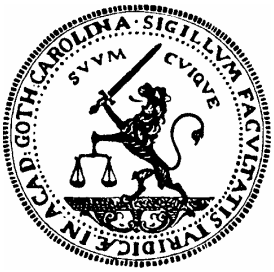

JURIDISKA FAKULTETEN
vid Lunds universitet

Pontus Eriksson

Datalagring och personlig integritet –
En analys av datalagringsdirektivets genomförande i Sverige

Examensarbete
30 högskolepoäng

Handledare
Helén Örnemark Hansen

Ämnesområde
Straffrätt, Processrätt

Termin
HT 2008

Innehåll

Summary

Data storage and privacy - Implementation of the Data Retention Directive in Sweden

The main purpose of the essay is to determine whether the Swedish proposal for the implementation of the so-called Data Retention Directive contains adequate protection for privacy.

In March 2006 the Data Retention Directive was adopted within the EU. The directive aims to harmonize national legislation regarding the storage of data generated or processed in different kinds of communication in order to make this information available for the purpose of the investigation, detection and prosecution of serious crime. In May 2006, a government investigation was appointed to submit a proposal on how the directive should be implemented in Swedish law. The result of this investigation was presented by the Traffic Data Inquiry (Trafikuppgiftsutredningen) at the end of 2007.

The Data Retention Directive represents an extraordinary measure, without any historical counterpart because it leads to a very comprehensive registration of people’s communication without any suspicion of crime. As a legal obligation to store such data will be introduced the directive and the subsequent founding of national legislation will result in a weakening of the protection of privacy. In the present case this weakening has been justified because the interest of an effective law enforcement of serious crimes is considered to outweigh privacy.

The national legislators are mostly bound by the regulations in the Data Retention Directive and are thus in most parts prevented to affect the privacy intrusion that the storage of traffic data brings with it. The main focus of this essay is directed towards one of the areas not covered in detail in the directive, but instead forwarded to each Member State to regulate; the authorities' access to the stored information. The solution that the Traffic Data Inquiry advocated in this part means that the existing legal framework, which allows law enforcement authorities to gain access to the stored traffic data in Sweden, also will apply to the extended storage that is introduced with the Data Retention Directive. At present, Swedish law contains two parallel legal frameworks that allow such access, the rules about secret telecommunication surveillance (hemlig teleövervakning) and the rules for exceptions from confidentiality in the Electronic Communications Act (lagen om elektronisk kommunikation). These sets of rules, however, show significant differences in legal security and in the protection of privacy, differences that by imposing the directive will increase significantly in importance.

I believe that the Traffic Data Inquiry did not take the protection of privacy into sufficient consideration in its proposal, since no approach was made to resolve the differences in these existing legal frameworks, despite their vital role. A change should be required for Sweden to clearly live up to the European Convention's demands on restrictions of the right to respect for correspondence and access to an effective national remedy.

Sammanfattning

Det övergripande syftet med uppsatsen är att utröna huruvida det svenska förslaget till genomförandet av det s.k. datalagringsdirektivet innehåller tillräckligt skydd för den personliga integriteten.

I mars 2006 antogs datalagringsdirektivet inom EU. Direktivet syftar till att harmonisera medlemsstaternas lagstiftning angående lagring av vissa uppgifter som genereras eller behandlas vid olika slags kommunikation i syfte att göra denna information tillgänglig för utredning, avslöjande och åtal av allvarliga brott. I maj 2006 tillsattes en statlig utredning för att lämna förslag på hur direktivet ska genomföras i svensk rätt. Resultatet av denna presenterades av Trafikuppgiftsutredningen i slutet av 2007.

Datalagringsdirektivet innebär en extraordinär åtgärd utan historisk motsvarighet i det avseende att det innebär en mycket omfattande registrering av enskildas kommunikation utan krav på brottsmisstanke. Då en lagstadgad skyldighet att lagra sådana uppgifter kommer att införas innebär direktivet och den därpå grundade nationella lagstiftningen att skyddet för den personliga integriteten kommer att försvagas. Denna försvagning har i förevarande fall motiverats genom att intresset av en effektiv brottsbekämpning av allvarlig brottslighet ansetts väga tyngre än integritetsskyddet.

I stora delar är de nationella lagstiftarna bundna av datalagringsdirektivets bestämmelser och således förhindrade att i dessa delar påverka det integritetsintrång som lagringen av trafikuppgifter innebär. Uppsatsens huvudsakliga fokus riktas dock mot ett av de områden som inte reglerats närmare i direktivet utan istället överlämnats till varje medlemsstat att reglera, nämligen myndigheters rätt att få tillgång till den lagrade informationen. Den lösning som Trafikuppgiftsutredningen förespråkat i denna del innebär att de existerande regelverk som tillåter brottsbekämpande myndigheter att få tillgång till lagrade trafikuppgifter i Sverige även ska gälla för den utökade lagring som införandet av datalagringsdirektivet innebär. Svensk rätt innehåller i nuläget två parallella regelverk som tillåter sådan tillgång; reglerna om hemlig teleövervakning och reglerna om undantag från tystnadsplikt i lagen om elektronisk kommunikation. Dessa båda regelverk uppvisar dock stora skillnader från rättssäkerhetssynpunkt och i fråga om skydd för den personliga integriteten, skillnader som genom direktivets införande kommer att öka markant i betydelse.

Jag menar att Trafikuppgiftsutredningen i sitt förslag inte beaktat skyddet för den personliga integriteten i tillräckligt hög grad då ingen ansats gjorts för att utjämna skillnaderna i dessa två regelverk, trots deras väsentliga betydelse. En förändring bör krävas för att Sverige klart ska kunna sägas

leva upp till Europakonventionens krav på inskränkningar i rätten till respekt för korrespondens och tillgång till effektivt nationellt rättsmedel.

Förord

Med detta examensarbete avslutar jag studierna vid Juridiska Fakulteten vid Lunds universitet. Jag vill ta tillfället i akt och rikta ett varmt och innerligt tack till min familj som alltid stöttat mig på olika sätt, i studierna och i livet. Jag vill även tacka alla vänner som förgyllt min tillvaro under de gångna åren och gjort studierna lättare att ta sig igenom. Ett särskilt kärleksfullt tack vill jag rikta till min Anna, ditt stöd och din kärlek betyder allt för mig! Slutligen, ett stort tack till min handledare, Helen Örnemark Hansen, för vägledning och goda råd under arbetets gång.

Lund, januari 2009

Pontus Eriksson

Förkortningar

BrB	Brottsbalken
BRU	Beredningen för rättsväsendets utveckling
Dir	Direktiv
Dnr	Diarienummer
Ds	Departementsserien
Ds Ju	Departementsserien (Justitiedepartementet)
EKMR/Europakonventionen	Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna
EG	Europeiska Gemenskapen
EU	Europeiska Unionen
JK	Justitiekanslern
JO	Justitieombudsmannen
LEK	Lag (2003:389) om elektronisk kommunikation
Prop.	Proposition
PTS	Post- och telestyrelsen
RB	Rättegångsbalken (1942:740)
RF	Regeringsformen (1974:152)
SekrL	Sekretesslag (1980:100)
Skr.	Skrivelse (Regeringens skrivelse)
SOU	Statens offentliga utredningar
SvJT	Svensk Juristtidning

1 Inledning

1.1 Bakgrund

Den 11 mars 2004 skedde en omfattande terrorattack i den spanska huvudstaden Madrid då ett flertal sprängladdningar exploderade på pendeltåg och tågstationer. Efter terrordåden fördes en intensiv debatt inom EU om hårdare lagstiftning och utökade polisbefogenheter i kampen mot terrorism och allvarlig brottslighet. En åtgärd som bl.a. diskuterades var att införa en skyldighet för teleoperatörer att lagra information om sina kunders kommunikationer. Informationen som avsågs var s.k. trafikuppgifter som genereras vid i stort sett varje elektronisk kommunikation och därmed innefattar exempelvis fast-, mobil- och internettelefoni, e-post och telefaxmeddelande. Informationen anger bl.a. vem som har kommunicerat med vem, vid vilken tidpunkt kommunikationen ägde rum och var personerna som kommunicerade befann sig. Syftet med lagringen av trafikuppgifter är att dessa senare ska kunna användas av brottsbekämpande myndigheter i kampen mot allvarlig brottslighet. Ett förslag angående trafikuppgiftslagring arbetades fram men mötte hårt motstånd från olika håll och kritiserades för att vara för integritetskränkande. Förslaget röstades senare ner av Europaparlamentet.

Lite mer än ett år efter attentaten i Madrid skedde en ny terrorattack i Europa. På morgonen den 7 juli 2005 detonerade sprängladdningar på tre olika tunnelbanelinjer och på en stadsbuss i centrala London. Dessa bombattentat väckte nytt liv i förslaget om lagring av trafikuppgifter vilket slutligen ledde fram till att det s.k. datalagringsdirektivet antogs den 15 mars 2006.

Den 18 maj 2006 utsågs Ekobrottsmyndighetens generaldirektör, Gudrun Antemar, till särskild utredare för datalagringsdirektivets implementering i Sverige. Utredningen tog namnet Trafikuppgiftsutredningen och lade fram sitt betänkande i november 2007. Betänkandet bereds för närvarande inom Regeringskansliet.

1.2 Syfte och frågeställningar

I denna uppsats har jag för avsikt att granska det svenska förslaget till genomförande av datalagringsdirektivet. Det övergripande syftet med denna granskning är att närmare analysera hur väl skyddet för den personliga integriteten är tillgodosedd i vissa delar av förslaget.

Införandet av datalagringsdirektivet i svensk rätt kommer att innebära en lagring av information om alla privatpersoners elektroniska kommunikation i en väsentligt större utsträckning än vad som är fallet i dag. Dessa uppgifter

ska senare kunna lämnas ut till myndigheter för att användas i syfte att bekämpa allvarlig brottslighet. Denna utlämning ska enligt det liggande förslaget regleras genom de existerande svenska bestämmelserna utan att dessa genomgår några förändringar. Det svenska rättsystemet innehåller för tillfället två parallella regelverk som var för sig reglerar myndigheters tillgång till lagrade trafikuppgifter; rättegångsbalken och lagen om elektronisk kommunikation. Trots att dessa båda regelverk har samma användningsområde uppvisar de stora skillnader vad gäller främst hur skyddet för den personliga integriteten tillgodoses samt vilka rättssäkerhetsgarantier som omgärdar respektive process. Genom den ökning av lagringsvolym som införandet av datalagringsdirektivet kommer att innebära följer att dessa regelverk med största sannolikhet kommer utnyttjas i mycket större utsträckning efter direktivets genomförande än vad som skett hittills. Med detta i beaktande preciseras mitt syfte närmare i två frågeställningar. Den första rör de två parallella regelverken:

- På vilket sätt skiljer sig de existerande regelverken för utlämnande av trafikuppgifter sig åt i fråga om skydd för den personliga integriteten samt omgärdande rättssäkerhetsgarantier?

Både datalagringsdirektivet och Trafikuppgiftsutredningens förslag tog sin utgångspunkt i Europakonventionens bestämmelser angående skydd för enskildas personliga integritet. Det är därför av intresse att se närmare på hur väl Trafikuppgiftsutredningens förslag står i överensstämmelse med Europakonventionens bestämmelser. Detta behandlas i den andra frågeställningen:

- Uppfyller det svenska implementeringsförslaget de krav som uppställs i Europakonventionen på skydd av rätten till privatliv och korrespondens samt tillgång till effektivt nationellt rättsmedel, särskilt med beaktande av skillnaderna mellan regelverken för utlämnande av trafikuppgifter?

1.3 Metod och material

Den metod jag använt mig i författandet av uppsatsen är traditionell juridisk metod. Detta innebär att jag tagit utgångspunkt i skriven lag och genom förarbeten, praxis och doktrin sökt förklara och förtydliga denna. Framställningen är till stora delar av deskriptiv karaktär, särskilt i de inledande avsnitten. I de senare avsnitten sammanflätas vad som framkommit med mina egna analyser och reflektioner.

Materialet består företrädesvis av offentligt tryck och doktrin. Trafikuppgiftsutredningens betänkande, SOU 2007:76 - *Lagring av trafikuppgifter för brottsbekämpning*, har naturligtvis en framträdande roll eftersom detta utgör hörnstenen för hela uppsatsen. Reglerna om hemlig teleövervakning har dessutom genomgått ett flertal förändringar sedan dess införande i rättegångsbalken varvid flera aspekter som är av betydelse för

uppsatsen på något vis har diskuterats. Det har därför varit av stor betydelse att behandla dessa förarbeten och redogöra för vissa av de ståndpunkter som framkommit däri. Rättspraxis har använts i begränsad omfattning och den praxis som har använts härrör främst från Europadomstolen. Uppsatsen kommer i detta hänseende behandla vad som kan utläsas av dessa rättsfall och således refereras de inte i sin helhet.

1.4 Avgränsningar

Det svenska lagförslaget innehåller ett flertal avvägningar som, direkt eller indirekt, påverkar den personliga integriteten för svenska medborgare. Ett examensarbete är dock begränsat både i tid och utrymme och alla dessa avvägningar kommer därför inte att behandlas. Huvudsakligen fokuseras arbetet på den delen av lagförslaget jag anser vara av störst betydelse ur en integritetsskyddsaspekt, d.v.s. reglerna om utlämnande av lagrade trafikuppgifter. Denna del är dessutom av speciellt intresse då frågan inte regleras närmare i direktivet och således är helt lämnad åt den nationelle lagstiftaren att besluta om. Andra integritetskänsliga delar, t.ex. förslaget om att vissa omständigheter ska förmedlas i form av förordning istället för lag, berörs istället endast helt kort.

För de bestämmelser som reglerar myndigheters tillgång till trafikuppgifter kommer jag endast att behandla reglerna i rättegångsbalken och de i lagen om elektronisk kommunikation och således inte de motsvarande reglerna i sekretesslagen. Reglerna i den sistnämnda lagen överlappar de andra båda men har av olika skäl i stort förlorat sin praktiska betydelse för den brottsbekämpande verksamheten och faller därför utanför syftet med arbetet.

Vad gäller reglerna i lagen om elektronisk kommunikation kommer inte regleringen av trafikuppgifter i form av uppgift om abonnemang, s.k. ”kataloguppgifter”, att behandlas närmare då dessa är mindre känsliga ur integritetssynpunkt. Kataloguppgifter är sådana som namn, titel, adress och abonnentnummer, d.v.s. sådana uppgifter som för de allra flesta nummer finns tillgängliga för både enskilda och myndigheter genom telefonkatalog eller andra tjänster för abonnentupplysning.

1.5 Disposition

Uppsatsen består av nio kapitel. Efter inledningen följer ett kapitel om personlig integritet där betydelsen av begreppet diskuteras och skyddet i svensk grundlag presenteras. I *kapitel 3* presenteras det EG-direktiv som är grunden för det aktuella svenska lagförslaget, datalagringsdirektivet. I det efterföljande *kapitel 4* redogörs för hur det svenska implementeringsförslaget ser ut. *Kapitel 5* handlar främst om hemlig teleövervakning och förutsättningarna för dess användning. Kapitlet inleds dock med en mer allmän del där betydelsen av straffprocessuella

tvångsmedel och de principer som styr dess användande förklaras. *Kapitel 6* innehåller en kortfattad genomgång av det andra aktuella regelverket för utlämnande av trafikuppgifter, lagen om elektronisk kommunikation. Kapitlet är främst inriktat på den del av lagen som berör integritetsskydd och regler för utlämnande av uppgifter.

Kapitel 7 skiljer sig delvis åt från de tidigare kapitlen då det inte är av lika strikt deskriptiv karaktär. I kapitlet görs en jämförelse mellan hemlig teleövervakning och lagen om elektronisk kommunikation i fråga om reglerna för utlämnande av trafikuppgifter med fokus på skillnader i skyddet för den personliga integriteten och rättssäkerhetsgarantier regelverken emellan. Därmed har kapitlet nära anknytning till den första av mina frågeställningar. *Kapitel 8* redogör för innehållet i Europakonventionens skydd för den personliga integriteten (artikel 8) samt rätten till effektivt rättsmedel (artikel 13). I direkt anslutning till presentationen av respektive artikel görs även en genomgång av relevant rättspraxis från Europadomstolen. Uppsatsen avslutas med en analys i *kapitel 9*.

1.6 Vissa begreppsbestämningar

För att underlätta läsningen av uppsatsen har jag emellanåt gjort förenklingar av vissa begrepp. Ofta benämner jag exempelvis hemlig teleövervakning som bara teleövervakning. Det förutsätts dock att den är hemlig om inget annat direkt framgår. När polisen omnämns är det den öppna polisen som avses, i annat fall skrivs det uttryckligen att det är säkerhetspolisen som menas.

Som ett samlingsnamn på de olika myndigheter som har möjlighet att begära ut lagrade trafikuppgifter används begreppet brottsbekämpande myndigheter i stor utsträckning. Vad gäller tvångsmedelsanvändning sker denna i huvudsak för att utreda begångna brott, trots att ett preventivt användande i vissa situationer är tillåtet. En mer adekvat beskrivning av denna verksamhet hade möjligen varit ”brottsutredande myndigheter” då det i ordet bekämpning kan anses ligga åtgärder som företas i förebyggande syfte. Reglerna i lagen om elektronisk kommunikation kan dock användas innan det bedrivs någon förundersökning och således i andra fall än för utredning av händelser i förfluten tid. I det svenska lagförslaget angående datalagringsdirektivets införande i Sverige används begreppet ”brottsbekämpande myndigheter” i störst utsträckning och för enkelhetens skull har jag valt att göra detsamma i denna uppsats.

2 Personlig integritet

För att kunna värdera bedömningen avseende skyddet för den personliga integriteten som gjorts i utredningen angående datalagringsdirektivets genomförande i svensk rätt är det behövligt att fördjupa sig i vad begreppet ”personlig integritet” innebär. Någon entydig definition av begreppet har inte kunnat formuleras, trots att försök gjorts. En förklaring kan vara att betydelsen är beroende av i vilken kontext begreppet används och varierar beroende på tid, rum och även från person till person. Trots att begreppets omfattning och specifika innehåll inte bestämts allmängiltigt är innebörden oerhört viktig och står för en del av våra grundläggande rättigheter. Dessa rättigheter är för svensk del bl.a. lagfästa på grundlagsnivå och skyddade genom Europakonventionen. Man skulle kunna hävda att begreppet är lika starkt i sin innebörd som det språkligt sett är vagt.

I detta kapitel kommer jag att redogöra för hur begreppet kan beskrivas samt ge ett par exempel på försök till definitioner. Vidare kommer det skydd som garanteras genom bestämmelserna i regeringsformen att presenteras och slutligen presenteras den nyligen gjorda integritetsskyddsutredningen.

2.1 Begreppet integritet

Själva ordet integritet härstammar från det latinska ”integer” vilket betyder hel eller ren och innebär okränkbarhet, oberoende och frihet från inblandning eller obehörig påverkan. Betydelsen som nu avses med personlig integritet uppkom i slutet av 1800-talet då det motsvarande engelska begreppet ”privacy” myntades genom en artikel i Harvard Law Review, betitlad ”The Right to Privacy”. Författarna var de två amerikanska juristerna Samuel Warren och Louis Brandeis och bakgrunden till artikeln var författarnas upprördhet över utvecklingen i de amerikanska tidningarna som allt mer närgånget granskade framgångsrika människors privatliv. Syftet med artikeln var att hävda en rätt att bli lämnad ifred, ”*the right to be let alone*”.[1]

Att ge en entydig och allmänt accepterad definition av vad som innefattas under begreppet personlig integritet - eller liknande systerbegrepp som den privata sfären eller privatlivets helgd – är svårt av olika anledningar. Uppfattningen om vad som bör innefattas är bl.a. ett resultat av en samhällelig kontext och skiljer sig därför åt mellan olika platser och förändras dessutom i takt med tidens gång och den allmänna samhällsutvecklingen. Synen på vad som innefattas kan även skilja mellan olika personer och grundas på subjektiva faktorer som upplevelser, känslor

[1] SOU 1987:74, s. 45, Lännergren, Bengt, *Om integritet*, SvJT 1979, s. 161, Helmius, Ingrid, *Polisens rättsliga befogenheter vid spaning*, s. 98.

och värderingar.[2] Som en följd härav kan en rad olika situationer eller förfarande utgöra eller upplevas som ett angrepp på någons person eller personliga integritet. Det kan exempelvis röra sig om personliga eller känsliga uppgifter som blir offentliga, övervakning i form av kameror på vissa platser, fysiska eller psykiska övergrepp eller en kränkning av hemfriden genom ett inbrott.[3] Att begreppet är applicerbart på en så stor variation av företeelser eller situationer utgör ett hinder då man försöker ringa in begreppets betydelse. Definitionen tenderar att antingen vara för vid och därför endast utgöra en allmän beskriven rättighet att bli lämnad ifred eller alldeles för snäv och istället ange en rättighet för var och en att i varje situation samtycka till en viss åtgärd.[4]

2.2 Tidigare försök till definitioner

Det har gjorts ett flertal försök att konstruera en entydig definition av integriteten och vad som ryms under begreppet. Det har bl.a. gjorts försök att finna en positiv bestämning av uttrycket vilket dock visat sig vara problematiskt. Ansatser har gjorts att exempelvis fastställa vad som hör till den enskilda sfären eller privatlivet och till det offentliga livet och därigenom dra slutsatser om integritetens omfattning. Dessa försök har generellt sett varit mindre lyckade då det visat sig svårt att finna en positiv definition som är konsekvent samtidigt som den är heltäckande. Som exempel kan nämnas det förhållande att det handlande som för en person utgör något absolut privat istället kan uppfattas som något offentligt då det utförs av exempelvis en politiker eller av någon annan offentlig person.[5]

Istället för att finna en positiv begreppsbestämning har Stig Strömholm försökt beskriva innebörden negativt, genom att göra en uppställning av vilka handlingar som kan anses utgöra en integritetskränkning. Utan ambitionen att verka uttömmande har en kränkningskatalog bestående av 14 punkter framställts:

1. tillträde till och genomsökande av privata lokaler eller annan egendom;
2. kroppsundersökning;
3. medicinska undersökningar, psykologiska tests osv.;
4. intrång i en persons privata sfär genom skuggning, spionerande, telefonterror o.d.;
5. som ett särfall till grupp 1 och 4; ofredande genom företrädare för massmedierna;
6. olovlig ljudupptagning, fotografering eller filmupptagning;
7. brytande av brevhemligheter;
8. telefonavlyssning;
9. utnyttjande av elektronisk avlyssningsapparatur;

[2] Helmius, s. 97, SOU 2007:22 del 1, s. 53.
[3] Collste, Göran, *Behandling av personuppgifter och personlig integritet: En etisk analys* , i SOU 1997:39, *Integritet – Offentlighet – Informationsteknik*, bilaga 4, s. 789f., SOU 1984:54, s. 42.
[4] Freese, Jan m.fl., *Privatlivets helgd. Tillåtet och otillåtet enligt datalagen, kreditupplysningslagen och inkassolagen,* s. 16.
[5] Helmius, s. 99ff., Strömholm, Stig, *Individens skyddade personlighetssfär*, antologin *Om våra rättigheter*, s. 29f.

