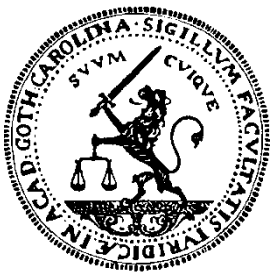

JURIDISKA FAKULTETEN
vid Lunds universitet

Charlotta Zander

Hemliga tvångsmedel i it-samhället

Hemlig avlyssning och övervakning av elektronisk kommunikation

LAGM01 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Sverker Jönsson

Termin för examen: HT 2015

Innehåll

Summary

The area of covert interception of electronic communication (telephone tapping) and covert surveillance of electronic communication (covert telephone surveillance or metering) is an area which at times causes much debate in the legal profession and among the general public as well. There are probably few legal acts of the European Union that have received as much attention in the media as the Data Retention Directive which was recently declared invalid by the European Court of Justice. The debate is justified as covert coercive measures are effective means to combat crimes while at the same time constitute an interference with the fundamental rights and freedoms which are guaranteed by the Swedish constitution, the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the Charter of Fundamental Rights of the European Union. Despite this, it is not entirely easy to get an overview of the meaning of the legislation and what is actually possible from a technological perspective. The area may appear difficult to grasp as the procedural criminal law not only exists in the Code of Judicial Procedure but also in separate special laws. To complicate matters further, the duties of actors in the electronic communication sector to cooperate with crime fighting authorities is regulated in the Electronic Communications Act (2003:389).

As a result of this the purpose of this essay is trying to understand the meaning of the legislation. The questions are therefore which actors have a duty to cooperate with the authorities for crime fighting purposes and how the legislator justified the legislation on covert coercive measures. Since covert coercive measures constitute an interference with fundamental rights and freedoms it is vital that the legislation is perceived as legitimate. To be able to discuss the legitimacy of the legislation it is of great value to understand in which extent the secret coercive measures are used in practice and if the legislation is utilized for those crimes which justified its creation. It is also necessary to understand what the implications of the regulations in the Code of Judicial Procedure and in Electronic Communications Act (2003:389) are. To get an accurate image of which information that may be obtained it is finally of value to understand which information that does not fall within these regulations. All of these parts are needed to understand the complete picture, hold a discussion and get closer to be able to answer the questions.

Sammanfattning

Området för hemlig avlyssning av elektronisk kommunikation (hemlig teleavlyssning) och hemlig övervakning av elektronisk kommunikation (hemlig teleövervakning) är ett område som tidvis vållar stor debatt bland jurister och även bland allmänheten. få EU-rättsliga akter har nog varit så medialt uppmärksammade som datalagringsdirektivet som nyligen ogiltigförklarades av Europeiska unionens domstol. Debatten är motiverade eftersom hemliga tvångsmedel är effektiva för att bekämpa brott samtidigt som de utgör ett intrång i de grundläggande fri- och rättigheter som garanteras av bl.a. svensk grundlag, den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) och Europeiska unionens stadga om de grundläggande rättigheterna. Trots detta är det inte helt lätt att få en överblick över vad lagstiftningen innebär och vad som egentligen är möjligt ur ett teknologiskt perspektiv. Området kan upplevas svåröverskådligt på grund av att den straffprocessuella regleringen inte enbart finns i rättegångsbalken utan även i olika speciallagar. För att ytterligare komplicera saken så regleras vilka skyldigheter aktörer i sektorn för elektronisk kommunikation har att samarbeta med brottsbekämpandemyndigheter i lagen (2003:389) om elektronisk kommunikation (LEK).

Som ett resultat av detta är syftet med denna uppsats att försöka förstå vad lagstiftningen egentligen innebär. Frågeställningarna är därför vilka verksamheter som har en skyldighet att samarbeta med myndigheterna för brottsbekämpande ändamål och hur lagstiftaren motiverat lagstiftning om hemliga tvångsmedel. Eftersom hemliga tvångsmedel utgör ett intrång i de grundläggande fri- och rättigheterna är det viktigt att lagstiftningen upplevs som legitim. För att det ska vara möjligt att diskutera lagstiftningens legitimitet är det av stor vikt att förstå i vilken omfattning de hemliga tvångsmedlen används i praktiken och om lagstiftningen används mot de brott som motiverad dess tillkomst. Det är även nödvändigt att förstå vad regleringen i rättegångsbalken och LEK egentligen innebär. För att få en rättvisande bild av vilken information som kan inhämtas är det slutligen av vikt att förstå vilka uppgifter som inte omfattas av denna reglering. Alla dessa delar behövs för att förstå helheten, kunna föra en diskussion och komma närmare ett svar på frågeställningarna.

Förord

Arbetstiteln på detta arbete har varit ”hotet från androiderna”. Att vår nyttiga elektronik även kan innebära en risk för integritetsintrång är ett faktum som blivit mer uppmärksammat under de senare åren och var och varannan dag kommer nya nyhetsartiklar som larmar om hur mycket information som egentligen sparas om oss. Under arbetets gång har jag därför gradvis insett att jag borde ha varit tekniker för att till fullo kunna förstå och redogöra för regleringen på området. Ett antal personer har bidragit till att detta arbete trots det blivit klart. Jag vill här särskilt tacka min handledare Sverker Jönsson för goda råd, inspiration och konstruktiv handledning.

Jag vill även tacka min familj för allt stöd och uppmuntran utan vilket denna uppsats inte blivit vad den blivit. Särskilt vill jag tacka Lena, för uppmuntran och hjälp med korrekturläsning, samt Erik och Olof för hjälp att förstå den teknologiska grunden till lagstiftningen. Slutligen vill jag tacka Mikael för det ständiga stödet och för att du påminner mig om vad som egentligen är viktigt här i livet.

Förkortningar

2007 års preventivlag	Lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott
2008 års utredningslag	Lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott
2012 års inhämtningslag	Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet
AK-nät	Allmänt kommunikationsnät
ATEK-tjänst	Allmänt tillgänglig elektronisk kommunikationstjänst
DI	Datainspektionen
EKMR	Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna
EU	Europeiska unionen
FEK	Förordningen (2003:396) om elektronisk kommunikation
HAEK	Hemlig avlyssning av elektronisk kommunikation
HÖEK	Hemlig övervakning av elektronisk kommunikation
LEK	Lagen (2003:389) om elektronisk kommunikation
PuL	Personuppgiftslagen (1998:204)
PTS	Post- och telestyrelsen
RB	Rättegångsbalken
RF	Regeringsformen

1 Inledning

1.1 Syfte

Syftet med denna uppsats är att utreda gällande rätt inom området övervakning och avlyssning av elektronisk kommunikation, regleringens förhållande till grundläggande fri- och rättigheter samt att undersöka skälen och argumenten för regleringen. Beskrivningen av gällande rätt innefattar bl.a. en beskrivning av vilken typ av information som kan inhämtas, men eftersom viss oklarhet råder om vilken typ av kommunikation som kan avlyssnas eller övervakas så är det nödvändigt att även redogöra för vilken typ av kommunikation som inte omfattas av detta regelsystem, utan där andra regler istället är aktuella. Eftersom Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) utgör en del av svensk rätt är det naturligt att både konventionen och RF beaktas när gällande rätt och regleringens förhållande till grundläggande fri- och rättigheter utreds. För att på ett kritiskt sätt kunna undersöka regleringen är det nödvändigt att jämföra motiveringarna som återfinns i förarbetena med hur tvångsmedlen faktiskt används och även att beakta praktikers och akademikers perspektiv. Av samma skäl är det av intresse att jämföra regleringen i dagsläget med regleringen innan användningen av elektronisk kommunikation kraftig ökade, samt om möjlig redogöra för utvecklingstendenser.

1.2 Frågeställningar och avgränsningar

Inom detta område finns otaliga frågor av intresse, men i detta arbete ska endast två frågor behandlas, nämligen:

- Hur ökade befogenheter för polis[1] och åklagare gällande hemliga tvångsmedel har motiverats, samt;
- Vilka verksamheter som omfattas av skyldigheten att samarbeta med bl.a. polisen för brottsbekämpande ändamål enligt lagen (2003:389) om elektronisk kommunikation (LEK).

[1] Sedan 1 januari 2015 är "polisen" benämningen på samhällsfunktionen medan benämningen på de ansvariga myndigheterna är "Polismyndigheten" och "Säkerhetspolisen". Detta skrivsätts kommer att användas även för tiden innan omorganisationen. Se SOU 2012:13 s. 24, 263-264.

Denna uppsats kommer framförallt behandla Polismyndighetens möjlighet att inhämta information om elektronisk kommunikation. Säkerhetspolisens möjligheter att inhämta uppgifter kommer till viss del att behandlas, däremot kommer inte Försvarets radioanstalts möjligheter att signalspana att beröras i denna uppsats. Hur inhämtad information sedan används kommer inte vara fokus i denna uppsats, och frågan om hantering av s.k. överskottsinformation kommer därför att förbigås. Operatörernas perspektiv i datalagringsfrågan kommer inte att redogöras för, utan utgångspunkten kommer vara den enskildes perspektiv. Inte heller kommer det att utredas hur andra länder ser på datalagringsdirektivet, dvs. skälen till att bl.a. Storbritannien ogiltigförklarat sin datalagringslagstiftning, utan endast konstateras att så är fallet.

Problematiken kring polisens användning av tekniska hjälpmedel, såsom IMSI-fångare, s.k. ”falska basstationer”, för att inhämta telefonnummer till misstänka individers telefoner, är mycket intressant men är tyvärr inte möjligt att undersöka inom ramen för detta arbete. Ifråga om vilken information brottsbekämpande myndigheter kan utfå från sociala medier och vilket lands lagstiftning som är tillämplig så kommer detta område endast behandlas mycket översiktligt. Systemet för ömsesidig rättslig hjälp i brottmål och vilken inverkan det har för brottsbekämpande myndigheters arbete och den enskildes integritet kommer i stort sett att förbigås i denna uppsats. Likaså kommer möjligheten enligt lagen (1991:572) om särskild utlänningskontroll att använda hemliga tvångsmedel att förbigås i denna uppsats.

1.3 Metod och material

För att fastställa gällande rätt kommer rättsdogmatisk metod användas. Det innebär att rättskällorna undersöks, vilket på detta område lag, förarbeten, rättspraxis och doktrin. Fokus i denna uppsats kommer att vara lag och förarbeten och materialet kommer därför till stor del bestå av lagtext och lagförarbeten. Ett fåtal principiellt viktiga rättsfall kommer att behandlas, framförallt rättsfall från Europadomstolen gällande brott mot den europeiska konventionen om skydd för de mänskliga rättigheterna. Ett urval av myndigheters och särskilda arbetsgruppers rapporter och utredningar kommer även att användas. Doktrin kommer framförallt att användas för att visa på debatten bland juristerna, men även i viss mån för att utröna rättsläget.

1.4 Perspektiv

Perspektivet som kommer att användas i denna uppsats är Jareborgs klassiska modell för en defensiv straffrättspolitik respektive en offensivt inriktad straffrättspolitik. Enligt Jareborg utgör den defensiva modellen ett ideal som konstruerades för att illustrera de grundläggande värderingarna i en rättsstat.[2] Jareborg menar att det inte finns någon renodlat offensiv modell av straffrättspolitiken som konkurrerar med den defensiva modellen eftersom det i stort sett funnits en önskan om att bevara de rättsstatliga principerna, men att det däremot finns en offensiv inriktning av straffrättspolitiken som i viss mån håller på att underminera den defensiva straffrättspolitikens dominans.[3]

1.4.1 Defensiv straffrättspolitik

Den defensiva modellen för straffrättspolitik kan sägas ha två viktiga utgångspunkter. Den första utgångspunkten är att staten inte nödvändigtvis alltid är god, och den andra utgångspunkten är att ett behov av brottsprevention aldrig får överordnas värden som rättssäkerhet och rättvisa. Enligt den defensiva modellen har straffrätten därför som syfte att inte endast skydda staten och enskilda från kränkningar från andra enskilda, utan även att skydda enskilda från kränkningar från staten såsom maktmissbruk och överdriven repression.[4] Enligt den defensiva synen så kan straffrätten rättfärdigas just för att den utgör ett system för att hantera oönskade handlingar som samtidigt förhindrar maktmissbruk genom att den sätter gränser för myndigheter och politiker. Att bidra till att lösa problem i samhället är däremot inte ett av straffrättens primära syften enligt den defensiva modellen.[5]

En viktig aspekt av den defensiva straffrätten är att ett antal grundläggande principer ska följas när gärningar kriminaliseras. Som exempel på dessa principer kan nämnas principen att oönskade gärningar endast ska kriminaliseras i sista hand (ultima ratio), och synen att det inte är gärningsmän som primärt är i fokus utan det är brott, vilka består i enstaka onda handlingar eller underlåtelser, som är straffrättens fokus. Förutom att den defensiva modellen uppställer principer för kriminalisering så uppställer den

[2] Jareborg (1994) s. 43.
[3] Jareborg (1994) s. 46.
[4] Jareborg (1994) s. 44.
[5] Jareborg (1994) s. 46.

defensiva modellen även krav på existens av vissa processuella rättssäkerhetsgarantier. De rättssäkerhetsgarantier som Jareborg uppställer är (1) att domstolarna är oavhängiga och (2) att den enskilde har tillgång till ett oberoende juridiskt biträde för att föra sin talan. I domstolen krävs det (3) att det tillämpas höga beviskrav och (4) att bevisbördan ligger på åklagaren. Vidare ska det inte vara tillåtet att till den tilltalades nackdel tillämpa lagstiftning (5) analogiskt eller (6) retroaktivt. Det ska (7) vara möjligt för en tilltalad att överklaga en dom, både i skuldfrågan och i fråga om påföljdsbestämningen. Slutligen menar Jareborg att det (8) ska finnas möjlighet att få ett beslut om tvångsmedel prövat av domstol.[6]

1.4.2 Offensiv inriktning av straffrättspolitiken

Den modell som står emot den defensiva modellen benämns av Jareborg som den offensiva inriktningen av straffrättspolitiken. Denna inriktning hyser inte samma skepsis till staten som den defensiva modellen. Istället för att se staten som en möjlig motståndare som den defensiva modellen gör, så ser den offensiva inriktningen staten som en allierad. Straffrättssystemet anses kunna hjälpa till att lösa samhällsproblem och sociala problem, och brottsprevention ses som det viktiga. Det väsentliga problemet i straffrättssystemet upplevs därför vara systemets bristande effektivitet och inte dess eventuella bristande rättssäkerhet eller orättvisa.[7] För att straffrätten ska kunna fylla denna funktion och nå verkliga resultat krävs en viss flexibilitet, t.ex. genom att principer omtolkas och skyddsmekanismer försvagas. Fokus är därmed inte i samma utsträckning på principer och rättssäkerhetsgarantier som i den defensiva modellen, utan snarare på att hitta effektiva metoder och att uppnå resultat.[8] Enligt Jareborg kännetecknas den offensiva inriktningen även av användningen av ett antal metoder. Den viktigaste metoden att nämna för denna uppsats är ”rationaliseringen” av brottmålsprocessen, vilket innebär en strävan att minska kostnaden för att processa varje fall, en ökad repressionsnivå samt att somliga människor som har begått brott behandlas och betraktas som fiender istället för medmänniskor.[9]

[6] Jareborg (1994) s. 44–45.
[7] Jareborg (1994) s. 46–47.
[8] Jareborg (1994) s. 48.
[9] Jareborg (1994) s. 48, Jareborg (1995) s. 29.

Den offensiva inriktningen kännetecknas även av dess konsekvenser, vilka Jareborg menar är bl.a. att förutsägbarheten i systemet minskar, att de processuella rättssäkerhetsgarantierna försvagas och att synen i allt större grad blir att brottsbekämpning är en ”kamp mot brottsligheten” och mot de individer som begått brott. Effektivitetssträvan leder till att polis i större utsträckning blir behörig att fatta beslut som tidigare endast fattats av åklagare, och att åklagare blir behörig att fatta beslut som tidigare tagits av domstol. Samtidigt blir det på alla nivåer, men främst på åklagarnivå, ett större utrymme för skönsmässigt beslutsfattande. Vidare innebär en offensiv inriktning enligt Jareborg överkriminaliseringar och ökade kriminalisering av osjälvständiga brottsformer och oaktsamhetsbrott, vilket leder till att rättsväsendet överbelastas och att det blir svårare att upptäcka om brott förövats.[10]

Detta leder, enligt Jareborg, lätt till en ond cirkel av prestationsunderskott och utökade repression, eftersom det finns en övertro till att kriminalisering, uppkriminalisering och strängare påföljder på allvar kan påverka kriminalitetsnivå i samhället samt ett synsätt att straffrätten är legitim endast om den är effektiv i sin brottsprevention. Någon egentlig förändring av kriminalitetsnivån i samhället är dock något som straffrätten inte förmår åstadkomma, enligt Jareborg. Denna diskrepans leder till ett prestationsunderskott, vilket förespråkarna för den offensiva inriktningen menar beror på att inte tillräckligt repressiva åtgärder vidtagits och att mer av samma typ av repressiva åtgärder därför ska vidtas. Enligt Jareborg kan dock denna onda cirkel slutligen leda till att kriminalitetsnivån påverkas, men detta sker på bekostnad av att systemet blivit ett system präglat av statsterrorism.[11]

En ytterligare konsekvens av övertron till kriminalisering är att lagstiftningen i större utsträckning blir symbolisk. Symbolisk innebär i denna betydelse att lagstiftningens uttalade syfte skiljer sig från lagstiftningens egentliga och outtalade syfte, som ofta är att lugna en oroad allmänhet.[12] Jareborg menar att det inte går att försvara att samhället med dessa kostsamma och overksamma metoder försöker uppnå samhällsmål, och menar att straffrätten inte kan ha någon annan rationell funktion än att ge uttryck för en samhällsmoral och om möjligt stärka en sådan. Kostnaden för effektiv brottsprevention

[10] Jareborg (1994) s. 48–49.
[11] Jareborg (1994) s. 50–51.
[12] Jareborg (1994) s. 51.

är nämligen stor, menar Jareborg, både vad gäller den ekonomiska kostnaden och kostnaden av minskad personlig frihet för medborgarna, eftersom effektiv brottsprevention kräver att möjligheterna att begå brott minskas och att kontroller av integritetskränkande natur därför införs.[13]

1.5 Forskningsläget

Området för hemlig övervakning och avlyssning av elektronisk kommunikation är ett område som är ständigt i förändring. Tyvärr framgår det inte särskilt tydligt i förarbetena vad de hemliga tvångsmedlen innebär ur ett teknologiskt perspektiv. I doktrinen på detta område görs därför sällan en redogörelse av de tekniska aspekterna i någon större utsträckning. Legitimitetsfrågor och frågor av fri- och rättighetskaraktär hanteras desto oftare i doktrin. I en antologi av Agrell, Wilhelm (red.) "*Övervakning och integritet – en antologi*" utreds dock både fri-och rättighetsfrågor och i viss mån tekniska frågor.

1.6 Disposition

Efter detta inledande kapitel 1 kommer en översikt av regelkomplexet att göras i kapitel 2 och därefter kommer i kapitel 3 att redogöras för skyddet av de grundläggande fri- och rättigheterna i RF, EKMR och EU:s rättighetsstadga samt tillämpliga straffprocessuella grundprinciper. I kapitel 4 kommer en kort historisk tillbakablick göras innan argumenten som förekommer i debatten behandlas i kapitel 5. Därefter kommer i kapitel 6 redogöras för redovisningen av användningen av hemliga tvångsmedel. I kapitel 7 kommer det sedan att redogöras för lagstiftningen i RB och i kapitel 8 för regleringen i *lagen* (2003:389) *om elektronisk kommunikation* (LEK). Efter den redogörelsen kommer ett försök göras i kapitel 9 att klargöra hur regleringen i RB och LEK förhåller sig till andra tvångsmedel såsom beslag och husrannsakan, samt kommunikation genom tjänster som inte omfattas av LEK. Slutligen kommer en analys att genomföras och slutsatser redovisas i kapitel 10.

[13] Jareborg (1994) s. 52–53.

2 Översikt av regelkomplexet

Regleringen av detta område kan upplevas som något svåröverskådlig, och det kan därför vara lämpligt att ge en kortfattad överblick innan regleringen redovisas i detalj. En del verksamheter och elektroniska kommunikationsmedel faller inte inom det regelkomplex som kommer att beskrivas här nedan, och för att få ut dessa uppgifter gäller istället generella regler (se avsnitt 9.1).

2.1 Översikt av regleringen i RB m.m.

Bestämmelser om avlyssning och övervakning av elektronisk kommunikation återfinns i ett flertal lagar. De ”vanliga” reglerna om hemlig avlyssning av elektronisk kommunikation (HAEK) och hemlig övervakning av elektronisk kommunikation (HÖEK) återfinns i 27 kap. RB, och dessa bestämmelser förutsätter i huvudregel att en förundersökning har inletts för att vara tillämpliga (jfr 27:18 2 st., 27:19 3 st.).

Tillstånd utifrån 27 kap. RB kan dock även ges innan en förundersökning inletts enligt undantagsreglerna i *lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott* (2007 års preventivlag), om det finns en påtaglig risk för sådan särskilt allvarlig brottslighet som anges i 2007 års preventivlag. Uppgifter kan även inhämtas innan en förundersökning har inletts med stöd av *lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* (2012 års inhämtningslag). Vidare kan abonnemangsuppgifter inhämtas enligt 6:22 *lagen (2003:389) om elektronisk kommunikation* (LEK).

2.2 Översikt av lagen (2003:389) om elektronisk kommunikation

Vilka uppgifter som kan inhämtas är emellertid beroende av vilka uppgifter som har lagrats, och det är därför av stor betydelse att utröna vilka uppgifter som ska lagras samt vilka verksamheter som är skyldiga att lagra dessa uppgifter. Detta, samt definitioner av begrepp som används i 27 kap. RB, återfinns i LEK (jfr 27:25 2 st. RB) samt i förordningen (2003:396) om elektronisk kommunikation (FEK).

De bestämmelser i LEK som är relevanta för HAEK och HÖEK återfinns i 6 kap. LEK, bortsett från definitionerna i 1:7 och anmälningsplikten i 2:1. I 6:19 regleras den s.k. ”anpassningsskyldigheten”, dvs. vilka verksamheter som måste anpassa sina system för att kunna bistå myndigheter vid hemlig övervakning och avlyssning av elektronisk kommunikation. Den s.k. datalagringen regleras i 6:16a–16d och innebär en skyldighet för anmälningspliktiga verksamheter att lagra bl.a. trafikuppgifter för brottsbekämpande ändamål. Bestämmelserna utgör undantag till huvudregeln i 6:5 att trafikuppgifter ska utplånas, och har tillkommit som en följd av det nu upphävda datalagringsdirektivet. Det finns även, enligt 6:8 1 st. 2, möjlighet att inhämta andra trafikuppgifter än lagrade samt lokaliseringsuppgifter enligt 6:10a. I 6:20 regleras tystnadsplikten, bestämmelsen är relevant både för datalagringen och skyldigheten att lämna ut uppgift om abonnemang som återfinns i 6:22 1 st. 2. Uppgift om abonnemang ingår i de uppgifter som ska lagras och kan därför utfås genom 27 kap. RB, men kan även begäras ut i enlighet med 6:22 1 st. 2.

2.3 Översikt EU-direktiv

Framförallt tre direktiv är relevanta för integritetsfrågan inom sektorn för elektronisk kommunikation. Det äldsta av de tre direktiven är dataskyddsdirektivet[14], vilket anger huvudregler för behandlingen av personuppgifter och som har genomförts i svensk rätt genom personuppgiftslagen (1998:204). Det andra är direktivet om integritet och elektronisk kommunikation,[15] som anger specifika regler för behandling av personuppgifter inom sektorn elektronisk kommunikation, och som införts genom LEK. Det tredje direktivet är det numera ogiltigförklarade s.k. datalagringsdirektivet[16], som ändrar i direktivet om integritet och elektronisk kommunikation och som genomförts genom ändring av bl.a. LEK.

[14] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.
[15] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation. Ändrat genom Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 (datalagringsdirektivet) och Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009.
[16] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

3 Grundläggande fri- och rättigheter

3.1 Skyddet i regeringsformen

Rätten till förtroligt meddelande skyddas som bekant av en av våra svenska grundlagar, regeringsformen (RF). Rätten till förtroligt meddelande är en av de grundläggande rättigheterna i RF och innebär att var och en, mot det allmänna är skyddade mot bl.a. ”undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande” (2:6 RF).

I RF finns även ett målsättningsstadgande i 1:2 4 st. som bl.a. har innebörden att det allmänna ska värna den enskildes privatliv och familjeliv. Sedan grundlagsändringen år 2010 finns även ett uttryckligt skydd för den personliga integriteten i 2:6 2 st. Innebörden av skyddet i 2:6 2 st. är att var och en, förutom skyddet som följer av 2:6 1 st., även är skyddad mot betydande intrång i den personliga integriteten som innebär övervakning eller kartläggning av en enskilds personliga förhållande (2:6 2 st.). Stycket infördes för att erkänna rätten till personlig integritet som en självständig rättighet, i likhet med vad som är fallet enligt Europeiska konventionen om skydd för de mänskliga rättigheterna (EKMR), samt markera vikten av att skyddet för privatlivet tas i beaktan när ny integritetsbegränsande lagstiftning föreslås.[17]

Vad begreppet personlig integritet innebär är emellertid inte entydigt definierat i svensk rätt.[18] Lagstiftaren har dock, bl.a. i samband med att skyddet för den personliga integriteten gavs grundlagstatus, försökt att beskriva kärnan av begreppet:

> ”att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som enskilde bör vara tillförsäkrad och där ett oönskat ingrepp bör kunna avvisas”[19]

Rätten till förtroligt meddelande och rätten till skydd mot betydande intrång i den personliga integriteten är relativa rättigheter och begränsningar av rättigheterna får enligt 2:20 1 st. 2. RF därför göras genom lag. Sådana bestämmelser som medför begränsningar i skyddet för förtroligt meddelande finns i bl.a. 27 kap RB. För att begränsa rättigheterna för svenska medborgare är förutsättningarna enligt 2:21 RF att

[17] SOU 2008:125, Del 1 s. 469–471.
[18] SOU 2015:31 s. 51–52.
[19] Citat från prop. 2009/10:80 s. 175. Samma lydelse även i SOU 2015:31 s. 51–52.

begränsningen har ett ändamål som är godtagbart i ett demokratiskt samhälle, att begränsningen inte går längre än vad som är nödvändigt med hänsyn till ändamålet och att begränsningen inte hotar den fria åsiktsbildningen. Begränsningen får inte heller göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning. För andra än svenska medborgare får särskilda begränsningar av rättigheterna göras enligt 2:25 1 st. 3. Sådana begränsningar finns t.ex. i 19–20 §§ lagen (1991:572) om särskild utlänningskontroll.

