 oktober 2023 bort. Ändringen innebär att rättegångsbalkens regler gäller för användning av överskottsinformation samt bevarande och förstöring av uppteckningar och

upptagningar från hemlig dataavläsning under förundersökning (se prop. 2022/23:126 s. 221 och 222).

29 § När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12–*14* §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

I paragrafen anges vad som ska gälla bl.a. beträffande hur överskottsinformation får användas vid hemlig dataavläsning i preventivlagsfallen. Övervägandena finns i avsnitt 8.5 och 8.6.

Genom ändringen i *första stycket* tas hänvisningen till preventivlagens bestämmelser i dess lydelser före den 1 oktober 2023 bort. Ändringen innebär att preventivlagens regler gäller för användning av överskottsinformation samt bevarande och förstöring av uppteckningar och upptagningar från hemlig dataavläsning i preventivlagsfallen (se prop. 2022/23:126 s. 232 och 233 samt prop. 2023/24:117 s. 194 och 195).

31 § När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och *7* §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.

I paragrafen anges vad som ska gälla för bl.a. överskottsinformation när hemlig dataavläsning används i inhämtningslagsfallen. Övervägandena finns i avsnitt 8.5 och 8.6.

I paragrafen tas hänvisningen till 6 och 8 §§ inhämtningslagen i dess lydelser före den 1 september 2024 bort. Vidare byts hänvisningen till nuvarande 8 § inhämtningslagen ut till 7 § samma lag, eftersom motsvarande ändring har gjorts i den lagen (se lagen [2024:564] om ändring i lagen [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet). Ändringen innebär att de nya regler om användning av överskottsinformation samt granskning, bevarande och förstöring som gäller enligt inhämtningslagen gäller även för hemlig dataavläsning (se prop. 2023/24:117 s. 204 och 205). Det hittillsvarande *andra stycket* utgår som en följd av ändringen.

Dokumentation

34 § *Beslut och åtgärder som rör hemlig dataavläsning ska dokumenteras.*

Paragrafen, som är ny, innehåller en dokumentationsskyldighet. Övervägandena finns i avsnitt 8.7.

Av paragrafen framgår att det finns en skyldighet att dokumentera beslut och åtgärder som rör hemlig dataavläsning. Bestämmelsen motsvarar 27 kap. 35 § rättegångsbalken, 19 § preventivlagen och 8 § inhämtningslagen. Uppgifterna ska dokumenteras på ett sådant sätt att det är möjligt att på ett överskådligt sätt följa beslut och andra åtgärder avseende tvångsmedelsanvändningen. Exempel på uppgifter som bör dokumenteras är uppgifter om tillståndet, såsom när det beviljats och om det har ändrats eller upphävts. Även datum och tidpunkt för verkställigheten samt vilken adress, kommunikationsutrustning eller plats som verkställigheten avsett eller skett på bör dokumenteras. Om det funnits tillträdestillstånd eller samtycke från innehavaren av en plats som omfattats av verkställigheten bör det också dokumenteras. Dokumentationsskyldigheten omfattar även frågor om förstöring av upptagningar och uppteckningar, liksom om förbudsbestämmelserna i 23 eller 27 §§ har aktualiserats. Även en uppgift som har betydelse för förstöringstidpunkten bör dokumenteras, t.ex. en uppgift om när förundersökningen avslutades. Därutöver bör åtgärder som gäller användning av överskottsinformation och uppgift om en underrättelse till en enskild dokumenteras, detta gäller särskilt om underrättelsen lämnats muntligen, exempelvis vid ett förhör (jfr prop. 2022/23:126 s. 225).

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 april 2025.

2. Äldre föreskrifter gäller fortfarande för tillstånd som har beviljats före ikraftträdandet.

3. För uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet gäller 28, 29 och 31 §§ i den äldre lydelsen.

Övervägandena finns i avsnitt 9.

Enligt *första punkten* träder lagen i kraft den 1 april 2025.

I *andra punkten* anges att äldre föreskrifter fortfarande gäller för tillstånd som har beviljats före ikraftträdandet. Bestämmelsen träffar sådana tillstånd till hemlig dataavläsning som har beslutats före ikraftträdandet, men där tiden för tillståndet ännu inte har löpt ut när lagen träder i kraft. Det innebär bl.a. att de hittillsvarande reglerna om avbrytande av verkställighet ska tillämpas om det kommer fram uppgifter som omfattas av beslags- eller avlyssningsförbuden.

I *tredje punkten* anges att 28, 29 och 31 §§ gäller i den äldre lydelsen för uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet. Det innebär bl.a. att det inte är tillåtet att använda överskottsinformation i större utsträckning än vad som var tillåtet vid den tidpunkt då informationen samlades in.

11.3 Förslaget till lag om ändring i lagen (2020:62) om hemlig dataavläsning

7 § Ett tillstånd till hemlig dataavläsning som inte gäller rumsavlyssningsuppgifter får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för

1. att en person kommer att utöva brottslig verksamhet som innefattar brott som anges i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, eller
2. att brottslig verksamhet som innefattar brott som anges i 1 § den lagen kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Ett tillstånd enligt första stycket får beviljas endast om åtgärden är av synnerlig vikt för att förhindra den brottsliga verksamheten.

I paragrafen finns bestämmelser om vad som gäller för tillstånd till hemlig dataavläsning vid sådana förhållanden som kan ligga till grund för tillstånd till tvångsmedelsanvändning enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Övervägandena finns i avsnitt 5.

I *första stycket* ändras hänvisningen till vilken brottslig verksamhet som omfattas av bestämmelsen. Ändringen görs med anledning av att 1 a § preventivlagen endast gäller under en viss tid (se lagen [2024:562] om ändring i lagen [2007:979] om åtgärder för att förhindra vissa särskilt allvarliga brott). Med anledning av att möjligheten att bevilja ett tillstånd till hemlig dataavläsning som avser rumsavlyssningsuppgifter endast ska gälla under en viss tid tas regleringen om det tvångsmedlet bort i *andra stycket*. I övrigt görs en redaktionell ändring.

8 a § Ett tillstånd till hemlig dataavläsning enligt 7 § som gäller kameraövervakningsuppgifter får endast avse en plats där den person som åtgärden riktas mot kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Paragrafen innehåller bestämmelser om vilken plats som ett tillstånd till hemlig dataavläsning som gäller kameraövervakningsuppgifter enligt 7 § får avse (preventivlagsfallen). Övervägandena finns i avsnitt 5.

Med anledning av att möjligheten att i preventivlagsfallen knyta ett tillstånd som gäller kameraövervakningsuppgifter till en person i stället för en plats endast ska gälla under viss tid tas *andra stycket* bort. Det innebär att ett sådant tillstånd endast kan avse en plats.

10 § Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Vid hemlig dataavläsning enligt första stycket får meddelanden inte hindras att nå fram enligt 2 § andra stycket.