10. spridande av förtrolig information (t.ex. genom advokater, läkare, själasörjare o.d.);
11. avslöjande inför offentligheten av annans privata förhållanden
12. olika former av nyttjande av annans namn, bild eller liknande identifieringsmedel;
13. missbruk av annans ord eller meddelanden (t.ex. genom förvrängda eller uppdiktade intervjuer);
14. angrepp på annans heder och ära. [6]

I tvångsmedelskommitténs betänkande, *Tvångsmedel – Anonymitet – Integritet*, gjordes ett försök att ringa in begreppet med ledning av bl.a. de grundläggande fri- och rättigheter i regeringsformens andra kapitel. Man skiljde här mellan den rumsliga integriteten (hemfriden), den materiella integriteten (egendomsskyddet), den kroppsliga integriteten (skydd för liv och hälsa, mot ingrepp i eller mot kroppen), den personliga integriteten i fysisk mening (skyddet för den personliga friheten och rörelsefriheten) och den personliga integriteten i ideell mening (skyddet för privatlivet och för personligheten inklusive den privata ekonomin).[7]

Sedan 1970-talet har integritetsbegreppet periodvis debatterats intensivt i Sverige. I takt med att samhället utvecklats och både behovet och möjligheterna till olika former av övervakning och kontroll ökat har det blivit allt mer nödvändigt för samhällets beslutsfattare och lagstiftare att reflektera över begreppet personlig integritet och hur denna ska skyddas. Begreppet har diskuterats av flertalet statliga utredningskommittéer, varav de flesta varit inriktade på något speciellt problemområde där integritetshot har konstaterats eller befarats. Det har i dessa utredningar uttalats att individer som lever i den gemenskap med andra människor som samhället utgör inte kan göra gällande något absolut anspråk på att få leva i fred för andra individer eller ostört av samhällets organ. Då individens intressen i många fall står i motsats till andra människors och samhällets intressen behöver skyddet för den enskildes personliga integritet med nödvändighet begränsas eller förses med undantag för att samhället ska fungera. Sammantaget är uppfattningen i utredningarna att det inte går att formulera en allmängiltig definition av integritetsbegreppet utan detta är något man får ta ställning till i varje specifik situation.[8]

I en bilaga till datalagskommitténs betänkande, *Integritet – Offentlighet – Informationsteknik* har Göran Collste, professor i tillämpad etik vid Linköpings universitet, yttrat sig angående definitionsproblematiken. Han menar, likt Strömholm, att det är lättare att identifiera en kränkning av den personliga integriteten än att identifiera begreppet i sig. Han anser därför att personers integritet kränks i den mån som det sker ett intrång i deras privata sfär och/eller uppgifter om dem, som det finns rimliga skäl att beteckna som integritetskänsliga (t.ex. angående personers egenskaper, uppfattningar eller handlingar), sprids ut.[9] Likt vad som presenterats ovan anser Collste att

[6] Strömholm, Stig, *Integritetsskyddet. Ett försök till internationell lägesbestämning*, SvJT 1971, s. 698f.
[7] SOU 1984:54, s. 42.
[8] Se t.ex. SOU 1970:47, s. 56, SOU 1974;85, s. 56.
[9] Collste, s. 796.

rättigheten till personlig integritet inte kan vara absolut då det kan finnas andra skyddsvärda intressen i samhället som vid en kollision bör väga tyngre. Rätt till personlig integritet bör således betraktas som en relativ rättighet eller som en *prima facie*-rättighet, d.v.s. en rättighet som är giltig och välgrundad men som i en konkret handlinssituation kan sättas ur spel om den kommer i konflikt med en annan rättighet som anses väga tyngre.[10]

Som framgått är det svårt, om inte omöjligt, att fullständigt ringa in och definiera betydelsen av begreppet personlig integritet. Sammantaget kan man beskriva en integritetskränkning som ett intrång i en individs privata och fredade zon för vilken individen bör tillförsäkras ett rättmätigt skydd. Vad som innefattas i denna zon och hur begreppet närmare ska bestämmas får sedan avgöras i varje enskilt fall där frågan är aktuell.

2.3 Integritetsskyddet i svensk rätt

I svensk rätt finns det inte någon allmän bestämmelse till skydd för den personliga integriteten, förutom i Europakonventionen[11]. Bestämmelser som ger integritetsskydd i olika avseenden finns dock på särskilda rättsområden och det har nyligen lagts fram förslag på att stärka skyddet i svensk rätt genom att införa en ny bestämmelse om integritetsskydd i regeringsformen. Redan nu är dock bestämmelserna i regeringsformen, tillsammans med Europakonventionen, det mest centrala skyddet för den personliga integriteten i svensk rätt.

2.3.1 Regeringsformen

I regeringsformens första kapitel framgår vissa grundläggande principer, exempelvis stadgas det i 1 kap. 2 § fjärde stycket RF att det allmänna bl.a. ska värna den enskildes privatliv och familjeliv. Bestämmelsen är dock ingen rättsligt bindande regel utan fungerar som ett politiskt målsättningsstadgande som ska vara vägledande för myndigheter som utövar den offentliga makten. Innebörden är alltså att det allmänna bör beakta den enskildes integritet, så långt detta är möjligt.[12]

Kapitel 2 i rättegångsbalken innehåller grundläggande fri- och rättigheter och stadgar genom rättsligt bindande regler ett skydd för den enskildes integritet i förhållande till det allmänna. Av 2 kap. 6 § RF framgår bl.a. att varje medborgare gentemot det allmänna är skyddad mot husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Det som bestämmelsen avser att trygga är alltså brev- och telehemligheten och omfattar således dels telefoni, telegrafi

[10] Collste, s. 801 och 807.
[11] Se kapitel 8.
[12] Prop. 1975/76:209, s. 136ff, Holmberg, Erik m.fl., *Grundlagarna*, s. 19ff.

samt meddelanden som på något viss kommuniceras.[13] Skyddet gäller enbart förhållandet mellan enskilda och det allmänna, främst i form av det allmännas verkställande organ så som domstolar, andra myndigheter och ibland även privaträttsliga subjekt.[14]

Förhållandet mellan målsättningsstadgandet i 1 kap. 2 § RF och bestämmelsen i 2 kap. 6 § RF är alltså att det förra innebär ett skydd *med hjälp av* det allmänna medan den senare tillförsäkrar den enskilde ett skydd *mot* det allmänna. Syftet med den senare bestämmelsen är alltså att, i förhållande till 8 kap. RF, begränsa riksdagens möjlighet att stifta lag i vissa fall och på så vis utgöra ett skydd för den enskilde. Det var främst av denna anledning som man valde att grundlagsfästa skyddet, för att det skulle gälla gentemot lagstiftaren, dvs. riksdagen, och då måste ges i en form som binder denna.[15]

Vissa av fri- och rättigheterna i regeringsformens andra kapitel är absoluta i den meningen att de endast kan inskränkas efter en grundlagsändring. Flertalet är dock relativa och får begränsas genom lag under de förutsättningar som ges i 2 kap. 12 § andra stycket RF. Regleringen i 2 kap. 6 § RF är en sådan relativ rättighet och bestämmelsen har flertalet undantag, bl.a. i rättegångsbalkens regler om straffprocessuella tvångsmedel och exekutiva åtgärder.[16]

Begränsningar i en rättighet enligt 2 kap. 12 § RF får endast utföras efter iakttagande av vissa allmänna rättsprinciper. Detta innebär bl.a. att begränsningen endast får företas för att tillgodose ändamål som är godtagbart i ett demokratiskt samhälle och den får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Dessutom måste en avvägning ha gjorts gentemot motstående intressen så att begränsningen inte innebär en större inskränkning i rättigheten än vad som är acceptabelt i ett demokratiskt samhälle.[17]

2.3.2 Integritetsskyddsutredningen

Frågan om skyddet för den personliga integriteten är ständigt aktuell och under de senaste åren har debatten främst varit inriktad mot skyddets förhållande till en effektiv brottsbekämpning. Frågan har dock diskuterats mer eller mindre intensivt i lagstiftningsärenden under de senaste 40 åren, med början i 1966 års integritetsskyddskommitté. Vid den tiden gällde emellertid frågan hur tekniken möjliggjorde medborgares kränkning av

[13] Petrén, Gustav; Ragnemalm, Hans, *Sveriges Grundlagar*, s. 55.
[14] Prop. 1975/76:209, s. 86 och 140f.
[15] SOU 2008:3, s. 101 och 257.
[16] Strömberg, Håkan; Lundell, Bengt, *Sveriges författning*, s. 87ff, Petrén & Ragnemalm, s. 41f och 68ff.
[17] Strömberg & Lundell, s. 93, Petrén & Ragnemalm, s. 70.

varandras integritet och inte som nu, statens övervakning och kontroll av medborgare.[18]

Skyddet för enskildas privatliv och integritet kan generellt sett anses hålla en hög nivå i Sverige men trots det framställdes det från olika håll krav på en total översyn av integritetsskyddet. En orsak var det lagstiftningsärende som under en längre tid pågått angående införandet av det omdebatterade tvångsmedlet buggning.[19] Mot denna bakgrund tillsattes en parlamentarisk kommitté i april 2004 med uppgift att kartlägga och analysera sådan lagstiftning som rör den personliga integriteten. Kommittén skulle bl.a. se hur integritetsaspekten hanterats och reglerats i gällande lagstiftning och överväga ifall skyddet behövde kompletteras.[20] Resultatet av arbetet presenterades i januari 2008 i slutbetänkandet SOU 2008:3 – *Skyddet för den personliga integriteten.*

Ett av de främsta förslagen som kommittén lade fram var att regeringsformen bör kompletteras med ett nytt stadgande med innebörden att varje medborgare gentemot det allmänna är skyddad mot intrång som sker i hemlighet eller utan samtycke och som i betydande mån innebär övervakning eller kartläggning av den enskildes personliga förhållanden.[21]

De nuvarande bestämmelserna i regeringsformens andra kapitel har enligt kommittén främst motiverats utifrån syftet att skydda den fria åsiktsbildningen och alltså inte av hänsyn till det värdet av att skydda den personliga integriteten. Genom att lagstiftaren tydligare erkänner den självständiga betydelsen av rätten till personlig integritet betonas vikten av respekt för människovärdet och för varje människas rätt till självbestämmande. Kommittén anser att risken annars kan bli att det inte läggs tillräcklig vikt vid integritetsskyddsaspekterna när ny lagstiftning arbetas fram. Dessutom fann man att det relativt låga skydd för den personliga integriteten som den rådande regleringen i RF innebär står i kontrast till det högre skydd som uppfattningen i Europakonventionen ger uttryck för, något som möjligen kan påverka Sveriges trovärdighet som konventionsstat.[22]

Det påtalas i betänkandet att det föreslagna grundlagsskyddet kommer att omfatta den lagring av trafikuppgifter som kommer att bli obligatorisk vid införandet av datalagringsdirektivet. Det konstateras dock att det inte kommer bli några omedelbara konsekvenser för denna typ av integritetsintrång då den redan är reglerad i gällande lagstiftning, i rättegångsbalken respektive lagen om elektronisk kommunikation.[23]

[18] Abrahamsson, Olle, *Integritetsskyddet i lagstiftningen*, SvJT 2006, s. 413.
[19] Abrahamsson, s. 410f., Dir. 2004:51, s. 13.
[20] Dir. 2004:51, s. 18.
[21] SOU 2008:3, s. 13.
[22] SOU 2008:3, s. 15f.
[23] SOU 2008:3, s. 17ff, 260 och 273.

3 Datalagringsdirektivet

Som en följd av terrorattacken i New York den 11 september 2001 sattes en gemensam ansats mot terrorism på EU-medlemsstaternas agenda. Bombdåden i Madrid 2004 och London 2005 ökade trycket på ett gemensamt krafttag ytterligare. Ansatsen har bl.a. inneburit en gemensam handlingsplan mot terrorism för EU:s medlemsstater samt olika lagstiftningsåtgärder.

Efter bombattentatet i Madrid som skedde den 11 mars 2004 fick rådet för rättsliga och inrikes frågor (RIF) i uppdrag av Europeiska rådet att anta gemensamma åtgärder för lagring av trafikuppgifter. Detta arbete ledde till att Storbritannien, Frankrike, Irland och Sverige lade fram ett förslag i form av ett utkast till rambeslut under sommaren 2004. Förslaget mötte hårt motstånd, bl.a. från den Europeiske datatillsynsmannen[24]. Sedermera röstades förslaget ner av Europaparlamentet då åtgärderna som föreslogs inte sågs som proportionerliga i förhållande till syftet och dessutom innebar en alltför långtgående integritetskränkning som inte var förenlig med Europakonventionens bestämmelser.[25]

Efter bombattentaten i London 2005 blåstes nytt liv i förslaget och kommissionen uppmanades att lägga fram ett nytt förslag om gemensamma åtgärder på området. Kommissionen ansåg att detta förslag var bättre lämpat i form av ett direktiv i stället för ett rambeslut. Förslaget, det s.k. datalagringsdirektivet[26], antogs sedermera av ministerrådet och Europaparlamentet den 15 mars 2006.[27]

3.1 Direktivets syfte

Datalagringsdirektivet syftar till att harmonisera medlemsstaternas regler om de skyldigheter som leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät har att lagra vissa uppgifter som genereras eller behandlas i samband med att en kommunikation sker med fast eller mobil telefoni, eller på internet. Anledningen härtill är att säkerställa att uppgifterna finns tillgängliga för utredning, avslöjande och åtal av allvarliga brott såsom de definieras av varje medlemsstat i den nationella lagstiftningen. Uppgifterna som avses är

[24] Europeiska datatillsynsmannen är en oberoende myndighet som övervakar behandlingen av personuppgifter inom EU:s alla institutioner och organ.
[25] Förslag till betänkande av den 18 april 2005, LIBE, 2004/0813(CNS).
[26] Europaparlamentets och rådets direktiv 2006/24/EG 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.
[27] http://www.eu-upplysningen.se/Amnesomraden/Straffratt-och-brottsbekampning/Terrorbekampning/, 2009-01-23.

trafik- och lokaliseringsuppgifter samt uppgifter för att identifiera en abonnent eller användare.[28] I en tid då den elektroniska kommunikationen ökat i betydande utsträckning anses sådana uppgifter vara ett värdefullt verktyg i strävan mot att förebygga, utreda, avslöja och åtala brott och särskilt gäller detta den organiserade brottsligheten.[29]

Som anledningen till att en harmonisering behövs anges att flertalet medlemsstater har antagit lagstiftning av tjänsteleverantörers skyldighet att lagra trafikuppgifter och att skillnader i rättsliga och tekniska bestämmelser medlemsstaterna emellan utgör hinder för den inre marknaden för elektronisk kommunikation. Skälet härtill är att tjänsteleverantörer ställs inför olika krav angående vilken typ av trafik- och lokaliseringsuppgifter som ska lagras samt skillnader i villkoren för lagring och lagringstider.[30]

Då målsättningen med direktivet, att harmonisera tjänsteleverantörernas skyldigheter att lagra vissa uppgifter och säkerställa att de är tillgängliga för brottsbekämpande myndigheter, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna själva får gemenskapen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i EG-fördraget för att på gemenskapsnivå säkerställa detta.[31]

3.2 Integritetsskyddet i direktivet

I direktivets ingress lyfts betydelsen av integritetsskyddet fram genom beaktandet av artikel 8 i Europakonventionen. Enligt artikeln har alla personer rätt till skydd för sitt privatliv och sin korrespondens. Denna rättighet kan endast inskränkas av en offentlig myndighet under vissa angivna förutsättningar, bl.a. får detta endast ske i enlighet med lag och om det är nödvändigt i ett demokratiskt samhälle. Inskränkningar får vidare endast göras för vissa syften, bl.a. med hänsyn till den allmänna säkerheten eller för att förebygga oordning eller brott. Eftersom lagring av uppgifter visat sig vara ett nödvändigt och effektivt redskap för de brottsbekämpande myndigheternas verksamhet i många medlemsstater påpekas det i direktivet att det är av stor vikt att myndigheterna får tillgång till dessa lagrade uppgifter under en viss tid i enlighet med de regler som anges i direktivet.[32]

Det är enligt direktivet även nödvändigt att medlemsstaterna ser till att tillgången till de uppgifter som ska lagras är förbehållen behöriga nationella myndigheter i enlighet med nationell lagstiftning. Det faller dock utanför tillämpningsområdet för gemenskapens lagstiftning att närmare reglera frågor om tillgången till de lagrade uppgifterna. Trots att antagandet av ett instrument om lagring av trafikuppgifter anses som en nödvändig åtgärd i enlighet med artikel 8 EKMR erinras det i direktivet om att

[28] Dir. 2006/24/EG, art. 1.1, 1.2.
[29] Dir. 2006/24/EG, skäl 7.
[30] Dir. 2006/24/EG, skäl 5, 6.
[31] Dir. 2006/24/EG, skäl 21.
[32] Dir. 2006/24/EG, skäl 9.

medlemsstaternas lagar eller lagstiftningsåtgärder om rätten till tillgång och användning av de lagrade uppgifterna till fullo måste respektera de grundläggande rättigheter som är garanterade genom Europakonventionen. Innebörden av detta beskrivs närmare i direktivet som ett krav på att offentliga myndigheters intrång i rätten till privatliv måste stå i förhållande till vad som är nödvändigt och proportionerligt och därför tjäna närmare angivna, tydliga och legitima syften som utövas på ett sätt som är rimligt och relevant och som inte är överdrivet i förhållande till syftet med intrånget.[33]

[33] Dir 2006/24/EG, skäl 9, 17, 25.

4 Trafikuppgiftsutredningens förslag

Den 18 maj 2006 tillsattes Trafikuppgiftsutredningen med uppdrag att lämna förslag på hur datalagringsdirektivet ska genomföras i svensk rätt.[34] Utredningen hade till uppgift att lämna förslag på nödvändiga författningsändringar samt övriga åtgärder som skulle vara motiverade för införlivandet av direktivet och som både tillgodoser behovet av att bekämpa allvarlig brottslighet och skyddet för medborgarnas integritet.[35]

I kommittédirektivet konstaterades behovet av en utredning då det i Sverige inte finns några krav på att nät- och tjänsteleverantörer ska lagra historiska trafikuppgifter för brottsbekämpningsändamål.[36] Snarare är det rådande rättsläget det motsatta, huvudregeln är att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande enligt 6 kap. 5 § lagen (2003:389) om elektronisk kommunikation. Från denna regel finns det vissa undantag, bl.a. får uppgifter sparas och behandlas om det krävs för leverantörens abonnentfakturering eller betalning av samtrafikavgifter[37] till dess fordran är betald eller preskription har inträtt. Syftet med datalagringsdirektivet innebär att det efter införlivandet i svensk rätt uppställs en skyldighet för varje leverantör att lagra samtliga de trafikuppgifter som anges i direktivet under en viss bestämd tid i brottsbekämpande syfte. Genom dessa uppgifter ska de brottsbekämpande myndigheterna kunna få svar på frågorna: vem kommunicerade med vem, när skedde kommunikationen, var befann sig de som kommunicerade och vilken typ av kommunikation användes.[38]

4.1 Trafikuppgifter som ska lagras

Artikel 5 i direktivet anger vilka kategorier av uppgifter som ska lagras och även de syften som lagringen ska tjäna. Lagringsskyldigheten rör uppgifter som är nödvändiga för att:

- spåra och identifiera en kommunikationskälla
- identifiera slutmålet för en kommunikation
- identifiera datum, tidpunkt och varaktighet för en kommunikation
- identifiera typen av kommunikation

[34] Utredningens författningsförslag i aktuella delar återfinns i bilaga A.
[35] Dir. 2006:49, s. 1, SOU 2007:76, s. 17.
[36] Dir. 2006:49, s. 3.
[37] Samtrafik innebär fysisk och logisk sammankoppling av allmänna kommunikationsnät för att göra det möjligt för användare att kommunicera med varandra eller få tillgång till tjänster som tillhandahålls i näten.
[38] SOU 2007:76, s. 17.

- identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt
- identifiera lokaliseringen av mobil kommunikationsutrustning

Dessa uppgifter ska lagras oavsett vilket elektroniskt kommunikationsmedel som används och gäller således för fast och mobil telefoni, meddelandehantering (t.ex. e-post, SMS- och MMS-meddelanden), internettelefoni och internetåtkomst.[39]

Lagringsskyldigheten innebär inte att den enskilde operatören förpliktigas att införskaffa alla de uppgifter som omfattas av lagringsskyldigheten utan endast de uppgifter som operatören genererar eller behandlar i sin verksamhet ska lagras. Detta innebär att om uppgifterna någon gång har befunnit sig hos operatören, om än för en ytterst kort tid, omfattas de av lagringsskyldigheten.[40] Det påpekas dock av utredning att de uppgifter som lagringsskyldigheten omfattar inte är att betrakta som en uttömmande uppräkning av vilka uppgifter som de brottsbekämpande myndigheterna har rätt att få ut från operatörerna. Då förutsättningarna för utlämnande i övrigt är uppfyllda ska även andra uppgifter som lagras av operatören kunna begäras ut.[41] Den uppräkning av vad lagringsskyldigheten innefattar är således att anse som en minimilista av uppgifter.

Viktigt att poängtera är att de uppgifter som sparas inte får avslöja innehållet i kommunikationen, t.ex. telefonsamtalet, e-postmeddelandet, SMS-meddelandet eller telefaxmeddelandet.[42]

4.2 Lagringstiden

Artikel 6 i direktivet anger att den tid som de lagringspliktiga uppgifterna ska sparas ska vara minst sex månader och högst två år från det datum kommunikationen ägde rum. För Trafikuppgiftsutredningen angavs dock att utgångspunkten för utredningens arbete skulle vara att lagringstiden inte skulle understiga ett år men att andra lagringstider kunde vara möjliga ifall det vore lämpligt.[43]

Utredningen konstaterar att det genom uppgifternas betydelse i brottsutredningar och allmänhetens och brottsoffrens intresse av att allvarliga brott utreds finns ett behov av att bestämma lagringstiden till maximala två år. Samtidigt innebär en längre lagringstid att de negativa konsekvenserna för den personliga integriteten ökar. Längre lagringstid innebär exempelvis att större volymer integritetskänslig information finns lagrade vilket leder till att risken för otillåten spridning och läckage ökar.

[39] SOU 2007:76, s. 21f.
[40] SOU 2007:76, s. 139.
[41] SOU 2007:76, s. 23.
[42] SOU 2007:76, s. 139.
[43] Dir. 2006:49, s. 7.

För att tillgodose brottsbekämpningens behov av trafikuppgifter och samtidigt upprätthålla skyddet för den personliga integriteten föreslår utredningen därför en lagringstid på ett år för samtliga lagringspliktiga uppgifter.[44]

Efter lagringstidens slut uppställs ett krav på att uppgifterna ska utplånas, förutsatt att de brottsbekämpande myndigheterna inte begärt att få tillgång till uppgifterna men ännu inte fått ut dem eller att leverantören fortsättningsvis har en rätt att behandla uppgifterna för exempelvis abonnent- eller kundfakturering.[45]

4.3 Myndigheternas tillgång till trafikuppgifterna

EG-direktivet anger inte närmare förutsättningarna som gäller för att de brottsbekämpande myndigheterna ska få tillgång till de sparade uppgifterna utan detta lämnas till medlemsstaterna och den nationella lagstiftningen.[46] Detta följer av direktivets syfte inte är att reglera utlämnandet av uppgifterna utan att säkerställa att uppgifterna de facto finns lagrade när de behövs och därmed säkra tillgången till dem för brottsbekämpande ändamål.