Kravet på svensk lags förenlighet med EKMR fick vid grundlagsändringen ny placering och kravet återfinns för tillfället i 2:19[20]. Stadgandet finns för att tydligt markera att svensk lag inte får strida mot EKMR, om en svensk lag strider mot EKMR så strider lagen även mot detta grundlagsstadgande. Vilken innebörd detta stadgande faktiskt har för t.ex. lagprövningen är dock en fråga som är föremål för diskussion i doktrin, men som inte kommer att behandlas här.[21]

3.2 EKMR

Den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR)[22], är avsett att fungera som minimistandard för mänskliga rättigheter i Europa.[23] Ett antal intressanta rättsfall har rört de fyra rättigheter (rätten till privat- och familjeliv, hem och korrespondens) som skyddas av artikel 8. Ett antal av dessa rättsfall, särskilt ifråga om rätten till hem och korrespondens, har handlat om staters övervakning av enskilda medborgare och övervakningens förenlighet med denna artikel.[24]

I artikel 8 EKMR stadgas att ”var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens”. Inskränkningar i rättigheterna som skyddas av artikeln får dock göras om inskränkningen anses som rättfärdigad på grund av att den är gjord ”i enlighet med lag” och ”nödvändig i ett demokratiskt samhälle” med hänsyn till ett av de erkända syftena som anges i artikeln. Artikel 8 innebär att en enskild är skyddad från

[20] Tidigare var stadgandet placerat i 2:23 RF.
[21] Se t.ex. Nergelius (2014) s. 174–180.
[22] Rom den 4 november 1950, SÖ 1952:35.
[23] SOU 2010:103 s. 497.
[24] Cameron (2014) s. 121, 128.

ingrepp från det allmänna, men även att det allmänna ska skydda enskilda från ingrepp från andra enskilda. Staten har därmed inte bara en skyldighet att avstå från att göra ingrepp i enskildas integritet, utan även en skyldighet att skydda enskilda från ingrepp gjorda av andra enskilda genom att skapa ett effektivt skydd för enskildas rättigheter med hjälp av lagstiftning och upprätthållande av lagstiftningen.[25]

3.2.1 Omfattningen av artikel 8

Europadomstolen har i ett antal fall klargjort omfattningen av rättigheterna som skyddas av artikel 8. Begreppen ”privatliv” och ”korrespondens” täcker enligt domstolen även telefonkonversationer.[26] Likaså omfattas privat användning av internet och e-post av rätten till respekt för privatliv och rätten till respekt för korrespondens, även när användningen sker på en arbetsplats.[27]

Att telefonbolag har uppgifter kring samtalsmottagarare och längd på samtal för en abonnent i syfte att korrekt fakturera abonnenten innebär i sig inte ett intrång i rättigheterna, däremot menar domstolen att det utgör ett intrång om telefonbolaget utan abonnentens samtycke lämnar över informationen till polis.[28] Vidare menar domstolen att redan förekomsten av en lagstiftning som medger avlyssning av individer i sig innebär ett intrång i utövandet av rättigheter som garanteras av artikel 8 för alla de som kan tänkas vara föremål för avlyssningen, eftersom ett hot om avlyssning påverkar möjligheten att kommunicera fritt.[29]

3.2.2 Rättfärdigat intrång i rättigheterna

Finner Europadomstolen att ett intrång i en rättighet har skett så har domstolen att bedöma om intrånget var rättfärdigat. För att avgöra om intrånget är rättfärdigat bedömer domstolen om intrånget i fråga är gjort ”i enlighet med lag”, och om intrånget är ”nödvändigt i ett demokratiskt samhälle” med hänsyn till ett erkänt syfte.

[25] SOU 2015:31 s. 52.
[26] Klass m.fl. mot Tyskland § 41.
[27] Copland mot Förenade kungariket § 41.
[28] Malone mot Förenade kungariket §§ 83–84.
[29] Klass m.fl. mot Tyskland § 41.

3.2.2.1 I enlighet med lag

Kravet på att åtgärden ska vara ”i enlighet med lag” innebär både att åtgärden i fråga ska ha stöd i nationell lag, men även att den nationella lagen håller viss kvalitet. För att lagen ska anses vara av tillräcklig kvalitet måste den vara tillgänglig, lagens konsekvenser måste vara möjliga att förutse och lagen måste stämma överens med rättsstatliga principer (rule of law).[30]

3.2.2.1.1 Grund i nationell lagstiftning och tillgänglig

Kravet på grund i nationell lag innebär att åtgärden måste vara laglig enligt nationell rätt, vilket innebär i enlighet med lagen såsom den utvecklats och tolkats i rättspraxis.[31] Att en lag är oskriven räknas i sig inte som ett hinder för att räknas som lag enligt domstolens praxis.[32] Däremot är det inte svårt att se att det kan bli problematiskt för en stat att visa att en oskriven lag är tillgänglig.

I fallet Khan mot Förenade kungariket ansåg domstolen att avlyssningen inte var i enlighet med lag eftersom hemlig avlyssning vid den tiden endast reglerades av riktlinjer som varken var bindande eller direkt allmänt tillgängliga, eftersom riktlinjerna ifråga fanns i underhusets bibliotek och endast möjliga att få ut efter ansökan.[33] I Liberty m.fl. mot Förenade kungariket ansågs intrånget inte vara i enlighet med lag särskilt på grund av att reglerna kring proceduren gällande hantering, vidarebefordring, lagring och gallring inte var allmänt tillgängliga.[34]

3.2.2.1.2 Förutsägbar

Domstolen har räknat upp minimikrav för att en lagstiftning om hemlig avlyssning ska anses uppfylla kravet på förutsägbarhet. Det krävs att lagstiftningen reglerar vilka kategorier av brott som kan föranleda avlyssning, vilka kategorier av personer som kan avlyssnas, hur länge avlyssning får pågå, vilka procedurer som gäller för granskning, användning och lagring av materialet, vilka säkerhetsåtgärder som ska vidtas om materialet delges andra parter samt vilka regler som gäller angående förstöring av

[30] Kopp mot Schweiz § 55.
[31] Weber och Saravia mot Tyskland § 90.
[32] Kopp mot Schweiz § 60, alternativt Malone mot Förenade kungariket § 66.
[33] Khan mot Förenade kungariket §§ 27 och 16.
[34] Liberty m.fl. mot Förenade kungariket § 69.

upptagningar.[35] Domstolen har vidare menat att det är särskilt viktigt att ha en tydlig och detaljerad lagstiftning eftersom metoderna för hemlig avlyssning utvecklas över tid.[36] Kravet på förutsägbarhet måste dock tolkas något annorlunda ifråga om hemliga avlyssning än på andra områden. Domstolen har uttalat att:

> ”kravet på förutsägbarhet inte kan innebära att en individ ska kunna förutse när det är sannolikt att myndigheterna fångar upp hans kommunikation så att han kan anpassa sitt beteende därefter. Trots det måste lagen vara tillräckligt tydlig i sina uttryck för att ge medborgare en skälig indikation på under vilka omständigheter och förutsättningar som myndigheter är bemyndigade att tillgripa detta hemliga och potentiellt farliga intrång i rätten till respekt för privatliv och korrespondens”[37]

Vilka krav på kvalitet som ställs på lagen ifråga om förutsägbarhet och frånvaro av godtycke är enligt domstolen beroende av hur ingripande intrånget är.[38] I Uzun mot Tyskland ansågs mindre strikta krav på förutsägbarhet kunna ställas på lagstiftningen, eftersom fallet gällde övervakning via en GPS-mottagare som byggdes in i en bil som brukades av bl.a. Uzun. Domstolen menade att övervakning via GPS var ett mindre ingrepp i rätten till privatliv än metoder för visuell övervakning och avlyssning, eftersom sådana metoder, enligt domstolen, avslöjar mer om känslor, åsikter och beteenden än vad som kunde utläsas av att följa en persons rörelse i det offentliga rummet.[39]

Domstolen har förklarat att kravet på förutsägbarhet inte förhindrar att regler utvecklas genom förtydligande och tolkning av en regels innebörd i rättspraxis, så länge utvecklingen av regeln kan förutses och stämmer överens med essensen av regeln.[40] I Uzun mot Tyskland bedömde domstolen att det var förutsägbart att GPS-övervakning kunde omfattas av en skrivning som möjliggjorde användning av ”andra speciella tekniska metoder avsedda för övervakning” (”other special technical means intended for the purpose of surveillance”).[41] En generell skrivning att en högskola tilläts göra allt som var nödvändigt (“anything necessary or expedient”) för att främja högre utbildning, ansågs i fallet Copland mot Förenade kungariket däremot inte tillräckligt förutsägbart för att ska kvalificera som en lag som medgav övervakning av en anställds e-post.[42]

---

[35] Weber och Saravia mot Tyskland § 95.
[36] Weber och Saravia mot Tyskland § 93 och Uzun mot Tyskland § 61.
[37] Citat (min översättning) från Malone mot Förenade kungariket § 67.
[38] P.G. och J.H. mot Förenade kungariket § 46.
[39] Uzun mot Tyskland §§ 12, 52 och 66.
[40] Uzun mot Tyskland § 62.
[41] Uzun mot Tyskland §§ 67–68, 29.
[42] Copland mot Förenade kungariket § 47.

3.2.2.1.3 Överensstämmande med rättsstatliga principer

Att lagen måste överensstämma med rättsstatliga principer innebär ifråga om hemlig övervakning eller avlyssning av kommunikation att lagen måste ha mekanismer för att skydda enskilda mot godtyckliga intrång.[43] Vilka mekanismer som krävs är beroende av omständigheterna i fallet, såsom typen av tvångsmedel, förutsättningarna för att tvångsmedel ska få lov att användas, vilka myndigheter som har möjlighet att använda tvångsmedlet m.m.[44]

3.2.2.2 Nödvändigt i ett demokratiskt samhälle med hänsyn till ett erkänt syfte

Frågan om en inskränkning är gjord med hänsyn till ett erkänt syfte bedöms ofta i samband med kravet på att inskränkningen ska vara ”nödvändig i ett demokratiskt samhälle”.[45] De erkända syftena som kan rättfärdiga en inskränkning framgår av andra stycket i artikel 8[46]. Domstolen har klargjort att de erkända syftena är uttömmande, men enligt Cameron är de så brett formulerade att det sällan är svårt att finna att en lagregel är motiverad med hänsyn till ett av de uppräknade syftena.[47]

Ifråga om kravet på att inskränkningen är nödvändig i ett demokratiskt samhälle så har domstolen klargjort att det inte är fråga om att inskränkningen måste vara strikt nödvändig, utan att kravet snarast ska tolkas som att inskränkningen ska vara gjord på grund av ett ”pressing social need” och vara proportionell i förhållande till sitt syfte.[48] Kravet innebär vidare att staten måste kunna ge godtagbara skäl för inskränkningen.[49] Vad som anses som proportionerligt beror på en mängd faktorer. När domstolen i fallet Uzun mot Tyskland bedömde om övervakningen varit nödvändig i ett demokratiskt samhälle så beaktades brottets grovhet, att mindre ingripande åtgärder inte lyckats och att övervakningen varat en relativt kort tid enligt domstolen (tre månader).[50]

---

[43] Malone mot Förenade kungariket § 67.
[44] Uzun mot Tyskland § 63.
[45] Se Cameron (2014) s. 115, som har en annan mening gällande domstolens lösningsschema.
[46] De erkända syftena är (i svensk översättning): ”den nationella säkerheten, den allmänna säkerheten eller landets ekonomiska välstånd, till förebyggande av oordning eller brott, till skydd för hälsa eller moral eller till skydd för andra personers fri- och rättigheter”.
[47] Cameron (2014) s. 115.
[48] Cameron (2014) s. 117–118, alternativt Uzun mot Tyskland § 78.
[49] Cameron (2014) s. 118.
[50] Uzun mot Tyskland § 80.

Vilket spelrum en stat har att avgöra om en inskränkning är nödvändig i ett demokratiskt samhälle kallas ”margin of appreciation”.[51] Europadomstolen har uttalat att särskilt när begränsningar görs med hänsyn till den nationella säkerheten så har stater en stor frihet att själva avgöra om en åtgärd är nödvändig i ett demokratiskt samhälle.[52]

3.3 EU:s rättighetsstadga

Det finns som bekant även en rättighetsstadga för EU, Europeiska unionens stadga om de grundläggande rättigheterna. Rätten till respekt för privatlivet är fastställd i artikel 7 i stadgan. I stadgans artikel 8 finns även en uttrycklig rätt till skydd för personuppgifter. Av artikel 52.3 följer det att om samma rättigheter finns reglerad både i stadgan och EKMR, så ska rättigheten tolkas på samma sätt som följer av EKMR med tillhörande praxis. Rättighetsstadgan är dock enligt artikel 51.1 enbart tillämpbar när en medlemsstat tillämpar unionsrätten. Detta har av EU-domstolens emellertid tolkas på så sätt att rättighetsstadgan är tillämpbar så fort nationell lagstiftning faller inom unionsrättens tillämpningsområde och inte endast på nationell lagstiftning som genomför EU-rätt.[53]

3.4 Straffprocessuella grundprinciper

Ett antal grundläggande principer måste iakttas vid användningen av tvångsmedel för att förfarandet inte ska komma i konflikt med grundlagen. Ändamålsprincipen, behovsprincipen och proportionalitetsprincipen är de principer som i förarbetena vanligtvis framhålls som nödvändiga att iaktta. Att dessa tre principer måste beaktas påtalas, ofta med identiska formuleringar, i bakgrunden i förarbeten gällande inskränkningar i de grundläggande fri- och rättigheterna.[54] Westerlund framhåller att även legalitetsprincipen, likhetsprincipen och objektivitetsprincipen måste beaktas vid användningen av tvångsmedel.[55]

[51] Cameron (2014) s. 119.
[52] Weber och Saravia mot Tyskland § 106.
[53] SOU 2015:31 s. 54.
[54] Exempelvis i SOU 2009:1 s. 60, prop. 2011/12:55 s. 47 och SOU 2015:31 s. 83.
[55] Westerlund (2013) s. 23.

Ändamålsprincipen, vilken anses följa av 2:21 RF, innebär att tvångsmedel inte får användas för något annat ändamål än vad som anges i lagtexten. Behovsprincipen innebär att endast om det är nödvändigt och verkningsfullt med hänsyn till syftet med åtgärden så får straffprocessuella tvångsmedel användas, och om det finns olika tvångsmedel att tillgå så ska det alternativ som är minst ingripande för den enskilde användas. Proportionalitetsprincipen återfinns i ett flertal stadgande, bl.a. i 27:1 RB. Ett straffprocessuellt tvångsmedel får enligt denna princip endast användas om skälen för åtgärden uppväger det intrång som åtgärden innebär för den misstänkta eller för något annat motstående intresse.[56] Principen kan även sägas framgå av 2:21 RF, dvs. att en begränsning inte får gå längre än nödvändigt med hänsyn till det ändamål som föranlett begränsningen ifråga.[57] I förarbeten uttrycks denna princip ofta på så sätt att ”en tvångsmedelsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden.”[58]

Legalitetsprincipen, som är fastslagen i 1:1 3 st. RF, och som förstärks av stadgandet i 2:20 RF, innebär att varje åtgärd som begränsar grundläggande fri- och rättigheter måste ha stöd i skriven lag som har tillräcklig begriplighet och precision. Principen innebär även ett förbud mot extensiv tolkning, vilket innebär att en lagregel som begränsar grundläggande fri- och rättigheter inte får tolkas så att lagregelns tillämpningsområde utvidgas utöver vad som medges av lagtext och förarbeten. Det innebär dock inte att ett straffbud inte får tolkas enligt vedertagna principer för att utröna dess rätta mening. Likhetsprincipen är fastslagen i 1:2 1 st. RF och innebär att den offentliga makten ska respektera alla människors lika värde och den enskilda människans frihet och värdighet. Objektivitetsprincipen, vilken är fastslagen i 1:9 RF, innebär att förvaltningsmyndigheter ska beakta allas likhet inför lagen och iaktta saklighet och opartiskhet i sin verksamhet.[59]

[56] Westerlund (2013) s. 24.
[57] Nergelius (2014) s. 156.
[58] Prop. 2011/12:55 s. 47.
[59] Westerlund (2013) s. 23–25.

4 Kort historisk tillbakablick

Bestämmelser om hemlig telefonavlyssning[60] har funnits i 27 kap. RB sedan rättegångsbalken trädde i kraft 1 januari 1948. Innan ikraftträdandet av RB så fanns endast tidsbegränsande lagar för säkerhetstjänsten behov under andra världskriget.[61] Efter kriget ansågs utifrån det utrikespolitiska läget att säkerhetstjänsten fortfarande hade särskilda behov som inte tillgodoseddes av bestämmelserna i RB, och därför infördes den tidsbegränsade lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål. I denna lag, som benämns 1952 års lag och var en föregångare till 2008 års utredningslag, fanns en möjlighet till hemlig teleövervakning. Först år 1989 infördes detta tvångsmedel i RB.[62]

Utredningen om vissa hemliga tvångsmedel, som gjort en redogörelse för lagstiftningen historiskt sett, konstaterar att det under andra världskriget och kalla kriget förekom en mycket omfattande användning som inte motsvarade den nytta som medfördes. Ett exempel är att svenska kommunister som troddes vara kapabla att genomföra en revolution i Sverige övervakades under lång tid. När sovjetiska spioner senare under 1980-talet avslöjades så framställdes detta som en framgång för kontraspionaget, trots att avslöjandena inte på något vis var ett resultat av den verksamheten.[63]

4.1 2006 – EU utfärdar datalagringsdirektivet

Datalagringsdirektivet[64] utfärdades den 15 mars 2006 och senast den 15 september 2007 skulle nödvändig nationell lagstiftning träda i kraft. En möjlighet fanns att skjuta upp genomförandet av bestämmelser kring lagring av uppgifter om Internetåtkomst, Internettelefoni och Internetbaserad e-post till 15 mars 2009, vilket utnyttjades av Sverige.[65]

---

[60] Benämning på tvångsmedlet ändrades 1989 till ”hemlig teleavlyssning” och 2012 till ”hemlig avlyssning av elektronisk kommunikation”, se SOU 2012:44 s. 239 och Prop. 2011/12:55 s. 63.
[61] SOU 2012:44 s. 237–238.
[62] SOU 2012:44 s. 178, 241, 239.
[63] SOU 2012:44 s. 177–178.
[64] Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.
[65] Artikel 15 och 16 i datalagringsdirektivet samt SOU 2007:76 s. 17-18.

4.1.1 Bakgrunden till datalagringsdirektivet

Motiveringen till att datalagringsdirektivet antogs, och därmed ändrade den tidigare huvudregeln att uppgifter inte fick sparas, har framförallt varit att det varit nödvändigt för att bekämpa terrorism. Frågan om lagring av trafikuppgifter kom att utredas av ministerrådet i samband med Europeiska rådets fördömande av bombattentatet i Madrid år 2004.[66] I samband med fördömandet av bombattentatet i London år 2005 upprepade ministerrådet vikten av att snarast få till stånd en gemensam reglering i frågan.[67]

I skälen till direktivet anges att det är nödvändigt, i enlighet med kraven i artikel 8 EKMR, att brottsbekämpande myndigheter får tillgång till lagrade uppgifter om elektronisk kommunikation. Detta eftersom omfattningen av elektronisk kommunikation har ökat kraftigt och det i många länder har visat sig att uppgifterna varit ett nödvändigt och effektivt redskap i brottsutredningar, särskilt gällande organiserad brottslighet och terrorism.[68] Det angavs vidare, utan närmare förklaring, att direktivet inte kom i konflikt med Europeisk unionens stadga om mänskliga rättigheter, utan att direktivet ”syftar särskilt att säkerställa full respekt för medborgarnas grundläggande rättigheter”.[69]

I ingressen till direktivet framhålls även att införande av direktivet inte kom i konflikt med subsidiaritetsprincipen eller proportionalitetsprincipen i artikel 5 fördraget om Europeiska unionen. Detta förklaras med att målen med direktivet, harmonisering av tjänstetillhandahållares skyldigheter och säkerställande av att uppgifter finns tillgängliga för bekämpning av allvarliga brott, inte i tillräcklig utsträckning kan nås av de enskilda medlemsstaterna utan bättre kan uppnås på gemenskapsnivå. Vidare anges det att direktivet är i enlighet med proportionalitetsprincipen eftersom ”detta direktiv inte [går] utöver vad som är nödvändigt för att uppnå dessa mål”.[70]

[66] Skäl 8 i ingressen till datalagringsdirektivet samt SOU 2007:76 s. 43.
[67] Skäl 10 i ingressen till datalagringsdirektivet.
[68] Skäl 9 i ingressen till datalagringsdirektivet.
[69] Skäl 22 i ingressen till datalagringsdirektivet.
[70] Skäl 21 i ingressen till datalagringsdirektivet.

4.1.2 Införandet av datalagringsdirektivet i Sverige

Sverige införde emellertid inte datalagringsdirektivet inom utsatt tid, vilket fastslogs av EU-domstolen i en dom 2010.[71] Bestämmelserna om lagring av trafikuppgifter m.m., 6:16a–f LEK, infördes dock slutligen, och bestämmelserna trädde i kraft 1 maj 2012[72], mer än 4,5 år efter att tiden för införande hade gått ut.

4.2 2007–2012 – Sverige inför tidsbegränsad tvångsmedelslagstiftning

I början av 2000-talet infördes en rad tidsbegränsade lagar med det uttalade syftet att förbättra möjligheterna att bekämpa allvarliga brott. Detta ledde till att debatten bland jurister om rätten till personlig integritet kontra effektiv brottsbekämpning blossade upp igen, vilket kommer att redogöras för i avsnitt 5.2.

Fyra lagar av särskilt intresse infördes; *lagen (2007:978) om hemlig rumsavlyssning*, *lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott* [2007 års preventivlag], *lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott* [2008 års utredningslag] och *lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* [2012 års inhämtningslag]. Alla de fyra lagarna var tidsbegränsade, utom 2012 år inhämtningslag som frånsett dess 3 § var permanent giltig. Bestämmelserna i 2008 års utredningslag var egentligen inte nya, eftersom den lagen i själva verket ersatte den tidsbegränsade lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål (1952 års lag).[73] Lagen om hemlig rumsavlyssning och 2008 års utredningslag var enbart tillämpliga i pågående förundersökningar gällande vissa brott som angavs i respektive lag[74]. Både 2007 års preventivlag och 2012 års inhämtningslag får däremot användas i syfte att förebygga brott och innan en förundersökning har inletts och de kan därför betraktas som preventiva tvångsmedel.[75]

[71] Prop. 2010/11:46 s. 71.
[72] Lag (2012:127) om ändring i lagen (2003:389) om elektronisk kommunikation.
[73] SOU 2012:44 s. 239.
[74] Införda i 27 kap. RB sedan 1 januari 2015.
[75] Prop. 2013/14:237 s. 98, 100; jfr 2 § och 8 § 2012 års inhämtningslag.

4.3 2014 – Datalagringsdirektivet ifrågasätts

Den 8 april 2014 ogiltigförklarade emellertid EU-domstolen datalagringsdirektivet genom det uppmärksammade målet Digital Rights m.fl.[76] Som en följd av EU-domstolens dom gav regeringen en utredare i uppgift att snabbutreda konsekvenserna av EU-domstolens dom för den svenska regleringen som baserar sig på datalagringsdirektivet.[77]

Utredaren Sten Heckscher, f.d. justitieråd, menade i sin utredning som presenterades senare under år 2014, bl.a. att EU-domstolens dom skulle tolkas som att det inte nödvändigtvis var oproportionerligt med obegränsad lagring ifall det fanns andra skyddsmekanismer i lagstiftningen, t.ex. att åtkomst till uppgifterna var begränsad.[78] EU-domstolens dom skulle inte heller tolkas som att det stod i konflikt med proportionalitetsprincipen att använda lagrade uppgifterna för annat än det ursprungliga syftet att bekämpa allvarlig brottslighet, menade utredaren. Det är därför inte problematiskt om uppgifterna även används för mindre allvarlig brottslighet.[79]

Den 20 april 2014, dvs. i snar anslutning till att domen presenterades, men innan utredningen presenterades, meddelade Post- och telestyrelsen (PTS) på sin hemsida att de ”inte i nuläget [kommer] att vidta åtgärder utifrån datalagringsreglerna” eftersom de såg ”stora svårigheter att vidta åtgärder med stöd i datalagringsreglerna, som de är utformade i dag”.[80] Som en konsekvens av domen upphörde även ett antal operatörer att lagra data för brottsbekämpande ändamål. Efter att utredaren i Ds 2014:23 bedömde att den svenska regleringen inte stred mot EU-rätten återupptog PTS sin tillsyn och riktade föreläggande mot operatörerna att återuppta lagringen av data.[81]

Att utredningen gjort en korrekt analys ifrågasattes emellertid av vissa operatörer. Internetleverantören Bahnhof valde därför att anmäla Sverige för fördragsbrott till EU-kommissionen.[82] Tele2 överklagade PTS föreläggande att lagra data, eftersom Tele2

[76] Digital Rights Ireland m.fl., förenade målen C-293/12 och C-594/12, (ECLI:EU:C:2014:238).
[77] Justitiedepartementet, Dnr. Ju2014/3010/P.
[78] Ds 2014:23 s. 55.
[79] Ds 2014:23 s. 69.
[80] PTS (2014). ”PTS kommer inte i nuläget att vidta åtgärder utifrån datalagringsreglerna” (webbsida).
[81] SOU 2015:31 s. 133–134.
[82] Bahnhof (2014). ”Vi anmäler Sveriges datalagring till EU-kommissionen” (webbsida); SOU 2015:31 s. 134, 139.

menade att den svenska lagringsskyldigheten stred mot EKMR och RF. Förvaltningsrätten i Stockholm gjorde emellertid bedömningen att lagringsskyldigheten inte stred mot varken EU:s rättighetsstadga, EKMR eller RF och avslog därför Tele2:s överklagan.[83] Förvaltningsrättens dom överklagades dock av Tele2 till Kammarrätten i Stockholm. Kammarrätten beslutade att inhämta ett förhandsavgörande från EU-domstolen och att vilandeförklara målet i avvaktan på EU-domstolens svar.[84]

4.4 2014–2015 – Sverige permanentar tidsbegränsad lagstiftning

Vid årsskiftet 2014–2015 permanentades ett flertal av de tidsbegränsade bestämmelserna gällande tvångsmedel samtidigt som vissa förändringar skedde för att stärka rättssäkerheten. De två preventiva lagarna, 2007 års preventiv och 2012 års inhämtningslag, kvarstod som separata lagar, medan 2008 års utredningslag och lagen (2007:978) om hemlig rumsavlyssning inarbetades i RB. Genom att bestämmelserna i 2008 års utredningslag och lagen (2007:978) om hemlig rumsavlyssning inarbetades i RB gjordes bestämmelserna permanenta.

