



JURIDISKA FAKULTETEN
vid Lunds universitet

Marcus Grudén

Hemlig dataavläsning

Ett viktigt verktyg i kampen mot allvarlig brottslighet, eller en alltför långtgående inskränkning av individens rättigheter?

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Sverker Jönsson

Termin för examen: period 1 VT20

Innehåll

SUMMARY	1
SAMMANFATTNING	4
FÖRORD	6
FÖRKORTNINGAR	7
1 INLEDNING	8
1.1 Bakgrund	8
1.2 Syfte och frågeställningar	8
1.3 Avgränsningar	9
1.4 Metod och material	10
1.5 Disposition	11
2 GÄLLANDE RÄTT	12
2.1 Äldre hemliga tvångsmedel	12
2.1.1 Hemlig avlyssning av elektronisk kommunikation	12
2.1.2 Hemlig övervakning av elektronisk kommunikation	14
2.1.2.1 Inhämtning av elektronisk kommunikation i underrättelseverksamhet	16
2.1.3 Hemlig kameraövervakning	17
2.1.4 Hemlig rumsavlyssning	18
2.2 Nationellt skydd för den personliga integriteten	19
2.2.1 Lag	19
2.2.2 Principer för användning av tvångsmedel	20
2.2.2.1 Legalitetsprincipen	20
2.2.2.2 Ändamålsprincipen	20
2.2.2.3 Behovsprincipen	21
2.2.2.4 Proportionalitetsprincipen	21

2.3	Europakonventionen	22
2.3.1	Integritetsskyddet i artikel 8	22
2.3.2	Rättvis rättegång enligt artikel 6	23
2.3.3	Användning av hemliga tvångsmedel i Europadomstolens praxis	25
3	LAG (2020:62) OM HEMLIG DATAAVLÄSNING	30
3.1	Behovet av nya verktyg	30
3.1.1	Kryptering	31
3.1.2	Anonymisering	32
3.2	Tidigare överväganden	33
3.2.1	SOU 2005:38	33
3.2.2	SOU 2012:44	34
3.2.3	SOU 2017:89	35
3.3	Förutsättningar för användande av hemlig dataavläsning	37
3.3.1	De uppgifter som får inhämtas	38
3.3.2	Hemlig dataavläsning inom ramen för förundersökning	39
3.3.2.1	Särskilt om kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter	41
3.3.2.2	Särskilt om rumsavlyssningsuppgifter	43
3.3.2.3	Särskilt om kameraövervakningsuppgifter	45
3.3.3	Hemlig dataavläsning utanför förundersökning	45
3.3.3.1	Förhindrande av vissa särskilt allvarliga brott	46
3.3.3.2	Särskild utlänningskontroll	49
3.3.3.3	För att upptäcka brottslig verksamhet	51
3.4	Rättssäkerhetsgarantier	52
3.4.1	Tillståndsprövning	52
3.4.2	Aktsamhetskrav	54
3.4.3	Förbud mot hemlig dataavläsning	55
3.4.3.1	Fredade verksamheter	55
3.4.3.2	Övriga förbud	56
3.4.4	Användning av överskottsinformation	57
3.4.5	Granskning, bevarande och förstörande av uppgifter	59
3.4.6	Underrättelse till enskilda	60
3.5	Sammanfattning av lagen	60

4	DEN PRAKTISKA EFTERLEVNADEN	66
4.1	Säkerhets- och integritetsskyddsmyndighetens tillsyn	66
4.1.1	Allmänna synpunkter	66
4.1.2	Tillståndsprövning	67
4.1.3	Verkställighet utanför tillstånd	68
4.1.4	Skyldighet att häva tillstånd	69
4.1.5	Avlyssningsförbud	69
4.1.6	Dokumentation och förstöring av material	70
4.1.7	Underrättelse i efterhand till enskilda	71
4.1.8	Nämndens efterhandskontroll	71
4.1.9	Partsinsyn	72
4.2	Effektivitetsbegreppet	72
4.2.1	Språklig definition	73
4.2.2	Definition i tvångsmedelssammanhang	73
4.3	Lagstiftarens användning av effektivitetsbegreppet	75
4.3.1	Kvantitativ effektivitet	76
4.3.2	Kvalitativ effektivitet	77
4.4	De brottsbekämpande myndigheternas användning av tvångsmedel under 2018	78
4.4.1	Nyttan av hemliga tvångsmedel	79
4.4.1.1	Hemlig avlyssning av elektronisk kommunikation	80
4.4.1.2	Hemlig övervakning av elektronisk kommunikation	81
4.4.1.3	Hemlig kameraövervakning	82
4.4.1.4	Hemlig rumsavlyssning	82
5	ANALYS	84
5.1	Har hemlig dataavläsning utformats i enlighet med integritetsskyddet i gällande rätt?	84
5.2	Uppfyller lagstifningen kraven på processens kontradiktion och likställdhet i Europakonventionen?	87
5.3	Hur förhåller sig hemlig dataavläsning och dess inskränkningar till tidigare tvångsmedel?	90

5.4 Respekteras avvägningen mellan effektivitet och integritet vid införandet och tillståndsprovningen?	93
6 SLUTSATS	99
BILAGA A – REDOVISNING AV NYTTA	100
BILAGA B – ANTAL TILLSTÅND	101
KÄLL- OCH LITTERATURFÖRTECKNING	102
RÄTTSFALLSFÖRTECKNING	106

Summary

This essay will investigate the Swedish Act of 2020:62 Regarding Secret Reading of Data in an attempt to gain an understanding of the law itself as well as create a comparative and evaluative matrix to older acts concerning governmental coercive measure. By doing so, it will be possible to analyze the suitability of the act and the prioritization between effective crimefighting measures and privacy concerns brought into the limelight by the act's implementation into law.

In the interest of establishing a framework for the essay's research, introductory remarks will give an overview of current legal schemes in this area. Moreover, the protection of individual rights under Swedish national law as well as European Union law will be covered in addition to earlier national regulatory instruments for governmental coercive measures.

After establishing such a framework, this essay will then provide a thorough and detailed description of the Act of 2020:62 Regarding Secret Reading of Data. Through this process, the essay sets out to provide the reader with a deeper understanding of the act's repercussions on individual rights and freedoms and under what circumstances said act's provisions might take effect. In addition to the aforementioned, previous investigations into the matter and their evaluations will be presented.

This essay will present its content by taking on a critical perspective in viewing the crimefighting authorities' use of coercive measures. By presenting an evaluation of the use of coercive measures previous, as well as data over its usage under the year 2018 and the definition of the effectivity parameter, this essay sets out to create a baseline from which the usage of coercive measures as defined in this paper can be analyzed.

This essay will show how the Act of 2020:62 Regarding Secret Reading of Data to a high degree fulfills the demands put on regulatory instruments concerning coercive measures in a formal sense, as well as how protective measures to ensure compliance with Swedish rule of law – like the existence of certain restrictions – are adequate for the law’s purpose.

Questions regarding integrity concerns are by and large acknowledged and respected – something that deemed the act suitable to become a law in the first place – turns out to be a matter of adaptation, as investigatory exploration of the act shows serious shortcomings in the executory departments’ practice when undertaking actions supported by the act itself.

These shortcomings are evidential of the importance of protective measures to ensure compliance with Swedish rule of law, such as proper documentation and given notice to private parties and independent watchdogs. The lackluster protective measures in these cases demonstrates how such instruments of the law could be inclusive in theory whilst still enabling misuse of legal instruments by governmental entities.

Finally, this essay makes the case that the usage of coercive measures prior to the Act of 2020:62 Regarding Secret Reading of Data over time has transformed in such a way that central principles vis-à-vis coercive measures in fact carries little value as deterrents to those who would misappropriate said measures.

Whilst governmental departments claim that the efficiency to coercive measures has lessened, that claim does in fact not line up with attainable statistics, which rather seems to indicate a significant increase in the use of such measures.

By comparing these new coercive measures, as laid out in the aforementioned act of 2020:62, as well as how they are being applied, with older coercive measures, it can be deduced that they all but align – seeing that the new

measures are set to be subject to harsher curtailing than their predecessors. The conclusion to this essay will thus be that the act of 2020:62 – current restrictions notwithstanding – should not have been implemented into law.

Sammanfattning

Syftet med uppsatsen är att undersöka lagen (2020:62) om hemlig dataavläsning samt att jämföra den med tidigare tvångsmedelslagstiftningar och utvärdera tillämpningen av dem. Detta görs för att få möjlighet att analysera lagens lämplighet och den avvägning som lagen aktualiserar i dess införande och tillämpning, nämligen intresset av en effektiv brottsbekämpning å ena sidan och intresset av den personliga integriteten å andra sidan.

För att sätta ramarna för uppsatsens undersökningsområde ges inledningsvis en redogörelse för gällande rätt. Rättighetsskyddet enligt såväl nationell rätt som enligt europakonventionen redogörs för såväl som tidigare lagstiftning över hemliga tvångsmedel. Efter att en grund lagts för förståelsen av rättighetsskyddets omfattning i tvångsmedelssammanhang ges en genomgående och detaljerad beskrivning av lagen (2020:62) om hemlig dataavläsning. Detta görs i syfte att ge en djupare förståelse för dess ingrepp i individens rättigheter och under vilka förutsättningar dessa, genom lagens införande, numera tillåts. Även tidigare utredningars ståndpunkter och argument rörande hemlig dataavläsning presenteras.

I uppsatsen ges ett kritiskt perspektiv på de brottsbekämpande myndigheternas tvångsmedelsanvändning. Genom att presentera en granskning av användningen av tidigare tvångsmedel, redovisa data över tvångsmedelsanvändningen under 2018 samt undersöka effektivitetsbegreppets definition i sammanhanget, ges ett underlag från vilket tvångsmedelsanvändningen ur ett praktiskt perspektiv kan analyseras.

Uppsatsen visar att lagen i hög grad uppfyller de krav som rättighetsskyddet ställer på en tvångsmedelslagstiftning i formell mening och att rättssäkerhetsgarantierna i lagstiftningen, såsom restriktioner, vid en helt lagenligt tillämpning är tillräckliga. Frågan om integritetsintresset respekteras

och om lagen därmed är lämplig visar sig istället i stor utsträckning vara en tillämpningsfråga, där granskningar visar att allvarliga brister förekommer i de verkställande myndigheternas tillämpning av regelverket. Dessa brister visar vikten av rättssäkerhetsgarantier som dokumentation, underrättelser till enskilda och oberoende granskningsorgan, samt att dessa i formell mening kan vara heltäckande men i praktiken ändå kan missbrukas.

Uppsatsen redogör för data som visar att användningen av tidigare tvångsmedel över tid utvecklats i en riktning som tyder på att centrala principer för tvångsmedelsanvändning inte respekteras i praktiken. Samtidigt som verkställande myndigheter påstår att tvångsmedlens effektivitet har minskat, visar statistiken på en väsentligt ökad tvångsmedelsanvändning. Genom att sätta den jämföra den nya lagstiftningen med äldre tvångsmedel och dess tillämpning, då de nya mer ingripande åtgärderna ska ges striktare restriktioner, konstateras att de i allt väsentligt överensstämmer. Uppsatsens slutsats blir därför att lagen, med nuvarande restriktioner, inte borde ha införts.

Förord

Den nionde och sista terminen på Juristprogrammet har nått vägs ände. Denna uppsats har färdigställts med hjälp och stöd från en rad personer.

Tack till min handledare Sverker Jönsson för värdefulla synpunkter och konstruktiv kritik. Till Joacim Wallgren och Henrik Olsson Lilja med flera för råd och inspiration, såväl för detta arbete som för framtiden. Till Victor Ask, Ludvig Hambræus och Oliver Törn för korrekturläsning, språklig hjälp och nyttiga diskussioner.

Men framförallt till alla goda vänner, nya och gamla, som förgyllt de fyra senaste åren.

Avslutningsvis riktas ett stort tack till Daniel Lamac för brandtalen i skåpbilen mellan Borås och Skövde. Du vet vad jag menar.

Stockholm, maj 2020

Marcus Grudén

Förkortningar

EKMR	Europakonventionen
Prop.	Proposition
SIN	Säkerhets- och integritetsnämnden
Skr.	Skrivelse
SOU	Statens offentliga utredningar

1 Inledning

1.1 Bakgrund

Den 19 februari 2020 hördes en hätsk debatt i Sveriges riksdag mellan i huvudsak Liberalernas Johan Pehrsson och Vänsterpartiets Linda Westerholm Snecker. Debatten avsåg införandet av hemlig dataavläsning och i denna stundvis anklagande ordväxling representerade Pehrsson den till förslaget positiva majoriteten och Snecker minoriteten. Det var nämligen endast Vänsterpartiet som satte sig emot lagförslaget i sak. Efter debatten antogs lagförslaget med ett rungande ”ja”.¹

Det som samtliga debattörer var överens om var att införandet av hemlig dataavläsning innebar en balansgång mellan behovet av en effektiv brottsbekämpning och skyddet för den personliga integriteten.² Regeringen uttrycker det som att det integritetsintrång som hemliga tvångsmedel medför endast kan accepteras om det belagda behovet och nyttan av åtgärden är tillräckligt stora.³

Lag (2020:62) om hemlig dataavläsning har varit i kraft sedan den 1 april 2020 och gäller fram till den 31 mars 2025.

1.2 Syfte och frågeställningar

Syftet med uppsatsen är att utvärdera den nya lagstiftningen om hemlig dataavläsning utifrån avvägningen mellan intresset för en effektiv brottsbekämpning å ena sidan, och den enskildes grundlagsstadgade

¹ Prot. 2019/20:77 s. 71-74.

² Prot. 2019/20:77 s. 61-75.

³ Skr. 2019/20:56 s. 35.

rättigheter å andra sidan. De rättigheter som effektiviteten av hemlig dataavläsning ska vägas mot är skyddet för den enskildes personliga integritet och rätten till en rättvis rättegång. För att göra denna avvägning måste begreppet effektivitet definieras och rättighetsskyddens omfattning fastställas, båda i kontexten av hemlig tvångsmedelsanvändning.

Effektiviteten av hemlig dataavläsning kan endast uppskattas då tvångsmedlet när detta arbete färdigställs endast varit tillgängligt i knappt två månader. Genom att studera nyttan av den tidigare tvångsmedelsanvändningen, och hur denna har förhållit sig till rättighetsskyddet, kan en uppskattning av den nya lagens förmodade tillämpning i förhållande till rättighetsinskränkningen analyseras.

Konventioner och principer för användning av hemliga tvångsmedel ställer upp en rad krav på utformningen och tillämpningen av tvångsmedelslagstiftningar. Lagen analyseras därför med utgångspunkt i dessa krav.

Arbetets frågeställningar kan sammanställas i fyra frågeställningar:

- Har lagen om hemlig dataavläsning utformats i enlighet med integritetsskyddet i gällande rätt?
- Uppfyller lagstiftningen kraven på processens kontradiktion och likställdhet i Europakonventionen?
- Hur förhåller sig hemlig dataavläsning och dess rättighetsinskränkningar till tidigare tvångsmedel?
- Respekteras avvägningen mellan effektivitet och integritet vid införandet och tillståndsprövningar?

1.3 Avgränsningar

Arbetet avgränsas till att utvärdera lag (2020:62) om hemlig dataavläsnings utformning.

All data som redovisas över tvångsmedelsanvändningen finns inte utrymme här att analysera, varför arbetet avgränsas till att endast analysera den data som ansetts mest relevant i förhållande till arbetets syfte.

Arbetet syftar av utrymmesskäl inte heller till att beskriva de tekniska hinder för tillämpningen av hemlig dataavläsning som refereras till i arbetet.

1.4 Metod och material

Arbetet har i huvudsak präglats av en rättsdogmatisk metod men innehåller såväl en teoretisk som en kvalitativ del.

I den rättdogmatiska delen har de traditionella rättskällorna använts för att beskriva gällande rätt. Nationell lagstiftning om hemliga tvångsmedel har utvärderats utifrån en beskrivning av det nationella och internationella rättighetsskyddet bestående av lagar, förarbeten, konventioner, praxis och doktrin. Denna metod riktar sig på lagens faktiska utformning och dess teoretiska funktion vid en bokstavstrogen tillämpning, oberoende av den mänskliga faktorn.

I det teoretiska avsnittet har effektivitetsbegreppet i språklig mening definierats för att få en konkret avvägning att ta ställning till. I den kvalitativa delen har redovisad data över tvångsmedels nytta återgetts och satts i relation till effektivitetsbegreppet för att kvantitativt utvärdera tvångsmedelsanvändningen utifrån föreskrivna rättssäkerhetsgarantier. Detta har gjorts för att, till skillnad från den rättsdogmatiska delen, ge det praktiska perspektivet på lagens förhållande till rättssäkerheten i dess tillämpning.

Materialet som har använts har nästan uteslutande utgjorts av primärkällor, i andra fall har materialet publicerats av personer med en erkänd trovärdighet

på området. De viktigaste källorna för detta arbete är lagen om hemlig dataavläsning och dess förarbeten.

I uppsatsen syftar termen ”brottsbekämpande myndigheter” på Polismyndigheten, Åklagarmyndigheten, Säkerhetspolisen och Tullverket. Termerna målobjekt och målperson syftar på den utrustning respektive person som är föremål för övervakningen. Målperson kan avse en person som inte är misstänkt för brottet, men som på grund av sin koppling till den misstänkte övervakas.

1.5 Disposition

Uppsatsen har sex avsnitt. Inledningsvis ges i avsnitt två en kort redogörelse över tvångsmedelslagstiftningen som fanns innan lagen om hemlig dataavläsning trädde i kraft den 1 april 2020. Därefter följer en redogörelse över de nationella och internationella bestämmelser, principer och avgöranden som i tvångsmedelssammanhang är avsedda att skydda den enskildes rättighet och integritet.

I avsnitt tre ges en genomgående redogörelse för innehållet i den nya lagstiftningen om hemlig dataavläsning. De brottsbekämpande myndigheternas uttryckta behov av hemlig dataavläsning förklaras och slutsatser från tidigare utredningar som behandlat detta behov redogörs för.

I nästföljande avsnitt fyra återges delar ur Säkerhets- och integritetsskyddsnämndens granskning av de brottsbekämpande myndigheternas användning av tvångsmedel. Därefter följer en genomgång av effektivitetsbegreppet och avsnittet avslutas med en redogörelse för den av regeringen redovisade nyttan av tvångsmedelsanvändning under 2018.

Uppsatsen avslutas med avsnitt fem och sex, i vilka materialet analyseras och en sammanfattande slutsats ges.

2 Gällande rätt

För att få möjlighet sätta den nya lagen och det nya hemliga tvångsmedlet som detta arbete avser i ett sammanhang fordras en översiktlig genomgång av för ämnet relevant gällande rätt. För att utvärdera lagen krävs en förståelse för den enskildes personliga integritet enligt såväl nationell som internationell rätt. Vidare krävs en förståelse för vilka hemliga tvångsmedel som, före lagändringens ikraftträdande, tilläts och därmed hur avvägningen mellan integriteten och tvångsmedlens ingrepp i den samma gjordes tidigare.

2.1 Äldre hemliga tvångsmedel

Straffprocessuella tvångsmedel är en typ av åtgärder som har en funktion inom straffprocessen men som inte är straff eller andra sanktioner. De utgör en form av myndighetsutövning som innebär ett intrång i individens rättssfär. Tvångsmedelsanvändningen riktar sig i regel mot person eller egendom.⁴

Användningen av hemliga tvångsmedel inbegriper oftast inget tvång, eftersom en grundförutsättning för dess effektivitet givetvis är att målpersonen inte känner till att han är föremål för åtgärden. Det skiljer de hemliga tvångsmedlen från övriga straffprocessuella tvångsmedel. Mot bakgrund av de avsevärda intrång i målpersonens personliga integritet som de medför betecknas de dock ändå som tvångsmedel.⁵

2.1.1 Hemlig avlyssning av elektronisk

⁴ Lindberg (2018), s. 5, Ekelöf m.fl. (2006), s. 38 f.

⁵ Ekelöf m.fl. (2006), s. 42.

kommunikation

Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel. Med ett elektroniskt kommunikationsnät menas ett system för överföring och i vissa fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs.⁶ Begreppet adress omfattar nummer, till exempel telefonnummer, och andra identifikationsnummer och adresser, som till exempel mejladresser.⁷

Hemlig avlyssning får tillämpas på alla former av kommunikation genom elektroniska kommunikationsnät och kan tillämpas på muntlig, skriftlig och datakommunikation.⁸ Tillstånd till hemlig avlyssning får lämnas vid misstanke om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, för vissa särskilt uppräknade brott som framför allt Säkerhetspolisen utreder eller om det i ett enskilt fall kan antas att brottets straffvärde överstiger fängelse i två år. Under en förundersökning krävs för att få tillstånd till hemlig avlyssning att misstankegraden når upp till skäligen misstänkt för ett brott.⁹

Hemlig avlyssning får enligt preventivlagen¹⁰ i vissa fall tillåtas i underrättelseverksamhet, till exempel om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva sådan brottslig verksamhet som nämns i lagrummet, såsom till exempel mord,

⁶ 1 kap 7 § lag (2003:389) om elektronisk kommunikation.

⁷ Prop. 2011/12:55 s. 62.

⁸ Prop. 2019/20:64 s. 37.

⁹ 27 kap 18 § rättegångsbalken.

¹⁰ Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

mordbrand eller terroristbrott. Tillstånd får även beviljas utom förundersökning vid särskild utlänningskontroll om tillståndet är av betydelse för att utreda om en person eller grupp planlägger eller förbereder terroristbrott och det finns synnerliga skäl för att misstänka det.¹¹

Under såväl förundersökning som i underrättelseverksamhet får den hemliga avlyssningen avse ett telefonnummer eller annan adress som, under tillståndstiden, innehas eller har innehafts av den misstänkte eller som annars kan antas ha använts eller komma att användas av personen.¹² Åtgärden får även avse ett nummer eller annan adress som det finns synnerlig anledning att anta att personen, under tillståndstiden, har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta.¹³

När en myndighet fått tillstånd till hemlig avlyssning av elektronisk kommunikation får de använda de tekniska hjälpmedel som behövs för åtgärden.¹⁴ Det innebär att polisen utöver traditionell avlyssningsutrustning även får använda annan hårdvara och programvara för att verkställa beslutet om hemlig avlyssning.¹⁵

2.1.2 Hemlig övervakning av elektronisk kommunikation

Vid hemlig övervakning av elektronisk kommunikation hämtas i hemlighet uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress. Uppgifterna ger information om vilka elektroniska

¹¹ 2 § lag (2003:148) om straff för terroristbrott, 19-20 §§ lag (1991:572) om särskild utlänningskontroll.

¹² Prop. 2019/20:64 s. 38.

¹³ 27 kap 20 § första stycket rättegångsbalken, 2 § preventivlagen.

¹⁴ 27 kap 25 § första stycket rättegångsbalken, 9 § preventivlagen.

¹⁵ Prop. 1994/95:227 s. 29.

kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.¹⁶

Myndigheterna kan även genom tvångsmedlet hindra meddelanden från att nå fram till mottagaren.¹⁷ Informationen ger tillgång till trafikuppgifter och uppgifter om lokalisering av kommunikationsutrustningen, till skillnad från hemlig data avlyssning, som ger tillgång till uppgifter om innehållet i kommunikationen.¹⁸

De förundersökningsfall där tillstånd för hemlig övervakning av elektronisk kommunikation kan ges är vid brott med ett minimistraff om fängelse i sex månader, för vissa särskilt uppräknade brott som framför allt Polismyndigheten utreder, som t.ex. dataintrång, narkotikabrott och icke ringa barnpornografibrott, och för vissa särskilt uppräknade brott som framför allt Säkerhetspolisen utreder.¹⁹

I förundersökningsfallen får åtgärden tillåtas om någon är skäligen misstänkt för brott och om åtgärden avser de telefonnummer eller adresser som gäller vid hemlig avlyssning. Tillstånd kan även ges i syfte att utreda vem som skäligen kan misstänkas för brottet, dock endast om det för brottet även kan tillåtas hemlig avlyssning av elektronisk kommunikation. Det krävs vidare att åtgärden är av synnerlig vikt för utredningen samt att övervakningen som innebär att uppgifter hämtas in om meddelanden endast får avse förfluten tid.