Utgångspunkten för utredningens arbete var att de förutsättningar för att få tillgång till trafikuppgifter som finns i den befintliga lagstiftningen även ska gälla efter det att direktivet genomförts i svensk rätt. Detta innebär att de två befintliga regelverk som möjliggör tillgång till trafikuppgifter för de brottsbekämpande myndigheterna även ska gälla för de uppgifter som kommer att lagras till följd av direktivet; reglerna om hemlig teleövervakning i rättegångsbalken samt lagen (2003:389) om elektronisk kommunikation.[47] Det som anges i direktivet i denna del är att uppgifterna ska lagras för att kunna lämnas ut i syfte att bekämpa allvarlig brottslighet så som denna definieras i den nationella lagstiftningen.[48]

Utredningen konstaterar att frågan om myndigheters rätt att få ut uppgifterna inte reglerats närmare i direktivet men samtidigt anses detta inte vara en fråga som i första hand ska undersökas. Istället fokuseras utredningens analys på frågan om ifall de brott som idag kan utredas med hjälp av lagrade trafikuppgifter anses som tillräckligt allvarliga i direktivets mening. För ledning i denna fråga görs en hänvisning till ett uttalande som gjorts av ministerrådet enligt vilket medlemsstaterna ska ta vederbörlig hänsyn till de brott som finns upptagna i artikel 3 i den europeiska arresteringsordern för att avgöra om de brott för vilket utlämnande får ske enligt de nationella bestämmelserna är tillräckligt allvarliga. Utredningen konstaterar att

[44] SOU 2007:76, s. 171-179.
[45] SOU 2007:76, s. 179.
[46] Dir. 2006/24/EG, art. 4.
[47] SOU 2007:76, s. 27f.
[48] Dir 2006/24/EG, art. 1.

svårighetsgraden för de brott vid vilka hemlig teleövervakning och utlämnande enligt lagen om elektronisk kommunikation får användas stämmer väl överens med de krav som ställs i det här avseendet och att de nuvarande förutsättningarna för utlämnande därför inte behöver förändras.[49]

4.4 Normgivningsnivå

I syfte att bestämmelserna så långt som möjligt ska vara beständiga över tid och oberoende av den tekniska utvecklingen eftersträvades en teknikneutral lösning av utredningen. I de två existerande regelverken för utlämnande av trafikuppgifter, rättegångsbalken respektive lagen om elektronisk kommunikation, anges inte i detalj vilken typ av uppgifter det rör sig om. Dessa betecknas istället ”uppgift om telemeddelanden” respektive ”uppgift som angår ett särskilt elektroniskt meddelande”, vilket medför att bestämmelserna är teknikneutrala och mer flexibla för skillnader i behov och utveckling. För att behålla denna flexibilitet även då det ska anges exakt vilka uppgifter som ska lagras ansåg utredningen att den närmare regleringen och den mer tekniska beskrivningen av vilka trafikuppgifter som lagringsskyldigheten omfattar ska regleras i förordning och inte i lag. Detta innebär att en större flexibilitet tillåts och att förändringar snabbare kan komma till stånd jämfört med om en lagreglering hade valts. Samtidigt innebär förslaget att om en eventuell utökning av de uppgifter som ska lagras av någon anledning är önskad kan en sådan förändring beslutas av regeringen ensam och således utan inhämtning av riksdagens godkännande.[50]

Den föreslagna ordningen har kritiserats av flertalet remissinstanser. Bland andra har *Datainspektionen* och *Brottsförebyggande rådet* (BRÅ) invänt mot denna del av förslaget.[51] *Advokatsamfundet* påpekar att regeringen tidigare uttalat att myndighetsregister med stora mängder känsliga uppgifter ska regleras i lag. Samfundet menar att den aktuella lagringen utan tvekan är av sådan karaktär och därmed i sin helhet bör regleras i lag.[52] *Justitieombudsmannen* menar att den föreslagna lösningen för med sig en möjlighet för regeringen att göra klara utvidgningar av övervakningen utan riksdagens medverkan och att principen måste vara sådant som rör integritetsintrångets omfattning ska regleras i lag.[53] *Post- och telestyrelsen* (PTS) anser det vara anmärkningsvärt att föreslå en reglering genom förordning med tanke på det förslag till grundlagsskydd för den personliga integriteten som integritetsutredningen lagt fram.[54] I ett skiljaktigt yttrande i

[49] SOU 2007:76, s. 221f och 227ff.
[50] SOU 2007:76, s. 137f.
[51] Datainspektionens remissvar i anledning av SOU 2007:76, s. 2, Brottsförebyggande rådets remissvar i anledning av SOU 2007:76, s. 1.
[52] Advokatsamfundets remissvar i anledning av SOU 2007:76, s. 4f.
[53] Justitieombudsmannens remissvar i anledning av SOU 2007:76, s. 2.
[54] Post- och telestyrelsens remissvar i anledning av SOU 2007:76, s. 10.

utredningen har även datarådet Hans-Olof Lindblom och advokat Per Furberg invändningar mot förslaget på denna punkt.[55]

4.5 Brottsbekämpning och integritet

4.5.1 Behovet av trafikuppgifter för brottsbekämpning

Trafikuppgifter används på något sätt i princip i alla utredningar av grövre brott. Det rör sig därmed om brott såsom mord, människorov, olaga hot (grovt brott), våldtäkt, grovt rån, utpressning (grovt brott), mordbrand, grovt narkotikabrott eller brott som utreds av Säkerhetspolisen, som exempelvis terroristbrott. Vid denna typ av brott inleds ofta utredningen med en kontroll av trafikuppgifter som på något sätt kan knytas till en viss plats eller viss person som är av intresse för utredningen.[56]

Genom att kombinera trafikuppgifter med annan information som tas fram i brottsutredningen kan händelsekedjor både före, under och efter brottets fullgörande klarläggas. Dessutom kan uppgifterna hjälpa utredningen genom att hitta samband mellan olika personer, lokalisera platser av intresse samt avfärda personer från utredningen genom att visa att misstankarna mot dem var grundlösa. Sammantaget menas att trafikuppgifters betydelse för de brottsbekämpande myndigheternas verksamhet vad gäller förundersökningar av grova brott inte kan överskattas. Tillgången till uppgifterna är av en så fundamental betydelse att de ofta är direkt kopplade till om det över huvudtaget går att driva förundersökningen framåt. Även i de fall där uppgifterna inte direkt går att använda som bevis i rättegång är de ofta av stor betydelse då de så att säga ”sätter polisen på spåret”.[57]

Den nuvarande regleringen innebär att det inte finns någon skyldighet att lagra trafikuppgifter för brottsbekämpande ändamål. Snarare råder ett motsatt förhållande där uppgifterna i stort sett endast får sparas om det finns skäl för det utifrån förhållandet mellan operatören och kunden/abonnenten och annars ska uppgifterna utplånas. Innebörden av detta är att det i många fall innebär en slump om de brottsbekämpande myndigheterna kan få tillgång till uppgifterna då dessa ska ha lagrats av andra skäl och därmed finns tillgängliga hos operatörerna.

Behovet av trafikuppgifterna konstaterades av Beredningen för rättsväsendets utveckling (BRU) i ett av beredningens delbetänkanden, SOU 2005:38 - *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* Beredningen menade att den nuvarande regleringen innebär stora problem för brottsbekämpningens effektivitet. Ett fåtal månader efter BRU givits i uppdrag att se över den rådande regleringen sattes arbetet med

[55] SOU 2007:76, s. 313ff.
[56] SOU 2005:38, s. 323.
[57] SOU 2005:38, s. 325.

datalagringsdirektivet igång inom EU och beredningen lade därför inte fram något förslag som berörde detta område.[58]

4.5.2 Lagringens påverkan av integriteten

Själva syftet med datalagringsdirektivet är att uppgifter angående enskildas kommunikation ska lagras för en viss tid. Följden blir därför med nödvändighet att en mycket stor mängd information kommer att lagras om i stort sett alla medborgare i landet, information som dessutom i många fall är av integritetskänslig karaktär. Den absolut största delen av dessa uppgifter kommer heller inte att användas för de syften för vilka de lagrats då endast en ytterst begränsad del av uppgifterna innehåller information som är av intresse för utredningen av allvarliga brott.[59]

Enbart det faktum att en så omfattande lagring kommer äga rum innebär i sig själv konsekvenser för det upplevda integritetsintrånget. Att ett regelverk tillåter en insamling av privat kommunikation innebär att friheten att kommunicera upplevs som inskränkt, oavsett om uppgifterna senare används eller inte. Det kan uttryckas som att integritetsintrånget sker redan då det allmänna säkrar tillgången till trafikuppgifterna genom lagringen.[60] Den största risken för den enskildes integritet anses dock enligt utredningen vara ifall de lagrade uppgifterna sprids från nätoperatörerna till obehöriga och om operatörerna använder uppgifterna för andra ändamål än de tillåtna.[61]

För att få en uppfattning om lagringsskyldighetens omfattning och därmed den integritetsskada som denna kan föra med sig kan man se på antalet abonnemang som finns i Sverige. Den siste december 2007 fanns det 10 371 000 stycken mobilabonnemang, 5 506 000 stycken fasta telefonabonnemang samt 3 933 000 stycken kunder med Internetaccess.[62] Då uppgifter ska lagras om i stort sett all elektronisk kommunikation innebär det att ett flertal uppgifter ska lagras vid varje enskilt kommunikationstillfälle för vart och ett av dessa abonnemang.

Vid en hearing om integritetsfrågor anordnad av Trafikuppgiftsutredningen behandlades ett flertal olika integritetsaspekter som ansågs viktiga vid ett genomförande av datalagringsdirektivet. De psykologiska aspekterna av ett införande, såsom en ökad rädsla och misstänksamhet bland medborgarna samt minskad tilltro till myndigheterna ansågs som större integritetsskador än det förhållandet att vissa uppgifter begärs ut av de brottsbekämpande myndigheterna i ett begränsat antal ärenden årligen. Förslaget befaras även innebära en risk för att trafikuppgifter kommer att användas i mycket högre utsträckning än tidigare. Vad gäller själva utlämnandet av uppgifterna

[58] SOU 2005:38, s. 308.
[59] SOU 2007:76, s. 110.
[60] SOU 2007:76, s. 109f.
[61] SOU 2007:76, s. 235.
[62] PTS-rapport, *Svensk Telemarknad 2007*, tabell 1, s. 9.

påpekades vikten av en för- och efterhandskontroll av utlämnandet samt att andra rättssäkerhetsgarantier omgärdar regelsystemet.[63]

4.5.3 Balansen mellan brottsbekämpning och integritetsskydd

En viktig del av Trafikuppgiftsutredningens uppdrag innebar att göra en avvägning mellan brottsbekämpningens intresse av att trafikuppgifter lagras i angiven omfattning och skyddet för den personliga integriteten. För att uppdraget ska anses uppfyllt i denna del måste det nationella genomförandet av direktivet bl.a. anses stå i överensstämmelse med de integritetsskydd som framgår av 2 kap. regeringsformen och artikel 8 i Europakonventionen. Detta innebär att utredningen även hade att föreslå regler som behövs för att stärka integritetsskyddet och motverka missbruk av uppgifterna som ska lagras.[64]

För att uppnå en balans mellan dessa två intressen har en rad integritetsskyddande bestämmelser införts i förslaget. Dessa är i huvudsak:

- lagringen sker på flera håll och alltså inte i ett centrallager
- lagringstiden begränsas till ett år och därefter ska uppgifterna utplånas
- vid fullgörande av lagringsskyldigheten ska tekniska och organisatoriska åtgärder vidtas för att säkerställa ett tillräckligt skydd vid uppgiftsbehandlingen
- tillsynsmyndigheten PTS ska tillse att operatörernas lagring följer gällande regelverk
- tydliga regelverk så att var och en kan bedöma integritetsintrånget man drabbas av och
- tydliga förutsättningar för utlämnande av uppgifterna enligt reglerna i rättegångsbalken och lagen om elektronisk kommunikation [65]

Utredningen beaktade även kontrollen av de myndigheter som utnyttjar de lagrade uppgifterna i sin brottsbekämpande verksamhet vid bedömningen av om balansen mellan de motstående intressena var god. Det påpekades här att utöver en förhandskontroll av domstol för användning av hemlig teleövervakning finns även andra möjligheter till tillsyn och efterhandskontroll. Denna utgörs främst av JO, JK och datainspektionen som i sin verksamhet övervakar den brottsbekämpande verksamheten. Även den nyinrättade Säkerhets- och integritetsskyddsnämnden och krav på underrättelse till den som utsätts för tvångsmedel lyftes fram.[66]

[63] SOU 2007:76, s. 111ff.
[64] Dir. 2006:49, s. 7.
[65] SOU 2007:76, s. 233ff.
[66] SOU 2007:76, s. 237f.

Vad gäller bestämmelserna om utlämnanden av trafikuppgifter enligt lagen om elektronisk kommunikation påpekade utredningen att det vore fördelaktigt ur rättssäkerhetssynpunkt om dessa sammanfördes med reglerna i rättegångsbalken och instämmer därför i det förslag BRU lagt fram[67] i frågan.[68]

Sammantaget konstaterar utredningen att genom de åtgärder som föreslås samt de integritetsskydd och rättssäkerhetsgarantier som finns tillgängliga i existerande regelverk uppnås inte bara en rimlig utan en god balans mellan brottsbekämpningens intresse och skyddet för den personliga integriteten.[69]

[67] Se kap. 7.
[68] SOU 2007:76, s. 238.
[69] SOU 2007:76, s. 238.

5 Hemlig teleövervakning

Hemlig teleövervakning är ett s.k. *hemligt straffprocessuellt tvångsmedel* och utgör tillsammans med hemlig teleavlyssning de tvångsmedel som finns inom teleområdet i svensk rätt. Hemlig teleövervakning och teleavlyssning regleras båda i 27 kap. RB och flertalet av kapitlets bestämmelser är gemensamma.

Hemlig teleövervakning innebär att det i hemlighet hämtas in uppgifter om telemeddelande som har expedierats eller beställts till eller från en viss teleadress eller att sådana meddelande hindras från att nå fram.[70] Uppgifterna det rör sig om är dels trafikuppgifter och dels lokaliseringsuppgifter. Hemlig teleavlyssning innebär däremot att innehållet i telemeddelandet avlyssnas eller tas upp av ett tekniskt hjälpmedel för att senare återgivas.[71] Som beskrivits innebär datalagringsdirektivet att endast uppgifter om själva trafiken ska lagras och således inte innehållet i befordringen. Av denna anledning ligger fokus i det följande på hemlig teleövervakning.

Bestämmelser om hemlig teleövervakning infördes i rättegångsbalken 1989 och tidigare användes tvångsmedlet endast vid brott enligt 1952 års tvångsmedelslag. Det tidigare användningsområdet innefattade främst att kunna fördröja telefonsamtal eller att hindra dem från att expedieras. Den nuvarande tillämpningen fungerar främst som ett verktyg för att kartlägga den misstänktes kontakter under en viss tidsperiod.[72]

I detta kapitel ges först en allmän beskrivning av begreppet straffprocessuellt tvångsmedel, dess innebörd och de rättsprinciper som styr dess användande. Därefter ges en mer ingående beskrivning av just hemlig teleövervakning och under vilka förutsättningar denna åtgärd får användas.

5.1 Straffprocessuella tvångsmedel

För att samhällets brottsbekämpning ska fungera effektivt är det en nödvändighet att åklagare och polis har tillgång till vissa hjälpmedel, bl.a. straffprocessuella tvångsmedel. Dessa regleras främst i 24-28 kap. RB men det finns inte någon allmängiltig definition av begreppet i lagtexten. Generellt sett innebär dessa metoder ett direkt ingripande mot en person, s.k. personellt tvångsmedel, eller mot egendom, s.k. reellt tvångsmedel, som företas i myndighetsutövning och som utgör intrång i någons rättssfär.[73] De straffprocessuella tvångsmedlen behövs för att de brottsbekämpande myndigheterna ska kunna ha möjlighet att genomföra utredning om brott

[70] Jfr. 27 kap. 19 § RB.
[71] Jfr. 27 kap. 18 § RB.
[72] Lindberg, Gunnel, *Straffprocessuella Tvångsmedel*, s. 494.
[73] Lindberg, s. 5f.

och säkerställa lagföring och verkställighet av påföljd och annan rättsverkan av brott. Möjligheten att använda sådana metoder är nödvändig för att polis och åklagare ska kunna genomföra en effektiv lagföring av brott, vilket i sin tur stärker brottspreventionen i samhället och rättsskyddet för målsäganden.[74]

5.1.1 Hemliga tvångsmedel

Reglerna om straffprocessuella tvångsmedel förutsätter vanligen att dessa kan användas under tvång. Emellertid hänförs även andra åtgärder som i praktiken aldrig verkställs med tvång till denna kategori, t.ex. tvångsmedlen på teleområdet; hemlig teleavlyssning och teleövervakning. Anledningen till att dessa betraktas som tvångsmedel trots den direkta avsaknaden av tvång är möjligen att det är fråga om en integritetskränkning mot den avlyssnade/övervakade då man kan förutsätta att åtgärden företas mot dennes vilja.[75] Som namnet antyder används de hemliga tvångsmedlen i hemlighet, d.v.s. utan den misstänktes vetskap och som en följd härav utan dennes samtycke.

5.1.2 Viktiga rättsprinciper vid användandet av straffprocessuella tvångsmedel

Användningen av tvångsmedel utgör intrång i privatlivet och i den personliga integriteten, d.v.s. i rättigheter skyddade i grundlagen genom bl.a. 2 kap. 6 § RF. Dessa inskränkningar har stöd av 2 kap. 12 § RF och denna bestämmelse har legat till grund för de allmänna rättsprinciper som gäller för både regleringen och användningen av tvångsmedlen.[76] Dessa principer utgörs främst av legalitets-, ändamåls-, behovs- och proportionalitetsprinciperna.

5.1.2.1 Legalitetsprincipen

Legalitetsprincipen är den mest fundamentala principen för tvångsmedelanvändning. Den följer av regelsystemet i 1 och 2 kap. RF och kommer bl.a. till uttryck i 1 kap. 1 § RF, där det stadgas att all offentlig makt ska utövas under lagarna. Innebörden av principen i förhållande till de straffprocessuella tvångsmedlen är att en myndighet inte får ingripa i en enskilds rättssfär utan stöd i lag eller annan författning.[77]

Enligt Bylund för principen med sig att reglerna om straffprocessuella tvångsmedel bör vara obligatoriska, tvingande och detaljerat utformade vad gäller handlingsmönster. Reglerna bör även vara begränsat tänjbara i det att

[74] Lindberg, s. 6 och Ekelöf m.fl., *Rättegång, - Tredje häftet*, 2006, s. 45.
[75] Lindberg, s. 5f. och Ekelöf m.fl., 2006, s. 42f.
[76] Ekelöf m.fl. 2006, s. 46 och Dir 2004:51, s. 5.
[77] Lindberg, s. 18, Westerlund, Gösta, *Straffprocessuella tvångsmedel*, s. 12.

vaga, obestämda och mångtydiga rekvisit helst inte ska finnas. På detta viset kan en förutsebarhet uppnås i tvångsmedelsanvändningen och godtyckliga, slumpmässiga och överraskande ingripande undgås vilket leder till en ökad rättssäkerhet. För att det här resultatet ska uppnås poängterar Bylund även vikten av att beslutsfattarna tillämpar tvångsmedlen restriktivt.[78]

5.1.2.2 Ändamålsprincipen

Ändamålsprincipen innebär att tvångsmedel inte får användas godtyckligt utan endast för de ändamål som specificerats av lagstiftaren. Principen kan därmed sägas komplettera legalitetsprincipen vid bedömning av tvångsmedelsbeslutets lagliga grund.[79] Principen, som inte är lagreglerad, anses följa av stadgandet i 2 kap. 12 § RF som säger att begränsningar i de grundläggande fri- och rättigheterna endast får vidtas för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och de får aldrig gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett dem.[80] Principen ska återspeglas i lagstiftningen genom att varje föreskrift för tvångsmedel uttryckligen ska innefatta de ändamål för vilka den aktuella åtgärden får användas.[81]

5.1.2.3 Behovsprincipen

Behovsprincipen innebär att en myndighet endast får använda ett tvångsmedel när det föreligger ett påtagligt behov och en mindre ingripande metod inte är tillämplig.[82] Åtgärden ska därmed inte bara vara *nödvändig* utan också *verkningsfull* med den innebörden att det avsedda resultatet kan uppnås genom åtgärden. Om uppgiften kan lösas utan att man använder ett tvångsmedel eller i vart fall med ett mindre ingripande tvångsmedel ska detta alternativ väljas istället.[83]

Behovsprincipen innebär vidare att användandet av ett tvångsmedel ska upphöra när syftet med det har uppnåtts eller när det av andra skäl inte längre finns behov för det. Detta innebär att om åtgärden enbart eller huvudsakligen används för att myndigheten lättare eller bekvämare ska kunna utföra sina uppgifter strider det mot behovsprincipen. Principen leder även till att ett tvångsmedelsbeslut inte får ges större omfattning än vad som är sakligt motiverat.[84]

5.1.2.4 Proportionalitetsprincipen

I förhållande till de straffprocessuella tvångsmedlen innebär proportionalitetsprincipen att dessa endast får användas om skälen för

[78] Ekelöf m.fl., 2006, s. 47.
[79] Helmius s. 66.
[80] Westerlund, s. 12f.
[81] Lindberg, s. 20 och Ekelöf m.fl., 2006, s. 47.
[82] Prop. 1984/89:124, s. 26.
[83] Bylund, Torleif, *Tvångsmedel I*, s. 58.
[84] Lindberg, s. 23 och SOU 1984:54, s. 77.

åtgärden väger tyngre än de olägenheter som åtgärden innebär för den misstänkte eller något annat motstående intresse. Den aktuella tvångsåtgärden ska således i fråga om art, styrka, räckvidd och varaktighet stå i förhållande till det syfte man vill uppnå.[85] Principen är alltså inriktad på de negativa konsekvenser som tvångsmedelsanvändningen kan innebära, främst i förhållande till de skador denna kan medföra för den enskilde.

En proportionalitetsprincip har kommit till direkt uttryck i samtliga tvångsmedelskapitel (24-28 kap.) i rättegångsbalken och för de hemliga tvångsmedlen på teleområdet innebär detta att principen kommer till uttryck i 27 kap. 1 § RB.[86] Enligt den lagfästa principens ordalydelse är det endast själva beslutet om tvångsmedlets användande som omfattas. Det har dock varit lagstiftarens mening att principen även ska tillämpas vid verkställandet av en sådan åtgärd.[87]

På grund av den integritetskränkande karaktären samt den höga risken för att helt utomstående personer drabbas genom användandet av de hemliga tvångsmedlen på teleområdet har bl.a. Lindberg påpekat vikten av att principen tillämpas strikt.[88]

5.2 Begreppsdefinitioner

Telemeddelande
Med begreppet telemeddelande åsyftas ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.[89] Definitionen infördes i den upphävda telelagen (1993:597) och återfinns numera i lagen om elektronisk kommunikation och anses tillämplig även på rättegångsbalkens bestämmelser.

Teleadress
Tidigare medgavs hemlig teleövervakning och hemlig teleavlyssning av viss teleanläggning, d.v.s. en telefon, telefax, mobiltelefon eller liknande. När reglerna moderniserades 1995 eftersträvades en teknikneutral benämning och begreppet teleadress introducerades. Teleadress avser den icke fysiska adress som ett telemeddelande skickas till eller från.[90] Med detta menas exempelvis ett telefonnummer, ett abonnemang, en e-postadress eller s.k. IP-nummer vid datakommunikation.[91]

Trafikuppgifter

[85] Prop. 1988/89:124, s. 26, SOU 1998:46, s. 376.
[86] Bylund, s. 58f.
[87] SOU 1995:47, s. 324.
[88] Lindberg, s. 473.
[89] Lagen (2003:389) om elektronisk kommunikation, 19 §.
[90] Prop. 1994/95:227, s. 31.
[91] Lindberg, s. 459.

Trafikuppgifter består av uppgifter som behandlas i syfte att befordra ett elektroniskt meddelande via elektroniska kommunikationsnät eller för att fakturera ett sådant meddelande.[92] Dessa anger var meddelandet kommer ifrån, var det är på väg, tidpunkter för befordringen, varaktighet och vid exempelvis datakommunikation även storleken på meddelandet.[93] När övervakningen t.ex. gäller telefonnummer kan trafikuppgifterna alltså ange vilka telefonnummer som expedieras till och från det övervakade numret, tidpunkten för expedieringen, längden på samtalen etc.

Lokaliseringsuppgifter
Lokaliseringsuppgifter anger från vilket geografiskt område en viss kommunikationstjänst använts. Denna sorts information används främst för att bestämma var den som använder en viss mobiltelefon befinner sig.[94]

5.3 Förutsättningarna för hemlig teleövervakning

Hemlig teleövervakning får enligt huvudregeln användas vid förundersökning angående brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader. Tvångsmedlets karaktär har även funnits nödvändigt i utredandet av ett fåtal brott som anses allvarliga men som har en lägre strafftröskel än fängelse i sex månader och därför kompletteras huvudregeln med en brottskatalog innehållande narkotikabrott och narkotikasmuggling, dataintrång och barnpornografibrott. I den mån de är belagda med straff får hemlig teleövervakning även användas vid försök, förberedelse och stämpling till ovan angivna brott.[95]

Ett system med straffvärdesventil har diskuterats men inte genomförts då detta skulle ge ett alltför omfattande tillämpningsområde.[96]

5.3.1 Skälig misstanke om brott

Enligt 27 kap. 20 § RB krävs det för beslut om hemlig teleövervakning att någon är *skäligen misstänkt* för ett konkret brott.

Vid införandet av reglerna om hemlig teleövervakning i rättegångsbalken 1989 fördes en diskussion om vilken grad av misstanke som skulle vara lämplig då bl.a. narkotikakommissionen fört fram förslag på en sänkning av brottsmisstanken. Departementschefen ansåg att en lägre misstankegrad i vissa fall skulle vara till fördel för brottsbekämpningen då tvångsmedlen kunde sättas in i ett tidigare skede i utredningen. Men då en högre

[92] Prop. 2002/03:110, s. 257f.
[93] Lindberg, s. 494f.
[94] Prop. 2002/03:110, s. 260f.
[95] Lindberg, s. 496.
[96] Prop. 2002/03:74, s. 35.

misstankegrad innebär en större säkerhet från utredningens sida skulle en sänkning av densamma leda till en ökad risk för att brottsmisstanken visar sig vara obefogad och att övervakningen således riktats mot en oskyldig.[97] Avvägningen gjordes alltså mot integritetsaspekten som slutligen tillmättes störst vikt.