4.4.1 2007 års preventivlag permanentas

I 1 § 2007 års preventivlag föreskrivs att tillstånd till HAEK, HÖEK och hemlig kameraövervakning enligt RB får användas när det finns ”en påtaglig risk att en person kommer att utöva brottslighet” som innefattar ett eller flera av de ”särskilt allvarliga brotten” som räknas upp i paragrafen. De ”särskilt allvarliga brotten” som räknas upp i paragrafen är bl.a. sabotage, mordbrand, uppror, terrorism, och spioneri (se 1 §). Lagen var tidigare tidsbegränsad till utgången av 2014, men från och med 1 januari 2015 gäller lagen utan tidsbegränsning.[85] I och med att lagen permanentades så genomfördes även ett antal ändringar för att utvidga tillämpningsområdet för lagen och förenkla tillämpningen. Ändringarna genomfördes eftersom Säkerhetspolisen menade att lagen fått för snävt tillämpningsområde. Säkerhetspolisen menade att detta var en följd av att

[83] Förvaltningsrätten i Stockholm, mål nr. 14891-14, dom 2014-10-13.
[84] Kammarrätten i Stockholm, mål nr. 7380-14, beslut 2015-04-28.
[85] Lagen (2014:1421) om ändring i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

allt för höga krav på konkret misstanke ställdes och att detta inneburit att lagen inte tillgodosett Säkerhetspolisens behov av verksamma medel för förebygga och förhindra systemhotande verksamhet.[86] Uttrycket ”särskild anledning att anta” (att en person kommer att utöva brottslig verksamhet...) som tidigare använts i 1 § byttes därför ut mot ”påtaglig risk”. Att ett misstankerekvisit har bytts ut mot ett riskrekvisit innebär att det inte längre måste föreligga en misstanke om en konkret brottslig gärning, det räcker med att ett flertal omständigheter starkt talar för att en risk kommer att förverkligas utan att det är känt hur risken förverkligas. Det ska dock gälla faktiska omständigheter, det räcker inte med endast generella bedömningar eller spekulationer.[87]

Vid permanentandet av lagen gjordes även viss lättnad av vilka beviskrav som gäller i förhållande till medlemmar inom en grupp för vilken det finns en påtaglig risk ska utöva brottslig verksamhet (1 § 2 st.). När en individ ”tillhör eller verkar för” en sådan grupp eller organisation är det inte nödvändigt att det finns en påtaglig risk för att individen ska begå brottslighet, det räcker med att individen kan befaras medvetet främja en sådan verksamhet. Enbart medlemskap innebär inte att detta krav är uppfyllt, men om medlemmen innehar en ställning i organisationen eller är tidigare dömd för annan ”relevant” brottslighet är det sådant som kan tala för att det föreligger en ”främjandefara”, enligt propositionen.[88]

4.4.2 2012 års inhämtningslag utreds

I samband med utredningen av konsekvenserna av EU-domstolens ogiltigförklarande av datalagringsdirektivet framkom det att det även fanns skäl att utreda om någon ändring krävdes i 2012 års inhämtningslag för att stärka integritetsskyddet för enskilda. En utredning, vars betänkande mycket kort kommer att presenteras i avsnitt 4.5.2, tillsattes därför i detta syfte.[89]

Inhämtning enligt 2012 års inhämtningslag får ske i syfte att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Den brottsliga verksamheten ska antingen innefatta brott för vilket lägsta föreskrivna straff är fängelse i 2 år (2 § 1 st. 1), eller brott som

[86] Prop. 2013/14:237 s. 103.
[87] Prop. 2013/14:237 s. 106, 195.
[88] Prop. 2013/14:237 s. 196–197.
[89] Dir. 2014:101 s. 1, 10–11.

räknas upp i den tidsbegränsade 3 §.[90] En förutsättning för att inhämtning ska få lov att ske är att åtgärden bedöms som proportionerlig av myndigheten som inhämtar uppgifterna (2 § 1 st. 2). Myndigheterna ifråga är Polismyndigheten, Tullverket och Säkerhetspolisen (1 §). Det är myndigheterna själva som fattar beslut om när inhämtning ska ske, men om en myndighet beslutat om inhämtning så ska underrättelse lämnas till tillsynsorganet Säkerhets- och integritetsskyddsnämnden (4 § och 6 §). Inhämtning sker i underrättelseverksamhet och uppgifterna får därför användas i en förundersökning endast om ett tillstånd för HÖEK senare ges (1 § och 8 §). De uppgifter som kan inhämtas motsvarar vad som kan inhämtas enligt RB:s regler om HÖEK, frånsett att endast historiska trafikuppgifter kan inhämtas genom 2012 års inhämtningslag till skillnad från regleringen i RB (jfr 27:19 1 st. 1 RB och 1 § 2012 års inhämtningslag).

4.4.3 2008 års utredningslag införs i 27 kap RB

Den tidsbegränsade lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott upphörde att gälla vid årsskiftet 2014–2015 och bestämmelserna infördes istället i 27 kap. RB samtidigt som de blev permanent giltiga.[91] Lagtekniskt genomfördes det genom att brottskatalogen över ”samhällsfarliga brott” som återfanns i 1 § 2008 års utredningslag överfördes till 27:2 2 st. 2–7 RB, med undantag för brottet olovlig kårverksamhet. Bestämmelserna innebär bl.a. att tillstånd till HAEK och HÖEK kan medges även om lindrigare straff än två år respektive sex månaders fängelse är föreskrivet för brottet, om brottet är ett av de ”samhällsfarliga” brott som räknas upp i 27:2 2 st. 2–7 RB (se 27:18 2 st. och 27:19 3 st.). Det motsvarar, med undantag för olovlig kårverksamhet, de brott som angavs i 2008 års utredningslag. Till skillnad mot vad som gällt enligt 2008 års utredningslag, och som en konsekvens av ändringen i 27:18 2 st. RB och hänvisningen till den paragrafen i 27:19 4 st., så kan HÖEK användas i syfte att utreda vem som kan misstänkas för ett samhällsfarligt brott eller en osjälvständig form av ett sådant brott.[92]

[90] I november 2014 förlängdes giltigheten för 3 § tills utgången av 2016, se SFS 2014:1422.
[91] Lag (2014:1419) om ändring i rättegångsbalken.
[92] Prop. 2013/14:237 s. 176–178.

4.4.4 Lagen om hemlig rumsavlyssning permanentas

Den tidigare tidsbegränsade lagen (2007:978) om hemlig rumsavlyssning upphörde att gälla vid utgången av 2014. Från och med 1 januari 2015 regleras hemlig rumsavlyssning istället i 27 kap. RB, se särskilt 27:20d.[93] Hemlig rumsavlyssning, s.k. ”buggning” får, i likhet med vad som gällde enligt den upphävda lagen, användas mot någon som är skäligen misstänkt för ett brott vars minsta föreskrivna straff är fängelse fyra år eller ett brott som kan antas ha ett straffvärde på minst 4 år om brottet är ett av de brott som räknas upp i paragrafen (27:20d 2 st. 1 och 4, samt 27:20e)[94]. I samband med att reglerna permanentades skedde även viss förändring av tillämpningsområdet för hemlig rumsavlyssning. Efter permanentandet kan hemlig rumsavlyssning användas även när en gärnings straffvärde bedöms vara lägre än fängelse i fyra år om förundersökningen gäller spioneri eller s.k. statsstyrt företagsspioneri som kan antas ge mer än böter, samt osjälvständiga former av dessa brott som är straffbelagda (27:20d 2 st. 2–3 och 5).[95]

4.4.5 Ändringar i syfte att stärka integritetsskyddet

I samband med att de tidigare tidsbegränsade lagarna permanentades gjordes även vissa lagändringar för att stärka skyddet för enskildas integritet. Bland annat försvann möjligheten för domstol att fatta beslut utan ett offentligt ombuds närvaro från 27:28 2 st. RB.[96] Det infördes även en möjlighet för rätten att föreskriva villkor till skydd för enskildas integritet i tillståndet för tvångsmedlet (27:21 6 st. RB).[97] Vidare utvidgades avlyssningsförbudet i 27:22 gällande HAEK till att omfatta fler personer än tidigare. Ändringen innebära att inte endast samtal mellan misstänkt och försvarare omfattas av avlyssningsförbudet, utan alla som inte kan höras som vittne p.g.a. bestämmelserna i 36:5 2–6 st. RB omfattas. Det innebär att avlyssningsförbudet vid HAEK har samma omfattning som avlyssningsförbudet vid hemlig rumsavlyssning.[98]

[93] Lag (2014:1419) om ändring i rättegångsbalken.
[94] Reglerades tidigare i 2–3 §§ i lagen om hemlig rumsavlyssning.
[95] Prop. 2013/14:237 s. 179.
[96] Prop. 2013/14:237 s. 189.
[97] Prop. 2013/14:237 s. 181.
[98] Prop. 2013/14:237 s. 184.

4.5 2015 – EU-länder ogiltigförklarar respektive försvarar datalagring

Frågan om vilka konsekvenser EU-domstolens ogiltigförklarande av datalagringsdirektivet har för nationell lagstiftning som baseras på direktivet har hanterats på skilda sätt av de olika EU-länderna. En del medlemsstater har valt att ogiltigförklara lagstiftning som baseras på direktivet medan andra länder, bl.a. Danmark, har granskat sin lagstiftning och funnit att den inte strider mot grundläggande fri- och rättigheter.[99]

4.5.1 Storbritannien, Nederländerna m.fl. ogiltigförklarar

Domstolar i ett antal EU-länder har som ett resultat av EU-domstolens dom ogiltigförklarat nationell lagstiftning som baserar sig på direktivet. I juni 2014 förklarade Österrikes författningsdomstol att den nationella datalagringslagstiftnigen var oförenlig med landets konstitution.[100] Även Belgiens författningsdomstol har i juni 2015 ogiltigförklarat nationell lagstiftning som baserades på direktivet.[101] I Nederländerna har Haags distriktsdomstol i mars 2015 ogiltigförklarat den nationella lagstiftningen.[102] I juli 2015 ogiltigförklarade även en domstol (High Court of Justice, Queen's bench division) i Storbritannien den nationella datalagringslagstiftningen.[103]

4.5.2 Svenska lagstiftaren försvarar datalagring

I Sverige tillsattes en utredning av bl.a. 2012 års inhämtningslag som konsekvens av EU-domstolens dom. Utredningen, som antagit namnet Datalagringsutredningen, presenterades i mars 2015 betänkandet SOU 2015:31. Datalagringsutredningen bestod, liksom utredningen som presenterade Ds 2014:23 och SOU 2012:44, av ensam utredningsman Sten Heckscher, f.d. justitieråd. Expertkunskap inhämtades av bl.a. Iain Cameron.[104]

---

[99] SOU 2015:31 s. 145, 140-157.
[100] SOU 2015:31 s. 150–153.
[101] Cour constitutionelle, n°84/2015, 11/06/2015;
http://www.europeanrights.eu/index.php?lang=eng&funzione=S&op=2&id=4401
[102] Rechtbank Den Haag, C09/480009/KG ZA 14/1575 (ECLI:NL:RBDHA:2015:2498),
http://www.europeanrights.eu/index.php?funzione=S&op=2&id=4288
[103] David Davis MP case UK, Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014.
[104] SOU 2015:31, förord: "Till statsrådet Anders Ygeman".

4.5.2.1 Utredningen av inhämtningslagen presenteras

Datalagringsutredningen föreslog i betänkandet ändringar av 2012 års inhämtningslag, men även ändringar i RB och 2007 års preventivlag vad gällde förstöring av upptagningar. Förslaget till ändringar av 2012 års inhämtningslag innebar att den brottskatalog som fanns i den tidsbegränsade 3 § infördes i den permanent giltiga 2 § samt utökades med ytterligare brottsrubriceringar.[105]

4.5.2.2 Datainspektionen uttalar sig om utredningen

Datainspektionen (DI) har i ett yttrande riktat kritik mot utredning och sagt sig välkomna EU-domstolens prövning av den svenska lagstiftningens förenlighet med de grundläggande fri- och rättigheterna. Enligt DI innebär datalagringen och möjligheterna att sammanställa lagrad information stora risker ur ett integritetsperspektiv, eftersom det går att få en detaljerad bild av individer och deras liv. Samtidigt är datalagring mycket effektivt ur ett brottsbekämpnings perspektiv, och det är därför nödvändigt att ha en lagstiftning som är välbalanserad, menar DI.[106]

DI menar att det i Datalagringsutredningen saknas ett proportionalitetsresonemang för att stödja slutsatsen att inga förändringar behövs. Vidare menar DI att det behövs ett bättre underlag än det som presenterats för att kunna styrka att lagstiftningen är strikt nödvändigt i den formen och att alla uppgiftskategorier som lagras verkligen behövs. Att det saknas en analys av hur människor upplever övervakning och om de anpassar sitt beteende av oro över att vara eller bli övervakade är ytterligare en brist i utredningen, enligt DI.[107]

DI menar att man borde överväga ytterligare åtgärder för att stärka integritetsskyddet när abonnemangsuppgifter lämnas ut av operatörer. Förvisso håller DI med utredningen om att abonnemangsuppgifter generellt sett är mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter, men menar att abonnemangsuppgifter samtidigt kan vara mycket känsliga när de består av uppgifter om vem som innehaft en viss IP-adress under en viss tid. Detta menar DI är p.g.a. att människor gör så mycket mer och lämnar så mycket fler spår vid användning av internet än vid telefonsamtal och sms. DI ifrågasätter

[105] SOU 2015:31 s. 305, 309, 327.
[106] Datainspektionen (2015). ”Datalagring och integritet (SOU 2015:31)” s. 1–2.
[107] Datainspektionen (2015). ”Datalagring och integritet (SOU 2015:31)” s. 2–3.

även om det är lämpligt att utredningen utgår ifrån att myndigheter enbart vill få kännedom om vilken person som varit tilldelad en viss IP-adresser vid en viss tidpunkt i syfte att utreda en konkret händelse och inte för att kartlägga individers beteende på internet generellt.[108]

För att förbättra integritetsskyddet föreslår DI därför att en särskild myndighet får i uppdrag att kontrollera att inhämtning av abonnemangsuppgifter inte görs på felaktiga grunder. Enligt DI har det nämligen framkommit att brottsbekämpande myndigheter och operatörer ibland har haft olika åsikt gällande om en viss typ av uppgift utgjort en abonnemangsuppgift eller endast fått inhämtas med stöd av HAEK eller HÖEK. DI menar vidare att inhämtning av abonnemangsuppgifter inte borde komma ifråga vid bagatellartade brott med hänsyn till proportionalitetsprincipen.[109]

DI är inte lika säker som Datalagringsutredningen på att 2012 års inhämtningslag lever upp till de krav som ställs enligt Europarätten. Särskilt problematiskt menar DI det är att de brottsbekämpande myndigheterna själva fattar inhämtningsbeslut utan inblandning av domstol. Att Datalagringsutredningen föreslår att den tidsbegränsade 3 § ska göras permanent giltig samt att inhämtning ska få ske vid ytterligare brottsrubriceringar är ytterligare omständigheter som gör att DI ställer sig tveksam.[110]

4.5.3 Regeringen presenterar ny strategi mot terrorism

För att visa på utvecklingstendensen i Sverige, kan det lite parentetiskt nämnas att inrikesminister Ygeman i slutet av augusti år 2015 presenterade en ny strategi mot terrorism i en skrivelse till riksdagen. I skrivelsen anges bl.a. att tekniken förändrats, att brottslingar anpassar sig till utvecklingen och att en adekvat reglering av användningen av hemliga tvångsmedel är nödvändig.[111] Regeringen angav att den särskilt ska verka för att:

> ”de brottsbekämpande myndigheterna ges förutsättningar att, med hänsyn till skydd av den personliga integriteten och rättssäkerheten, upprätthålla sin förmåga att inhämta information”[112]

[108] Datainspektionen (2015). ”Datalagring och integritet (SOU 2015:31)” s. 4–5.
[109] Datainspektionen (2015). ”Datalagring och integritet (SOU 2015:31)” s. 5.
[110] Datainspektionen (2015). ”Datalagring och integritet (SOU 2015:31)” s. 6.
[111] Skr. 2014/15:146 s. 16–17.
[112] Citat från skr. 2014/15:146 s. 17.

På den tillhörande presskonferensen[113] klargjorde inrikesminister Ygeman att detta bl.a. innebar en planerad översyn av lagstiftningen gällande hemliga tvångsmedel och att frågan om införande av det i dagsläget otillåtna tvångsmedlet hemlig dataavläsning återigen lyfts. Hemlig dataavläsning innebär i klartext att brottsbekämpande myndigheter tar sig in i (”hackar”) misstänktas telefoner eller datorer för att installera spionprogram som sedan låter brottsbekämpande myndigheter se vad en användare gör på telefonen eller datorn.[114]

Regeringen har fått både beröm och kritik för den presenterade strategin. Terrorforskaren Hans Brun har uttalat att den presenterade strategin är ”ganska genomarbetad” och ”med ganska tydliga idéer och riktlinjer” när SVT tillfrågar honom.[115] Framstående advokater som har uttalat sig är däremot kritiska och menar att strategin kommer att vara ineffektiv samtidigt som den kommer att utgöra ett ”hot mot den demokratiska rättsstaten”. Anne Ramberg menar att man inte kan frångå grundläggande fri- och rättigheter bara för att Säkerhetspolisen står inför svåra utmaningar. Thomas Olsson menar att det vore ett stort misstag om hemlig dataavläsning skulle införas eftersom det skulle skapa en ständig oro hos människor som en konsekvens av att man inte kan veta om man är övervakad.[116]

[113] Presskonferensen finns tillgänglig via http://www.regeringen.se/pressmeddelanden/2015/08/sveriges-nya-strategi-mot-terrorism/
[114] Kleja (2015). ”Spiontrojan kan bli polisens nya verktyg” (webbsida), NyTeknik.
[115] Berger (2015). ”Terrorforskaren: ”En genomarbetad strategi”” (webbsida), Svt Nyheter..
[116] Berger, Ella och Bering, Sofia (2015). ”Strategin ”ett hot mot den demokratiska rättsstaten”” (webbsida), Svt Nyheter. För en fördjupad diskussion om hemlig dataavläsning se t.ex. Ramberg (2007) s. 163–164.

5 Debatten kring lagstiftningen

5.1 Lagstiftarens motivering

I Utredningen om vissa hemliga tvångsmedel har Sten Heckscher undersökt de föreställningar och utgångspunkter som anges i direktiven till utredningen och som ofta legat till grund för andra utredningar om utökade befogenheter. I direktivet till utredningen anges ”att brottsutvecklingen under senare år har präglats av en ökad internationalisering, förbättrad teknisk kapacitet och tydligt organiserade, resursstarka kriminella grupperingar.”[117]

Utredningen menar att det inte stämmer att problemet med den organiserade brottsligheten blivit allt värre. Istället har den organiserade brottligheten minskat inom vissa områden, t.ex. dobbleri och illegal alkoholförsäljning, vilket utredningen menar beror på att utbudet ökat genom att Svenska spel m.fl. tagit över spelmarknaden och krogtätheten och privatimporten ökat.[118] Det är även en förhastad slutsats, menar utredningen, att tro att teknikutvecklingen lett till att brottsligheten radikalt förändrats och att den organiserade brottsligheten i en allt snabbare takt hittar nya områden att utöva sin verksamhet inom.[119] Det var inte heller korrekt enligt utredningen, att påstå att människor och grupper som begår brott ”alltid ligger ’steget före’ och att myndigheterna alltid ’hamnar på efterkälken’”. Personer som begår brott gör istället minsta möjliga arbete och anpassar sitt beteende först när det är nödvändigt.[120]

Utredningen har även tittat på hur förändringar av lagstiftningen har motiverats. Utredningen drar slutsatsen att det återkommande argumentet för att motivera annat än integritetsstärkande ändringar av lagstiftningen varit att ”samhället har utvecklats på så sätt att brottslighet eller teknik förändrats”.[121] Ett exempel på ett sådant argument är påstående om att brottsligheten blivit mer organiserad genom en nätverksstruktur och att den grova brottsligheten utökat sin verksamhet till fler brott än tidigare.[122]

[117] Citat från SOU 2012:44 s. 174.
[118] SOU 2012:44 s. 222.
[119] SOU 2012:44 s. 224.
[120] SOU 2012:44 s. 217.
[121] Citat från SOU 2012:44 s. 242.
[122] SOU 2012:44 s. 242.

Förutom påstående att brottsligheten blivit mer svårbekämpad så motiveras ändringar i lagstiftningen ofta utifrån effektivitetsskäl. Att en viss typ av uppgifter är värdefulla eller av stor vikt för brottsutredningar gällande grövre brott anges ofta som argument för att myndigheterna ska få lov att ta del av dem. Inte sällan anges det sedan kort att det inte utgör något större intrång i den personliga integriteten.[123]

> ”BRU konstaterade att [lokaliserings]uppgifterna många gånger är värdefulla i brottsbekämpningen, att uppgifterna kan ha mycket stor betydelse i effektivitetshänseende, att det tveklöst finns ett mycket stort behov av att få tillgång till sådana uppgifter och att det inte möter några avgörande hinder från integritetssynpunkt med en ordning där sådana uppgifter lämnas ut vid hemlig teleövervakning”.[124]

På senare tid har utredningar i större grad uppmärksammat den intressekonflikt som existerar mellan effektivitet i de brottsbekämpande myndigheternas arbete och enskildas rätt till integritet vid datalagring. Framförallt uppmärksammats att allmänhetens förtroende för rättssystemet påverkas av datalagring. För att myndigheter i hemlighet ska få lov att samla in integritetskänsliga uppgifter krävs därför starka skäl om inte allmänhetens förtroende ska förloras. Samtidigt minskar även förtroendet för de brottsbekämpande myndigheterna om de inte har möjlighet att genomföra sina uppdrag. I Datalagringsutredningen, SOU 2015:31, uttalas därför att ”en viktig utgångspunkt är att myndigheterna inte får ges sådana befogenheter att medborgarnas tilltro till dem påverkas negativt”.[125]

5.2 Akademikerna och praktikernas debatt

Framförallt vid två tillfällen under de senaste åren har jurister brett engagerat sig i en debatt om integritet, rättssäkerhet och tvångsmedel. Med anledning av lagen om hemlig rumsavlyssning och 2007 års preventivlag debatterades år 2006 integritet och rättssäkerhet, vilket bl.a. resulterade i ett temanummer i Svensk Juristtidning (SvJT). I samband med debatten kring ”FRA-lagen”[126] och beredningen inför grundlagstadgandet av rätten till skydd mot betydande intrång i den personliga integriteten diskuterades problematiken återigen. Ett axplock av dessa debattinlägg ska presenteras här.

[123] Exempelvis i prop. 2011/12:55 s. 91, 97.
[124] Citat prop. 2011/12:55 s. 97.
[125] SOU 2015:31 s. 55.
[126] Lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, se även 6:19a LEK.

