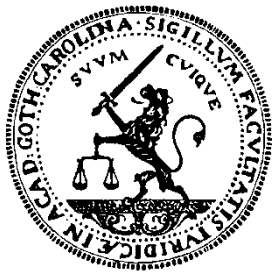


JURIDISKA FAKULTETEN
vid Lunds universitet

Karin Henriksson

Reformbehov i beslagslagstiftningen?

En studie om den tekniska utvecklingens och mobiltelefonins påverkan på beslagslagstiftningen

JURM02 Examensarbete

Examensarbete på juristprogrammet
30 högskolepoäng

Handledare: Helén Örnemark Hansen

Termin för examen: VT2014

Innehåll

Summary

The aim of this study is to examine the seizure legislation and the need to initiate legislative measures to adapt the legislation to technical progress, especially mobile telephones. An effective law enforcement perspective and an integrity perspective are used to determine whether or not the seizure legislation is adapted to technical progress. Finally, whether or not any legislative action needs to be done is discussed.

A mobile telephone can be seized according to chapter 27 paragraph 1 RB. Four issues regarding seizure of mobile telephones have been identified. How should mobile telephones be examined? How should data be seized? How should the law enforcement manage data which continually changes? Are the provisions in the seizure law regarding integrity protection applicable to mobile telephones containing stored data?

The examination of material in mobile telephones should be made as efficient as possible still maintaining integrity of individuals. The material in the telephone is copied and the seizure legislation is not applicable on copies. To maintain the integrity of individuals the seizure legislation should be remodelled in this regard.

Data is something intangible that cannot be seized. However, it should be possible to seize data if it is stored on an electronic device. The seizure legislation should explicitly clarify that the seizure of an electronic device also means that the stored data is seized.

Messages received after the mobile telephone has been seized should not be included in the seizure since it is considered to be ongoing communication. Instead legislation regarding interception should be applied to that sort of messages. The legislature should establish that seizure includes information available at the moment of the seizure and that messages received later is ongoing communication.

According to the wording, it is unclear whether chapter 27 paragraph 2 and 12 RB are applicable to mobile telephones containing data. The provisions' purpose is to protect correspondence and confidential information and therefore data should be included. This should explicitly be stated in the law.

In conclusion it can be stated that the seizure law is outdated. The seizure legislation needs to be remodelled to meet the requirements of seizure of mobile telephones. An altered legislation will increase the protection of the individuals' integrity while the law enforcement becomes more effective.

Sammanfattning

Studien syftar till att undersöka beslagslagstiftningen utifrån mobiltelefoni och analysera behovet av att införa lagstiftningsåtgärder för att anpassa lagstiftningen till teknisk utveckling. Undersökningen har gjorts utifrån ett brottsbekämpande perspektiv och ett integritetsperspektiv. Med en rättsdogmatisk metod fastställs gällande rätt och problem vid beslag av mobiltelefoner innehållande elektronisk information identifieras. För att få en heltäckande bild av problematiken har en intervju gjorts med kammaråklagare Jan Tibbling. En rättspolitisk argumentationsmetod har sedan använts för att undersöka och analysera om lagstiftningsåtgärder behöver vidtas.

Mobiltelefoner kan beslagtas enligt de villkor som uppställs i 27 kap. 1 § RB. Vid beslag av mobiltelefoner har fyra problemområden identifierats. Hur ska mobiltelefoner undersökas? Hur ska elektronisk information beslagtas? Hur ska föränderlig information hanteras? Är integritetsskyddet i beslagslagstiftningen tillämpligt på elektronisk information?

Beslagsundersökningen av mobiltelefoner ska ske så effektivt som möjligt samtidigt som den enskildes integritet ska upprätthållas i största möjliga mån. Kopieringsförfarandet vid beslag av mobiltelefoner riskerar att kringgå beslagslagstiftningens integritetsskydd, vilket gör att det uttryckligen borde framgå att integritetskyddet även ska tillämpas på kopierad egendom.

Elektronisk information är något immateriellt som inte kan beslagtas. Lagras information på en elektronisk enhet borde den dock kunna beslagtas. I beslagslagstiftningen borde det införas ett förtydligande om att beslag av elektroniska enheter även inkluderar den elektroniska information som finns lagrad på enheten.

Beslag borde inte omfatta meddelanden som inkommer till en mobiltelefon efter beslagstillfället eftersom dessa anses vara pågående kommunikation. Istället ska reglerna om hemlig avlyssning av elektronisk kommunikation vara tillämpliga. För att tydliggöra detta borde lagstiftaren klargöra att beslag omfattar information som finns vid beslagstillfället och att meddelanden som inkommer därefter är pågående kommunikation.

Enligt ordalydelsen är det oklart om 27 kap. 2 § och 12 § RB är tillämpliga på mobiltelefoner innehållande elektronisk information. Eftersom bestämmelsernas ändamål är att skydda korrespondens och förtrolig information borde all informationen oavsett om den är skriftlig eller elektronisk inbegripas i bestämmelsen. Detta ska uttryckligen framgå av lagtexten.

Avslutningsvis kan det konstateras att beslagslagstiftningen är omodern och behöver reformeras för att möta de krav som ställs vid beslag av mobiltelefoner. Detta för att skydda den personliga integriteten samtidigt som brottsbekämpningen blir mer effektiv.

Förord

Ett särskilt tack riktas till min handledare Helén Örnemark Hansen och kammaråklagare Jan Tibbling för all hjälp och vägledning.

Jag vill rikta ett stort tack till mina föräldrar för ert stöd under min studietid och skrivandet av denna uppsats. Ett tack riktas även till alla ni andra som korrekturläst eller på annat sätt hjälpt mig under mitt skrivande.

Lund, maj 2014

Karin Henriksson

Förkortningar

Ds	Departementsserien
EKMR	Europeiska konventionen den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna
FN	Förenta Nationerna
GPS	Global Positioning System
HD	Högsta domstolen
IT	Informationsteknik
JK	Justitiekanslern
JO	Justitieombudsmannen
LEK	Lag (2003:389) om elektronisk kommunikation
MMS	Multi Media Messaging Service
NJA	Nytt juridisk arkiv
Prop.	Proposition
RB	Rättegångsbalk (1942:740)
RF	Regeringsreformen (1974:152)
SCB	Statistiska Centralbyrån
SIM	Subscriber Identity Module
SMS	Short Message Service
SOU	Statens offentliga utredningar
SvJT	Svensk Juristtidning
TF	Tryckfrihetsförordningen (1949:105)

1 Inledning

Lagstiftarens syfte har varit att införa en neutral tvångsmedelslagstiftning som inte ska påverkas av yttre omständigheter. I takt med det senaste decenniets tekniska framsteg har denna utgångspunkt ifrågasatts. Det har bland annat föreslagits att beslagslagstiftningen ska bli mer teknikinriktad. En anledning till detta är att elektroniska enheter, till exempel mobiltelefoner, innehåller elektronisk information som kontinuerligt förändras. Beslag av mobiltelefoner skiljer sig således från beslag av skriftliga handlingar där texten och innehållet är konstant. Inga lagstiftningsåtgärder har vidtagits trots att flera statliga utredningar rekommenderat att beslagslagstiftningen ska moderniseras och göras mer tekniskt anpassad.

Beslagslagstiftningens anpassning till teknisk utveckling utifrån beslag av mobiltelefoner innehållande elektronisk information är av särskilt intresse. Den tekniska utvecklingen inom detta område har varit markant och mobiltelefoner innehåller stora mängder information som kan ha betydelse som bevis i brottmål. Inte heller har beslag av mobiltelefoner behandlats i någon större utsträckning inom den rättsvetenskapliga forskningen.

Problematiken vid beslag av mobiltelefoner beror främst på att mobiltelefoner innehåller stora mängder information. Det är därför svårt att undersöka och sortera ut relevant information som finns i mobiltelefoner. Teknisk utveckling har också resulterat i att informationen i mobiltelefonen är föränderlig och kan lagras på olika sätt. Huruvida beslag av mobiltelefoner omfattar information som inkommer efter beslagstillfället och information som lagras på andra ställen än i själva telefonen är ovisst. Beslagslagstiftningen innehåller dessutom ett uttryckligt stadgande om att skriftlig information har ett utvidgat integritetsskydd och det är oklart om information i mobiltelefoner inbegrips i detta skydd. Ingen vägledning fås i beslagslagstiftningen utan det är framför allt åklagarväsendet som instiftat riktlinjer på områdena. Med tanke på de senaste två årens explosionsartade utveckling inom mobiltelefoni och det oklara rättsläget är det aktuellt att utreda om lagstiftningsåtgärder avseende beslag behöver vidtas och ifall dessa ska vara teknikanpassade.