Även buggningsutredningen, SOU 1998:46 - *Om buggning och andra hemliga tvångsmedel*, tog upp frågan om vilken misstankegrad som skulle krävas och ansåg att detta innebar en balansgång mellan effektiviteten för den brottsbekämpande verksamheten å ena sidan och integritetsintresset å andra sidan. En högre misstankegrad än ”skäligen misstänkt” ansågs inte kunna komma på fråga då detta skulle innebära ett för högt ställt krav och därmed förta tvångsmedlens effektivitet helt och hållet och frågan gällde därför ifall kravet skulle sänkas. Utredningen hänvisade till argumenten i 1989 års lagstiftningsärende och ansåg att en lägre misstankegrad oundvikligen skulle leda till att ett större antal oskyldiga kunde komma att utsättas för integritetskränkande tvångsmedel, något som så långt som möjligt skulle undvikas. Även här ansågs alltså integritetsaspekten väga tyngst.[98]

5.3.1.1 Innebörden av uttrycket *skälig misstanke*

Att ge ett generellt svar på hur mycket som krävs för att nå upp till en viss misstankegrad är förenat med naturliga svårigheter och låter sig därför knappast göras. En lagstiftning kan inte i detalj redogöra för vad som krävs i det enskilda fallet och alla de uttryck som används i lagstiftningen är medvetet vaga i sin rent språkliga innebörd.[99] Någon vägledning om vad de olika graderna av misstanke innefattar ges inte heller i rättegångsbalkens förarbeten då detta inte är närmare redovisat.[100] För att finna ledning och riktlinjer får man istället vända sig till doktrinen och i viss mån till de principiella uttalande som exempelvis JO eller JK gjort i enskilda ärenden.

Uttrycket *kan misstänkas* är den lägsta formen av misstankegrad riktat mot en person och det är vad som enligt rättegångsbalkens bestämmelser krävs för att hålla kvar någon för polisförhör i mer än sex timmar. För att nå upp till denna misstankegrad räcker det med mycket svag bevisning och det har uttryckts som att det under förundersökning uppenbaras någon omständighet som kastar misstankar på en eller annan person.[101]

En betydligt högre grad av misstanke är *sannolika skäl* vilket enligt huvudregeln är kravet för häktning. Här måste omständigheterna som föreligger vara sådana att misstanken vid en objektiv bedömning av

[97] Prop. 1988/89:124, s. 43f.
[98] SOU 1998:46, s. 388ff.
[99] Ekelöf SvJT 1982, *Ett problem med avseende på hemlig avlyssning*, s. 655 och Elwing, Carl M, *Tillräckliga skäl – Studier över förutsättningarna för allmänt åtal*, s. 59.
[100] Prop. 1975/76:202, s. 105.
[101] Elwing, s. 62.

situationen framstår som berättigad.[102] Om inte särkskilda omständigheter talar för motsatsen ska ett erkännande av den misstänkte göra att det anses föreligga sannolika skäl.[103]

Skälig misstanke kan på en graderad skala placeras in mellan de båda ovan redovisade och är det beviskrav som krävs för de flesta tvångsmedel. JO har uttalat att det är omöjligt att med någon högre grad av precision i generella termer ange när en skälig misstanke mot någon kan anses föreligga. Det har dock uttalats att det krävs konkreta omständigheter av viss styrka som talar för att den misstänkte begått den gärning som misstanken avser.[104] Grunderna för misstanken ska därmed vara påtagligt objektiva och vid beslut av åtgärd mot den misstänkte saknar beslutsfattarens subjektiva uppfattning om den misstänktes skuld betydelse.[105] Inte heller kan beslutet grundas på allmänna kunskaper om den misstänktes livsföring eller tidigare brottslighet.[106]

Enligt Ekelöf motsvarar begreppet *skäligen misstänkt* ungefär detsamma som uttrycket *antagligt*.[107]

5.3.2 Synnerlig vikt för utredningen

Det uppställs ett krav på att teleövervakningen ska vara av *synnerlig vikt för utredningen* för att åtgärden ska få tillgripas.[108] För att anses vara av synnerlig vikt ska åtgärden i det enskilda fallet påverka förundersökningen positivt och denna påverkan ska vara påtaglig och betydande.[109] Däremot krävs inte åtgärden tillhandahåller avgörande bevisning som omedelbart kan leda till fällande dom. Bedömningen av om åtgärden kommer vara av synnerlig vikt ska göras i varje enskilt fall. För det första innebär rekvisitet att ett kvalitetsmått säkras avseende den information som framkommer med åtgärden. Nyttan med åtgärden får alltså inte endast vara obetydliga detaljer som man båda kan ha och mista. För det andra uppställs det även krav på att avlyssningen är nödvändig i utredningens läge. Man ska inte kunna nå samma resultat som övervakningen med andra, mindre ingripande metoder. Det ska i princip konstateras att inga andra utredningsåtgärder kan föra utredningen framåt och i vart fall ska man vid en skälighetsbedömning slå fast att man inte kan avstå från övervakningen.[110]

[102] SOU 1995:47 s. 164, Elwing, s. 62.
[103] JO 1953, s. 325.
[104] JO 1986/87, s. 83, JO 1992/93, s. 206, JO 1993/94, s. 103, JK 1991, s. 57.
[105] JO1994/95 s. 140, Elwing s. 62.
[106] JO 1993/94, s. 103.
[107] Ekelöf m.fl., *Rättegång – Femte häftet*, 2005, s. 113.
[108] 27:20 1 st. RB.
[109] DsJu 1981:22, s. 88.
[110] Lindberg, s. 468.

5.4 Teleadresser som får övervakas

Ett tillstånd för hemlig teleövervakning kräver en för övervakningen utpekad teleadress. Därtill kommer krav på anknytning mellan teleadressen och den misstänkte personen som ska övervakas. För det första får övervakningen gälla teleadresser som *innehas eller har innehafts av den misstänkte*. Det kan därmed röra sig om ett eller flera olika abonnemang för t.ex. fast telefoni och mobiltelefoni eller en eller flera e-postadresser o.s.v. Flera olika teleadresser kan blir föremål för övervakningen ifall den misstänkte rör sig mellan flera olika adresser. För det andra får även sådana *teleadresser som den misstänkte kan antas använda* övervakas. Härtill finns ett krav på att det måste föreligga konkreta omständigheter som talar för ett sådant antagande med viss styrka och det räcker således inte endast med en allmän förmodan.[111] Innebörden är att exempelvis teleadresser som tillhör den misstänktes familj, nära vänner, arbetsplats, skola eller annan teleanläggning som den misstänkte troligen kan använda kan omfattas av övervakningen. För det tredje får övervakningen avse *teleadress som den misstänkte kan förväntas ringa till eller på annat sätt kontakta*. För det sistnämnda ställs dock det högre kravet om synnerlig anledning att anta att den misstänkte tar sådan kontakt.[112]

5.5 Beslutsförfarandet

Enligt 27 kap. 21 § rättegångsbalken är det åklagaren som ansöker om tillstånd för hemlig teleövervakning och denna ansökan prövas av tingsrätten som första instans. Beslutet ska tas av en lagfaren domare och i praktiken är det vanligen lagmannen eller annan chefsdomare som handlägger frågor angående hemliga tvångsmedel.[113]

Domstolens beslut ska innehålla uppgifter om *vilken eller vilka teleadresser* som tillståndet gäller samt vilken anknytning som den misstänkte personen har till dessa. Alla beslut som gäller för teleövervakning som ska verkställas framåt i tiden ska dessutom tidsbegränsas av domstolen. Tiden som beslutet gäller för får aldrig bestämmas till längre än vad som är nödvändigt och får i vart fall inte överstiga en månad från den dag då beslutet togs.[114] Beslutet kan dock förlängas och denna möjlighet utnyttjas ofta. Någon gräns för hur många gånger en förlängning får göras finns inte men domstolen ska vid varje förlängningsansökan pröva behovet av åtgärden på nytt.[115]

För att minska integritetsintrånget kan domstolen förena beslutet med villkor. Särskilt viktigt anses denna möjlighet vara då tillståndet gäller teleövervakning av en teleadress som den misstänkte personen kan tänkas

[111] JO 1994/95, s. 42.
[112] 27 kap. 20 § RB.
[113] Lindberg, s. 475.
[114] 27 kap. 21 § RB.
[115] Lindberg, s. 480.

kontakta, då tvångsmedlet inte riktar sig mot den person vars teleadress ställs under övervakning. Villkoret kan i sådana fall vara att övervakningen enbart gäller inkommande kommunikation.[116]

För att få ett mer heltäckande resultat av åtgärden kombineras regelmässigt ett tillstånd till hemlig teleavlyssning med ett tillstånd till hemlig teleövervakning. Den hemliga teleavlyssningen ger nämligen endast information om vad meddelandet som avlyssnas innehåller men för att få tillgång till uppgifter som rör meddelandet, exempelvis var det kommer ifrån eller vart det skickas, behövs ett beslut om hemlig teleövervakning.[117]

[116] Prop. 2002/03:74, s. 38.
[117] SOU 2005:38, s. 216f.

6 Lagen om elektronisk kommunikation

I lagen (2003:389) om elektronisk kommunikation regleras de elektroniska kommunikationsnäten och de kommunikationstjänster som förmedlas däri. Exempel på sådana nät är telenät, kabel-TV-nät och bredbandsnät. För dessa nät omfattar lagen den tekniska infrastrukturen men är däremot inte tillämplig på innehåll som överförs i de tjänster som utnyttjar näten.[118] Bestämmelserna i lagen syftar bl.a. till att garantera enskilda och myndigheter tillgång till säkra och effektiva elektroniska kommunikationer bl.a. genom att främja konkurrensen på området.[119]

I och med tillämpningsområdet är det främst genom denna lag som de olika nätoperatörernas och nätleverantörernas verksamhet regleras.[120] Detta innebär att lagen bl.a. innehåller bestämmelser om dessa operatörers rättigheter och skyldigheter gentemot konsumenter av olika kommunikationstjänster samt i förhållande till de brottsbekämpande myndigheterna.

I det här kapitlet kommer en genomgång göras av integritetsskyddet i lagen om elektronisk kommunikation samt under vilka förutsättningar som detta skydd får ge vika för myndigheters verksamhet i brottsbekämpande syfte.

6.1 Bakgrund

År 2000 presenterades förlag på ett nytt regelverk för elektronisk kommunikation av EG-kommissionen. Syftet var att modernisera gemenskapens lagstiftning på området och därmed balansera upp för den snabba utvecklingen av teknik och marknader för elektronisk kommunikation. Förslaget mynnade ut i ett regelverk bestående av sex stycken direktiv som sammanlagt syftar till att öka konkurrensen och den fria rörligheten av elektroniska kommunikationstjänster i EU.[121] Ett av dessa är enbart inriktat på integritetsfrågor, direktiv (2002/58/EG) om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

För att genomföra direktiven tillsattes den s.k. e-komutredningen 2001 och på grundval av dess arbete infördes lagen om elektronisk kommunikation (LEK).[122] Lagen började gälla den 25 juli 2003 och ersatte därmed telelagen (1993:597) och lagen (1993:599) om radiokommunikation.

---

[118] PTS, *Faktablad - Lagen om elektronisk kommunikation*, s. 1.
[119] 1 kap. 1 § LEK.
[120] I det följande benämns dessa samlat med ”nätoperatörer” eller ”operatörer”.
[121] http://www.regeringen.se/sb/d/2373/a/16378, 2008-11-12.
[122] SOU 2005:38, s. 128, SOU 2007:22 del 1, s. 294f, Prop., 2002/03:110, s. 64ff.

6.2 Integritetsskyddet i lagen

Det sjätte kapitlet i LEK innehåller lagens specifika integritetsskydd. Det är i detta kapitel som direktivet (2002/58/EG) om integritet och kommunikation i huvudsak har genomförts. Kapitlets bestämmelser har företräde framför personuppgiftslagen vad gäller behandling av personuppgifter inom de områden som lagen reglerar.[123]

I 6 kap 5 § återfinns huvudregeln vad gäller operatörers skyldighet vid behandling av trafikuppgifter. Denna bestämmelse innebär att trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver anmälningspliktig verksamhet ska utplånas eller avidentifieras när det inte längre behövs för att överföra ett elektroniskt meddelande.

Från huvudregeln finns undantag som tillåter att trafikuppgifter sparas för viss behandling. Enligt 6 kap 6 § får trafikuppgifter sparas och behandlas om det krävs för operatörens abonnentfakturering eller betalning av samtrafikavgifter till dess fordran är betald eller preskription har inträtt och det inte längre lagligen går att göra invändningar mot faktureringen eller avgiften.

Om ett beslut om hemlig teleövervakning eller hemlig teleavlyssning finns för en viss adress i ett elektroniskt kommunikationsnät gäller inte skyldigheten att utplåna eller avidentifiera meddelanden som benhandlas till eller från den adressen, enligt 6 kap 8 § 2p LEK.

Det finns ytterligare undantag huvudregeln men dessa utvecklas inte närmare då deras innebörd faller utanför syftet med framställningen.

6.3 Myndigheters tillgång till trafikuppgifter

För flertalet uppgifter som nät- eller tjänsteoperatörer får del av eller tillgång till gäller tystnadsplikt, enligt 6 kap 20 § LEK. Denna rör enligt paragrafens första stycke:

> *1. uppgift om abonnemang,*
> *2. innehållet i ett elektroniskt meddelande, eller* [124]
> *3. annan uppgift som angår ett särskilt elektroniskt meddelande*[125]

[123] Prop. 2002/03:110, s. 248.
[124] Begreppet ”elektroniskt meddelande” knyter an till definitionen av ”kommunikation” i 2002/58/EG art 2 och avser all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst.

Med utgångspunkt i tystnadsplikten innehåller LEK regler som ger de brottsbekämpande myndigheterna möjlighet att vid misstanke om brott få ut uppgifter om ett visst elektroniskt meddelande, med undantag från innehållet i detta. Bestämmelserna om utlämnande är formulerade som undantag från tystnadsplikten och återfinns i 6 kap. 22 § 1 st. 3 LEK. Det anges där att den som fått del av eller tillgång till sådan uppgift som tystnadsplikten gäller för på begäran ska lämna denna uppgift till den brottsbekämpande myndighet som har att ingripa mot brottet. Dessa regler står i konkurrens med reglerna om hemlig teleövervakning men angår endast historiska uppgifter. I övrigt är det i princip fråga om samma typ av uppgifter som de båda lagarna reglerar.[126]

Den enda begränsning som uppställs vid brytande av tystnadsplikten till förmån för den myndighet som ska ingripa mot brott är brottsmisstanken måste avse ett brott för vilket det inte är föreskrivet lindigare straff än fängelse i två år. Detta innebär att begäran inte kan gälla försöks-, förberedelse-, eller stämplingsbrott.[127]

[125] Med annan uppgift avses i princip trafikuppgifter, se PTS, *sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter*, s. 5.
[126] SOU 2007:76, s. 62ff.
[127] 23 kap. 1 och 2 §§ BrB.

7 Jämförelse mellan regelverken för utlämnande av trafikuppgifter

Som framgår av framställningen ovan finns det i svensk rätt två olika regelverk som möjliggör för de brottsbekämpande myndigheterna att ta del av uppgifter som uppstår i och med elektronisk kommunikation; reglerna i rättegångsbalken angående hemlig teleövervakning samt reglerna för utlämnande av trafikuppgifter i LEK. De två regelsystemen har ett flertal beröringspunkter vad avser deras syfte samt de brottsbekämpande myndigheternas användningsområden för dem. Samtidigt finns det viktiga skillnader mellan de båda regelverken, vad gäller främst hur skyddet för den personliga integriteten tillgodoses samt vilka rättssäkerhetsgarantier som omgärdar processen. I det följande kapitlet utförs en jämförande genomgång av regelverkens väsentliga delar, angående användningsområdet i allmänhet och integritets- och rättssäkerhetsskyddet i synnerhet.

7.1 Vilka uppgifter som omfattas

Då hemlig teleövervakning infördes avsåg tillämpningsområdet endast framtida trafikuppgifter och uppgifter som hänförde sig till förfluten tid omfattades alltså inte. Denna ordning framkom ingalunda klart vare sig i lagtextutförandet eller i förarbetena.[128] Att detta var lagstiftarens mening kunde istället utrönas genom vissa uttalanden som gjordes i förarbetena till telelagen.[129] Oklarheten hade då lett till att tillstånd till teleövervakning hade beviljats av domstol till att gälla även förfluten tid, en möjlighet som således inte varit lagstiftarens mening. Förhållandet föranledde kritik från JO som menade på att oklarheten i lagtexten var otillfredsställande. Samma bedömning gjordes då buggningsutredningen utförde en översikt av tvångsmedelsregleringen. Förhållandet att ett beslut om hemlig teleövervakning inte gav tillgång till historiska uppgifter sågs dessutom som en brist av de brottsutredande myndigheterna då sådan information kunde vara av stor vikt, bl.a. för att kartlägga kontaktnät och kunna styrka att det vid en viss tidpunkt förekommit kontakt mellan olika personer.[130] På grundval av detta lade buggningsutredningen fram ett förslag på att tillämpningsområdet för hemlig teleövervakning skulle vidgas till att även omfatta historiska uppgifter. Förslaget togs upp oförändrat i denna del i propositionen 2002/03:74 - *Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering*, och infördes i rättegångsbalken den 1 oktober 2004.

[128] Jmf prop. 1988/89:124, s. 47ff.
[129] SOU 1992:70, s. 329, prop. 1992/93:200, s. 258.
[130] SOU 1998:46, s. 275-317.

Utlämnande av uppgifter genom reglerna i 6 kap. LEK tar endast sikte på historiska uppgifter. Reglerna tillkom under Televerkets tid av faktisk, men inte formell, monopolställning på den svenska marknaden för teletjänster. Televerket var ett affärsdrivande verk samtidigt som det var en myndighet, och var som sådan underkastad tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet. I likhet med andra myndigheter upprätthölls skyddet för den personliga integriteten genom att sekretesslagens bestämmelser inskränker offentlighetsprincipen.[131] Sekretessen kunde dock brytas om uppgiften behövdes i brottsutredande verksamhet.[132]

Televerket ombildades 1993 till det statliga aktiebolaget Telia AB och samtidigt överfördes myndighetsfunktionerna till den fristående Post- och telestyrelsen. I samband med detta infördes Telelagen (1993:597) som bl.a. skulle reglera de nya telepolitiska målen. Då teleområdet i och med avskaffandet av Televerkets de facto monopol öppnades upp för enskilda, privata teleaktörer behövde regleringen av uppgifters utlämnanden förändras. Detta eftersom sekretessbestämmelserna som var tillämpliga på myndigheten Televerket inte gällde för de privaträttsliga subjekt för vilka marknaden nu öppnades. För att inte försämra integritetsskyddet för teleanvändare eller möjligheterna att i brottsutredande syfte kunna inhämta uppgifter infördes ett system med tystnadsplikt för teleföretag angående uppgifter om telemeddelanden samt bestämmelser om undantag från denna till förmån för de brottsbekämpande myndigheternas verksamhet.[133] Då telelagen senare ersattes av lagen om elektronisk kommunikation överfördes nämnda reglering i stort sett i sin helhet till den nya lagen.[134]

Innebörden av ovan nämnda är att sedan regleringen i rättegångsbalken angående vilka uppgifter ett beslut om hemlig teleövervakning får avse förändrades under 2004 finns det två olika regelverk som parallellt och oberoende av varandra ger de brottsbekämpande myndigheterna möjlighet att begära ut uppgifter som är hänförliga till förfluten tid. Oavsett vilket lagrum ett utlämnande av uppgifter stödjer sig på gäller det dock i princip samma typ av uppgifter.[135] Det kan således röra sig om exempelvis uppgifter om kommunikationsmeddelandets ursprung, destination, färdväg, datum, tid, storlek, varaktighet eller typ av kommunikationstjänst som används.

[131] 9 kap. 8 § 2 st. SekrL.
[132] 14 kap. 2 § 1 st. SekrL.
[133] SOU 1992:70, s. 324ff, prop. 1992/93:200, s. 162f.
[134] SOU 2002:60, s. 506, prop. 2002/03:110, s. 397.
[135] SOU 2005:38, s. 129, SOU 2007:76, s. 62.

7.2 Förutsättning avseende brottets svårighetsgrad

Hemlig teleövervakning kan som huvudregel endast användas i förundersökningar av brott som har ett straffminimum på sex månaders fängelse. Då tvångsmedelskommittén 1981 i sitt delbetänkande, Ds Ju 1981:22, presenterade ett förslag på införandet av tvångsmedlet i rättegångsbalken ansåg man att det för tvångsmedlets användande skulle räcka med att det fanns fängelse med i straffskalan för brottet. Förslaget blev, bl.a. av denna anledning, hårt kritiserat av remissinstanserna vilket ledde till att kommitténs slutgiltiga förslag modifierats på en mängd punkter. Bl.a. förordades i slutbetänkandet istället en minimigräns på sex månaders fängelse.[136] I den efterföljande propositionen ansågs inte hemlig teleövervakning vara lika integritetskränkande som hemlig teleavlyssning och därmed inte heller ställa lika höga krav på brottets svårighetsgrad. Avgränsningen på sex månaders straffminimum ansågs godtagbar och detta var den gräns som infördes då lagstiftningen trädde i kraft 1989.[137]

Utlämnande enligt LEK uppställer ett krav på att det för brottet inte ska vara föreskrivet lindrigare straff än fängelse i två år. Till skillnad mot vad som gäller angående hemlig teleövervakning omfattas alltså inte försöks-, förberedelse- och stämplingsbrott av regleringen i enlighet med vad som anges i 23 kap. 1 och 2 §§ brottsbalken. Minimigränsen på två års fängelse har sin grund i de bestämmelser som gällde för Televerkets utlämnande genom undantag i sekretesslagen. I förarbetena till regleringen ansåg man att det kunde röra sig om väldigt känsliga uppgifter för enskilda personer och att det därför inte var berättigat att sätta gränsen lägre då detta skulle leda till en alltför långtgående uppmjukning av sekretessbestämmelserna.[138]

Vad gäller brottets svårighetsgrad uppställer alltså LEK högre krav för utlämnande av uppgifter än vad som är fallet vid hemlig teleövervakning.

7.3 Misstankegrad och utpekad teleadress

Tvångsmedelskommittén framförde i sitt delbetänkande förslag om att hemlig teleövervakning skulle kunna användas innan det fanns någon misstänkt gärningsman. I likhet med kommitténs förslag om straffminimum kritiserades detta av remissinstanserna vilket ledde till att förslaget i slutbetänkandet var att misstankegraden skulle sättas till den lägre nivån ”kan misstänkas”. I den följande propositionen ansågs inte denna låga misstankegrad vara godtagbar då en sådan nivå inte ens gällde för tvångsmedlets användande genom 1952 års tvångsmedelslag vid utredande av allvarlig brottslighet som exempelvis brott mot rikets säkerhet. För att

[136] SOU 1984:54, s. 233ff.
[137] Prop. 1988/89:124, s. 48ff.
[138] Prop. 1983/84:142, s. 39.

inte öppna upp möjligheterna för en tvångsmedelsanvändning på alltför lösa grunder och därmed öka risken för oacceptabla integritetsintrång ansågs ett krav på skälig misstanke krävas.[139]

Hemlig teleövervakning innehåller även krav på att beslutet ska avse en i förväg utpekad teleadress med anknytning till den misstänkte. Kravet gällde vid tvångsmedlets införande i rättegångsbalken endast sådana telefonapparater som innehades av den misstänkte eller som kunde antas komma att användas av den misstänkte. En utvidgning till att omfatta även telefonapparater som den misstänkte kunde förväntas kontakta diskuterades vid införandet men avfärdades då risken att för brottsutredningen helt ovidkommande personer skulle drabbas ansågs allt för stor.[140] Denna utvidgning kom senare att införas genom lagändringen den 1 oktober 2004, dock med ett högre krav på anknytning mellan den misstänkte och den ifrågavarande teleadressen. Förutsättningen i nu rådande reglering är således att det ska finnas synnerlig anledning att anta att den misstänkte kommer att ta kontakt med teleadressen. Detta innebär att man ska vara så gott som säker på att teleadressen kommer kontaktas av den misstänkte och detta ska stödjas av tillförlitliga uppgifter.[141]

I LEK uppställs det inget krav på att det ska finnas en för brottet misstänkt person, d.v.s. det saknas helt krav på misstanke av någon grad. I och med att det inte uppställs krav på att brottsutredningen ska kunna utpeka en potentiell gärningsman kan därmed uppgifterna komma att inhämtas vid ett mycket tidigt skede i utredningen. På grund av detta är risken stor för att inhämtningen i efterhand kan visa sig vara helt obefogad och därmed ha drabbat en oskyldig, vilket var vad som uttryckligen ville undvikas då man vid hemlig teleövervakning valde krav på misstankegrad. Väger man dessutom in att det i LEK saknas ett krav på anknytning mellan person och teleadress förstoras därmed risken för det eventuella integritetsintrånget ytterligare.