5.2.1 Rättschefens perspektiv

Rättschefen Abrahamsson har i sitt bidrag till debatten i SvJT strukturerat upp och redogjort för de argument som ofta används i övervakningsdebatten. Han menar att det saknas nyanser och att debattörerna ofta antingen framför ”övervakningsanhängare” eller ”integritetsvännernas” argument och bortser från andra argument. Abrahamsson efterlyser därför ett mer rationellt förhållningssätt både i debatten och av lagstiftaren.[127]

Abrahamsson menar att övervakningsanhängares argument ofta innebär att: (1) Den som har rent mjöl i påsen inte har något att dölja och den personen behöver därför inte oroa sig över att bli övervakad. Enligt Abrahamsson är detta enkelt att motsäga, alla förtjänar rätt till privatliv och integritet enligt RF och EKMR ”oavsett vilket slags mjöl vederbörande har i sin påse”. (2) De som utsätts för grova brott får utstå den största integritetskränkningen. Abrahamsson menar att offrets lidande är ett relevant skäl, men att uttalandet inte ger vägledning i avvägningen mellan integritet och effektivitet, särskilt när tvångsmedlen används innan någon är misstänkt. (3) Människor delar frivilligt mycket information om sig själva på internet och låter sina beteendemönster bli kartlagda genom användning av t.ex. kreditkort, och de kan därför inte ha något emot att bli övervakade av staten. Abrahamsson menar att även om en del människor delar mycket information, så är det skillnad mellan att frivilligt dela och att ofrivilligt bli kartlagd av staten. Den enskilde kan inte välja vad som delas när staten kartlägger och får inga fördelar som status, social acceptans etc. av att informationen delas.[128]

(4) Statsmakterna har hävdat att det inte utgör ett intrång att samla in information, utan att ett integritetsintrång sker först när man analyserar eller på annat sätt utnyttjar informationen. Även detta argument går att tillbakavisa enligt Abrahamsson, lagrådet har nämligen klargjort att ett intrång sker redan när informationen samlas in. (5) Om inhämtad information enbart behandlas av behörig personal med tystnadsplikt sker inget intrång, enbart missbruk utgör intrång. Abrahamsson menar att det alltid sker ett integritetsintrång och att det måste erkännas att det är två motstående intressen för att ett försök att balansera dessa ska kunna göras.[129]

[127] Abrahamsson (2009) s. 423, 427.
[128] Abrahamsson (2009) s. 424.
[129] Abrahamsson (2009) s. 424–425.

Abrahamsson menar att integritetsvännernas argumentation samtidigt hindrar en seriös debatt eftersom de använder sig av (1) osakliga åberopande av referenser från populärkultur, t.ex. Orwells roman 1984, utan att visa varför hänvisningen är relevant i sammanhanget. (2) Svepande och icke-verifierade påstående, som t.ex. att befolkningen motsätter sig kameraövervakning, vilket enligt Abrahamsson inte har visats av undersökningar som har genomförts. Han menar vidare (3) att det är en intellektuell elit som säger sig tala för folket, men som inte egentligen representerar folkets åsikt. Att (4) integritetsvännerna är okunniga om vad tekniken medger och hyser för stor oro över vad som i framtiden kommer att kunna utläsas av olika typer av information. Abrahamsson menar vidare att (5) integritetsvännerna ofta fokuserar på fel saker och engagerar sig i onödiga diskussioner vilket gör att fokus flyttas från betydelsefulla frågor.[130]

Abrahamssons förslag för att lösa situationen är ökad rationalitet i lagstiftningsarbetet. Lagstiftaren bör göra en mycket mer omsorgsfull proportionalitetsprövning vid införandet av tvångsmedelslagstiftning än som görs idag, och i den prövningen ta hänsyn till det integritetsintrång som alla tvångsmedel innebär sammanlagt. Detta menar Abrahamsson är lämpligt att göra för att undvika att medborgarna får uppfattningen att de lever i ett övervakningssamhälle.[131]

5.2.2 Åklagarnas perspektiv

Vice chefsåklagare Hilding Qvarnström menar att grova brott blivit vanligare, grövre och mer komplicerade, och att denna trend troligtvis kommer att fortsätta. Enligt Hilding Qvarnström är det mycket svårt att utreda grov och komplicerad brottslighet när den misstänkte (eller med Hilding Qvarnströms ord ”motståndaren”) är yrkeskriminell eller del av ett internationellt nätverk, och utan hemliga tvångsmedel hade det inte gått att komma vidare i ”lejonparten” av fallen. Hon menar att Sverige har en skyldighet jämtemot andra länder att ha hemliga tvångsmedel, eftersom utan dem skulle Sverige riskera att bli en fristad, ”safe haven”, för kriminella.[132] Hilding Qvarnström menar vidare att nästan alla andra EU-länder har regler om buggning. Hemliga tvångsmedel är enligt Hilding Qvarnström en förutsättning för att ”laglydiga medborgare” ska få det

[130] Abrahamsson (2009) s. 425–426.
[131] Abrahamsson (2009) s. 427–428.
[132] Hilding Qvarnström (2007) s. 136.

fungerande rättsväsende som de har betalat för, och Hilding Qvarnström menar att hon tror sig kunna säga att det ”i princip är ’samma människor’ som tidigare” som blir föremål för nya tvångsmedel, bara att ny teknik används. Hilding Qvarnström menar att fokus i debatten blivit fel när integritetsintrång av vitt skilda grader diskuteras tillsammans, och det på så sätt ”blandas friskt mellan äpplen och päron” för att visa på att vi går mot ett samhälle med mer övervakning.[133]

Att lagstiftningen hela tiden behöver ändras på grund av att tekniska förutsättningar förändras gör systemet tungrott, menar Hilding Qvarnström, och efterlyser därför en mer teknikneutral lagstiftning. Hilding Qvarnström uttrycker att det är frustrerande att inte få tillgång till viktig information för att kunna förhindra eller utreda brott. Hemliga tvångsmedel är endast avsedda för allvarliga brott, som ofta har starka målsägarintressen, enligt Hilding Qvarnström. Vidare menar Hilding Qvarnström att det är mycket integritetskränkande att bli utsatt för brott och att brottsoffer därför förväntar sig att man ska lägga ”alla tänkbara resurser” på att utreda brott.[134]

Ett annat åklagarperspektiv kommer från överåklagare Gunnel Lindberg. Enligt Lindberg kan man se vissa tydliga tendenser i hur tvångsmedelsanvändning utvecklats, t.ex. tog många länder, bl.a. Sverige, attacken 11 september 2001 som en förevändning att utöka myndigheters befogenheter och hemliga tvångsmedlens tillämpningsområde. Under de senaste 10 åren har tvångsmedelsregleringen i RB förändrats många gånger och i stor utsträckning, och dessa förändringar har framförallt varit i för myndigheter befogenhetsutvidgande och för enskilda integritetsbegränsande riktning. Det föreligger enligt Lindberg även en tendens till att tvångsmedelslagstiftning placeras utanför RB och att tvångsmedel används i andra syften än att utreda brott, t.ex. förebygga brott. En ytterligare tendens är att nya tvångsmedel tillkommer samtidigt som äldre tvångsmedel blir kvar och att tidigare tidsbegränsade lagar permanentas.[135]

Teknikneutral lagstiftning är både en fördel och en nackdel, menar Lindberg. Det är naturligtvis praktiskt att lagstiftningen inte behöver ändras hela tiden, men det utgör ett problem att det blir mycket svårt att förutse hur ett tvångsmedel kommer att användas i

[133] Hilding Qvarnström (2007) s. 137–138.
[134] Hilding Qvarnström (2007) s. 138–140.
[135] Lindberg (2007) s. 52–53.

framtiden. Man kan inte låta de brottsbekämpande myndigheternas önskemål om effektivare verktyg styra, utan måste även beakta integritetsaspekter, men samtidigt är det ibland bättre att lagstifta eftersom myndigheterna annars använder metoderna oreglerat. Den samlade övervakningen kan oavsett bli mycket integritetskränkande eftersom man kan få en väldig omfattande bild av en person när tvångsmedel kombineras.[136] Lindberg menar att det är särskilt allvarligt när staten kränker enskilda eftersom enskilda inte har någon annan att vända sig till för att få upprättelse. Därför menar Lindberg att det borde vara större kontroll och uppföljning av användningen av tvångsmedel, samt att konsekvenserna borde vara allvarligare för staten när ett felaktigt beslut tas. Detta skulle enligt Lindberg leda till större legitimitet hos allmänheten.[137]

5.2.3 Advokatperspektivet

Anne Ramberg, generalsekreterare för Advokatsamfundet, menar att man måste se tvångsmedelsanvändning i ett helhetsperspektiv, undersöka den samlade övervakningen av alla tvångsmedel och på så vis låta ”äpplen och päron packas i samma korg”.[138] Ramberg menar att samtidigt som generella påstående om otydligt definierade företeelser som “gränsöverskridande brottslighet” och “systemhotande brottslighet” frekvent förekommer i förarbeten, så är utredningar om behov av nya tvångsmedel och dess förmodade effektivitet, vanligtvis undermåliga.[139]

Ett ytterligare problem som Ramberg ser när behovet beskrivs är att undersökningar i stor utsträckning utgår ifrån argument och uppgifter som lämnats av brottsbekämpande myndigheter, som enligt Ramberg bevakar sina egna intressen i saken.[140] Ramberg menar vidare att nya tvångsmedel ofta motiveras med att liknande tvångsmedel finns i andra länder, och att en slags ”nödvändighetsargumentation” ofta används. Denna argumentation innebär att nya tvångsmedel måste införas eftersom de yrkeskriminella har förändrat sitt beteende, t.ex. påstås att buggning behövs eftersom kriminella slutat tala i telefon. Samtidigt införs långtgående övervakning och lagring av trafikuppgifter med hänvisning till att yrkeskriminella använder just telefoner för att planera brott. Ett

[136] Lindberg (2007) s. 55–56.
[137] Lindberg (2007) s. 57–58.
[138] Ramberg (2007) s. 169
[139] Ramberg (2007) s. 156.
[140] Ramberg (2007) s. 161.

annat argument som Ramberg menar ofta används är att tvångsmedlen endast drabbar grovt kriminella. Detta är inte med sanningen överensstämmande, menar Ramberg, och nämner frysningen av tillgångar under lång tid för svenskar av somaliskt ursprung.[141] Enligt Ramberg finns det en övertro till att staten är god bara för att den är demokratisk. Även om terrorism och annan grov brottslighet utgör hot mot människor och stater, så utgör statens missbruk av maktmedel ett ännu värre hot eftersom maktmissbruk hotar rättsstaten och det demokratiska samhällsbygget. Värdet av brottslighet är låg upplevs av vissa debattörer som nästan överordnat, menar Ramberg. Detta menar hon är ett resultat av att deras synsätt är att den största integritetskränkningen någon kan råka ut för är att bli utsatt för brott. Enligt Ramberg står emellertid inte kostnaden för ett samhällen med en låg brottslighet i proportion till värdet av ett sådant, eftersom kostnaden är att vi får en annan, betydligt mer totalitär, form av samhälle.[142]

5.2.4 Kriminologens perspektiv

Janne Flyghed, professor i kriminologi, menar att krav på utökade övervakning ofta kommer när politiker vill visa handlingskraft efter nyckelhändelser som terrordådet 11 september 2001. Vid sådana tillfällen menar Flyghed att oavsett om det finns belägg för tolkningen att nya integritetskränkande metoder bör införas, så ges de som gör denna tolkning företräde framför de som vill värna skyddet av den personliga integriteten.[143]

Flyghed menar att argumenten som används för att legitimera införandet av nya integritetskränkande metoder bygger på hotbilder som ofta är exceptionella och dramatiska, och som dessutom ofta bygger på vaga begrepp som ”grov organiserad brottslighet” och ”terrorism”. Hotbilderna används för att legitimera tvångsmedel, såväl redan införda som nya metoder, men hotbilder kan även ha andra syften som är outtalade, menar Flyghed. Sådana syften kan vara att avleda uppmärksamhet från en känsligare fråga, att verka identitetsskapande genom att skapa uppslutning mot en gemensam fiende eller för att legitimera en organisations existens eller krav på ökade resurser.[144] Samtidigt saknas ofta underlag för hotbilden existens och de nya metodernas

[141] Ramberg (2007) s. 156–157.
[142] Ramberg (2007) s. 169–170.
[143] Flyghed (2015) s. 55.
[144] Flyghed (2007) s. 60–61.

effektivitet. Flyghed menar att även om nya exceptionella åtgärder införs med hänvisning till hotbilder som ”terrorism”, så stannar det sällan där, de nya metoderna normaliseras och tillämpningsområdet utvidgas till att omfatta andra, lindrigare, typer av brott.[145] Detta har Flyghed kallat ”normalisering av det exceptionella” och mer specifik av undertypen ”medelnormalisering”, vilket innebär normalisering och utvidgning av metodernas tillämpningsområde. En annan form av medelnormalisering är att lagstiftaren, när det står klart att brottsbekämpande myndigheters tillämpning av en tvångsmedelsbestämmelse befinner sig i gråzonen för vad som är tillåtet, i efterhand ändrar lagstiftningen så att myndigheternas tillämpning blir uttryckligen laglig.[146]

Den andra typen av ”normalisering av det exceptionella” är ”hotbildsnormalisering”. Hotbildsnormalisering innebär att samhället uppfattas befinna sig i ett tillstånd av konstant kris. Detta är en konsekvens av att en hotbild, med svagt empiriskt stöd, accepterats som sanning, och detta legitimerar i sin tur att repressionsnivån ständigt ökar.[147] Ovanliga och skrämmande händelser, som är långt ifrån representativa för brottsligheten i stort, utnyttjas på detta sätt för att måla upp en bild av att de är konstant närvarande faror och att samhället är i kris. Vidare sker en polarisering, vilket innebär att människor mentalt delar upp sig själva och andra människor i ”vi vanliga” som ska skyddas och de där andra, de ”onda”, terroristerna och de grova brottslingarna.[148]

Ett argument som ofta används av övervakningsanhängare är att det enbart är de ”onda”, de som inte har ”rent mjöl i påsen”, som behöver oroa sig över övervakning. Detta argument leder tanken på fel väg och strider mot rättsstatliga principer, menar Flyghed. Detta eftersom det blir som att alla medborgare åläggs en börda att bevisa sin oskuld för staten genom att acceptera att bli övervakade. Flyghed menar att frågan därför är om ”vi vill att övervakarnas smutsiga fingrar ska få peta i vårt rena mjöl”.[149] Likaså förkastar Flyghed argumentet att myndigheter inte kan utnyttja information de har möjlighet att samla in p.g.a. resursbrist, och menar att det i dagens läge inte är något problem att lagra samt, vid behov, söka igenom och sammanställa stora mängder data individer.[150]

[145] Flyghed (2015) s. 59.
[146] Flyghed (2007) s. 64.
[147] Flyghed (2007) s. 63–64.
[148] Flyghed (2007) s. 66.
[149] Flyghed (2015) s. 67.
[150] Flyghed (2015) s. 57.

En ytterligare förklaring till att övervakningen ständigt expanderar trots det magra empiriska stödet handlar enligt Flyghed om fem centrala aktörers interna och externa rationalitet.[151] Politikers externa rationalitet är att med hjälp av ny lagstiftning bekämpa brott, men den interna rationaliteten handlar om att visa handlingskraft och lugna allmänheten. Polisens uttalade syfte handlar även det om att bekämpa brott, medan den interna rationaliteten för att kräva ökad övervakning är att legitimera organisationen, tilldelas mer resurser och utöka verksamheten. För de tre kvarvarande aktörerna, den privata kontrollindustrin, medierna och experterna, är förenklat den interna rationaliteten profit genom försäljning av teknik, lösnummer respektive karriärgynnande citeringar. Detta under förevändning att erbjuda öka trygghet genom teknologi, förmedla information respektive bistå med kunskap.[152]

5.2.5 Processrättsprofessorns perspektiv

Torleif Bylund, professor emeritus i processrätt, menar att det är osannolikt att brottsbekämpande myndigheter aldrig skulle missbruka tvångsmedel och pekar på att Säkerhetspolisen under lång tid missbrukade tillstånd till teleavlyssning (dvs. HAEK i dagens terminologi). Missbruket bestod i att kartlägga och övervaka medlemmar i vissa politiska partier och organisationer under lång tid utan att förundersökningen gällande det brott, t.ex. olovlig kårverksamhet, som angetts som grund för avlyssning fördes framåt.[153] Ett annat exempel är att signalspaning i eter använts, med hänvisning till att ”etern är fri” och utan föregående domstolsbeslut, för att avlyssna samtal mellan mobiltelefoner när dessa överförts radioburet istället för i ledning.[154]

[151] Flyghed (2007) s. 66; Flyghed (2015) s. 59.
[152] Flyghed (2015) s. 59–61.
[153] Ekelöf, Bylund och Edelstam (2006) s. 101–102.
[154] Ekelöf, Bylund och Edelstam (2006) s. 89.

6 Användning och nytta av hemliga tvångsmedel

Myndigheterna lämnar varje år en redovisning över föregående års användning av hemliga tvångsmedel till regeringen som sammanställer uppgifterna och redovisar dem i en skrivelse i slutet av året. Åklagarmyndigheten har tidigare redovisat användning av HAEK, HÖEK och hemlig kameraövervakning för varje år. Enligt den senaste lydelsen av uppdraget så ska Åklagarmyndigheten även redovisa tvångsmedelsanvändning enligt 2007 års preventivlag och användningen av hemlig rumsavlyssning. Med undantag för siffrorna gällande 2007 års preventivlag, där det inte går att skilja ut de olika tvångsmedlen, så kommer här endast att återges siffrorna över användningen av HAEK och HÖEK samt inhämtning enligt 2012 års inhämtningslag. I Åklagarmyndighetens uppdrag ingår däremot inte att redovisa i vilken omfattning Säkerhetspolisen använt tvångsmedel, uppgiften är endast att redovisa Åklagarmyndighetens, Polismyndighetens, Ekobrottsmyndighetens och Tullverkets tvångsmedelsanvändning.[155] Säkerhetspolisens användning av hemliga tvångsmedel inkluderas inte heller i regeringens skrivelser gällande tvångsmedelsanvändningen.[156] I olika förarbeten kan det dock finnas redogörelser för tillämpningen av bestämmelserna, t.ex. i SOU 2012:44, där det även finns en redogörelse för Säkerhetspolisens användning.

6.1 Regeringens och Åklagarmyndighetens redovisningar

Det är svårt att få en klar bild av utvecklingen över tid, vilket dels är på grund av att lagstiftningen har ändrats under tiden, dels att direktiven för vad som ska redovisas och hur detta ska göras har ändrats ett flertal gånger. Begreppet tillstånd har t.ex. ändrats inför redovisningen av användning av tvångsmedel under år 2011. Tidigare kunde ett tillstånd avse flera adresser, medan numera registreras varje adress som är föremål för HAEK eller HÖEK som ett separat tillstånd i statistiken.[157]

[155] Åklagarmyndigheten (2015) s. 1.
[156] Skr. 2013/14:60 s. 1; Skr. 2014/15:36 s. 1.
[157] Skr. 2012/13:47 s. 10.

I regeringens skrivelse 2013/14:60 anges det att p.g.a. att lagstiftningen har ändrats så att uppgifter som tidigare kunde hämtas utan domstolsbeslut numera kräver domstolsbeslut, så är det svårt att göra en rättvisande jämförelse med tidigare år. Av det skälet har regeringen inte redovisat föregående års siffror i denna skrivelse.[158] Detta är en skillnad mot tidigare år då regeringen har redogjort för utvecklingen av antalet tillstånd och den genomsnittliga avlyssnings- och övervakningstiden. I skrivelse 2011/12:39 finns t.ex. en redogörelse för den kraftiga ökningen av antalet tillstånd under åren 2001–2010.[159] På grund av de ovan nämnda problemen, samt utrymmesskäl, kommer redogörelsen nedan framförallt att gälla åren 2014, 2013 och 2012.

6.1.1 Användningen av HAEK

År 2012 meddelades 3 432 tillstånd till HAEK, vilket innebar en minskning från år 2011 då antalet tillstånd som meddelades var 4 199 stycken. Däremot ökade totala avlyssningstiden från 138 886 dagar under år 2011 till 147 211 dagar år 2012. Endast ett fåtal ansökningar (9 stycken) avslogs av domstol år 2012. Huvuddelen av tillstånden för HAEK avsåg ”narkotikabrott/smuggling” (77 %), medan våldsbrott (10 %) var näst vanligaste angivna skäl år 2012.[160] Både antalet tillstånd som meddelades år 2013 (3 384 tillstånd) och total avlyssningstid (120 926 dagar) minskade jämfört med år 2012. Något fler ansökningar avslogs (11 stycken) år 2013 än år 2012. Narkotikabrott/smuggling var liksom föregående år det vanligaste skälet till tillstånd, dock minskade andelen något (69 %).[161]

Enligt Åklagarmyndighetens redovisning för år 2014 så har antalet tillstånd till HAEK ökat till 3 564 tillstånd sedan föregående år, samtidigt som avslagen även ökat något (13 avslag under år 2014). Vanligaste brottsmisstanken som låg till grund för beslutet var även detta år narkotikabrott/smuggling, 64 % av tillstånden avsåg dessa brott.[162] I Åklagarmyndighetens redogörelse för användningen av hemliga tvångsmedel år 2014 har den totala avlyssningstiden inte redovisats.

[158] Skr. 2013/14:60 s. 12–13.
[159] Skr. 2011/12:39 s. 10–14
[160] Skr. 2013/14:60 s. 13–14.
[161] Skr. 2014/15:36 s. 14.
[162] Åklagarmyndigheten (2015) s. 3–4.

Antalet personer som varit föremål för HAEK har legat relativt konstant under de tre åren det finns uppgifter om detta, dock en liten minskning från 1 268 personer år 2012 till 1 235 personer år 2014.[163] Den genomsnittliga avlyssningstiden per tillstånd har varierat mellan 43–36 dagar under perioden 2012–2014. Den längsta avlyssningstiden ett tillstånd varit giltigt har sjunkit från 338 dagar år 2012 till 286 dagar år 2014.[164]

6.1.2 Användningen av HÖEK

Av redovisningen framgår att domstol meddelade 4 095 tillstånd till HÖEK år 2012, jämfört med 1 238 år 2011.[165] Ett tillstånd till HAEK brukade regelmässigt förenas med ett tillstånd till HÖEK, men de 1 238 tillstånd som meddelades år 2011 inkluderar enbart de tillstånd som inte meddelades i samband med HAEK.[166] Siffrorna går enligt regeringen trots det inte att jämföra med siffror från tidigare år, vilket regeringen menar beror på ändring av begreppet tillstånd år 2011 och ändringar år 2012 av vad som omfattades av HÖEK. Sedan år 2012 ingår nämligen basstationstömning i HÖEK och ett tillstånd från domstol krävs därför för att få ut dessa uppgifter. Ändringen innebär även att HÖEK kan användas innan det finns en skäligen misstänkt person.[167] Trots detta meddelades färre tillstånd (3 935 tillstånd) år 2013 jämfört med året innan, vilket myndigheterna menar kan bero på att ett tillstånd till HAEK numera även ger rätt att vidta åtgärder som innefattas i HÖEK. Därför behövs inte ett separat tillstånd till HÖEK längre för att t.ex. ta reda på vilka telefonnummer som används av en misstänkt.[168] Åklagarmyndighetens redovisning för år 2014 visar dock att antalet tillstånd återigen har gått upp, år 2014 meddelades 4 398 tillstånd till HÖEK.[169]

Den vanligaste anledningen till att tillstånd till HÖEK meddelades under år 2012 var, liksom vid HAEK, ”narkotikabrott/smuggling” (48 %). Efter narkotikabrott var våldsbrott (24 %) och tillgreppsbrott (15 %) de vanligaste anledningarna till tillstånd.[170] Detta innebär en skillnad jämfört med tidigare år då det vanligaste tillämpningsområdet

[163] Skr. 2014/15:36 s. 14; Åklagarmyndigheten (2015) s. 3.
[164] Skr. 2014/15:36 s. 14–15; Åklagarmyndigheten (2015) s. 4.
[165] Skr. 2013/14:60 s. 14–15.
[166] Skr. 2012/13:47 s. 13.
[167] Skr. 2013/14:60 s. 11–13.
[168] Skr. 2014/15:36 s. 16, 22.
[169] Åklagarmyndigheten (2015) s. 3.
[170] Skr. 2013/14:60 s. 14–15.

för HÖEK varit tillgreppsbrottslighet. Att narkotikabrott var vanligast även vid användning av HÖEK år 2012 kan enligt myndigheterna bero på att telefonlistor som är mycket viktiga vid utredningar av narkotikabrott tidigare kunnat inhämtas med stöd av LEK, medan det efter lagändringen krävts beslut om HÖEK enligt RB för att åtkomma informationen.[171] Under år 2013 minskade emellertid andelen tillstånd som avsåg narkotikabrott/smuggling till 27 %, och våldsbrott blev återigen det vanligaste skälet för tillstånd till HÖEK (41 %).[172] Utifrån siffrorna för år 2014 kan man dock utläsa att detta förhållande förändrats återigen. Narkotikabrott/smuggling angavs som skälet till 32 % av tillstånden och var därmed med minsta möjliga marginal den vanligaste grunden till tillstånd år 2014 (1 421 tillstånd avseende narkotikabrott jämfört med 1 420 tillstånd avseende våldsbrott).[173]

Uppgifter om längsta övervakningstid, total övervakningstid och genomsnittlig övervakningstid anges inte sedan år 2012 då HÖEK utvidgades till att även omfatta basstationstömning, eftersom det skulle vara missvisande enligt myndigheterna.[174] Av redovisningarna från tidigare år kan man dock utläsa att den längsta varaktigheten för ett enskilt tillstånd till HÖEK år 2011 varit 300 dagar, medan motsvarande siffra år 2010 varit hela 1 095 dagar (inklusive retroaktiv inhämtning av övervakningsuppgifter).[175]

6.1.3 Användning utifrån 2007 års preventivlag

Av Åklagarmyndighetens redovisning framgår det att ingen tvångsmedelsanvändning enligt 2007 års lag som ska redovisas förekommit under år 2014, men som ovan angetts så ska inte Säkerhetspolisens användning ingå i den redovisning som lämnas av Åklagarmyndigheten.[176] I SOU 2012:44 redovisas dock både Polismyndighetens och Säkerhetspolisens användning av hemliga tvångsmedel enligt 2007 års preventivlag under perioden 2008–2011. Under perioden 2008–2011 beviljades Polismyndigheten totalt 11 tillstånd enligt 2007 års preventivlag. Åtta av dessa tillstånd avsåg HAEK i kombination med HÖEK, ett tillstånd enbart HÖEK och två tillstånd avsåg hemlig

[171] Skr. 2013/14:60 s. 19.
[172] Skr. 2014/15:36 s. 16.
[173] Åklagarmyndigheten (2015) s. 3.
[174] Skr. 2013/14:60 s. 15.
[175] Åklagarmyndigheten (2012) s. 6; Åklagarmyndigheten (2011) s. 6.
[176] Åklagarmyndigheten (2015) s. 1–2.

kameraövervakning. Inget tillstånd avsåg hemlig postkontroll. Alla tillstånd utom ett meddelades med hänvisning till dåvarande 1 § 1 st. 6[177], dvs. s.k. systemhotande brottslighet vilket innebär exempelvis mord eller en grov misshandel i syfte att påverka eller hämnas på ett offentligt organ eller en journalist.[178]

Säkerhetspolisen beviljades under perioden totalt 132 tillstånd, även här var HAEK i kombination med HÖEK vanligast (107 tillstånd). Näst vanligaste typen av tillstånd var HÖEK (19 tillstånd), följt av hemlig kameraövervakning (6 tillstånd). I likhet med uppgifterna gällande Polismyndigheten så meddelandes inget tillstånd till hemlig postkontroll. Till skillnad från tillstånden som beviljades Polismyndigheten så var inte systemhotande brottslighet det vanligaste skälet till att Säkerhetspolisen beviljades tillstånd. Istället var det vanligast att tillstånd beviljades med hänsyn till dåvarande 1 § 1 st. 5[179], dvs. terroristrelaterade brott m.m. (54 tillstånd), därefter med stöd av 1 § 1 st. 3., dvs. p.g.a. högmålsbrott såsom uppror m.m. (42 tillstånd) och först därefter p.g.a. systemhotande brottslighet med stöd av dåvarande 1 § 1 st. 6 (25 tillstånd).[180]

6.1.4 Beslut enligt 2012 års inhämtningslag

Polismyndigheten och Tullverket fattade 647 inhämtningsbeslut med stöd av 2012 års inhämtningslag under 2014. Av Polismyndighetens beslut gällde 80,8 % av ärendena grovt narkotikabrott, medan det näst vanligaste skälet var grovt rån (11,6 %). Samtliga 121 fall som Tullverket beslutade om inhämtning i gällde grov narkotikasmuggling.[181] År 2013 var motsvarande siffror totalt 595 beslut, 82 % av Polismyndighetens beslut gällde grovt narkotikabrott och alla 42 beslut som fattades av Tullverket gällde grov narkotikasmuggling.[182] Antalet beslut om inhämtning för perioden från lagens ikraftträdande 1 juli 2012 till utgången av år 2012, var 369 stycken. Av de beslut som Polismyndigheten fattade var 82 % hänförliga till grovt narkotikabrott medan samtliga 36 beslut som fattades av Tullverket gällde grov narkotikasmuggling.[183]

[177] Sedan 1 januari 2015 regleras detta istället i 1 § 1 st. 7, se SFS 2014:1421.
[178] SOU 2012:44 s. 316.
[179] Sedan 1 januari 2015 regleras detta istället i 1 § 1 st. 6, se SFS 2014:1421.
[180] SOU 2012:44 s. 317–318.
[181] Åklagarmyndigheten (2015) s. 12–13.
[182] Åklagarmyndigheten (2014) s. 12–13
[183] Åklagarmyndigheten (2013) s. 12–13.