Det faktum att mobiltelefoner lagrar stora mängder information om den enskilde individen är även problematiskt så till vida att beslag av mobiltelefoner idag kan bidra till omfattande kartläggningar av enskilda individers privatliv, vilket inte kunnat ske tidigare. Att kunna sammanställa så mycket information om enskilda individer genom att endast undersöka en informationskälla är positivt ur ett brottsbekämpande perspektiv men negativt ur ett integritetsperspektiv. Mot bakgrund av detta är det av vikt att åskådliggöra vilka konsekvenser och effekter tekniska framsteg får för effektiv brottsbekämpning och personlig integritet. Därmed bör frågan om en eventuell ny beslagslagstiftning även belysas utifrån effektiv brottsbekämpning och personlig integritet.

1.1 Syfte och problemformulering

Syftet är att undersöka beslagslagstiftningen utifrån mobiltelefoni och analysera behovet av att införa lagstiftningsåtgärder för att anpassa beslagslagstiftningen till den tekniska utvecklingen. Detta görs utifrån de teoretiska angreppssätten, effektiv brottsbekämpning och personlig integritet. Följande frågeställningar behandlas:

- Under vilka förutsättningar kan mobiltelefoner beslagtas?
- Vilka lagtekniska och praktiska problem uppstår vid beslag av mobiltelefoner innehållande elektronisk information?
- Vilka lagstiftningsåtgärder behöver vidtas för att komma till rätta med de problem som uppstår i samband med beslag av mobiltelefoner innehållande elektronisk information?

1.2 Avgränsning

Studien behandlar beslag i 27 kap. RB eftersom dessa regler är normerande. Utifrån reglerna i 27 kap. RB har innebörden och definitionen av beslag fastställts. Andra beslagsregler som återfinns i speciallagar lämnas utan hänseende. Flera närliggande rättsregler, LEK samt lagreglerna om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation får betydelse för den huvudsakliga problematiken gällande beslag av mobiltelefoner innehållande elektronisk information. Dessa regler berörs endast i korthet och då de har betydelse för studiens problematik.

För att få en heltäckande bild av beslag av mobiltelefoner innehållande elektronisk information behöver jämförelser till viss del göras med beslag av skriftliga handlingar och datorer. Jämförelsen med skriftliga handlingar är intressant då beslagslagstiftningen och dess integritetsskydd uttryckligen är tillämpligt på den sortens handlingar. Då utvecklingen av mobiltelefoni har resulterat i att mobiltelefoner alltmer liknar datorer kan den rättsvetenskaplig forskning avseende datorer till viss del vara relevant för beslag av mobiltelefoner. En stor del av forskningen har inriktats på kopiering av innehållet i datorer. Eftersom innehållet i mobiltelefoner och datorer kopieras på olika men snarlika sätt redogör studien endast för de övergripande aspekterna i förfarandet med kopiering avseende datorer. Övriga föremål som kan beslagtas nämns inte.

Vid beslag av mobiltelefoner innehållande elektronisk information fås överskottsinformation. Då problematiken gällande överskottsinformation är gemensam för alla tvångsmedel som inhämtar information har den uteslutits ur studien. Andra aspekter som tidpunkten då beslag ska hävas, dokumentation vid beslag, samtyckesproblematik, beslagsföremålets bevisvärde samt gränsdragningen mellan föremål som ska beslagtas och föremål som inte

behöver beslagtas lämnas utan hänseende. Inte heller görs någon ingående redogörelse för själva beslagsförfarandet.

Historiska och komparativa perspektiv på beslagslagstiftningen behandlas inte. Äldre statliga utredningar har dock använts för att belysa argument som talar för och emot lagstiftningsåtgärder som berör beslagslagstiftningen och elektronisk information. Statistiska uppgifter som visar hur ofta och för vilka ändamål de brottsbekämpande myndigheterna tillämpar beslag har inte inkluderats i studien. Det beror på att inga undersökningar inom området gjorts och att det därmed saknas statistik.

Avsnittet om personlig integritet avser endast den enskildes skydd mot det allmänna. Den enskildes integritetsskydd gentemot andra individer utreds således inte. Avvägningen mellan effektiv brottsbekämpning och personlig integritet åskådliggörs huvudsakligen utifrån tekniska aspekter, framför allt utifrån elektronisk kommunikation. Den tekniska redogörelsen gör inte anspråk på att vara heltäckande utan ges för att fördjupa förståelsen för de juridiska problemen.

1.3 Begreppsbestämning

I studien används följande grundläggande begrepp; tvångsmedel, brottsbekämpande myndigheter, mobiltelefon, smartphone, elektronisk information, data, databehandlingsbara uppgifter, elektroniska enheter, kommunikationsmedel, digitala informationsbärare och elektronisk kommunikation. Nedan sker ett förtydligande om vilken innebörd begreppen har i denna studie.

Tvångsmedel kan delas in i två kategorier, straffprocessuella och civilrättsliga. När begreppet tvångsmedel brukas i studien avses straffprocessuella tvångsmedel då beslag tillhör denna kategori.

Med brottsbekämpande myndigheter menas myndigheter som utövar brottsutredande verksamhet. Detta är exempelvis Rikspolisstyrelsen, Säkerhetspolisen, Åklagarmyndigheten och polismyndigheterna.[1]

Förr ansågs mobiltelefoner vara trådlösa handhållna telefoner vars huvudsakliga syfte var telefoni. Teknikutvecklingen har lett till att mobiltelefoner är något mer än bara en telefon. Användaren kan exempelvis lyssna på musik, surfa, skicka textmeddelanden och bilder med sin telefon.[2] I studien anses en mobiltelefon vara något mer än en telefon då beslag av mobiltelefoner innehållande elektronisk information inte endast syftar till beslag av telefoni. Parallellt med begreppet mobiltelefon används begreppet

[1] SOU 2012:44 s. 113.
[2] http://www.ne.se/enkel/mobiltelefon.

smartphone då detta är en telefon som härstammar från den senaste tekniska utvecklingen.[3]

Elektronisk information åsyftar information som lagras elektroniskt. Detta kan bland annat vara textfiler, bildfiler, ljudfiler eller en blandning av samtliga filer.[4] Begreppen data och databehandlingsbara uppgifter ges samma innebörd som elektronisk information.

Olika hjälpmedel kan nyttjas för att lagra, förmedla och avläsa elektronisk information. I generella sammanhang där flera hjälpmedel åsyftas samtidigt benämns dessa som elektroniska enheter, kommunikationsmedel eller digitala informationsbärare. Samlingsnamnen används synonymt.

Elektronisk kommunikation innebär att elektronisk information överförs från en plats till en annan. Överföringen sker med hjälp av tråd eller radio på optisk väg eller via andra elektromagnetiska överföringsmedier. Meddelanden som förmedlas via telefoni, datakommunikation samt sändningar från radio och TV är olika typer av elektronisk kommunikation.[5]

1.4 Forskningsläge

Det rättsdogmatiska perspektivet avseende beslag har avhandlats i den rättsvetenskapliga forskningen. Tre verk som ingående redogör för tvångsmedlet är *Straffprocessuella tvångsmedel* av Gunnel Lindberg[6], *Tillgången till handlingar för brottsutredare* av Mattias Hjertstedt[7] samt *Förundersökning* av Thomas Bring och Christian Diesen[8]. Lindberg och Hjertstedt problematiserar även till viss del beslag av mobiltelefoner och beslag av elektronisk information medan Bring och Diesen inte alls nämner dessa områden.

Teknisk utveckling och dess påverkan på svensk strafflagstiftning har inte behandlats i någon större omfattning inom den juridiska forskningen. Detta trots att flera statliga utredningar[9] alltmer inriktats på att studera hur den tekniska utvecklingen påverkar lagstiftningen. En sådan utveckling tyder på ett behov av att dryfta frågan om hur teknikens influenser påverkar såväl lagstiftningen som tolkningen av grundläggande svenska rättsprinciper och rättsliga begrepp. Den bok som ger en övergripande bild av vilken lagstiftning som påverkats av tekniska framsteg och varför är Stefan

[3] http://www.ne.se/lang/smartmobil.
[4] Prop. 2002/03:110 s. 58.
[5] SOU 2005:38 s. 18-19.
[6] Lindberg, Gunnel, *Straffprocessuella tvångsmedel: när och hur får de användas?* uppl 3, 2012.
[7] Hjertstedt, Mattias *Tillgången till handlingar för brottsutredare: en rättsvetenskaplig studie av beslag med husrannsakan, myndigheter utlämnandeskyldighet sam editions- och exhibitionsplikt*, 2011.
[8] Bring, Thomas, Diesen, Christian, *Förundersökning*, uppl 4, 2009.
[9] Se t.ex. Prop. 2002/03:110, SOU 2001:28, SOU 2005:38, SOU 2008:3.