Då dessa väsentliga begränsningar saknas öppnas möjligheterna för att genom LEK inhämta uppgifter om en mycket stor personkrets. Inget hinder uppställs för att uppgifter hämtas in om såväl misstänkt gärningsman som målsägande, vittne eller tredje man. Om uppgiften angår misstanke om ett grövre brott och således uppfyller straffvärdets minimum kan uppgifter alltså inhämtas i stort sett utan begränsning i fråga om vem uppgifterna rör. Detta förhållande gör det möjligt att för de brottsbekämpande myndigheterna att begära om s.k. basstationstömning där uppgifter tas fram om vilka telefonnummer eller telefoner som haft kontakt med en viss basstation under en tidsperiod. Genom denna metod kan uppgifter inhämtas om t.ex. alla mobiltelefoner som befunnit sig inom ett visst område, t.ex. i närheten av en brottsplats, under en viss tidpunkt.[142] Innebörden blir därmed

[139] Prop. 1988/89:124, s. 47ff.
[140] Prop. 1988/89: 124, s. 45f.
[141] Prop. 2002/03:74, s. 38.
[142] SOU 2007:76, s. 65.

att uppgifter hänförliga till ett i det närmast oöverskådligt antal personer, som för brottsutredningen är helt ovidkommande, tillgängliggörs.

7.4 Betydelse för utredningen

För hemlig teleövervakning gäller begränsningen att åtgärden måste vara av synnerlig vikt för utredningen för att den ska få tillgripas. Bedömningen om ifall detta krav är uppfyllt ska göras vid varje enskilt fall och betyder att uppgifterna som inhämtas kan förväntas nå upp till en viss kvalitet samt att någon mindre ingripande åtgärd inte kan ge samma resultat.[143]

I LEK uppställs det inget krav på att uppgifternas utlämnande ska vara av betydelse för utredningen. Detta innebär att det inte behöver föreligga någon förväntning på att de uppgifterna som inhämtas kommer att tillföra utredningen något väsentligt över huvud taget. Med andra ord kan uppgifter begäras ut trots att mindre ingripande, mindre resurskrävande samt mer tidssparande åtgärder istället kunde ha tillgripits.

Som jämförelse kan nämnas vad JO uttryckte i ett granskningsärende som bl.a. gällde hemlig teleavlyssning, vilket innehar samma krav som hemlig teleövervakning vad gäller betydelsen för utredningen. I fallet hade hemlig teleavlyssning tillgripits för att få fram uppgifter om var en person, som var häktad i sin frånvaro, befann sig. JO ansåg det vara tveksamt ifall åtgärden kan användas då vinsterna enbart är av indirekt betydelse för brottsutredningen.[144]

7.5 Beslutsförfarandet

Reglerna i rättegångsbalken om straffprocessuella tvångsmedel ger uttryck för en grundläggande princip. Ju mer ingripande ett tvångsmedel är för den enskilde desto högre krav uppställs på beslutsfattarens kompetens. Besluten om de mest ingripande tvångsmedlen är förbehållen domstolen. För större delen av de tvångsmedel som inte kräver domstolsprövning har åklagaren beslutanderätt medan en polisman har en mycket snävare beslutsbehörighet. Anledningen är att det anses krävas större juridiska kunskaper ju mer ingripande en tvångsåtgärd är.[145]

De hemliga tvångsmedlen är till sin natur de som innebär störst intrång ur en integritetsaspekt och behörigheten att besluta om dess användande tillkommer därför domstol. Dock har inte domstol en rätt att besluta om åtgärden ex officio utan det krävs en begäran från åklagare. En av de främsta anledningarna till att denna beslutsstruktur valdes var att hemlig teleavlyssning och hemlig teleövervakning genom sitt element av hemlighållande skiljer sig åt från de flesta övriga tvångsmedel. Vanligtvis

[143] Prop. 1988/89:124, s. 44f.
[144] JO 1994/95, s. 34.
[145] Lindberg, s. 62.

verkställs tvångsmedel öppet och den de används mot blir därmed generellt sett medveten om åtgärden och kan med hjälp av olika rättsmedel få lagligheten av ingripandet prövat av exempelvis domstol, överordnad myndighet, JO, eller JK. Då själva syftet med de hemliga tvångsmedlen är att den de används mot inte ska få vetskap om att han eller hon står under övervakning fråntas därmed den övervakade denna möjlighet. För att säkerställa att den misstänktes intressen och andra integritetsintressen tillvaratas står alltså domstolen som en motpol till förundersökningen.[146]

LEK innehåller inte en så strikt beslutsstruktur. Lagtexten talar om utlämnande till åklagarmyndighet, polismyndighet eller annan myndighet som ska ingripa mot brottet.[147] Detta öppnar för att bl.a. var polisman, tulltjänsteman, åklagare eller tjänsteman på annan myndighet som ska ingripa mot brottet i praktiken kan begära ut uppgifterna.

När en begäran om utlämnande av uppgifter enligt 6 kap. 22 § 3 LEK framställs har operatören vare sig skyldigheten eller rätten att göra någon självständig prövning av den begärande myndighetens behov av uppgifterna.[148] Denna ordning uppstod som en konsekvens av hur den tidigare regleringen för utlämnande var utformad i sekretesslagen. Då Televerket som myndighet hade ett de facto monopol på teleområdet innebar sekretesslagens regler nämligen att det var den utlämnande myndigheten som hade att pröva ifall förutsättningarna för utlämnandet var uppfyllda och gjorde denna prövning under myndighetsansvar. Då nya privaträttsliga aktörer skulle släppas in på telemarknaden valde man i telelagen därför systemet med tystnadsplikt för att undvika att överföra denna myndighetsfunktion på de nya aktörerna. Enligt uttalande i propositionen till telelagen skulle avvägningen mellan enskildas personliga integritet och det allmännas intresse att bekämpa brott inte lämpligen göras av ett privaträttsligt subjekt och därför lades denna uppgift på den myndighet som begärde ut uppgifterna.[149]

Samma historiska uppgifter som genom rättegångsbalkens regler kräver en skriftlig framställning från en åklagare samt en prövning av en lagfaren domare för att kunna utlämnas kan alltså med hjälp av LEK begäras ut av en stor krets personer, utan rättslig förprövning och utan en självständig prövning av den utlämnande parten.

7.6 Tillståndstiden

Ett beslut om hemlig teleövervakning måste alltid innehålla en angivelse av för vilken tid beslutet gäller. Vad gäller historiska uppgifter finns i lagtexten

[146] Prop. 1988/99:124, s. 50ff.
[147] Se 6 kap. 22 § 3 p. LEK.
[148] PTS, *sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter*, s. 7.
[149] Prop. 1992/93:200, s. 162ff.

ingen angiven maximal tillståndslängd men övervakningen får aldrig bestämmas längre än vad som är nödvändigt.[150]

LEK uppställer ingen begränsning på för hur lång tid uppgiftslämnandet får omfatta, eller med andra ord hur gamla uppgifterna som begärs ut får vara. Utlämnandet begränsas dock i praktiken av huvudregeln i 6 kap. 5 § LEK om avidentifiering och utplåning av trafikuppgifterna, vilket naturligtvis även begränsar utlämnande med stöd av reglerna i rättegångsbalken i fråga om historiska uppgifter.

7.7 Underrättelseskyldighet och säkerhets- och integritetsskyddsnämnden

Som en huvudregel i svensk rättsordning ska den som blir föremål för myndighetsutövning underrättas om det, oavsett om denne är misstänkt för något brott eller inte. Denna ordning har i rättegångsbalkens regler bl.a. inneburit att den som blir utsatt för en husrannsakan eller ett beslag och inte varit närvarande vid verkställandet ska underrättas om ingreppet i efterhand.[151] Trots att ett införande diskuterats vid ett flertal tillfällen tidigare fanns det dock inte någon motsvarande möjlighet i fråga om hemliga tvångsmedel förrän den 1 januari 2008.[152] Reglerna återfinns numera i 27 kap. 31 § RB.

Redan tidigare gällde dock ordningen att den misstänkte som blir föremål för åtal har rätt att ta del av förundersökningens hela utredningsmaterial vid utnyttjande av sin rätt till partsinsyn.[153] Vid den s.k. slutdelgivningen har den misstänkte och dennes försvarare rätt att få del av hela förundersökningsmaterialet och därmed även om ett hemligt tvångsmedel har använts under förundersökningen.[154]

En särskild underrättelse till enskild som varit utsatt för ett hemligt tvångsmedel, utöver vad som gäller angående åtalades rätt till partsinsyn, infördes som ovan nämnts i början av 2008. Anledningen till införandet var att den utsatte ska kunna få möjlighet att undersöka om tvångsmedelsanvändningen har skett i enlighet med gällande regler. Då processen runt de hemliga tvångsmedlen, domstolarnas prövning samt de brottsbekämpande myndigheternas verkställande, är kringgärdad av sekretess är allmänhetens insyn i övrigt starkt begränsad. Genom underrättelseskyldigheten ges den enskilda möjligheten att självständigt

[150] 27 kap 21 § RB.
[151] Lindberg, s. 81f.
[152] Se bl.a. SOU 1998:46, s. 436f. och prop. 2005/06:177, s. 46f.
[153] 23 kap. 18 § RB.
[154] SOU 2006:98, s. 47f.

tillvarata sin rätt genom att exempelvis få det prövat om han eller hon blivit utsatt för en felaktig användning av det hemliga tvångsmedlet.[155]

Underrättelseskyldigheten gäller för alla de hemliga tvångsmedlen utom postkontroll. Kravet på anknytning till teleadress för hemlig teleövervakning för med sig att den som tvångsmedlet riktas mot inte nödvändigtvis behöver sammanfalla med innehavaren av teleadressen. På grund av detta gäller skyldigheten för underrättelse inte bara mot den som misstänkts för brott utan även andra som kan ha blivit drabbade av tvångsmedelsanvändningen, exempelvis innehavaren av den övervakade teleadressen.[156]

Samtidigt som underrättelseskyldigheten infördes inrättades även säkerhets- och integritetsskyddsnämnden som en fristående myndighet under regeringen med uppdrag att genom inspektioner och andra undersökningar utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel.[157] Då underrättelsen om tvångsmedelsanvändning till enskild i många fall kan vara begränsad p.g.a. sekretessbestämmelser och därför inte vara tillräckligt omfattande för att den enskilde ska kunna avgöra lagenligheten med åtgärden kan nämnden även på begäran av enskild utföra en kontroll om användningen skett i strid med gällande författningar. För att nämnden ska kunna utföra dessa kontroller gäller en uppgiftsskyldighet med sekretessbrytande effekt för de myndigheter som granskas.[158]

Nämndens tillsyn kan utmynna i uttalande till regeringen, till den granskade myndigheten eller till enskild. Nämnden har däremot inte befogenhet att överpröva ett beslut av den granskade myndigheten eller besluta om rättelser vid konstaterade felaktigheter. Om tillsynen av en myndighet resulterar i att ett brott uppdagats ska nämnden anmäla detta till åklagarmyndigheten. Grundar felaktigheten skadeståndsansvar gentemot enskild ska detta anmälas till den myndighet som utpekas av förordningen (1995:1301) om handläggning av skadeståndsanspråk mot staten för prövning.[159]

Då reglerna i LEK använts för utfående av uppgifter finns det ingen motsvarighet till underrättelseskyldigheten. Om utredningen av brottet leder fram till att någon anses som skäligen misstänkt och därmed ska underrättas enligt reglerna om partsinsyn får denne person insyn i förundersökningen och därmed även det förhållande att uppgifterna har begärts ut. I annat fall finns det inte någon skyldighet för myndigheten som begärt ut uppgifterna att underrätta om åtgärden och detta gäller oavsett om den vars uppgifter har begärts ut själv varit misstänkt för brott, är målsägande eller om denna endast har koppling till utredningen som tredjeman. Därmed finns inte heller någon möjlighet för den enskilde att bli medveten om, och än mindre påtala, eventuellt begångna fel eller försummelser vid myndighetsutövningen.

[155] SOU 2006:98, s. 77ff.
[156] Prop. 2006/07:133, s. 38.
[157] Se Lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet, 1 och 2 §§.
[158] Prop. 2006/07:133, s. 67.
[159] Prop. 2006/07:133, s. 69f.

Utlämnande enligt LEK omfattas inte heller av integritets- och säkerhetsskyddsnämndens tillsynsområde då detta i aktuellt hänseende endast omfattar de hemliga tvångsmedlen. Trots att det ofta rör sig om samma uppgifter som lämnas ut oavsett om begäran har sin utgångspunkt i rättegångsbalken eller LEK utgör inte den senare i formell mening ett tvångsmedel.[160]

7.8 Parlamentarisk kontroll och statistik

För att i viss mån kompensera för den bristande insyn som av nödvändighet gäller för de hemliga tvångsmedlen används en form av parlamentarisk kontroll över dess användning. Kontrollen innebär att regeringen, i en årlig skrivelse till riksdagen, redovisar tillämpningen av bestämmelserna om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning.[161] Skrivelsen grundar sig på uppgifter som sammanställs av Åklagarmyndigheten och Rikspolisstyrelsen. I skrivelsen redovisas, för var och ett av tvångsmedlen, bl.a. antalet beviljade och avslagna ansökningar, vilket brott misstanken har avsett, den genomsnittliga övervakningstiden samt ett effektivitetsmått i form av vilken betydelse tvångsmedlen haft för brottsutredningarna.[162] Kontrollen fyller syfte som en allmän överblick över användningen av de hemliga tvångsmedlen men då uppgifterna är offentliga och därmed avidentifierade erbjuder den ingen övervakning av enskilda fall.

För hemlig teleövervakning har antalet beviljade tillstånd stadigt ökat sedan år 1999. Då var det totala antalet 297 st. vilket kan jämföras med 1119 st. beviljade tillstånd under år 2006. Förklaringen till ökningen anger man i skrivelsen som en konsekvens av bl.a. en mer organiserad brottslighet som involverar ett större antal personer varvid det oftare är fler misstänkta personer inom ramen för en samma förundersökning. Även den ökade internationaliseringen för brottsligheten nämns som en anledning.[163]

Vad gäller avslagna ansökningar är antalet mer blygsamt. År 2003 avslogs sju st., år 2004 endast en, år 2005 elva st. och år 2006 fjorton st.[164] Under de senaste tre skrivelserna har det låga antalet beskrivits med samma förklaring: underlagen som presenteras för domstolen är välgrundade och har föregåtts av en noggrann avvägning vad gäller behovet, proportionaliteten samt möjligheten att använda andra spaningsmetoder.[165] Anledningen anses alltså vara att ansökningarna näst intill uteslutande varit berättigade.

---

[160] Se SOU 2007:76, s. 238 och 282, Ds 2005:53, s. 27.
[161] Rskr. 1981/82:298, bet. 1981/82:JuU54 och prop. 1995/96:85, s. 37.
[162] Jfr. skr. 2007/08:34.
[163] Skr. 2007/08:34, s. 14f.
[164] skr. 2004/05:36 s. 10, skr. 2005/06:53, s. 12, skr. 2006/07:28, s. 11, skr. 2007/08:34, s. 11.
[165] Se t.ex. skr. 2007/08:34, s. 16.

Skrivelserna innehåller även ett mått på hur effektiv tvångsmedelsanvändningen har varit genom att redogöra för det antal fall där åtgärden haft betydelse för förundersökningen i fråga om den misstänkte. Resultatet av mätningen framställs genom att se på i hur många fall per år som åtgärden lett till användningen av ett annat tvångsmedel, t.ex. att den misstänkte grips, anhålls eller häktas. Detta effektivitetsmått fluktuerar vanligtvis ett par procentenheter varje år men har under de senaste tio åren legat någonstans mellan 40 och 50 procent.[166] Enligt regeringens bedömning innebär detta dock inte att tvångsmedlet i resterande fall varit resultatlöst. Åtgärden kan ha fört utredningen framåt trots att den inte lett till användningen av ett annat tvångsmedel[167], ingripande kan ha gjorts mot annan än den misstänkte och åtgärden kan ha gjort att misstankarna mot en person avfärdats.[168]

Över hur många fall årligen som de brottsbekämpande myndigheterna begär uppgifter från operatörerna genom reglerna i LEK förs det ingen statistik. Vid användningen av hemlig teleövervakning går ett utlämnande alltid genom Säkerhetspolisen som sköter all kontakt med operatören, vilket underlättar sammanställningen av hur många fall vari åtgärden utnyttjas. Som nämnts ovan sker begäran av uppgifter enligt LEK mer formlöst av varje begärande myndighet för sig och kan utföras av exempelvis en enskild polisman eller tulltjänsteman. Detta förhållande leder till att de siffror som finns om användningen av sistnämnda regelverk endast utgör uppskattningar.

I ett delbetänkande av Beredningen för rättsväsendets utveckling (BRU) analyseras behovet av trafikuppgifter för brottsbekämpningen. Det konstateras att tillgången till sådana uppgifter är en av de viktigaste faktorerna för att förundersökningar i grövre brott över huvud taget kan föras framåt och att dess betydelse inte kan överskattas. Metoden används i stort sett i alla utredningar som rör grövre brott och Säkerhetspolisen uppskattade att runt år 2004 inhämtades uppgifterna med stöd av reglerna i LEK i ca 4000 fall årligen. Säkerhetspolisen drog även slutsatsen att historiska trafikuppgifter är av större betydelse för brottsutredningar än vad realtidsuppgifter är.[169]

Trafikuppgiftsutredningen hänvisade till uppskattningen som gjordes av BRU och konstaterade samtidigt att en ny uppskattning gjord av polisen två år senare visar att antalet fall av utlämnande genom LEK ökat ansenligt till ca 8000 fall årligen.[170]

---

[166] Se skr. 2007/08:34, s. 11.
[167] Dock inkluderade effektivitetsmåttet fram till och med år 2004 även de fall då åtgärden på annat sätt lett till att förundersökningen förts framåt. Ändringen har dock inte påverkat statistiken i någon större utsträckning.
[168] Se exv. skr. 2007/08:34, s. 18.
[169] 2005:38, s. 323.
[170] SOU 2007:76, s. 130.

En jämförelse mellan regleringen för utlämnande i rättegångsbalken respektive LEK ger vid handen att den sistnämnda uppskattningsvis används i mer än 6500 fler fall årligen. Att LEK används i större omfattning än reglerna om teleövervakning framgår även om man ser till uttalandet som Säkerhetspolisen gjorde om just historiska uppgifters betydelse och jämför det med den relativt blygsamma ökningen av antalet beviljade teleövervakningsansökningar i direkt anslutning till att det år 2004 blev möjligt att få ut just historiska uppgifter genom tvångsmedlet.[171] Troligt är att uppgifterna tenderar att inhämtas med stöd av LEK:s regler snarare än genom reglerna i rättegångsbalken då reglernas förutsättningar tillåter det.

Om effektivitetsmåttet för hemlig teleövervakning är giltigt som måttstock även för uppgiftsinhämtning genom LEK innebär det att det i ungefär 4000 fall årligen begärs ut uppgifter som inte har betydelse för förundersökningen mot den misstänkte. Det ska dock klargöras att en sådan jämförelse givetvis är behäftad med vissa felkällor. Förutom de som nämndes ovan för effektivitetsmåttet i stort påpekas även av BRU att det ofta är så att uppgifterna så att säga ”sätter polisen på spåret” och därigenom i viss mån ändå kan anses föra förundersökningen framåt. Detta antyder att tvångsmedlet i realiteten kan anses vara mer effektivt än vad siffrorna faktiskt visar. I motsatt riktning kan man anföra att tvångsmedelsanvändningen har, som ovan beskrivits, föregåtts av flertalet noggranna avvägningar medan detta inte är fallet för utlämnande enligt LEK. Rimligtvis borde effektiviteten vara än lägre då åtgärden inte gått igenom sådana prövningar innan dess användning och det inte heller i övrigt uppställs lika hårda krav för när åtgärden får användas. Att använda effektivitetsmåttet för en sådan jämförelse bör alltså inte ses som ett exakt tvärsnitt av hur det verkligen förhåller sig, men kan sannolikt godtas som en fingervisning.

Det bör påpekas att Trafikuppgiftsutredningen föreslår att statistik ska föras över när utlämnande sker, oavsett vilken lag åtgärden stöds på. Ett krav på sådan statistik följer uttryckligen av artikel 10 i datalagringsdirektivet. Statistiken ska bl.a. avse antalet verkställda beslut och vilken lag dessa stöds på, vilken typ av brott ärendet avser samt i hur många ärenden operatören inte kunnat tillgodose begäran.[172] Statistikens syfte verkar dock vara att få till stånd en effektivitetskontroll av själva utlämningssystemet och således inte en motsvarighet till den parlamentariska kontrollen av tvångsmedlen. Ingen mätning ska exempelvis göras över uppgifternas betydelse för utredningen.

7.9 Proportionalitetsprincipen

Som nämnts har proportionalitetsprincipen kommit till direkt uttryck i samtliga tvångsmedelskapitel i rättegångsbalken. Denna ordning föreslogs

[171] Jfr tabell i skr. 2007/08:34, s. 9.
[172] SOU 2007:76, s. 281.

1984 i Tvångsmedelskommitténs betänkande. Kommittén påpekade att dessa principer var gällande för all utövning av tvångsmedelsbefogenheter men att avsaknaden av ett faktiskt lagstöd för tvångsmedelsanvändningen sågs som en brist.[173] I propositionen som följde var man av samma uppfattning. För att principerna skulle uppmärksammas tillräckligt vid tvångsmedelsanvändningen ansågs inte en hänvisning till mer eller mindre underförstådda rättsgrundsatser som tillräckligt utan ett klart lagstöd ansågs behövligt.[174]

I LEK finns ingen motsvarande hänvisning till proportionalitetsprincipen i kapitel 6 som reglerar utlämnandet av trafikuppgifter. Dock framgår det av 1 kap. 2 § att:

”*Åtgärder som vidtas med stöd av denna lag får inte vara mer ingripande än som framstår som rimligt och skall vara proportionella med hänsyn till lagens syfte och de övriga intressen som anges i 1 §.* “

Lagens syften och de övriga intressen som paragrafen hänvisar till är dock som bekant inte främst samhällets brottsbekämpning eller skyddet för personers integritet utan syftar snarare till att garantera säkra och effektiva kommunikationstjänster. Den proportionalitetsprincip som anges här kan därmed inte anses få någon betydande verkan vad gäller utlämnandet av trafikuppgifter för brottsbekämpning.

För polisens verksamhet finns principen reglerad i 8 § polislagen (1984:387). För tullens del finns kravet på proportionalitet reglerat i bl.a. 6 kap. 1 § tullagen (2000:1281). Generellt anses principen också gälla utan uttryckligt lagstöd vid ingripande åtgärder från myndigheternas sida mot enskilda.[175]

Sammantaget kan alltså sägas att ett utlämnande av trafikuppgifter kan förutsättas ske efter en tillämpning av proportionalitetsprincipen oavsett vilket regelverk detta stödjer sig på. Dock ska det i sammanhanget nämnas att det för tvångsmedlen gäller en dubbel avvägning mot principen, dels då beslut om ingreppet tas i domstol och dels vid verkställandet av tvångsmedlet, varvid polislagens reglering får en självständig betydelse.[176]

7.10 Kritik mot rättsläget

Förhållandet med de två olika regelverken som i praktiken erbjuder väldigt liknande möjligheter för de brottsbekämpande myndigheterna att få tillgång till trafikuppgifter samtidigt som de uppvisar stora skillnader i rättssäkerhetsgarantier för den enskilde har föranlett kritik från olika håll i lagstiftningsarbetet. Redan Telelagsutredningen påpekade att det borde

[173] SOU 1984:54, s. 48 och 77ff.
[174] Prop. 1988/89:124, s. 27.
[175] SOU 2007:76, s. 231.
[176] Jmf. Lindberg, s. 30.