I paragrafen regleras att tillstånd till hemlig dataavläsning i vissa fall får beviljas för inhämtning av uppgifter i underrättelseverksamhet (inhämtningslagsfallen), motsvarande de som gäller för inhämtning av

sådana uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Övervägandena finns i avsnitt 5.

I *första stycket* ändras hänvisningen till vilken brottslig verksamhet som omfattas av bestämmelsen. Ändringen görs med anledning av att 2 a § preventivlagen endast gäller under en viss tid (se lagen [2024:565] om ändring i lagen [2012:278] om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet).

15 § Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser ett brott som anges i 27 kap. 34 § rättegångsbalken, får frågan även prövas av Stockholms tingsrätt.

Frågor om hemlig dataavläsning enligt 7–*10* §§ prövas av *Stockholms tingsrätt*.

Paragrafen anger vilken domstol som är behörig att pröva frågor om tillstånd till hemlig dataavläsning. Övervägandena finns i avsnitt 5.

Andra stycket ändras på så sätt att hänvisningen till regleringen om behörig domstol i 6 § preventivlagen tas bort. Ändringen görs med anledning av att upplysningsbestämmelsen i 6 § andra stycket preventivlagen om att regeringen i förordning kan bestämma vilka tingsrätter som är behöriga att pröva en ansökan om tillstånd till tvångsmedel enligt 1 a och c §§ i samma lag endast gäller under viss tid (se lagen [2024:562] om ändring i lagen [2007:979] om åtgärder för att förhindra vissa särskilt allvarliga brott). Ändringen innebär att samtliga frågor om hemlig dataavläsning enligt 7–10 §§ prövas av Stockholms tingsrätt.

29 § När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12–14§§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

Paragrafen reglerar bl.a. hur överskottsinformation får användas vid hemlig dataavläsning i preventivlagsfallen. Övervägandena finns i avsnitt 5.

Med anledning av att möjligheten att bevilja ett tillstånd till hemlig dataavläsning som avser rumsavlyssningsuppgifter endast ska gälla under en viss tid tas regleringen om det tvångsmedlet bort i andra stycket.

11.4 Förslaget till lag om ändring i lagen (2024:326) om hemliga tvångsmedel i syfte att verkställa frihetsberövande påföljder

9 § I fråga om hemlig dataavläsning ska följande bestämmelser i lagen (2020:62) om hemlig dataavläsning tillämpas*:*

– 11 § om förbud mot hemlig dataavläsning,
– 12 och 13 §§ om tillträdestillstånd,
– 16 § om offentligt ombud och sammanträde,
– 18 § om tillståndets innehåll,
– 20 § om verkställbarhet och upphävande av beslutet,
– 21 § om underrättelse till Säkerhets- och integritetsskyddsnämnden,
– 22–26 §§ om genomförande av hemlig dataavläsning,
– 32 § om tystnadsplikt*, och*
– *34 § om dokumentation.*

Det som i bestämmelserna sägs om den misstänkte ska i stället avse den eftersökte.

Paragrafen anger vilka bestämmelser i lagen om hemlig dataavläsning som ska tillämpas i fråga om hemlig dataavläsning enligt lagen. Övervägandena finns i avsnitt 8.7.

I *första stycket* införs en hänvisning till den nya bestämmelsen om dokumentation i 34 § lagen om hemlig dataavläsning. Ändringen innebär att bestämmelserna om dokumentation i lagen om hemlig dataavläsning ska tillämpas vid hemlig dataavläsning enligt lagen.

10 § Åklagare får besluta att uppgifter som har kommit fram vid användning av hemlig övervakning av elektronisk kommunikation enligt 3 § *och hemlig dataavläsning enligt 4 §* får användas för ett annat ändamål än det som har legat till grund för åtgärden.

Paragrafen reglerar hur överskottsinformation från hemliga tvångsmedel får användas. Övervägandena finns i avsnitt 8.5.

Första stycket ändras på så sätt att samma regler som gäller för användandet av överskottsinformation från hemlig övervakning av elektronisk kommunikation nu också ska gälla för uppgifter från hemlig dataavläsning. Regleringen blir då densamma som för hemlig dataavläsning i övrigt, se författningskommentaren till 28 § lagen om hemlig dataavläsning.

Som en följd av ändringen tas det hittillsvarande *andra stycket*, om användande av uppgifter från hemlig dataavläsning, bort.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 april 2025.
2. Äldre föreskrifter gäller fortfarande för tillstånd som har beviljats före ikraftträdandet.
3. För uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet gäller 10 § i den äldre lydelsen.

Övervägandena finns i avsnitt 9.

Enligt *första punkten* träder lagen i kraft den 1 april 2025.

I *andra punkten* anges att äldre föreskrifter fortfarande gäller för tillstånd som har beviljats före ikraftträdandet. Bestämmelsen träffar sådana tillstånd till hemlig dataavläsning som har beslutats före ikraftträdandet, men där tiden för tillståndet ännu inte har löpt ut när lagen träder i kraft. Det innebär att den lagstadgade dokumentationsskyldigheten endast gäller för tillstånd som har beslutats efter ikraftträdandet.

I *tredje punkten* anges att 10 § gäller i den äldre lydelsen för uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet. Det innebär att det inte är tillåtet att använda överskottsinformation i större utsträckning än vad som var tillåtet vid den tidpunkt då informationen samlades in.

Sammanfattning av betänkandet Hemlig dataavläsning – utvärdering och permanent lagstiftning (SOU 2023:78)

Uppdraget

Vårt uppdrag har varit att utvärdera lagen (2020:62) om hemlig dataavläsning och ta ställning till om lagen bör permanentas samt om den i så fall bör ändras i något avseende. Genom lagen om hemlig dataavläsning, som trädde i kraft den 1 april 2020, infördes ett nytt hemligt tvångsmedel som de brottsbekämpande myndigheterna kan använda vid misstankar om allvarlig brottslighet. Lagen är tidsbegränsad till utgången av mars 2025. I uppdraget har bland annat ingått att analysera nyttan och behovet av hemlig dataavläsning, att ta ställning till om lagstiftningen bör permanentas och föreslå de åtgärder som behövs för ett permanentande, att analysera om lagstiftningen har fått en ändamålsenlig och proportionerlig utformning eller om det behövs förändringar i regelverket, samt att lämna förslag på de författningsändringar och andra åtgärder som bedöms nödvändiga. Uppdraget har innefattat att säkerställa att en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel upprätthålls. Det har också ingått i uppdraget att noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för grundläggande fri- och rättigheter, såsom den personliga integriteten, och säkerställa att förslagen uppfyller högt ställda krav på rättssäkerhet.

Vad är hemlig dataavläsning?