20

¹⁶ Prop. 2019/20:64 s. 38.

¹⁷ 27 kap 19 § andra stycket rättegångsbalken.

¹⁸ Prop. 2019/20:64 s. 38.

¹⁹ 27 kap 19 § tredje stycket rättegångsbalken.

²⁰ 27 kap 19 § fjärde stycket rättegångsbalken, 27 kap 20 § andra stycket rättegångsbalken.

Hemlig övervakning av elektronisk kommunikation får användas under samma förutsättningar som hemlig avlyssning i fall som lyder under preventivlagen samt lagen om särskild utlänningskontroll. Det gäller såväl beträffande vilken brottslighet som krävs som för vilka telefonnummer eller adresser som får övervakas, samt att samtliga tekniska hjälpmedel som behövs för åtgärden får användas.²¹

2.1.2.1 Inhämtning av elektronisk kommunikation i underrättelseverksamhet

Polismyndigheten, Säkerhetspolisen och Tullverket får under vissa förutsättningar inhämta övervakningsuppgifter om elektronisk kommunikation från teleoperatörer. Dessa förutsättningar återfinns i den s.k. inhämtningslagen.²² Uppgifterna som får inhämtas enligt lagen är desamma som får inhämtas när hemlig övervakning av elektronisk kommunikation används för att utreda vem som skäligen kan misstänkas för det brott som utreds. Uppgifterna får inhämtas om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott med ett minimistraff om fängelse i två år, eller om det gäller någon av de i paragrafen särskilt angivna brotten som utreds av Säkerhetspolisen.²³

Uppgifterna får dock bara inhämtas om skälen för det uppväger det intrång eller men i övrigt som åtgärden innebär för målpersonen eller för något annat motstående intresse.²⁴

²¹ Prop. 2019/20:64 s. 39.

²² Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

²³ 2 § första stycket inhämtningslagen.

²⁴ 2 § andra stycket inhämtningslagen.

2.1.3 Hemlig kameraövervakning

Vid hemlig kameraövervakning får fjärrstyrda tv-kameror, andra optisk-elektroniska instrument eller därmed jämförbar utrustning användas för optisk personövervakning vid förundersökning i brottmål utan målpersonens eller andras vetskap.²⁵ Hemlig kameraövervakning omfattar inte ljudupptagning.²⁶

Den brottslighet som kan motivera tillstånd till hemlig kameraövervakning kan i förundersökningsfallen är densamma som för tillstånd till hemlig avlyssning av elektronisk kommunikation.²⁷ Övervakningen får som huvudregel endast användas om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får vidare, som huvudregel, endast avse sådan plats där den misstänkte kan antas²⁸ komma att uppehålla sig.²⁹ Hemlig kameraövervakning kan dock, om det inte finns någon skäligen misstänkt för brottet, även användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till platsen om syftet är att fastställa vem som skäligen kan misstänkas för brottet.³⁰

Hemlig kameraövervakning får inte användas inom ramen lagen för särskild utlänningskontroll. Enligt preventivlagen får hemlig kameraövervakning användas för brott som motsvarar de brott som gäller för hemlig avlyssning av elektronisk kommunikation.³¹ Åtgärden får endast avse en plats där den målpersonen kan antas³² komma att uppehålla sig eller en plats där den

²⁵ 27 kap 20 a § rättegångsbalken.

²⁶ Prop. 1995/96:85 s. 37.

²⁷ 27 kap 20 a § andra stycket rättegångsbalken.

²⁸ Se avsnitt 3.4.2.3.

²⁹ 27 kap 20 b § rättegångsbalken.

³⁰ 27 kap 20 c § rättegångsbalken.

³¹ 1 § preventivlagen.

³² Se avsnitt 3.4.2.3.

brottsliga verksamheten kan antas komma att utövas eller en nära omgivning till denna plats.³³

2.1.4 Hemlig rumsavlyssning

Hemlig rumsavlyssning innebär en avlyssning eller upptagning som görs i hemlighet och är avsett att återge ljud. Avlyssningen sker med ett tekniskt hjälpmedel och avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.³⁴

Vid förundersökning får hemlig rumsavlyssning användas vid brott med ett minimistraff om fängelse fyra år, eller vid spioneri, vissa brott enligt lagen (2018:558) om företagshemligheter, eller andra i paragrafen uppräknade brott, som till exempel människohandel, våldtäkt och grovt narkotikabrott, om det i det enskilda fallet kan antas att brottets straffvärde är högre än fängelse i fyra år.³⁵

Hemlig rumsavlyssning får endast användas om någon är skäligen misstänkt för något av de ovan uppräknade brotten och om det är av synnerlig vikt för utredningen.³⁶ Även en plats där det finns anledning att anta att den misstänkte kommer att uppehålla sig på kan bli föremål för hemlig rumsavlyssning. Om det inte avser den misstänktes bostad får hemlig rumsavlyssning användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.³⁷ Tvångsmedlet får inte användas i underrättelseverksamhet.³⁸

³³ 3 § preventivlagen.

³⁴ 27 kap 20 d § rättegångsbalken.

³⁵ 27 kap 20 d § andra stycket rättegångsbalken.

³⁶ 27 kap 20 e § första stycket rättegångsbalken.

³⁷ 27 kap 20 e § andra stycket rättegångsbalken.

³⁸ Prop. 2019/20:64 s. 40.

2.2 Nationellt skydd för den personliga integriteten

2.2.1 Lag

Bestämmelsen i 1 kap 2 § regeringsformen stadgar att den offentliga makten ska utövas med respekt för alla människors lika värde och den enskilda människans frihet och värdighet, samt att det allmänna ska värna den enskildes privat- och familjeliv.

Var och en är enligt 2 kap 6 § första stycket regeringsformen gentemot det allmänna skyddad mot bl.a. husrannsakan och liknande intrång, undersökning av brev eller annan förtrolig försändelse och hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Enligt paragrafens andra stycke åtnjuter den enskilde ett skydd mot betydande intrång i den personliga integriteten från det allmänna, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Det skydd som stadgas i 2 kap 6 § kan endast begränsas genom lag. Rent allmänt kan sägas att vid användning av tvångsmedel blir det i regel fråga om intrång i den enskildes grundläggande fri- och rättigheter.³⁹ Av 2 kap 21 § framgår att en rad allmänna principer ska beaktas vid inskränkningar av de relativa friheterna. Begränsningen ska tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den eller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Vidare får begränsningen inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan livsåskådning. Förbudet mot åsiktsdiskriminering gäller bara vid inskränkningar av de relativa rättigheterna, detta förbud har inte

³⁹ Ekelöf m.fl. (2006), s. 46.

samma vidsträckta tillämpningsområde som förbuden mot diskriminering i 2 kap 12 och 13 §§ regeringsformen.⁴⁰

2.2.2 Principer för användning av tvångsmedel

Vid beslut om, och tillämpning av, alla hemliga tvångsmedel gäller tre allmänna principer. De principerna är ändamålsprincipen, behovsprincipen och proportionalitetsprincipen.⁴¹ I sammanhanget kan även legalitetsprincipen nämnas, då även den är central för all tvångsmedelsanvändning då en inskränkning av individens rättigheter ska anges i lag.

2.2.2.1 Legalitetsprincipen

Lagtexten för användning av tvångsmedel bör innehålla en tydlig definition av ändamålet med tvångsmedlet för att förhindra godtyckligt åsidosättande av individens rättigheter. Reglernas utformning bör även präglas av tydlighet. Att reglerna så långt som möjligt saknar vaga, obestämda och mångtydiga rekvisit samt att tillämpningen förblir förutsebar och återhållsam tjänar som skydd för den allmänna rättssäkerheten i samhället.⁴²

2.2.2.2 Ändamålsprincipen

Principen innebär att det i varje regel om tvångsmedel uttryckligen måste anges för vilket ändamål tvångsmedlet får användas.⁴³ Att ange ändamålet är nödvändigt av två anledningar. Dels för att lagstiftaren i varje enskilt fall ska kunna ta ställning till om begränsningen av det aktuella rättighetsskyddet är förenlig med grundlagsskyddet, dels för att den tillämpande myndigheten ska

⁴⁰ Strömberg, Lundell (2016), s. 106.

⁴¹ Prop. 2019/20:64 s. 35.

⁴² Ekelöf m.fl. (2006), s. 47, Ehrenkrona (2016), s. 110.

⁴³ SOU 1984:54 s. 76.

kunna förstå i vilket syfte tvångsmedlet tillåtits av lagstiftaren. Om den tillämpande myndigheten inte uppfattar det skulle det kunna bli mycket svårt att avgöra om tillämpningen av tvångsmedlet är grundlagsenlig eller inte.⁴⁴

Ändamålsprövningen bör enligt förarbeten ske före behovs- och proportionalitetsbedömningen. Det spelar ingen roll om det finns ett stort behov och åtgärden anses vara proportionerligt om tvångsmedlet inte ska användas för det syfte det är till för.⁴⁵

2.2.2.3 Behovsprincipen

Behovsprincipen innebär att ett tvångsmedel bara får användas om uppgiften inte kan lösas utan att tvånget eller tvångsmedlet utnyttjas. Tvånget ska vara både nödvändigt för att syftet uppnås och verkningsfullt, alltså att det avsedda resultatet uppnås. Principen medför även att om tvångsmedel är nödvändigt för att uppnå syftet ska den minst ingripande metoden väljas samt att när syftet uppnåtts eller om åtgärden inte längre förväntas uppfylla syftet, ska tvångsåtgärden omedelbart avbrytas.⁴⁶ Åtgärder som har som huvudsakliga syfte att enbart underlätta polisens arbete anses bryta mot behovsprincipen.⁴⁷

2.2.2.4 Proportionalitetsprincipen

Proportionalitetsprincipen innebär att de negativa skadeverkningar som användningen av ett tvångsmedel medför för målpersonen eller tredjeman, ska stå i rimlig proportion till myndigheternas vinning med användningen. Ett tvångsmedel får användas endast om skälet för användningen väger upp det intrång som användandet innebär för målpersonen eller något annat till åtgärden motstående intresse. En tillämpning av principen vid till exempel häktning medför att om en person kan förväntas endast bli tilldömd

⁴⁴ Ekelöf m.fl. (2006), s. 47 f.

⁴⁵ SOU 2017:75 s. 91.

⁴⁶ Ekelöf m.fl. (2006), s. 48.

⁴⁷ SOU 2017:75 s. 91.

skyddstillsyn som påföljd häktas den misstänkte i vissa fall inte, på grund av den inskränkning av hans frihet som åtgärden skulle innebära.⁴⁸

Vid proportionalitetsavvägningen anses ingrepp som endast avser egendom eller ekonomiska intressen som mindre allvarliga än de som avser kränkningar av en persons frihet och integritet. Bedömningen innehåller överväganden kring vilket tvångsmedel som ska användas, hur åtgärden ska genomföras, och hur länge åtgärden ska användas i förhållande till det resultat som förväntas.⁴⁹

2.3 Europakonventionen

Lag eller annan föreskrift får enligt 2 kap 19 § regeringsformen inte meddelas i strid med Sveriges åtaganden på grund av den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Europakonventionen gäller som svensk lag, varför de för ämnet relevanta rättigheterna enligt konventionen och dess tillhörande praxis är av avgörande betydelse för tillämpningen av hemliga tvångsmedel.

2.3.1 Integritetsskyddet i artikel 8

Av artikel 8 i EKMR följer att myndigheterna har en skyldighet att respektera varje individs privat- och familjeliv, hem och korrespondens. Rätten till respekt skyddar i första hand individen från godtycklig inblandning från myndigheterna.⁵⁰ Skyddet för privatlivet är tämligen allmänt hållet och skyddar bland annat rätten att etablera och utveckla relationer med andra

⁴⁸ SOU 1984:54 s. 78, Ekelöf m.fl. (2006), s. 48 f.

⁴⁹ Ekelöf m.fl. (2006), s. 49.

⁵⁰ Ehrenkrona (2016), s. 110.

människor och omvärlden.⁵¹ Korrespondens kan definieras som meddelanden mellan individer genom någon form av överföring. Det kan röra sig om brev, överförande av meddelanden med hjälp av telefon, telefax, radio och datorer. Det uttryckliga skyddet för individens korrespondens medför därmed att hemliga tvångsmedel som telefonavlyssning, brev- och e-postkontroll som huvudregel förbjuds enligt Europakonventionen.⁵²

Precis som för en inskränkning i skyddet i regeringsformen kan rättigheten i artikel 8(2) EKMR endast inskränkas genom lag. Inskränkningen måste vidare vara nödvändig i ett demokratiskt samhälle med hänsyn till, och ägnad att tillgodose, något av de allmänna eller enskilda intressen som räknas upp i artikel 8(2) EKMR. De intressen som räknas upp är till exempel den nationella och allmänna säkerheten, förebyggande av oordning eller brott samt skyddet för hälsa eller andra personers fri- och rättigheter. Nödvändighetskravet i artikel 8(2) kan sägas innebära att det måste finnas ett angeläget samhällsligt behov av ingreppet, samtidigt som det måste stå i proportion till det syfte som skall tillgodoses av ingreppet.⁵³

2.3.2 Rättvis rättegång enligt artikel 6

I artikel 6 EKMR stadgas skyddet för varje misstänkts rätt till en rättvis rättegång. Artikeln medför en grundläggande princip om att varje tilltalad har rätt att bli hörd av domstol. Den tilltalade har en rätt att framföra det han har att säga till stöd för sina ståndpunkter och försöka övertyga domstolen om sin rätt i saken. En eventuell kränkning av rättigheten ska bedömas mot bakgrund av processens helhet, vilket följer av att en felaktighet i en förundersökning eller underrätt givetvis kan rättas i en högre instans, eller om en tilltalad frias och därför inte längre är föremål för processen. Om en felaktighet ska kunna rättas i en högre rätt krävs det att omprövning blir tillräckligt omfattande för

⁵¹ Danelius (2015), s. 432.

⁵² Ibid.

⁵³ Danelius (2015), s. 369 f.

att felet ska kunna rättas och att den tilltalade ges möjlighet att föra bevisning om felet i den högre instansen.⁵⁴

En brottmålsprocess ska grundas på presumptionen att den tilltalade är oskyldig tills motsatsen bevisats och för att denna princip ska få någon praktisk verkan måste den tilltalades ges de rättigheter som är nödvändiga för att han ska kunna försvara sig på ett fullgott sätt. Den rättvisa rättegången ska vidare säkras genom principen om parternas likställdhet och principen om ett kontradiktoriskt förfarande. I brottmål medför principen om parternas likställdhet inte att den tilltalade och åklagaren ska ges samma processuella rättigheter men den tilltalade får inte ha sämre möjligheter att framföra sin talan inför domstolen.⁵⁵ Principen hindrar inte att den tilltalade ges en mer gynnsam ställning, till exempel genom principen om ”in dubio pro reo” som medför att tveksamheter bör tolkas till den tilltalades fördel. Åklagaren ges därmed också bevisbördan. Den kontradiktoriska principen är tätt förknippad med likställighetsprincipen och syftar till att garantera att båda parter får kännedom om allt material i processen och ges tillfälle att yttra sig över materialet. Den syftar även till att försäkra att den tilltalade har lika goda möjligheter, som sin motpart, att åberopa bevisning och föra sin talan i processen.⁵⁶

Vid användning av hemliga tvångsmedel finns det vissa oklarheter kring artikelns tillämplighet, men den blir i vart fall av intresse när överskottsinformation från hemliga tvångsmedel eller uppgifter som inhämtats genom olagliga övervakningsåtgärder åberopas som bevis i en rättegång.⁵⁷

⁵⁴ Danelius (2015), s. 259 f.

⁵⁵ Danelius (2015), s. 260.

⁵⁶ Ibid.

⁵⁷ SOU 2018:61 s. 76.

I Europadomstolens praxis har intrångets karaktär varit avgörande för bedömningen om den utgör en kränkning av artikel 6. Till exempel har det varit avgörande om den tilltalade i ett mål har haft möjlighet att ifrågasätta tillförlitligheten i en inspelning genom hemlig teleavlyssning varit av stor betydelse för bedömningen. Andra exempel är om den tilltalade och hans försvarare har haft möjlighet att höra ansvarig polis om olagligt inhämtade bevis när just det beviset varit det enda som legat till grund för fällande dom, om det finns en risk att beviset inte är tillförlitligt genom att det t.ex. inte är det tilltalades röst som hörs i inspelningen, och om avlyssningen är olaglig eller om det bara inte finns nationellt lagstöd för åtgärden.⁵⁸

2.3.3 Användning av hemliga tvångsmedel i Europadomstolens praxis

I målet *Roman Zakharov mot Ryssland* prövades huruvida en nationell reglering som innebar att ryska telefonoperatörer gavs en laglig skyldighet att installera utrustning som möjliggjorde telefonavlyssning av enskilda utan att beslut behövde inhämtas av någon judiciell instans. Mot bakgrund av att landet saknade en tydlig rättslig reglering av den avlyssning som möjliggjordes samt att inga effektiva rättsmedel mot åtgärden fanns ansåg domstolen att regleringen bröt mot artikel 8 i Europakonventionen.⁵⁹ I målet ställde domstolen upp ett antal rättssäkerhetskriterier som hemlig tvångsmedelslagstiftning bör innehålla för att minska missbruk. Denna praxis sammanfattas som att det i lag ska föreskrivas:

- Brottsstypen som kan leda till ett avlyssningsbeslut,
- En definition av personkategorin som riskerar att bli föremål för avlyssning,

⁵⁸ Se *Khan mot Förenade Kungariket, P.G. och J.H. mot Förenade Kungariket* nedan i avsnitt 2.3.3.

⁵⁹ Ehrenkrona (2016), s. 126, *Zakharov mot Ryssland*, nr. 47143/06, Europadomstolens dom den 4 december 2015, p. 305.

- En begränsning av telefonavlyssningens varaktighet,
- Rutiner som ska följas vid undersökning och användning samt lagring erhållna data,
- Gällande försiktighetsmått vid utlämnande av data till andra parter, samt
- Omständigheter där inspelningar kan eller måste raderas eller förstöras.⁶⁰

Avgörandet *Klass m.fl. mot Tyskland* ingår i den praxis som domstolen sammanfattade i *Roman Zakharov mot Ryssland*. Domstolen ansåg att artikel 8(2) EKMR ger utrymme att använda hemliga tvångsmedel när det är nödvändigt för att skydda det demokratiska systemet. Mot bakgrund av de allt mer avancerade former av spionage och terroristrelaterad verksamhet som samhället hade att skydda sig mot, ansåg domstolen att staters användning av hemliga tvångsmedel var motiverad, under förutsättning att en effektiv kontroll mot missbruk fanns att tillgå.⁶¹

I målet *Uzun mot Tyskland* ansåg domstolen inte att rättigheten i artikel 8 hade kränkts när en GPS-sändare installerades i en bil för att följa en terrorismstänkt persons rörelser. Domstolen ansåg att åtgärden var motiverad eftersom att åtgärden hade stöd i tysk lag, att det var ett tungt vägande intresse att hindra allvarliga brott, att andra mindre inskränkande metoder hade prövats samt att övervakningen endast pågick under en kortare tid. Av avgörandet följer även att bestämmelser om åtgärder som innebär ett större intrång i den personliga integriteten bör föreskrivas med en större tydlighet och innehålla fler restriktioner än de som innebär mindre intrång.⁶²

⁶⁰ Zakharov mot Ryssland, nr. 47143/06, Europadomstolens dom den 4 december 2015, p. 231.

⁶¹ Klass m.fl. mot Tyskland, nr. 5029/71, Europadomstolens dom 6 september 1978, p. 48-50.

⁶² Uzun mot Tyskland, nr. 35623/05, Europadomstolens dom den 2 september 2010, 43-48.

Avgörandet *Association for European Integration and Human Rights och Ekimdzhev mot Bulgarien* gällde en bulgarisk lag om hemlig övervakning. Lagen innehöll regler om användning av tekniska medel för fotografering och upptagning av ljud och bild. Domstolen underkände lagen eftersom att den inte innefattade något oberoende organ som övervakade dess tillämpning. Det gavs inte heller någon underrättelse i efterhand till den som utsattes för en sådan övervakning, varför domstolen ansåg att rättigheten i artikel 8 kränkts.⁶³ Det kan nämnas att domstolen i *Kennedy mot Förenade kungariket* angett att information om åtgärden i efterhand inte alltid måste ges, under förutsättning att det finns en effektiv kontroll av åtgärden.⁶⁴

I avgörandet *Khan mot Förenade Kungariket* hade en person blivit föremål för en hemlig avlyssning, för vilken det inte fanns något nationellt lagstöd. I den senare rättegången kom uppgifter från denna avlyssning att utgöra den enda bevisningen mot den tilltalade. Med hänvisning till bl.a. att bevisningen med hänsyn till omständigheterna var stark och tillförlitlig och att den centrala frågan var om rättegången som helhet kunde anses rättvis, ansåg domstolen att artikel 6 inte hade kränkts. Särskilt framfördes att den tilltalade hade getts fullgoda möjligheter att ifrågasätta äktheten av upptagningen.⁶⁵

Avgörandet *P.G. och J.H. mot Förenade Kungariket* avsåg en avlyssningsanordning som placerades i B:s lägenhet efter att uppgifter hade framkommit som tydde på att P.G. och J.H. planerade ett väpnat rån. När de både hade arresterats på grund av de upptagningar som gjordes i lägenheten vägrade det samarbeta och låta polisen spela in röstprov för att jämföra med upptagningarna. Polisen spelade då in deras röster genom inspelningsutrustning som installerades i deras celler och på polisernas

⁶³ *Association for European Integration and Human Rights och Ekimdzhev mot Bulgarien*, nr. 62540/00, Europadomstolens dom den 28 juni 2007, p. 91-94.

⁶⁴ *Kennedy mot Förenade kungariket*, nr. 26839/05, Europadomstolens dom den 18 maj 2010, p. 153.

⁶⁵ *Khan mot Förenade Kungariket*, nr. 35394/97, Europadomstolens dom den 12 maj 2000, p. 34-40.

kläder. Domstolen fann att avlyssningen i B:s lägenhet stred mot artikel 8 eftersom att den gjord utan lagstöd samt att den dolda övervakningen i polisens lokaler saknade lagstöd, varför även den stred mot artikel 8. Domslutet fastslog dock att det inte hade varit fråga om en kränkning enligt artikel 6. Avgörandet visar att rättegången som helhet fortfarande kan vara rättvis, även om en artikel kränkts i processen.⁶⁶

I avgörandet *Natunen mot Finland* var det fråga om hemlig avlyssning av en person. En del av de samtal som spelades in åberopades av åklagaren till styrkande av att Natunen var inblandad i en narkotikaaffär. När Natunens ärende skulle upp i hovrätten begärde han och hans försvarare att få del av alla de inspelningar som fanns, inte bara de som åklagaren åberopat, eftersom att de skulle bevisa att samtalen inte rörde narkotika. Då visade det sig att polisen hade destruerat alla inspelningar förutom de som åberopats som bevisning. Enligt nationell lagstiftning var det inte tillåtet att behålla inspelningar som inte avsåg brottslig verksamhet, varpå resterande inspelningar hade destruerats då de inte bedömdes handla om någon brottslig verksamhet. Europadomstolen ansåg att det inte var förenligt med rätten till en rättvis rättegång enligt artikel 6 att polisen, ens i samråd med åklagaren, ska få bedöma vilket material som är relevant och inte, utan något samråd med den tilltalade eller hans försvarare.⁶⁷

Domstolen anförde dock i *Natunen mot Finland* att det kan förekomma motstående intressen inom ramen för en brottmålsprocess, och att den tilltalades rätt till insyn i vissa fall kan inskränkas om det är strikt nödvändigt för att tillgodose någon annans grundläggande rättigheter. Som exempel angav domstolen att ett sådant inskränkande kan ske för att skydda nationell säkerhet, skydda vittnen eller hemlighålla polisens metoder. Om den

⁶⁶ P.G. och J.H. mot Förenade Kungariket, nr. 44787/98, Europadomstolens dom den 25 september 2001, p. 76-81.