6.2 Bedömningen av nytta av tvångsmedlen

Det är svårt att redogöra för och bedöma nyttan av hemliga tvångsmedel utifrån redovisningarna. Detta beror på att det inte är lätt för åklagare att bedöma nyttan av hemliga tvångsmedel, och att det inte heller är helt lätt att förstå redovisningarna. Åklagarmyndigheten redogör dels för de så kallade särskilda nyttorna, dels för nyttan i utredningen i förhållande till en misstänkt som varit utsatt för tvångsmedel.[184] Vidare har även definitionen av nytta ändrats över tid.[185]

6.2.1 Nytta av HAEK och HÖEK

Enligt redovisningen för år 2014 har åklagare uppskattat att HAEK varit till nytta i utredningen av 65 % av de 1 235 misstänkta som varit föremål för HAEK under det året. Vanligaste nyttan var att misstankarna mot den misstänkte stärkts.[186] Gällande år 2013 uppskattade åklagarna att HAEK varit till nytta gällande 63 % av de 1 251 misstänkta personerna, respektive 73 % av de 1 268 misstänkta personerna år 2012. Även år 2013 var den vanligaste nyttan att avlyssningen hade stärkt misstankarna mot den misstänkte, medan den vanligaste nyttan[187] år 2012 uppgavs vara att avlyssningen fungerat som spaningshjälpmedel.[188]

I skrivelsen 2013/14:60 anges att nyttan av HÖEK framöver inte ska redovisas genom uppskattning av hur stor andel av tillstånden som varit till nytta, utan istället ska nyttan av HÖEK redovisas genom typexempel.[189] Skälen som anges är att det är för resurskrävande för åklagarna att bedöma, och att det är svårt att redovisa nyttan i förhållande till någon person eftersom HÖEK sedan år 2012 även innefattar basstationstömning samt får användas innan någon person är skäligen misstänkt.[190] Typfallen som valts är enligt Åklagarmyndigheten anonymiserade fall där åtminstone en tingsrättsdom meddelats. Dessa typexempel är avsedda att illustrera vilken nytta de

[184] Se t.ex. Skr. 2014/15:36 s. 15.
[185] SOU 2012:44 s. 259–260.
[186] Åklagarmyndigheten (2015) s. 9–10.
[187] Det måste dock påpekas att kategorierna av typerna av nytta förändrats, spaningshjälpmedel fanns inte som kategori 2013–2014 och stärka misstankar fanns inte som kategori år 2012.
[188] Skr. 2014/15:36 s. 15 och Skr. 2013/14:60 s. 14.
[189] Skr. 2013/14:60 s. 15.
[190] Skr. 2012/13:47 s. 23.

brottsbekämpande myndigheterna har av det hemliga tvångsmedlet.[191] Gällande år 2014 redovisade Åklagarmyndigheten två typfall där HÖEK varit till nytta, ett fall gällande två grova bedrägerier och ett fall gällande försökt till mord, rån och grovt rån.[192] I redovisningen av användning under år 2014 som Åklagarmyndigheten lämnat till regeringen har dock fortfarande åklagarnas nyttobedömningar redovisats. Den andelen av de 2 022 misstänkta för vilket HÖEK enligt åklagares uppskattning varit till nytta år 2014 var 74 %.[193] Åklagarnas uppskattningar för år 2013 var att det varit till nytta gällande 69 % av de 2 381 misstänkta det året och gällande 62 % av de misstänkta år 2012.[194]

6.2.2 Nytta av tvångsmedel enligt 2007 års preventivlag

Av redogörelsen i Utredningen av vissa hemliga tvångsmedel framgår det att Polismyndigheten uppgett att endast vid ett av de åtta fall som tillstånd till tvångsmedel enligt 2007 års preventivlag hade beviljats så hade tvångsmedlet medfört nytta.[195] Till större nytta var Säkerhetspolisens tvångsmedelsanvändning, i 71 % av fallen där tvångsmedelsanvändning enligt 2007 års preventivlag använts så ledde detta till någon av former av nytta. Emellertid framgår även att den enda nyttan i ett betydande antal fall (50 fall) varit ”att det inte längre funnits anledning att anta att [den] person som tillståndet avser ska komma att utöva sådan brottslig verksamhet som tillståndet omfattar”. Om denna form av nytta räknas bort så var tvångsmedelsanvändningen till nytta i 44 fall, vilket motsvarar 33 % av det totala antalet tillstånd som Säkerhetspolisen beviljades. Näst vanligast var att tvångsmedlet innebar ”annan effekt av betydelse för att förhindra brott” (18 % av tillstånden), vilket av myndigheten förtydligades till att innebära kartläggning av den misstänkte eller en grupp den misstänka tillhörde. Endast i tre fall (2 % av tillstånden) ledde tvångsmedlet till ”att brottslig verksamhet som tillstånd i ärendet avse[tt] kunnat förhindras”.[196]

[191] Åklagarmyndigheten (2015) s. 4.
[192] Åklagarmyndigheten (2015) s. 8.
[193] Åklagarmyndigheten (2015) s. 10.
[194] Åklagarmyndigheten (2014) s. 6.
[195] SOU 2012:44 s. 322.
[196] SOU 2012:44 s. 322–323.

6.2.3 Nytta av inhämtning enligt 2012 års inhämtningslag

Ifråga om nyttan av inhämtning enligt 2012 års inhämtningslag så redovisas enbart anonymiserade exempel, och dessa anonymiserade exempel behöver inte ha lett till en dom. Av de femton anonymiserade exempel som redovisats så är det bara i ett fall som misstankarna visat sig vara ogrundade, enligt redovisningen.[197] I redovisningen anges att den typiska nyttan varit att hantering av stora mängder narkotika kunnat upptäckas och att nätverk kunnat kartläggas, vilket lett till att förundersökningar kunnat inledas eller brottsmisstankar verifieras. I redovisningen menas vidare att 2012 års inhämtningslag varit ”avgörande för att inleda förundersökning avseende en lång rad grova brott”.[198]

[197] Åklagarmyndigheten (2015) s. 13–16.
[198] Åklagarmyndigheten (2015) s. 13–14.

7 Hemlig avlyssning och övervakning av elektronisk kommunikation

Hemlig avlyssning av elektronisk kommunikation (HAEK) innebär förenklat uttryckt att innehållet i ett meddelande som skickats eller skickas i ett elektroniskt kommunikationsnät avlyssnas och sparas. Hemlig övervakning av elektronisk kommunikation (HÖEK) innebär istället bl.a. övervakning av mellan vilka elektroniska kommunikationsutrustningar (t.ex. mobiltelefoner) som meddelande skickas och var en viss kommunikationsutrustning befinner sig geografiskt.

Benämningen på tvångsmedlen var tidigare hemlig teleavlyssning respektive hemlig teleövervakning, men i samband med att prefixet ”tele” togs bort från det i paragraferna tidigare använda begreppen ”teleadress”, ”telenät” och ”telemeddelande” så ansågs det lämpligt att även ändra benämningen på tvångsmedlen.[199] Skälet till att prefixet ”tele” togs bort från begreppen var att det ansågs eftersträvansvärt att ha samma begrepp i 27 kap. RB som i LEK, samt att de ansågs lämpligt att använda mer generella och teknikneutrala begrepp för att lagstiftningen inte skulle bli föråldrad allt för fort som en konsekvens av den snabba teknikutvecklingen.[200] Redan de tidigare bestämmelserna ansågs dock av Beredningen för rättsväsendets utveckling (BRU) vara teknikneutrala eftersom de i utredningens mening var tillämpbara oavsett vilken teknik som används för att överföra meddelandet.[201]

Regleringen av hemliga tvångsmedel, såsom HAEK och HÖEK, återfinns framförallt i 27 kap. RB, men som redogjorts för i avsnitt 4.4 så finns även avvikande regleringar i särskilda lagar såsom 2012 års inhämtningslag och 2007 års preventivlag. Tidigare reglerades även hemlig rumsavlyssning och hemliga tvångsmedel vid förundersökningar gällande ”samhällsfarliga brott” i särskilda tidsbegränsade lagar, men bestämmelserna är sedan 2015 permanentade genom att de införts i 27 kap. RB.[202]

[199] Prop. 2011/12:55 s. 63.
[200] Prop. 2011/12:55 s. 57.
[201] SOU 2005:38 s. 279.
[202] Hemlig rumsavlyssning regleras sedan år 2015 i 27 kap. RB, se särskilt 27:20d. Tidigare reglerades detta tvångsmedel i lagen (2007:978) om hemlig rumsavlyssning. Se avsnitt 4.4.

7.1 Meddelande som kan avlyssnas

Hemlig avlyssning av elektronisk kommunikation innebär enligt 27:18 att meddelande avlyssnas eller tas upp med hjälp av ett tekniskt hjälpmedel för återgivning av innehållet. Meddelandet ska skickas eller ha skickats i ett elektroniskt kommunikationsnät till ett telefonnummer eller annan adress. Som nämnts ovan så användes tidigare andra begrepp för att avgränsa vilka meddelade som kunde avlyssnas eller övervakas, nämligen ”telemeddelande”, ”teleadress” och ”telenät”. Dessa begrepp har ersatts av begreppen ”meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts”, ”adress” och ”elektroniskt kommunikationsnät”.[203]

7.1.1 Meddelande

Enligt nu gällande lydelse är det ”meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts” som kan avlyssnas eller övervakas genom HAEK och HÖEK. Avsikten när detta begrepp ersatte det tidigare begreppet ”telemeddelande” var inte att utvidga tillämpningsområdet för tvångsmedlet utan att begreppen i RB skulle stämma bättre överens med begreppen i LEK. Samtidigt ansågs begreppet ”telemeddelande” inte kunna ersättas med begreppet ”elektroniskt meddelande” som används i LEK.[204]

Enligt förarbetena kan ”alla former av kommunikation genom elektroniska kommunikationsnät”, skriftlig eller muntlig, omfattas av avlyssning. Exempel på kommunikationssätt som enligt förarbetena omfattas är elektronisk post, SMS och telefax.[205] Regleringen är därmed tillämplig även på datakommunikation. Ett tillstånd till HÖEK kan därför, enligt förarbetena, innebära att uppgifter om mellan vilka e-postadresser ett meddelande har skickats samt uppgifter om t.ex. vilka webbsidor som en abonnent besökt kan inhämtas.[206]

[203] Prop. 2011/12:55 s. 58–62.
[204] Prop. 2011/12:55 s. 57–59.
[205] SOU 2012:44 s. 119.
[206] SOU 2012:44 s. 119; prop. 2011/12:55 s. 48.

7.1.2 Överförts i ett elektroniskt kommunikationsnät

För att ett meddelande ska kunna vara avlyssnas (eller övervakas) måste meddelandet överföras eller ha överförts genom ett elektroniskt kommunikationsnät (27:18 1 st. och 27:19 1 st. 1). Begreppet elektroniskt kommunikationsnät i RB är enligt förarbeten avsett att ha samma innebörd som i 1:7 LEK.[207] I de flesta fall verkställs HAEK eller HÖEK i ett elektroniskt kommunikationsnät som är allmänt tillgängligt (ATEK-nät), men ett beslut om HAEK eller HÖEK kan även verkställas utanför ett ATEK-nät, såvida nätet inte är ”av mindre betydelse från allmän kommunikationssynpunkt” (se 27:21 3 st. andra meningen och 27:20 3 st.). Detta innebär enligt förarbetena att bl.a. porttelefoner, hörselslingor, kommunikation inom en bostads interna nätverk samt mindre interna företagsnätverk ska vara undantagna från avlyssning eftersom de utgör elektroniska kommunikationsnät av mindre betydelse. Avlyssning är däremot tillåten när en adress inom nätverket används för att kommunicera via ett allmänt tillgängligt nät eller inom ett större företagsnät.[208]

7.1.3 Adress

Begreppet ”adress” innefattar, i likhet med det tidigare använda begreppet ”teleadress”, enligt regeringen ”olika typer av nummer, t.ex. telefonnummer och andra identifikationsnummer och adresser, t.ex. e-postadresser”.[209] Både IMEI-nummer (International Mobile Equipment Identity) och IMSI-nummer (International Mobile Subscriber Identity) är att betrakta som adresser enligt förarbetena. Ett IMEI-nummer är ett unikt nummer som är kopplat till hårdvaran i telefonen medan ett IMSI-nummer är kopplat till ett SIM-kort som används i en mobiltelefon.[210] Viss oklarhet verkar dock råda ifråga om ett IMEI-nummer även kan betraktas som en adress.[211]

[207] Prop. 2011/12:55 s. 127.
[208] Prop. 1994/95:227 s. 27, 31; alternativt SOU 2007:76 s. 60–61.
[209] Prop. 2011/12:55 s. 62.
[210] SOU 2010:103 s. 295; SOU 2015:31 s. 262.
[211] Prop. 2011/12:55 s. 62.

7.2 Typer av hemlig övervakning av elektronisk kommunikation

I tvångsmedlet hemlig övervakning av elektronisk kommunikation (HÖEK) inkluderas tre typer av förfarande. Den första typen är uppgifter gällande ”meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress” (27:19 1 st. 1). Sedan juli 2012 innefattas ytterligare två typer av förfaranden i tvångsmedlet, s.k. ”basstationstömning” (27:19 1 st. 2), samt lokalisering av en elektronisk kommunikationsutrustning (27:19 1 st. 3).

7.2.1 Basstationstömning

En basstationstömning innebär att uppgifter inhämtas om vilka kommunikationsutrustningar, t.ex. mobiltelefoner, som har funnits inom ett visst geografiskt område.[212] Innan juli 2012 kunde dessa uppgifter istället inhämtas med stöd av 6:22 1 st. 3 LEK (i sin tidigare lydelse), eftersom dessa uppgifter ansågs vara uppgifter som angick särskilda meddelande (se 6:20 1 st. 3 LEK). Inhämtningen enligt 6:22 1 st. 3 LEK var dock begränsad till uppgifter som genererats i samband med kommunikation, och kunde därför inte avse sådana uppgifter som genererats av att en utrustning varit i kontakt med en basstation, när detta inte skett i samband med kommunikation.[213] Såsom basstationstömning regleras i RB är det möjligt att inhämta lokaliseringsuppgifter trots att utrustningen vid tillfället inte används för kommunikation.[214]

Lydelsen i propositionen till lagändringen är dock svårförstådd samtidigt som den ofta nästan ordagrant och utan vidare förklaring återges i doktrin.[215]

> ”Uppgifter kan hämtas in dels om vilka kommunikationsutrustningar som har funnits inom ett visst geografiskt område (s.k. basstationstömning), dels om inom vilket område en viss sådan utrustning finns eller har funnits. Inhämtning av lokaliseringsuppgifter får ske även om utrustningens identifikationsnummer är okänt. Som framgår av 20 § första stycket kan inhämtningen avse ett telefonnummer eller annan adress. På samma sätt ska en basstationstömning kunna ge upplysningar om telefonnumret till ett kontantkort som använts i en mobiltelefon som befunnit sig på den aktuella platsen.” [216]

[212] Prop. 2011/12:55 s. 128.
[213] Prop. 2011/12:55 s. 96.
[214] Prop. 2011/12:55 s. 128.
[215] Se t.ex. Westerlund (2013) s. 161.
[216] Citat prop. 2011/12:55 s. 128.

Hänvisningen till 20 § 1 st. betyder troligtvis att en utrustnings identifikationsnummer inte behövs, om det istället finns ett telefonnummer eller en liknande adress. När en basstationstömning görs är det rimligtvis en basstations identifikationsnummer eller adress som krävs, och inte en mobiltelefons identifikationsnummer eller ett telefonnummer. Att det anges att en basstationstömning ”[p]å samma sätt ska […] kunna ge upplysningar om telefonnumret till ett kontantkort” får troligtvis tolkas som att en basstationstömning kan ge uppgifter om telefonnumret till ett abonnemang likväl som ett kontantkort. Vad som menas med en utrustnings identifikationsnummer anges inte uttryckligen, men däremot anges på annat ställe att ett IMEI-nummer är ”ett unikt nummer som identifierar utrustningen eller hårdvaran”, även om det ibland också anses vara en adress.[217] Ur ett tekniskt perspektiv är det möjligt att även andra unika nummer och adresser kan betraktas som identifikationsnummer, t.ex. MAC-adresser (media access control adress).

7.2.2 Lokalisering av en viss elektronisk kommunikationsutrustning

Till skillnad mot vad som gäller vid en basstationstömning, så är det vid lokalisering av en viss elektronisk kommunikationsutrustning (27:19 1 st. 3) möjligt att inhämta både historiska lokaliseringsuppgifter och lokaliseringsuppgifter i realtid. Enligt regeringen var ett skäl att det var angeläget för de brottsbekämpande myndigheterna att kunna följa t.ex. en telefon i en flyktbil i realtid och ett annat skäl att tillgången till historiska lokaliseringsuppgifter antogs vara starkt begränsad.[218]

7.3 Förutsättningar för tillstånd

Beslut om tillstånd till HAEK eller HÖEK fattas som huvudregel av rätten efter ansökan av åklagaren (27:21 1 st.). Om det skulle innebära ett väsentligt dröjsmål att inhämta beslut av rätten, så har en åklagare möjlighet att ta ett tillfälligt beslut i avvaktan på rättens beslut (27:21a 1 st.). Sedan januari 2015 har åklagaren denna möjlighet inte enbart ifråga om HÖEK, utan även ifråga om HAEK och hemlig kameraövervakning.[219]

[217] Prop. 2011/12:55 s. 62.
[218] Prop. 2011/12:55 s. 98.
[219] SFS 2014:1419.

För att ett tillstånd till HAEK eller HÖEK ska kunna meddelas så måste åtgärden vara proportionerlig, dvs. skälen för åtgärden måste uppväga det intrång som åtgärden innebär för den misstänkta eller annan person (jfr 27:1 1 st.). Bylund menar emellertid att proportionalitetsprincipen i själva verket innebär ett minimalt skydd för tredjemansintressen, och att detta skydd inte fungerar i praktiken p.g.a. svårigheten att avskilja de för utredningen relevanta samtalen som förs av en misstänkt från en misstänkts övriga samtal samt från samtal som andra människor för via samma kommunikationsenhet (t.ex. fast telefon i bostad).[220]

7.3.1 Typ av brott

För att tillstånd till HÖEK respektive HAEK ska kunna meddelas ska förundersökningen avse ett sådant brott som, enligt 19 § 3 st. respektive 18 § 2 st., medger att HÖEK och HAEK kan användas. För att tillstånd till HÖEK ska medges ska brottet vara sådant att lindrigaste föreskrivna straff är fängelse i sex månader, brottet är ett av de uppräknade brotten, dvs. bl.a. narkotikabrott, eller en osjälvständiga form av ett sådant brott. HAEK får användas för att utreda brott där det lindrigaste föreskrivna straff är två års fängelse, osjälvständiga former eller där det kan antas att brottets straffvärde överstiger fängelse i två år (den s.k. straffvärdesventilen).[221] Sedan år 2015 kan HÖEK och HAEK även användas vid förundersökningar gällande de samhällsfarligabrott som anges i 27:2 (se avsnitt 4.4.3).[222]

7.3.2 Synnerlig vikt

För att tillstånd ska ges krävs att åtgärden är av synnerlig vikt för utredningen. Detta betyder inte att åtgärden måste vara av avgörande betydelse, men att den ska vara av verklig betydelse för utredningen. Bylund menar att det krävs att andra, förvisso mer resurskrävande åtgärder, men mindre integritetskränkande åtgärder, som t.ex. skuggning och övervakning inte bedömts som tillräckliga för att detta krav ska vara uppfyllt.[223]

[220] Ekelöf, Bylund och Edelstam (2006) s. 99.
[221] Westerlund (2013) s. 157.
[222] SFS 2014:1419.
[223] Ekelöf, Bylund och Edelstam (2006) s. 91.

Om det finns en skäligen misstänkt person så kan HÖEK och HAEK avse en elektronisk kommunikationsutrustning som det kan antas att den misstänkte kommer att använda, alternativt en som det finns ”synnerlig anledning att anta” att den misstänkte har eller kommer att kontakta (se 27:20 1 st.). HÖEK får enligt 20 § 2 st. även användas i syfte att utreda vem som kan misstänkas för ett brott. Det krävs då enligt 19 § 4 st. att förundersökningen avser ett sådant brott som anges 18 § 2 st., vilket innebär att straffvärdesventilen i 18 § 2 st. 3 blir tillämplig.[224] HÖEK kan enligt bestämmelsen användas när det inte finns någon skäligen misstänkt, men får enligt förarbetena även användas när det finns en skäligen misstänkt, om det sker i syfte att identifiera ytterligare personer som kan misstänkas för brott.[225] När HÖEK används i syftet är att utreda vem som kan misstänkas för brott så får uppgifter om meddelande endast avse förfluten tid, däremot får uppgifter om lokalisering av en viss kommunikationsutrustning avse både realtid och förfluten tid.[226]

[224] Prop. 2013/14:237 s. 78–79.
[225] Prop. 2011/12:55 s. 129.
[226] Prop. 2011/12:55 s. 98.

8 Operatörers skyldigheter enligt lagen om elektronisk kommunikation

Marknaden för elektronisk kommunikation regleras av *lagen (2003:389) om elektronisk kommunikation* (LEK). Elektronisk kommunikation innefattar överföring av elektroniska signaler genom telefoni, datakommunikation samt radio- och tv-utsändningar till allmänheten.[227] Samtidigt som LEK trädde i kraft så upphörde *Telelagen (1993:597)* (TL) att gälla och ett antal EG-direktiv, bl.a. direktivet om integritet och elektronisk kommunikation, genomfördes i svensk rätt.[228]

8.1 Operatörer, leverantörer och anmälningsplikt

Trots att begreppet ”operatör” definieras i 1:7 är det något oklart vad det egentligen innebär. I SOU 2013:39 verkar begreppet tolkas något annorlunda än i 1:7, här uttalas att ”lagringsskyldigheten enligt LEK gäller enbart operatörer (sådana leverantörer som är anmälningspliktiga enligt 2 kap. 1 § LEK)”.[229] PTS verkar tolka begreppet på liknande sätt, på PTS:s webbsida under ”alla anmälda operatörer” finns ett dokument med en lista på över 500 företag som är anmälda enligt 2:1 LEK.[230] Alla anmälningspliktiga verksamheter enligt 2:1 är även lagringsskyldiga enligt 6:16a, men enligt PTS så är det i praktiken ett fåtal tjänsteleverantörer som innehar större delen av den marknad som berörs av skyldigheten att lagra uppgifter.[231] På marknaden för fast telefoni var år 2014 de stora aktörerna TeliaSonera, Tele2, Telenor och Comhem. Även på marknaden för fast bredband så var de stora aktörerna TeliaSonera, Telenor och Comhem, medan Tele2 hade en mindre andel av marknaden än Bahnhof, Bredband2 och AllTele. På marknaden för mobila samtals- och datatjänster och marknaden för mobilt bredband dominerade TeliaSonera, Tele2, Telenor och Hi3g.[232]

[227] Prop. 2011/12:55 s. 50.
[228] Prop. 2002/03:110 s. 111.
[229] SOU 2013:39 s. 130.
[230] PTS (2016). ”Operatörer” (webbsida); PTS (2016). ”Anmälda enligt 2 kap. 1§LEK”.
[231] PTS (2013). ”Konsekvensutredning avseende föreskrifter om ersättning vid utlämnande av lagrade uppgifter för brottsbekämpande ändamål” s. 9–10.
[232] PTS (2015). ”Svensk telemarknad 2014” s. 51, 52, 54–55.