Hemlig dataavläsning är ett verktyg som ger de brottsbekämpande myndigheterna möjlighet att komma åt information som är svårtillgänglig, till exempel på grund av kryptering. Hemlig dataavläsning används i första hand när andra tvångsmedel eller metoder inte är framkomliga alternativ. I praktiken handlar hemlig dataavläsning om att de brottsbekämpande myndigheterna med hjälp av tekniska hjälpmedel i hemlighet får hämta in uppgifter som är åtkomliga i en dator, en mobiltelefon, ett användarkonto på internet eller något annat avläsningsbart informationssystem. För att få använda hemlig dataavläsning krävs som en grundläggande förutsättning att det är fråga om allvarlig brottslighet, exempelvis spionerі, terroristbrott, grovt dataintrång, grovt narkotikabrott, grovt vapenbrott, våldtäkt eller mord. Hemlig dataavläsning får under vissa närmare förutsättningar användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll, liksom i det internationella straffrättsliga samarbetet.

En permanent lagstiftning – avvägningar om behov, effektivitet och integritet

Sverige befinner sig i en situation där brottsligheten har stegrat i omfattning och blivit mer samhällshotande. Som exempel kan nämnas den markanta ökningen av dödligt skjutvapenvåld som skett de senaste åren. Våldsbrottsligheten är i sin tur starkt kopplad till den ökade narkotikabrottsligheten. En betydande ökning av den allvarliga brottsligheten har noterats också i underrättelsemiljön. Även den internationella säkerhetssituationen har fått konsekvenser för Sverige. Kriminellas handlingssätt och hur de kommunicerar är i förändring. Särskilt inom den allvarliga och organiserade brottsligheten används ofta krypterade tjänster och elektronisk utrustning för att kommunicera, i direkt syfte att undgå myndigheternas insyn. Globaliseringen, den tekniska utvecklingen och förändrade kommunikationsvanor har inneburit att de brottsbekämpande myndigheterna inte längre kan ta del av information som tidigare var tillgänglig genom traditionella tvångsmedel. Sedan möjligheten till hemlig dataavläsning infördes har betydelsen av effektiv tillgång till elektronisk bevisning blivit ännu mer framträdande. Detta gäller även i det internationella rättsliga samarbetet, eftersom den allvarliga brottslighet som kan föranleda hemlig dataavläsning inte sällan är av gränsöverskridande natur. Vid en internationell utblick kan det konstateras att i princip alla EU-länder samt USA, Kanada och Australien har lagstadgade möjligheter att använda hemlig dataavläsning, eller en motsvarighet till åtgärden, som ett verktyg i brottsbekämpningen. Det kan konstateras att den svenska tvångsmedelslagstiftningen måste hålla jämna steg med såväl teknik- och samhällsutvecklingen som den internationella rättsutvecklingen för att fortsatt kunna bekämpa den allvarliga brottsligheten.

De brottsbekämpande myndigheterna har nu haft möjlighet att använda hemlig dataavläsning i drygt 3,5 år. Våra analyser visar att hemlig dataavläsning har kommit till användning i större omfattning än vad som förutsågs när det nya tvångsmedlet infördes. De brottsbekämpande myndigheternas erfarenheter av hemlig dataavläsning har också varit mycket goda. De beskrivningar och praktiska exempel som har lämnats visar att hemlig dataavläsning i många fall har varit ett helt avgörande verktyg i den brottsbekämpande verksamheten. Hemlig dataavläsning har både lett till konkreta uppgifter om brott som redan begåtts och uppgifter som har kunnat användas för att förhindra allvarlig brottslighet. Hemlig dataavläsning har också i flera fall använts för att komma åt information om hur olika typer av grov brottslighet är organiserad och vilka personer som finns högre upp i hierarkin. Eftersom informationen inte varit åtkomlig genom andra tvångsmedel har hemlig dataavläsning i dessa fall inneburit ett genombrott i kampen mot den allvarliga och organiserade brottsligheten. Det står klart att användningen av hemlig dataavläsning är ett effektivt verktyg för att få tillgång till information och att åtgärden har medfört avsevärd nytta i brottsbekämpningen. Vi bedömer sammantaget att det finns ett fortsatt påtagligt behov av hemlig dataavläsning för att kunna bekämpa den allvarliga brottsligheten. Inget talar för att behovet skulle vara av tillfällig natur. Behovet kan inte heller tillgodoses med befintliga

bestämmelser om straffprocessuella tvångsmedel. Samtidigt bedömer vi att hemlig dataavläsning innebär risker för den personliga integriteten.

Vi har vägt behovet av en effektiv brottsbekämpning för att förebygga, förhindra, upptäcka och utreda allvarlig brottslighet, effektiviteten av åtgärden och den nytta som möjligheten att använda hemlig dataavläsning har medfört och kan förväntas medföra, mot de integritetsrisker som åtgärden innebär. I denna avvägning har vi även beaktat statens skyldighet att upprätthålla rättstrygghet för enskilda och skydda sina medborgare mot ingrepp i privatlivet från andra. Vi har sammantaget funnit att det är proportionerligt att hemlig dataavläsning blir ett permanent tvångsmedel. Åtgärden bedöms helt nödvändig med hänsyn till intresset av att bekämpa den allvarliga brottsligheten och för att kunna upprätthålla enskildas rättstrygghet och rätt till skydd mot kränkningar från andra enskilda. Vårt förslag om att permanenta lagstiftningen gäller under förutsättning att tillämpningsområdet är avgränsat på ett tydligt och ändamålsenligt sätt samt att lagstiftningen innehåller särskilda kvalifikationskrav och rättssäkerhetsgarantier som kan balansera de ökade risker som åtgärden innebär för den personliga integriteten. Vi föreslår därför även vissa ändringar i det nuvarande regelverket om hemlig dataavläsning.

Tydligare bestämmelser och ett utökat tillämpningsområde

Våra förslag på ändringar i lagen om hemlig dataavläsning innebär till övervägande del förtydliganden av lagstiftningen. Dessa syftar till att förenkla ansöknings- och beslutsprocessen samt undanröja den osäkerhet som i dag kan finnas angående ett tillstånds omfattning. Vi har i alla våra överväganden strävat efter att upprätthålla en välfungerande systematik i regelverket kring såväl hemliga som öppna tvångsmedel. De viktigaste konsekvenserna av våra förslag är att det blir tydligare under vilka förutsättningar som hemlig dataavläsning får användas, hur det inhämtade materialet ska hanteras och vilka skyldigheter som åligger tillämparen. Vi bedömer att våra förslag om en tydligare och mer förutsebar lagstiftning medför att lagen om hemlig dataavläsning kommer att stå i bättre överensstämmelse med de högt ställda krav på rättssäkerhet och de krav på skydd för enskildas personliga integritet som följer av regeringsformen, Europakonventionen och EU-rätten. Några av våra förslag innebär även en viss utvidgning av tillämpningsområdet för hemlig dataavläsning och att de brottsbekämpande myndigheterna får mer effektiva verktyg i arbetet med att utreda samt förebygga, förhindra och upptäcka viss allvarlig brottslighet. Vid en intresseavvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet har vi funnit att den ökade risk för ingrepp i den personliga integriteten som våra förslag innebär är försvarlig.