⁶⁷ *Natunen mot Finland*, nr. 21022/04, Europadomstolens dom 31 mars 2009, p. 39. Se även *Janatuinen mot Finland*, nr. 28552/05, Europadomstolens dom 8 december 2009.

tilltalades rätt inskränks ska det balanseras upp till hans fördel för att säkra att han får en rättvis rättegång.⁶⁸

⁶⁸ Natunen mot Finland, nr. 21022/04, Europadomstolens dom 31 mars 2009, p. 40.

3 Lag (2020:62) om hemlig dataavläsning

Hemlig dataavläsning innebär att brottsbekämpande myndigheter får en möjlighet att med hjälp av ett tekniskt hjälpmedel ta del av innehållet i en dator eller annan teknisk utrustning som kan användas för kommunikation och på så vis få reda på hur utrustningen används eller har använts och vilken information som finns i den.⁶⁹ Tvångsmedlet möjliggör till exempel att myndigheterna i större utsträckning kan avlyssna telefon-, mejl- och internettrafik samt aktivera funktioner i målpersonens tekniska utrustning såsom kameror, GPS-funktioner och mikrofoner.

3.1 Behovet av nya verktyg

I dagens teknologiska samhälle ökar IT-relaterad brottslighet och traditionell brottslighet tar sig allt mer in i IT-miljön.⁷⁰ Mobilapplikationer krypterar och anonymiserar meddelanden och krypterade internetnätverk används för att t.ex. lagra barnpornografiskt material eller handla med narkotika med hjälp av anonymiserade IP-adresser och kryptovalutor.⁷¹ Den tekniska expertis och de digitala verktyg som krävs försvårar utredningarna och minskar chanserna att hitta förövarna.⁷² Samtidigt har rättsväsendet svårt att anpassa sig efter den tekniska utvecklingen, som exempel kan nämnas att Brå 2016 redovisade statistik⁷³ som visade att över hälften av åklagarna och nio av tio av polisens förundersökningsledare helt saknade vidareutbildning inom IT-brottslighet.

⁶⁹ SOU 2005:38 s. 50.

⁷⁰ Brå 2016:17 s. 7.

⁷¹ Prop. 2019/20:64 s. 64.

⁷² IOCTA 2017 s. 35.

⁷³ Brå 2016:17 s. 9.

Därtill gör sofistikerade krypterings- och anonymiseringstjänster, enligt brottsbekämpande myndigheter, många av de befintliga hemliga tvångsmedlen i vissa fall verkningslösa. De uppgifter som ska inhämtas vid den hemliga dataavläsningen är dock i allt väsentligt densamma som kan inhämtas genom befintliga hemliga tvångsmedel, men som utredaren på grund av krypteringen och anonymiseringen i många fall inte kan få tillgång till.⁷⁴

3.1.1 Kryptering

När en brottsbekämpande myndighet erhåller ett tillstånd till hemlig avlyssning av en viss elektronisk kommunikation får de rätt att ta del av innehållet i kommunikationen de ska avlyssna. Om den brottsmisstänkte använder ett datorprogram eller en mobilapplikation som krypterar kommunikationen kan utredarna inte ta del av innehållet i klartext vilket blir ett hinder för utredaren. De utredningstekniska svårigheter som krypteringen skulle komma att medföra kunde förutses redan för 15 år sedan.⁷⁵ Det är dock först under de senare åren som problemet växt sig större då krypteringstjänsterna blivit allt vanligare, i synnerhet bland kriminella.⁷⁶

Krypteringstjänster används dagligen av vanligt folk, de flesta vet troligtvis inte ens om att deras mobilapplikationer krypterar deras information. Som exempel kan nämnas mobilapplikationer som Messenger, Whatsapp och Instagram (Facebook), Gmail (Google) och Imessage (Apple). Dessa applikationer krypterar kommunikationen och ser till att utomstående inte kan ta del av den. Krypteringens syfte är till övervägande del att möjliggöra en säker kommunikation mellan vanliga människor.⁷⁷ Även operativsystem i

⁷⁴ Prop. 2019/20:64 s. 69.

⁷⁵ SOU 2005:38 s. 50.

⁷⁶ Prop. 2019/20:64 s. 67.

⁷⁷ Prop. 2019/20:64 s. 66.

datorer och mobiltelefoner har inbyggda krypteringssystem likväl som servrar och mängder av annan teknisk utrustning. Fördelen med krypteringen är till exempel att en mobiltjuv inte får tillgång till informationen i den stulna mobiltelefonen eftersom tjuven inte kan koden för att låsa upp den. Krypteringens baksida är alltså de svårigheter som de brottsbekämpande myndigheterna stöter på när de till exempel beslagtar en mobiltelefon för att kunna bevisa att narkotikahandel bedrivits mellan två misstänkta personer genom exempelvis Messenger-konversationer.⁷⁸

Idag är mer än 90 procent av den avlyssnade internettrafiken krypterad menar Polismyndigheten. Det innebär att myndigheterna enligt egen utsago endast kan läsa av mindre än tio procent av den datakommunikation som får avlyssnas eller övervakas.⁷⁹ I många typer av utrustning arbetar den misstänkte med informationen öppet innan den sparas och i många fall krypteras. Ett införande av hemlig dataavläsning skulle ge myndigheterna möjligheten att ta del av informationen när den fortfarande bearbetas öppet och på så sätt säkra bevisning innan ett eventuellt beslag eller liknande.⁸⁰

3.1.2 Anonymisering

Krypteringen begränsar utredarens möjligheter att tillgodogöra sig innehållet i den brottsmisstänktes kommunikation. Anonymiseringen begränsar istället möjligheterna att fastställa identiteten på den vars kommunikation man är intresserad av. För en person som önskar dölja sin aktivitet på internet finns en mängd tjänster vilket ger upphov till stora svårigheter i såväl utrednings- som i bevishänseende då en persons kontakter ska dokumenteras.⁸¹ Ett exempel på en avancerad anonymiseringstjänst är internetnätverket Darknet,

⁷⁸ Brå 2016:17 s. 36.

⁷⁹ Prop. 2019/20:64 s. 262.

⁸⁰ SOU 2012:44 s. 766.

⁸¹ Prop. 2019/20:64 s. 67.

vilket inte sällan används för narkotikaförsäljning och andra olagliga aktiviteter.⁸²

Hemlig dataavläsning skulle underlätta myndigheternas möjligheter att kringgå även anonymiseringen av kriminella aktiviteter och ta del av information som innehåller viktiga bevis. Exempelvis när myndigheterna genom inhämtande av uppgifter om vilken IP-adress som används försöker identifiera användaren av en specifik teknisk utrustning. Då skulle ett införande av dataavläsning bereda möjligheter att till exempel aktivera en kamera eller mikrofon på mobiltelefonen eller datorn som används och på så vis fastställa användarens identitet.⁸³

3.2 Tidigare överväganden

3.2.1 SOU 2005:38

I utredningen ”Tillgång till elektronisk kommunikation” aktualiserades frågan om hemlig dataavläsning för första gången. Utredningen syftade inte specifikt på att utreda ett eventuellt införande av hemlig dataavläsning men det framtida behovet av hemlig dataavläsning kunde redan då förutses av utredningen.⁸⁴

Utredningen pekade på den ökade IT-användningen bland kriminella och det största behovet av hemlig dataavläsning ansågs finnas vid brottslighet som var organiserad och planerad. Det berodde bland annat på att det främst vid organiserad brottslighet ofta fanns inblandade personer som var mycket tekniskt skickliga, vilket gjorde dessa personers brottslighet svårutredd genom att mycket material krypterades och anonymiserades. Vidare

⁸² IOCTA 2017 s. 35.

⁸³ SOU 2005:38 s. 266.

⁸⁴ SOU 2005:38 s. 51, 365 f.

konstaterades att även utanför den kriminella världen ökade krypteringen och de uppgifter som gick att få från till exempel teleoperatörer visade inte vem som använt den tekniska utrustningen, bara vilket IP-adress den använts från. Således såg utredningen inga fler alternativ till hur den dolda informationen skulle inhämtas än genom hemlig dataavläsning.⁸⁵

Utredningen poängterade att man inte utan svårigheter kan väga intresset av att skydda enskildas personliga integritet och rätt till privatliv mot vikten av att myndigheterna ges effektiva verktyg för brottsutredning. Det ansågs dock inte mot bakgrund av fördelarna kunna anses försvarligt att inte införa lagen. Beredningen ansåg att ett införande av hemlig dataavläsning inte skulle medföra ett större integritetsintrång än de redan existerande tvångsmedlen som till exempel hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning.⁸⁶

3.2.2 SOU 2012:44

När ”Utredningen om vissa hemliga tvångsmedel” sju år efter SOU 2005:38 lämnade delbetänkandet ”Hemliga tvångsmedel mot allvarliga brott” ingick det inte heller denna gång i utredningens uppdrag att lämna förslag om införande av hemlig dataavläsning.

I utredningen framförde de brottsbekämpande myndigheterna tydligt att behovet av hemlig dataavläsning var stort och att tvångsmedlet borde införas. Behovet av nya metoder betonades med anledning av den tekniska utvecklingen och de kriminellas snabba anpassning till densamma. Det framfördes att de aktiva inom den organiserade brottsligheten börjat räkna med att till exempel hemlig telefonavlyssning används och därför ofta gjorde stora ansträngningar för att kommunicera utan att avlyssnas. Som exempel

⁸⁵ SOU 2005:38 s. 52.

⁸⁶ SOU 2005:38 s. 367 f.

nämndes krypterade mejl- och telefontjänster och gemensamma mejlkontot för att undvika att meddelanden skickas mellan de inblandade.⁸⁷ Säkerhetspolisen framförde exempelvis att spioneri blev allt svårare att upptäcka på grund av den tekniska utvecklingen samt att terrorister på grund av den uppsjö av kommunikationsmedel som fanns ständigt kunde förändra sitt sätt att kommunicera, varför ett införande av hemlig dataavläsning skulle underlätta även för deras verksamhet.⁸⁸

Sammanfattningsvis nådde utredningen slutsatsen att det fanns visst stöd för att hemlig dataavläsning skulle medföra beaktansvärd nytta. Tvångsmedlet skulle dock med den utformning som föreslogs i SOU 2005:38, medföra avsevärda integritetsintrång. Intrången skulle dock, på samma sätt som vid hemlig rumsavlyssning, i vissa fall kunna vara berättigade ansågs det. Mot bakgrund av det ovan anförda ansågs det angeläget att frågan om hemlig dataavläsning utreds.⁸⁹

3.2.3 SOU 2017:89

När utredningen ”Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet” initierades var det första gången en beredning uttryckligen fått i uppdrag att utreda ett införande av hemlig dataavläsning. I uppdraget ingick bland annat att fastställa behovet av tvångsmedlet, undersöka dess effektivitet som metod för att bekämpa terroristbrott och allvarlig brottslighet, klargöra om intresset av den personliga integriteten tillåter tvångsmedlet, analysera tvångsmedlets lämplighet samt lämna fullständiga förslag till förändringar i lagstiftningen.⁹⁰

⁸⁷ SOU 2012:44 s. 767.

⁸⁸ SOU 2012:44 s. 183, 193.

⁸⁹ SOU 2012:44 s. 768.

⁹⁰ Prop. 2019/20:64 s. 261.

Utredningen resulterade i en uppfattning som väl överensstämde med de två tidigare beredningarnas uppfattningar. Mot bakgrund av den tekniska utvecklingen har behovet ökat de senaste åren. Uppgifter som myndigheterna tidigare fick del av genom användande av de befintliga hemliga tvångsmedlen som hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation får man inte längre tag i. Det pekades på den ökande användningen av kryptering och anonymisering i kombination med att en allt större del av brottsligheten, och därmed kommunikationen i samband med brottsligheten, bedrivs på internet.⁹¹

Beredningen ansåg att det fanns ett tungt vägande behov av utökade och förbättrade metoder för myndigheterna att i hemlighet komma åt uppgifter som redan fick hämtas in genom de befintliga hemliga tvångsmedlen. Särskilt tungt vägde de kriminellas medvetenhet om hur de befintliga metoderna fungerade i kombination med de svårigheter som kan uppstå vid tillämpningen av hemliga tvångsmedel i vissa fall. Behovet var enligt beredningen lika tungt vägande i den brottsutredande verksamheten som i underrättelseverksamheten.⁹²

Hemlig dataavläsning ansågs i de flesta fall vara en effektiv metod även om den inte ansågs vara möjlig i alla de fall där det kommer finnas ett behov av den. I de fall tvångsmedlet skulle kunna användas förväntades det dock leda till betydligt bättre resultat än de befintliga tvångsmedlen. Tvångsmedlet förutsågs dock bli resurskrävande och medföra kostnadsökningar vilket enligt beredningen skulle leda till att hemlig dataavläsning i första hand skulle användas vid den allra allvarligaste brottsligheten. I de fallen ansåg beredningen att hemlig dataavläsning skulle bli en effektiv åtgärd.⁹³

⁹¹ Prop. 2019/20:64 s. 262.

⁹² Ibid.

⁹³ Ibid.

Beträffande det motstridande intresset av att upprätthålla ett starkt skydd för den personliga integriteten och förenligheten med en lag om hemlig dataavläsning konstaterades följande. Beredningen identifierade tre största riskerna och angav att ett införande skulle kunna medföra att en person närmast fullständigt kartläggs och övervakas om inte tydliga begränsningar görs, att metoden riskerar att medföra en mycket långtgående övervakning vid optisk övervakning eller avlyssning om inte tydliga begränsningar görs, samt att införandet kan innebära att informationssäkerheten även utanför den tekniska utrustning som övervakas minskar om inte särskilda krav ställs upp för tillämpningen.⁹⁴

Det huvudsakliga resultatet av utredningen blev till slut att beredningen ansåg att riskerna med ett införande inte vägde tyngre än den vinst i effektivitet som ett införande skulle medföra för de brottsbekämpande myndigheterna. Det var mot den bakgrunden som beredningen ansågs att tillämpandet av hemliga tvångsmedel skulle anses proportionerligt. Betänkandet föreslog en tidsbegränsad lag för att kunna utvärdera lagen efter att den tillämpats under fem års tid.⁹⁵ Utredningen ligger till grund för lag (2020:62) om hemlig dataavläsning.

3.3 Förutsättningar för användande av hemlig dataavläsning

Nedan följer en omfattande genomgång av bestämmelser och rekvisit, samt hur dessa ska tolkas. Avsnittets detaljrikedom är viktig för att få en djupare inblick i den nya lagen om hemlig dataavläsning och därmed kunna analysera och utvärdera densamma. Tolkningar av enskilda rekvisit kan vara av stor praktisk betydelse vid tillämpningen av lagen.

⁹⁴ Prop. 2019/20:64 s. 263.

⁹⁵ Ibid.

Inledningsvis kan sägas att det för alla typer av tillstånd till hemlig dataavläsning krävs att skälen för åtgärden uppväger det intrång eller men som åtgärden innebär för målpersonen eller för något annat motstående intresse.⁹⁶ Denna bestämmelse ger uttryck för den proportionalitetsprincip som ska genomsyra lagstiftningen kring de straffprocessuella tvångsmedlen och som beskrivits ovan.⁹⁷

3.3.1 De uppgifter som får inhämtas

De brottsbekämpande myndigheterna kan beviljas tillstånd för att läsa av eller ta upp följande:

- Uppgifter om innehållet i meddelanden som överförs eller har överförts till eller från ett telefonnummer eller någon annan adress i ett elektroniskt kommunikationsnät, s.k. *kommunikationsavlyssning*,
- Uppgifter om meddelanden som överförs eller har överförts till eller från ett telefonnummer eller någon annan adress i ett elektroniskt kommunikationsnät, s.k. *kommunikationsövervakning*,
- Uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits, s.k. *platsuppgifter*,
- Uppgifter som inhämtas genom optisk personövervakning, s.k. *kameraövervakning*,
- Uppgifter i form av tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till, s.k. *rumsavlyssning*,
- Uppgifter som lagrats i ett avläsningsbart informationssystem men som inte avses ovan i uppräkningsdelen,
- Uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses ovan i uppräkningsdelen.⁹⁸

⁹⁶ 3 § lag (2020:62) om hemlig dataavläsning.

⁹⁷ Se avsnitt 2.2.2.4.

⁹⁸ 1-2 §§ lag (2020:62) om hemlig dataavläsning.

Hemlig dataavläsning ger även myndigheterna en möjlighet att hindra att meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät når fram vid kommunikationsavlyssning eller kommunikationsövervakning.⁹⁹

3.3.2 Hemlig dataavläsning inom ramen för förundersökning

Under förundersökning får de brottsbekämpande myndigheterna beviljas tillstånd till hemlig dataavläsning om åtgärden är av *synnerlig vikt* för utredningen.¹⁰⁰ Med formuleringen att åtgärden är av synnerlig vikt för utredningen avses i propositionen samma innebörd som för övriga tvångsmedel. Det innebär att de upplysningar som åtgärden kan ge ska uppnå en viss kvalitet och det ska gå att räkna med att åtgärden verkligen kan få effekt, antingen ensam eller i förening med andra åtgärder. Mot bakgrund av ovan angivna principer¹⁰¹ för användning av hemliga tvångsmedel innebär kravet på synnerlig vikt kan anses uppfyllt om andra åtgärder inte är tillräckliga, väsentligt svårare att genomföra eller förväntas leda till ett större integritetsintrång. Det finns inget krav på att andra tvångsmedel ska ha prövats och misslyckats men det ställs ett utredningskrav på den som ansöker om tillstånd till hemlig dataavläsning. Den som ansöker ska utreda eller uttömma möjligheterna till användande av andra åtgärder före ansökan görs.¹⁰²

Tillstånd till hemlig dataavläsning beviljas som huvudregel endast vid en förundersökning vid följande brottslighet. Det gäller brott med ett minimistraff om två års fängelse, sådana samhällsfarliga brott som återfinns

⁹⁹ 2 § andra stycket lag (2020:62) om hemlig dataavläsning.

¹⁰⁰ 4 § lag (2020:62) om hemlig dataavläsning.

¹⁰¹ Se avsnitt 2.2.2.

¹⁰² Prop. 2019/20:64 s. 216.

i listan i 27 kap 2 § andra stycket andra till sjunde punkten rättegångsbalken, försök, förberedelse eller stämpling de hittills angivna brotten, eller vid andra brott om det med hänsyn till omständigheterna *kan antas* att brottets straffvärde är högre än två års fängelse.¹⁰³

I 27 kap 2 § andra stycket rättegångsbalkens andra till sjunde punkt anges därmed de brott som även de kan motivera ett tillstånd till hemlig dataavläsning. I paragrafen anges till exempel mordbrand, allmänfarlig ödeläggelse, spioneri och terroristbrott.

Den punkt som anger att även brott som med hänsyn till omständigheterna kan antas ha ett straffvärde som överstiger två års fängelse ger uttryck för en s.k. straffvärdesventil. Bedömningen av det specifika brottets, inte brottstypens, straffvärde ska göras med utgångspunkt i 29 kapitlet i brottsbalken och både höjande och sänkande faktorer ska beaktas vid bedömningen. Eventuella osäkerhetsmoment i bedömningen ska bedömas till den misstänktes fördel och straffvärdesventilen ska i allmänhet tillämpas restriktivt vilket innebär att åtgärden endast bör tillämpas när det finns goda skäl att anta att straffvärdet överstiger två års fängelse.¹⁰⁴

Ett tillstånd till hemlig dataavläsning får i förundersökningsfallen endast avse ett avläsningsbart informationssystem som används, eller som det finns *särskild anledning att anta* har använts eller kommer att användas, av målpersonen om han är *skäligen misstänkt* för brottet.¹⁰⁵ Bestämmelsen innebär att det ska vara fråga om en målperson ,med en koppling till det avläsningsbara informationssystem som uppnått misstankegraden skäligen misstänkt. Det finns dock inget krav på att den misstänkte äger eller är den enda som brukar exempelvis en mobiltelefon eller ett gemensamt konto. En användning av ett informationssystem kan exempelvis vara att spela spel på

¹⁰³ 4 § lag (2020:62) om hemlig dataavläsning.

¹⁰⁴ Lindberg (2018), s. 558 f.

¹⁰⁵ 4 § andra stycket lag (2020:62) om hemlig dataavläsning.

en mobiltelefon eller endast kopplar upp sig mot internet på en dator. Om målpersonen inte använder informationssystemet men man misstänker att personen har använt det eller kommer att använda det, krävs att det att det finns särskild anledning att anta det. Det innebär i sin tur att det ska finnas någon faktisk omständighet som med viss styrka talar för att målpersonen har använt eller kommer att använda informationssystemet under tiden för tillståndet.¹⁰⁶

Skälig misstanke är den misstankegrad som krävs för de flesta tvångsmedel men exakt vad som krävs för att nå upp till misstankegraden är i sammanhanget någorlunda oklart.¹⁰⁷ Det som krävs för att uppnå misstankegraden skäligen misstänkt har dock i doktrin ansetts vara att misstanken avser ett konkret brott, att misstanken är individualiserad genom att någon konkret omständighet pekar på att just den personen begått brottet, att utredningen är robust och ärendet tillräckligt utrett, samt att det finns en sannolikhetsövertikt. En sannolikhetsövertikt innebär att det är mer sannolikt att personen begått brottet än att vederbörande inte gjort det.¹⁰⁸ Ingen närmare fördjupning i beviskravet ska göras här men som ledning kan sägas att skäligen misstänkt i doktrin liknats vid uttrycket ”antagligt”.¹⁰⁹ I propositionen har angetts att bedömningen ska göras utifrån omständigheter i varje enskilt fall. Misstankens styrka ska vidare prövas utifrån en objektiv och allsidig bedömning av det material som utredningen innehåller vid tidpunkten. Vidare anges att ett tillstånd till hemlig dataavläsningen, precis som för övriga tvångsmedel, aldrig får grundas enbart på allmänna kunskaper om en persons livsstil eller tidigare brottslighet.¹¹⁰

3.3.2.1 Särskilt om kommunikationsavlyssnings-,

¹⁰⁶ Prop. 2019/20:64 s. 217, 123.

¹⁰⁷ Lindberg (2018), s. 46.

¹⁰⁸ Lindberg (2018) s. 46, Andersson (2016), s. 223 f., 180 f., 201 f., 168 f.

¹⁰⁹ Ekelöf m.fl. (2011), s. 113.

¹¹⁰ Prop. 2019/20:64 s. 216 f.

kommunikationsövervaknings- och platsuppgifter

Vid inhämtning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får ett tillstånd om hemlig dataavläsning även avse ett informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.¹¹¹ Kravet på synnerlig anledning att anta medför en restriktiv tillämpning av bestämmelsen och innebär att det ska finnas tillförlitliga uppgifter som medför att det är så gott som säkert att den misstänkte kommer att kontakta informationssystemet.¹¹²

Hemlig dataavläsning som avser kommunikationsövervaknings- och platsuppgifter får även beviljas tillstånd i syfte att utreda vem som skäligen kan misstänkas för ett brott i förundersökningsfallen. Bestämmelsen utgör alltså ett undantag från huvudregeln i 4 §. Tillstånd till hemlig dataavläsning kan beviljas även utan att det finns en skäligen misstänkt för brottet. Avläsning eller upptagning av kommunikationsövervakningsuppgifter får då endast avse förfluten tid, för platsuppgifter finns dock ingen sådan begränsning. Användningen får dock endast avse ett avläsningsbart informationssystem som använts vid ett brott eller i anslutning till en brottsplats vid tidpunkten för brottet eller som av annan anledning är *av synnerlig vikt för utredningen*.¹¹³

Kravet på att det avläsningsbara informationssystemet ska ha använts vid brottet medför att det ska ha haft avgörande betydelse för brottets genomförande eller använts för att understödja brottet. Som exempel anges om det i polisens förundersökning av till exempel grovt narkotikabrott upptäcks att det från en viss IP-adress har förmedlats stora mängder narkotika kan polisen få tillstånd att använda hemlig dataavläsning för att fastställa vem

¹¹¹ 4 § tredje stycket lag (2020:62) om hemlig dataavläsning.