övervägas att endast reglera utlämnande av uppgifter i rättegångsbalken. Utredningen menade dock att denna övervägning borde göras i ett annat sammanhang.[177]

Förslaget som Telelagsutredningen presenterade kritiserades i remissförfarandet av bl.a. JO och RÅ som pekade på bristerna avseende rättssäkerhetsgarantier vid utlämnande av uppgifterna. I propositionen, 1992/93:200 *om en telelag och en förändrad verksamhetsform för Televerket, m.m.*, bemöttes kritiken huvudsakligen genom att skillnaderna i rättegångsbalken och den föreslagna regleringen påpekades. En tvångsmedelsanvändning ansågs innebära ett planerande av att ta in framtida uppgifter medan telelagens regler förutsatte att uppgifterna redan fanns tillgängliga. Dock ansåg regeringen att frågan om de inneboende skillnaderna borde tas upp i ett annat sammanhang.[178]

I buggningsutredningens direktiv ingick att se över regleringen av utlämnande av uppgifter och lämna förslag på en samlad reglering i rättegångsbalken. Utredningen föreslog bl.a. att historiska uppgifter skulle kunna inhämtas med stöd av reglerna för hemlig teleövervakning och att reglerna i dåvarande Telelagen därmed skulle bli överflödiga och därför upphävas.[179] Samtidigt ansåg utredningen att det fanns fördelar med regleringen i Telelagen som skulle gå förlorade i och med upphävandet och för att inte försämra förutsättningarna för brottsbekämpningen behövde reglerna för hemlig teleövervakning modifieras. Det föreslogs bl.a. undantag från huvudregeln om kravet på brottsmisstanke mot viss person vid vissa utpekade fall av inhämtning av historiska uppgifter samt möjlighet att övervaka en teleadress som den misstänkte kan antas söka kontakt med.[180]

I lagrådsremissen som följde på betänkandet delades buggningsutredningens bedömningar i stort av regeringen. Det uttrycktes bl.a. att ett regelverk för utlämnande av integritetskänslig information utan krav på domstolsprövning var otidsenligt och mindre förenligt med Europakonventionens syften och krav. En sammanförning av reglerna i rättegångsbalken ansågs som det lagtekniskt mest logiska och samtidigt mest fördelaktigt för den enskilde.[181] Utöver vissa lagtekniska justeringar yttrade inte lagrådet något i frågan om upphävande av de aktuella bestämmelserna i telelagen.

Buggningsutredningens förslag ledde till att det 2004 blev möjligt att inhämta även historiska uppgifter med stöd av reglerna om hemlig teleövervakning samt att tillämpningsområdet utökades till att inte bara avse teleadress som den misstänkte själv använder sig av utan även sådana som denne söker kontakt med. Däremot behandlades inte förslaget om upphävandet av reglerna i telelagen i propositionen med hänvisning till att

[177] SOU 1992:70, s. 329f.
[178] Prop. 1992/93:200, s. 163.
[179] SOU 1998:46, s. 368.
[180] SOU 1998:46, s. 395ff.
[181] Lagrådsremiss, *Hemlig avlyssning m.m.*, 6 april 2000, s. 77.

frågan skulle övervägas inom ramen för en kommande översyn.[182] Värt att anmärka här är att vissa av de förslag som Buggningsutredningen ansåg behövde genomföras angående hemlig teleövervakning som en konsekvens av upphävandet av telelagens regler genomfördes trots att telelagens regler lämnades orörda.

Den översyn som regeringen hänvisat till i ovan nämnda proposition utfördes av beredningen för rättsväsendets utveckling, som lade fram sina förslag i denna del i maj 2005. Beredningen kom fram till samma slutsats rörande uppgiftsutlämnande enligt LEK som buggningsutredningen hade föreslagit gällande telelagen sju år tidigare; reglerna om utlämnande i LEK bör upphävas och istället föras samman i rättegångsbalken. Även BRU ansåg att förslaget på denna punkt skulle innebära en effektivitetsförlust för brottsbekämpningen om inte tvångsmedelsbestämmelserna samtidigt förändrades. I detta syfte föreslogs bl.a. att kraven på skäligen misstänkt gärningsman skulle lättas i vissa situationer. För att inte förlora den snabba procedur som reglerna i LEK medger för utlämnande föreslogs även en rätt för åklagare att fatta interimistiska beslut angående teleövervakning i brådskande fall. En domstol ska sedan i efterhand granska den vidtagna åtgärden.[183] BRU:s förslag bereds för närvarande av Justitiedepartementet.

Även i lagstiftningsförfarandet om datalagringsdirektivets införande har flera kritiska röster höjts mot det aktuella rättsläget. Flertalet remissinstanser menar att förhållandet med de dubbla regelverken för utlämnande av trafikuppgifter är en allvarlig brist ur rättssäkerhetssynpunkt. *Datainspektionen* nämner att det borde ses som ett minimikrav att utlämnandet av uppgifter alltid är underkastat en oberoende rättslig prövning.[184] *Säkerhets- och integritetsskyddsnämnden* anser att reglerna om utlämnande i LEK bör utmönstras och att det vore mest naturligt om nämndens tillsyn inte bara omfattade myndigheters användning av hemliga tvångsmedel utan all tillgång till trafikuppgifter som de brottsbekämpande myndigheterna har.[185] Både JO och JK anser att BRU:s förslag angående att allt utlämnande av trafikuppgifter för brottsbekämpande ändamål ska regleras i rättegångsbalken borde ha inordnats i det nu aktuella lagstiftningsärendet. De menar att detta vore mer naturligt och att rättssäkerheten skulle gagnas av en sammanhållen reglering.[186]

Hans-Olof Lindblom anser i sitt skiljaktiga yttrande i Trafikuppgiftsutredningens betänkande att ett genomförande av BRU:s förslag om att upphäva reglerna om utlämnande i LEK skulle innebära en ökad rättssäkerhet för den enskilde och en förstärkning av integritetsskyddet. Genom att lagringen vid införandet av datalagringsdirektivet blir obligatorisk kommer uppgifter om enskildas

[182] Prop. 2002/03:74, s. 12, 17 och 40.
[183] SOU 2005:38, s. 22ff.
[184] Datainspektionens remissvar i anledning av SOU 2007:76, s. 2.
[185] Säkerhets- och integritetsskyddsnämndens remissvar i anledning av SOU 2007:76, s. 1f.
[186] Justitieombudsmannens remissvar i anledning av SOU 2007:76, s. 5f, Justitiekanslerns remissvar i anledning av SOU 2007:76, s. 1.

kommunikation lagras i mycket större omfattning än tidigare. Detta förhållande menar Lindblom gör det än mer angeläget att åtgärda de skillnader i rättssäkerhetskrav som finns mellan reglerna i LEK och reglerna i rättegångsbalken, särskilt för att nå upp till de krav som ställs i Europakonventionen. Även Per Furberg framför liknande invändningar och ansluter sig i sitt särskilda yttrande till Lindbloms ståndpunkt.[187]

[187] SOU 2007:76, s. 314ff.

8 Europakonventionen

Sverige ratificerade den Europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna 1953 och inkorporerade den i svensk rätt den 1 januari 1995.[188] Därmed kom konventionen samt dess tilläggsprotokoll att gälla så som svensk lag. Genom införandet av bestämmelsen i 2 kap 23 § RF får lag eller annan föreskrift inte meddelas i strid med Sveriges åtagande som konventionsstat.[189] Detta innebär att konventionen ska tillämpas direkt av svenska domstolar och myndigheter men införlivandet har inte givit konventionens regler något formellt företräde framför svensk lag.[190]

Konventionens första artikel ålägger samtliga fördragsslutande parter att garantera var och en som befinner under deras jurisdiktion de fri- och rättigheter som skyddas genom konventionen. Staternas skyldighet att leva upp till sina åtagande enligt konventionen kan prövas av Europadomstolen som behandlar både mellanstatliga mål och enskilda klagomål. Domstolens domar är bindande för den berörda staten men domstolen fungerar inte som någon överinstans till nationella domstolar eller myndigheter. Om domstolen finner att en kränkning ägt rum kan den dock döma ut ett skadestånd till den klagande parten.[191]

I detta sammanhang är det främst konventionens artiklar 8 och 13 som är av intresse varför övriga artiklar lämnas utanför framställningen.

8.1 Artikel 8 – rätt till respekt för privat- och familjeliv, hem och korrespondens

Av de mänskliga rättigheter som är skyddade genom Europakonventionen är det främst artikel 8 som är av betydelse för den personliga integriteten. Genom de begrepp som den innefattar och deras inneboende vaghet blir rättigheten dock svårdefinierad och mångfacetterad. Exempelvis kan ett flertal olika företeelser föras in under begreppet privatliv och för att få en tydligare bild får ledning i första hand sökas i den praxis som utarbetats av Europadomstolen.[192]

Av artikeln följer att:

[188] Inkorporationen skedde genom lag (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna.
[189] Danelius, Hans, *Mänskliga rättigheter i europeisk praxis*, s. 41f.
[190] Bernitz, Ulf; Kjellgren, Anders, *Europarättens grunder*, s.128.
[191] Danelius, s. 24ff.
[192] Danelius, s. 260.

1. *Var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens.*

2. *Offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.*

Den första punkten innehåller själva skyddsstadgandet i artikeln. Detta ska tillförsäkra enskilda ett skydd mot godtycklig myndighetsinblandning och innebär en skyldighet för myndigheter att avhålla sig från ingrepp i den privata sfären. Denna skyldighet gäller inte bara ingrepp i enskilda fall utan även generella inskränkningar i människors frihet att forma sin tillvaro.[193]

Av praxis framgår att artikel 8 inte enbart gäller ett förbud mot ingrepp utan även föreskriver en skyldighet för staten att företa ett positivt handlande för att tillförsäkra skydd för enskildas privata sfär. Det behöver alltså inte ha förekommit ett faktiskt ingrepp från en myndighet eller tjänsteman för att ett brott mot artikeln ska kunna föreligga. Att staten tolererar en viss rådande situation eller inte tillhandahåller ett tillräckligt rättsligt skydd kan utgöra tillräckliga skäl. I huvudsak innebär detta att det åligger staten en plikt att stifta lagar och förordningar för att skyddet för den enskilde upprätthålls på en tillfredsställande nivå.[194]

Av artikelns andra punkt framgår vissa undantagsbestämmelser som möjliggör inskränkningar i rättigheten under förutsättning att vissa villkor är uppfyllda. Om ett ingrepp inte uppfyller dessa villkor är ingreppet konventionsstridigt. De krav som uppställs är att ingreppet måste ske *med stöd av lag* och vara ägnat att tillgodose något av de i punkten uppräknade *allmänna eller enskilda intressena* samt att ingreppet är *nödvändigt i ett demokratiskt samhälle* för att de dessa intressen ska kunna tillgodoses. Vid bedömningen av om det sistnämnda kravet är uppfyllt används proportionalitetsprincipen.[195]

Kravet på laglighet innebär att det måste finnas ett nationellt författningsmässigt stöd[196] för inskränkningen och detta måste uppfylla rimliga krav på rättssäkerhet. Stödet måste ge skydd mot godtycke, vara tillgängligt för allmänheten samt vara utformat med erforderlig precision för att på så vis åstadkomma förutsebarhet i den konventionskränkning dess tillämpning medför. Kravet på förutsebarhet innebär dock inte ett hinder mot att ett visst mått av tolkningsutrymme och skönsmässig bedömning tillåts för den tillämpande myndigheten. Däremot måste ramarna för det

[193] Danelius, s. 261.
[194] Danelius, s. 261f.
[195] Danelius, s. 263.
[196] Det uppställs dock inget krav på att detta stöd ska ligga på någon viss normgivningsnivå.

tillåtna utrymmet vara så pass begränsande att skyddet mot godtycklighet upprätthålls.[197]

De intressekategorier som ingreppet ska tillgodose är breda och allmänt utformade varvid många ändamål kan hänföras hit vilket gör att detta krav vanligtvis går att uppfylla. Däremot innebär det sista kravet, nödvändighetskravet, desto större osäkerhet. Europadomstolen har här uttalat att ordet ”nödvändig” (”necessary”) inte ska uppfattas som synonymt med ”oundgängligt” (”indispensable”). Det som menas är att ingreppet måste svara mot ett ”angeläget samhälleligt behov” (”pressing social need”). Inskränkningen måste dessutom stå i rimlig proportion till det syfte som det ska tillgodose.[198]

För att bedöma nödvändigheten och proportionaliteten av en inskränkning har konventionsstaterna medgivits ett visst tolkningsutrymme (”margin of appreciation”). Denna möjlighet är dock inte obegränsad för konventionsstaterna och Europadomstolen förbehåller sig rätten att övervaka att den inte missbrukas.[199]

8.1.1 Rätt till respekt för korrespondens

Den del av rättighetsskyddet i artikel 8 som är av störst betydelse för implementeringen av datalagringsdirektivet samt rättsläget med två parallella regelverk för uppgiftsutlämnande är skyddet för korrespondens. Med korrespondens aves enligt Europakonventionen olika former för överföring av meddelande mellan individer. Det är dock inte endast befordran av skrivet material som brev eller andra postförsändelser som omfattas av skyddet, utan även telefoniska och telegrafiska kommunikationer liksom överförande av meddelanden med hjälp av radio och datorer.[200] Detta innebär att flertalet av de uppgifter som ska komma att lagras enligt artikel 5 i datalagringsdirektivet omfattas av skyddet för korrespondens. Sådana tvångsmedel som teleavlyssning/teleövervakning och brevkontroll utgör alltså ingrepp i den skyddade rättigheten samtidigt som de också berör den allmänna rätten till respekt för privatlivet.

8.1.2 Relevanta domar från Europadomstolen

De svenska lagar som är aktuella vid implementeringen av datalagringsdirektivet begränsas till trafikuppgifter och berör alltså inte innehållet i korrespondensen. Europadomstolen har i flertalet fall bedömt

[197] Danelius, s. 263f. van Dijk, Pieter m.fl., *Theory and practice of the European Convention on Human Rights*, s. 747.
[198] Danelius, s. 264, van Dijk, s. 750.
[199] Danelius, s. 264, van Dijk, s. 703, Stubbings m.fl. mot Förenade Konungariket, dom den 22/10 1996, p. 50, Hatton m.fl. mot Förenade Konungariket, dom den 2/10 2001, p. 130.
[200] Danelius, s. 270, Ovey, Clare; White, Robin, *European Convention on Human Rights*, s. 225.

reglering av tvångsmedel på teleområdet men det har företrädesvis rört sig om olika slag av teleavlyssning. Domstolens bedömningar är dock giltiga även på teleövervakning och andra jämförbara ingrepp då det inte är inskränkningen som sådan som bedöms utan huruvida den sker i överensstämmelse med villkoren i konventionens artikel 8:2.

Rättsfallet *Amann mot Schweiz* gällde teleavlyssning. Den klagande, Amann, hade blivit uppringd av den sovjetiska ambassaden vars telefon var avlyssnad av Schweiziska myndigheter p.g.a. nationella säkerhetsintressen. Efter samtalet sparades uppgifter om kontakten av den schweiziska säkerhetspolisen i ett register. Europadomstolen hänvisade till tidigare praxis och framhöll kravet på lagligt stöd och vad detta innebär i form av kvalitet, tillgänglighet och precision. I anslutning härtill konstaterade domstolen att ingreppet inte kunde anses ha skett med stöd av lag då de bestämmelser som låg till grund för avlyssningen var alltför allmänt utformade. På liknande grunder ansågs även lagringen av uppgifterna i registret utgöra ett otillåtet intrång i Amanns privatliv, trots att informationen inte innehöll några känsliga uppgifter. Kravet på överensstämmelse med lag var därmed inte uppfyllt.[201]

I målet *Valenzuela Contreras mot Spanien* prövades en bestämmelse i den spanska konstitutionen som utgjorde laglig grund för teleavlyssning. Enligt denna bestämmelse kunde domstol besluta om åtgärden men det angavs inget om vilka villkor som behövde vara uppfyllda för ett sådant beslut. Lagstödet var därför enligt Europadomstolen alltför allmänt utformat och laglighetskravet ansågs inte uppfyllt. I anslutning härtill uttalade Europadomstolen:

> "The requirement that the effects of the "law" be foreseeable means, in the sphere of monitoring telephone communications, that the guarantees stating the extent of the authorities' discretion and the manner in which it is to be exercised must be set out in detail in domestic law so that it has a binding force which circumscribes the judges' discretion in the application of such measures"[202]

I fallet *Klass m.fl. mot Tyskland* behandlades vissa frågor kring teleavlyssning och särskilt behovet av kontroll av en sådan åtgärd som vidtas utan att den närmast berörde informeras härom i förväg. Europadomstolen konstaterade bl.a. att avlyssning får användas enligt artikel 8:2 om det är nödvändigt för att skydda de demokratiska institutionerna. Domstolen påpekade dock att detta inte innebär att konventionsstaterna därmed har obegränsade befogenheter att övervaka enskilda, särskilt då en alltför utbredd lagstiftning på det här området kan underminera själva grunden för det demokratiska samhället. Vidare uttalades att det måste finnas effektiva kontrollmekanismer i syfte att förhindra missbruk av systemet. Sammantaget ansåg domstolen att den

[201] Amann mot Schweiz, dom den 16/2 2000.
[202] Valenzuela Contreras mot Spanien, dom den 30/7 1998, p. 60.

tyska lagstiftningen för sådan teleavlyssning innefattade tillräckliga rättssäkerhetsgarantier.[203]

I rättsfallet *Malone mot Förenade Konungariket* hade den klagande blivit utsatt för både telefonavlyssning och brevkontroll samt s.k. samtalsmätning som innebär att utrustning används för att automatiskt registrera antalet samtal som rings upp samt tidpunkt och samtalslängd. Europadomstolen konstaterade att den engelska lagregleringen för teleavlyssningen var dunkel och lämnande utrymme för flera olika tolkningar. Det var bl.a. oklart hur stor del av teleavlyssningen som kunde anses reglerad i lag och hur stor del som lämnades åt polisens självständiga beslut. I och med detta ansågs inte lagen uppfylla kravet på precision och därmed hade inte ingreppet skett i enlighet med lag. Den registrering av telefonnummer som hade skett ansågs inte heller ha uppfyllt kravet på laglighet då bestämmelserna som reglerade dess tillämpning varit alltför otydliga.[204]

Europadomstolens ställningstagande i *Malone mot Förenade Konungariket* utvecklades ytterligare i två rättsfall, *Huvig* och *Kruslin*, båda två *mot Frankrike*. I båda dessa fall klargjordes att teleavlyssning innebar ett allvarligt ingrepp i rättigheten till respekt för korrespondensen och privatlivet och därför måste ett tydligt lagstöd krävas. Det var därför viktigt att de regler som skulle tillämpas var klara och tydliga.[205]
I fallet *Kruslin* uttalade Europadomstolen:

> "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."[206]

Domstolen fann att den franska straffprocesslagen inte uppfyllde detta tydlighetskrav och att reglerna framför allt inte innebar tillräckliga garantier mot missbruk. Domstolen uttalade vidare att den personkrets som kunde bli föremål för teleavlyssning och de brott som åtgärden kunde beslutas för inte hade definierats och att det dessutom saknats krav på att beslut om telefonavlyssning begränsades i tiden. På grund härav hade Kruslin inte åtnjutit den minimumnivå av rättssäkerhet som medborgare i ett demokratiskt samhälle har rätt att kräva.

Fallet *Kruslin* har berörts i ett beslut av JO den 18 november 1996 som bl.a. avsåg ett initiativärende rörande en framställning om editionsföreläggande. JO konstaterade att de då gällande reglerna i telelagen angående utlämnade av uppgifter i brottsbekämpande syfte uppvisade likheter med regleringen i den franska straffprocesslagen som kritiserades i *Kruslin*. Telelagens regler innehöll inte något krav på att uppgifter som begärs ut endast ska vara hänförliga till misstänkta personer och någon begränsning till tiden av den

[203] Klass m.fl. mot Tyskland, dom den 6/9 1978.
[204] Malone mot Förenade Konungariket, dom den 2/8 1984.
[205] Kruslin mot Frankrike, dom den 24/4 1990, Huvig mot Frankrike, dom den 24/4 1990.
[206] Kruslin mot Frankrike, p. 33.

information som får inhämtas uppställs inte heller. Detta föranledde JO att ställa sig frågande till om reglerna i telelagen uppfyllde de krav på klarhet och förutsägbarhet som Europakonventionen ställer på regler om intrång i skyddet för privatliv och korrespondens.[207]

Kopp mot Schweiz handlade om teleavlyssning av en schweizisk advokats telefon. I avlyssningsbeslutet föreskrevs det att advokatsamtal inte skulle kontrolleras. Det framgick dock inte på vilket sätt man skulle skilja mellan de samtal som rörde advokatverksamheten och andra samtal. Vid verkställandet av avlyssningen ankom det på en tjänsteman vid postförvaltningen att avgöra vilka samtal som inte skulle kontrolleras och vilka som skulle undantas. Europadomstolen ansåg det minst sagt förvånande att denna kontroll utfördes av en av de parter som hade att verkställa avlyssningen och att detta skedde utan en domstolskontroll. Systemet sågs därmed inte som tillräckligt rättssäkert och uppfyllde inte laglighetskravet i artikel 8.[208]

8.2 Artikel 13 – Rätten till ett effektivt rättsmedel

Trots Europadomstolens uppgift att tillförsäkra efterlevnaden av konventionen är den generella utgångspunkten att ett missförhållande i första hand ska rättas på det nationella planet. Detta uppfylls dels genom kravet på att de inhemska rättsmedlen ska ha uttömts för att Europadomstolen ska kunna ta upp ett klagomål till prövning och dels genom den materiella bestämmelsen i artikel 13 i konventionen som stadgar att den vars konventionsrättigheter kränkts ska ha tillgång till ett effektivt rättsmedel inför en inhemsk myndighet.

I artikeln uttrycks det som att:

Var och en, vars i konventionen angivna fri- och rättigheter kränkts, skall ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta även om kränkningen förövats av någon under utövning av offentlig myndighet.

Stadgandets utformning till trots så krävs det inte att en annan rättighet enligt konventionen de facto har överträtts för att artikel 13 ska kunna anses överträdd. Detta konstateras genom Europadomstolens domar i *Klass m.fl. mot Tyskland* och *Silver m.fl. mot Förenade Konungariket*[209] där det uttalats att det räcker med att någon på *rimliga grunder* påstår sig vara offer för ett brott mot konventionen. Innebörden är då att personen ska ha möjlighet att få sitt påstående prövat och därtill erhålla rättelse eller gottgörelse för konstaterade kränkningar. Om denna möjlighet saknas innebär det att ett

[207] JO 1997/98, s. 47ff.
[208] Kopp mot Schweiz, dom den 25/3 1998.
[209] Silver m.fl. mot Förenade Konungariket, dom den 25/3 1983.

brott mot artikel 13 föreligger även om någon annan bestämmelse i konventionen i realiteten inte har överträtts.[210]

Det uppställs inte något absolut krav på att rättsmedlet ska innebära en prövning inför domstol, utan även administrativa rättsmedel kan vara tillräckliga för att uppfylla konventionens krav. För att rättsmedlet ska kunna godtas som effektivt i konventionens mening måste dock vissa krav vara uppfyllda. Avgörande för denna bedömning är det prövande organets befogenheter och de garantier som gäller vid förfarandet inför organet. Dessutom måste rättmedlet erbjuda verkliga möjligheter till prövning samt vara ägnat att leda till rättelse.[211] Det krävs inte att ett enda rättsmedel ensamt uppfyller kravet på ett effektivt rättsmedel utan flera rättsmedel som den nationella lagstiftningen tillhandahåller kan sammantaget uppfylla kravet.[212]

8.2.1 Relevanta rättsfall från Europadomstolen

I fallet *Klass m.fl. mot Tyskland*, som nämnts ovan, framställdes även klagomål om brott mot artikel 13. Domstolen påpekade att det vid teleavlyssning som till sin natur är hemlig är svårt, eller till och med omöjligt, för den enskilde att utnyttja vanliga rättsmedel. I dessa sammanhang måste ett effektivt rättsmedel förstås som ett rättsmedel som är så effektivt som möjligt med hänsyn till de särskilda omständigheterna. Detta innebar att det förhållandet att någon underrättelse om avlyssningen inte lämnats till den klagande inte i sig kunde anses utgöra ett brott mot artikel 13. Domstolen betonade vidare att det i den tyska rätten fanns vissa rättsmedel tillgängliga för den som blivit utsatt för ett hemligt tvångsmedel, som att klaga till en särskild kommission eller till författningsdomstolen. Dessutom innehöll tysk rätt bestämmelser om att underrättelse om tvångsmedelsanvändningen skulle lämnas i efterhand om detta kunde ske utan risk för utredningen eller liknande. Efter att underrättelsen lämnats blev fler rättsmedel tillgängliga för den enskilde. Innebörden blev, enligt domstolen, att kravet på effektivt rättsmedel fick anses uppfyllt.