Kronqvists *Brott och digitala bevis*[10]. Beslagslagstiftningen och därmed beslag av elektronisk information och mobiltelefoner berörs endast i korthet.

Avvägningen mellan brottsbekämpning och personlig integritet samt teknikens betydelse för denna avvägning har problematiserats generellt och utifrån hemlig tvångsmedelsanvändning. En stor debatt på området fördes i *Svensk Juristtidning*[11] 2007. Hur avvägningen ska göras vid användning av beslag har inte uttryckligen avhandlats.

1.5 Metod och material

Eftersom forskningen endast i begränsad omfattning behandlat beslag av mobiltelefoner innehållande elektronisk information är det aktuellt att ingående redogöra för såväl det rättsdogmatiska läget som den problematik som uppstår vid den sortens beslag. Det är även aktuellt att undersöka mobiltelefoner då teknikutvecklingen lett till att dessa telefoner innehar stora mängder information som kan ha värde som bevis i brottmål. För att utreda beslag av mobiltelefoner behöver en studie göras av hur den tekniska utvecklingen dels påverkat beslagslagstiftningen, dels förändrat synsättet vid avvägningen mellan effektiv brottsbekämpning och personlig integritet.

De metoder som tillämpats är en rättsdogmatisk metod, en empirisk kvalitativ undersökning och en rättspolitisk argumentationsmetod. En rättsdogmatisk metod påvisar gällande rätt utifrån rättskälleläran. Juridisk doktrin innefattas i rättskälleläran men har inte lika högt värde som lagtext, förarbeten och rättspraxis.[12] Gällande rätt avseende beslag av mobiltelefoner innehållande elektronisk information fastställs med denna metod. Materialet som bestämmer rättsläget, är till största del förarbeten och juridisk doktrin då inga lagregeler uttryckligen berör beslag av information som lagras elektroniskt. Inte heller finns det någon rättspraxis som preciserar rättsläget.

Förarbeten och juridisk doktrin är generellt sett tillförlitliga rättskällor eftersom de innehåller sammanställningar och resonemang kring gällande rätt. Inom juridisk doktrin har framför allt Lindbergs och Hjertstedts litteratur använts eftersom dessa författare är auktoriteter på området. Detta kan exempelvis ses genom att det hänvisats till författarnas resonemang i statliga utredningar.

En empirisk kvalitativ undersökning[13] har gjorts för att påvisa ett praktiskt perspektiv av problematiken vid beslag av mobiltelefoner innehållande elektronisk information. Med både ett teoretiskt och praktiskt angreppssätt ges en mer heltäckande bild av beslag av mobiltelefoner innehållande

[10] Kronqvist, Stefan, *Brott och digitala bevis: en handledning*, uppl 3, 2013.
[11] SvJT 2007 s. 1-180.
[12] För ytterligare information, se Lehrberg, Bert, *Praktisk juridisk metod*, uppl 6, 2010.
[13] För ytterligare information, se Bryman Alan, *Samhällsvetenskapliga metoder*, uppl 2, 2011.

elektronisk information och dess problematik. En intervju genomfördes med Jan Tibbling, Kammaråklagare på Ekobrottsmyndigheten i Stockholm, se bilaga A. Tibbling intervjuades eftersom han använder både öppna och hemliga tvångsmedel i sin normala verksamhet och är därmed väl insatt i den problematik som uppstår vid beslag av mobiltelefoner som innehåller elektronisk information. Endast en intervju gjordes eftersom syftet med intervjun inte var att ge en bild av hur åklagare agerar vid beslag av mobiltelefoner utan att definiera vilka praktiska problemområden som finns vid beslag av mobiltelefoner. Den intervju som genomfördes var semistrukturerad, vilket innebär att den som intervjuar ställer frågor inom specifika teman och den intervjuade får stor frihet att utforma sina svar. Därmed utgår intervjun ifrån hur den intervjuade tolkar och uppfattar situationen i frågorna.

Även Åklagarmyndighetens och Ekobrottmyndighetens riktlinjer[14] samt en undersökning från Säkerhets- och Integritetsskyddsnämnden[15] har studerats för att vidga det praktiska perspektivet. Då både teoretiska och praktiska källor behandlas ges en mer utförlig bild av de lagstekniska och praktiska problem som uppstår vid beslag av mobiltelefoner innehållande elektronisk information.

Säkerhets- och Integritetsskyddsnämndens undersökning, åklagarnas riktlinjer och intervjun med Tibbling är inte neutrala källor. Intervjun och riktlinjerna belyser beslag av mobiltelefoner och elektronisk information utifrån ett brottsbekämpande perspektiv medan Säkerhets- och Integritetsskyddsnämnden belyser samma frågor utifrån ett integritetsperspektiv. Eftersom källorna uttrycker två motstående perspektiv måste de relateras till varandra för att ge en komplett bild av beslagslagstiftningen och dess problematik avseende beslag av mobiltelefoner och elektronisk information.

Den rättspolitiska argumentationsmetodens utgångspunkt är att analysera rättsläget samt studera fördelar och nackdelar med föreslagna lagstiftningsåtgärder. I enlighet med denna metod ska de lagstiftningsåtgärder som leder till att lagregler bättre tillgodoser sitt ändamål rekommenderas.[16] Den rättspolitiska argumentationsmetoden har tillämpats för att undersöka vilka lagstiftningsåtgärder som behöver vidtas för att komma till rätta med de problem som uppstår i samband med beslag av mobiltelefoner innehållande elektronisk information. De lagstiftningsåtgärder som presenteras i studien har främst baserats på olika statliga utredningar eftersom dessa förelagit förändringar i beslagslagstiftningen. Statliga utredningar är ofta skrivna utifrån ett visst perspektiv eftersom de tillsätts för att exempelvis se över en lagstiftnings effektivitet eller integritetsskydd. Därmed ska lagstiftningsåtgärderna kritiskt granskas utifrån de perspektiv som står emot utredningarnas. Argumentationsmetoden tillämpas även i analysen då syftet är att

[14] Åklagarmyndigheten och Ekobrottsmyndigheten, Beslag: en handbok, 2013.

[15] Säkerhets- och Integritetsskyddsnämnden, Rapport 2011-06-09.

[16] För ytterligare information, se Sandgren, Claes, *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*, 2007.

avgöra om mer teknikanpassade regler behöver införas i beslagslagstiftningen och i sådana fall vilka förändringar som är motiverade.

I de statliga utredningarna om beslag[17] har ingen sammanställning av teknikutvecklingens påverkan på beslagslagstiftningen gjorts. Eftersom forskningsläget gällande teknikutveckling och beslag är begränsat är det av vikt att ge en bakgrund till den tekniska utveckling som påverkat beslagslagstiftningen. Bakgrunden ges i kapitel tre och inriktas främst på utvecklingen inom kommunikation, framför allt mobiltelefoni, samt teknikens påverkan på brottsbekämpning, personlig integritet och lagstiftningsförfarandet. Andra statliga utredningar[18] har berört teknisk utveckling och vissa grundläggande utgångspunkter om teknik, integritet och lagstiftning har fastställts. Dessa utgångspunkter bör kunna tillämpas även i denna redovisning då resonemangen avser teknikutvecklingen i generell mening.

För att öka förståelsen om den tekniska utvecklingen har studien också kompletterats med viss teknisk litteratur och statistik. Litteraturen grundas främst på Stefan Kronqvists *Brott och digitala bevis*[19] eftersom detta verk behandlar både teknik och juridik. Statistiken är hämtad från Stiftelsen för Internetinfrastrukturs rapport *Svenskarna och internet 2013*[20] och illustrerar övergripande utvecklingen inom det tekniska området. Stiftelsen för Internetinfrastruktur publicerar årligen statistik om svenskarnas internetanvändning tillsammans med SCB vilket gör uppgifterna trovärdiga. På grund av den snabba tekniska utvecklingen kan forskning om mobiltelefoner och beslag av mobiltelefoner innehållande elektronisk information som gjordes för något år eller flera år sedan redan vara inaktuell. Därmed har varje källas aktualitet prövats innan den använts.