¹¹² Prop. 2019/20:64 s. 217, prop. 2002/03:74 s. 49.

¹¹³ 5 § lag (2020:62) om hemlig dataavläsning.

som är skäligen misstänkt för brottet, alltså vem som använder informationssystemet som är kopplat till IP-adressen.¹¹⁴

I propositionen anges att ett informationssystem på annat sätt är av synnerlig vikt för utredningen när det inte står klart att informationssystemet befunnit sig vid eller i närheten av brottsplatsen, men ändå kan ha en avgörande betydelse för utredningen. Som exempel anges situationer när ett informationssystem befunnit sig längs en flyktväg från en brottsplats eller när det finns skäl att tro att gärningsmannen kan tänkas förflytta sig medan brottet fortfarande pågår, exempelvis vid människorov eller grov narkotikasmuggling.¹¹⁵

3.3.2.2 Särskilt om rumsavlyssningsuppgifter

Hemlig dataavläsning får endast användas till inhämtning av rumsavlyssningsuppgifter i en förundersökning om det rör sig om ett brott med ett minimistraff om minst fyra års fängelse, spioneri eller brott som begåtts på uppdrag av främmande makt eller för dess räkning och som rör företagshemligheter.¹¹⁶ Rumsavlyssningsuppgifter får även inhämtas vid en förundersökning om det med hänsyn till omständigheterna *kan antas* att brottets straffvärde överstiger fängelse i fyra år och det är fråga om till exempel människohandel, våldtäkt, grov utpressning, grovt narkotikabrott med flera.

Beträffande kravet på att det med hänsyn till omständigheterna kan antas att straffvärde överstiger fängelse i fyra år, den så kallade straffvärdesventilen, gäller att bedömningen ska ske utifrån det enskilda brottet, inte brottstypen, och ske med utgångspunkt i 29 kapitlet brottsbalken. Både försvårande och förmildrande omständigheter ska beaktas vid bedömningen och för att

¹¹⁴ Prop. 2019/20:64 s. 218 f.

¹¹⁵ Prop. 2019/20:64 s. 219.

¹¹⁶ 4 och 6 §§ lag (2020:62) om hemlig dataavläsning, 27 kap 20 d § andra stycket rättegångsbalken.

tvångsmedel ska få användas bör straffvärdet med marginal överstiga fyra års fängelse. Denna straffvärdesventil ska enligt förarbeten tillämpas restriktivt och eventuella osäkerheter i avvägningar ska tolkas till den misstänktes fördel. Det innebär att hemlig rumsavlyssningsuppgifter endast får inhämtas vid brott vars straff väl överstiger fyra års fängelse och finns uppräknade i bestämmelserna.¹¹⁷ Den i stycket omnämnda straffvärdesventil härstammar från lagstiftningen kring hemlig rumsavlyssning men ska enligt propositionen även gälla för inhämtning av rumsavlyssningsuppgifter genom hemlig dataavläsning.¹¹⁸

Under samma förutsättningar som för de brott som uppräknats i avsnittets första stycke får hemlig dataavläsning användas vid förundersökning av försök, förberedelse eller stämpling till brottet om försöks- eller medverkansgärningen är belagd med straff.¹¹⁹ Sådan hemlig dataavläsning får endast äga rum på en plats där det finns *särskild anledning att anta* att den misstänkte kommer att uppehålla sig¹²⁰. Om platsen för åtgärden är någon annan än den misstänktes stadigvarande bostad krävs att det finns *synnerlig anledning att anta* att den misstänkte kommer att uppehålla sig där.¹²¹

Beträffande rekvisitet synnerlig anledning att anta att den misstänkte kommer att uppehålla sig på platsen framgår av propositionen att det innebär att man måste vara så gott som säker på att den misstänkte kommer att uppehålla sig på platsen någon gång under tillståndstiden. Som exempel på en situation när rekvisitet ska anses uppfyllt anges om det vid spaning visat sig att den misstänkte brukar besöka en bekants bostad vid en viss bestämd tidpunkt.¹²²

¹¹⁷ Lindberg (2018), s. 579 f.

¹¹⁸ Prop. 2019/20:64 s. 116.

¹¹⁹ 27 kap 20 d § andra stycket rättegångsbalken.

¹²⁰ Se avsnitt 3.4.2.

¹²¹ 6 § andra stycket lag (2020:62) om hemlig dataavläsning.

¹²² Prop. 2019/20:64 s. 220.

3.3.2.3 Särskilt om kameraövervakningsuppgifter

Vid inhämtning av kameraövervakningsuppgifter genom hemlig dataavläsning får åtgärden endast avse en plats där den misstänkte *kan antas* komma att uppehålla sig. Med formulering menas att en direkt koppling mellan den misstänkte och platsen måste finnas. Platsen för åtgärden får dock inte vara någons stadigvarande bostad.¹²³

Bestämmelsen motsvarar förbudet för hemlig kameraövervakning men blir tämligen komplicerad vid hemlig dataavläsning. Vid en traditionell kameraövervakning installeras en kamera på en plats, vilket gör det mycket enkelt att kontrollera om det är i en stadigvarande bostad som kameran installeras. Vid hemlig dataavläsning installeras eller aktiveras istället en kamera som redan finns i till exempel en mobiltelefon som den misstänkte använder. Detta skapar ett ansvar för den brottsbekämpande myndighet som verkställer åtgärden att kontrollera att mobiltelefonen, vilket är en rörlig enhet, inte befinner sig i en stadigvarande bostad vid aktiveringstillfället. Med anledning av denna problematik anförs i propositionen att det ankommer på den som beslutar om tillstånd till hemlig dataavläsning att försäkra sig om att platskravet kan respekteras. Ett sätt att säkerställa det är att använda sig av fysisk spaning.¹²⁴

3.3.3 Hemlig dataavläsning utanför förundersökning

I vissa undantagsfall får tillstånd ges till hemlig dataavläsning även utanför en förundersökning. Undantagen motiveras genom att åtgärden görs i syfte att förhindra vissa särskilt allvarliga brott, att göra en särskild

¹²³ 4 § fjärde stycket lag (2020:62) om hemlig dataavläsning.

¹²⁴ Prop. 2019/20:64 s. 218.

utlänningskontroll eller att förebygga, förhindra och upptäcka brottslig verksamhet.¹²⁵

3.3.3.1 Förhindrande av vissa särskilt allvarliga brott

Hemlig dataavläsning för förhindrande av vissa särskilt allvarliga brott får användas i tre fall. Det första är om 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 § preventivlagen¹²⁶. Det andra fallet är om det finns en påtaglig risk för att sådan brottslig verksamhet som avses i första fallet 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 verksamheten.¹²⁷

Formuleringen om det med hänsyn till omständigheterna finns en påtaglig risk att brottslighet kan komma att utövas ska ges samma innebörd här som i preventivlagen.¹²⁸ Åtgärden är inte tillämplig på brottslighet i det förflutna och med att ”utöva” brottslighet åsyftas även varje medverkans- eller främjandegärning.¹²⁹ Bedömningen om brottslig verksamhet kan komma att utövas ska bygga på faktiska omständigheter i det enskilda fallet eller händelseförloppet, som till exempel uttalanden, hotelser eller andra faktiska handlanden som talar för att brottsligheten kan komma att utövas.¹³⁰ Risken ska ta fasta på en utifrån omständigheterna klart förutsebar utveckling som till exempel att ett terrorattentat kan komma att inträffa.¹³¹ Bedömningen av om risken är påtaglig ska göras utifrån de omständigheter som framkommit

¹²⁵ 7-11 §§ lag (2020:62) om hemlig dataavläsning.

¹²⁶ Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

¹²⁷ 7 § lag (2020:62) om hemlig dataavläsning.

¹²⁸ Prop. 2019/20:64 s. 221.

¹²⁹ Ds 2005:21 s. 255 f.

¹³⁰ Lindberg (2018), s. 735 f.

¹³¹ Prop. 2013/14:237 s. 195.

genom polisens underrättelse-, och spaningsverksamhet, men även genom internationellt polissamarbete.¹³²

Beträffande bedömningen av ”påtaglig risk” kan ledning hämtas ur regleringen av vård av unga¹³³. Påtaglig risk innebär att det ska finnas viss sannolikhet att risken ska förverkligas. Det finns dock inte något krav på en konkret gärning.¹³⁴ Det medför att tvångsmedlet kan tillåtas i preventivt syfte när det finns flera inträffade omständigheter som starkt talar för en risk att ett brott av visst slag kommer att begås men det inte kan konkretiseras hur risken för brottet kan förverkligas. Som exempel kan nämnas svårigheten att konkretisera vilket närmare tillvägagångssätt som kommer att användas vid ett terrorattentat eller mot vilket mål det kommer riktas. I bedömningen bör risken utgå ifrån både avsikt och förmågan hos gärningspersonen.¹³⁵

Formuleringen ”en person” medför att de brottsbekämpande myndigheterna inte behöver känna till vem personen är. Myndigheterna ska knyta risken till en person, även om de inte känner till personens identitet. Det kan till exempel röra sig om en person som ska komma till Sverige för att utföra ett terrordåd.¹³⁶ Ett tillstånd som istället kopplas till en organisation ska avse en viss person i gruppen eller organisationen. Gentemot gruppen ska samma riskbedömning som i stycket ovan göras, vilket innebär att det ska finnas en koppling mellan organisationen och den brottsliga verksamheten och att det ska finnas en påtaglig risk att brottsligheten utövas inom gruppen. Vid sidan av gruppens riskbedömning ska även en riskbedömning för den person i gruppen som tvångsmedlet riktar sig mot göras. Kravet är i den delen att det ska kunna befaras att personen kommer att främja den brottsliga verksamheten.¹³⁷ Bedömningen ska främst avse de omständigheter som talar

¹³² Prop. 2005/06:177 s. 83.

¹³³ Lag (1990:52) med särskilda bestämmelser om vård av unga.

¹³⁴ Prop. 2013/14:237 s. 106.

¹³⁵ Prop. 2013/14:237 s. 195 f.

¹³⁶ Prop. 2005/06:177 s. 83.

¹³⁷ Prop. 2013/14:237 s. 107 f., 196.

för risken att personen främjar brottet och inte vad ett sådant främjande kan anses vara.¹³⁸ Det ska dock finnas objektiva omständigheter som talar för att ett främjande kommer att ske. Som exempel på sådana omständigheter är till exempel personens ställning i organisationen eller om personen tidigare har dömts för brottslighet som liknar eller är relevant för den aktuella brottsligheten. Enbart ett medlemskap i organisationen är dock inte tillräckligt för att grunda ett beslut om tillstånd till tvångsmedlet.¹³⁹ Främjandet måste även vara medvetet, att en person till exempel stödjer organisationen ekonomiskt är inte tillräckligt om personen inte vet om att organisationen bedriver brottslig verksamhet.¹⁴⁰

Den brottslighet som åsyftas är till exempel mordbrand, spioneri, terroristbrott eller våldsbrott som mord, dråp, grov misshandel, synnerligen grov misshandel, människorov eller olaga frihetsberövande om avsikten är att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

Även denna användning av hemlig dataavläsning beviljas endast om den är av *synnerlig vikt för att förhindra* sådan brottslig verksamhet som anges i stycket ovan.¹⁴¹ Om åtgärden används för inhämtning av kameraövervakningsuppgifter måste det ske på en plats där målpersonen *kan antas* komma att uppehålla sig¹⁴², vilket inte får vara någons stadigvarande bostad. Utanför förundersökning är det förbjudet att använda hemlig dataavläsning i syfte att inhämta rumsavlyssningsuppgifter.¹⁴³

¹³⁸ Lindberg (2018), s. 736.

¹³⁹ Prop. 2013/14:237 s. 109, 196 f.

¹⁴⁰ Prop. 2013/14:237 s. 109, 197.

¹⁴¹ 7 § andra stycket lag (2020:62) om hemlig dataavläsning.

¹⁴² Se avsnitt 3.4.2.3.

¹⁴³ 7 § tredje och fjärde stycket lag (2020:62) om hemlig dataavläsning.

Rekvisitet *synnerlig vikt för att förhindra allvarlig brottslighet* ska förstås på samma sätt som för huvudregeln där formuleringen är *synnerlig vikt för utredningen*.¹⁴⁴ Tolkningen ska dock göras utifrån förståelsen att syftet med denna åtgärd inte är att utreda, utan istället att förhindra allvarlig brottslighet.¹⁴⁵ Detta innebär att kravet ska tolkas som att åtgärden måste vara nödvändig för att förhindra brottsligheten och att alternativa åtgärder för att uppnå samma ändamål i princip ska vara uttömda.¹⁴⁶

Det tredje fallet är när det finns ett avläsningsbart informationssystem som används, eller som det finns *särskild anledning att anta*¹⁴⁷ har använts eller kommer att användas, av en person som anges i någon av de två första fallen. Om åtgärden gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får den även avse ett avläsningsbart informationssystem som det finns *synnerlig anledning att anta*¹⁴⁸ att en person som anges i de två första fallen under tillståndstiden har kontaktat eller kommer att kontakta.¹⁴⁹

3.3.3.2 Särskild utlänningskontroll

Hemlig dataavläsning får användas för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem som används eller som det finns *särskild anledning att anta*¹⁵⁰ har använts eller kommer att användas av en utlänning, i olika två situationer. Användning får i första fallet tillåtas mot en utlänning som omfattas av ett utvisningsbeslut, om det med hänsyn till vad som är känt om utlänningens tidigare verksamhet och övriga omständigheter kan befaras att han kommer att begå eller medverka till ett terroristbrott eller försök,

¹⁴⁴ Se avsnitt 3.4.2, 3.4.2.1.

¹⁴⁵ Prop. 2019/20:64 s. 221.

¹⁴⁶ Lindberg (2018), s. 738.

¹⁴⁷ Se avsnitt 3.4.2.

¹⁴⁸ Se avsnitt 3.4.2.1.

¹⁴⁹ 8 § lag (2020:62) om hemlig dataavläsning.

¹⁵⁰ Se avsnitt 3.4.2.

förberedelse eller stämpling till brottet.¹⁵¹ Det krävs inte att det finns några konkreta bevis om ett visst brott. De uppgifter som finns att tillgå om utlänningen ska dock ge anledning att befara att han kommer att begå eller medverka till gärningen som åsyftas i bestämmelsen.¹⁵² Tillstånd ges även vid ett avvisning- eller utvisningsbeslut enligt 8 eller 8 a kapitlet i utlänningslagen¹⁵³ eller motsvarande äldre bestämmelser och det finns sådana omständigheter som framgår av första fallet.¹⁵⁴

Paragrafen ställer även upp ett krav på att det ska finnas en koppling mellan utlänningen och det avläsningsbara informationssystemet som ska bli föremål för åtgärden. Denna personkoppling tolkas likadant som den i förundersökningsfallen¹⁵⁵ med skillnaden att det här handlar om en utlänning som omfattas av ett avvisnings- eller utvisningsbeslut och således inte en misstänkt person i den meningen.¹⁵⁶

Tillstånd till kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får också beviljas för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem om det finns *synnerlig anledning att anta att* utlänningen under tillståndstiden har kontaktat det eller kommer att kontakta det.¹⁵⁷ Bestämmelsen ska tolkas likadant beträffande personkopplingen som i stycket ovan.¹⁵⁸

För att tillstånd enligt bestämmelsen ska beviljas krävs *synnerliga skäl* och att det är av betydelse för att utreda om utlänningen eller en organisationen

¹⁵¹ 9 § första stycket lag (2020:62) om hemlig dataavläsning, 1 § 2 p lag (1991:572) om särskild utlänningskontroll.

¹⁵² Prop. 2002/03:38 s. 96.

¹⁵³ Utlänningslag (2005:716).

¹⁵⁴ 9 § första stycket lag (2020:62) om hemlig dataavläsning.

¹⁵⁵ Se avsnitt 3.4.2, 4 § lag (2020:62) om hemlig dataavläsning.

¹⁵⁶ Prop. 2019/20:64 s. 223.

¹⁵⁷ 9 § första och andra stycket lag (2020:62) om hemlig dataavläsning.

¹⁵⁸ Prop. 2019/20:64 s. 223.

eller grupp som personen tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott.¹⁵⁹ Det medför att tillstånd enligt bestämmelsen om hemlig dataavläsning i detta avsnitt endast kan beviljas för att utreda utlänningens eller organisationens inblandning i sådan brottslighet som anges i den lagen.¹⁶⁰ Ett tillstånd enligt bestämmelsen om hemlig dataavläsning i utvisnings-, avvisningsfallen får inte avse kameraövervaknings- eller rumsavlyssningsuppgifter.¹⁶¹

3.3.3.3 För att upptäcka brottslig verksamhet

Tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får tillåtas för att förebygga, förhindra eller upptäcka brottslighet som innefattar brott som anges i 2 § inhämtningslagen¹⁶². Det krävs dock att åtgärden är av *synnerlig vikt*. Sådan hemlig dataavläsning får inte användas för att hindra att meddelanden når fram och får i fall som gäller kommunikationsövervakningsuppgifter endast avse uppgifter i förfluten tid.¹⁶³

Kraven för att få använda hemlig dataavläsning enligt bestämmelsen motsvarar kraven från inhämtningslagen i den mån att det ska vara fråga om brott med ett minimistraff om två års fängelse eller viss särskilt angivna brott, som till exempel spioneri. Skillnaden är dock att åtgärden inom ramen för hemlig dataavläsning endast får användas om den är av synnerlig vikt, inte särskild vikt som i inhämtningslagen. Rekvisitetet synnerlig vikt tar i paragrafens kontext sikte på förebyggandet, förhindrandet eller upptäckandet av den brottsliga verksamheten och inte utredningen som i

¹⁵⁹ 9 § fjärde stycket lag (2020:62) om hemlig dataavläsning.

¹⁶⁰ Prop. 2019/20:64 s. 223.

¹⁶¹ 9 § femte stycket lag (2020:62) om hemlig dataavläsning.

¹⁶² Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

¹⁶³ 10 § lag (2020:62) om hemlig dataavläsning.

förundersökningsfallen. I övrigt är bedömningen densamma avseende kravet på synnerlig vikt.¹⁶⁴

3.4 Rättssäkerhetsgarantier

Rättssäkerhetsgarantier är den av lagstiftningen som är avsedda att slå vakt om de intressen som vägs vid till exempel tillståndsprövningen och verkställandet av hemlig dataavläsning. Denna del av lagstiftningen är alltså av stor vikt för att kunna utvärdera lagstiftningen utifrån ett integritetsperspektiv.

3.4.1 Tillståndsprövning

Huvudregeln är att alla frågor om hemlig dataavläsning ska prövas av en domstol på ansökan av åklagaren. När det gäller åtgärder för särskild utlänningskontroll ska dock ansökan inges av Säkerhetspolisen eller Polismyndigheten.¹⁶⁵

När ansökan eller anmälan om hemlig dataavläsning väl kommer in till rätten ska rätten så snart som möjligt förordna ett offentligt ombud i ärendet och hålla sammanträde i ärendet. Den som upprättat ansökan eller anmälan och det offentliga ombudet utgör parterna i ett sådant sammanträde.¹⁶⁶

I undantagsfall kan tillstånd dock ges av åklagaren. Det gäller i fall där det kan befaras att man genom att vänta på domstolens tillstånd skulle skapa en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten. Om åklagaren i ett sådant fall ger tillstånd ska åklagaren utan dröjsmål skriftligt

¹⁶⁴ Prop. 2019/20:64 s. 224. Se avsnitt 3.4.2.1.

¹⁶⁵ 14 § lag (2020:62) om hemlig dataavläsning.

¹⁶⁶ 16 § lag (2020:62) om hemlig dataavläsning.

anmäla sitt beslut till domstolen och däri ange skälen för åtgärden. Ärendet ska därefter skyndsamt prövas och om domstolen anser att skäl inte föreligger för åtgärden, det vill säga om åklagaren gjort fel eller förutsättningarna ändrats, ska domstolen upphäva beslutet. Om åtgärden redan hunnit verkställas innan domstolens prövning ska domstolen pröva om åklagaren haft skäl för åtgärden. Om rätten finner att åtgärden inte skulle ha tillåtits får de uppgifter som framkommit genom åtgärden inte användas i en brottsutredning till nackdel för någon som omfattats av åtgärden eller uppgifterna som framkommit.¹⁶⁷

Beslut om tillstånd till hemlig dataavläsning kan som huvudregel på samma sätt som övriga tvångsmedel i rättegångsbalken överklagas och handläggning ska även då ske skyndsamt.¹⁶⁸ Beslut om tillstånd får dock verkställas omedelbart efter att de meddelas. Om skälen för åtgärden försvinner ska dock den som ansökt om tillståndet eller domstolen omedelbart upphäva beslutet. När ett beslut om tillstånd till hemlig dataavläsning fattats i domstolen ska domstolen alltid skyndsamt underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.¹⁶⁹

I ett tillstånd till hemlig dataavläsning ska alltid anges vilken tid tillståndet avser, vilket informationssystem tillståndet avser, vilken typ av uppgift som får läsas av eller tas upp, villkor för att tillgodose att enskildas personliga integritet inte kränks i onödan, och vem som är skäligen misstänkt för brottet om åtgärden gäller rumsavlyssningsuppgifter. Tillståndstiden får inte vara längre än nödvändigt och om den avser tid efter beslutet får den inte överstiga en månad från beslutsdagen.¹⁷⁰

¹⁶⁷ 17 § lag (2020:62) om hemlig dataavläsning.

¹⁶⁸ 19 § lag (2020:62) om hemlig dataavläsning.

¹⁶⁹ 20-21 §§ lag (2020:62) om hemlig dataavläsning.

¹⁷⁰ 18 § lag (2020:62) om hemlig dataavläsning.

Vid ett verkställande ska den teknik som används anpassas efter hur långtgående tillståndet är. Den använda tekniken får inte möjliggöra upptagningar eller avläsningar av någon annan typ av uppgift än vad som anges i tillståndet. Om sådana uppgifter ändå skulle upptas eller avläsas ska dessa omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden ska underrättas. Sådana uppgifter får inte heller användas i en brottsutredning till nackdel för målpersonen eller någon annan som uppgifterna avser.¹⁷¹

3.4.2 Aktsamhetskrav

Ett beslut om hemlig dataavläsning får i sitt verkställande inte medföra någon olägenhet eller skada utöver den som är absolut nödvändig. Avläsningsbara informationssystem som tillståndet avser får inte påverkas i den mån att informationssäkerheten åsidosätts, försämras eller skadas på grund av verkställigheten. Efter avslutad verkställighet ska den verkställande myndigheten se till att det avläsningsbara informationssystem som tillståndet avser återgår till den informationssäkerhet som rådde vid verkställighetens början. De tekniska hjälpmedel som använts vid verkställigheten ska tas bort, avinstalleras eller göras obrukbara så snabbt som möjligt efter att av någon anledning tillståndet upphör.¹⁷²

Den eller de personer som av myndigheten utses för att verkställa åtgärden ska vara särskilt lämpade för uppdraget och ha särskilda kunskaper om informationssäkerhet och annan behövlig kompetens, utbildning och erfarenhet i övrigt.¹⁷³

I övrigt får alla de tekniska hjälpmedel som behövs för avläsningen och upptagningen användas när ett tillstånd om hemlig dataavläsning beviljats.

¹⁷¹ 23 § lag (2020:62) om hemlig dataavläsning.

¹⁷² 25 § lag (2020:62) om hemlig dataavläsning.

¹⁷³ 26 § lag (2020:62) om hemlig dataavläsning.