8.2 LEK:s tillämpningsområde

Tillämpningsområdet för LEK är framförallt elektroniska kommunikationsnät och kommunikationstjänster (1:4 1 st.). Begreppet ”elektroniskt kommunikationsnät” är centralt både i LEK och regleringen av HÖEK och HAEK i RB. Begreppet, som definieras i 1:7 med hjälp av en 43 ord lång beskrivning, kan lite förenklat sägas innebära ett system för överföring av signaler med hjälp av t.ex. tråd eller radiovågor, oberoende av vilken typ av information som överförs.

Lagen är däremot inte tillämplig på *innehåll* som överförs i ett kommunikationsnät genom elektroniska kommunikationstjänster (1:4 2 st. LEK). Som exempel på innehåll anges i propositionen innehållet i radio- och tv-utsändningar samt tillhandahållande av innehåll på internet.[233] Anledningen är att det vid tillkomsten av LEK inte ansågs lämpligt att reglera innehållsrelaterad frågor och frågor gällande infrastruktur i samma lag.[234] Enligt förarbetena omfattar LEK därför inte ”informationssamhällets tjänster”, såvida de inte helt eller delvis utgörs av överföring av signaler.[235] Begreppet informationssamhällets tjänster innefattar förutom e-handel bl.a. webbhotell, informationstjänster och söktjänster. Den avgörande förutsättningen är att tjänsten möjliggör interaktiv kommunikation.[236] Informationssamhällets tjänster tillhandahållas normalt mot ersättning, men ersättningen behöver inte utges av den som använder tjänsten, så även tjänster såsom sökmotorer som är avgiftsfria för användaren men som finansieras av reklamintäkter anses som en av informationssamhällets tjänster.[237]

8.2.1 Elektronisk kommunikationstjänst

En elektronisk kommunikationstjänst ska tillhandahållas på kommersiell basis, dvs. den tillhandahålls vanligtvis mot ersättning, men den kan även vara reklamfinansierad (jfr definition i 1:7). Meningen var enligt förarbetena att undanta forskarnätverk och liknande nät som tillhandahålls på rent ideell basis. Avsikten med att ange att en

[233] Prop. 2002/03:110 s. 356.
[234] Prop. 2002/03:110 s. 107–108. Innehållsrelaterad frågor regleras istället i bl.a. *radio- och tv-lagen (2010:696), lagen (2002:562) om elektronisk handel och andra informationssamhällets tjänster* och *lagen (1998:112) om ansvar för elektroniska anslagstavlor.*
[235] Prop. 2002/03:110 s. 116.
[236] Prop. 2001/02:150 s. 19.
[237] Prop. 2001/02:150 s. 56–57.

elektronisk kommunikationstjänst är en ”tjänst […]som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät” var enligt förarbetena att klargöra att begreppet elektronisk kommunikationstjänst inte omfattar innehållstjänster såsom ”webbsidor där musik eller spel tillhandahålls eller webbsidor för elektronisk handel” eller innehållet i radio- och tv-utsändningar.[238]

Enligt Post- och telestyrelsens (PTS:s) vägledning är en (allmänt tillgänglig) elektronisk kommunikationstjänst (ATEK-tjänst) en tjänst som möjliggör kommunikation genom ett nät för användare som köper tjänsten.[239] PTS menar att det är svårt att avgöra vad som utgör elektroniska kommunikationstjänster respektive innehållstjänster, men enligt PTS:s uppfattning är det endast tjänster som möjliggör kommunikation som utgör elektroniska kommunikationstjänster och som därför omfattas av LEK. Därmed utgör inte ”Skype Classic” och ”communities” på internet elektroniska kommunikationstjänster i LEK:s mening, utan denna typ av förädlade tjänster räknas som kommunikation genom befintliga elektroniska kommunikationstjänster (dvs. internetanslutningar). IP-telefoni kan innefattas i begreppet elektronisk kommunikationstjänst, men endast om tillhandahållaren har rådighet över signalerna.[240]

8.2.2 Anmälningspliktiga verksamheter

De verksamheter som är anmälningspliktiga enligt 2:1 LEK är ”[a]llmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster”. Allmänt tillgängliga elektroniska kommunikationstjänster (ATEK-tjänster) är sådana kommunikationstjänster (dvs. tjänster för överföring av signaler) som sker i allmänna kommunikationsnät (AK-nät) till skillnad från slutna nät (t.ex. interna datanät för företag eller myndigheter) där kommunikationstjänsterna endast är åtkomliga för en begränsad grupp användare.[241] Som framgår av definitionen av elektronisk kommunikationstjänst så ska tjänsten tillhandahållas på kommersiell basis. Det krävs inte att en verksamhet äger ett nät för att verksamheten ska anses tillhandahålla det, och

[238] Prop. 2002/03:110 s. 358–359.
[239] PTS (2015). ”Vägledning för anmälan av anmälningspliktig verksamhet” s. 2.
[240] PTS (2009). ”Vilka tjänster och nät omfattas av LEK? En vägledning” s. 21–22.
[241] Prop. 2002/03:110 s. 362.

därför är även verksamheter som till en slutkund tillhandahåller kapacitet som de köpt från en annan verksamhet anmälningspliktiga.[242] Anmälningsplikten gäller enligt 2:2 inte nät som endast överför radio eller tv, och utsändning av tv och radio räknas enligt författningskommentaren inte heller som en allmänt tillgänglig elektronisk kommunikation*stjänst* eftersom utbudet är förutbestämt vilket innebär att det inte är en tjänst för överföring av signaler. Om utbudet inte anses förutbestämt, och utsändningarna därmed blir att se som en ATEK-tjänst, faller utsändningar som sker i tråd in under undantaget från anmälningsplikten i 2:2.[243]

8.3 Behandling av trafikuppgifter och lokaliseringsuppgifter

Direktiv om integritet och elektronisk kommunikation[244], som bl.a. föreskriver regler för hur trafikuppgifter och lokaliseringsuppgifter ska behandlas, införlivades i svensk rätt i huvudsak genom 6 kap. LEK. Ett antal av definitionerna i LEK härrör från detta direktiv, bl.a. definitionen av trafikuppgift.[245]

En trafikuppgift utgör enligt 6:1 en ”uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande”. Ett elektroniskt meddelande innebär enligt samma paragraf ”all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst…”. Av definitionen kan man utläsa att både skriftliga och muntliga meddelande (”all information”) är att betrakta som elektroniska meddelande. Däremot anses inte meddelande som överförs genom elektroniska kommunikationstjänster som inte är allmänt tillgängliga som ett ”elektroniskt meddelande”.[246] I Utredningen om vissa hemliga tvångsmedel uttalas mer konkret, och något förenklat, att trafikuppgifter kan vara uppgifter om ”ursprung, mål och färdväg samt kommunikationens datum, tid, storlek och varaktighet”.[247]

[242] PTS (2015). ”Vägledning för anmälan av anmälningspliktig verksamhet” s. 2.
[243] Prop. 2002/03:110 s. 362-263.
[244] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.
[245] Se art 2(b) i direktiv om integritet och elektronisk kommunikation.
[246] Se 6:1 LEK.
[247] SOU 2012:44 s. 119.

Definitionen av lokaliseringsuppgift härrör även den från direktivet och integritet och kommunikation.[248] Lokaliseringsuppgift definieras i 1:7 som en ”uppgift som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst och som visar den geografiska positionen för terminalutrustningen för en användare”. Lokaliseringsuppgifter kan vara av två typer, nämligen lokaliseringsuppgifter som samtidigt är trafikuppgifter och lokaliseringsuppgifter som inte samtidigt är trafikuppgifter. Lokaliseringsuppgifter som samtidigt är trafikuppgifter är information som behövs för att vidarebefordra ett meddelande, t.ex. information om inom vilken eller vilka basstationers sändningsradie en mobiltelefon befinner sig. Med lokaliseringsuppgifter som inte är trafikuppgifter menades vid LEK:s tillkomst primärt positioneringsuppgifter som behandlades i ett elektroniskt kommunikationsnät och inhämtades via satellit.[249] Det är emellertid inte säker att denna typ av positioneringsuppgifter är de vanligast förekommande i dag.

8.3.1 Behandling av trafikuppgifter

Anmälningspliktiga verksamheter ska som huvudregel utplåna eller avidentifiera trafikuppgifter som gäller fysiska personer när de inte längre behövs för att överföra ett elektroniskt meddelande (6:5). Detta gäller inte om uppgifterna sparas för att behandlas enligt vissa i paragrafen angivna bestämmelser, bl.a. i faktureringssyfte i enlighet med 6:6 eller lagring för brottsbekämpande ändamål enligt 6:16a.

Om samtycke föreligger får trafikuppgifter även behandlas för att ”tillhandahålla andra tjänster där uppgifterna behövs” (6:6 2 st.). Med det uttrycket avses sådana tjänster som i direktivet om integritet och elektronisk kommunikation benämns mervärdestjänster.[250] Mervärdestjänster definieras i direktivet som ”tjänster som kräver behandling av trafik- eller lokaliseringsuppgifter utöver vad som är nödvändigt för överföring eller fakturering av en kommunikation”.[251] Som exempel på vad dessa kan vara anges i skäl 18 i direktivet bl.a. information om vägval, väderutsikter och turistinformation.[252]

[248] Se art 2(c) i direktiv om integritet och elektronisk kommunikation, såsom ändrad genom Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009.
[249] Prop. 2002/03:110 s. 359; jfr skäl 35 i direktivet om integritet och elektronisk kommunikation.
[250] Prop. 2002/03:110 s. 391–392, 258.
[251] Art 2(g) i direktivet om integritet och elektronisk kommunikation.
[252] Skäl 18 i direktivet om integritet och elektronisk kommunikation.

Enligt 6:8 ”gäller inte” 6:5–7 bl.a. när meddelandena omfattas av beslut om HAEK, HÖEK eller beslut enligt 2012 års inhämtningslag (6:8 1 st. 2). Trots lydelsen innebär detta troligtvis inte att ett beslut om hemliga tvångsmedel innebär att tjänstetillhandahållaren blir förhindrad att spara uppgifter för faktureringssyfte i enlighet med 6:6 1 st. Avsikten med bestämmelsen var nämligen att den skulle motsvara den tidigare bestämmelsen i 50 § 1 st. 1 telelagen (TL).[253] Innebörden av detta lagrum var att skyldigheten i 49 § 1 st. TL att utplåna uppgifter när ett meddelande nått mottagaren inte gällde när meddelandet omfattades av ett beslut om hemliga tvångsmedel. Detta påverkade inte möjligheten i 49 § 2 st. TL att spara uppgifter för faktureringssyfte.

Innan datalagringsskyldigheten i 6:16a infördes var följden av denna bestämmelse att när ett beslut om HAEK eller HÖEK hade fattats och delgetts en verksamhet så var verksamheten skyldig att spara uppgifterna, men trafikuppgifter som härrörde från tiden innan beslutet delgetts verksamheten kunde endast var tillgängliga för brottsbekämpande myndigheter i den mån som verksamhet sparat uppgifterna av andra skäl. Tillgången till historiska uppgifter varierade därför stort beroende på vilka kostnadsavvägningar verksamheten ifråga hade gjort och dess behov.[254]

8.3.2 Behandling av lokaliseringsuppgifter som inte är trafikuppgifter

Lokaliseringsuppgifter som inte är trafikuppgifter och som gäller fysiska personer får som huvudregel endast behandlas om samtycke föreligger alternativt uppgifterna har avidentifierats och endast i den mån uppgifterna behövs för att tillhandahålla en tjänst. Uppgifterna får behandlas av den tjänst där de behövs eller av den som fått i uppdrag av en tillhandahållare av ett AK-nät eller ATEK-tjänst (se 6:9–10). Detta innebär enligt förarbeten att även mervärdestjänster kan få behandla lokaliseringsuppgifter som inte är trafikuppgifter, om uppgifterna har avidentifierats alternativt samtycke från personen föreligger.[255]

[253] Prop. 2002/03:110 s. 259, 392.
[254] SOU 2005:38 s. 329.
[255] Prop. 2002/03:110 s. 393.

8.3.3 Begreppet ”behandling”

Begreppet ”behandling” har enligt 6:1 LEK samma betydelse som i personuppgiftslagen (1998:204) (PuL). Begreppet innefattar därmed bl.a. insamling och utlämnande av uppgifter (se 3 § PuL). Därmed innefattar begreppet enligt ett beslut från Justitiekanslern (JK) även utlämning av uppgifter till brottsbekämpande myndigheter. Enligt JK:s beslut kunde därför lokaliseringsuppgifter som avsåg en mobiltelefon som enbart var påslagen men vid tillfället inte användes för kommunikation inte lämnas ut till brottsbekämpande myndigheter eftersom de var sådana uppgifter som reglerades av 6:9 LEK och det vid tillfället inte fanns något undantag för behandling genom utlämnande till brottsbekämpande myndigheter.[256]

Efter JK:s beslut infördes 6:10a LEK som medger undantag för när uppgifterna omfattas av beslut om inhämtning enligt 27 kap. RB eller 2012 års inhämtningslag. Samtidigt ändrades även regleringen av HÖEK så att det blev möjligt att inhämta uppgifter om lokalisering av en utrustning som vid tillfället inte används för kommunikation (jfr 27:19 1 st. 2 RB). När ett beslut om inhämtning är fattat får uppgifterna enligt 6:10a LEK ”behandlas utan hinder av 9 och 10 §§”, vilket enligt författningskommentaren innebär att uppgifter som ”avser en enbart påslagen mobiltelefon” kan inhämtas.[257]

Frågan är dock om det är det enda regleringen innebär. Om en mervärdestjänst har historiska lokaliseringsuppgifter som inte är trafikuppgifter sparade, är det då möjligt att behandla dessa genom utlämnande till brottsbekämpande myndigheter när det finns ett beslut om t.ex. HÖEK? Innebär det att mervärdestjänster får behandla lokaliseringsuppgifter utan hinder av samtycke om kommunikationsenheten omfattas av ett beslut om inhämtning? Samma frågor uppkommer vad gäller skrivningen i 6:8 att ”5–7 §§ gäller inte” när uppgifterna omfattas av ett beslut om t.ex. HÖEK, innebär det att ingen av reglerna i 5–7 §§ gäller?

[256] JK-beslut 2008-08-15 Dnr: 6545-06-21.
[257] Prop. 2011/12:55 s. 142–143.

8.4 Tystnadsplikt och utlämnande av abonnemangsuppgifter

Tystnadsplikt gäller för de uppgifter som anges i 6:20 1 st. 1–3, dvs. uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och ”annan uppgift som angår ett särskilt elektroniskt meddelande”. Avgränsningen av de uppgifter som omfattas av tystnadsplikten i 6:20 1 st. 1 och 3 avgör samtidigt vilka uppgifter som anmälningspliktiga verksamheter är skyldiga att lagra (jfr 6:16a) och vilka uppgifter som kan lämnas ut med stöd av 6:22. Potentiellt fler tillhandahållare omfattas av denna bestämmelse och 6:22 än som omfattas av anpassningsskyldigheten i 6:19 och lagringsskyldigheten i 6:16a, eftersom 6:20 och 6:22 inte avgränsar till att omfatta endast nät och tjänster som är allmänt tillgängliga, utan avser alla elektroniska kommunikationsnät och elektroniska kommunikationstjänster.

Med ”uppgift om abonnemang” i 6:20 1 st. 1 avses ”uppgifter som identifierar en abonnent eller ett abonnemang, framför allt namn, titel, adress och abonnentnummer”.[258] Även IMSI-nummer har ansetts kunna vara en uppgift om abonnemang.[259] IMEI-nummer och IP-adresser, även dynamiska sådana, anses även de kunna vara en uppgift om abonnemang.[260] Regeringen påpekar särskilt att uppgifter om abonnemang däremot inte omfattar uppgifter om med vilka IP-nummer kommunikation skett eller vilka hemsidor som besökts.[261] Ifråga om ”annan uppgift som angår ett särskilt elektroniskt meddelande” i 6:20 1 st. 3 så anges i Ds 2014:23 att detta i praxis har tolkats som uppgifter om deltagare i kommunikationen, uppgifter om när och varifrån kommunikation skett och under hur lång tid.[262]

Som angetts ovan i avsnitt 7.2.1 har denna bestämmelse även tolkats som att möjliggöra s.k. basstationstömning, innan detta reglerades i RB.[263] Vid den tiden innebar 6:22 1 st. 2 nämligen att Polismyndigheten kunde inhämta uppgift om abonnemang och ”annan uppgift som angår ett särskilt meddelande” (6:20 1 st. 1 och 3) när uppgiften behövdes

[258] Prop. 2011/12:55 s. 52.
[259] RK 2010:1.
[260] SOU 2009:1 s. 71.
[261] Prop. 2011/12:55 s. 102.
[262] Ds 2014:23 s. 64.
[263] Prop. 2011/12:55 s. 96.

för att utreda ett brott som hade fängelse i straffskalan och som bedömdes kunna föranleda annan påföljd än böter. Ändringen innebär att Polismyndigheten endast kan inhämta uppgift om abonnemang, men i gengäld krävs inte längre att brottet ska vara av visst allvar, det räcker att det är ett brott som Polismyndigheten ska ingripa mot.[264]

8.5 Lagring av trafikuppgifter m.m. för brottsbekämpande ändamål

Bestämmelserna om lagringsskyldighet m.m. i 6:16a-f baseras delvis på datalagringsdirektivet, vilket som bekant (se avsnitt 4.3) har ogiltigförklarats av EU-domstolen.[265] De verksamheter som träffas av lagringsskyldigheten är de verksamheter som är anmälningspliktiga enligt 2:1. Det innebär att fler aktörer är lagringsskyldiga än som är anpassningsskyldiga enligt 6:19. Av detta skäl har regeringen ansett det motiverat att införa en separat anpassningsbestämmelse för de lagringsskyldiga verksamheterna.[266] Denna bestämmelse, som placerats i 6:16f, innebär att lagringsskyldiga verksamheter måste organisera sin verksamhet så att lagrade uppgifter enkelt kan tas om hand av brottsbekämpande myndigheter. Detta gäller enligt propositionen även om uppgifterna finns i krypterad eller komprimerad form hos lagringsskyldiga verksamheter.[267] Detta innebär dock inte att lagringsskyldiga verksamheter är tvungna att avkryptera *innehållet* i ett meddelande (t.ex. innehållet i ett IP-paket). Detta framgår enligt regeringen av att innehåll i meddelande inte ska lagras.[268]

Uppgifter som lagrats i enlighet med 6:16a får enligt 6:16c endast behandlas för att lämnas ut med stöd av 6:22 1 st. 2 LEK, 27:19 RB eller 2012 års inhämtningslag. De uppgifter som ska lagras är de uppgifter som omfattas av tystnadsplikten i 6:20 1 st. 1 och 3, och som, förenklat uttryckt, är nödvändiga för att klargöra vem som kommunicerade med vem, när, hur länge och genom vilken typ av kommunikation och kommunikationsutrustning samt var parterna befann sig (se 6:16a). Lagringen gäller endast uppgifter som den lagringsskyldige redan behandlar och innebär ingen

[264] Prop. 2011/12:55 s. 100-101.
[265] Digital Rights Ireland m.fl., förenade målen C-293/12 och C-594/12, (ECLI:EU:C:2014:238), se § 71.
[266] Prop. 2010/11:46 s. 50.
[267] Prop. 2010/11:46 s. 81.
[268] Prop. 2010/11:46 s. 24–25.

skyldighet att skaffa sig uppgifterna.[269] Vilka uppgifter som konkret ska lagras för de olika formerna av kommunikation anges närmare i 39–43 §§ i förordningen (2003:396) om elektronisk kommunikation (FEK). Lagringen av uppgifter om meddelandehantering regleras i 42 § FEK. Med begreppet meddelandehantering menas enligt förarbetena överföring av framförallt SMS, MMS och e-post, dvs. tjänster som använder sig av olika kommunikationsprotokoll. Som exempel på sådana protokoll nämns ett vanligt kommunikationsprotokoll för e-post kallat SMTP (Simple Mail Transfer Protocol, RFC 2821 och RFC 2822, IETF) och ett kommunikationsprotokoll för SMS kallat SMPP (Short Message Peer-to-Peer Protocol v5.0).[270] Uppgifter om surfhistorik (dvs. besök på hemsidor), besök på chattsidor och filöverföring med hjälp av FTP (File Transfer Protocol) omfattas däremot inte av lagringsskyldigheten. Enligt regeringen var det inte lämplig med mer omfattande lagring med hänsyn till både integritets- och kostnadsaspekter.[271]

Uppgifter om användning av webbaserade e-posttjänster (t.ex. Hotmail) omfattas enligt PTS:s bedömning som huvudregel inte att lagringsskyldigheten. Webbaserade e-posttjänster kan dock omfattas av lagringsskyldigheten om de tillhandahålls av någon som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst.[272] Lagringsskyldigheten gäller däremot inte informationssamhällets tjänster (t.ex. webbhotell och söktjänster, se avsnitt 8.1) eftersom dessa inte omfattas av LEK.[273]

Ifråga om internetåtkomst ska enligt 43 § FEK bl.a. en användares IP-adress lagras. Enligt regeringen finns det ingen anledning att tro att detta kan leda till att en användares surfhistorik och beteende på internet kan kartläggas. Detta menar regeringen nämligen är tekniskt omöjligt eftersom IP-adresser vanligtvis inte är statiska utan dynamiska och därför byts med oregelbundna intervall.[274]

[269] Prop. 2010/11:46 s. 23–24, 77.
[270] Prop. 2010/11:46 s. 30; SOU 2007:76 s. 143.
[271] Prop. 2010/11:46 s. 77, 35.
[272] PTS (2012). ”Uppgifter som ska lagras för brottsbekämpande ändamål – en vägledning” s. 10.
[273] PTS (2012). ”Uppgifter som ska lagras för brottsbekämpande ändamål – en vägledning” s. 2.
[274] Prop. 2010/11:46 s. 25.

8.6 Anpassningsskyldigheten i 6:19

Anpassningsskyldigheten i 6:19 reglerar vilka verksamheter som måste anpassa sina system för att underlätta för brottsbekämpande myndigheter att verkställa beslut om HAEK och HÖEK. Bestämmelsen avser tre olika grupper av verksamheter; tillhandahållare av nät, tillhandahållare av fast telefonitjänst och tillhandahållare av mobil kommunikationstjänst.[275]

Ifråga om vilka nätoperatörer som omfattas, så är det endast de som tillhandahåller ett allmänt kommunikationsnät som inte enbart är avsett för utsändning av tv, radio eller liknande grundlagsskyddade typer av utsändningar. Det är därmed inte alla som tillhandahåller ett elektroniskt kommunikationsnät som inkluderas (jfr definitioner i 1:7). I motsats till vad som gäller anmälningsplikten i 2:1, så föreskrivs här dock inte ett krav på att nätet är ”av sådant slag som vanligen tillhandahålls mot ersättning”.

Vad gäller vilka tjänster som omfattas så är det svårare att bedöma utifrån lagtexten. Enligt 6:19 1 st. 2 omfattas:

> ”tjänster inom ett allmänt kommunikationsnät vilka består av
>
> a) en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller
>
> b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt”

Avsikten när bestämmelsen utformades var att den skulle omfatta samma område som omfattades av anpassningsskyldigheten i 17 § TL.[276] De verksamheter som var anpassningsskyldiga enligt 17 § TL var de som beviljats tillstånd enligt 7 § TL. Tillstånd krävdes för verksamheter som innebar tillhandahållande av telefonitjänst till fast nätanslutningspunkt, mobil teletjänst och nätkapacitet, genom allmänt tillgängligt nät. Telefonitjänst definierades i TL som ”teletjänst bestående i överföring av tal och som medger överföring av telefaxmeddelanden samt datakommunikation via låghastighetsmodem” (1 § TL).

[275] SOU 2005:38 s. 36.
[276] Prop. 2002/03:110 s. 396.

Skrivningen i 6:19 1 st. 2 a) tar alltså sikte på telefoni till fast nätanslutningspunkt. Detta innebär enligt förarbetena att även den som tillhandahåller IP-telefoni kan träffas av bestämmelsen om tjänsten uppfyller kriterierna för allmänt tillgänglig telefonitjänst.[277] De krav som behövde uppfyllas för att falla inom bestämmelsen sänktes när definitionen av samtal och telefonitjänst ändrades så att samtal inte nödvändigtvis behövde vara i realtid och en telefonitjänst inte krävde att man kunna ringa nödsamtal. Detta innebar enligt förarbetena att de ”internettelefonitjänster” som tidigare inte omfattades endast p.g.a. möjligheten att ringa nödsamtal saknades efter ändringen skulle omfattas.[278]

Alla verksamheter, eller med BRU:s ord ”samtliga tekniker som är aktuella”, omfattas alltså inte av anpassningsskyldigheten, vilket BRU menar innebär stora effektivitetsförluster eftersom verkställandet av tvångsmedlet antingen fördröjs eller inte alls kan genomföras.[279] BRU menar även att bestämmelsen är otydlig och har därför föreslagit en ändrad lydelse. Deras förslag innebär att även verksamheter ”som avser tillhandahållande av Internettjänster” ska omfattas p.g.a. det stora allmänintresset av att förhindra brott.[280] PTS kritiserade förslaget och menade att det skulle innebära att inte enbart internetleverantörer skulle bli anpassningsskyldiga, utan även innehållstjänster. Det skulle även innebära stora tekniska svårigheter att överlämna en dataström i läsbart format till brottsbekämpande myndigheter.[281] Det är inte helt otänkbart att PTS:s kritik har inneburit att bestämmelsen inte ändrades i enlighet med BRU:s förslag.