För att tydliggöra avvägningsproblematiken mellan effektiv brottsbekämpning och personlig integritet samt teknikutvecklingens påverkan på denna avvägning har flera artiklar använts. Artiklarna är uteslutande hämtade från juridiska tidskrifter eftersom de då garanterar praktisk eller akademisk kunskap i ämnet. Under året 2007 fördes en debatt i *Svensk Juristtidning*[21] som belyste tvångsmedel, effektiv brottsbekämpning och integritet. Debatten berörde främst de hemliga tvångsmedlen men även tvångsmedelsanvändning i stort vilket gör att artiklar från denna debatt kan appliceras på beslag.

1.6 Teori

Effektiv brottsbekämpning och personlig integritet är de två teoretiska angreppssätt som tillämpas. Först används teorierna för att urskilja och

[17] Se t.ex. SOU 1984:54, SOU 1992:110, SOU 1995:47 och SOU 2011:45.
[18] Se t.ex. Prop. 2002/03:110, SOU 2001:28, SOU 2005:38, SOU 2008:3.
[19] Kronqvist, 2013.
[20] Stiftelsen för Internetinfrastruktur, *Svenskarna och internet 2013*.
[21] SvJT 2007 s. 1-180.

fastställa svårigheter med beslag av mobiltelefoner innehållande elektronisk information. Utifrån teorierna avgörs sedan vilka lagstiftningsåtgärder som är lämpliga att införa för att komma till rätta med svårigheterna.

Teorierna har valts då den teknisk utveckling har påverkat avvägningen mellan brottsbekämpning och integritet samt då brottsbekämpning och integritet är två perspektiv som får betydelse vid lagstiftning gällande beslag. Frågan om hur brottsbekämpning kan anpassas till ny teknik utan att den enskildes personliga integritet inskränks i allt för stor omfattning har fått stor betydelse i samhället. Brottsutredande myndigheter behöver tillgång till elektronisk information för att kunna utreda brott men då individer förmedlar alltmer personlig information via elektronisk kommunikation finns risk för grova integritetsintrång om myndigheter utan samtycke säkrar exempelvis mobiltelefoner som bevisning. Därmed är det aktuellt att utreda hur teknisk utveckling påverkat avvägningen mellan effektiv brotts-bekämpning och personlig integritet vid beslag.

De senaste lagförslagen som lagts fram rörande beslag har utretts utifrån både effektiv brottsbekämpning och personlig integritet. Således är det av stor vikt att bedöma nya lagstiftningsåtgärder som syftar till att anpassa beslagslagstiftningen till teknisk utveckling utifrån dessa perspektiv.

1.7 Disposition

I kapitel två redovisas innebörden av effektiv brottsbekämpning och personlig integritet. Begreppens innebörd och funktioner är studiens ramverk då beslag av mobiltelefoner innehållande elektronisk information belyses utifrån dessa aspekter. Därefter, i tredje kapitlet, behandlas teknisk utveckling avseende kommunikation och dess påverkan på brotts-bekämpning, personlig integritet och lagstiftning. En övergripande redo-görelse för de grundläggande förutsättningarna för beslag ges i fjärde kapitlet. Detta görs för att ge en djupare förståelse för den problematik som behandlas i femte kapitlet. Där görs en genomgång av lagtekniska och praktiska problem vid beslag av mobiltelefoner. Kapitlet är utformat så att det nuvarande rättsläget avhandlas samtidigt som problemområdena presenteras. Därefter redovisas argument som talar för och emot nya lag-stiftningsåtgärder. Avslutningsvis, i sjätte kapitlet, görs en analys där studiens frågeställning besvaras. Först analyseras beslag av mobiltelefoner och därefter presenteras de områden som är problematiska vid beslag av mobiltelefoner innehållande elektronisk information. I samband med redo-görelsen för problemområdena förs en argumentation om lagstiftnings-åtgärder behöver vidtas och i så fall vilka åtgärder som är lämpliga. Sist utreds om beslagslagstiftningen behöver förändras eller om den nuvarande lagstiftningen är anpassad till teknisk utveckling och därmed även till beslag av mobiltelefoner innehållande elektronisk information.

2 Brottsbekämpning och integritet

Varje gång brottsbekämpande myndigheter ska nyttja tvångsmedel görs en bedömning om det brottsbekämpande intresset är så stort att den enskildes personliga integritet får inskränkas. Hur bedömningen ska göras har debatterats inom den juridiska forskningen och två argument som präglat debatten är risken för ett övervakningssamhälle likt samhället i George Orwells bok *1984* och föreställningen om att oskyldiga individer inte har något att dölja.[22] Dessa argument behandlar inte den relevanta problematik som uppstår vid avvägningen mellan effektiv brottsbekämpning och personlig integritet. Tekniken för att skapa ett övervakningssamhälle finns redan och därmed är det inte tvångsmedelsanvändning i sig som ökar risken för att människor ska bli övervakade. Istället riskerar människor att bli övervakade om tvångsmedel missbrukas.[23] Vidare framgår det av EKMR och RF att ingen oskyldig eller ej ska behöva oroa sig för en ständig övervakning. Den relevanta problematik som bör lyftas är snarare när det är rimligt att nyttja tvångsmedel och i vilken utsträckning.[24] Detta perspektiv behandlas i studien. Nedan redogörs för vad som innefattas i effektiv brottsbekämpning och personlig integritet samt hur dessa begrepp förhåller sig till insamling av information.

2.1 Effektiv brottsbekämpning

Effektiv brottsbekämpning ska minska antalet felaktigt friande domar genom att brott utreds så effektivt att brottslingar lagförs.[25] Det finns två sätt att lagföra brottslingar. Lagföring kan ske om den misstänkte erkänner brott eller om brottsbekämpande myndigheter funnit tillräckligt med bevis för att få en fällande dom vid en rättegång. Bevisningen måste då uppnå bevis-kravet ”ställt bortom rimligt tvivel”.[26]

Brottsbekämpande myndigheter bedriver brottsutredande verksamhet genom förundersökningar som syftar till att utreda om brott begåtts, vem som begått brottet och omständigheter om brottet. I en förundersökning insamlas även bevis mot den misstänkte. Således har myndigheterna legitima behov av att eftersöka information och säkra bevisning i den brottsutredande verksamheten. Utredning, rapportering, spaning, samt förhör med vittnen

[22] Abrahamsson, Olle, ”Integritetsskydd med eller utan förnuft”, *Svensk Juristtidning*, 2009 s. 424-425.
[23] Axberger, Hans-Gunnar, ”Integritetsskydd i perspektiv”, *Svensk Juristtidning*, 2009 s. 482.
[24] Abrahamsson, 2009 s. 424, 427.
[25] Hjertstedt, 2011 s. 113.
[26] Lindberg, 2012 s. 17.

och andra personer är olika sätt att insamla information.[27] Det saknas lagregler om hur informationsinhämtning får ske och hur informationen ska hanteras. Avsaknaden av lagregler beror på att det är tillåtet att åberopa all slags bevisning i brottmål och att domstolen fritt kan pröva bevisningen som lagts fram, så kallad fri bevisföring och fri bevisprövning.[28] Insamling av information är inte en tvångsmedelsåtgärd. Tvångsmedelsanvändning underlättar dock informationshämtning på grund av att vissa tvångsmedel, så som husrannsakan och beslag gör information tillgänglig.[29]

En effektiv brottsbekämpning ökar allmänhetens förtroende för de brotts-bekämpande myndigheterna. Dock minskar allmänhetens förtroende om mänskliga rättigheter inskränks till följd av en mer effektiv brotts-bekämpning. En ökad tvångsmedelanvändning kan på så sätt minska allmänhetens förtroende om tvångsmedlen inte är rättssäkra och beaktar den enskildes integritet.[30]

2.2 Personlig integritet

En allmän definition av begreppet personlig integritet saknas.[31] Den språkliga innebörden av begreppet är att alla har ”[…] rätt att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp”[32]. Innebörden av personlig integritet har även utretts i olika statliga utredningar. Sammanfattningsvis är grundtanken med begreppet att den enskilde individen har en egen personlig sfär och att oönskade intrång inom denna sfär ska kunna avvisas. Privata angelägenheter ska således inte vara tillgängliga utan den enskildes tillstånd.[33] Den personliga sfären omfattar den rumsliga, materiella och kroppsliga integriteten samt den personliga integriteten i fysisk och ideell mening.[34] Dessutom är sfären föränderlig och påverkas av kulturell, etnisk, religiös och social bakgrund.[35] Således har erfarenheter, känslor, värderingar samt samhällsutvecklingen och allmänhetens uppfattning om vad som är personlig integritet inverkan på vad som inbegrips i den personliga sfären.[36]

