



Svensk författningssamling

Lag om hemlig dataavläsning

Utfärdad den 27 februari 2020

SFS 2020:62

Publicerad
den 3 mars 2020

Enligt riksdagens beslut¹ föreskrivs följande.

Ord och uttryck i lagen

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.

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,

kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon 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

2 § Tillstånd till hemlig dataavläsning får beviljas för att läsa av eller ta upp

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,
6. uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i 1–5, eller
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.

¹ Prop. 2019/20:64, bet. 2019/20:JuU19, rskr. 2019/20:170.

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.

Grundläggande förutsättning för hemlig dataavläsning

3 § Ett tillstånd till hemlig dataavläsning får beviljas endast 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.

Hemlig dataavläsning under en förundersökning

4 § Ett tillstånd till hemlig dataavläsning får, om åtgärden är av synnerlig vikt för utredningen och inte annat anges i 6 § första stycket, beviljas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. brott som avses i 27 kap. 2 § andra stycket 2–7 rättegångsbalken,
3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, om en sådan gärning är belagd med straff, eller
4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Ett tillstånd enligt första stycket får, om inte annat anges i 5 §, endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet.

Ett tillstånd enligt första stycket som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får, om inte annat anges i 5 §, 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 första stycket 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.

5 § Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller kommunikationsövervaknings- eller platsuppgifter får även beviljas för att utreda vem som skäligen kan misstänkas för ett brott som avses i 4 §. Avläsning eller upptagning av kommunikationsövervakningsuppgifter får då endast avse förfluten tid.

Hemlig dataavläsning enligt första stycket får 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.

6 § Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller rumsavlyssningsuppgifter får endast beviljas vid en förundersökning om brott som avses i 27 kap. 20 d § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om platsen är någon annan stadigvarande bostad än den misstänktes, får tillstånd till hemlig dataavläsning beviljas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

Hemlig dataavläsning enligt första stycket får aldrig användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas.

SFS 2020:62

Hemlig dataavläsning utanför en förundersökning

Förhindrande av vissa särskilt allvarliga brott

7 § Ett tillstånd till hemlig dataavläsning får beviljas om

1. det med hänsyn till omständigheterna finns en påtaglig risk för 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. det finns en påtaglig risk för att sådan brottslig verksamhet 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 sådan brottslig verksamhet som anges i det stycket.

Hemlig dataavläsning som gäller kameraövervakningsuppgifter får användas endast på en plats där den person som anges i första stycket kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Ett tillstånd får inte avse rumsavlyssningsuppgifter.

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.

Särskild utlänningskontroll

9 § 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

1. ett utvisningsbeslut enligt 1 § 2 lagen (1991:572) om särskild utlänningskontroll, eller

2. ett avvisnings- eller utvisningsbeslut enligt 8 eller 8 a kap. utlänningslagen (2005:716) eller motsvarande äldre bestämmelser och det finns sådana omständigheter i fråga om utlänningsen som avses i 1 § 2 lagen om särskild utlänningskontroll.

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 utlänningsen under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 19–22 §§ lagen om särskild utlänningskontroll samt denna lag ska tillämpas på utlänningsen. Det förfarande och de förutsättningar som gäller för ett beslut om att 19–22 §§ lagen om särskild

utlänningskontroll 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 utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott.

Ett tillstånd får inte avse kameraövervaknings- eller rumsavlyssningsuppgifter.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

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.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervakningsuppgifter får endast avse uppgifter i förfluten tid.

Förbud mot hemlig dataavläsning

11 § Ett tillstånd till hemlig dataavläsning får inte avse ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas

1. i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,

2. i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller

3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård.

Tillträdestillstånd

12 § Vid hemlig dataavläsning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en sådan person som anges i 7 § första stycket eller 9 § första stycket, får tillstånd beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där.