Eftersom lagstiftningen om hemlig dataavläsning och andra hemliga tvångsmedel är under utveckling har det också varit nödvändigt att göra en samlad proportionalitetsbedömning av hela det utökade och tilltänkta tillämpningsområdet för hemlig dataavläsning. Flera lagändringar som påverkar tillämpningsområdet för hemlig dataavläsning trädde i kraft så

sent som den 1 oktober 2023 och ytterligare lagförslag som kan komma att påverka tillämpningsområdet är för närvarande under beredning. Vid en samlad bedömning har vi funnit att hela det utökade och tilltänkta tillämpningsområdet för hemlig dataavläsning är tillräckligt ändamålsenligt och tydligt avgränsat för att kunna skydda enskilda mot godtyckliga ingrepp i deras fri- och rättigheter. Även med beaktande av det samlade integritetsintrång som genomförandet av våra förslag innebär, tillsammans med nuvarande lagstiftning och de ytterligare lagförslag som nu bereds och kan komma att träda i kraft inom kort, är det vår bedömning att regelverket för hemlig dataavläsning ger uttryck för en rimlig avvägning mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

Innebörden av hemlig dataavläsning förtydligas

Vi föreslår att innebörden av hemlig dataavläsning förtydligas. Förfarandet vid hemlig dataavläsning omfattar *inhämtning* (avläsning och överföring) samt *bearbetning* (förädling, sortering, filtrering och granskning) av uppgifter. Med hänsyn till hur hemlig dataavläsning fungerar kan det uttryck som för närvarande används för att definiera hemlig dataavläsning – att uppgifter ”läses av eller tas upp” – i vissa avseenden vara missvisade och orsaka tillämpningssvårigheter. Uttrycket ersätts därför med ”inhämtas”. I lagens portalparagraf klargörs således att hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling och som är åtkomliga i ett avläsningsbart informationssystem, *inhämtas* i hemlighet och med ett tekniskt hjälpmedel. Genom andra bestämmelser i lagen tydliggörs hur de inhämtade uppgifterna sedan får *bearbetas*. Ändringen medför därför vissa förtydliganden även i andra bestämmelser i lagen.

En tydligare bestämmelse om de olika uppgiftstyperna

I lagen om hemlig dataläsning anges sju olika uppgiftstyper, se 2 § första stycket 1–7. Uppgiftstyperna i 1–5 (kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter, platsuppgifter, kameraövervakningsuppgifter och rumsavlyssningsuppgifter) har sin motsvarighet i andra permanenta hemliga tvångsmedel. Uppgiftstyperna i 6 och 7 är unika för hemlig dataavläsning. Punkt 6 avser uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i punkt 1–5, och punkt 7 avser uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i punkt 1–6. I praktiken innebär denna uppdelning att lagrade uppgifter som inte är att sortera under punkt 1–3 utgör punkt 6-uppgifter och att realtidsuppgifter som inte är att sortera under punkt 1–5 och som visar hur ett informationssystem används utgör punkt 7-uppgifter.

Uppdelningen i olika uppgiftstyper får betydelse redan vid tillståndsgivningen, eftersom det i ett tillstånd till hemlig dataavläsning alltid ska anges vilken uppgiftstyp som får hämtas in. Detta s.k. differentieringskrav har orsakat vissa praktiska tillämpningsproblem. Orsaken är att det sällan före verkställighet går att avgöra hur lagstiftningens kategorisering av olika

uppgiftstyper ska appliceras på den information som kan komma att påträffas. Gränsdragningsproblematiken mellan uppgiftstyperna i punkt 6 och 7 har varit särskilt svår. Vi föreslår därför att punkt 6 och 7 slås ihop till en ny punkt 6 som inte gör skillnad på om uppgifterna är lagrade eller om de utgör realtidsuppgifter. Vi bedömer samtidigt att det även fortsatt ska göras en åtskillnad mellan var och en av uppgiftstyperna i 1–5 respektive uppgifter som sorterar under den nya punkten 6. Även om uppdelningen medför vissa praktiska utmaningar bedöms differentieringskravet utgöra en viktig skyddsåtgärd för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

Den hittillsvarande tillämpningen visar att det som regel finns ett påtagligt behov av hemlig dataavläsning av flera uppgiftstyper i varje enskilt fall. Ett typiskt tillstånd till hemlig dataavläsning behöver omfatta uppgiftstyperna i 1–3 och den nya punkten 6 för att åtgärden ska bli ändamålsenlig. Risken är annars att tillståndet får mindre räckvidd än avsett och att de brottsbekämpande myndigheterna därmed går miste om relevant information. En annan risk är att inhämtade uppgifter kan komma att betraktas som otillåten tilläggsinformation, om de eftersökta uppgifterna visar sig sortera under en annan punkt än förväntat. Ur rättssäkerhetssynpunkt framstår det som angeläget att fokus vid tillståndsprövningen ligger på den rättsliga prövningen och inte på hur behovet av information tekniskt sett är att kategorisera. Vi föreslår därför en förtydligande huvudregel som innebär att ett tillstånd till hemlig dataavläsning ska omfatta uppgiftstyperna i 1–3 och den nya punkten 6, om inget annat särskilt beslutas eller framgår av andra bestämmelser. Införandet av en sådan huvudregel balanseras av att vi samtidigt föreslår tydligare bestämmelser om villkor. Om det vid tillståndsprövningen inte är ändamålsenligt att begränsa vilka *uppgiftstyper* som får inhämtas talar det för att tillståndet bör förenas med villkor som anger vilka *uppgifter* som får inhämtas eller (inte) granskas och som därigenom begränsar åtgärden. Se närmare härom nedan.

Utökade möjligheter att utreda vem som skäligen kan misstänkas

Det finns i dag inte någon möjlighet att använda hemlig dataavläsning som gäller kameraövervakningsuppgifter eller uppgifter hänförliga till den av oss föreslagna nya punkten 6 i syfte att utreda vem som skäligen kan misstänkas för visst brott eller delaktighet i viss brottslighet. Det finns dock situationer, t.ex. i vissa utredningar om allvarliga brott över internet, där det finns ett påtagligt behov av en sådan möjlighet.