Den enskilde är skyddad mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning och avlyssning av förtrolig kommunikation enligt RF.[37] Skyddet för förtrolig kommunikation omfattar alla föremål som

[27] SOU 2012:44 s. 113, 173.
[28] Ds 2005:6 s. 305.
[29] Bring, Diesen, 2009 s. 282-284.
[30] Ramberg, Anne, ”Tvångsmedel, rättssäkerhet, integritet – går det att förena?”, *Svensk Juristtidning*, 2007 s. 167, 170.
[31] SOU 2007:22 s. 52.
[32] http://www.ne.se.ludwig.lub.lu.se/sok?q=integritet.
[33] Jfr. SOU 1970:47 s. 58, SOU 2002:18 s. 53.
[34] SOU 1984:54 s. 42.
[35] SOU 2002:18 s. 53.
[36] Ds 1994:51 s. 8-9.
[37] 2 kap. 6 § RF.

kan beslagtas.[38] I internationella konventioner, EKMR och FN:s allmänna förklaring om de mänskliga rättigheterna, innefattas skyddet för den personliga integriteten i rätten till privatliv. I FN:s allmänna förklaring om de mänskliga rättigheterna anses rätten till privatliv omfatta individens rätt att leva sitt liv utan inblandning från staten.[39] Artikel 8 i EKMR skyddar rätten till privat- och familjeliv, hem och korrespondens genom att förhindra staten från att ingripa i enskilda personers privatliv. Skyddet för den enskildes korrespondens omfattar överförande av meddelanden mellan individer. Hit hör brev, telefoniska och telegrafiska kommunikationer samt överförande av meddelanden med hjälp av radio och elektronisk teknik.[40] EKMR skyddar även enskildas egendom då det i EKMR stadgas att ingen ska berövas sin egendom annat än i vissa undantagsfall.[41] Egendomsrätten inskränks vid beslag eftersom den enskilde berövas sin egendom eller förlorar rätten att förfoga över sin egendom.[42] Det finns inga motsvarande regler i RF.[43]

Enligt EKMR och RF får regler om personlig integritet, rätten till privatliv och egendom inskränkas genom lag. Inskränkningen måste skydda ett visst legitimt intresse, vara lagstadgad, vara nödvändigt i ett demokratiskt samhälle och stå i proportion till ändamålet som föranlett det.[44] Den inskränkande regleringen ska vara så preciserad att den är förutsebar och kan skydda individer mot godtyckliga ingrepp.[45]

Tvångsmedelsanvändning medför alltid ett integritetsintrång vilket innebär att lagregler tydligt ska ange när det är tillåtet att bruka straffprocessuella tvångsmedel, så som beslag.[46] Dock kan tvångsmedel vara rättssäkra om dess reglering är tydlig, om tillämpningen är förutsebar och om det finns skydd mot maktmissbruk.[47] Ett integritetsintrång kan också avse insamling och offentliggörande av uppgifter om en persons privata förhållanden. Dessa uppgifter får endast i undantagsfall presenteras som bevis i brottmål eftersom det enbart är den enskilde som får sprida informationen.[48] Myndigheter kan därmed inte utan lagstöd, i exempelvis tvångsmedels-lagstiftningen, samla in information om enskilda personer i syfte att kart-lägga deras personliga förhållanden.[49] Varje gång staten genom lag tillåts ta del av personlig information sker ett integritetsintrång och detta intrång varierar beroende på ingreppets utformning och tillämpning.[50] Det görs också skillnad på abstrakta och konkreta integritetsintrång då abstrakta

[38] SOU 2008:3 s. 102.
[39] Artikel 12 i FN:s allmänna förklaring av de mänskliga rättigheterna.
[40] Danelius, Hans, *Mänskliga rättigheter i europeisk praxis – En kommentar till Europakonventionen om de mänskliga rättigheterna*, uppl 4, 2012, s. 347, 403.
[41] Artikel 1 tilläggsprotokollet den 20 mars 1952 Europakonventionen.
[42] Hjertstedt, 2011 s. 121.
[43] Jfr 2 kap 15 § RF.
[44] 2 kap. 20-21 §§ RF, artikel 8.2 EKMR.
[45] Danelius, 2012 s. 351.
[46] Lindberg, 2012 s. 13.
[47] SOU 2012:44 s. 478.
[48] Strömholm, Stig; ”Integritetsskyddet”, *Svensk Juristtidning*, 1971 s. 698.
[49] SOU 2008:3 s. 18.
[50] SOU 2012:44 s. 480.

intrång innebär att myndigheter kan övervaka en enskild individ medan konkreta intrång avser ett faktiskt handlande.[51] För att skydda den enskildes integritet jämförs den förväntade skadan på den personliga integriteten med den förväntade skadan ett upprätthållande av integriteten orsakar på andra beaktansvärda intressen. Skadan som är störst ska skyddas. Integritets-skyddet påverkas därmed av motstående intressen i varje enskilt fall.[52]

[51] Axberger, 2009 s. 481.
[52] SOU 2007:22 s. 52.

3 Teknisk utveckling

Tekniken inom informationsområdet har det senaste decenniet kontinuerligt förändrats. Med den senaste tekniken har det skapats hjälpmedel som används både på arbetsplatsen, i skolan och på fritiden. Dessutom nyttjar allt fler personer den senaste tekniken till att hålla kontakt med andra personer, spela spel och lyssna på musik. Utvecklingen inom informationsområdet har inte enbart varit positiv då de tekniska framstegen möjliggjort fler och större intrång i enskilda personers integritet. Eftersom samhället inte har någon möjlighet att kontrollera utvecklingen kan inte heller integritetsintrång som uppstår till följd av tekniska framsteg begränsas i förväg.[53] Dessutom kan den tekniska utvecklingen utnyttjas för brottsliga syften.[54] I det följande presenteras i korthet den tekniska utvecklingen på informationsområdet avseende kommunikation och mobiltelefoni samt dess påverkan på brotts-bekämpning, den personliga integriteten och lagstiftningsförfarandet.

3.1 Kommunikation

Kommunikation innebär ett utbyte av information mellan två eller flera personer och kan delas in i direkt och indirekt kommunikation. Direkt kommunikation sker när mottagaren uppfattar meddelandet samtidigt som det kommuniceras. Därmed sker kommunikationen i realtid. Ett exempel på detta är när personer samtalar med varandra. Indirekt kommunikation innebär att avsändaren kommunicerar på ett längre avstånd med ett hjälpmedel så som en dator, en telefon eller ett papper. E-post, telefonsamtal eller meddelanden via brev är exempel på indirekt kommunikation. Denna sortens kommunikation kan antingen ske i realtid eller med en tids-fördröjning.[55]

Den tekniska utvecklingen har förändrat sättet som människor kom-municerar på eftersom elektroniska kommunikationstjänster, så som e-post, SMS, MMS och chat, blir alltmer mobila och inriktade på information. Konsekvensen av utvecklingen är att traditionell telefoni får stå tillbaka för datakommunikation. Olika kommunikationsmedel, så som datorer, mobil-telefoner, radioapparater och TV-appareter kan idag i stort sett förmedla samma sorts elektronisk kommunikation, lagra samma sorts elektroniska information och tillhandahålla samma funktioner och tjänster. Det är exempelvis möjligt att koppla upp sig till internet i TV:n och se på TV i mobiltelefonen.[56] E-post kan läsas av och skickas inte bara från datorer utan

[53] SOU 2008:3 s. 331-332.
[54] Eriksson, Anders ”Några ord om reformbehovet i den lagstiftning som rör tvångsmedel m.m.”, *Svensk Juristtidning*, 2007 s. 130.
[55] SOU 2001:28 s. 129-130.
[56] Prop. 2002/03:110 s. 58.