I fallet *Leander mot Sverige* hade Leander gått miste om en viss arbetsanställning då säkerhetspolisen lämnat vissa hemliga uppgifter om honom vid en s.k. personalkontroll. Klagan gällde bl.a. att Leander själv inte fått tillgång till dessa uppgifter och heller inte haft möjligheten att få sin sak prövad av en självständig myndighet och att det därmed förelåg ett brott mot konventionens artikel 13. Europadomstolen fann, likt avgörandet i *Klass m.fl. mot Tyskland*, att underlåtenheten att kommunicera de aktuella uppgifterna till Leander inte i sig utgjorde ett brott mot artikel 13 samt att det rättsmedel som kan krävas vid omständigheter av sådan speciell natur som rådde måste vara av relativt begränsad effektivitet. Därmed fastslogs att de rättsmedel som fanns att tillgå genom JK, JO, parlamentarisk kontroll

[210] Danelius, s. 351f.
[211] Danelius, s. 352.
[212] van Dijk m.fl., s. 1006.

och möjligheten till klagomål hos regeringen tillsammans ansågs uppfylla kraven i artikel 13.[213]

Ett annat fall med direkt anknytning till Sverige var *Segerstedt-Wiberg m.fl. mot Sverige*. Målet gällde fem svenska medborgare som begärt att få ta del av all information som fanns lagrade om dem i Säkerhetspolisens register. Då de klagande inte fick ut fullständig information om registeranteckningarna anförde de bl.a. att det saknades tillgång till effektivt rättsmedel för att erhålla rättelse. Domstolen fann att kontroll över området utövades av JK, JO, Datainspektionen, och Registernämnden men att inte ens den samlade effekten av denna kontroll nådde upp till kravet på effektivt rättsmedel i konventionens mening. Domstolen påpekade bl.a. att det inte fanns något tillgängligt rättsmedel med befogenhet att besluta om att en uppgift skulle avlägsnas ur Säkerhetspolisens register. Samtliga klagandes rätt enligt artikel 13 i konventionen hade därmed kränkts.[214]

[213] Leander mot Sverige, dom den 26/3 1987.
[214] Segerstedt-Wiberg m.fl. mot Sverige, dom den 6/6 2006.

9 Analys

9.1 Inledning

Personlig integritet är ett svårdefinierat begrepp och trots att flertalet försök gjorts i skiljda sammanhang har man inte lyckats formulera en entydig och allmänt accepterad definition. Skyddet för privatlivet och den personliga integriteten utgör trots det en fundamental del i en rättsstat. Skyddet för dessa grundläggande värden och friheter framgår i svensk rätt dels av bestämmelsen i 2 kap. 6 § RF och dels genom artikel 8 EKMR. Innebörden är att var och en ska vara tillförsäkrad en privat och fredad zon fri från intrång från andra enskilda personer och från offentliga myndigheter. Trots detta kan en individ som lever i den gemenskap som samhället utgör knappast göra gällande något absolut anspråk på att få leva i fred för andra individer eller ostört från samhällets organ. Dels skulle ett sådant anspråk vara näst intill omöjligt att förverkliga i dagens samhälle och dels krävs det en viss acceptans av begränsningar av och intrång i den skyddade zonen för att samhället ska fungera. Bland annat behövs detta för att kunna garantera en fungerande och effektiv brottsbekämpning.

Trots sin betydelse är det alltså en nödvändighet att skyddet för privatlivet kan begränsas eller inskränkas för att inte andra skyddsvärda intressen i ett fungerande samhälle ska trädas för när. Av denna anledning har skyddet gjorts relativt och genom 2 kap. 12 § RF respektive artikel 8:2 EKMR finns möjligheten till sådana inskränkningar, bl.a. under förutsättningen att dessa kan anses godtagbara och nödvändiga i ett demokratiskt samhälle. En sådan avvägning blir av yttersta vikt i frågan om straffprocessuella tvångsmedel eller därmed jämförliga åtgärder, dels vid införandet av nya sådana men även vid tillämpningen av redan existerande. Implementeringen av datalagringsdirektivet i Sverige innebär inte att det införs någon ny sådan övervakningsåtgärd i svensk rätt. Däremot ökar de redan existerande i betydelse då deras användningsområde utökas och förutsättningarna för att uppnå resultat med hjälp av dem förbättras. En olycklig följd av detta är att det integritetsintrång som dessa åtgärder onekligen innebär riskerar att öka i samma takt varvid en utförlig avvägning mellan dessa motstående intressen är nödvändig.

Vad gäller införandet av datalagringsdirektivet så innebär det en förändring i synen på lagring av trafikuppgifter som fram tills nu varit ett mot operatörerna riktat lagringsförbud. Den nu rådande huvudregeln, som även den hade sitt ursprung i ett EG-direktiv, infördes 2003 och innebär att trafikuppgifter som inte längre behövs för att överförföra ett elektroniskt meddelande ska utplånas eller avidentifieras. Regeln tillkom för att upprätthålla skyddet för personuppgifter och integritet för användare av elektroniska kommunikationstjänster. Genom datalagringsdirektivet införs nu istället en skyldighet för operatörerna att lagra sådana uppgifter under en viss tid och för ett visst syfte, dock med samma krav på avidentifiering eller

utplåning efter denna tids utgång. På en relativt kort tid ersätts alltså vad som vid införandet uppfattades som ett principiellt grundat ställningstagande av ett med i stort sett rakt motsatt innebörd. Det förra perspektivet är i grunden präglat av en strävan mot ett fullgott skydd för enskildas personliga integritet trots samhällets alltmer avancerade och digitala kommunikationsteknik. Det nu aktuella perspektivet är huvudsakligen inriktat på vad denna tekniska utveckling för med sig i fråga om förändrade beteendemönster i samhället och därmed knutna behov av att inskränka den personliga integriteten till förmån för samhällets brottsbekämpande verksamhet. Perspektivförskjutningen innebär en extraordinär åtgärd utan historisk motsvarighet då den innebär en mycket omfattande registrering av uppgifter härrörande från telefon- och datakommunikation. Lagringen berör i praktiken hela befolkningen och därmed, i det absolut övervägande antalet fall, personer som inte är misstänkta för något brott. Detta förhållande borgar för att det vid genomförandet på det nationella planet är av yttersta vikt att integritetsskyddsaspekten tas i största möjliga beaktande, bl.a. genom att bestämmelserna utformas så tydligt som möjligt och att reglerna angående utlämnande av de lagrade uppgifterna är klara och omgärdas av tillräckliga rättssäkerhetsgarantier.

9.2 Skillnaden mellan regelverken för utlämnande av trafikuppgifter

Som visats i föregående kapitel uppvisar reglerna i LEK för utlämnande av trafikuppgifter och reglerna om hemlig teleövervakning i rättegångsbalken stora likheter vad gäller användningsområde. Uppgifterna som lämnas ut är av samma typ oavsett vilken lag beslutet stödjer sig på. Alla de uppgifter som får lämnas ut enligt gällande rätt omfattas av de båda regelverken och detsamma kommer gälla för de ytterligare uppgifter som kommer att lagras i och med införandet av datalagringsdirektivet. Tidigare fanns det en skillnad i fråga om till vilken tid uppgifterna var hänförliga; framtida eller historiska uppgifter. Ett beslut om hemlig teleövervakning gällde då endast sådana uppgifter som genererades efter det att beslutet om tvångsmedlet hade beviljats, d.v.s. omfattades inte uppgifter hänförliga till förfluten tid. Efter lagändringen som genomfördes 2004 undanröjdes denna skillnad då reglerna om teleövervakning utökades till att även omfatta historiska uppgifter.

Bortsett från dessa likheter är det stor skillnad mellan regelverken vilket främst gäller i fråga om vilka rättssäkerhetsgarantier som omgärdar ett utlämnande. För att hemlig teleövervakning över huvud taget ska övervägas krävs i normalfallet att det pågår en förundersökning. De krav som ställs därutöver har till syfte att dels förhindra att tvångsmedlet används i ett allt för tidigt skede i utredningen och därmed på grunder som inte är tillräckligt stabila och dels att minska den personkrets som på ett eller annat vis kan få sin integritet kränkt av åtgärden. Av naturliga skäl är dessa krav högt ställda

då det är angeläget att begränsa användningen av så integritetskränkande åtgärder som hemliga tvångsmedel så långt som möjligt. Dessa tvångsmedel är bland de mest integritetskränkande åtgärder en stat kan företa mot enskilda och de saknar dessutom genom sin hemliga natur den möjlighet till insyn och öppen prövning som sådana kränkningar principiellt ska omgärdas med. Det är därför anmärkningsvärt att reglerna i LEK saknar alla dessa krav. En förundersökning behöver inte föreligga utan det är tillräckligt att en begäran om utlämnande enligt LEK kan knytas till en misstanke om ett allvarligt brott för att uppgifterna ska lämnas ut. Det ställs inga krav på hur stark denna koppling ska vara eller av vilken anledning den anses existera. Reglerna som för teleövervakning existerar bl.a. för att minimera risken av att ovidkommande personer drabbas kan därför med lätthet kommas runt genom att välja att begära ut uppgifterna enligt LEK istället, om straffskalan för brottsmisstanken medger det.

Den mest betydande skillnaden regelverken emellan måste anses ligga i att hemlig teleövervakning är föremål för en oberoende rättslig kontroll. Denna består främst av den förhandskontroll som görs i och med tillståndsprövningen i domstol. Domstolsprövningen syftar till att tillförsäkra det skydd som av naturliga skäl saknas då personen som blir utsatt för tvångsmedelsanvändningen inte själv är medveten om intrånget. Förutom att pröva ifall förutsättningar föreligger för övervakningstillstånd i det enskilda fallet kan domstolen dessutom vidta vissa åtgärder för att ytterligare begränsa integritetsintrånget. Detta sker dels genom att tidsbegränsa tillståndet och dels genom att förena tillståndet med villkor. Ett beslut om samma uppgifter som för teleövervakning ställer stora krav på juridisk kompetens och vanligtvis är förbehållet lagfarna domare i chefspositioner inom domstolen kan, då ett utlämnande beslutas genom LEK:s regler, i praktiken tas av vilken polisman eller tulltjänsteman som helst.

I sammanhanget förtjänar även proportionalitetsprincipens uttryck i de båda regelverken att nämnas. I rättegångsbalken ansågs det finnas ett behov av att lagfästa principen i inledningen av de kapitel i rättegångsbalken som behandlar tvångsmedelsanvändningen. Principen gäller samtidigt för ingripande av både polis och tulltjänstemän genom de regelverk som styr respektive myndighets ingripande. Innebörden måste bli att oavsett vilken lag som ett utlämnande av trafikuppgifter stödjer sig på kommer beslutet att begära ut trafikuppgifter om en enskild person med nödvändighet att prövas gentemot proportionalitetsprincipen. En betydande skillnad i det här avseendet är dock att denna bedömning vad gäller hemlig teleövervakning görs av två skiljda instanser vid två olika tillfällen. Bedömningen sker dels genom domstolsprövningen som föregår beslutet om åtgärden och dels vid tvångsmedlets användning, varvid polislagen eller tullagen får en självständig betydelse. Trots att utlämnande av trafikuppgifter inte är en lika integritetskänslig åtgärd som exempelvis hemlig teleavlyssning, i och med att innehållet i kommunikationen inte blir tillgängligt, så är tillämpningen av proportionalitetsprincipen av stor vikt. En tillgång till trafikuppgifter om en viss person, inhämtade över en viss tid, kan medge en näst intill fullständig

bild av denna persons kommunikationsmönster. Med hjälp av lokaliseringsuppgifter kan även personens rörelsemönster fastställas under övervakningstiden. Det kan därför med rätta hävdas att intrånget i den övervakades privatliv blir väl så betydande även vid övervakning av denna sort vilket gör att en strikt tillämpning av proportionalitetsprincipen är påkallad. Det är rimligt att anta att detta krav uppfylls till en högre grad genom den dubbla tillämpning av principen som med nödvändighet följer av att ett utlämnande av uppgifter stödjer sig på reglerna i rättegångsbalken.

Vidare saknar en person vars uppgifter lämnats ut genom reglerna i LEK den efterhandskontroll som för hemlig teleövervakning medges genom dels underrättelseskyldigheten och dels tillsynen av säkerhets- och integritetsskyddsnämnden. Efter ett utlämnande enligt LEK är det därmed, förutom i de fall där reglerna om partsinsyn inträder, högst osannolikt att den övervakade över huvud taget blir medveten om intrånget som gjorts och än mindre bereds möjligheten att få till stånd en laglighetsprövning av detta. Även om fallet skulle vara att den övervakade får vetskap om att uppgifterna har lämnats ut så inryms inte användningen av reglerna i LEK under säkerhets- och integritetsskyddsnämndens tillsynsområde då förfarandet formellt sett inte är ett tvångsmedel. Följden blir att den enskilde, vars integritet har kränkts, i flertalet fall inte kommer att ha tillgång till tillräckligt mycket information för att själv avgöra ifall intrånget haft laglig grund och därmed i praktiken sakna möjligheten att utnyttja vetskapen för att söka upprättelse. Teoretiskt sett finns möjligheten att med hjälp av sådana extraordinära tillsynsorgan som JO eller JK få till stånd prövning av myndighetsutövningen. I de allra flesta fall saknar dock den övervakade personen kännedom om ingreppet vilket gör att denna möjlighet i det närmaste blir illusorisk.

Rättsläget vad gäller myndigheters tillgång till trafikuppgifter uppvisar alltså i dagsläget en betydande brist. Trots att två parallella regelverk i all väsentlighet erbjuder samma möjligheter för de brottsbekämpande myndigheterna är det bara det ena av dessa som upprätthåller ett godtagbart skydd för att minimera de integritetskränkningar som åtgärden ofrånkomligt leder till. Förhållandet kritiserades redan för 16 år sedan vid telelagens införande och har påtalats vid flertalet utredningar sedan dess. Hittills har dock den enda åtgärd som föranletts av kritiken varit en förskjutning av frågan till kommande utredningar. Detta trots att användningsområdet för reglerna i rättegångsbalken respektive LEK fördes än närmare varandra då reglerna om teleövervakning utökades 2004 till att även omfatta historiska uppgifter.

Att tillgång till trafikuppgifter är av stor betydelse för bekämpning av framför allt allvarlig brottslighet är odiskutabelt. Detta framgår inte minst av den statistik och de uppskattningar som presenterades i kapitel 7. Det är även tydligt att utlämnande till största delen sker med stöd av reglerna i LEK. Därtill kommer att antalet utlämnanden stadigt ökar och ingenting tyder på att denna trend kommer att brytas. Det är tvärtemot ett högst rimligt antagande att utlämnandefrekvensen kommer öka markant i och med

införandet av datalagringsdirektivet. Anledningen är bl.a. att en större mängd uppgifter kommer lagras efter direktivets införande än vad som är fallet idag. Dessutom kommer operatörerna att beläggas med en lagringsskyldighet som eliminerar den slumpfaktor som för nuvarande begränsar myndigheternas tillgång till trafikuppgifterna. Detta kommer ofrånkomligen leda till att betydelsen av skillnaderna i rättssäkerhet mellan de båda regelverken kommer öka ytterligare i betydelse efter införandet av direktivet.

Mot bakgrund av de skillnader som redovisats ovan är det av intresse att se närmare på hur det svenska implementeringsförslaget står i förhållande till Europakonventionens krav på inskränkningar i rätten till respekt för privatliv och korrespondens (artikel 8) och tillång till effektivt rättsmedel (artikel 13).

9.3 Europakonventionen

I datalagringsdirektivet framgår att vid en avvägning mellan lagringsskyldighetens syfte som brottsbekämpande instrument och skyddet för den personliga integriteten framstår införandet som en nödvändig åtgärd i överensstämmelse med Europakonventionens bestämmelser. Inte desto mindre måste dock varje medlemsstat vid införandet av direktivet i nationell lagstiftning göra en självständig bedömning av om de specifika lagstiftningsåtgärder som vidtas kan anses respektera de grundläggande rättigheter som garanteras genom konventionen. Trafikuppgiftsutredningen hade därmed att analysera ifall införandet av lagringsskyldigheten förde med sig ett behov av att förändra de förutsättningar som gäller för de brottsbekämpande myndigheternas tillgång till trafikuppgifter för att nå upp till kraven som ställs i Europakonventionen. Frågan, som är av väsentligt värde ur integritetssynpunkt, är inte närmare reglerad i direktivet och utredningen fäster i denna del stor vikt vid uttalandet som gjordes av ministerrådet. Uttalandet avser endast huruvida brotten som enligt den nationella lagstiftningen kan föranleda ett utlämnande av trafikuppgifter är tillräckligt allvarliga. Medlemsstaterna ska vid denna bedömning ta vederbörlig hänsyn till de brott som finns listade i artikel 3 i den europeiska arresteringsordern. Då reglerna i både rättegångsbalken och LEK har krav på ett relativt högt straffminimum för utlämnande, sex månaders respektive två års fängelse, bedömde utredningen att det inte föreligger något behov av att förändra någon av bestämmelserna för utlämnande i något avseende.

Då utredningen inte heller i övrigt ansåg att någon förändring var påkallad är det av intresse att analysera huruvida det rådande rättsläget i Sverige verkligen uppfyller de krav som Europakonventionen ställer. Tyngdpunkten kommer att ligga på reglerna för utlämnande enligt LEK samt i vilken mån dessa kan riskera att anses som konventionsstridiga medan reglerna om hemlig teleövervakning i rättegångsbalken främst kommer att beröras i jämförande syfte.

9.3.1 Förenlighet med artikel 8

I artikel 8 EKMR är det framförallt skyddet för förtrolig korrespondens som aktualiseras vid bedömningen av utlämnande av trafikuppgifter och i stort sett alla uppgifter som lagringsskyldigheten berör omfattas av skyddet. För att ett ingrepp i denna rättighet ska anses försvarbart uppställer konventionen en rad krav. Dessa är att ingreppet måste ske med *stöd av lag*, vara ägnat att *tillgodose ett skyddsvärt intresse* samt vara *nödvändigt i ett demokratiskt samhälle*. Då regleringen för utlämnande enligt LEK utan tvekan är stadgade i lag blir frågan istället om lagstödet kan anses uppfylla de närmare specifikationer som krävs enligt Europadomstolens praxis.

Europadomstolen har i flertalet fall slagit fast att det inte räcker att det finns ett författningsmässigt stöd, utan att detta snarare är att se som en grundläggande förutsättning som därutöver måste uppvisa visa kvalitetskrav. Innebörden av detta är att lagen måste uppfylla rimliga anspråk på rättssäkerhet, att lagen är tillgänglig och förutsebar, skyddar mot godtycke och är utformad med erforderlig precision. Reglerna i LEK må vara tillgängliga men då det enda krav som uppställs för att myndigheter ska kunna begära utlämnande av uppgifter är att dessa på något vis är hänförliga till ett brott med ett visst straffminimum är det ytterst tveksamt om regleringen uppfyller de övriga krav konventionen ställer. Frågan är om denna enda begränsning i LEK kan anses uppfylla de krav på tydlighet som var av avgörande betydelse i fallet *Amann mot Schweiz* där rättsystemet kritiserades för alltför allmänt utformade bestämmelser. Vid en jämförelse med reglerna om hemlig teleövervakning där det finns utförliga begränsningar, bl.a. i fråga om när uppgifterna får inhämtas och vems uppgifter det får gälla, framstår LEK:s regler som ytterst allmänt utformade. Exempelvis krävs det inte att uppgifterna är hänförliga till någon person som faktiskt kan ha gjort sig skyldig till ett brott utan de kan lika gärna gälla ett vittne eller tredjeman och uppgifterna kan dessutom inhämtas vid vilken tidpunkt som helst, så länge det gäller misstanke om ett allvarligt brott.

I nära anslutning till ovan sagda är det av vikt att påpeka vad Europadomstolen ansett om kravet på förutsebarhet. I det ovan citerade uttalandet i fallet *Valenzuela Contreras mot Spanien* beskriver domstolen detta förutsebarhetskrav med att bestämmelserna måste var utformade så att de tydligt begränsar befogenheterna hos den som har att besluta om den inträngande åtgärden. På detta vis kan medborgarna förutse i vilka fall de kan tänkas drabbas av en kränkning av sina rättigheter. Att genomförandet av datalagringsdirektivet medför att uppgifter kommer att finnas lagrade om alla elektroniska kommunikationer i Sverige är det inga problem att förutse. Däremot är möjligheten att förutse när dessa uppgifter kan komma att lämnas ut med stöd av reglerna i LEK näst intill obefintlig. Detta blir än mer sant med de beskrivna möjligheterna till s.k. basstationstömning då uppgifter om i stort sett alla elektroniska kommunikationer inom ett visst område, t.ex. i anknytning till en brottsplats, begärs ut av myndigheterna. Innebörden av detta är att uppgifter om ett oöverskådligt antal personer kan inhämtas enbart grundat på att dessa befunnit sig inom ett visst avstånd från

en basstation. Det här förhållandet kan inte anses uppfylla förutsebarhetskravet som konventionen uppställer.

För ytterligare ledningen i fråga om reglerna uppfyller laglighetskravet är fallet *Kruslin mot Frankrike* av intresse. Europadomstolen uttalade här att regleringen som var aktuell i fallet inte uppfyllde kraven på tydlighet och skydd mot missbruk. Avgörande var dock att de inte begränsade den personkrets som kunde bli föremål för den teleavlyssning som fallet gällde och dessutom saknades krav på tidsbegränsade beslut. Jag har svårt att se hur dessa krav skulle anses uppfyllda av reglerna i LEK då nämnda begränsningar uppenbarligen saknas även där. Jag delar därmed den tveksamhet JO uttryckte då han på denna punkt kritiserade den tidigare telelagen av just nämnda anledning.

Genom regleringen i LEK lämnas det helt och hållet upp till den verkställande myndigheten att avgöra vilka uppgifter som ska inhämtas och i vilket syfte inhämtningen ska göras. Tydliga paralleller kan i detta avseende dras till fallet *Kopp mot Schweiz* där det ankom på verkställande part att avgöra vilka uppgifter som skulle inhämtas utan att detta underkastades domstolskontroll. I det fallet ansågs inte förfarandet vara tillräckligt rättssäkert vilket föranleder ett berättigat tvivel angående om det svenska systemet skulle anses uppfylla kravet. Avsaknaden av en förhandskontroll av domstol vid utlämnande av trafikuppgifter bör i högsta grad påverka bedömningen av om reglerna i LEK kan anses uppfylla konventionens krav. Domstolsprövningen är en av de viktigaste och mest effektiva rättssäkerhetsgarantier som omgärdar ett tvångsmedelsbeslut och det faktum att krav på sådan saknas i LEK och beslutet istället tas av den verkställande myndigheten kan alltså inte anses överensstämma med kravet på rimligt rättssäkerhetsanspråk.

Kravet i artikel 8:2 om att inskränkningen ska tillgodose ett skyddsvärt intresse är allmänt formulerad och det uppstår därför sällan problem att hänföra ett ingrepp till någon accepterad kategori. Syftet med utlämnanderegleringen i LEK är dessutom brottsbekämpning vilket uttryckligen är uppräknat i artikeln. Intressant är istället att se närmare på kravet på nödvändighet i ett demokratiskt samhälle och den därtill knutna tillämpningen av proportionalitetsprincipen. Det uppställs inget krav på att ingreppet ska vara oundgängligt, snarare ska det svara mot ett angeläget samhälleligt behov. Det torde vara ostridigt att det föreligger ett angeläget behov för de brottsbekämpande myndigheterna att ha verktyg anpassade till rådande omständigheter och som svarar mot den brottslighet de har att bekämpa. Det förefaller däremot mer tveksamt om inte detta behov för svensk del redan är tillgodosett genom regleringen om hemlig teleövervakning. Tidigare har visats att regelverken omfattar samma användningsområde och de egentliga skillnaderna reglerna emellan är endast är hänförliga till de lägre kraven i LEK. För att ingreppet ska anses som rättfärdigat krävs vidare att inskränkningen måste stå i proportion till det syfte som ska tillgodoses. Då syftet, tillgången till trafikuppgifter i brottsbekämpningen, redan är tillgodosett genom den mer rättsäkra

regleringen i rättegångsbalken måste det anses tveksamt om den vidare inskränkning som LEK:s regler medger verkligen kan anses proportionerlig. Man bör i sammanhanget även beakta uttalandet i fallet *Klass mot Tyskland* angående Europadomstolens restriktivitet gentemot alltför utbredd lagstiftning på området för övervakning då sådan riskerar att underminera själva grunden för det demokratiska samhället.