Den verkställande myndigheten får även bryta och kringgå systemskydd och utnyttja tekniska sårbarheter i informationssystemen.¹⁷⁴

3.4.3 Förbud mot hemlig dataavläsning

3.4.3.1 Fredade verksamheter

Det kan aldrig beviljas tillstånd till hemlig dataavläsning av ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas i en verksamhet där tystnadsplikt gäller enligt grundlagen, i en verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer eller familjerådgivare, eller i verksamheter av präster eller personer med motsvarande ställning inom trossamfund, i verksamhet för bikt eller enskild själavård.¹⁷⁵

Förbudet är absolut och omfattar alla uppgiftstyper som genom hemlig dataavläsning kan tillgodogöras myndigheten. Bestämmelsen innebär att informationssystemet måste vara en beständig del av verksamheten och att det används i något av verksamhetens syften eller att det är särskilt avsett att användas i verksamheten. Ett exempel på när ett informationssystem är särskilt avsett att användas i en verksamhet är när en advokat ska starta en verksamhet och i förberedelserna har tagit med sin klientdatabas från sin tidigare arbetsgivare och lagrat den i den nya, ännu öppnade, verksamhetens informationssystem.¹⁷⁶

Internetbaserade tjänster som användaren kan nå genom informationssystemet omfattas inte alltid. Även om till exempel en advokat uteslutande använder den av förbudet fredade datorn för att logga in på sina privata konton på sociala medier eller privata internetbaserade mejlprogram

¹⁷⁴ 22 § lag (2020:62) om hemlig dataavläsning.

¹⁷⁵ 11 § lag (2020:62) om hemlig dataavläsning.

¹⁷⁶ Prop. 2019/20:64 s. 225.

kan hemlig dataavläsning tillåtas för avseende själva kontona. Förbudet ska inte heller typiskt sett omfatta de anställdas privata mobiltelefoner eller datorer även om de används i verksamheten vid enstaka tillfällen.¹⁷⁷

Informationssystem som endast i undantag eller tillfälligt används i verksamheten, som exempelvis besöksdatorer på en läkarmottagning eller liknande inrättning, omfattas inte av förbudet. Inget krav ställs på att informationssystemet måste användas på den fysiska arbetsplatsen för en verksamhet och det spelar ingen roll om informationssystemet befinner sig utanför arbetsplatsen vid avläsningen. Om en brottsutredande myndighet ansöker om tillstånd till hemlig dataavläsning som avser ett informationssystem som kan bli föremål för förbudet måste myndigheterna presentera uppgifter som tydligt visar att informationssystemet inte omfattas av förbudet. Visar det sig i efterhand att det gör det ska åtgärden avbrytas omedelbart.¹⁷⁸

3.4.3.2 Övriga förbud

Hemlig dataavläsning får inte användas för att få del av lagrade uppgifter eller uppgifter som visar hur ett informationssystem används, om det enligt rättegångsbalken¹⁷⁹ inte får tas i beslag. Detta förbud motsvarar det så kallade beslagsförbudet som hindrar att vissa skriftliga handlingar tas i beslag.¹⁸⁰ För hemlig dataavläsning gäller det filer eller andra informationsenheter som innehåller uppgifter om till exempel sådant som en person inte får höras som vittne om och som innehas av personen eller av den som tystnadsplikt gäller till förmån för, exempelvis en advokat eller läkare. För dataavläsning gäller alltså att de uppgifter som finns i filer och liknande som inte skulle ha fått tagits i beslag inte heller får bli föremål för hemlig dataavläsning. Undantaget är dock sådana uppgifter som inte omfattas av tystnadsplikten, till exempel i

¹⁷⁷ Prop. 2019/20:64 s. 225.

¹⁷⁸ Prop. 2019/20:64 s. 225 f.

¹⁷⁹ 27 kap 2 § första stycket rättegångsbalken.

¹⁸⁰ 27 § första stycket lag (2020:62) om hemlig dataavläsning.

vissa fall om det är fråga om grövre brott och tystnadsplikt därför inte gäller, då finns det inte heller något förbud mot att läsa av eller ta upp uppgiften.¹⁸¹

Vidare förbjuds hemlig dataavläsning som avser kommunikations- eller rumsavlyssningsuppgifter som framkommer i telefonsamtal, samtal eller andra meddelanden, om den som på liknande sätt som i stycket ovan inte skulle ha kunnat höras som vittne om uppgiften som yttrats eller på annat sätt kommit fram.¹⁸² Det gäller exempelvis samtal där uppgifter från en advokat eller läkare framkommer.¹⁸³ Detta förbud motsvarar avlyssningsförbudet i rättegångsbalken och förbudet mot hemlig avlyssning av elektronisk kommunikation i preventivlagen.¹⁸⁴

Skulle en uppgift som omfattas av förbuden i de två styckena ovan komma fram ska åtgärden omedelbart avbrytas och de förbjudna uppgifter som framkommit ska omedelbar förstöras.¹⁸⁵

3.4.4 Användning av överskottsinformation

I förundersökningsfallen gäller samma regler för överskottsinformationen som vid hemlig avlyssning av elektronisk kommunikation. Det innebär att om det under verkställigheten framkommer uppgifter om ett annat brott än det som föranlett tillståndet får uppgifterna användas för att utreda brottet. Uppgifterna kan även ligga till grund för en förundersökning eller motsvarande utredning om det för brottet är föreskrivet ett års fängelse eller

¹⁸¹ Prop. 2019/20:64 s. 240, 36 kap 5 § rättegångsbalken.

¹⁸² 27 § andra stycket lag (2020:62) om hemlig dataavläsning.

¹⁸³ Prop. 2019/20:64 s. 240.

¹⁸⁴ 27 kap 22 § rättegångsbalken, 11 § lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

¹⁸⁵ 27 § tredje stycket lag (2020:62) om hemlig dataavläsning.

mer och det kan antas att brottet inte endast leder till böter, eller om det finns särskilda skäl för det.¹⁸⁶

Om det däremot handlar om hemlig dataavläsning som avser rumsavlyssningsuppgifter gäller motsvarande som gäller för rumsavlyssning i rättegångsbalken. Det innebär att uppgifterna endast får användas för att utreda brottet om de avser ett sådant allvarligt brott som kan motivera ett tillstånd för rumsavlyssning¹⁸⁷, eller annat brott som det föreskrivs tre års fängelse eller mer för. Vid alla typer av uppgifter om andra brott än det tillståndsgrundande gäller att de får användas om det är i syfte att förhindra brott.¹⁸⁸

Om hemlig dataavläsning används eller har använts i syfte att förebygga, förhindra eller upptäcka brottslighet får sådana uppgifter om annan brottslighet användas i en förundersökning, om ett tillstånd om hemlig dataavläsning avseende kommunikationsövervaknings- eller platsuppgift också kan beviljas till följd av uppgifterna. Även utan ett sådant tillstånd får de dock ligga till grund för ett beslut om att inleda förundersökning.¹⁸⁹

Vid användning av hemlig dataavläsning i syfte att förhindra viss särskilt allvarlig brottslighet¹⁹⁰, gäller samma som gäller för motsvarande uppgifter i preventivlagen.¹⁹¹ Det betyder att överskottsinformation som huvudregel får användas för att förhindra brott. Innehåller de uppgifter om brott får uppgifterna användas för att utreda brottet om det rör sig om brottslighet som motiverar användning av tvångsmedlet och försök, förberedelse eller

¹⁸⁶ 28 § lag (2020:62) om hemlig dataavläsning, 27 kap 23 a § rättegångsbalken.

¹⁸⁷ Se avsnitt 3.4.2.2.

¹⁸⁸ 28 § lag (2020:62) om hemlig dataavläsning, 27 kap 23 § § rättegångsbalken.

¹⁸⁹ 10, 4, 5 och 31 §§ andra stycket lag (2020:62) om hemlig dataavläsning.

¹⁹⁰ Se avsnitt 3.4.3.1.

¹⁹¹ Lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

stämpling till ett sådant brott om gärningen är belagd med straff, eller andra brott för vilka det finns straff om tre års fängelse eller mer föreskrivet.¹⁹²

Om det i utlänningsfallen¹⁹³ framkommer uppgifter om ett brott som inte är av betydelse för ändamålet med den hemliga dataavläsning får de användas för att utreda brottet. Förundersökning eller motsvarande utredning om brottet får inledas på grund av uppgifterna om det är föreskrivet ett års fängelse eller mer för brottet och det kan antas att straffet för brottet inte stannar vid böter, eller om det finns särskilda skäl för det. Om uppgifterna gäller ett brott som kommer att begås får de alltid användas för att förhindra brottet.¹⁹⁴

3.4.5 Granskning, bevarande och förstörande av uppgifter

Om en upptagning eller uppteckning gjort vid verkställandet av hemlig dataavläsning ska den granskas snarast möjligt. Sådan granskning görs av åklagaren, undersökningsledaren eller rätten. Dessa ska, i de delar de är av betydelse för utredningen, bevaras fram till förundersökningens nedläggande eller avslutande, alternativt om åtal väcks, till målets slutliga avgörande. De delar som är av betydelse för att förhindra ett brott som inte redan begåtts ska bevaras så länge som de behövs för att förhindra brottet, därefter ska de förstöras.¹⁹⁵ I allt väsentligt gäller samma för granskningen, bevarandet och förstörandet av uppgifter utanför förundersökning.¹⁹⁶

¹⁹² 29 § lag (2020:62) om hemlig dataavläsning, 12 § lag (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

¹⁹³ Se avsnitt 3.4.3.2.

¹⁹⁴ 30 § lag (2020:62) om hemlig dataavläsning, 21 a § lag (1991:572) om särskild utlänningskontroll.

¹⁹⁵ 28 § lag (2020:62) om hemlig dataavläsning, 27 kap 12, 24 §§ rättegångsbalken.

¹⁹⁶ Se 29-31 §§ lag (2020:62) om hemlig dataavläsning och däri hänvisade bestämmelser.

3.4.6 Underrättelse till enskilda

Vid hemlig dataavläsning under förundersökning gäller samma i stort sett samma bestämmelser kring underrättelser som för motsvarande uppgiftstyper som framkommer vid användning av övriga hemliga tvångsmedel.

Vid kameraövervaknings- eller rumsavlyssningsuppgifter ska därmed utöver innehavaren av informationssystemet, även innehavaren av den plats som tillståndet avsett typiskt sett ska underrättas. För övriga uppgiftstyper gäller istället i allt väsentligt de regler om underrättelser som gäller för hemlig avlyssning av elektronisk kommunikation. Det innebär som huvudregel att den som är eller har varit misstänkt för brottet ska, om inte annat följer av sekretess, underrättas om den åtgärd som verkställts mot den misstänkte och att om någon annan än den misstänkte innehar informationssystem ska även den underrättas om den övervakning som den utsatts för.¹⁹⁷

3.5 Sammanfattning av lagen

Uppgifter som kan inhämtas eller avläsas

Hemlig dataavläsning får användas av de brottsbekämpande myndigheterna för att verkställa sådana åtgärder som motsvarar de som tidigare kunde verkställas genom andra hemliga tvångsmedel, det vill säga kommunikationsavlyssnings-, kommunikationsövervaknings-, plats-, kameraövervaknings- och rumsavlyssningsuppgifter. Hemlig dataavläsning kan dock utöver de ovan uppräknade uppgifterna även ge tillgång till alla övriga uppgifter som lagrats i ett avläsningsbart informationssystem samt uppgifter som visar hur informationssystemet används utöver de ovan uppräknade. Myndigheterna kan även i vissa fall hindra att meddelanden når fram.

¹⁹⁷ 28 § lag (2020:62) om hemlig dataavläsning, 27 kap 31-33 §§ rättegångsbalken.

Huvudregel för användning inom förundersökning

Huvudregeln är att hemlig dataavläsning får användas inom en förundersökning om åtgärden är av synnerlig vikt för utredningen och om brottet som utreds har två års fängelse som minimistraff, om brottet är ett av de uppräknade samhällsfarliga brott, om gärningen är straffbar och en osjälvständig brottstyp som hänför sig till någon av de två tidigare, eller om brottet kan antas ha ett straffvärde på över två års fängelse. Det måste vidare finnas särskild anledning att anta att informationssystemet som tillståndet avser har använts eller kommer att användas av åtgärdens målperson. Målpersonen måste även vara skäligen misstänkt för brottet.

Särskilt om kommunikationsövervakning, kommunikationsavlyssning och platsuppgifter

Vid inhämtning eller avläsning av uppgifter som inte avser kameraövervakning eller rumsavlyssning får åtgärden även avse ett informationssystem som det finns synnerlig anledning att den misstänkte har kontaktat eller kommer att kontakta. Hemlig dataavläsning får även i vissa fall användas för att utreda vem som skäligen kan misstänkas för ett brott. Det gäller kommunikationsövervaknings- och platsuppgifter och måste avse ett informationssystem som har använts vid ett brott eller i anslutning till brottsplatsen vid brottstillfället eller som är av synnerlig vikt för utredningen.

Särskilt om rumsavlyssning och kameraövervakning

Beträffande rumsavlyssningsuppgifter gäller högre krav. De får endast inhämtas genom hemlig dataavläsning vid brott med minimistraff om fyra års fängelse, vid vissa speciella brottstyper eller när det kan antas att brottets straffvärde överstiger fyra års fängelse och det är fråga om viss allvarlig brottslighet som uppräknas i bestämmelsen. Även dessa uppgifter får inhämtas vid osjälvständiga brottsformer till de uppräknade brotten om

gärningen är belagd med straff och det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig där. Är platsen någon annans stadigvarande bostad krävs istället synnerlig anledning. Vid användning som avser kameraövervakningsuppgifter får åtgärden avse en plats där den misstänkte kan antas komma att uppehålla sig. Platsen för åtgärden får dock aldrig vara någons stadigvarande bostad, vilket medför att en mobiltelefons kamera aldrig får aktiveras i någons hem och att detta måste säkerställas av den verkställande myndigheten.

Användning utanför förundersökning

Hemlig dataavläsning får även användas utanför förundersökning i tre undantagsfall, i syfte att förhindra viss särskilt allvarlig brottslighet, för särskild utlänningskontroll och i syfte att upptäcka brottslig verksamhet.

I preventivfallen beviljas tillstånd om det finns en påtaglig risk för att en person kommer att utföra ett av de i preventivlagen uppräknade brotten eller om en grupp kommer att utföra ett brott och en person kan befaras främja gruppens verksamhet. Åtgärden måste vara av synnerlig vikt för att förhindra brottsligheten och får inte avse rumsavlyssningsuppgifter. Avser åtgärden kameraövervakning får den inte verkställas mot någons stadigvarande bostad. Åtgärden kan även avse ett informationssystem som används eller som det finns särskild anledning att anta har använts eller kommer att användas av en sådan person som har beskrivits i detta stycke. I andra fall än rumsavlyssning och kameraövervakning får åtgärden även avse ett informationssystem som det finns synnerlig anledning att antas att personen har kontaktat eller kommer att kontakta.

I utlänningsfallen krävs även där att personen använder informationssystemet eller att det finns särskild anledning att anta att personen gör det. Åtgärden får i vissa fall avse ett informationssystem som används av en utlänning som omfattas av ett utvisnings- eller avvisningsbeslut och som det kan befaras kommer att begå eller medverka till ett terroristbrott eller försök, förberedelse

eller stämpling till terroristbrott. I samma fall som i preventivfallen får åtgärden även avse ett informationssystem som det finns synnerlig anledning att anta att utlänningen under tillståndstiden har kontaktat eller kommer att kontakta. För all användning i utlänningsfallen krävs synnerliga skäl och att åtgärden är av betydelse för att utreda om utlänningen eller en grupp han tillhör planlägger eller förbereder terroristbrott. Åtgärden får aldrig avse kameraövervakning eller rumsavlyssning.

I underrättelsefallen får åtgärden avse kommunikationsövervakning eller platsuppgifter om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslighet som räknas upp i inhämtningslagen. Åtgärden får inte i dessa fall användas för att hindra meddelanden och vid kameraövervakning får åtgärden endast avse uppgifter i förfluten tid. Det ska vara fråga om ett brott med två års fängelse som minimistraff eller vissa särskilt angivna brott.

Rättssäkerhetsgarantier

Tillstånd om hemlig dataavläsning ska som huvudregel prövas av en domstol på ansökan av åklagaren. Offentlig ombud ska utses och denne ska utgöra motpart till den ansökande myndigheten. I undantagsfall kan tillstånd även ges av åklagaren direkt, det gäller när dröjsmål är av väsentlig betydelse för syftet med åtgärden. Åklagaren ska i sådana fall genast anmäla detta till domstolen varpå domstolen prövar ärendet skyndsamt. Har ett tillstånd utfärdats utan tillräckliga skäl får de uppgifter som framkommit till följd av verkställigheten inte ligga personer som omfattats av den till last i en brottsutredning. Beslut verkställs direkt men kan överklagas och ska då skyndsamt handläggas. Finns det inte skäl för åtgärden ska tillståndet omedelbart upphävas. Domstolen ska alltid skyndsamt underrätta Säkerhets- och integritetsskyddsmyndigheten vid beslut om tillstånd till hemlig dataavläsning.

Verkställandet av åtgärden får inte medföra någon olägenhet eller skada som inte är absolut nödvändig. Det informationssystem som åtgärden avser ska återställas till den informationssäkerhet som det hade innan verkställigheten och göras obrukbara så snabbt som möjligt efter tillståndets upphörande.

Hemlig dataavläsning får aldrig användas för att ta upp eller avläsa uppgifter från personer i verksamheter som omfattas av tystnadsplikt eller ingår i trossamfund, såsom mot advokater, präster eller läkare med flera. Åtgärden får inte heller användas mot informationssystem som är en beständig del av en sådan verksamhet och som används i något av verksamhetens syften eller som är särskilt avsett att användas i verksamheten. Förbudet mot åtgärden i syfte att få del av lagrade uppgifter eller uppgifter som visar hur informationssystemet används motsvarar uppgifter som omfattas av rättegångsbalkens beslagsförbud. Från detta undantas sådant som i vissa fall undantas från tystnadsplikten, i de fallen kan ändå uppgiften inhämtas. Kommunikations- eller rumsavlyssningsuppgifter som framkommer i telefonsamtal, samtal eller andra meddelanden som avser en person som enligt ovan inte kan vittna i domstol får inte förekomma. Detta motsvarar avlyssningsförbudet i rättegångsbalken och preventivlagen. Om en uppgift som omfattas av någon av de ovan beskrivna förbuden bli föremål för hemlig dataavläsning ska åtgärden omedelbart avbrytas och de förbjudna uppgifterna omedelbart förstöras.

Vid överskottsinformation i förundersökningsfallen gäller som huvudregel följande. Uppgifter om brott som tillståndet inte avser får användas för att utreda brottet. Uppgifterna får ligga till grund för förundersökning om brottet har ett maxstraff om minst ett års fängelse och det kan antas att påföljden överstiger böter eller om det finns särskilda skäl för det. Vid rumsavlyssning får uppgifterna endast användas i utredningen om de avser ett sådant allvarligt brott som motiverar rumsavlyssning eller annat brott med ett maxstraff om minst tre års fängelse. Uppgifter om andra brott än det tillståndsgrundande får alltid användas för att förhindra brott. I preventivfallen får uppgifterna användas om de kan grunda ett tillstånd till hemlig dataavläsning avseende

kommunikationsövervaknings- eller platsuppgifter och även utan ett sådant tillstånd får de användas för att inleda en förundersökning. I utlänningsfallen får de användas för att utreda brottet och får ligga till grund för en förundersökning vid samma omständigheter som för förundersökningsfallen. I underrättelsefallen får uppgifterna användas för att utreda brottet om det rör sig om brottslighet som användning av tvångsmedlet och försök, förberedelse eller stämpling till sådant brott om gärningen är belagd med straff, eller andra brott med ett maxstraff om minst tre års fängelse.

Uppgifter som framkommer vid verkställandet av hemlig dataavläsning ska granskas snarast möjligt. Granskningen görs av åklagaren, undersökningsledaren eller rätten. De delar som är av betydelse för utredningen sparas fram till förundersökningens nedläggande eller avslutande eller när åtal väcks, tills målets slutliga avgörande. De delar som är av betydelse för att förhindra ett brott bevaras så länge de behövs för att uppfylla det syftet och förstörs därefter.

Enskilda ska som huvudregel underrättas om den brottsmisstanke som riktas eller har riktats mot dem och om den en åtgärd som verkställts mot dem. Någon annan som innehar ett informationssystem som blivit föremål för åtgärden ska också underrättas om åtgärden. Vid kameraövervaknings- eller rumsavlyssningsuppgifter ska även innehavaren av den plats som åtgärden avsett underrättas om åtgärden. Underrättelse är i vissa fall inte möjligt på grund av sekretess.

4 Den praktiska efterlevnaden

Här ska en kortare studie av resultaten av de brottsbekämpande myndigheternas tidigare användning av hemliga tvångsmedel presenteras. Detta görs för att ge en mätbar enhet i begreppet ”effektivitet”, och således skapa en faktisk tyngd att väga mot den enskildes integritetsintresse.

4.1 Säkerhets- och integritetsskyddsnämndens tillsyn

I avsnittet ges ett kritiskt perspektiv på de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. Det är en viktig del av att förstå syftet med relevanta rättighetsskydd och de rättssäkerhetsgarantier som måste ingå i en lagstiftning kring hemliga tvångsmedel.

Avsnittet visar att det i verkställigheten förekommer brister, men ger inte en varken fullständig eller rättvisande bild av myndigheternas arbete. Det visar inte att det finns ett uppsåt till misskötsamhet inom de brottsbekämpande myndigheterna, i många fall har det klarlagts av nämnden att bristerna beror på exempelvis organisatoriska utmaningar eller hög arbetsbelastning. Syftet är att illustrera att det inte bör föreligga en presumtion för att användningen kommer vara lagenlig. Verkställigheten måste präglas av ständig tillsyn och utvärdering för att säkerställa en rättssäker tillämpning, anser jag.

4.1.1 Allmänna synpunkter

Säkerhets- och integritetsskyddsnämnden, härafter kallad SIN, är den instans som ska utöva tillsyn över tvångsmedelsanvändningen och som ovan anförts ska beslut om tillstånd till hemlig dataavläsning rapporteras till nämnden. I

SOU 2018:61 ”Rättssäkerhetsgarantier och hemliga tvångsmedel” granskades samtliga utlåtanden från nämnden sedan 2013.¹⁹⁸

SIN har framfört kritik mot såväl Åklagarmyndighetens som Polismyndighetens dokumentation och tvångsmedelsanvändning. Om Åklagarmyndigheten anmärker SIN att beslut om förstörande av material och om berörda ska underrättas eller inte tas för sent. Även att dokumentation om datum för förundersökningars avslut och nedläggande saknas, vilka behövs för att undersöka om beslut tagits i rätt tid.¹⁹⁹ Inom Polismyndigheten finns det, enligt utredningen, problematik rörande materials förstörande och dess anslutning till åklagarens beslut om förstörande. Det är enligt SIN inte ovanligt att det går flera månader mellan åklagarens beslut att uppgifter ska förstöras och Polismyndighetens åtgärd faktiskt förstör materialet. Intyg om materialets förstörande skickas inte heller alltid till ansvarig åklagare. Polismyndigheten har i flera fall kritiserats av SIN för att verkställigheten av hemliga övervakningsåtgärder fortlöpt en tid efter att tillståndstiden löpt ut. Tvångsmedlens tillämpning har dock generellt verkställts i enlighet med gällande tillstånd.²⁰⁰ SIN har i flera fall anmält att brott i samband med verkställighet kan ha begåtts, till exempel vid övervakning efter att tillståndstiden löpt ut.²⁰¹

4.1.2 Tillståndsprovning

SIN anmärkte 2016 att det vid förlängningar av tillstånd till tvångsåtgärder under året inte angavs skäl för åklagarens begäran, men att tillstånden ändå beviljades. Nämnden påpekade att det var av stor vikt att skäl för åtgärden anges, både för rättens provning och för kontroll i efterhand.²⁰²

¹⁹⁸ SOU 2018:61 s. 85.