[277] Prop. 2002/03:110 s. 270,
[278] Prop. 2010/11:115 s. 157.
[279] SOU 2005:38 s. 279.
[280] SOU 2005:38 s. 280–282.
[281] PTS (2007). ”Kostnader p.g.a. nya krav på hemlig avlyssning och övervakning av ”internettjänster” m.m.” s. 12, 36.

9 Uppgifter som inte omfattas av LEK

9.1 Tvångsmedel och elektroniskt lagrad information

Information rörande elektronisk kommunikation kan även inhämtas med hjälp av tvångsmedlen beslag, husrannsakan och editionsföreläggande. Information kan t.ex. inhämtas genom att ett medium som innehåller lagrade meddelande tas i beslag. Enligt förarbetena följer dock av principerna om lex specialis och lex posterior att beslag, husrannsakan och editionsföreläggande inte kan tillämpas på de uppgifter som omfattas av regleringen av HÖEK och HAEK.[282] Detta exemplifieras av ett beslut av Justitiekanslern (JK) (se avsnitt 8.3.3), där JK menade att det inte var tillåtet för polis att från operatörer begära ut ”uppgifter om var en mobiltelefon befinner sig när den är påslagen men inte används”. Uppgifterna kunde inte begäras ut med stöd av 6:22 LEK, eftersom uppgifterna inte kunde ses som ”annan uppgift som angår ett särskilt elektroniskt meddelande”, och inte med stöd av HÖEK (i sin dåvarande lydelse). Eftersom uppgifterna omfattades av 6:9 LEK kunde de inte heller utan tillstånd från abonnenten behandlas i den meningen att operatörerna frivilligt kunde lämna ut uppgifterna. Däremot kunde editionsföreläggande eller beslag användas eftersom uppgifterna inte omfattades av HÖEK.[283] Efter JK:s beslut har både 6:10a LEK införts och regleringen av HÖEK ändrats så att uppgifterna omfattas, och uppgifterna bör därför inte längre kunna inhämtas med hjälp av editionsföreläggande eller beslag.

Möjligheten för domstol att utfärda editionsföreläggande regleras i 23:14 2 st. RB och 38 kap. RB. Editionsföreläggande kan enligt NJA 1998 s. 829 även tillämpas på elektroniskt lagrad information och det utgör inget hinder att visst arbete kan behövas utföras för att efterkomma föreläggandet. För att ett editionsföreläggande ska kunna meddelas krävs enligt NJA 2003 s. 107 att det finns en för brottet skäligen misstänkt person.[284] Editionsföreläggande används dock sällan i brottmål eftersom reglerna om beslag och husrannsakan är avsedda att tillämpas istället.[285]

[282] Prop. 2002/03:74 s. 45–46; SOU 2015:31 s. 82–83.
[283] JK-beslut 2008-08-15 Dnr: 6545-06-21.
[284] Jfr SOU 2013:39 s. 135–136.
[285] Ds 2005:6 s. 237.

Gällande husrannsakan och beslag så anses brottsbekämpande myndigheter ha rätt att söka efter t.ex. dokument och spår av kommunikation i en dator som påträffas i en lokal under en husrannsakan.[286] Det är dock vanligare att en informationsbärare som en dator tas i beslag än att den genomsöks på plats eftersom det är resurskrävande att genomsöka den mängd information som en dator vanligtvis innehåller.[287] Vad gäller gränsdragningen mellan undersökning av beslag och HAEK så anses beslagsreglerna för post m.m. i 27:12 RB även gälla e-post, sms m.m. i de fall meddelandet finns lagrat i ett medium som är taget i beslag. Är meddelandet istället del av en pågående kommunikation så anses meddelandet endast kunna undersökas med stöd av HAEK. Ifråga om meddelandet som förvisso kan nås från mediet men är lagrat hos en operatör, så spelar det ingen roll om en mottagare tagit del av ett meddelande eller inte, meddelandet kan endast tas del av med hjälp av HAEK.[288]

Om en polis via en dator uppkopplad till en server tar del av uppgifter som är lagrade utomlands, så utgör det en husrannsakan utomlands.[289] Rättslig hjälp måste därför begäras för att få fram information som lagras utomlands, såvida informationen inte är allmänt tillgänglig på internet.[290] Det är möjligt att genomföra husrannsakan hos företag som erbjuder lagringsutrymme, s.k. hostingföretag, eftersom de inte omfattas av LEK. Eftersom hostingföretag kan inneha hundratals servrar behövs i praktiken hjälp av t.ex. en systemadministratör för att få tag i t.ex. lösenord eller få upplysningar om på vilken server den sökta informationen lagras. Det är inte alltid att brottsbekämpande myndigheter får denna hjälp, t.ex. av det skälet att företaget känner lojalitet mot sina kunder, och ofta är det inte praktiskt möjligt eller proportionerligt att ta alla servrar i beslag. Enligt Utredningen om it-brottskonventionen finns det därför skäl att överväga om en möjlighet att meddela föreläggande att lämna information i syfte att underlätta husrannsakan i it-miljö bör införas.[291]

[286] SOU 2013:39 s. 149.
[287] SOU 2013:39 s. 152.
[288] Westerlund s. 151, 158.
[289] Ds 2005:6 s. 131.
[290] Ds 2005:6 s. 282.
[291] SOU 2013:39 s. 160–161.

9.2 Innehålls- och informationssamhällets tjänster

Innehållstjänster och informationssamhällets tjänster regleras som sagt inte av LEK (se avsnitt 8.2). Brottsbekämpande myndigheter har trots detta vissa möjligheter att få ut uppgifter från sådana tjänster, med det är inte fullständigt tydligt vilka uppgifter som kan utfås och med vilket lagstöd det görs. Stephan Uttersköld, vice chefsåklagare, menar t.ex. i ett opinionsinlägg i Svenska Dagbladet att brott genom innehållstjänster, t.ex. ”Facebook” och bloggar inte omfattas av LEK och att det därför inte finns någon skyldighet för tillhandahållare av dessa tjänster att lämna ut uppgifter till brottsbekämpande myndigheter, men att vissa tillhandahållare samarbetar på frivillig basis.[292] Enligt senare uppgifter i Svensk Polis, kan dock vissa uppgifter inhämtas från Facebook om uppgifterna behövs i en brottsutredning. Facebook kan enligt artikeln lämna ut ”abonnentuppgifter, det vill säga de uppgifter som en kontohavare lämnat om sig själv, och IP-adresser som använts då inloggningar skett”. För att däremot få ut innehåll (t.ex. bilder och inlägg) som finns på ett konto krävs att en åklagare begär rättslig hjälp.[293] Enligt Rikspolisstyrelsen så har merparten av de förfrågningar de skickat under perioden december 2013 till och med september 2014 lett till att Facebook har lämnat ut uppgifter (501 förfrågningar av 512). Att uppgifter inte alltid har lämnats ut beror enligt artikeln på skillnader mellan amerikansk och svensk lagstiftning.[294]

Eftersom Facebook tillhandahålls till Europeiska användare av ”Facebook Ireland Ltd” är det även möjligt att det är irländsk lagstiftning som ska tillämpas ifråga om vissa uppgifter. Den irländska tillsynsmyndigheten, ”Data Protection Commissioner”, har i vart fall granskat om ”Facebook Ireland Ltd” följt den irländska lagstiftningen som införlivar dataskyddsdirektivet.[295] Tillsynsmyndigheten har konstaterat att bolaget har följt reglerna genom att de gjort en adekvat granskning av förfrågningar som inkommit från olika brottsbekämpande myndigheter i Europa innan de lämnat ut uppgifter om t.ex. användares kontaktinformation och vilka IP-adresser en användare haft.[296]

[292] Uttersköld (2011). ”Bra kompetens för internetrelaterade brott”, Svenska Dagbladet.
[293] Magnusson (2014). ”De har nyckeln till näthatarna”, Svensk Polis – En tidning från Rikspolisstyrelsen.
[294] Näfver (2014). ”Polisen och Facebook i samarbete mot näthat”, nyhet från Rikspolisstyrelsen.
[295] Data Protection Commissioner (2011). ”Facebook Ireland Ltd: Report of Audit” s. 3.
[296] Data Protection Commissioner (2012). ”Facebook Ireland Ltd: Report of Re-Audit” s. 34–35.

10 Analys och slutsatser

Frågeställningarna till detta arbete var hur ökade befogenheter för polis och åklagare gällande hemliga tvångsmedel har motiverats samt vilka verksamheter som omfattas av skyldigheten att samarbeta med bl.a. polisen för brottsbekämpande ändamål enligt LEK. För att få en korrekt bild måste man som Abrahamsson påpekar ta hänsyn till alla tvångsmedel, man måste med Rambergs ord låta ”äpplen och päron packas i samma korg”. Innan frågeställningarna besvaras ska därför den nya regleringen först sammanfattas och analyseras utifrån Jareborgs modell för en defensiv straffrättspolitik.

10.1 Nya regleringen

Det finns som sagt tre olika typer regelkomplex som innebär att uppgifter om elektronisk kommunikation kan inhämtas för brottsbekämpande ändamål: tillstånd till HAEK eller HÖEK enligt RB, inhämtning enligt 2012 års inhämtningslag samt inhämtning av uppgifter om abonnemang enligt 6:22 LEK. Till det ska läggas 2007 års preventivlag som inte innebär andra tvångsmedel än i RB, men där andra förutsättningar ifråga om bl.a. misstanke om fullbordat brott gäller.

Införandet och permanentandet av 2007 års preventivlag, samt utvidgningen av tillämpningsområdet och regelförenklingen, får betecknas som ett steg mot en offensivare straffrättspolitik. Regelförenklingen innebär bl.a. en bevislättnad när individer tillhör en grupp som misstänkts för brottslig verksamhet, vilket innebär att människor snarare ses som en grupp av brottslingar än som enskilda individer som begår brott. Ändringen av 6:22 LEK, så att bestämmelsen kan tillämpas även vid bötesbrott, är utifrån Flygheds begreppsbildning ett exempel på normalisering av medel, och kan även det ses som ett tecken på en allt offensivare inriktning.

Ett annat tecken på en offensiv inriktning är enligt Jareborg att beslutsbehörighet överflyttas från domstol till åklagare och från åklagare till polis. Som angetts i 7.3 har åklagare sedan år 2015 möjlighet att ta ett tillfälligt beslut om HAEK, HÖEK och hemlig kameraövervakning. Ännu tydligare framträder det offensiva draget i 2012 års inhämtningslag, eftersom beslut om inhämtning fattas direkt av myndigheter, och Säkerhets- och integritetsskyddsnämnden endast utövar tillsyn över beslut i efterhand.

10.1.1 Ibland är det bättre att reglera

Lindberg menar att införda tvångsmedel sällan upphävs, oavsett om de gör någon nytta, samtidigt som nya tvångsmedel tillkommer. Detta kan illustreras med användning av hemlig postkontroll enligt 2007 års lag, vilken varit obefintlig de senaste åren. Lindberg menar även att det ibland är bättre att reglera ett oreglerat tvångsmedelsliknande verktyg än att låta myndigheterna använda det efter eget behag. Det är även ofta att när myndigheterna befinns agera utanför eller i gråzonen för vad som är tillåtet och detta sedan uppmärksammas som lagstiftningen sedan ändras så att myndigheterna agerande blir uttryckligen tillåtet. Detta kallar Flyghed för en form av medelnormalisering, och skulle kunna illustreras med att polis begärde ut lokaliseringsuppgifter som inte samtidigt var trafikuppgifter innan detta var tillåtet. När detta förhållande uppmärksammades i en anmälan till JK blev det tydligt att detta inte var tillåtet enligt den dåvarande regleringen. Något år senare ändrades lagstiftningen uttryckligen på grund av detta förhållande.

10.1.2 Rättssäkerhetsgarantier

I SOU 2015:31 menas, i likhet med tidigare utredningar Ds 2014:23 och SOU 2012:44, att svensk lagstiftning har tillräckliga rättssäkerhetsgarantier och att möjligheterna för brottsbekämpande myndigheter att inhämta uppgifter istället ska öka. EU-domstolens dom innebär därför inte några egentliga konsekvenser för den svenska lagstiftningen. Som en slump har alla dessa tre utredningar som kommit till liknande resultat bestått av ensamutredaren Sten Heckscher, förvisso assisterad av experter såsom Iain Cameron.

I detta betänkande menas att EU-domstolens dom inte betyder att det är oproportionerligt att använda uppgifterna för att lösa mindre grova brott. Frågan är om detta verkligen är självklart. Ändamålsprincipen innebär förvisso enbart att tvångsmedel ska användas för det ändamål som angetts i lag, men en liknelse kan ändå göras till att datalagring får användas för andra brott än som angetts i datalagringsdirektivet. Flyghed skulle troligtvis benämna detta ”normalisering av de exceptionella” och specifikt normalisering av medel, vilket innebär att tillämpningsområdet för medlen med tiden utvidgas till att även angripa andra problem än som ursprungligen avsetts.

10.1.3 Kritik av typfallsmetoden

Det är problematiskt att endast anonymiserade exempel respektive typfall ska redovisas för att visa på nyttan av 2012 års inhämtningslag och HÖEK. Det ligger nämligen i brottsbekämpande myndigheters intresse att framställa sin verksamhet som lyckad och tvångsmedelsanvändningen som nödvändig, vilket påpekas av både Flyghed och Ramberg. Risken är därför att det inte blir typfall som redovisas, utan istället optimala fall. Typfallen ska vara anonymiserade vilket gör att det är svårt att undersöka om de är representativa och korrekt återgivna. Det är även svårt att dra slutsatser om generell nytta utifrån ett fåtal exempel, den enda slutsats som kan dras är att tvångsmedlet varit till nytta i de fallen, om dessa är korrekt återgivna. Att typfallen baserar sig på ärende där en dom har meddelats torde betyda att de fall där övervakningen inte varit till nytta inte kan komma med i redogörelsen. Även om myndigheterna inte medvetet försöker vara missvisande är det därför tveksamt om detta faktiskt inte blir konsekvensen.

Åklagarmyndigheten ska framöver inte redovisa uppskattningar av nytta utan endast typfall. I redovisningen för 2014 redovisades emellertid både uppskattad nytta och typfall. Det är därför möjligt att jämföra typfallen med nyttouppskattningarna, i syfte att få en uppfattning om typfallen är representativa. Av de två typfallen framstår det som att användningen av HÖEK har varit av avgörande betydelse för att förhindra grova brott. Jämför man detta med nyttouppskattningen framstår detta som något missvisande, åklagarna uppskattade att nytta förelåg i förhållande till 74 % av individerna som var misstänkta. Inget av de två redovisade typfallen gällde narkotikabrott, trots att detta brott var det vanligaste, om än med liten marginal, skälet till att tillstånd gavs.

Att redovisa genomsnittstid eller mediantid för tillstånd till HÖEK blir naturligtvis missvisande eftersom basstationstömning numera innefattas. Eventuellt är det trots allt möjligt och av värde att redovisa den längsta tid ett tillstånd till HÖEK har varat. Det ger onekligen en tydligare bild att veta att åtminstone vid ett tillfälle (år 2010) så har övervakningsuppgifter gällande 1095 dagar inhämtats. Avsaknaden av redovisning efter år 2011 gör dock att det inte går att avgöra om detta var en engångsföreteelse. Det förefaller som att det hade varit lämpligt om olika typer av HÖEK hade särredovisats, och eftersom basstationstömning inte riktar sig till ett visst telefonnummer förefaller det möjligt att särskilja när ett tillstånd avser ett telefonnummer respektive en mast.

10.2 Motivering av ökade befogenheter

10.2.1 Vi vanliga människor har inget att frukta

Den som inte har något att dölja, som har ”rent mjöl i påsen”, behöver inte vara orolig över att bli övervakade, lyder ofta argumentet från övervakningsanhängare. Som Abrahamsson påpekar är detta inte ett giltigt argument, enligt EKMR och RF har alla rätt till respekt för sin integritet. Flyghed menar att argument som ”rent mjöl i påsen” leder fel och närmast blir en omvänd bevisbörda. De flesta människor har nog något som de vill hålla för sig själv, t.ex. angående hälsa, kontroversiella åsikter eller umgängeskrets, men frågan är egentligen inte om det finns något att dölja, utan vilken information staten egentligen ska få ta reda på och spara. Flyghed frågar sig därför om vi verkligen vill att staten ska peta runt i vårt rena mjöl med sina smutsiga fingrar.

Som Ramberg påpekar, med hänvisning till frysningen av tillgångar för svenskar med somaliskt ursprung, så innebär den omständigheten att man har ”rent mjöl” inte att man inte riskerar att bli utsatt för statens maktmissbruk. Bylund ifrågasätter påståendet att myndigheten aldrig skulle missbruka sina maktbefogenheter, historien visar snarast att detta har skett, t.ex. när Säkerhetspolisen under lång tid övervakade människor med vissa politiska åsikter under förevändningen att de utredde olovlig kårverksamhet. Detta uppmärksammas även i SOU 2012:44, samt att Säkerhetspolisen sedan försökte påskina att deras kommunistjakt inneburit att sovjetiska underrättelseofficerare kunnat gripas. Till detta kommer att skyddet för den som inte är misstänkt inte är så starkt som man skulle kunna tro utifrån proportionalitetsprincipen i 27:1 RB, enligt Bylund. Det är även svårt för individer att veta om alla människor de har kontakt med har ”rent mjöl”, eller om dessa människor har t.ex. politiska åsikter eller berusningsvanor som misshagar staten i sådan utsträckning att de och deras kontakter övervakas.

Abrahamsson menar emellertid att det är en intellektuell elit som är integritetsvänner och som tror sig tala för folket, men som i själva verket inte gör det, vilket visats av undersökningar. Det är dock möjligt att sakens natur gör att de vanliga människor som hyser misstro mot staten och är starkt emot övervakning inte uttalar sig därom just p.g.a. oro över att bli övervakade. Det är även troligt att dessa individer av samma skäl är underrepresenterade i undersökningar om människors attityder till tvångsmedel.

Hilding Qvarnström ger däremot i mycket uttryck för vad Jareborg kallar en offensiv inriktning av straffrättspolitik, t.ex. genom en uppdelning av människor i ”laglydiga medborgare” och ”motståndarna”, de som är yrkeskriminella. Hon menar även att det är samma människor som kommer vara föremål för de nya tvångsmedel som de gamla. Vi vanliga människor bör därför inte ha något att oroa oss för, förutom att bli utsatta för brott, vilket är det mest integritetskränkande en människa kan råka ut för, enligt Hilding Qvarnström. Hildings Qvarnströms påstår att brottsoffren förväntar sig att staten ska lägga ”alla tänkbara resurser” på att utreda brott. Detta påstående är intressant utifrån Jareborgs uppdelning i defensiv och offensiv inriktning av straffrätten, Jareborg menar som bekant att kostnaden för verkligt effektiv brottsprevention är statsterrorism. Även Ramberg är inne på samma spår, enligt henne utgör maktmissbruk ett långt allvarligare hot än terrorism och grov brottslighet. Att bli utsatt för maktmissbruk utgör i många fall en kränkning med svårare konsekvenser än att bli utsatt för brott, eftersom det som Lindberg påpekar är svårare för enskilda att göra något när staten kränker än när kränkningar kommer från andra enskilda, eftersom människor inte egentligen har någon att vända sig till när staten står för kränkningen.

Som Abrahamsson påpekat ger uttalandet att det är integritetskränkande att bli utsatt för brott ingen ledning i avvägningsfrågan, särskilt när någon annan än en misstänkt är föremål för övervakning. Hilding Qvarnström skulle troligtvis med Abrahamsson terminologi kallas ”övervakningsanhängare”, argumentet om brottsoffrens integritet och förväntan som Hilding Qvarnström för fram känns t.ex. igen som övervakningsanhängarnas argument nr. 2 utifrån Abrahamssons uppställning.

10.2.2 Uppgifterna är inte känsliga

Slutsatsen att människor inte skulle ha något emot att deras uppgifter samlas in och sparas eftersom vissa individer delar mycket personlig information bl.a. på internet och genom användning av kreditkort, kritiseras av Abrahamsson som menar att det är mycket stor skillnad på vad som frivilligt delas och vilka uppgifter som inhämtas med tvång. Det går därför inte att dra slutsatser om människors attityder till övervakning utifrån att vissa människor frivilligt delar viss information. En annan fråga är om människor egentligen vet hur mycket deras inköp med konto- och kreditkort avslöjar om

dem, och vilka val människor i praktiken har. Det finns kanske inte alltid en reell valmöjlighet i dagens samhälle, att t.ex. inte bruka sociala medier såsom Facebook eller ha en smartphone med appar kan i sig verka misstänkt. Det går sällan att åka buss utan att betala med kort eller resekort och med övervakningskamerorna som är uppsatta av säkerhetsskäl så är det enkelt att kartlägga individers resmönster. Myndigheter behöver visserligen inte ta denna omväg för att fastställa en individs rörelsemönster, uppgifter om var en mobiltelefon befinner sig även när samtal inte görs kan hämtas in via HÖEK.

Myndigheter har stundtals hävdat att enbart insamlandet av information inte utgör ett intrång i sig, i vart fall inte om det sköts av behörig personal, utan att det är först när informationen utnyttjas som ett intrång sker. Som Abrahamsson påpekar så är detta inte i enlighet med lagrådets bedömning. Det stämmer inte heller överens med praxis från Europadomstolens, utifrån uttalande i bl.a. Klass m.fl. mot Tyskland, är det istället så att redan förekomst av lagstiftningen utgör ett intrång. Att det endast är behörig personal som får tillgång till uppgifterna innebär inte att det inte utgör ett intrång, men det kan däremot påverka bedömningen av om lagstiftningen kan rättfärdigas.

Regeringens uppfattning är att uppgifter om vem som haft en viss IP-adresser vid ett visst tillfälle inte är särskilt integritetskänsliga eftersom IP-adresser vanligtvis är dynamiska, och att det därför inte går att dra några slutsatser om en individs allmänna beteende på internet. Samtidigt menar regeringen att uppgifterna är värdefulla för att kunna utreda brott. Datainspektionen menar däremot att dessa uppgifter är särskilt känsliga bland de ”abonnemangsuppgifterna” som går att utfå via 6:22 LEK, eftersom människor generellt sätt gör så mycket mer via internet än över telefon, och att det därför går att utläsa mycket av människors förehavande. Lagstiftaren menar även att lokaliseringsuppgifter är mycket värdefulla för brottsbekämpande myndigheter, men samtidigt inte särskilt integritetskränkande. Frågan är om detta verkligen stämmer, i städer sitter ofta basstationer (och wifi-nät) mycket tätt och det är därför möjligt att få detaljerad information om vilka gator och byggnader som en individ besökt. Frågan är även om lokaliseringsuppgifter som inhämtats via satellit, t.ex. GPS, i dagens läge fortfarande är den vanligaste formen av ”lokaliseringsuppgifter som inte samtidigt är trafikuppgifter”. Sannolikt är positionering via beräkning av avstånd till närbelägna wifi-nät vanligare på många platser i Sverige.

10.2.3 Alla andra länder har tvångsmedlet

Som Ramberg observerat så motiveras tvångsmedel ofta utifrån att andra länder har liknande tvångsmedel. Detta gör t.ex. Hilding Qvarnström, när hon menar att nästan alla andra länder har bestämmelser om buggning och det därför finns en skyldighet för Sverige att inte bli ett ”safe haven” för människor som begår brott. Hilding Qvarnström verkar mena att människor som begår brott i stor utsträckning flyttar över gränser för att undkomma buggning. Utifrån uttalandena i SOU 2012:44, om att människor som begår brott generellt sett inte alls ligger ”steget före” polisen utan istället gör minsta möjliga ansträngning och anpassar sig först när det är nödvändigt, så är frågan om människor som begår brott är så driftiga och välinformerade att de byter land när lagstiftning ändras.

Denna typ av argument som Hilding Qvarnström framför skulle kunna liknas vid en ”alla andra gör det”-argumentation. Saken är dock att bara för att andra länder gör på ett visst sätt innebär det inte att det är rätt i Sverige och passar in i det svenska rättssystemet. Med samma logik skulle det även kunna hävdas att många andra länder tänker om ifråga om datalagring, och att det därför skulle vara rätt väg att gå. På senare tid (2014–2015) kan man nämligen se två parallella riktningar i Europa, samtidigt som den finns en tendens hos domstolar i andra EU-länder och operatörer att ifrågasätta datalagring, är tendensen i Sverige snarast att försvara datalagring samt att permanenta tidsbegränsad tvångsmedelslagstiftning och föreslå utökat tillämpningsområde och nya tvångsmedel.

10.2.4 Tvångsmedlen är effektiva och används bara mot allvarliga brott

Nya tvångsmedel motiveras ofta av att politiker vill visa handlingskraft efter en uppmärksammas händelse såsom ett terrordåd. Terrordåd utgör relativt ovanliga händelser, men trots det utmålas de som ständigt hotande faror. Dessa hotbilder är dåligt underbyggda, enligt Flyghed och Ramberg, och bygger allt för mycket på brottsbekämpande myndigheters egna uppgifter. Detta kan illustreras av Hilding Qvarnström inlägg i debatten, där hon menar att brottsligheten blir värre och grövre medan utredningen som faktiskt undersökte frågan, SOU 2012:44, menar att så inte är fallet.

Det är som tidigare nämnts svårt att bedöma nyttan av de hemliga tvångsmedlen när så få uppgifter lämnas och formen för redovisning och definitionen av nytta ofta ändras. Nyttan av 2007 års preventivlag under 2008–2011 kan i vart fall inte säga vara särskilt stor utifrån vad lagen var tänkt att användas till, nämligen att förhindra brott. I mycket få fall där lagen tillämpats så har det lett till att brott kunnat förhindras, nämligen endast 3 fall (2 %). Lagen har trots detta permanentats, men samtidigt har reglerna ändrats för att förenkla tillämpningen. Detta skedde efter att Säkerhetspolisen länge drivit på för att kraven för att lagen skulle få tillämpas skulle sänkas. Myndigheternas önskemål har alltså fått vara avgörande för lagens utformning.