även från mobiltelefoner. Vidare kan användaren lyssna på radio, se på olika TV-program, chatta, skicka SMS och nyttja traditionella teletjänster via internet.[57]

Utvecklingen har resulterat i en ökad integration av kommunikations-tjänster. Integreringen är ett resultat av digitaliseringen, den ökande överföringskapaciteten och den tekniska standardiseringen. Digitaliseringen har lett till att data baseras på det binära talsystemet. Filer med text, ljud, bild, video eller dataprogram har därmed olika koder som består av elektroniska impulser i form av ettor och nollor.[58] Skillnaden mellan filerna består enbart av den binära koden. I övrigt är det ingen skillnad mellan en textfil, bildfil eller webbsida.[59] Då datorer kan läsa av och förstå all digitalt lagrad data kan alla filer, oberoende av om det är text, ljud eller bild, behandlas integrerat. Digitaliseringen möjliggör även att informationen kan komprimeras mer än analog information vilket gör att överförings-kapaciteten ökar. Överföringskapaciteten har även ökat i takt med telenätens utveckling. Dessutom har standardiseringen som en följd av internet lett till att allt fler, både nationellt och internationellt, tillämpar samma standarder.[60]

3.2 Mobiltelefoni

Dagens smartphone är utrustad med många olika funktioner och tjänster så som kamera, kalender, radio, musikspelare, applikationer och GPS.[61] Dessutom har mobiltelefoner stora lagringsutrymmen för data. Detta och det faktum att telefoner innehåller en extern hårddisk, SIM-kortet, har lett till att smartphone nästan ersatt den handburna datorn. En mobiltelefon kan idag ses som en liten dator då en dator enligt definitionen ska inneha en processor och något form av minne vilket även en mobiltelefon numera har.[62]

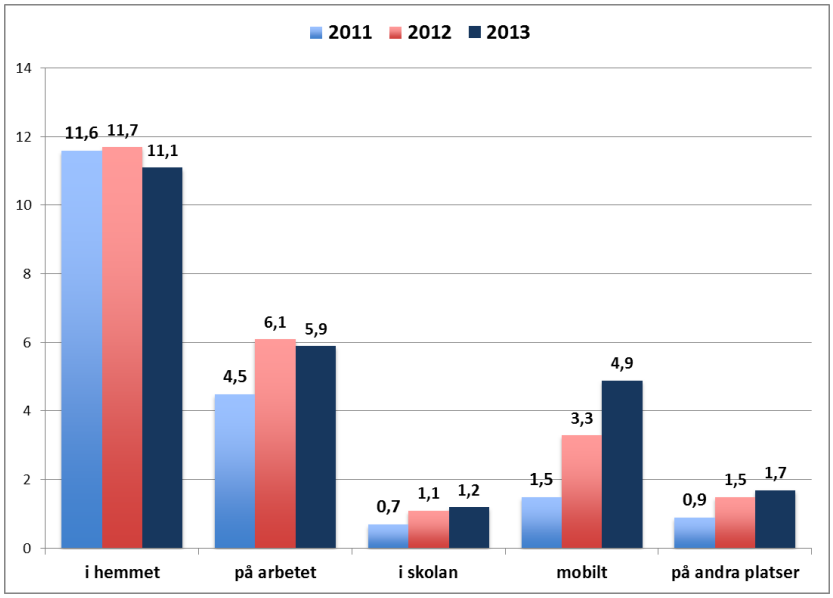
En smartphone innehåller en mängd olika typer av information. Information som bland annat kan finnas på telefonen är SMS, MMS, bilder, datafiler, e-post, kontaktuppgifter, samtalsloggar, uppgifter om vem som är operatör och telefonens ID-nummer.[63] Uppgifterna som finns i telefonen kan lagras på olika sätt. De kan lagras på telefonen, på telefonens SIM-kort eller på servrar. SIM-kortet är kopplat till abonnemanget vilket innebär att det inte finns någon direkt koppling mellan själva telefonen och abonnemanget. En mobiltelefon kan ha mer än ett SIM-kort eftersom dessa kan flyttas mellan

[57] SOU 2001:28 s. 137, 149.
[58] SOU 2001:28 s. 131.
[59] Kronqvist 2012 s. 29.
[60] SOU 2001:28 s. 131-132.
[61] *Svenskarna och internet* 2013 s. 14.
[62] Kronqvist, 2012 s. 25-26.
[63] Beslag: en handbok, 2013 s. 31.

telefoner.[64] Ofta är röstbrevlådor och e-postbrevlådor lagrade på olika servrar. Servrarna kan antingen finns i Sverige eller utomlands.[65]

För inte så länge sedan skedde uppkopplingen till internet med hjälp av datorer genom fasta uppkopplingar eller via olika nätverk. Idag kan internet nås nästan överallt, i hemmet, på arbetsplatsen eller på bussen. Allt som behövs är en mobiltelefon och tillgång till ett mobilt internet.[66] Tillgång till ett mobilt internet fås genom att användaren kopplar upp sig till ett trådlöst nätverk, exempelvis WiFi eller 3G/4G-nät.[67] Detta har lett till att den mobila internetanvändningen har ökat markant till skillnad från övrig internet-användning, se diagram 1.

Diagram 1: Svenskarnas internetanvändning över tid

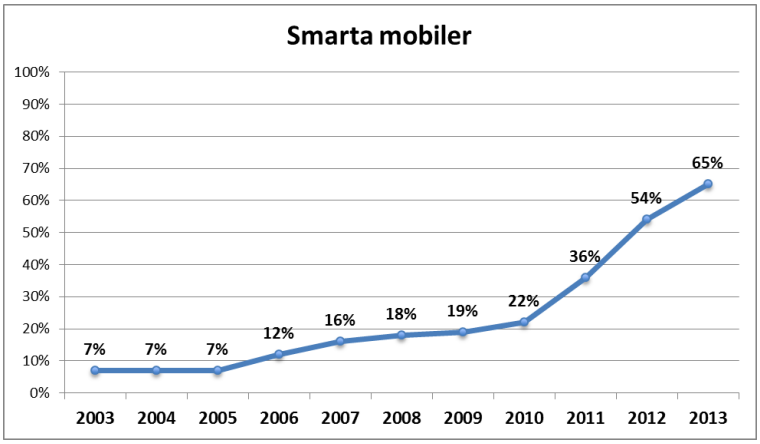


Källa: *Svenskarna och internet 2013*

I diagramet visas hur många timmar per vecka en genomsnittlig svensk internetanvändare surfar mobilt. Varje svensk internetanvändare nyttjade mobilt internet 5 timmar i veckan 2013 jämfört med 2011 då motsvarande tid var 1,5 timme. Enligt Stiftelsen för Internetinfrastruktur beror ökningen till stor del på att smartphone kan användas för internetsurf. Diagram 2 påvisar antalet svenskar som innehar och använder smartphone.

[64] Lindberg, 2012 s. 429.
[65] Beslag: en handbok, 2013 s. 36.
[66] *Svenskarna och internet* 2013 s. 10, 25.
[67] Kronqvist, 2012 s. 25.

Diagram 2: Andelen svenskar som använder smartphone över tid



Källa: *Svenskarna och internet 2013*

Sedan 2002 har det varit möjligt att koppla upp sig till internet i telefonen. Trots det blev det inte populärt med internet i telefonen förrän 2011 och 2013 hade 65% av den svenska befolkningen en smartphone som kunde användas för att surfa på internet. Anledningen till ökningen av internet-användning i smartphone är den förbättrade tekniken och mer skäliga mobilsurfsavgifter.[68]

3.3 Teknik, brottsbekämpning och integritet

Brottsligheten har förändrats i takt med den tekniska utvecklingen. Brottslingar brukar tekniska hjälpmedel eller utnyttjar samhällets tekniska begränsningar i sin brottsliga verksamhet.[69] Används exempelvis anonyma kontantkort i mobiltelefoner kan inte brottsbekämpande myndigheter fastslå vem som äger eller nyttjar telefonen.[70] En ny sorts bevis har även uppstått till följd av utvecklingen, nämligen elektronisk bevisning. Med detta avses information eller data som lagras i eller förmedlas av en elektronisk enhet.[71] Bevissäkring är också ett område som har påverkats. Bevis kan exempelvis lagras utomlands i elektronisk form trots att brottet begåtts i Sverige.[72]

Brottsbekämpande myndigheter måste anpassa sina utredningsmetoder för att bekämpa den förändrade brottsligheten.[73] Detta har varit ett argument för

[68] *Svenskarna och internet* 2013 s. 14.
[69] Eriksson, 2007 s. 130-131.
[70] SOU 2005:38 s. 26.
[71] Kronqvist, 2012 s. 19.
[72] Lindberg, Gunnel ”Straffprocessuella tvångsmedel – några utvecklingslinjer”, *Svensk Juristtidning*, 2007 s. 51.
[73] Eriksson, 2007 s. 130-131.

en ökad tvångsmedelsanvändning. Så länge lagstiftningen inte tar hänsyn till teknisk utveckling riskerar brottsbekämpningen att vara ineffektiv.[74] Ur effektivitetssynpunkt är det därmed relevant att bruka tvångsmedel i varje brottsutredning.[75]

Teknikutvecklingen har också resulterat i ökade möjligheter till integritetsintrång och ökade möjligheter att göra grova sådana. Detta beror på att det blivit lättare att kartlägga och övervaka individer i och med den nya tekniken. Digitala lagringsutrymmen gör det nämligen möjligt att lagra obegränsade mängder information om individer och därmed är det enkelt att söka och sammanställa information om specifika individer. Tidigare har det varit svårt att sammanställa information om individer eftersom den funnits utspridd i olika manuella arkiv.[76]

Individers internetanvändning har också resulterat i en ökad möjlighet att övervaka individer. Detta beror på att individer delar personlig information på internet.[77] I tabell 1 påvisas svenskars privata internetvanor.