Vid exempelvis narkotikahandel under alias på Darknet, grova dataintrång, cyberbrott genom användning av skadlig programvara som t.ex. virus, trojaner eller spionprogram, eller internetrelaterade sexuella övergrepp mot barn används vanligen en komplex digital infrastruktur. Anonymisering och kryptering gör att det är svårt och många gånger omöjligt att genom traditionella tvångsmedel utreda vem eller vilka som ligger bakom den i övrigt fullt synliga brottsligheten. Information härom skulle dock kunna bli åtkomlig genom användning av hemlig dataavläsning som gäller s.k. punkt 6-uppgifter. Åtgärden skulle kunna användas för att hämta in t.ex. sparade bilder, källkoder, loggfiler, noder och andra

uppgifter som inte har kommunicerats. Vid en analys av sådana uppgifter skulle sedan digitala spår från olika håll kunna kombineras och utredas parallellt för att upptäcka eventuella samband, vilket många gånger är en förutsättning för att kunna identifiera personerna bakom brottsligheten. Ett exempel som belyser behovet av att använda kameraövervakningsuppgifter för att utreda vem som skäligen kan misstänkas är följande. Många gånger känner de brottsbekämpande myndigheterna till att ett visst informationssystem används som brottsverktyg för att begå allvarlig brottslighet, men saknar samtidigt verktyg för att identifiera den misstänkte. En vanlig invändning vid allvarlig brottslighet som exempelvis internetrelaterade sexuella övergrepp mot barn och narkotikabrottslighet över internet är att den misstänkte vid tiden för brottet hade lånat ut sin dator eller telefon till någon annan. Genom att aktivera kamerafunktionen på den informationsutrustning som används som brottsverktyg skulle användaren kunna identifieras. En möjlighet att använda hemlig dataavläsning i dessa situationer skulle således innebära en avsevärd nytta för brottsbekämpningen.

En sådan möjlighet innebär samtidigt ökade risker för enskildas personliga integritet och en ökad risk för att ovidkommande drabbas av åtgärden. Vid en intresseavvägning bedömer vi dock att behovet av en möjlighet att använda de olika åtgärderna är så påtagligt att det överväger nackdelarna ur ett integritetsperspektiv. Vi föreslår därför att det ska införas en möjlighet att använda kameraövervakningsuppgifter och den nya punkten 6-uppgifter i syfte att utreda vem som skäligen kan misstänkas för visst brott eller delaktighet i viss brottslighet. Med beaktande av de begränsade tillämpningsområden och de höga kvalifikationskrav som föreslås framstår det integritetsintrång som förslagen innebär som försvarligt i förhållande till behovet och nyttan av att utöka tillämpningsområdet på föreslaget sätt.

Tydligare bestämmelser om verkställighet

Den hittillsvarande tillämpningen visar att kravet på att i tillståndet ange vilken tid tillståndet avser har orsakat vissa tolknings- och tillämpningssvårigheter. Rent generellt får det anses missvisande med tillstånd som avser historiska tidsperioder, eftersom det vid hemlig dataavläsning endast är möjligt att ta del av den information som finns lagrad vid tidpunkten för verkställighet. Vidare har det visat sig svårt och många gånger omöjligt att redan före inhämtningen tidsbestämma lagrad information. Risken med att begränsa ett tillstånd till att endast avse uppgifter som har lagrats under viss tid är att tillståndet får mindre räckvidd än avsett. Lagrade uppgifter kan vara skapade och ändrade vid flera olika tidpunkter samt ingå i komplexa mappstrukturer. Lagrad information går sällan att tidsbestämma före själva inhämtningen. Den hittillsvarande tillämpningen visar också på ett behov av att klargöra under vilken tid som inhämtning av lagrade uppgifter får ske.

Vi föreslår därför att kravet på att ange vilken tid tillståndet avser ska tas bort. I stället föreslår vi att det i ett tillstånd till hemlig dataavläsning ska anges under vilken tid som verkställighet får ske. Tiden för verkställighet får inte bestämmas längre än nödvändigt och får inte överstiga en

månad från dagen för beslutet. Förslaget innebär ett förtydligande av att ett tillstånd till hemlig dataavläsning ska verkställas inom en viss tid som inte får överstiga en månad. Vidare föreslår vi att alla uppgifter som omfattas av tillståndet och som är åtkomliga under verkställighetstiden får hämtas in, om inte annat framgår av tillståndets villkor.

Förslaget innebär att inhämtningen inte längre behöver begränsas till information som lagrats under en viss tid, om det inte är möjligt eller lämpligt med en sådan begränsning. Härigenom undanröjs behovet att på förhand tidsbestämma lagrad information och verkställighetsproblematiken kring historiska tidsperioder för uppgifter som är lagrade i informationssystemet. Ändringen knyter an till vårt förslag om att tidsmässiga villkor som avser själva granskningen av inhämtade uppgifter ska bli mer framträdande.

Tydligare bestämmelser om villkor

Även kravet på att i tillståndet ange villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan har orsakat tolknings- och tillämpningssvårigheter. Det råder en osäkerhet i rättstillämpningen om hur villkor som tillgodoser intresset av att enskilda personliga integritet inte kränks i onödan bör utformas. Villkorskravet har därför inte alltid efterlevts i praktiken.

Vi bedömer att det även fortsatt ska vara obligatoriskt att förena ett tillstånd till hemlig dataavläsning med villkor. Detta utesluter inte att det kan finnas situationer där ett villkor för tillståndet framstår som överflödigt. Vi föreslår därför att det införs en ventil för obehövliga villkor. Vidare bör det tydliggöras vad villkoren ska avse. Vi föreslår därför att det i ett tillstånd till hemlig dataavläsning ska anges vilka uppgifter som inte får granskas och övriga villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, om sådana villkor inte framstår som obehövliga. Förslaget återknyter dels till förslaget om en tydligare bestämmelse om de olika uppgiftstyperna, dels till förslaget om tydligare bestämmelser om verkställighet. Vårt förslag om villkor balanserar det faktum att det vid tillståndsprövningen ofta inte är ändamålsenligt att begränsa antalet uppgiftstyper eller att tidsmässigt avgränsa vilka uppgifter som får *inhämtas*. Eftersom sådana avgränsningar dock är möjliga att göra i en inledande bearbetning av de inhämtade uppgifterna, ska det som huvudregel anges villkor för vilka inhämtade uppgifter som inte får *granskas*. Övriga villkor för tillståndet tar sikte på andra omständigheter än granskningen. I de fall som det är möjligt och lämpligt kan övriga villkor avse själva inhämtningen av uppgifter. Villkoren måste anpassas efter omständigheterna i det enskilda fallet. I våra överväganden ger vi exempel på villkor och beskriver hur både inhämtningen och granskningen av inhämtade uppgifter kan avgränsas på ett ändamålsenligt sätt, samtidigt som intresset av att enskildas personliga integritet inte kränks i onödan tillgodoses.

För att syftet med villkorsgivningen ska uppfyllas krävs att villkoren generellt sett håller en högre kvalitet än i dag. Vi föreslår därför att åklagaren, eller i förekommande fall Säkerhetspolisen, i samband med en ansökan om hemlig dataavläsning ska vara skyldig att föreslå de villkor

som tillståndet ska förenas med, om sådana villkor inte framstår som obehövliga.