Hilding Qvarnström menar att hemliga tvångsmedel enbart används mot allvarliga brott som ofta har mycket starka målsägarintressen. Frågan är om detta påstående överensstämmer med myndigheternas redovisningar under de senaste åren. Som framgår av avsnitt 6.1.1 så har narkotikabrott/narkotikasmuggling under de senaste åren varit den överlägset vanligaste brottsmisstanken för vilket tillstånd till HAEK har meddelats. Mönstret är likadant vad gäller inhämtning enligt 2012 års inhämtningslag, med modifikationen att det gällt grovt narkotikabrott och grov smuggling. En del av åren är narkotikabrott/narkotikasmuggling även den vanligaste anledningen till att tillstånd till HÖEK ges.

Nyttan av 2012 års inhämtningslag har enligt redovisningarna framförallt varit att nätverk som handlar med narkotika har kunnat kartläggas och grov narkotikasmuggling har förhindras. Här anges inte någon uppskattning av nyttan utan endast ”anonymiserade fall”. Mycket av kritiken mot nettoredovisningen av HÖEK gör sig även gällande mot redovisningen av nyttan av 2012 års inhämtningslag. Det är dock inte nödvändigt att en tingsrättsdom ska ha meddelats för att ärendet ska kunna vara med i redovisningen, vilket gör att även fall som inte lett till nytta kan redovisas som ett av de ”anonymiserade fallen”.

Att narkotikabrott skulle vara ett grovt brott finns det naturligtvis en hel del människor som påstår, men att påstå att det är ett brott där det finns starka målsägarintressen kan man bara göra om man ser staten eller samhället i stort som ett offer. Detta görs inte inom den defensiva inriktningen av straffrätten, men däremot inom den offensiva.

10.3 Oklara LEK-regler

Reglerna i lagen om elektronisk kommunikation är i viss del oklara. Det är t.ex. oklart vad 6:8 och 6:10a LEK egentligen innebär, och det är svårt att utröna vilka verksamheter som är anpassningsskyldiga enligt 6:19. Likaså finns det frågor vad gäller HAEK och HÖEK enligt RB. Sker t.ex. ”masttömning” när en skäligen misstänkt finns? Används triangulering mot någon som det finns ”synnerlig anledning att anta” att en misstänkt kommer att kontakta? Vad innebär en basstationstömning i praktiken, hur många basstationer kan omfattas och för hur lång tidsperiod kan uppgifter inhämtas?

10.3.1 Alla former av kommunikation omfattas inte

Regleringen av HAEK och HÖEK syftar som sagt till att vara teknikneutral och omfatta ”alla former av kommunikation genom elektroniska kommunikationsnät” (se avsnitt 7). Frågan är om detta stämmer helt med verkligheten. Som angetts så kan HAEK och HÖEK enligt RB inte endast verkställas i allmänna kommunikationsnät (AK-nät), utan även i elektroniska kommunikationsnät (se avsnitt 7.1.2). Skyldigheterna i 6 kap. LEK att samarbeta berör emellertid framförallt tillhandahållare av AK-nät och ATEK-tjänster. Det är bara vissa verksamheter som hanterar uppgifter om elektroniska meddelande som är anpassningsskyldiga enligt 6:19 (se avsnitt 8.6). Ytterligare en grupp av verksamheter är skyldiga att lagra trafikdata enligt 6:16a och anpassningsskyldiga i enlighet med 6:16f (se avsnitt 8.5). Flest verksamheter, nämligen alla tillhandahållare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, träffas av skyldigheten att iaktta tystnadsplikt enligt 6:20 och att lämna ut vissa uppgifter till brottsbekämpande myndigheter enligt 6:22 (se avsnitt 8.4).

Förutom att regleringen i RB omfattar fler nät än som omfattas av skyldigheterna att samarbeta i 6 kap. LEK, så är begreppet “meddelande, som i ett elektroniskt kommunikationsnät överförs…” i RB vidare än begreppet ”elektroniskt meddelande” i 6:1 LEK, vilket endast innefattar de meddelande som överförts genom en ATEK-tjänst. Som framgår av avsnitt 8.2, 8.4 och 9.2, så omfattar regleringen inte heller alla former av vad som ofta ses som kommunikation, t.ex. omfattas inte meddelande via chattprogram, och inte heller alla e-posttjänster (i princip ingen tjänst för webbmail omfattas).

10.3.2 En teknikneutral reglering

Som Hilding Qvarnström påpekar gör det naturligtvis systemet mer tungrott när lagstiftningen uttryckligen avser en viss teknik för kommunikation och därför ständigt måste uppdateras när tekniken förändras. Det är emellertid problematiskt att lagstiftaren inte tydliggör i tekniska termer vad lagstiftningen innebär. Detta leder kanske till mindre arbete för lagstiftaren eftersom lagstiftningen inte blir föråldrad lika fort, men mer arbete för de som ska uttolka lagstiftningen, samt ökad rättsosäkerhet eftersom få straffprocessrättsliga fall tas upp av domstol. Detta leder till att författare av doktrin har att välja mellan att antingen förbigå tekniska beskrivningar, eller riskera att genast bli förbisprungna av teknikutvecklingen. Frågan är om otydligheten i lagstiftningen beror på att lagstiftaren inte har förståelse för tekniken, om det är ett medvetet val för att låta rättstillämpningen lösa problemen eller om det är av ovilja att avslöja metoderna för att människor som begår brott inte ska kunna anpassa sig lika lätt?

Abrahamsson har till viss del rätt i sin kritik av integritetsvännerna, det hänvisas ofta till ”1984” utan egentliga skäl och det förekommer svepande uttalande och overifierade påstående. Jurister ska naturligtvis ta till sig tillgänglig information, men utifrån hur förarbetena och lagarna är skrivna så är det ibland mycket svårt att få en klar bild av vad lagstiftningen innebär vid teknikförändringar. Det är även svårt att veta vad som är tekniskt möjligt i framtiden. Kanske skulle det vara lämpligt att tekniker (eller optimalt tekniska it-jurister) bidrog mer i lagstiftningsarbetet. På så sätt skulle lagstiftningen eventuellt behöva ändras mer sällan.

Europadomstolen menar att lagstiftningen måste var tydlig med vilken teknik som den avser just för att tekniken förändras konstant. Enligt Europadomstolen, och även utifrån legalitetsprincipen, så är det naturligt att en lagregel ibland måste tolkas för att dess rätta mening ska utrönas. Frågan kan dock ställas om den svenska lagstiftarens ambition att vara så teknikneutral som möjligt inte går lite väl långt och därför kommer i konflikt med kraven som Europadomstolen ställer på förutsägbarhet.

10.3.3 Trafikuppgifter och lokaliseringsuppgifter

I förarbetena till 27:19 RB uttrycks inte alltid tydligt vilka uppgifter som enligt LEK:s begreppsbildning kan inhämtas med stöd av de olika typerna av HÖEK, och begreppen används inte alltid på samma sätt som begreppen i LEK. Utifrån hur de olika typerna av HÖEK beskrivs i lagtext och uttalanden i förarbetena så kan det dock göras vissa antaganden om vilka uppgifter som enligt LEK:s begreppsbildning kan inhämtas. Det är primärt tre typer av uppgifter enligt LEK som är relevanta: trafikuppgifter (se 6:1 LEK), lokaliseringsuppgifter som samtidigt är trafikuppgifter, och lokaliseringsuppgifter som inte är trafikuppgifter (se 6:9–10a LEK). Trafikuppgifter är enkelt uttryckt uppgifter som krävs för att förmedla bl.a. samtal, medan lokaliseringsuppgifter är uppgifter om kommunikationsutrustningens geografiska position. Lokaliseringsuppgifter som samtidigt är trafikuppgifter är de uppgifter som krävs för att förmedla ett samtal eller annan kommunikation, medan lokaliseringsuppgifter som inte är trafikuppgifter kan vara t.ex. uppgifter från en GPS-funktion i en telefon.

Troligtvis innebär lagtexten och förarbetsuttalandena om HÖEK och lokaliseringsuppgifternas samband med kommunikation, att 27:19 1 st. 1 ger tillgång trafikuppgifter och lokaliseringsuppgifter som samtidigt är trafikuppgifter, både historiska uppgifter och uppgifter i realtid. Via basstationstömning enligt 27:19 1 st. 2 kan endast historiska uppgifter inhämtas, dock både lokaliseringsuppgifter som samtidigt är trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter. Via lokalisering av viss kommunikationsutrustning enligt 27:19 1 st. 3 kan både historiska uppgifter och realtidsuppgifter inhämtas, både av typen lokaliseringsuppgifter som samtidigt är trafikuppgifter och lokaliseringsuppgifter som inte är trafikuppgifter.

10.4 Nya kommunikationssätt – nya tvångsmedel

Som framgår av avsnitt 9.2 är frågan om hur meddelande via innehållstjänster och informationssamhälletstjänster, såsom sociala medier, hanteras väldigt oklar. Såsom Magnusson beskriver vilka uppgifter som kan inhämtas från Facebook påminner det om regleringen av vad som kan inhämtas via 6:20 och 6:22 LEK, men det är även möjligt att dessa uppgifter istället inhämtats via Facebook Ireland Ltd.

Några säkra slutsatser gällande hur meddelande som skickas via sociala medier hanteras kan dock inte göras, vilket beror på att detta inte varit det primära föremålet för utredning i denna uppsats, att det är svårt att hitta några säkra källor och att det inte heller har funnits plats att utreda detta i någon större utsträckning. Med tanke på områdets växande betydelse, och vikten av att se tvångsmedel och integritetsintrång i ett helhetsperspektiv så skulle detta kunna vara ett område för framtida forskning. Myndigheternas användning av tekniska hjälpmedel som i vissa avseende liknar tvångsmedel, såsom IMSI-fångare, som i praktiken kan inhämta uppgifter om kommunikation, är även det ett intressant område för framtiden. Ett annat område för framtida forskning skulle kunna vara ”hemlig dataavläsning”, som återigen diskuteras som nytt tvångsmedel. Med tanke på utvecklingen efter uppmärksammade händelser såsom terrordåd och politikers vilja att visa handlingskraft finns det risk att historien återupprepar sig och att dessa händelser leder till att en lagstiftning om hemlig dataavläsning införs inom en relativt snar framtid. Min förhoppning är emellertid att detta inte sker, att utspelet om hemlig dataavläsning var ett utspel utan faktiska konsekvenser, ett sätt för politiker att visa handlingskraft för allmänheten utan att införa ett tvångsmedel som skulle innebära en betydligt offensivare straffrättspolitik än i dagens läge. Kostnaden i form av förlust av personlig integritet i fall förslaget skulle bli verklighet skulle nämligen bli mycket stor.

Käll- och litteraturförteckning

BETÄNKANDEN

Ds 2005:6. Brott och brottsutredning i IT-miljö; Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll.

Ds 2014:23. Datalagring, EU-rätten och svensk rätt.

SOU 2005:38. Tillgång till elektronisk kommunikation i brottsutredningar m.m. Delbetänkande av Beredningen för rättsväsendets utveckling (BRU).

SOU 2007:76. Lagring av trafikuppgifter för brottsbekämpning. Betänkande av Trafikuppgiftsutredningen.

SOU 2008:125, Del 1. En reformerad grundlag. Betänkande av Grundlagsutredningen.

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

SOU 2010:103. Särskilda spaningsmetoder. Slutbetänkande av Polismetodutredningen.

SOU 2012:13. En sammanhållen svensk polis. Betänkande av Polisorganisationskommittén.

SOU 2012:44. Hemliga tvångsmedel mot allvarliga brott. Betänkande av Utredningen om vissa hemliga tvångsmedel.

SOU 2013:39. Europarådets konvention om it-relaterad brottslighet. Betänkande av Utredningen om it-brottskonventionen.

SOU 2015:31. Datalagring och integritet. Betänkande av Datalagringsutredningen.

PROPOSITIONER

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

Prop. 2001/02:150 Lag om elektronisk handel och andra informationssamhällets tjänster, m.m.

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

Prop. 2002/03:110 Lag om elektronisk kommunikation, m.m.

Prop. 2009/10:80 En reformerad grundlag.

Prop. 2010/11:46 Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG.

Prop. 2010/11:115 Bättre regler för elektroniska kommunikationer.

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

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

ÖVRIGT OFFENTLIGT TRYCK

Dir. 2014:101. Översyn av vissa bestämmelser om elektronisk kommunikation i brottsbekämpningen

Skr. 2011/12:39. Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2010.

Skr. 2012/13:47. Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2011.

Skr. 2013/14:60. Redovisning av användningen av vissa hemliga tvångsmedel under år 2012.

Skr. 2014/15:36. Redovisning av användningen av vissa hemliga tvångsmedel under år 2013.

Skr. 2014/15:146. Förebygga, förhindra och försvåra – den svenska strategin mot terrorism.

Justitiedepartementet, Dnr. Ju2014/3010/P. (”Uppdrag med anledning av EU-domstolens dom om datalagringsdirektivet”)

MYNDIGHETSRAPPORTER, VÄGLEDNINGAR OCH YTTRANDE

(Länkarna nedan har kontrollerats, och i vissa fall, uppdaterats 2016-02-04)

Datainspektionen

Datainspektionen (2015). ”Datalagring och integritet (SOU 2015:31)”, remissvar, datum 2015-08-28, Dnr: 902-2015.
http://www.datainspektionen.se/Documents/remissvar/2015-09-03-yttrande-datalagring.pdf

Post- och telestyrelsen

PTS (2007). ”Kostnader p.g.a. nya krav på hemlig avlyssning och övervakning av ”internettjänster” m.m.”, Dnr: 07-571, datum 2007-02-7
http://www.pts.se/upload/Documents/SE/hemlig_teleavlyssning_pm_07_571_070207.pdf

PTS (2009). ”Vilka tjänster och nät omfattas av LEK? En vägledning”, PTS-ER-2009:12, datum 2009-03-11
http://www.pts.se/upload/Rapporter/Internet/2009/ekomtjanster-2009-12.pdf

PTS (2012). ”Uppgifter som ska lagras för brottsbekämpande ändamål – en vägledning”, (utan Dnr.), datum 2012-05-23
http://www.pts.se/upload/Ovrigt/Internet/Tradala/Vagledning_Uppgifter-som-ska-lagras-for-brottsbekampande-andamal.pdf

PTS (2013). ”Konsekvensutredning avseende föreskrifter om ersättning vid utlämnande av lagrade uppgifter för brottsbekämpande ändamål”, Dnr: 12-4585, datum 2013-06-10
http://www.pts.se/upload/Remisser/2013/remiss-ersattningsforeskrifter/Konsekvensutredning-trafikdatalagring-TMP.pdf

PTS (2015). ”Svensk telemarknad 2014”, PTS-ER 2015:19, datum 2015-05-25
http://www.pts.se/upload/Rapporter/Tele/2015/Svensk-telemarknad-2014.pdf

PTS (2015). ”Vägledning för anmälan av anmälningspliktig verksamhet”, (utan Dnr.), datum 2015-01-08
http://www.pts.se/upload/Ovrigt/Tele/Anmalningsplikt/vagledning-for-anmalan-av-verksamhet-2015.pdf

PTS (2016). “Anmälda enligt 2 kap. 1§LEK”, datum 2016-01-15
https://www.pts.se/upload/Ovrigt/Tele/Bransch/anmalda-operatorer.pdf

Åklagarmyndighetens rapporter

Åklagarmyndigheten (2011). ”Hemlig teleavlyssning m.m. vid förundersökning avseende grova brott år 2010 samt återrapportering enligt 2011 års regleringsbrev”, Dnr. ÅM-A 2010/1867, 2011/0111
https://www.aklagare.se/globalassets/dokument/ovriga-rapporter/2011_-_hemlig_teleavlyssning_m.m..pdf

Åklagarmyndigheten (2012). ”Reviderad redovisning av användningen av hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning i förundersökningar under 2011”, Dnr. ÅM-A 2012/0505
https://www.aklagare.se/globalassets/dokument/ovriga-rapporter/2012_-_redovisning_av_hemliga_tvangsmedel.pdf

Åklagarmyndigheten (2013). ”Redovisning av användning av vissa hemliga tvångsmedel under 2012”, Dnr: ÅM-A 2013/0196
https://www.aklagare.se/globalassets/dokument/ovriga-rapporter/2013_-_anvandning_av_vissa_hemliga_tvangsmedel_ar_2012.pdf

Åklagarmyndigheten (2014). ”Redovisningen av användningen av visa hemliga tvångsmedel under 2013”, Dnr: ÅM-A 2013/1962
https://www.aklagare.se/globalassets/dokument/ovriga-rapporter/2014_-_rapport_om_anvandning_av_vissa_hemliga_tvangsmedel_ar_2013.pdf

Åklagarmyndigheten (2015). ”Redovisning av användning av vissa hemliga tvångsmedel under 2014”, Dnr: ÅM-A 2014/1569
https://www.aklagare.se/globalassets/dokument/ovriga-rapporter/2015_-_rapport_om_anvandning_av_vissa_hemliga_tvangsmedel_ar_2014.pdf

IRLÄNDSKA TILLSYNSMYNDIGHETEN FÖR DATASKYDD

(Länkarna nedan har kontrollerats 2016-02-04)

Data Protection Commissioner (2011). ”Facebook Ireland Ltd: Report of Audit”, datum 2011-12-21
https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf

Data Protection Commissioner (2012). ”Facebook Ireland Ltd: Report of Re-Audit”, datum 2012-09-21
https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

LITTERATUR

Abrahamsson, Olle (2009). ”Integritetsskydd med eller utan förnuft” I: *SvJT* 2009 s. 421–434.

Cameron, Iain (2014). *An introduction to the European Convention on Human Rights*. 7. uppl., Uppsala: Iustus.

Ekelöf, Per Olof, Bylund, Torleif & Edelstam, Henrik (2006). *Rättegång III.* 7., [rev.] uppl., Stockholm: Norstedts juridik.

Flyghed, Janne (2007). ”Kriminalitetskontroll – baserad på tro eller vetande?” i: *SvJT* 2007 s. 59–68.

Flyghed, Janne (2015). ”Nya aktörer och ny teknik i kontrollandskapet” i: Agrell, Wilhelm (red.): *Övervakning och integritet – en antologi*, Karlstad: Myndigheten för Samhällsskydd och beredskap, s. 55–69. (urn:nbn:se:su:diva-117535)
https://www.msb.se/Upload/konferenser/%C3%96vervakning%20och%20integritet%202015/Rapport%20till%20MSB.pdf

Hilding Qvarnström, Agnetha (2007). ”Rättssäkerhet och integritet – hur ser det ut i Sverige? Tankar ur ett åklagarperspektiv” I: *SvJT* 2007 s. 136–140.

Jareborg, Nils (1994). ”Defensiv och offensiv straffrättspolitik”, I: *Nordisk tidsskrift for kriminalvidenskab*, årg. 81, nr. 1, s. 41–53.

Jareborg, Nils (1995). ”Vilken sorts straffrätt vill vi ha? Om defensiv och offensiv straffrättspolitik.” I: Victor, Dag, (red.): *Varning för straff: Om vådan av den nyttiga straffrätten*, Stockholm: Norstedts Juridik.

Lindberg, Gunnel (2007). ”Straffprocessuella tvångsmedel – några utvecklingslinjer” I: *SvJT* 2007 s. 50–58.

Nergelius, Joakim (2014). *Svensk statsrätt*. 3. uppl., Lund: Studentlitteratur.

Ramberg, Anne (2007). ”Tvångsmedel, rättssäkerhet och integritet – går det att förena?” I: *SvJT* 2007 s. 154–170.

Westerlund, Gösta (2013). *Straffprocessuella tvångsmedel: en studie av rättegångsbalkens 24 till 28 kapitel och annan lagstiftning*. 5. uppl., Stockholm: Bruun.

WEBBSIDOR OCH TIDNINGSARTIKLAR FRÅN WEBBEN

(Länkarna nedan har kontrollerats, och i vissa fall, uppdaterats 2016-02-04)

Bahnhof (2014). ”Vi anmäler Sveriges datalagring till EU-kommissionen” (webbsida), publicerad 2014-09-12.
https://www.bahnhof.se/press/press-releases/2014/09/12/vi-anmaler-sveriges-datalagring-till-eu-kommissionen

Berger, Ella (2015). ”Terrorforskaren: ”En genomarbetad strategi”” (webbsida), Svt Nyheter, publicerad 2015-08-28.
http://www.svt.se/nyheter/inrikes/terrorforskaren-en-genomarbetad-strategi

Berger, Ella och Bering, Sofia (2015). ”Strategin ”ett hot mot den demokratiska rättsstaten”” (webbsida), Svt Nyheter, publicerad 2015-08-28.
http://www.svt.se/nyheter/inrikes/strategin-ett-hot-mot-den-demokratiska-rattsstaten

Kleja, Monica (2015). ”Spiontrojan kan bli polisens nya verktyg” (webbsida), NyTeknik, publicerad 2015-08-28.
http://www.nyteknik.se/tekniknyheter/article3926150.ece

Magnusson, Kerstin (2014). ”De har nyckeln till näthatarna” (webbsida), Svensk Polis – En tidning från Rikspolisstyrelsen, publicerad 2014-06-30.
http://www.svenskpolis.se/Artikelarkiv/Artiklar-2014/Juni-2014/De-har-nyckeln-till-nathatarna/

Näfver, Malin (2014). ”Polisen och Facebook i samarbete mot näthat” (webbsida), nyhet från Rikspolisstyrelsen, publicerad 2014-10-27.
https://polisen.se/Arkiv/Nyhetsarkiv/Gemensam/Polisen-och-Facebook-i-samarbete-mot-nathat/

PTS (2014). ”PTS kommer inte i nuläget att vidta åtgärder utifrån datalagringsreglerna” (webbsida), publicerad 2014-04-10.
http://www.pts.se/sv/Nyheter/Telefoni/2014/PTS-kommer-inte-i-nulaget-att-vidta-atgarder-utifran-datalagringsreglerna/

PTS (2016). ”Operatörer” (webbsida).
https://www.pts.se/sv/Bransch/Telefoni/Anmalningsplikt/Operatorer---anmalda-och-avanmalda/

Uttersköld, Stephan (2011). ”Bra kompetens för internetrelaterade brott” (webbsida), Svenska Dagbladet, publicerad 2011-08-11.
http://www.svd.se/opinion/vi-har-bra-kompetens-for-internetrelaterade-brott_6382678.svd

Förteckning över rättsfall och beslut

HÖGSTA DOMSTOLEN

NJA 1998 s. 829

NJA 2003 s. 107

RÄTTSFALL FRÅN KAMMARRÄTTER

RK 2010:1 (Kammarrätten i Stockholm)

Kammarrätten i Stockholm, mål nr. 7380-14, beslut 2015-04-28.

FÖRVALTNINGSRÄTTEN I STOCKHOLM

Förvaltningsrätten i Stockholm, mål nr. 14891-14, dom 2014-10-13.

JUSTITIEKANSLERN

JK-beslut 2008-08-15 Dnr: 6545-06-21. (”Fråga om s.k. lokaliseringsuppgifter från mobiltelefoner får inhämtas som ett led i hemlig teleövervakning m.m.”)

EU-DOMSTOLEN

Digital Rights Ireland m.fl., förenade målen C-293/12 och C-594/12, ännu ej publicerat i EUT, (ECLI:EU:C:2014:238).

EUROPADOMSTOLEN FÖR MÄNSKLIGA RÄTTIGHETER

Copland mot Förenade kungariket, no. 62617/00, dom 3 april 2007, ECHR 2007-I, (ECLI:CE:ECHR:2007:0403JUD006261700).

Khan mot Förenade kungariket, no. 35394/97, dom 12 maj 2000, ECHR 2000-V, (ECLI:CE:ECHR:2000:0512JUD003539497).

Klass m.fl. mot Tyskland, no. 5029/71, dom 6 september 1978, Series A no. 28, (ECLI:CE:ECHR:1978:0906JUD000502971).

Kopp mot Schweiz, no. 23224/94**,** dom 25 mars 1998, ECHR 1998-II, (ECLI:CE:ECHR:1998:0325JUD002322494).

Liberty m.fl. mot Förenade kungariket, no. 58243/00, dom 1 juli 2008, (ECLI:CE:ECHR:2008:0701JUD005824300).

Malone mot Förenade kungariket, no. 8691/79, dom 2 augusti 1984, Series A no. 82, (ECLI:CE:ECHR:1984:0802JUD000869179).

P.G. och J.H. mot Förenade kungariket, no. 44787/98, dom 25 september 2001, ECHR 2001-IX, (ECLI:CE:ECHR:2001:0925JUD004478798).

Uzun mot Tyskland, no. 35623/05, dom 2 september 2010, ECHR 2010, (ECLI:CE:ECHR:2010:0902JUD003562305).

Weber och Saravia mot Tyskland, no. 54934/00, beslut 29 juni 2006, ECHR 2006-XI, (ECLI:CE:ECHR:2006:0629DEC005493400).

RÄTTSFALL FRÅN ANDRA EUROPEISKA LÄNDER

Storbritannien

David Davis MP case UK, Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014, https://www.judiciary.gov.uk/judgments/david-davis-and-others-v-secretary-of-state-for-the-home-department/

Belgien

Cour constitutionelle, n°84/2015, 11/06/2015
http://www.europeanrights.eu/index.php?lang=eng&funzione=S&op=2&id=4401

Nederländerna

Rechtbank Den Haag, C09/480009/KG ZA 14/1575 (ECLI:NL:RBDHA:2015:2498)
http://www.europeanrights.eu/index.php?funzione=S&op=2&id=4288