¹⁹⁹ SOU 2018:61 s. 85 f.

²⁰⁰ SOU 2018:61 s. 86.

²⁰¹ Ibid.

²⁰² SOU 2018:61 s. 87.

Åklagarkammaren i Kalmar beviljades under 2017 tillstånd till hemlig avlyssning av elektronisk kommunikation trots att det saknades behov av det. Åklagaren hade ansökt om tillståndet på polisens begäran utan avsikt att faktiskt verkställa åtgärden. SIN konstaterade att tillståndet inte hade lagstöd.²⁰³

4.1.3 Verkställighet utanför tillstånd

I kategorin verkställighet av tillstånd utanför tillståndet redovisade utredningen uppgifter som tydde på att Polismyndigheten avbrutit en åtgärd om hemlig rumsavlyssning först tre dagar efter att tillståndet till åtgärden hävts. När samtliga tvångsmedelsärenden under 2015 och 2016 som rapporterats av åklagare vid Ekobrottsmyndigheten granskades visade det sig att det i ett ärende beslutades av åklagare att en hemlig avlyssning av två telefonnummer skulle avbrytas innan tillståndstiden löpt ut. Åklagaren upprättade en beslutshandling för respektive telefonnummer, men den ansvarige polisinspektören underrättade den centrala avlyssningsfunktionen om endast ett av de två hävningsbesluten vilket medförde att det ena telefonnumret avlyssnades fram tills den ursprungliga tillståndstiden löpte ut, tre veckor senare.²⁰⁴

I andra fall konstaterades att Polismyndigheten under 2013 utfört hemlig avlyssning i minst tolv timmar avseende ett nummer, efter att åklagaren hävt tillståndet. I ett liknande fall hade två telefonnummer avlyssnats under tolv timmar efter att tillståndet hävts. Under 2016 hade Polismyndigheten i Göteborg verkställt tillstånd till hemlig övervakning av elektronisk kommunikation utanför tillståndstiden. I första ärendet pågick hemlig övervakning i cirka 34 timmar helt utan tillstånd och uppgifter om meddelanden övervakades utan rätt tillstånd under över åtta dagar. I nästa

²⁰³ SOU 2018:61 s. 87.

²⁰⁴ SOU 2018:61 s. 89.

ärende verkställdes övervakningen i nio timmar utan tillstånd. Under en granskning av Åklagaren i Falun visade det sig att det hade verkställts övervakning av elektronisk kommunikation innan ett tillstånd meddelats under 2014.²⁰⁵

4.1.4 Skyldighet att häva tillstånd

När utredningen granskade efterlevnaden av hävningar av tillstånd framkom att åklagare vid Åklagarkammaren i Kalmar vid tre tillfällen i ärenden som inletts under 2015 eller 2016 underlåtit att häva tillstånd till hemliga tvångsåtgärder trots att de vetat att besluten inte skulle verkställas. Det var enligt nämnden inte tillräckligt att de vidtagit åtgärder för att hindra verkställighet.²⁰⁶

En åklagare vid Åklagarkammaren i Östersund brast i sin dokumentation vid en åtgärd om hemlig avlyssning av elektronisk kommunikation av tre personer. Tillståndstiden sträckte sig över fyra månader men teletrafik hade endast förekommit under de första tre dagarna och den sista månaden. Tillstånden till avlyssning av två personer hade hävts. Hävningarna fanns inte dokumenterade och det gick inte på något sätt klarlägga hur åklagaren hade resonerat kring den tredje personen. Nämnden ansåg att omständigheterna talade för att även det tredje tillståndet borde ha hävts.²⁰⁷

4.1.5 Avlyssningsförbud

SIN granskade i slutet av 2017 Polismyndighetens rutiner avseende avlyssningsförbudet²⁰⁸ i rättegångsbalken. Nämnden fick då ta del av polisens

²⁰⁵ SOU 2018:61 s. 89 f.

²⁰⁶ SOU 2018:61 s. 90.

²⁰⁷ Ibid.

²⁰⁸ Avlyssningsförbudet framgår i 27 kap 22 § rättegångsbalken.

riktlinjer avseende användning och hantering av hemliga tvångsmedel PM 2017:53. SIN ansåg att bestämmelserna kring förbudet var komplexa och svårtillgängliga. Polismyndigheten använde en försiktighetsprincip i fråga om avlyssningsförbudet men påpekade att det endast var vissa uppgifter som omfattades av förbudet. Överlag bedömde nämnden att riktlinjerna var kortfattade, ofullständiga och så generellt utformade att de inte gav någon egentlig vägledning. Vid en granskning hos Ekobrottsmyndigheten framgick att myndigheten 2013 av misstag avlyssnat ett samtal mellan en advokat och en tidigare klient. Nämnden ansåg att åklagaren borde ha omedelbart beslutat att förstöra materialet, istället tog åklagaren del av samtalet. Nämnden ansåg inte att försiktighetsprincipen hade efterlevts i ärendet.²⁰⁹

4.1.6 Dokumentation och förstöring av material

Vid en granskning av ett ärende avseende hemlig rumsavlyssning i Södertörns åklagarkammare hade beslutet att förstöra materialet fattats över tre månader efter lagakraftvunnen dom i målet. Vid en undersökning av samtliga tvångsmedelsärendens som inletts under 2015 eller 2016 av Åklagaren i Kalmar framgick att beslut om förstöring av material i en fjärdedel av ärendena fattats mellan två och fjorton månader efter att förundersökning lagts ned eller avslutats. I flera ärenden saknades även intyg om att förstöring hade ägt rum.²¹⁰

Vid en annan granskning fick Polismyndigheten skarp kritik för sitt förfarande vid beslut om förstöring av material under 2016. Granskningen visade att beslutet endast i två ärenden hade verkställts inom ett par veckor från beslutsdatumet och i vissa fall hade det dröjt upp till två år innan material hade förstörts.²¹¹

²⁰⁹ SOU 2018:61 s. 90 ff., 93.

²¹⁰ SOU 2018:61 s. 92.

²¹¹ SOU 2018:61 s. 94.

4.1.7 Underrättelse i efterhand till enskilda

Vid en granskning av ett ärende vid Västerorts åklagarkammare i Stockholm framförde SIN kritik efter att det visat sig att en åklagare missförstått reglerna kring underrättelse av enskilda. Personen hade underrättats nio månader för sent eftersom att åklagaren trodde att prövningen om personen ska underrättas skulle göras inom en månad efter förundersökningens avslutande, istället för en månad efter att personen avskrivits från utredningen.²¹²

Nämnden granskade samtliga tvångsmedelsärenden vid Åklagarkammaren i Uppsala under 2016. Utav alla kammarens ärenden där nämnden meddelats om att underrättelse inte skett, såg nämnden att den första prövningen om personen skulle underrättas endast i ett fall gjorts inom den tiden som lagen föreskriver. Nämnden kritiserade även åklagarkammaren för att sekretessprövningarna i besluten om uppskjuten eller underlåten underrättelse endast innehöll så standardiserade formuleringar att man kunde ifrågasätta om någon individuell sekretessprövning ens hade gjorts.²¹³

Vid en granskning av samma typ av ärenden under 2014 vid Åklagarkammaren i Uddevalla fick kammaren skarp kritik. Granskningen visade att den första prövningen i alla ärenden förutom ett hade försenats med mellan två och tolv månader.²¹⁴

4.1.8 Nämndens efterhandskontroll

SIN upptäckte vid en granskning av ärenden hos Åklagarkammaren i Östersund att dokumentationen i ett par ärenden varit så undermålig att nämnden inte lyckades följa hur handläggningen gått till. De lyckades inte heller klarlägga de faktiska förhållandena runt den användning som tillåtits

²¹² SOU 2018:61 s. 98.

²¹³ SOU 2018:61 s. 99 f.

²¹⁴ SOU 2018:61 s. 101.

beträffande de hemliga tvångsmedlen. Vid en granskning av Åklagarkammaren i Linköping visade det sig att det i två av de ärenden som nämnden granskade hade gått fem månader innan nämnden underrättats om åklagarens beslut om att underlåta underrättelse.²¹⁵

4.1.9 Partsinsyn

I tre ärenden som SIN granskade hade åtal väckts innan de åtalade fått reda på att de under förundersökningen hade varit föremål för övervakning genom hemliga tvångsmedel. Nämnden underströk den misstänktes ovillkorliga rätt att få del av uppgifter om att hemliga tvångsmedel använts i utredningen av den gärning som den misstänkte står åtalad för. Det gäller även om uppgifter från övervakningen inte åberopas av åklagaren. Parterna var dock inte helt eniga om rättsläget och vice riksåklagaren ställde sig i ärendet tveksam till om åklagarens underlåtelser att underrätta de åtalade hade varit lagenligt. Nämnden bedömde dock att åklagarens agerande varit rättsstridigt.²¹⁶

4.2 Effektivitetsbegreppet

Den centrala avvägningen som, i såväl lagstiftningsarbetet som vid tillämpningen av tvångsmedel, ska göras mellan intresset av en effektiv brottsutredning och intresset av personlig integritet förutsätter både att effektiviteten utvärderas och att integritetsintrången konkretiseras. Det är enligt min uppfattning mot denna bakgrund som effektivitetsbegreppet måste definieras och de tvångsmedlens förmodade effektivitet undersökas.

²¹⁵ SOU 2018:61 s. 102.

²¹⁶ SOU 2018:61 s. 103.

4.2.1 Språklig definition

I Svenska Akademiens ordbok kan läsas att innebörden av att något är ”effektivt” kan förstås vara att det ”medför avsedd verkan”.²¹⁷

Enligt Nationalencyklopedins digitala uppslagsverk är en ”effektiv” åtgärd en åtgärd som ”ger (gott) resultat”.²¹⁸ Synonymt med ordet ”effektiv” är enligt Nationalencyklopedin ord som till exempel ”verkningsfull” och ”ändamålsenlig”.²¹⁹

4.2.2 Definition i tvångsmedelssammanhang

I förarbeten kring användning och införande av hemliga tvångsmedel har effektivitetsbegreppet förekommit vid flertalet tillfällen. I utredningen SOU 2005:38 ”BRU” ovan, föreslogs till exempel att hemlig övervakning i vissa fall skulle få användas utan att det fanns någon som var skäligen misstänkt för brottet. Detta i syfte att öka effektiviteten i den brottsutredande verksamheten.²²⁰ Med effektivitet avsågs då till synes ökad upplärning av brott, det vill säga slutresultatet av brottsutredningen.²²¹

I den senare utredningen SOU 2009:1 ”Polismetodutredningen” var syftet att stärka och bygga ut rättssäkerheten och integritetsskyddet, samtidigt som man även syftade till att upprätthålla en effektiv brottsbekämpande verksamhet.²²²

²¹⁷ ”Effektiv”, Svenska Akademiens ordbok, <<https://www.saob.se/artikel/?seek=effektiv&pz=2>>, besökt 2020-04-29.

²¹⁸ ”Effektiv”, Nationalencyklopedin, <<https://www.nese.ludwig.lub.lu.se/uppslagsverk/encyklopedi/l%C3%A5ng/effektiv>>, besökt 2020-04-29.

²¹⁹ ”Effektiv”, Nationalencyklopedin, Svenska synonymer, <<https://www.nese.ludwig.lub.lu.se/ordb%C3%B6cker/#/search/norstedts-synonym-sv-sv?q=effektiv>>, besökt 2020-04-29.

²²⁰ SOU 2005:38 s. 19, 22 ff., 153, 195.

²²¹ Landström (2017), s. 197, 202 f.

²²² SOU 2009:1 s. 16, 107.

Både BRU och Polisutredningens förslag diskuterades i en senare proposition i vilken effektivitetsbegreppet även här främst kopplades till förmågan att klara upp brott.²²³

I BRU förslogs även att tillstånd till hemlig övervakning skulle omfattas av ett tillstånd till hemlig avlyssning. För detta fanns enligt utredningen ”effektivitetsskäl av såväl operativ som mer formell eller administrativ karaktär”²²⁴, vilket syftade på besparingar av resurser inom rättsväsendet.²²⁵ Utredningen föreslog även att åklagare skulle kunna fatta interimistiska beslut om tillstånd till hemliga tvångsmedel. Detta föreslogs i syfte att förhindra att de brottsbekämpande myndigheterna i akuta fall skulle ”förlora i effektivitet” till följd av att regler om obligatorisk tillståndsprövning i domstol införts.²²⁶ I Polismetodutredningen förslogs samma sak med hänvisning till att möjligheten att fatta snabba beslut var ”nödvändig för en framgångsrik brottsbekämpning”.²²⁷ I den efterföljande propositionen formulerades införandet av interimistiska åklagartillstånd som ”nödvändigt för en effektiv brottsbekämpning”.²²⁸ Utredningens användande av ”framgångsrik brottsbekämpning” verkar därför i sammanhanget motsvara begreppet ”effektiv brottsbekämpning”.

Ett annat exempel är SOU 2011:45 ”Förundersökningsutredningen” som föreslog den nu befintliga lagen som ger polisen rätt att i samband med förhör omhändertaga elektronisk kommunikationsutrustning tillfälligt och att kroppsvisitera förhörspersonen för att hitta utrustningen.²²⁹ Utredningen ansåg att en sådan befogenhet medförde effektivitetsvinster för den brottsutredande verksamhet vilka i sammanhanget vägde tyngre än det

²²³ Landström (2017), s. 203.

²²⁴ SOU 2005:38 s. 221.

²²⁵ Landström (2017), s. 203.

²²⁶ SOU 2005:38 s. 201.

²²⁷ 2009:1 s. 119.

²²⁸ Prop. 2011/12:55 s. 78 f.

²²⁹ 23 kap 9 a § rättegångsbalken.

personliga integritetsskyddet. Åtgärden var ämnad att förhindra kommunikation som kunde försvåra utredningen och motiverades med att det skulle öka möjligheterna att lagföra personer eller i alla fall minska utredningens omfattning, komplexitet och kostnader.²³⁰ Såväl ökad uppkläring av brott som minskad resursåtgång omfattades alltså av effektivitetsbegreppet i sammanhanget.²³¹

Sammanfattningsvis kan sägas att begreppet effektivitet vid lagstiftningsarbete kring tvångsmedelsanvändning och polisiära arbetsmetoder framför allt syftar på möjligheten att klara upp och lagföra brott, men kan också syfta på resursåtgång.²³²

4.3 Lagstiftarens användning av effektivitetsbegreppet

I SOU 2017:89 ”Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet” diskuteras den hemliga dataavläsningens förmodade effektivitet. Utredningen anser att en utgångspunkt bör vara att effektiviteten inte bör och knappas kan utvärderas genom siffror eller andelstal.²³³ Enligt utredningen ska effektivitetsanalysen vara bred och inte avgränsas till frågan om effektivitet av tvångsmedlet, bland annat mot bakgrund av att det enligt utredningen inte finns någon entydig definition av begreppen. Det som dock står klart är att utredningen ska utreda om hemlig dataavläsning kan förväntas vara en effektiv metod för brottsbekämpning i förhållande till behovet av åtgärden.²³⁴ Av betydelse för effektiviteten är hur bearbetning av informationen som inhämtas förväntas gå till, hur myndigheterna ska skaffa

²³⁰ SOU 2011:45 s. 381 f.

²³¹ Landström (2017), s. 204.

²³² Ibid.

²³³ SOU 2017:89 s. 281.

²³⁴ SOU 2017:89 s. 282.

sig tekniska möjligheter att använda metoden, risken för att kriminella anpassar sitt beteende för att kringgå det nya tvångsmedlets verktyg och vilka resurser metoden kräver. Uppgifterna i utredningen baseras i huvudsak på uppgifter från de brottsbekämpande myndigheterna.²³⁵

4.3.1 Kvantitativ effektivitet

Enligt utredningen bör den kvantitativa effektiviteten bedömas i förhållande till behovet av åtgärden. För uppgifter om meddelanden i elektroniska kommunikationsnät bedöms hemlig dataavläsning ge begränsad kvantitativ effektivitet i förhållande till det identifierade behovet av hemlig dataavläsning, bland annat på grund av kryptering och anonymisering. Effektiviteten i kvantitativ mening förväntas vara låg med anledning av till exempel omfattande förberedelser och tekniska svårigheter vid verkställighet.²³⁶

Beträffande platsuppgifter anförs att omfattningen av behovet av hemlig dataavläsning för att komma åt dessa är svårt att fastställa. I många fall är hemlig dataavläsning inte nödvändigt för att inhämta dessa uppgifter. I många fall torde tidigare teknik för inhämtning av platsuppgifter vara tillräcklig. Därutöver är redovisningen av användandet bristfällig, vilket i kombination med det tidigare anförda ledde utredningen till uppfattningen att införandet av hemlig dataavläsning skulle medföra en begränsad effektivitet beträffande uppgiftstypen.²³⁷

Hemlig dataavläsning för inhämtning av kameraövervaknings- och rumsavlyssningsuppgifter behövs inte, till skillnad från åtgärderna ovan, för att kunna verkställa tidigare tvångsmedel. Istället grundas behovet i de praktiska svårigheter som i vissa enskilda fall stöts på, till exempel

²³⁵ SOU 2017:89 s. 282 f.

²³⁶ SOU 2017:89 s. 283 f.

²³⁷ SOU 2017:89 s. 284 f.

svårigheterna att få tillgång till ett lämpligt ställe att montera utrustningen på. Vidare är det även relativt få personer som blir föremål för åtgärderna vilket gör att behovet avser mycket få fall vilket enligt utredningen gör att hemlig dataavläsning framstår som en i kvantitativt hänseende tämligen effektiv åtgärd i förhållande till behovet.²³⁸

För uppgifter som lagras på en utrustning och uppgifter som visar hur en utrustning används pekar utredningen även här på svårigheter att fastställa behovet. Eftersom att utrustning med lagrade uppgifter som myndigheten inte kommer åt ofta beslagtas, kommer det enligt utredningen vida överstiga det antal i vilka hemlig dataavläsning kommer att kunna verkställas. Därav är åtgärden vid dessa uppgifter av begränsad effektivitet. För uppgifter som visar hur utrustningen används, det vill säga uppgifter som varken lagras eller kommuniceras, är de ännu svårare att fastställa behovet. Även om behovet av att samla in dessa torde vara väsentligt lägre än behovet av att samla in lagrade uppgifter, verkar möjliga verkställighetstillfällen understiga behovstillfällena, därför framstår hemlig dataavläsning beträffande dessa uppgifter också som begränsat effektiv.²³⁹

4.3.2 Kvalitativ effektivitet

Med kvalitativ effektivitet menas om en åtgärd i ett enskilt fall kan förväntas ge de uppgifter som den är avsedd att inhämta. Utredningen redovisar en rad tekniska svårigheter med hemlig dataavläsning. Slutsatsen utifrån de redovisade tekniska åtgärderna blir dock att dessa kommer att beaktas av de brottsbekämpande myndigheterna innan verkställighet av en eventuell åtgärd, vilket medför att effektiviteten i kvalitativ mening enligt utredningen kan förväntas bli hög.²⁴⁰

²³⁸ SOU 2017:89 s. 285.

²³⁹ SOU 2017:89 s. 286.

²⁴⁰ SOU 2017:89 s. 286 ff.

Vidare ansåg utredningen beträffande hemlig dataavläsnings förväntade kvalitativa nyttoeffekter följande. Baserat på tidigare undersökningar²⁴¹ kunde utredningen anföra att den information som de brottsbekämpande myndigheterna hoppats få tillgång till genom användning av de tidigare tvångsmedel som funnit att tillgå, i stor utsträckning motsvarade de uppgifter som de lyckades erhålla. Vidare menade utredningen att det inte fanns något som talade emot att nyttoeffekterna av hemlig dataavläsning skulle vara mindre än de nyttoeffekter som följt av den tidigare hemliga tvångsmedelsanvändningen. Mot denna bakgrund ansåg utredningen att hemlig dataavläsning får anses vara en effektiv åtgärd i kvalitativ mening.²⁴²

4.4 De brottsbekämpande myndigheternas användning av tvångsmedel under 2018

Varje år redovisar regeringen hur reglerna om hemlig tvångsmedel har tillämpats under det gångna året. Redogörelsen bygger på uppgifter som Åklagarmyndigheten överlämnar till regeringen. Dessa uppgifter kommer ifrån Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Tullverket och Säkerhetspolisen. I Bilaga A framgår statistik från regeringens redovisning över nyttan av tvångsmedel under 2018, vilket är den nyaste statistiken. Den statistik som återges i bilagan avser uppgifter om i hur många fall tillstånd beviljats av domstolen, hur många gånger tillstånd nekats, hur många gånger åklagare beslutat om interimistiska tillstånd, samt hur många gånger interimistiska tillstånd upphävts av domstolen. Vidare framgår hur många procent av tillstånden som lett till någon nytta för olika delar av processen.

²⁴¹ Se SOU 2012:44 s. 496.

²⁴² SOU 2017:89 s. 289 f.

Regeringens redovisning är sammanställd så att en person som blir föremål för tillstånd till flera hemliga tvångsmedel redovisas i statistiken över samtliga tvångsmedel som personen utsatts för. Detta medför att det av statistiken inte framgår hur många av tillstånden som verkställts. Även nyttan riskerar att redovisas med för höga siffror, då en och samma nytta riskerar att redovisas under flera tvångsmedel på grund av svårigheterna att fastställa nyttan för en specifik åtgärd.

4.4.1 Nyttan av hemliga tvångsmedel

Regeringen anger i sin skrivelse att det i en rättsstat är grundläggande att skyddet för privat- och familjeliv respekteras. Detta intresse ställs mot behovet av tillräckliga befogenheter för de brottsbekämpande myndigheterna för att bedriva en *effektiv* brottsbekämpning. Myndigheterna måste i ”vissa väl avgränsade fall” kunna använda hemliga tvångsmedel som ”ett yttersta hjälpmedel”, anser regeringen. För att kunna avgöra vilken balans som ska råda mellan dessa intressen understryker regeringen att det är betydelsefullt att resultaten av användningen av hemliga tvångsmedel med tillräckligt god precision kan bedömas.²⁴³

Regeringen anger vidare att det, vid sidan av en noggrann proportionalitetsbedömning, är angeläget att redovisa *nyttan* som en tillämpning av de hemliga tvångsmedlen medför för den brottsbekämpande verksamheten. Med ”nytta” menas i skrivelsen vilken betydelse åtgärden har för utredningen. Nyttan för ett visst tvångsmedel är dock inte helt enkel att fastställa då en utredning kan lyckas genom att flera tvångsmedel kombineras menar regeringen. Syftet med redovisningen är dock att det så objektivt som möjligt ska gå att bedöma nyttan av användningen av hemliga tvångsmedel.²⁴⁴ Enligt regeringen kan det integritetsintrång som hemliga

²⁴³ Skr. 2019/20:56 s. 35.

²⁴⁴ Skr. 2019/20:56 s. 36.

tvångsmedel medför accepteras om behovet och nyttan av åtgärderna är tillräckligt stora.²⁴⁵

Under 2018 har det enligt regeringens skrivelse inte förekommit någon användning av tvångsmedel i Polismyndighetens underrättelseverksamhet enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.²⁴⁶

För tillämpningen av användning av tvångsmedel för inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet redovisas inte nyttan i annan form än genom anonymiserade exempel.²⁴⁷ Nyttan av säkerhetspolisens användning redovisas inte alls.²⁴⁸

4.4.1.1 Hemlig avlyssning av elektronisk kommunikation

Under 2018 ansökte de brottsbekämpande myndigheterna om tillstånd till hemlig avlyssning av elektronisk kommunikation vid 4673 tillfällen. Av dessa ansökningar avslogs 27 stycken, tillstånd beviljades därmed i 99,4 % av fallen. Antalet interimistiska tillstånd, så kallade åklagartillstånd, uppgick under året till 177 stycken, varav ett tillstånd sedan upphävdes av domstolen. Beviljandegraden för dessa tillstånd var även den 99,4 %. Nedan ska redovisas nyttan av de uppgifter som inhämtats genom åtgärden i de olika stadierna av lagförings- och utredningsprocessen.