Tydligare bestämmelser om överskottsinformation

Vi föreslår att användningsområdet för överskottsinformation från hemlig dataavläsning förtydligas, i enlighet med vad som redan gäller för hemliga tvångsmedel enligt rättegångsbalken och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Det innebär att åklagare, utan några särskilt stadgade begränsningar, ska få besluta att uppgifter som har kommit fram vid användning av hemlig dataavläsning under förundersökning och enligt reglerna i preventivlagen får användas för ett annat ändamål än det som har legat till grund för åtgärden. För det fall att bestämmelsen om överskottsinformation i inhämtningslagen ändras i enlighet med förslaget i slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60, föreslår vi att det, som en följd av förslaget, ska införas en motsvarande reglering om användning av överskottsinformation i inhämtningslagsfallen.

Tydligare bestämmelser om bevarande och förstöring

Vi föreslår att upptagningar och uppteckningar från hemlig dataavläsning under en förundersökning ska bevaras i enlighet med vad som redan gäller för hemliga tvångsmedel enligt rättegångsbalken. Det innebär att allt material som huvudregel ska bevaras. Om den misstänkte medger det ska upptagningar och uppteckningar få förstöras innan förundersökningen har lagts ned eller avslutats eller, om åtal har beslutats, målet har avgjorts slutligt. För det fall att bestämmelsen om bevarande och förstöring i inhämtningslagen ändras i enlighet med förslaget i slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60, föreslår vi att det, som en följd av förslaget, ska införas en motsvarande reglering om bevarande och förstöring i inhämtningslagsfallen.

Tydligare bestämmelser om otillåtna uppgifter

Vi föreslår att bestämmelsen om otillåten tilläggsinformation både förtydligas och utvecklas. Förslaget innebär att om otillåtna uppgifter påträffas så ska dessa uppgifter förstöras så snart det är möjligt. Undantaget från huvudregeln om bevarande gäller om upptagningar eller uppteckningar av följande uppgifter påträffas:

1. Uppgiftstyper som inte får inhämtas enligt tillståndet.
2. Uppgifter som inte får inhämtas enligt villkor för tillståndet.
3. Uppgifter som inte får granskas enligt villkor för tillståndet.
4. Uppgifter som omfattas av beslags- eller avlyssningsförbudet.

Ett lagstadgat dokumentationskrav införs

I dag finns ingen lagstadgad skyldighet att dokumentera användningen av hemlig dataavläsning. Vi föreslår att det i lagen om hemlig dataavläsning

ska införas ett dokumentationskrav för beslut och åtgärder som rör hemlig dataavläsning. Förslaget motsvarar vad som redan gäller för hemliga tvångsmedel enligt rättegångsbalken och preventivlagen. Ett förslag om att det ska införas ett lagstadgat dokumentationskrav även i inhämtningslagen är för närvarande under beredning, se slutbetänkandet *Utökade möjligheter att använda preventiva tvångsmedel 2*, SOU 2023:60.

Lagstiftningens struktur och placering

Vi föreslår att bestämmelserna om hemlig dataavläsning fortsatt bör regleras i en särskild lag – lagen om hemlig dataavläsning. Vi framhåller samtidigt att det vore önskvärt att bestämmelserna om tvångsmedelsanvändning blev föremål för en fullständig översyn i syfte att förenkla och harmonisera reglerna. I avvaktan på att det görs en samlad översyn av tvångsmedelsbestämmelserna anser vi dock att kraven på systematik, tydlighet och förutsebarhet bäst tillgodoses om hemlig dataavläsning fortsatt regleras i en egen lag.

Ikraftträdande

Lagändringarna föreslås träda i kraft den 1 mars 2025.

Konsekvenser

Ett genomförande av förslagen förbättrar de brottsbekämpande myndigheternas förutsättningar att utreda, förebygga, förhindra och upptäcka allvarlig brottslighet. På sikt kan våra förslag också ha brottsförebyggande effekter och leda till att färre brott begås. Våra förslag får indirekt genomslag även för det internationella straffrättsliga samarbetet. Bättre förutsättningar för internationellt rättsligt samarbete får särskilt stor betydelse vid gränsöverskridande brottslighet som t.ex. internetrelaterade sexuella övergrepp mot barn samt narkotika- eller cyberbrottslighet.

För enskilda innebär våra förslag en ökad risk för den personliga integriteten. De personer som berörs bedöms huvudsakligen vara samma personer som riskerar att bli föremål för andra hemliga tvångsmedel. Våra förslag innebär i flera avseenden också ett förstärkt skydd för enskildas personliga integritet och en ökad rättstrygghet för enskilda. Detta framför allt med hänsyn till statens positiva förpliktelser som innebär en skyldighet att skydda enskilda mot ingrepp i privatlivet från andra. Vissa av förslagen innebär också ett förbättrat skydd mot otillåtna och obefogade integritetsintrång. Våra förslag i dessa delar bedöms därmed innebära en förstärkt rättssäkerhet för den enskilde.

Att bedöma de ekonomiska konsekvenserna av våra förslag är förenat med flera svårigheter, inte minst eftersom frågan om användning av hemlig dataavläsning i varje enskilt ärende innefattar en prioritering utifrån nyttan respektive resursåtgången av en sådan åtgärd. Hemlig dataavläsning är jämfört med andra tvångsåtgärder ett mycket resurskrävande hemligt

tvångsmedel, eftersom åtgärden kräver både ett omfattande förberedelsearbete och en avancerad teknisk förmåga, särskilt anpassad efter det enskilda fallet. Säkerhetspolisen och Tullverket har uppskattat att myndigheternas resursbehov kommer att öka om våra förslag genomförs. De ökade kostnaderna avser huvudsakligen teknikkostnader och personalkostnader för att bibehålla och utveckla egen nödvändig teknisk förmåga på området. Säkerhets- och integritetsskyddsnämnden (SIN) har bedömt att nämndens tillsynsuppdrag, som en följd av våra förslag, kommer att öka i en sådan omfattning att nämnden bör tillföras ytterligare medel för att kunna utföra en effektiv och rättssäker tillsyn. De resursbehov som uppkommer för dessa myndigheter föreslås huvudsakligen finansieras genom att medel tillförs från andra utgiftsområden. Även Polismyndigheten och Sveriges Domstolar, inklusive anslaget för rättsliga biträden, kommer att få vissa ökade kostnader med anledning av våra förslag. Dessa kostnader bedöms dock rymmas inom befintliga anslag. Detsamma gäller de ökade kostnader som kan komma att uppstå för Skatteverket, Finansinspektionen och Kriminalvården. Beträffande övriga berörda aktörer – Åklagarmyndigheten, Ekobrottsmyndigheten och företag som medverkar vid verkställighet – bedöms genomförandet av våra förslag inte medföra några ökade kostnader.

De kostnader som den allvarliga brottsligheten medför är avsevärda. Mer effektiva verktyg för att utreda, förebygga, förhindra och upptäcka allvarlig brottslighet bedöms därför få stora positiva samhällsekonomiska konsekvenser. Våra förslag kan medföra betydande samhällsekonomiska besparingar kopplade till exempelvis rättsväsendet, sjukvården, sociala myndigheter, Skatteverket och Försäkringskassan. Besparingseffekterna är svåra att beräkna, men knappast obetydliga ens för ett enskilt fall.