13 § Ett tillträdestillstånd enligt 12 § får inte avse en plats som stadigvarande används eller är särskilt avsedd att användas

1. för verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,

2. för verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller

3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

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

15 § Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser brott som anges i 27 kap. 2 § andra stycket 2–8 rättegångsbalken får frågan även prövas av Stockholms tingsrätt.

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

16 § När en ansökan eller anmälan om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska den som gjort ansökan eller anmälan och det offentliga ombudet närvara.

För offentliga ombud i ärenden om hemlig dataavläsning gäller 27 kap. 26 och 27 §§, 28 § andra stycket samt 29 och 30 §§ rättegångsbalken.

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 inhämta rättens tillstånd i frågor om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning som gäller rumsavlyssningsuppgifter eller hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren utan dröjsmål 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.

18 § 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, vid åtgärd som gäller rumsavlyssningsuppgifter.

Om tillståndet avser en plats enligt 4 § fjärde stycket eller 6 § andra stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, 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.

19 § På förfarandet enligt denna lag tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i denna lag. Handläggningen ska ske skyndsamt.

20 § Ett beslut i frågor om hemlig dataavläsning får verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, ska den som ansökt om åtgärden eller rätten omedelbart upphäva beslutet.

21 § När rätten har beslutat i frågor om hemlig dataavläsning ska den skyndsamt underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

Genomförande av hemlig dataavläsning

Tillåtna tekniska metoder

22 § När ett tillstånd till hemlig dataavläsning har beviljats får de tekniska hjälpmedel som behövs för avläsningen och upptagningen användas. Om det är nödvändigt får systemskydd brytas eller kringgå och tekniska sårbarheter utnyttjas.

Teknikanpassning och otillåten tilläggsinformation

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.

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.

Skyldighet att medverka

24 § Den som bedriver verksamhet som är anmälningsskyldig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation är på begäran av den verkställande myndigheten skyldig att medverka i samband med verkställighet av hemlig dataavläsning.

Den som medverkar enligt första stycket har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den verkställande myndigheten.

Aktsamhetskrav

25 § När ett beslut om hemlig dataavläsning verkställs får någon olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser får dock inte åsidosättas, försämrats eller skadas till följd av verkställigheten.

När verkställigheten avslutas ska den verkställande myndigheten vidta de åtgärder som behövs för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla minst samma nivå som vid verkställighetens början.

Ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet upphävts.

26 § Den verkställande myndigheten ska utse en eller flera personer som får verkställa hemlig dataavläsning. Sådana personer ska vara särskilt lämpade för uppdraget och ha särskilda kunskaper om informationssäkerhet samt den särskilda kompetens, utbildning och erfarenhet som i övrigt är nödvändig.

Förbud att läsa av eller ta upp vissa uppgifter

27 § Hemlig dataavläsning enligt 2 § första stycket 6 eller 7 får inte avse uppgifter som enligt 27 kap. 2 § första stycket 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 styckena ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.

Överskottsinformation, granskning och underrättelse till enskilda

Förundersökning

28 § 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 rumsavlyssning 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.

Förhindrande av vissa särskilt allvarliga brott

29 § 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.

Särskild utlänningskontroll

30 § När hemlig dataavläsning används eller har använts i fall som anges i 9 § ska 21 a § och 22 § första och andra styckena lagen (1991:572) om särskild utlänningskontroll tillämpas. Det som anges där om hemlig avlyssning och övervakning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

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 under rättelseverksamhet tillämpas. Det som anges där om inhämtning av 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.

Tystnadsplikt

32 § Den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning, får inte obehörigen föra vidare eller utnyttja det han eller hon fått del av eller tillgång till.

Rätt att meddela föreskrifter

33 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. underrättelser enligt 23 §, och
2. medverkan och ersättning enligt 24 §.

1. Denna lag träder i kraft den 1 april 2020.

2. Lagen upphör att gälla vid utgången av mars 2025.

På regeringens vägnar

STEFAN LÖFVEN

MIKAEL DAMBERG
(Justitiedepartementet)