Tabell 1: Svenskarnas internetanvändning

Saker man själv gör	**någon gång**	**dagligen**
köpa/betala varor/tjänster	84%	0%
köpa/boka resor	71%	0%
betala räkningar	79%	1%
skriva blogg	7%	1%
Fildelning	24%	2%
söka jobb	30%	3%
lägga upp foton	65%	4%
Statusuppdatera	46%	4%
logga in på bank	84%	6%
se på video	46%	7%
läsa bloggar	41%	9%
telefon över internet	41%	9%
kommentera andra	52%	9%
besöka intressecommunity	46%	17%
ladda ner/lyssna på musik	62%	26%
Spel	55%	26%
skriva e-post	92%	42%
besöka socialt nätverk	69%	44%
läsa e-post	96%	73%

Källa: *Svenskarna och internet 2013*

[74] Träskman, Per Ole; ”Brottsligheten och dess bekämpande – en reflektion om hot och hotbilder”, *Svensk Juristtidning*, 2007 s. 117-118.
[75] Ramberg, 2007 s. 155.
[76] Strömholm, 1971 s 709-710.
[77] Abrahamsson, 2009 s. 424.

Många svenskar besöker sociala nätverk, uppdaterar status om privata angelägenheter och lägger upp digitala foton. Av alla internetanvändare över 12 år besöker 44% sociala nätverk dagligen, se tabell 1. En stor del av dem som besöker sociala nätverk och lägger upp bilder gör detta med smartphone, se tabell 2.[78]

Tabell 2: Användningsområden för smartphone

Mobil		
	Någon gång	Dagligen
e-post	88%	71%
socialt nätverk	84%	67%
Webbnyheter	87%	45%
lyssna på musik	70%	38%
tidtabeller m m	92%	34%
Spel	66%	31%
söka fakta	75%	26%
Hobby	79%	21%
lägga upp foton	69%	6%

Källa: *Svenskarna och internet 2013*

Tabellen visar i vilken omfattning svenskar använder olika tjänster på internet via smartphone i sin vardag. Det är främst e-post och socialt nätverk som dominerar den dagliga användningen.

Ett argument för en ökad användning av tvångsmedel är att människor i och med det ökade publika delandet av privat information på internet accepterat en ökad övervakning. Det är dock värt att skilja på frivilligt upplåtande av personlig information och att tvångsvis få sitt liv kartlagt och övervakat. Den enskilde har bestämmanderätt över sina personliga förhållanden och är den som bestämmer vilken personlig information som sprids på internet. Vid en statlig övervakning har den enskilde däremot ingen påverkan på vilken information som övervakas.[79]

3.4 Teknik och lagstiftning

Frågan om huruvida beslagstiftningen ska vara teknikneutral eller teknikanpassad har till stor del vuxit fram på grund av att den nuvarande regleringen skiljer på olika kommunikationssätt.[80] Generella utgångspunkter är att lagstiftningen ska vara hållbar under en längre tid samt att lag-

[78] *Svenskarna och internet* 2013 s. 21, 35, 37.
[79] Abrahamsson, 2009 s. 424.
[80] Ds 2005:6 s. 277.

stiftningen ska förhindra att allmänheten ifrågasätter effektiviteten av brottsbekämpningen och rättssäkerheten på grund av en otydlig reglering.[81]

En lag kan antingen vara teknikneutral eller teknikanpassad. Den teknikneutrala lagstiftningen tar inte hänsyn till tekniska konstruktioner eller yttre omständigheter vilket den teknikanpassade lagstiftningen gör. Fördelen med en teknikneutral lagstiftning är att den inte behöver ändras i takt med tekniska framsteg. Dock riskerar regleringen att bli oanvändbar på grund av teknisk utveckling och oförutsebar då tvångsmedels tillämpningsområde expanderar för att anpassas till den tekniska utvecklingen.[82] Dessa problem fås inte om lagstiftningen är teknikbaserad. En teknikbaserad lagstiftning måste däremot anpassas till utvecklingen inom IT-området och därmed vara i behov av ständiga förändringar i och med den snabba utvecklingen.[83]

Utöver detta finns andra aspekter som ska beaktas vid lagstiftning av teknisk art. Lagstiftaren behöver bland annat avgöra vilken teknikanvändning som ska regleras och vilken som inte bör regleras. Dessutom ska lagstiftningens utformning motiveras utifrån både ett brottsbekämpande perspektiv och ett integritetsperspektiv. Ur ett integritetsperspektiv har det framhävts att det är bättre att reglera tekniska arbetsmetoder än att låta brottsbekämpande myndigheter utnyttja tekniken efter egen subjektiv bedömning. I lagstiftningsprocessen behöver det även utredas hur olika tvångsmedel ska få kombineras. En kombination av tvångsmedel kan nämligen resultera i ett grövre integritetsintrång eftersom brottsbekämpande myndigheter då kan få en mer heltäckande bild av enskilda personers privata förhållanden.[84]

[81] SOU 2005:38 s. 19.
[82] Lindberg, 2007 s. 55.
[83] SOU 2005:38 s. 19.
[84] Lindberg, 2007 s. 55-56.

4 Beslag

RB definierar inte vad ett tvångsmedel är. En vanlig definition av begreppet är myndighetsutövning som innebär intrång i någons personliga sfär. Den enskilde individen ska dessutom få synbara eller kännbara verkningar av ingreppet.[85] Ett tvångsmedel kan vara personellt eller reellt, momentant eller perdurerande, öppet eller hemligt. Personella tvångsmedel riktar sig mot personer och reella tvångsmedel riktar sig mot egendom. Momentana tvångsmedel innefattar ingrepp som pågår under en kort tidsperiod medan perdurerande tvångsmedel innebär att ingreppet pågår under en längre tid.[86] Hemlig tvångsmedelsanvändning innebär att ingreppet sker mot den berördes vilja och utan att den berörde är medveten om ingreppet. Är något av dessa kriterier inte uppfyllt anses tvångsmedlet var öppet.[87]

Beslag är ett reellt och perdurerande tvångsmedel då det riktas mot föremål och då det beslagtagna föremålet förvaras under en längre tid innan beslaget upphör. Vidare är beslag ett öppet tvångsmedel då den berörde informeras om åtgärden. Härnäst ges en kort redogörelse för vilka principer som ska beaktas när brottsbekämpande myndigheter gör beslag och vilka förutsättningar som krävs för att beslagsanvändning ska bli aktuellt.

4.1 Grundläggande principer

Vid ett beslag ska beslutsfattaren i varje enskilt fall beakta rättssäkerhet samt ta hänsyn till avvägning mellan effektiv brottsbekämpning och personlig integritet. Legalitets-, ändamåls-, behovs- och proportionalitetsprinciperna får betydelse vid bedömningen. Tvångsmedelsutövning inskränker den personliga integriteten men eftersom det är accepterat att utreda brott i ett demokratiskt samhälle får den personliga integriteten begränsas till förmån för tvångsmedelsanvändning. Legalitetsprincipen uppställer krav på att begränsningen ska framgå av lag eller annan författning. Utan ett lagstiftat undantag är det inte tillåtet att vidta åtgärder som leder till intrång i den enskildes personliga sfär. Eftersom legalitetsprincipen ska tolkas strikt ska det av lagens ordalydelse framgå i vilka situationer tvångsmedel kan tillämpas. Ett ingrepp i en persons integritet som sker till följd av en extensiv eller analogisk tolkning av en rättsregel torde inte vara tillåtet. Vidare berättigar ändamålsprincipen endast ett brukande av tvångsmedel om åtgärden vidtas för att uppfylla tvångsmedlets syfte.[88] Syftet med beslag är att säkra föremål som kan ha betydelse för utredning om brott, säkra föremål som någon avhänts genom brott,

[85] SOU 1995:47 s. 137-138.
[86] Lindberg, 2012 s. 6.
[87] SOU 2014:44 s. 22.
[88] Lindberg, 2012 s. 5, 9, 20-22.