Betänkandets lagförslag

Förslag till lag om ändring i lagen (2020:62) om hemlig dataavläsning

Härigenom föreskrivs i fråga om lagen (2020:62) om hemlig dataavläsning som gäller till utgången av mars 2025

dels att lagen ska fortsätta gälla utan begränsning till viss tid,

dels att 1, 2, 4 a, 4 b, 8, 9, 14, 17, 18, 23, 27–29 och 31 §§ ska ha följande lydelse,

dels att rubrikerna närmast före 2 och 27 §§ ska ha följande lydelse,

dels att det ska införas en ny paragraf, 34 §, och närmast före 34 § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §
Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel *läses av eller tas upp* i ett avläsningsbart informationssystem.	Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling *och som är åtkomliga* i ett avläsningsbart informationssystem, *inhämtas* i hemlighet och med ett tekniskt hjälpmedel.
I lagen avses med	
avläsningsbart informationssystem: en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst,	
kommunikationsavlyssningsuppgifter: uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *någon* annan adress,	*kommunikationsavlyssningsuppgifter*: uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,
kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *någon* annan adress,	*kommunikationsövervakningsuppgifter*: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller *en* annan adress,
platsuppgifter: uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,	
kameraövervakningsuppgifter: uppgifter som framkommer genom optisk personövervakning,	
rumsavlyssningsuppgifter: uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.	

Typer av uppgifter* som får *läsas av eller tas upp	***Uppgiftstyper* som får *hämtas in***
2 §	
Tillstånd till hemlig dataavläsning får *beviljas för att läsa av eller ta upp*	Tillstånd till hemlig dataavläsning får *avse*
1. kommunikationsavlyssningsuppgifter,	
2. kommunikationsövervakningsuppgifter,	
3. platsuppgifter,	
4. kameraövervakningsuppgifter,	
5. rumsavlyssningsuppgifter,	5. rumsavlyssningsuppgifter *eller*
6. uppgifter som *finns lagrade* i ett avläsningsbart informationssystem men som inte avses i 1–5*, eller*	6. uppgifter som *är åtkomliga* i ett avläsningsbart informationssystem men som inte avses i 1–5.
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.	

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

Ett tillstånd enligt första stycket omfattar uppgiftstyperna i första stycket 1–3 och 6, om inget annat särskilt beslutas eller framgår av andra bestämmelser.

4 a §[1]

Ett tillstånd enligt 4 § får endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av den misstänkte.

Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.	Ett tillstånd enligt 4 § som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta.

Ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

[1] Senaste lydelse 2023:540.

Trots tredje stycket får ett tillstånd enligt 4 § som gäller kameraövervakningsuppgifter avse den skäligen misstänkte i stället för en viss plats, om det finns särskilda skäl för det. Den hemliga dataavläsningen får då endast användas på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

4 b §[2]

Ett tillstånd till hemlig dataavläsning som gäller *kommunikationsavlyssningsuppgifter* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.	Ett tillstånd till hemlig dataavläsning som gäller *uppgiftstyperna i 2 § första stycket 1–4 eller 6* får, om åtgärden är av synnerlig vikt för utredningen, även beviljas för att utreda vem som skäligen kan misstänkas för brottet eller brotten vid en förundersökning om brott som avses i 27 kap. 18 b § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får endast avse ett avläsningsbart informationssystem som

1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten *under den tid som tillståndet avser* har använt eller kommer att använda, eller	1. det finns särskild anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har använt eller kommer att använda, eller,
2. det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.	2. *om tillståndet gäller uppgiftstyperna i 2 § första stycket 1–3 eller 6,* det finns synnerlig anledning att anta att gärningsmannen eller någon annan som har medverkat till brottet eller brotten har kontaktat eller kommer att kontakta.
	Ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter får inte verkställas på en plats som är någons stadigvarande bostad.
	Trots tredje stycket får tillståndet verkställas på en sådan plats, om det finns synnerliga skäl att anta att den person som åtgärden riktar sig mot uppehåller sig i direkt anslutning till det avläsningsbara informationssystem som tillståndet avser.

[2] Senaste lydelse 2023:540.

8 §

Hemlig dataavläsning enligt 7 § får avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en person som anges i den bestämmelsen.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att en person som anges i 7 § *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att en person som anges i 7 § har kontaktat eller kommer att kontakta.

9 §[3]

Ett tillstånd till hemlig dataavläsning får beviljas för att *läsa av eller ta upp* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

Ett tillstånd till hemlig dataavläsning får beviljas för att *inhämta* uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

1. ett utvisningsbeslut enligt 2 kap. 1 § lagen (2022:700) om särskild kontroll av vissa utlänningar, eller

2. ett avvisnings- eller utvisningsbeslut enligt 8 kap. eller 8 a kap. utlänningslagen (2005:716) om det finns sådana omständigheter i fråga om utlänningen som avses i 2 kap. 1 § lagen om särskild kontroll av vissa utlänningar.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får också beviljas för att *läsa av eller ta upp* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen *under den tid som tillståndet avser* har kontaktat eller kommer att kontakta.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får också beviljas för att *hämta in* uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 5 kap. 5 och 6 §§ lagen om särskild kontroll av vissa utlänningar ska tillämpas i

[3] Senaste lydelse 2022:711.

fråga om utlänningen gäller också för ett beslut i fråga om hemlig dataavläsning.

Ett tillstånd får beviljas endast om det finns synnerliga skäl och det är av betydelse för att klarlägga om

1. utlänningen tillhör eller verkar för en organisation eller grupp som planlägger eller förbereder brott enligt terroristbrottslagen (2022:666) eller om det finns en risk för att utlänningen kan komma att engagera sig i en sådan organisation eller grupp,

2. det finns risk för att utlänningen själv planlägger eller förbereder brott som avses i 1, eller

3. det finns risk för att utlänningen själv eller tillsammans med andra medverkar i eller på annat sätt främjar ett allvarligt brott som rör Sveriges säkerhet.

Ett tillstånd får inte avse rumsavlyssningsuppgifter.

14 §[4]

Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen.

Om ansökan avser den skäligen misstänkte enligt 4 a § fjärde stycket eller 6 § fjärde stycket, ska åklagaren i samband med ansökan föreslå sådana villkor som avses i 18 § första stycket 4.