9.3.2 Förenlighet med artikel 13

Artikel 13 i Europakonventionen innebär att det i varje medlemsstat ska finnas en möjlighet för den som anser sig ha blivit utsatt för en kränkning av någon artikel i konventionen att genom ett effektivt nationellt rättsmedel få sin klagan prövad. Bestämmelsens betydelse får anses vara central då den utgör en garanti för att konventionens bestämmelser verkligen efterlevs.

Vid hemliga tvångsmedel, och därmed jämförbara ingrepp, uppkommer det onekligen tvivelaktiga situationer om förenligheten med artikeln. Ofta saknar dessa ingrepp med nödvändighet flera av de kontrollmöjligheter som mer eller mindre automatiskt är sammankopplade med ingrepp som till sin natur är öppna. När någon till exempel blir föremål för ett straffprocessuellt frihetsberövande används tvångsmedlet helt öppet och personen i fråga blir vid verkställandet vanligtvis omedelbart medveten om åtgärden. Därmed har personen, om denne upplever ingreppet som felaktigt på någon grund, en möjlighet att överklaga beslutet hos domstol, överordnad myndighet, JK, eller JO eller i vissa fall till och med söka bilda opinion mot förfarandet genom massmedia. Europadomstolen har i bl.a. *Klass mot Tyskland* slagit fast att det i dessa fall får anses tillräckligt att ett rättsmedel är så effektivt som det kan vara, givet omständigheterna. Likt avgörandet i *Leander mot Sverige* uttalade domstolen även att det inte är ett absolut krav att den som utsatts för ett tvångsmedel blir underrättad härom utan kravet kan tillgodoses genom andra former av rättsmedel, enskilt eller i förening.

Ett utlämnande av uppgifter enligt LEK föranleder inte att det lämnas någon information till den vars uppgifter lämnats ut. Detta faktum ensamt kan som visats inte tillmätas tillräcklig betydelse för att ett brott mot artikel 13 ska anses föreligga. Frågan blir då vad det finns för övriga rättsmedel som en enskild kan vända sig till för att få en upplevd kränkning prövad. Som nämndes ovan finns det en möjlighet att få ett utlämnande prövat av JO eller JK men denna möjlighet förblir enbart teoretiskt i de allra flesta fall. Förutom i de fall där reglerna om partsinsyn inträder förblir den övervakade i fråga lyckligt ovetande om ingreppet som företagits. Ett rimligt antagande är att det i förhållande till antalet utlämnanden, som enligt uppgifter närmar sig 10 000 fall årligen, är förhållandevis sällan som reglerna om partsinsyn faktiskt blir giltiga. Innebörden blir att det formellt sett kan anses finnas rättsmedel att tillgå men då dessa inte erbjuder någon reell möjlighet till prövning kan detta inte anses tillgodose konventionens krav. Reglerna i LEK är inte heller formellt sett ett tvångsmedel i strikt mening och därmed faller de utanför den tillsyn som utförs av den nyinrättade säkerhets- och

integritetsskyddsnämnden. Inte heller utförs någon övergripande tillsyn av användningsområdet i stort då regelverket inte omfattas av den parlamentariska kontroll som de hemliga tvångsmedlen är underkastade. De samlade rättsmedel som fällde avgörandet i *Leander mot Sverige* kan alltså inte anses föreligga för reglerna i LEK. I sammanhanget ska även nämnas att det måste anses vara av betydelse för Europadomstolens beslut att de rättsmedel som fanns tillgängliga i nämnda fall inte enbart möjliggjorde en prövning utan att dessa därutöver innehade befogenheter att lämna bindande beslut angående klagan. Betydelsen av denna omständighet framgår även av avgörandet i *Segerstedt-Wiberg m.fl. mot Sverige* där förhållandet att sådana befogenheter saknades av de organ som utgjorde rättsmedel på området tillmättes stor betydelse. Överfört på reglerna i LEK bör detta innebära att även om den övervakade personen blir medveten om intrånget och därmed kan utnyttja de rättsmedel som står till buds, dvs. JO eller JK, är det tveksamt om kravet på effektivt rättsmedel uppfylls. Dessa instanser kan visserligen rikta kritik mot beslut och eventuellt väcka talan mot tjänstemän då ett tjänstefel kan ha begåtts men de har inte möjlighet att överpröva beslutet i sak och även möjligheten till skadestånd då fel har begåtts torde vara mycket begränsad. Sammantaget bör det anses som högst osäkert huruvida Europadomstolen vid en framtida prövning bedömer reglerna om utlämnande i LEK som förenliga med artikel 13 i konventionen.

För jämförelsens skull ska nämnas att regleringen av hemlig teleövervakning uppvisar ett flertal olika kontrollmöjligheter relevanta för bedömningen; förhandsprövning i domstol, underrättelse till enskild om tvångsmedelsanvändningen, parlamentarisk kontroll, tillsyn av säkerhets- och integritetsskyddsnämnden och därtill den extraordinära kontrollen genom JO och JK. Vid beaktande av Europadomstolens praxis bör den sammanlagda effekten av dessa rättsmedel anses uppfylla det krav på effektivitet som konventionen uppställer.

9.4 Avslutande synpunkter

Det får anses klarlagt att tillgången till trafikuppgifter är av avgörande betydelse för den brottsbekämpande verksamheten. Samhällets och teknikens utveckling leder till förändrade beteendemönster samt ökad användning av olika tekniska kommunikationsvägar. Att inte anpassa lagstiftningen till detta växande informationsfält vore orealistiskt och i all väsentlighet förödande för utredningen och bekämpningen av allvarlig brottslighet. EG-direktivet om lagring av trafikuppgifter och den därpå grundade nationella lagstiftningen utgör en sådan anpassning som i mångt och mycket svarar mot ett behov av effektivare verktyg i kampen mot den grova brottsligheten. Samtidigt sker denna anpassning inom ett oerhört integritetskänsligt område vilket föranleder att skyddet för enskildas personliga integritet med nödvändighet måste beaktas och utvecklas i motsvarande omfattning. På denna punkt menar jag att förslaget som Trafikuppgiftsutredningen presenterat innehåller väsentliga brister vars

åtgärdande bör ses som en förutsättning för att förslaget ska kunna läggas till grund för lagstiftning.

Den största bristen, vilken varit föremål för arbetets huvudsakliga fokus, är reglerna för utlämnande av de lagrade trafikuppgifterna och det där aktuella rättsläget. Bestämmelserna om utlämnande i LEK uppvisar allvarliga brister i fråga om skydd för den personliga integriteten samtidigt som deras funktion i praktiken gjorts överflödig av de motsvarande bestämmelserna i rättegångsbalken. Jag anser att behovet av en förändring i vart fall förelegat sedan reglerna om hemlig teleövervakning reformerades 2004 och genom den utökade lagring som nu står för dörren ökar betydelsen av en förändring markant.

Trafikuppgiftsutredningen har själv påpekat att det vore en fördel om BRU:s förslag om att överföra bestämmelserna från LEK till rättegångsbalken fick genomslag då detta skulle innebära att ett starkare rättssäkerhetsskydd uppnås. Denna förhoppning från utredningen är dock i mitt tycke inte tillräcklig. Genom att förskjuta ställningstagandet av om reglerna i LEK ska behållas eller inte till en annan utredning, trots en medvetenhet om de föreliggande bristerna och de konsekvenser som lagringsskyldigheten sannolikt för med sig, måste ses som att utredningen inte uppfyller den skyldighet som datalagringsdirektivet ålägger medlemsstaterna i fråga om att utföra nödvändiga lagstiftningsåtgärder vid direktivets införande.

Själva förslaget om datalagring kommer i sig att innebära att skyddet för den personliga integriteten i Sverige generellt kommer att försvagas. Införandet innebär, föga smickrande, en historisk milstolpe genom startpunkten för en massiv insamling av information som till den absolut övervägande delen kommer att drabba personer som inte är misstänkta för något brott. Sveriges skyldigheter som EU-medlemsstat innebär dock att direktivet måste införas, denna integritetsförlust till trots.

Vad gäller de parallella regelverken står dessa utanför det av direktivet reglerade området och därmed står det Sverige fritt att förändra möjligheten för de brottsbekämpande myndigheterna att få tillgång till den lagrade informationen. Denna möjlighet bör, vilket påpekats i flertalet utredningar och förarbeten, uteslutande regleras av tvångsmedelsbestämmelserna i rättegångsbalken. En sådan ordning skulle innebära ett väsentligt förbättrat skydd för enskildas personliga integritet, en mer förutsebar rättstillämpning, en brottsbekämpning mer präglad av rättssäkerhetsgarantier samt, med största säkerhet, ett rättssystem i bättre samklang med Sveriges åtagande som fördragsslutande part i Europakonventionen.

Bilaga A

Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation[215]

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation

dels att 6 kap. 3 och 5 §§ ska ha följande lydelse,
dels att rubriken närmast före 6 kap. 5 § ska ha följande lydelse,
dels att det i lagen ska införas fem nya paragrafer, 6 kap. 6 a - 6 d och 19 a §§, av följande lydelse.

Nuvarande lydelse	Föreslagen lydelse
6 kap. Integritetsskydd	
3 §	
Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst *skall* vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Den som tillhandahåller ett allmänt kommunikationsnät *skall* vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna *skall* vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsintrång.	Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst *ska* vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Den som tillhandahåller ett allmänt kommunikationsnät *ska* vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna *ska* vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsintrång. *Lagringsskyldiga enligt 6 a § ska dessutom vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter.*
Behandling av trafikuppgifter	**Behandling av trafikuppgifter *m.m.***
5 §	
Trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 §, *skall* utplånas eller avidentifieras när de inte längre behövs för att	Trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 §, *ska* utplånas eller avidentifieras när de inte längre behövs för att överföra

[215] SOU 2007:76, s. 36ff.

överföra ett elektroniskt meddelande, om de inte *får* sparas för sådan behandling som anges i 6 eller 13 §.

ett elektroniskt meddelande, om de inte sparas för sådan behandling som anges i 6, *6 a* eller 13 §.

6 a §
Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § och som genererar eller behandlar uppgifter som avses i 20 § första stycket 1 och 3 ska lagra uppgifterna för brottsbekämpande syften.
Lagrade uppgifter får behandlas endast
1. för att lämnas ut enligt 22 § första stycket 2 och 3 eller 27 kap. 19 § rättegångsbalken, eller
2. enligt 30 § första stycket personuppgiftslagen (1998:204).

6 b §
Lagring enligt 6 a § ska pågå under ett år från det datum kommunikationen ägde rum. Vid lagringstidens slut ska uppgifterna utplånas, om de inte har begärts utlämnade men ännu inte lämnats ut eller den lagringsskyldige annars har rätt att fortsätta behandla dem.

6 c §
Regeringen meddelar föreskrifter om lagringsskyldighet enligt 6 a §.
Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om säkerhet enligt 3 § andra stycket och får i enskilda fall medge undantag från lagringsskyldigheten enligt 6 a §.

6 d §
Lagringsskyldiga enligt 6 a § har rätt till ersättning när lagrade trafikuppgifter lämnas ut enligt 22 § första stycket 2 och 3 eller 27 kap. 19 § rättegångsbalken. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.
Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om ersättningen.

19 a §
Lagringsskyldiga enligt 6 a § ska bedriva verksamheten så att uppgifterna enkelt kan tas om hand och lämnas ut utan dröjsmål.

Förslag till förordning (0000:00) om lagring av trafikuppgifter m.m. för brottsbekämpande syften[216]

Inledande bestämmelse

1 § I denna förordning ges föreskrifter om lagring av trafikuppgifter m.m. enligt 6 kap. 3 § andra stycket, 6 a, 6 c och 6 d §§ lagen (2003:389) om elektronisk kommunikation.

Definitioner

2 § I denna förordning avses med
1. *Internettelefoni*: telefoni som använder IP-paket via Internet för överföring,
2. *Internetåtkomst*: möjlighet till överföring av IP-paket som ger användaren åtkomst till Internet,
3. *meddelandehantering*: överföring av elektroniskt meddelande som inte är samtal,
4. *misslyckad uppringning*: samtal som kopplats fram utan att få svar eller samtal som kopplats fram utan att nå mottagaren,
5. *mobil telefoni*: elektronisk kommunikationstjänst till mobil nätanslutningspunkt som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering,
6. *slutpunkt*: ändpunkt för varje lagringsskyldigs behandling av kommunikation,
7. *telefoni*: elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering.

Uppgifter som ska lagras

3 § Den som är lagringsskyldig enligt 6 kap. 6 a § lagen (2003:389) om elektronisk kommunikation ska lagra de uppgifter som anges i 4-9 §§.

4 § Vid telefoni ska uppgifter om följande lagras:
– uppringande telefonnummer,
– nummer som slagits och nummer till vilka samtalet styrts,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid då kommunikationen påbörjades och avslutades,
– den tjänst som använts, samt
– slutpunkter.

5 § Vid mobil telefoni ska utöver det som anges i 4 § uppgifter om följande lagras:
– uppringande parts abonnemangsidentitet och utrustningsidentitet,
– uppringd parts abonnemangsidentitet och utrustningsidentitet,
– lokaliseringsinformation för kommunikationens början och slut, samt
– datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst.

6 § Vid Internettelefoni ska utöver det som anges i 4 § uppgifter

[216] SOU 2007:76, s. 39ff.

om följande lagras:
– uppringande parts IP-adresser, samt
– uppringd parts IP-adresser.

7 § Vid meddelandehantering ska uppgifter om följande lagras:
– avsändarens och mottagarens meddelandeadress,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid för på- och avloggning i meddelandetjänsten,
– datum och spårbar tid för avsändande och mottagande av meddelande, samt
– den tjänst som har använts och spårbar tid för användandet.

8 § Vid Internetåtkomst ska uppgifter om följande lagras:
– användarens IP-adresser,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid för på- och avloggning i Internettjänsten,
– typen av Internetanslutning som använts, samt
– slutpunkter.

9 § Vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst ska uppgifter om följande lagras:
– uppgifter om abonnent,
– vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet, samt
– slutpunkter.

10 § Lagringsskyldigheten för uppgifter enligt 4-6 §§ gäller även vid misslyckad uppringning.

Föreskrifter och undantag

11 § Post- och telestyrelsen får efter samråd med Rikspolisstyrelsen och Datainspektionen meddela verkställighetsföreskrifter om säkerhet enligt 6 kap. 3 § andra stycket lagen (2003:389) om elektronisk kommunikation.

12 § Post- och telestyrelsen får efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen i enskilda fall medge undantag från lagringsskyldigheten enligt 6 kap. 6 a § första stycket lagen (2003:389) om elektronisk kommunikation.

13 § Post- och telestyrelsen får efter samråd med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och Tullverket meddela föreskrifter om den ersättning som lagringsskyldiga har rätt till enligt 6 kap. 6 d § lagen (2003:389) om elektronisk kommunikation.

Denna förordning träder i kraft den 1 januari 2009.

Käll- och litteraturförteckning

Offentligt tryck

Departementsserien och Statens offentliga utredningar

Ds Ju 1981:22	*Hemlig avlyssning m.m.*
Ds 2005:53	*Hemliga tvångsmedel m.m. under en stärkt parlamentarisk kontroll.*
SOU 1970:47	*Skydd mot avlyssning.*
SOU 1974:85	*Fotografering och integritet.*
SOU 1984:54	*Tvångsmedel - Anonymitet – Integritet.*
SOU 1987:74	*Optisk-elektronisk övervakning.*
SOU 1992:70	*Telelag.*
SOU 1995:47	*Tvångsmedel enligt 27 och 28 kap. RB samt polislagen.*
SOU 1998:46	*Om buggning och andra hemliga tvångsmedel.*
SOU 2002:60	*Lag om elektronisk kommunikation.*
SOU 2005:38	*Tillgång till elektronisk kommunikation i brottsutredningar m.m.*
SOU 2006:98	*Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.*
SOU 2007:22	*Skyddet för den personliga integriteten - kartläggning och analys, Del 1.*
SOU 2007:76	*Lagring av trafikuppgifter för brottsbekämpning.*
SOU 2008:3	*Skyddet för den personliga integriteten - Bedömningar och förslag.*

Propositioner

Prop. 1975/76:202	*Förslag till nya regler om telefonavlysning vid förundersökning m.m.*
Prop. 1975/76:209	*Ändring i regeringsformen.*
Prop. 1983/84:142	*Ändring i sekretesslagen (1908:100) m.m.*
Prop. 1988/89:124	*Vissa tvångsmedelsfrågor.*
Prop. 1992/93:200	*En telelag och en förändrad verksamhetsform för Televerket, m.m.*
Prop. 1994/95:227	*Hemlig teleavlyssning och hemlig teleövervakning.*
Prop. 1995/96:85	*Hemlig kameraövervakning.*
Prop. 2002/03:74	*Hemliga tvångsmedel - offentliga ombud och en mer ändamålsenlig reglering.*
Prop. 2002/03:110	*Lag om elektronisk kommunikation, m.m.*
Prop. 2005/06:177	*Åtgärder för att förhindra vissa särskilt allvarliga brott*

Prop. 2006/07:133	*Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.*

Direktiv och utskottsbetänkanden m.m.

Dir. 2004:51	*Skyddet för den personliga integriteten.*
Dir. 2006:49	*Genomförande av EG:s direktiv om lagring av trafikuppgifter.*
Bet. 1981/82:JuU54	*Om parlamentarisk kontroll ifråga om telefonavlyssning.*
Rskr. 1981/82:298	*Angående bifallandet av vad utskottet hemställt i bet. 1981/82:JuU54.*
Lagrådsremiss	*Hemlig avlyssning m.m.,* 2000-04-06
Skr. 2004/05:36	*Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2003*
Skr. 2005/06:53	*Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2004*
Skr. 2006/07:28	*Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2005*
Skr. 2007/08:34	*Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2006*

EU-dokument

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

Europaparlamentets och rådets direktiv 2006/24/EG 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.

Förslag till betänkande av den 18 april 2005, LIBE, Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor, 2004/0813 CSN.

Övriga tryckta källor

Justitiekanslerns ämbetsberättelse

JK 1991, s. 55

Justitieombudsmannens ämbetsberättelse

JO 1953, s. 325
JO 1986/87, s. 77
JO 1992/93, s. 204
JO 1993/94, s. 101
JO 1994/95, s. 134
JO 1997/98, s. 47

Rapporter

Post- och telestyrelsen, *Faktablad - Lagen om elektronisk kommunikation*, PTS-F-2003-4, tillgänglig på http://www.pts.se
Post- och telestyrelsen, *Sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter*, tillgänglig på http://www.pts.se
Post- och telestyrelsen rapport, *Svensk Telemarknad 2007*, Rapportnr: PTS-ER-2008:15, tillgänglig på http://www.pts.se

Remissvar i anledning av SOU 2007:76

Advokatsamfundet, dnr. R-2008/0035
Brottsförebyggande rådet, dnr. D 1.1-0632/2007
Datainspektionen, dnr..1673-2007
Justitiekanslern, dnr: 8771-07-80
Justitieombudsmannen, dnr: 5927-2008
Post- och telestyrelsen, dnr: 07-13540
Säkerhets- och integritetsskyddsnämnden, dnr: 4-2008

Internetkällor

http://www.eu-upplysningen.se/Amnesomraden/Straffratt-och-brottsbekampning/Terrorbekampning/, hämtad 2009-01-23

http://www.regeringen.se/sb/d/2373/a/16378, hämtad 2008-11-12

Litteratur

Bernitz, Ulf; Kjellgren, Anders, *Europarättens grunder*, upplaga 2, Nordstedts Juridik AB, Stockholm 2002.

Bylund, Torleif, *Tvångsmedel I. Personella tvångsmedel i straffprocessen*, Iustus Förlag AB, Göteborg 1993.

Collste, Göran, *Behandling av personuppgifter och personlig integritet: En etisk analys*, bilaga 4 i SOU 1997:39, *Integritet, Offentlighet, Informationsteknik.*

Danelius, Hans, *Mänskliga rättigheter i europeisk praxis. En kommentar till Europakonventionen om de mänskliga rättigheterna*, Upplaga 2:1, Norstedts Juridik AB, Stockholm 2002.

Ekelöf, Per Olof; Bylund, Torleif; Edelstam, Henrik, *Rättegång - Tredje häftet*, Upplaga 7, Norstedts Juridik AB, Stockholm 2006.

Ekelöf, Per Olof; Henrik Edelstam; Robert Boman. *Rättegång – femte häftet*, upplaga 7, Norstedts Juridik AB, Göteborg 2005.

Elwing, Carl M, *Tillräckliga skäl – Studier över förutsättningarna för allmänt åtal*, Carl Bloms Boktryckeri AB, Lund 1960

Freese, Jan; Gavatin, Charles; Rydén, Nils, *Privatlivets helgd. Tillåtet och otillåtet enligt datalagen, kreditupplysningslagen och inkassolagen.* Bohusläningens AB, Uddevalla 1975.

Helmius, Ingrid, *Polisens rättsliga befogenheter vid spaning*, Akademisk avhandling, Iustus Förlag AB, Uppsala 2000.

Holmberg, Erik; Stjernquist, Nils; Isberg, Magnus; Eliason, Marianne; Regner, Göran, *Grundlagarna*, upplaga 2, Stockholm: Nordstedts Juridik AB 2006.

Lindberg, Gunnel, *Straffprocessuella tvångsmedel – när och hur får de användas?,* Thomson Fakta AB, Norge 2005.

Ovey, Clare; White Robin, *Jacobs & White, European Convention on Human Rights*, upplaga 3, Oxford University Press, Guildford; King's Lynn 2002.

Petrén, Gustav; Ragnemalm, Hans, *Sveriges grundlagar och tillhörande författningar*, upplaga 12, Institutet för offentlig och internationell rätt, LiberFörlag Stockholm 1980.

Strömberg, Håkan; Bengt Lundell. *Sveriges Författning*, upplaga 19, Studentlitteratur, Lund 2004.

Strömholm, Stig, *Individens skyddade personlighetssfär. Om våra rättigheter*, antologi utgiven av Rättsfonden, Stockholm 1980.

van Dijk, Pieter; van Hoof, Fried; van Rijn, Arjen; Zwaak, Leo, *Theory and Practice of the European Convention on Human Rights*, upplaga 4, Intersentia Publishers, Antwerpen-Oxford 2006.

Westerlund, Gösta, *Straffprocessuella tvångsmedel. En studie av rättegångsbalkens 24 till 28 kapitel och annan lagstiftning,* AB OTTO KR BRUUN, Göteborg 2000.

Artiklar

Abrahamsson, Olle, *Integritetsskyddet i lagstiftningen,* SvJT 2006.

Ekelöf, Per Olof, *Ett problem med avseende på hemlig teleavlyssning,* SvJT 1982.

Lännergren, Bengt, *Om integritet,* SvJT 1979.

Strömholm, Stig, *Integritetsskyddet. Ett försök till internationell lägesbestämning,* SvJT 1971.

Rättsfallsförteckning

Europadomstolens domar

Amann mot Schweiz, Appl. No 27798/95, 16/2 2000.

Hatton m.fl. mot Förenade Konungariket Appl. No 36022/97 2/10 2001

Huvig mot Frankrike, Appl. No 11105/84, 24/4 1990.

Klass m.fl. mot Tyskland, Appl. No 5029/71, 6/9 1978

Kopp mot Schweiz, Appl. No 23224/94, 25/3 1998

Kruslin mot Frankrike, Appl. No 11801/85, 24/4 1990

Leander mot Sverige, Appl. No 9248/81, 26/3 1987

Malone mot Förenade Konungariket, Appl. No 8691/79, 2/8 1984.

Segerstedt-Wiberg m.fl. mot Sverige, Appl. No 62332/00, 6/6 2006

Silver m.fl. mot Förenade Konungariket, Appl. No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25/3 1983

Stubbings m.fl. mot Förenade Konungariket Appl. No 22083/93; 22095/93 22/10 1996

Valenzuela Contreras mot Spanien, Appl. No 27671/95, 30/7 1998