²⁴⁵ Skr. 2019/20:56 s. 35.

²⁴⁶ Skr. 2019/20:56 s. 27.

²⁴⁷ Skr. 2019/20:56 s. 27 f.

²⁴⁸ Skr. 2019/20:56 s. 29.

Nyttan av uppgifter från hemlig avlyssning av elektronisk kommunikation under 2018			
UNDER FÖRUNDESRÖKNING	EFTER FÖRUNDESRÖKNING	ÖVERSKOTTINFORMATION	ÖVRIGT
Har i 47 % av fallen utgjort underlag i förhörssituation	Har i 19 % av fallen bidragit till att den misstänkte kunnat avföras från utredningen	Har i 19 % av fallen bidragit till att något tvångsmedel använts mot en annan person i samma förundersökning	Har i 42 % av fallen på annat sätt bidragit till att utredningen kunnat föras framåt
Har i 61 % av fallen medfört att effektiv spaning har kunnat genomföras	Har i 34 % av fallen bidragit till att den misstänkte kunnat åtalas	Har i 6 % av fallen använts för att utreda brott i en annan förundersökning	
Har i 34 % av fallen bidragit till att annat tvångsmedel använts mot den misstänkte	Har i 33 % av fallen åberopats som bevisning i stämningsansökan		
Har i 10 % av fallen bidragit till utredning av brottsutbyte			
Har i 46 % av fallen lett till stärkta misstankar mot den misstänkte			

4.4.1.2 Hemlig övervakning av elektronisk kommunikation

Under 2018 ansökte de brottsbekämpande myndigheterna om tillstånd till hemlig övervakning av elektronisk kommunikation vid 9233 tillfällen. Av dessa ansökningar avslogs 82 stycken, tillstånd beviljades därmed i 99,1 % av fallen. Antalet interimistiska tillstånd, så kallade åklagartillstånd, uppgick under året till 105 stycken, varav tre tillstånd sedan upphävdes av domstolen. Beviljandegraden för dessa tillstånd var 97,1 %. För dessa tillstånd har inte något nytta redovisats genom antal tillstånd eller procent av tillstånd som medfört nytta. Nyttan har endast redovisats genom ett fåtal anonymiserade exempel från tillämpningen, vilket endast tjänar till att visa att åtgärden *kan* medföra nytta, inte hur ofta så har varit fallet.

Tillstånd till hemlig övervakning av elektronisk kommunikation har utöver de fall i stycket ovan även meddelats vid 140 tillfällen med anledning av en begäran om internationell rättslig hjälp i brottmål. Dessa har dock medvetet exkluderats från statistiken då information om hur många ansökningar som avslagits saknas.

4.4.1.3 Hemlig kameraövervakning

Under 2018 ansökte de brottsbekämpande myndigheterna om tillstånd till hemlig kameraövervakning vid 153 tillfällen. Av dessa avslogs en ansökan, tillstånd beviljades därmed i 99,3 % av fallen. Antalet interimistiska tillstånd, så kallade åklagartillstånd, uppgick under året till 17 stycken, samtliga tillstånd fastställdes av domstolen. Beviljandegraden för dessa tillstånd var alltså 100 %. Nedan ska redovisas nyttan av de uppgifter som inhämtats genom åtgärden i de olika stadierna av lagförings- och utredningsprocessen.

Nyttan av uppgifter från hemlig kameraövervakning under 2018			
UNDER FÖRUNDERSÖKNING	EFTER FÖRUNDERSÖKNING	ÖVERSKOTTINFORMATION	ÖVRIGT
Har i 51 % av fallen utgjort underlag i förhörssituation	Har i 6 % av fallen bidragit till att den misstänkte kunnat avföras från utredningen	Har i 19 % av fallen bidragit till att något tvångsmedel använts mot en annan person i samma förundersökning	Har i 43 % av fallen på annat sätt bidragit till att utredningen kunnat föras framåt
Har i 61 % av fallen medfört att effektiv spaning har kunnat genomföras	Har i 40 % av fallen bidragit till att den misstänkte kunnat åtalas	Har i 4 % av fallen använts för att utreda brott i en annan förundersökning	
Har i 41 % av fallen bidragit till att annat tvångsmedel använts mot den misstänkte	Har i 41 % av fallen åberopats som bevisning i stämningsansökan		
Har i 8 % av fallen bidragit till utredning av brottsutbyte			
Har i 50 % av fallen lett till stärkta misstankar mot den misstänkte			

4.4.1.4 Hemlig rumsavlyssning

Under 2018 ansökte de brottsbekämpande myndigheterna om tillstånd till hemlig rumsavlyssning vid 130 tillfällen. Samtliga ansökningar beviljades, det vill säga i 100 % av fallen. Nedan ska redovisas nyttan av de uppgifter som inhämtats genom åtgärden i de olika stadierna av lagförings- och utredningsprocessen.

Nyttan av uppgifter från hemlig rumsavlyssning under 2018

UNDER FÖRUNDERSÖKNING	EFTER FÖRUNDERSÖKNING	ÖVERSKOTTINFORMATION	ÖVRIGT
Har i 24 % av fallen utgjort underlag i förhörssituation	Har i 3 % av fallen bidragit till att den misstänkte kunnat avföras från utredningen	Har i 0 % av fallen bidragit till att något tvångsmedel använts mot en annan person i samma förundersökning	Har i 33 % av fallen på annat sätt bidragit till att utredningen kunnat föras framåt
Har i 39 % av fallen medfört att effektiv spaning har kunnat genomföras	Har i 10 % av fallen bidragit till att den misstänkte kunnat åtalas	Har i 3 % av fallen använts för att utreda brott i en annan förundersökning	
Har i 16 % av fallen bidragit till att annat tvångsmedel använts mot den misstänkte	Har i 7 % av fallen åberopats som bevisning i stämningsansökan		
Har i 1 % av fallen bidragit till utredning av brottsutbyte			
Har i 33 % av fallen lett till stärkta misstankar mot den misstänkte			

5 Analys

5.1 Har hemlig dataavläsning utformats i enlighet med integritetsskyddet i gällande rätt?

Med avstamp i Europakonventionen kan inledningsvis upprepas att en inskränkning i den enskildes grundläggande fri- och rättigheter endast kan accepteras om den uppfyller vissa krav. Det som är av intresse är om inskränkningen tillgodoser ett ändamål som är godtagbart i ett demokratiskt samhälle och inte går utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett inskränkningen. De inskränkningar som lagstiftning om hemliga tvångsmedel aktualiserar och som ska analyseras här är intresset av personlig integritet, frihet att inte övervakas av staten, och rätten till en rättvis rättegång, att ha en faktisk möjlighet att försvara sig mot de anklagelser som riktas mot en.

Det kan inledningsvis konstateras att intresset av en effektiv brottsbekämpning och intresset av säkerhet i samhället är godtagbara i ett demokratiskt samhälle. Frågan blir istället om inskränkningen går utöver vad som är nödvändigt med hänsyn till ändamålet, alltså om inskränkningen är oproportionerligt långtgående i förhållande till vad som behövs för att uppnå en effektiv brottsbekämpning. Denna avvägning besvaras nedan i avsnitt 5.4.

Vidare ska tillåtandet och verkställandet av en åtgärd om hemliga tvångsmedel uppfylla de i svensk rätt stadgade principerna för tvångsmedelsanvändning. Proportionalitetsprincipen angränsar givetvis till inskränkningens tillåtenhet på det sätt att principen förbjuder åtgärder vars negativa skadeverkningar för målpersonen och andra som med för stor tyngd överväger vinningen som de medför för de brottsbekämpande

myndigheternas verksamhet. Beträffande lagens förhållande till övriga principer kan sägas följande.

Lagen kan sägas brista i legalitetshänseende då straffrätten ställer upp höga krav på lagstiftnings förutsebarhet och tydlighet. Den lagtekniska lösningen som lagstiftaren har valt på tvångsmedelsområdet präglas av komplexa lösningar och korshänvisningar mellan flertalet lagstiftningar. Lagstiftningen över hemlig dataavläsning utgör inte ett undantag från detta förfarande. Lagen har utformats på ett mycket komplicerat sätt med en stor mängd rekvisit som kräver efterforskningar och hög juridisk kompetens för att förstå. Rent allmänt framstår lagstiftningen som ett lappverk och mycket av tidigare lagstiftning används för att undvika att behöva skriva ut delar av hänvisad lagstiftning vid åtgärder som syftar till att till exempel inhämta motsvarande uppgifter som ett äldre tvångsmedel. Det är mycket svårt att överblicka lagstiftningen, i synnerhet för en person utan tidigare juridisk erfarenhet. 17 av lagens 33 paragrafer innehåller hänvisningar till andra lagstiftningar. Då lagstiftaren ska undvika att införa vaga, obestämda och mångtydiga rekvisit och sträva efter en förutsebar och återhållsam tillämpning måste tidigare lagstiftning över hemliga tvångsmedel sägas lämna en hel del i övrigt att önska. Då regeringen redovisar statistik som visar att tillstånd till hemliga tvångsmedel i genomsnitt beviljats i 99,2 % av fallen och interimistiska åklagartillstånd endast upphävts i 1,4 % av fallen, kan tillämpningen endast med svårighet betecknas som återhållsam. Statistiken kan dock tolkas som att åklagare och brottsbekämpande myndigheter i nästan samtliga fall gör helt korrekta bedömningar och näst intill aldrig ansöker om tillstånd i fall där behovet eller proportionaliteten brister.

Vid en sådan tolkning skulle ett välvilligt argument kunna bestå i att polisen utreder väldigt många brott per år och att drygt 14 000 st tillstånd på ett år skulle innebära en återhållsam tillämpning i kvantitativ mening. Problemet med en sådan tolkning bör på ett rent teoretiskt plan vara att statistiken i bilaga B visar att antalet tillstånd till hemliga tvångsåtgärder i genomsnitt har ökat med 53 % under en femårsperiod. I uppsatsen redovisas inte statistik över

nivåer av brottslighet eller vilken andel av brottsligheten som kan betecknas som allvarlig brottslighet och som därmed kan motivera tvångsmedelsanvändning av det aktuella slaget. Det verkar däremot osannolikt att sådan brottslighet har ökat med motsvarande procentsats under fem år, vilket leder mig till slutsatsen att tvångsmedelsanvändningen troligtvis på senare år har gått, eller är på god väg att gå, utanför ramarna för vad som kan anses utgöra en återhållsam tillämpning. Med anledning av att begränsningarna för och granskningen av tillämpningen av hemlig dataavläsning i allt väsentligt motsvarar desamma för tidigare tvångsmedel finns anledning att oroa sig för en liknande tillämpning för hemlig dataavläsning.

Beträffande ändamålsprincipen är min uppfattning att regelverket ger uttryck för det övergripande ändamålet, nämligen upprätthållandet av en effektiv brottsbekämpning. Tillämpningen av regelverket bör självklart utsättas för såväl tillsyn som minutiös granskning då åtgärden även i det enskilda fallet ska motiveras och ändamålet specificeras mer ingående. Detsamma gäller behovsprincipen, för vilken lagstiftningen även ger uttryck för genom exempelvis kravet att åtgärden ska vara av ”synnerlig vikt för utredningen”. I praktiken måste dock domstolen och de brottsbekämpande myndigheterna ansvara för att inga onödiga tillstånd beviljas. Statistik som visar att över 99 % av tillståndsansökningar beviljas och förekomsten av granskningar som visar att tillstånd har beviljats utan ambitionen att någonsin användas eller utan att motiveras, ger stöd för uppfattningen att regelverket inte på något sätt omöjliggör missbruk. En sådan hög beviljandegrad kan ur ett kritiskt perspektiv ses som en indikation på att tillståndsprövningen i domstol närmast tjänar som en processuell formalitet och att behovsprincipen inte ges särskilt stor betydelse vid en sådan prövning.

Vidare kan lagstiftningens utformning och innehåll i formell mening och på ett övergripande plan utvärderas utefter de kriterier som Europadomstolen

sammanställde i avgörandet *Roman Zakharov mot Ryssland*²⁴⁹. Brottskategorierna som kan motivera ett beslut om tillstånd till hemlig dataavläsning föreskrivs i flertalet paragrafer i lagen, exempelvis 4 §, där huvudregeln för tillstånd till användning inom förundersökning slås fast. Definitionen av de personkategorier som kan bli föremål för övervakningen framgår exempelvis av kravet att en person ska vara ”skäligen misstänkt” i 4 §. Begränsningar av övervakningens varaktighet återfinns i 25 § tredje stycket. Rutiner för undersökning, användning och lagring av data regleras i 28-31 §§. Vidare föreskrivs tystnadsplikt i 32 § och bestämmelser om uppgifters förstörande framgår av 23 och 27 §§. Lagstiftningen kan alltså på ett övergripande plan i sin utformning sägas nå upp till de krav som ställs på den i Europadomstolens praxis. Säkerhets- och integritetsnämndens granskning visar dock att lagstiftningens rättssäkerhet i hög utsträckning bestäms av den verkställande myndighetens tillämpning av densamma.

5.2 Uppfyller lagstiftningen kraven på processens kontradiktion och likställdhet i Europakonventionen?

Artikel 6 i EKMR tar sikte på och summerar rättsprocessen som helhet. Avgöranden visar att en rättegång kan anses rättvis trots att rättigheter kränkts i processen, dessa kan ”repareras” så att rättegången som helhet framstår som rättvis. I kombination med den svenska principen om den fria bevisprövningen riskerar en olikställdhet i processen att skapas genom att uppgifter som inhämtats olagligt genom hemlig övervakning åberopas som bevis i en rättegång. Detta förekommer inte på samma sätt i en rättsordning där olagligt framställd bevisning inte får åberopas under en rättegång. Det krävs därför att principen om parternas likställdhet och den kontradiktoriska principen respekteras för att garantera den tilltalade en rättvis rättegång. Det

²⁴⁹ Se avsnitt 2.3.3.

innebär att en misstänkt måste ges full insyn i den utredning som grundar misstankarna mot honom och bereda honom möjlighet att yttra sig över dessa. Den tilltalade måste ges möjligheter att ifrågasätta äktheten i uppgifter och till exempel få tillgång till samtliga upptagningar som lagrats över hans kontakter.

I praktiken är det lätt att se hur det kan samlas in stora mängder uppgifter och lagras timmar av upptagningar, där de brottsbekämpande myndigheterna endast åberopar en liten del som bevisning som kan tolkas till den tilltalades nackdel. Det finns en risk att resterande material hamnar i den så kallade ”slasken” och att en betydande arbetsinsats kommer att krävas av försvararen för att gå igenom denna. Det är av den anledningen av stor vikt att underrättelser lämnas till den som har utsatts för sådan övervakning men också viktigt ur integritetssynpunkt. I lagen finns bestämmelser om underrättelser till enskilda föreskrivna.

Även bestämmelser över bevarande av uppgifter finns som ovan beskrivits i den nya lagen. Efter en åklagares, undersökningsledares eller domstols granskning ska uppgifter som är av betydelse för utredningen bevaras fram till slutet av förundersökningen eller målets slutgiltiga avgörande. Det är en viktig bestämmelse ur kontradiktionssynpunkt då den stärker den tilltalades möjligheter att visa exempelvis hur de åberopade bevisuppgifterna kan sättas i sin rätta kontext och på så vis få en annan innebörd. Detta belystes av Europadomstolen i fallet *Natunen mot Finland*²⁵⁰. I avgörandet ansågs artikel 6 ha kränkts genom att polisen i samråd med åklagaren gjorde en bedömning över vilket material som var relevant för utredningen, utan att samråda med den tilltalade eller hans försvarare. Även avgörandet *Khan mot Förenade Kungariket*²⁵¹ stödjer denna uppfattning.

²⁵⁰ Se avsnitt 2.3.3.

²⁵¹ Ibid.

Den nya lagen kan tänkas lämna en öppning för just en sådan otillåten gallring då en omedelbar granskning görs efter verkställandet av hemlig dataavläsning, varpå åklagare, undersökningsledare eller rätten i sin granskning beslutar vad som är av betydelse för utredningen. I den granskning som har gjorts av Säkerhets- och integritetsnämnden över tillämpningen av regelverket framgår att underrättelser till enskilda i vissa fall har dröjt flertalet månader. Om ett samtal upptas och åberopas som bevisning i en annan kontext, och den tilltalade som övervakas inte har getts kännedom om övervakningen förrän flera månader passerat samtidigt som övriga samtal under övervakningsperioden gallrats ut, minskar den misstänktes möjligheter att försvara sig mot dessa uppgifter väsentligt. Det kan därför inte uteslutas att den som misstänks för ett brott eller än värre, övervakas i syfte att fastställa en misstanke om brott, i detta tidiga skede går miste om just denna rättighet att få ta del av och bemöta hela materialet som polisen har fått fram i utredningen.

En kränkning enligt artikel 6 ska som ovan anført utvärderas ur ett helhetsperspektiv över processen och en inskränkning av en rättighet medför i sig inte att rättegången är att anse som orättvis. Det visar den praxis från Europadomstolen som redogjorts för ovan.²⁵² Den nya lagen innehåller bestämmelser om ett oberoende granskande organ, SIN, samt bestämmelser om underrättelser till enskilda. SIN genomför omfattande granskningar och framför skarp kritik mot de brottsbekämpande myndigheterna. Detta organ i kombination med reglerna för underrättelser till enskilda får lagstiftningen i denna del, i formell mening, anses överensstämma med Europadomstolens praxis, såsom *Association for European Integration and Human Rights och Ekimdzhev mot Bulgarien*.²⁵³

²⁵² Se avsnitt 2.3.3, även avgörandet P.G. och J.H. mot Förenade Kungariket.

²⁵³ Se avsnitt 2.3.3.

5.3 Hur förhåller sig hemlig dataavläsning och dess inskränkningar till tidigare tvångsmedel?

Behovet av hemlig dataavläsning formuleras ett flertal ställen i förarbeten som att det bottnar i en ineffektivitet i befintliga tvångsmedels verkställande. Hemlig dataavläsning tjänar i en sådan kontext som ett hjälpmedel för att återfå den effektivitet som till exempel hemlig övervakning av elektronisk kommunikation i vissa fall kan uppskattas ha haft innan krypteringens och anonymiseringens verkliga utbredning i samhället. På samma linje anförs att de inskränkningar som verkställandet av hemlig dataavläsning medför för den enskildes integritet inte ökar nämnvärt då samma uppgifter inhämtas.

Lagstiftningens utformning ger i stor utsträckning stöd för denna uppfattning då regelverket ordnas efter vilken uppgift som åtgärden ska ge myndigheterna tillgång till. Som exempel kan anges hemlig dataavläsning i syfte att inhämta rumsavlyssningsuppgifter. Den i 27 kap 20 d § rättegångsbalken föreskrivna straffvärdesventilen och dess tillämpning översätts i propositionen direkt till tillämpningen av hemlig dataavläsning i syfte att inhämta rumsavlyssningsuppgifter enligt 4 och 6 §§ i nya lagen.²⁵⁴ Dessa korshänvisningar förekommer i bestämmelser för i stort sett samtliga uppgiftstyper, med undantag för de nya uppgiftstyper som hemlig dataavläsning möjliggör, såsom till exempel uppgifter om hur ett informationssystem har använts.

Det står dock klart att det nya tvångsmedlet hemlig dataavläsning i övriga hänseenden utgör ett större intrång i den enskildes personliga integritet än de tidigare hemliga tvångsmedlen, vilket är en uppfattning som delas av såväl regeringen som många av utredningarna. Den breda konsensus som råder beträffande den nyare lagstiftningens utökade inskränkningar i enskildas

²⁵⁴ Se avsnitt 3.4.2.2.

rättigheter borde enligt Europadomstolens praxis medföra att högre krav på rättssäkerhetsgarantier ska ställas. Kraven inkluderar större tydlighet och fler restriktioner i den nya, mer inskränkande, lagstiftningen.²⁵⁵

Det framstår som rimligt att en hackad mobiltelefon som medföljer den misstänkte i hans vardag, och som dessutom när som helst kan aktiveras för att uppta användnings-, avlyssnings- och kamerauppgifter utgör ett större integritetsintrång än ett beslag av en mobiltelefon, en övervakning av en specifik plats eller en avlyssning av telefonsamtal. I synnerhet då de brottsbekämpande myndigheterna bereds den faktiska möjligheten att fritt aktivera dessa funktioner, avsiktligt eller oavsiktligt, på platser och situationer där tvångsmedlet inte får användas i långt större utsträckning än för tidigare tvångsmedel. Ett exempel är den problematik som redovisas ovan, nämligen att kameraövervakningsuppgifter inte får upptas i någons stadigvarande bostad. Detta medför att efterlevnaden av förbud mot att uppta sådana uppgifter i användning av tidigare tvångsmedel var enkel att kontrollera. Utrustningen installerades helt enkelt på en plats som inte var någons stadigvarande bostad. Vid hemlig dataavläsning försvåras sådan tillämpning avsevärt då en hackad mobiltelefon i regel är mobil i den mening att den kan förväntas befinna sig på en mängd platser som då måste undersökas för att inte riskera en otillåten upptagning. Det blir en svårare tillämpning, såväl för den verkställande myndigheten som för dess granskare. En sådan svårighet i förhållande till de tidigare tvångsmedel gör följaktligen efterlevnaden av de tidigare regelverken högst aktuell för en bedömning av den förmodade efterlevnaden av den nya lagen. Särskilt då tydligare och fler restriktioner ska gälla för en mer ingripande åtgärd.

En kontroversiell del av den nya lagen är dess ökade integritetsinskränkningar i kombination med möjligheten att använda åtgärden mot andra än en misstänkt person. Ett avläsningsbart system, till exempel en mobiltelefon, som en misstänkt person lånar och använder för att spela ett spel kan bli

²⁵⁵ Se avsnitt 2.3.3, även avgörandet *Uzun mot Tyskland*.

föremål för övervakning. Detta riskerar givetvis att drabba en person som endast känner den person som polisen misstänker, endast genom att det fastställs att den misstänkte personen har använt mobiltelefonen.

Vidare får hemlig dataavläsning användas mot ett informationssystem i syfte att utreda vem som skäligen kan misstänkas för ett brott. Det kan exempelvis vara en mobiltelefon som befunnit sig vid en brottsplats vid tiden för brottet eller som på annat sätt är av synnerlig vikt för utredningen. Att övervakning i form av kommunikationsövervakning och avlyssning samt inhämtning av platsuppgifter tillåts verkställas mot informationssystem utan koppling till en person som uppfyller misstankekravet är ett stort teoretiskt undantag från integritetsskyddet och sedvanliga regler för användning av hemliga tvångsmedel. Kravet på att informationssystemet ska ha använts vid brottet eller i anslutning till brottsplatsen vid brottstillfället eller annars är av ”synnerlig vikt för utredningen”, såsom på väg bort ifrån brottsplatsen längs en flyktväg exempelvis, kan dock enkelt anses som mycket användbara det praktiska utredningsarbetet. Den måste dock i teoretiskt hänseende anses som kontroversiell. Bestämmelsen kan öppna för en mycket extensiv tillämpning i framtiden och ett krav på ”synnerlig vikt” tjänar som en svag tröst i sammanhanget då kravet uppställs även för äldre tvångsmedel, vilka getts en mycket extensiv tillämpning.

Även de bestämmelser om användning av hemlig dataavläsning i underrättelseverksamhet som framgår i exempelvis 7 § medför en oerhört vidsträckt tillämpning. Ett tillstånd till hemlig dataavläsning kan ges för övervakning av en oidentifierad person eller en person som ingår i en grupp eller främjar en grups handlande och det finns påtaglig risk att allvarlig brottslighet kommer att förekomma inom gruppen. För användning av dessa slag framgår en till synes tillfredställande tillämpning i förarbeten, såsom att riskbedömningen för personen i gruppen kan utgå ifrån till exempel personens ställning i gruppen eller om personen tidigare är dömd för liknande brottslighet och ett medlemskap i en sådan grupp som avses är inte tillräckligt. Det innebär att en gruppering sedan tidigare måste vara ordentligt kartlagd

och personen som ska övervakas måste ha en uppsatt ställning och historia av liknande brottslighet, vilket enligt min uppfattning inte kan jämföras med övervakning av grupperingar av oskyldigt slag som teoretiskt skulle kunna bli föremål för övervakning av staten. Denna typen av tvångsmedelsanvändning i preventivt syfte var sedan tidigare tillåten genom preventivlagen som beskrivits ovan.