Åklagaren*, eller i förekommande fall Säkerhetspolisen,* ska i samband med ansökan föreslå sådana villkor som avses i 18 § första stycket 4*, om sådana villkor inte framstår som obehövliga.*

17 §[5]

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens *tillstånd* i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens *beslut* i en fråga om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren snarast möjligt skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten

[4] Senaste lydelse 2023:540.
[5] Senaste lydelse 2023:540.

pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *lästs av eller tagits upp* inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.	pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som *hämtats in* inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

18 §[6]

I ett tillstånd till hemlig dataavläsning ska följande anges:

1. vilken tid tillståndet *avser*,	1. *under* vilken tid *som verkställighet får ske*,
2. vilket avläsningsbart informationssystem tillståndet avser,	
3. vilken *typ av uppgift* enligt 2 § första stycket som får *läsas av eller tas upp*,	3. vilken *uppgiftstyp* enligt 2 § första stycket som får *inhämtas*,
4. villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, och	4. *vilka uppgifter som inte får granskas och övriga* villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, *om det inte framstår som obehövligt,* och
5. vem som är skäligen misstänkt för brottet eller brotten, *vid åtgärd som gäller rumsavlyssningsuppgifter*.	5. vem som är skäligen misstänkt för brottet eller brotten, *om sådan uppgift finns*.

Om tillståndet avser en plats enligt 4 a § tredje stycket, 6 § tredje stycket eller 7 § tredje stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska det anges i beslutet.

Om tillståndet avser den skäligen misstänkte enligt 4 a § fjärde stycket eller 6 § fjärde stycket, ska det anges i beslutet.

Tiden för *tillståndet* får inte bestämmas längre än nödvändigt. *När det gäller tid som infaller efter beslutet* får *tiden* inte överstiga en månad från dagen för beslutet.	Tiden för *verkställighet* får inte bestämmas längre än nödvändigt *och* får inte överstiga en månad från dagen för beslutet.

23 §

Den teknik *som används i samband med* hemlig dataavläsning ska anpassas efter *det tillstånd som beviljats. Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet.* Om *sådana*	*Vid verkställighet av* hemlig dataavläsning ska teknik *och tillvägagångssätt* anpassas efter *tillståndet*. Om *någon annan uppgiftstyp än vad som anges i tillståndet har hämtats in* ska upptagningar och uppteckningar av dessa uppgifter

[6] Senaste lydelse 2023:540.

uppgifter har lästs av eller tagits upp ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas.	omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. *Upptagningar och uppteckningar av uppgifter som inte får inhämtas eller granskas enligt villkor meddelade med stöd av 18 § första stycket 4 ska förstöras i de delar de innehåller sådana uppgifter så snart det står klart att sådana uppgifter har inhämtats eller granskats.*

Uppgifter som anges i första stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.

Förbud att *läsa av eller ta upp* vissa uppgifter	**Förbud att *hämta in* vissa uppgifter**
27 §[7]	
Hemlig dataavläsning enligt 2 § första stycket 6 *eller 7* får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.	Hemlig dataavläsning enligt 2 § första stycket 6 får inte avse uppgifter som enligt 27 kap. 2 § rättegångsbalken hindrar beslag.

Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram.

Om det under verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *verkställigheten* omedelbart avbrytas *och* upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.	Om det under *eller efter* verkställigheten kommer fram uppgifter som omfattas av första eller andra stycket ska *granskningen av dessa uppgifter* omedelbart avbrytas. Upptagningar och uppteckningar *ska* omedelbart förstöras i de delar som de omfattas av förbudet.
28 §[8]	
När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken *i lydelsen före den 1 oktober 2023* tillämpas för åtgärden. Det	När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden. Det som gäller för hemlig rumsavlyss-

[7] Senaste lydelse 2023:540.
[8] Senaste lydelse 2023:540.

som gäller för hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

ning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

För underrättelse till en enskild vid hemlig dataavläsning under förundersökning gäller 27 kap. 31–33 §§ rättegångsbalken. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

29 §[9]

När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott *i lydelsen före den 1 oktober 2023* tillämpas.

När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

Lydelse enligt SOU 2023:60

Föreslagen lydelse

31 §

När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och *8* §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet *i lydelsen före den 1 januari 2025* tillämpas. Det som anges där om inhämtning av

När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6 och *7* §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.

[9] Senaste lydelse 2023:540.

uppgifter ska tillämpas för hemlig dataavläsning.

Uppgifter som har kommit fram vid hemlig dataavläsning enligt 10 § får användas i en förundersökning endast efter tillstånd till hemlig dataavläsning enligt 4 eller 5 § som gäller kommunikationsövervaknings- eller platsuppgifter. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för beslut om att inleda en förundersökning.

Nuvarande lydelse	*Föreslagen lydelse*
	Dokumentation
	34 §
	Beslut och åtgärder som rör hemlig dataavläsning ska dokumenteras.

---

1. Denna lag träder i kraft den 1 mars 2025.
2. Äldre föreskrifter gäller fortfarande för tillstånd som har beviljats före ikraftträdandet.
3. För uppgifter från hemlig dataavläsning som har verkställts före ikraftträdandet gäller 28, 29 och 31 §§ i den äldre lydelsen.

Förteckning över remissinstanserna

Efter remiss har yttrande över betänkandet lämnats av Bahnhof AB, Brottsförebyggande rådet, Brottsofferjouren Sverige, Brottsoffermyndigheten, Centrum för rättvisa, Civil Rights Defenders, Diskrimineringsombudsmannen, Domarnämnden, Domstolsverket, ECPAT Sverige, Ekobrottsmyndigheten, Finansinspektionen, Föreningen för Digitala fri- och rättigheter, Försvarets radioanstalt, Försvarsmakten, Förvaltningsrätten i Göteborg (Migrationsdomstolen), Göta hovrätt, Helsingborgs tingsrätt, Institutet för mänskliga rättigheter, Integritetsskyddsmyndigheten, Justitiekanslern, Kriminalvården, Kustbevakningen, Lunds universitet (juridiska fakulteten), Malmö tingsrätt, Migrationsverket, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen, Riksarkivet, Riksdagens ombudsmän (JO), Skatteverket, Solna tingsrätt, Stockholms tingsrätt, Svea hovrätt, Svenska Journalistförbundet (SJF), Svenska kyrkan, Sveriges advokatsamfund, Säkerhets- och integritetsskyddsnämnden, Säkerhetspolisen, Tidningsutgivarna (TU), Tullverket och Åklagarmyndigheten.

Kungl. Tekniska högskolan, Stiftelsen för Internetinfrastruktur och Stockholms universitet (juridiska fakulteten) har avstått från att yttra sig.

Följande remissinstanser har inte inkommit med något yttrande: Amnesty international, Apple Aktiebolag, Dataskydd.net Sverige, Facebook Sweden AB, Google Sweden AB, Hi3G Access AB, ISOC-SE, Judiska centralrådet i Sverige, Microsoft AB, Net at Once Sweden AB, Rädda barnen, Rättighetsalliansen, Samsung Electronics Nordic AB, Svenska muslimer för fred och rättvisa, Svenska stadsnätsföreningen, Svenskt Näringsliv, Sveriges läkarförbund, Sveriges psykologförbund, TechSverige, Tele2 Sverige AB, Telenor Sverige AB och Telia Sverige AB.