Hemlig dataavläsning i syfte att upptäcka brottslig verksamhet får endast användas för att inhämta kommunikationsövervaknings- eller platsuppgifter enligt 10 §. Denna användning motsvarar i stort sett tidigare lagstiftning i den så kallade inhämtningslagen. För hemlig avläsning krävs dock att åtgärden är av synnerlig vikt, istället för särskild vikt för utredningen. Detta ligger väl i linje med kraven på en med restriktiv reglering av en mer ingripande åtgärd.

Sammanfattningsvis kan sägas att lagstiftningen i stor utsträckning motsvarar den äldre lagstiftningen för tvångsmedel även för rättssäkerhetsgarantier som till exempel granskning, tillsyn och underrättelser. Detta medför att skyddet för den enskildes rättigheter inte ökat i takt med ökningen av intrångets storlek. Det kan även vara oroväckande då rättssäkerhetsgarantierna för tidigare hemliga tvångsmedel inte omöjliggjort ett mycket långtgående missbruk, det är därför befogat att ställa frågan om inte även hemlig tvångsmedel kan missbrukas och vilka följder det kan medföra.

5.4 Respekteras avvägningen mellan effektivitet och integritet vid införandet och tillståndsprövningen?

Vid införandet av lagen ska avvägningen mellan åtgärdens effektivitet och dess inskränkning i den enskildes rätt till att slippa bli övervakad göras. Avvägningen i en tillståndsprövning kretsar även här kring tvångsmedlets förmodade effektivitet – om åtgärden förväntas bli effektiv och det finns ett

behov kan det överväga intresset för den misstänktes integritet. Även kravet att åtgärden ska vara av ”synnerlig vikt för utredningen” ges en liknande innebörd i förarbeten, nämligen att det krävs att de upplysningar som kan inhämtas ska vara av viss kvalitet och att det ska gå att räkna med att åtgärden verkligen kan få effekt.

Ett behov förutsätter också, enligt min uppfattning, en förmodad effektivitet i åtgärden. Det kan i sammanhanget aldrig finnas ett behov av en förmodat ineffektiv åtgärd, då en ineffektiv åtgärd per definition inte leder till det önskade resultat som föranleder behovet av åtgärden. Om åtgärder av detta slag i hög grad tillåts men sedan visar sig vara ineffektiva bör det alltså ses som en misslyckad avvägning, då ett stort integritetsintrång tillåtits till ingen, eller liten, nytta. Det vore dessutom en lagstridig tillämpning enligt såväl nationell som internationell rätt, exempelvis enligt proportionalitets- och behovsprincipen.

Begreppet effektivitet ska i tvångsmedelssammanhang i första hand förstås som möjligheten att klara upp och lagföra brott, men kan även syfta på resursfrågor. Det vore enligt min uppfattning ologisk om det skulle vara resursfrågan som bör vägas mot den inskränkning i den enskildes integritet som åtgärden innebär. Det intresset som vägs mot integritetsinskränkningen torde alltså vara intresset av att ge de brottsbekämpande myndigheterna tillräckligt stora möjligheter att klara upp och lagföra brott. Med effektiv brottsbekämpning avses i sammanhanget alltså en brottsbekämpning som i hög grad klarar upp och lagför brott.

Beträffande den kvalitativa utvärderingen av åtgärdens förmodade effektivitet kan sägas följande. Utredningen SOU 2017: 89 avvisade som ovan beskrivits, kritik om att tekniska svårigheter skulle påverka effektiviteten av hemlig dataavläsning på följande sätt. Eftersom det tekniska svårigheterna kommer att betraktas av myndigheterna innan verkställigheten,

kommer effektiviteten av verkställigheten bli hög.²⁵⁶ Slutsatsen kan tolkas som att en åtgärd som enligt den verkställande myndighetens bedömning skulle kunna bli ineffektiv på grund av tekniska hinder inte kommer att verkställas, därmed kommer de åtgärder som verkställs bli effektiva eftersom de ineffektiva inte verkställs. Denna argumentation ter sig som ologisk. Om den argumentationen skulle appliceras på rättssäkerhetsgarantierna i lagstiftningen skulle till exempel ett utelämnande av efterhandsgranskning kunna motiveras med att en efterhandsgranskning av ett tillstånd inte behövs, eftersom myndigheterna gör en bedömning av lagligheten i den enskilda åtgärden innan den verkställs. Således kommer inga lagstridiga åtgärder verkställas av myndigheterna. Det framstår i teorin som ett cirkelargument där myndigheternas åtgärder alltid kommer vara effektiva eftersom myndigheterna bedömer att alla åtgärder som verkställs är effektiva.

Det andra argumentet för att hemlig dataavläsning kan förmodas bli en effektiv åtgärd i kvalitativ mening var följande. Eftersom tidigare undersökningar visar att tidigare åtgärder motsvarat de förhoppningar som de brottsbekämpande myndigheterna i förväg föreställt sig i fråga om vilken information åtgärderna skulle ge, var de bevisligen effektiva i kvalitativ mening. Då inget talade emot att hemlig dataavläsning i kvalitativ mening skulle bli mindre effektiv än de tidigare hemliga tvångsmedel som undersökningarna avsåg, ansågs hemlig dataavläsning kunna förmodas vara minst lika effektiv.²⁵⁷

Till att börja kan sägas att hemlig dataavläsning, om den kan verkställas i den form som beskrivs i förarbeten, troligtvis kommer att vara mer effektiv än tidigare tvångsmedel i kvalitativ mening. Om polisen kan hacka en telefon i realtid ger en sådan åtgärd givetvis i de flesta fall mer användbar information än en avlyssning av ett telefonsamtal på samma telefon. Utredningens slutsats att en åtgärd som motsvarar myndigheternas förväntningar är lika med en

²⁵⁶ Se avsnitt 4.2.3.2.

²⁵⁷ Ibid.

effektiv metod ter sig dock som en märklig slutsats. Om en myndighet inte förväntar sig att en åtgärd ska ge särskilt mycket information, och åtgärden inte heller ger särskilt mycket, betyder det inte att åtgärden i kvalitativt hänseende är effektiv, endast att den inte gav mer än vad som förväntades.

Jag ställer mig frågan om en lagstiftning på detta sätt kan utvärderas genom en uppskattning av kvalitativ effektivitet. Det spelar givetvis en roll i uppskattningen om den kommer att kunna bli effektiv men det ter sig som en märklig metod för att lösa integritetsavvägningen. Jag menar att exempelvis polisens möjligheter till husrannsakan knappast kan anses präglas av en övergripande effektivitet i den mening att brottslighet beivras, mot bakgrund av att en husrannsakan alltid ger tillgång till all information i den misstänktes bostad. En husrannsakan är i kvalitativ mening nära 100 % effektiv, den ger oftast svar på exakt vad som finns i bostaden. Men när bestämmelserna kring husrannsakan ska utvärderas genom att ställa dess effektivitet mot det integritetsintrång åtgärden medför för en misstänkt, är det knappast den kvalitativa effektiviteten av den specifika åtgärden som ska avses. Det är snarare den kvantitativa effektiviteten, som baseras på frågan om hur ofta en så integritetsingripande åtgärd medför att utredningen slutar med att en misstänkt lagförs eller avskrivs från utredningen, alternativt att brottet klaras upp, som måste vägas mot integritetsaspekten av att polisen har möjlighet att söka igenom misstänkta personers bostäder.

När man ser regeringens redovisning av nyttan i ljuset av denna definition av effektivitet framstår några kategorier av nytta som mer lämpliga än andra att väga in i en bedömning över en åtgärds effektivitet. Dessa är enligt min uppfattning i hur många procent åtgärden har lett till att den misstänkte kunnat avföras från utredningen eller åtalas och i hur många procent av fallen uppgifter från åtgärden har åberopats som bevisning eller använts för att utreda brott i annan förundersökning. Dessa nyttor visar resultatet av utredningen i vilken ett hemligt tvångsmedel har använts. Nyttor som exempelvis att uppgifter utgjort underlag i förhör, medfört att effektiv spaning har kunnat genomföras, bidragit till att annat tvångsmedel kunnat användas,

bidragit till utredning av brottsutbyte och lett till stärkta misstankar, säger inget om själva resultatet av utredningen, det vill säga den faktiska brottsbekämpningen. De nyttorna säger egentligen mer om den kvalitativa nyttan i en enskild åtgärd, i den mån det kan fastställas med tanke på redovisningens oprecisa sammanställning. Som ovan anført har nämligen inte åtgärdernas nytta i vissa fall kunnat skiljas åt i fall där flera åtgärder verkställts mot samma person eller i samma utredning.

Det kan här upprepas att en åtgärd vars huvudsakliga syfte är att enbart underlätta polisens arbete ska anses bryta mot behovsprincipen. Det kan därmed ifrågasättas i vilken utsträckning nyttokategorier som exempelvis att uppgifterna har ”utgjort underlag i förhörssituation” eller ”medfört att effektiv spaning har kunnat genomföras” verkligen är relevanta för att analysera effektiviteten i en åtgärd. Dessa är inte kopplade till behovet av åtgärden enligt principen. Samma sak kan sägas om ändamålsprincipen i förhållande till exempelvis kategorin ”har använts för att utreda brott i en annan förundersökning”. Principen anger som ovan anført att en åtgärd som inte används för det specifikt angivna ändamålet inte ska tillåtas, oavsett behov och proportionalitet. Den nämnda nyttokategorin innebär att den redovisade nyttan i åtgärden skett i en annan förundersökning, vilket oftast per definition måste innebära att den aktuella nyttan inte kan kopplas till ändamålet med åtgärden. Även denna kategori bör därmed vara ointressant för effektiviteten eftersom att varken den eller ovan nämnda nyttor har betydelse för åtgärdens tillåtlighet, även om de likväl är nyttor som följer av tvångsmedelsanvändningen.

Hemlig rumsavlyssning tilläts i 130 fall under 2018. 100 % av de brottsbekämpande myndigheternas ansökningar om tillstånd beviljades. Dessa tillstånd gav i 7 % av fallen uppgifter som kunde åberopas som bevisning i en stämningsansökan, i 10 % av fallen uppgifter som bidrog till att den misstänkte kunde åtalas, i 3 % av fallen uppgifter som bidrog till att den misstänkte kunde avföras från utredningen och i 3 % av fallen uppgifter som kunde användas till att utreda brott i en annan förundersökning. Detta är

inte en redovisning över uppgifter som varit avgörande för nyttan, endast uppgifter som på något sätt bidragit till nyttan. De får alltså utgöra den mätbara enheten för de kvantitativa analys som följer. Märk väl att en enskild åtgärd kan protokollföras i alla fyra av dessa kategorier samtidigt, vilket kan tyda på att procentsatserna skulle kunna vara för höga.

Domstolarna i Sverige tillät en åtgärd, som innebär ett stort intrång i den enskildes integritet och som ska förmodas kunna bli effektiv för att tillåtas, i 100 % av fallen, vilket i sig är en oroväckande siffra. Dessa tillstånd ledde till uppgifter som åberopades som bevisning i en rättegång i 7 % av fallen, vilket innebär att drygt 9 tillstånd ledde till uppgifter till bevisning, utav 130 beviljade tillstånd. Utan någon djupare inblick i det praktiska polisiära arbetet måste ändå denna siffra anses anmärkningsvärd. Samma typ av tillstånd ökade mellan 2014 och 2018 med 87 %, från 16 beviljade tillstånd till 130. Polisens problembeskrivning utgörs av faktumet att kryptering ökar och kriminellas beteende anpassas, vilket gör polisens övervakning allt mer verkanslös, det vill säga ineffektiv. Domstolens tillståndsprövning bör därför, enligt fastslagna principer om exempelvis förmodad effektivitet, bli allt mer restriktiv eftersom att åtgärderna enligt polisens egna utsago blir allt mer ineffektiva. Ändå ökar tillstånden drastiskt. En sådan utveckling framstår minst sagt som motsägelsefull och tyder inte på att avvägningen på ett godtagbart sätt respekteras, varken i lagens införande eller tillämpning.

För hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning gav åtgärderna uppgifter som i 33 respektive 41 % av fallen åberopades som bevisning. Det framstår som en något mer balanserad nivå. Ansökningar om tillstånd till dessa åtgärder beviljades i 99,4 respektive 99,3 % av fallen och antalet tillstånd ökade under samma period med 23 respektive 54 %. Detta skulle kunna vara tecken på en liknande utveckling även för dessa.

6 Slutsats

Hemlig dataavläsning uppfyller på ett övergripande plan de i gällande rätt uppställda kraven beträffande en tvångsmedelslagstiftnings utformning. Paragrafernas komplexa utformning och ständiga korshänvisningar till andra författningar bör dock noteras som befogad kritik mot lagen.

Lagstiftningen motsvarar i stor utsträckning de tidigare tvångsmedlens författningar i fråga om till exempel misstankekrav och rättssäkerhetsgarantier. Huruvida en rättssäker tillämpning upprätthålls blir dock ytterst en tillämpningsfråga. Det är därför oroande att se granskningar som visar att tidigare tvångsmedel i praktiken missköts samtidigt som statistik visar att användningen ökar drastiskt, trots minskande effektivitet. Det är helt enkelt motsägelsefullt.

Uppsatsen visar tydligt hur lagstiftningen inte omöjliggör missbruk och att brottsutredande myndigheter i praktiken ges mycket stora möjligheter att övervaka människor som i vissa fall inte ens är misstänkta för brott.

Mot bakgrund av det ovan anförda, leds jag till slutsatsen att tydligt mer inskränkande åtgärder, såsom hemlig dataavläsning, inte bör tillåtas utan en djupare konsekvensanalys över effektivitet och potentiellt missbruk, med strängare rättssäkerhetsgarantier som följd. Lagen borde således enligt min uppfattning aldrig ha införts.

Bilaga A – redovisning av nytta

Bilagan innehåller data som framgår av regeringens skrivelse (Skr. 2019/20:56) om redovisning av användningen av hemliga tvångsmedel under 2018. Syftet med bilagan är att återge relevanta delar av den data som återges i skrivelsen och summera den för att ge läsaren en övergripande bild över dels förhållandet mellan antal ansökningar och beviljade tillstånd, dels de procentandelar som regeringen rapporterat över nyttan av åtgärderna.

Redovisning av användningen av hemliga tvångsmedel (Skr. 2019/20:56) - Nyttan av åtgärden i procent och antalet beviljade/avslagna tillstånd under 2018

	Hemlig avlyssning av elektronisk kommunikation	Hemlig övervakning av elektronisk kommunikation	Hemlig kameraövervakning	Hemlig rumsavlyssning	Summa
Procent av ansökningar beviljade	4648 av 4673 = 99,4% (27 avslogs)	9151 av 9233 = 99,1 % (82 avslogs)	152 av 153 = 99,3 % (1 avslogs)	130 av 130 = 100 % (0 avslag 2017-)	14081 av 14191 = 99,2 % (110 avslag)
Interimistiska åklagarbeslut som godkändes av domstol	176 av 177 = 99,4% (1 upphävdes)	102 av 105 = 97,1 % (3 upphävdes)	17 av 17 = 100 % (0 avslogs)		295 av 299 = 98,6 % (4 avslag)
NYTTA AV ÅTGÄRDEN					
Under förundersökning					
Uppgifterna har utgjort underlag i förhörsituation	774 st = 47 %	Ej redovisat	87 st = 51 %	16 st = 24 %	40,60%
Uppgifterna har medfört att effektiv spaning har kunnat genomföras	1005 st = 61 %	Ej redovisat	103 st = 61 %	26 st = 39 %	53,60%
Uppgifterna har bidragit till att annat tvångsmedel använts mot den misstänkte	564 st = 34 %	Ej redovisat	70 st = 41 %	11 st = 16 %	30,30%
Uppgifterna har bidragit till utredning av brottsutbyte	160 st = 10 %	Ej redovisat	13 st = 8 %	1 = 1 %	6,30%
Uppgifterna har lett till stärkta misstankar mot den misstänkte	760 st = 46 %	Ej redovisat	84 st = 50 %	22 = 33 %	43%
Efter förundersökning					
Uppgifterna har bidragit till att den misstänkte kunnat avföras från utredningen	309 st = 19 %	Ej redovisat	10 st = 6 %	2 st = 3 %	9,30%
Uppgifterna har bidragit till att den misstänkte kunnat åtalas	569 st = 34 %	Ej redovisat	67 st = 40 %	7 st = 10 %	28%
Uppgifterna har åberopats som bevisning i stämningsansökan	540 st = 33 %	Ej redovisat	69 st = 41 %	5 st = 7 %	27%
Överskottsinformation					
Uppgifterna har bidragit till att något tvångsmedel använts mot en annan person i samma förundersökning	314 st = 19 %	Ej redovisat	32 st = 19 %	0 st = 0 %	12,60%
Uppgifterna har använts för att utreda brott i en annan förundersökning	91 st = 6 %	Ej redovisat	6 st = 4 %	2 st = 3 %	4,30%
Övrigt					
Uppgifterna har på annat sätt bidragit till att utredningen kunnat föras framåt	687 st = 42 %	Ej redovisat	73 st = 43 %	22 st = 33 %	39,30%

Källa: Skr. 2019/20:56 s. 13-26.

Bilaga B – Antal tillstånd

Bilagan innehåller data över antal tillstånd som meddelats av domstolar under en femårsperiod. Den data som redovisas i bilagan kommer från regeringens skrivelser om redovisning av användningen av hemliga tvångsmedel och är den nyaste data som redovisats. (Se Skr. 2015/16:49, skr. 2016/17:69, skr. 2018/19:19, skr. 2019/20:56.)

Tvångsmedelsanvändning 2015-2018 antal meddelade tillstånd						
	2014	2015	2016	2017	2018	Ökning i procent
Hemlig avlyssning av elektronisk kommunikation	3564	3465	3456	4465	4648	23%
Hemlig övervakning av elektronisk kommunikation	4398	5959	6800	7991	9151	51%
Hemlig kameraövervakning	69	114	143	153	152	54%
Hemlig rumsavlyssning	16	44	54	77	130	87%
Totalt	8047	9582	10453	12686	14081	Total faktisk ökning: 42 %
						Genomsnittlig ökning: 53%

Käll- och litteraturförteckning

Tryckta källor

Utredningsbetänkanden

SOU 1984:54 Tvångsmedel – anonymitet – integritet.

Ds 2005:21 Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet.

SOU 2005:38 Tillgång till elektronisk kommunikation i brottsutredningar m.m.

SOU 2009:1 En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen.

SOU 2011:45 Förundersökning – objektivitet, beslag, dokumentation m.m.

SOU 2012:44 Hemliga tvångsmedel mot allvarliga brott.

SOU 2017:75 Datalagring – brottsbekämpning och integritet.

SOU 2017:89 Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet.

SOU 2018:61 Rättssäkerhetsgarantier och hemliga tvångsmedel.

Propositioner och regeringskrivelser

Prop. 1994/95:227 Hemlig teleavlyssning och hemlig teleövervakning.

Prop. 1995/96:85 Hemlig kameraövervakning.

Prop. 2002/03:38 Straffansvar för terroristbrott.

Prop. 2002/03:74 Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering.

Prop. 2005/06:178 Hemlig rumsavlyssning.

Prop. 2011/12:55 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Prop. 2013/14:237 Hemliga tvångsmedel mot allvarliga brott.

Skr. 2015/16:49 Redovisning av användningen av hemliga tvångsmedel under 2014.

Skr. 2016/17:69 Redovisning av användningen av hemliga tvångsmedel under 2015.

Skr. 2018/19:19 Redovisning av användningen av hemliga tvångsmedel under 2017.

Skr. 2019/20:56 Redovisning av användningen av hemliga tvångsmedel under 2018.

Prop. 2019/20:64 Hemlig dataavläsning.

Prop. 2019/20:145 Ett förenklat förfarande vid vissa beslut om hemlig dataavläsning.

Övrigt riksdagstryck

Riksdagens protokoll 2019/20:77 Onsdagen den 19 februari 2020.

Litteratur

Andersson, Simon, *Skälig misstanke*, 1. uppl., Wolters Kluwer, Diss. Stockholm : Stockholms universitet, Stockholm, 2016.

Danelius, Hans, *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, 5., [uppdaterade] uppl., Norstedts juridik, Stockholm, 2015.

Ehrenkrona, Carl Henrik, *Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna: en kommentar*, Karnov Group, Stockholm, 2016.

Ekelöf, Per Olof, Bylund, Torleif & Edelstam, Henrik, *Rättegång H. 3, 7.*, [rev.] uppl., Norstedts juridik, Stockholm, 2006.

Ekelöf, Per Olof, Edelstam, Henrik & Pauli, Mikael, *Rättegång H. 5, 8.*, [rev. och utök.] uppl., Norstedt, Stockholm, 2011.

Korling, Fredric & Zamboni, Mauro (red.), *Juridisk metodlära*, 1. uppl., Studentlitteratur, Lund, 2013.

Landström, Lena: 'Brottsutredning och effektivitet: en analys av effektivitetsbegreppets användning vid lagstiftning', i: Örjan Edström, Johan Lindholm & Ruth Mannelqvist (red.), *Jubileumsskrift till Juridiska institutionen 40 år*. Umeå 2017 s. 193-206.

Lindberg, Gunnel, *Straffprocessuella tvångsmedel: när och hur får de användas?*, Fjärde upplagan, Karnov Group, Stockholm, 2018.

Strömberg, Håkan & Lundell, Bengt, Sveriges författning, 22., uppdaterade uppl., Studentlitteratur, Lund, 2016.

Trolle Önnerfors, Elsa & Wenander, Henrik, *Att skriva rätt: goda råd för att skriva uppsats i juridik*, 1. uppl., Wolters Kluwer, Stockholm, 2016.

Elektroniska källor

BRÅ 2016:17 IT-inslag i brottsligheten och rättsväsendets förmåga att hantera dem, <<https://www.bra.se/publikationer/arkiv/publikationer/2016-09-30-it-inslag-i-brottsligheten-och-rattsvasendets-formaga-att-hantera-dem.html>>, besökt 2020-04-30.

”Effektiv”, Svenska Akademiens ordbok, <<https://www.saob.se/artikel/?seek=effektiv&pz=2>>, besökt 2020-04-29.

”Effektiv”, Nationalencyklopedin, <<https://www-ne-se.ludwig.lub.lu.se/uppslagsverk/encyklopedi/l%C3%A5ng/effektiv>>, besökt 2020-04-29.

”Effektiv”, Nationalencyklopedin, Svenska synonymer, <<https://www-ne-se.ludwig.lub.lu.se/ordb%C3%B6cker/#/search/norstedts-synonym-sv-sv?q=effektiv>>, besökt 2020-04-29.

Internet Organised Crime Threat Assessment, Europol, EU, 2017, <<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>>, besökt 2020-04-30.

Rättsfallsförteckning

Rättsfall från Europadomstolen

Klass m.fl. mot Tyskland, nr. 5029/71, 6 september 1978.

Khan mot Förenade Kungariket, nr. 35394/97, 12 maj 2000.

P.G. och J.H. mot Förenade Kungariket, nr. 44787/98, 25 september 2001.

Association for European Integration and Human Rights och Ekimdzhiev mot Bulgarien, nr. 62540/00, 28 juni 2007.

Natunen mot Finland, nr. 21022/04, 31 mars 2009.

Janatuinen mot Finland, nr. 28552/05, 8 december 2009.

Kennedy mot Förenade kungariket, nr. 26839/05, 18 maj 2010.

Uzun mot Tyskland, nr. 35623/05, 2 september 2010.

Roman Zakharov mot Ryssland, nr. 47143/06, 4 december 2015.