säkerställa verkställighet av förverkandebeslag och säkra utredning angående förverkande av utbyte av brottslig verksamhet. Någon av dessa fyra beslagsgrunderna ska således vara tillämplig vid ett beslag.[89]

Om legalitets- och ändamålsprinciperna är uppfyllda är utgångspunkten att tvångsmedel får brukas om behovet och nyttan som fås genom åtgärden överväger integritetsintrånget.[90] Bedömningen är en framtidsprognos och görs utifrån behovs- och proportionalitetsprinciperna. Enligt behovsprincipen ska det finnas ett påtagligt behov av tvångsmedlet. Dessutom ska det förväntade resultatet inte kunna uppnås med ett mindre ingripande medel. Tvångsmedelsanvändningen ska upphöra när det avsedda resultatet uppnåtts eller när det är klart att resultatet inte kommer att kunna nås.[91] För att avgöra om det finns ett påtagligt behov ska hänsyn tas till vilken information som behövs, om det går att införskaffa informationen på något annat sätt och vilka möjligheter det går att erhålla informationen med hjälp av tvångsmedlet.[92] Enligt proportionalitetsprincipen ska skälen som motiverar ingreppet uppväga intrånget eller det men som ingreppet innebär. Faktorer som påverkar den här bedömningen är arten, styrkan, räckvidden och varaktigheten av ingripandet. Om dessa faktorer står i proportion till målet är åtgärden tillåten.[93]

4.2 Grundläggande förutsättningar

Vid ett beslag tar en myndighet hand om någons egendom. Det sker då en tillfällig besittningsrubbning eftersom ägaren inte längre förfogar över föremålet. Detta i sin tur innebär att ägarens rätt till egendomen begränsas. All lös egendom som har en fysisk form kan beslagtas. Skriftliga handlingar kan beslagtas både avseende handlingen och avseende innehållet i handlingen. I 27 kap. 2 § RB finns ett beslagsförbud som förhindrar beslag av vissa skriftliga handlingar. (Detta behandlas mer ingående i avsnitt 5.3.1.) Fast egendom och immateriella föremål kan inte beslagtas. Anledningen till att immateriella föremål, exempelvis bankkonton, inte kan beslagtas är att egendom som beslagtas måste ha fysisk form. Bankkonton är endast bärare av en fordringsrätt. Det är omdiskuterat ifall elektronisk information som inte lagrats på någon fysisk enhet kan beslagtas.[94] Elektronisk information anses dock kunna beslagtas om den finns lagrad på en elektronisk bärare så som exempelvis en mobiltelefon. Då beslagtas föremålet i sig vilket leder till att beslagsreglerna kan tillämpas på den elektroniska information som finns lagrad i föremålet.[95]

[89] 27 kap. 1 § RB.
[90] SOU 2012:44 s. 21-22.
[91] Bring, Diesen, 2009 s. 276.
[92] SOU 2012:44 s. 171.
[93] Bring, Diesen, 2009 s. 276.
[94] Lindberg, 2012 s. 383, 401, 404.
[95] SOU 2013:39 s. 134.

Det huvudsakliga syftet med beslag är att säkra bevisning och säkerställa verkställighet av en brottmålsdom. Tvångsmedlet tillämpas främst i förundersökningar och anses vara ett av de vanligaste tvångsmedlen på grund av att beslagsgrunderna ger det ett brett tillämpningsområde. Beslag används ofta i kombination med andra tvångsmedel, så som husrannsakan och kroppsbesiktning.[96] Detta beror på att föremål enbart får beslagtas om de är tillgängliga. Då det inte är tillåtet att söka efter ett specifikt föremål med ett beslagbeslut kan brottsbekämpande myndigheter genom husrannsakan eller kroppsvisitation finna föremål de vill beslagta. Kravet på tillgänglighet uppställs för att skydda den enskildes integritet och motverka att brottsbekämpande myndigheter söker efter vissa specifika föremål.[97]

För att göra ett beslag ska det finnas skäl att tro att ett brott begåtts och det ska finnas ett samband mellan beslagsgrunderna och utredningen avseende brottet.[98] Beviskravet, ”skäligen kunna antas”, måste vara uppfyllt för att beslag ska få tillämpas. Detta anses vara uppfyllt om konkreta omständigheter av viss styrka talar för att föremålet ska ha betydelse för utredningen. Det uppställs inga villkor på att den som utsätts för beslaget ska vara misstänkt för det brott som utreds vilket innebär att beslag kan riktas mot vem som helst, exempelvis vittnen, målsäganden och andra personer.[99]

[96] Lindberg, 2012 s. 383, 385.
[97] Hjertstedt, 2011 s. 206-207.
[98] Lindberg, 2012 s. 399.
[99] SOU 1995:47 s. 357-358.

5 Mobiltelefoner och elektronisk information

Beslag av mobiltelefoner blir allt vanligare eftersom de innehåller elektronisk information vilket under de senaste åren har fått stor betydelse som bevis i brottmål. Därmed riktas beslaget sällan mot telefonen i sig utan snarare mot informationen i den. Vid ett beslag får brottsbekämpande myndigheter ta del av den informationen som finns vid beslagstillfället. Eftersom mobiltelefonens innehåll kontinuerligt uppdateras måste telefonen isoleras så att den beslagtagna informationen inte förändras.[100] Det faktum att information kan lagras på olika sätt i en mobiltelefon och att informationen ständigt förändras leder till att det uppstår flera svårigheter vid beslag av mobiltelefoner innehållande elektronisk information.

Det har ifrågasatts om beslag och andra traditionella tvångsmedel är effektiva för inhämtning av bevis i elektronisk form och därmed om värdet av den traditionella tvångsmedelsregleringen minskar i takt med teknisk utveckling. Är inte beslagslagstiftningen anpassad till teknisk utveckling finns risk för att beslagslagstiftningens bestämmelser och integritetsskydd endast blir tillämpliga på vissa kommunikationssätt så som skriftliga handlingar. Andra kommunikationssätt så som e-post, SMS och MMS riskerar således inte omfattas av beslagslagstiftningens integritetsskydd.[101]

I det följande görs en genomgång av beslagundersökningen och dess problematik vid beslag av mobiltelefoner. Därefter redogörs det för hur brottsbekämpande myndigheter hanterar meddelanden som inkommer efter beslagstillfället och vilket integritetsskydd den enskilde har vid beslag av mobiltelefoner. Eventuella lagstiftningsåtgärder som föreslagits i syfte att klargöra eller förändra rättslaget behandlas i samband med gällande rätt.

5.1 Beslagsundersökningen

En informationsbärare får vid en husrannsakan eller kroppsbesiktning undersökas men då digitala informationsbärare innehåller stora mängder information brukar detta inte ske. Istället beslagtas informationsbäraren, exempelvis mobiltelefonen eller datorn.[102] Efter att mobiltelefonen beslagtagits undersöks den genom tömning.[103] När brottsbekämpande myndigheter beslagtar datorer undersöks de oftast genom spegling vilket innebär att en exakt kopia av hårddisken upprättas med hjälp av en programvara. Speglingsförfarandet används för att minska integritetsintrång och underlätta den

[100] Kronqvist, 2012 s. 25-26, 115-116.
[101] Ds 2005:6 s. 202, 279-280.
[102] SOU 2013:39 s. 152.
[103] Beslag: en handbok, 2013 s. 32.

praktiska undersökningen av stora datamängder.[104] Tömningsförfarandet är snarlikt speglingsförfarandet eftersom även detta förfarande innebär att innehållet kopieras. Detta görs för att informationen vid beslagstillfället inte ska manipuleras. Information kan annars fjärraderas eller tillföras telefonen. Det är även av denna anledning som telefonen stängs av eller försätts i flygplansläge vid beslagstillfället. Materialet, som fås vid tömningen, genomsöks utifrån valda sökord. Sökorden kan bestå av telefonnummer, ord eller bilder. Undersökningen kan ske med successiv relevans vilket innebär att sökningar kan ske i flera omgångar och utifrån olika sökord. Detta beror på att information som inte var relevant från början kan få betydelse i ett senare skede av brottsutredningen.[105] Att undersöka en mobiltelefon är inte en rutinåtgärd eftersom det är oerhört resurs- och tidskrävande.[106] Nedan redogörs för kopieringsförfarandet samt vilken information som finns i en mobiltelefon och som kan avläsas i samband med en beslagsundersökning av en mobiltelefon.

5.1.1 Kopiering

Kopieringsförfarandet uppstod till följd av att de som drabbats av beslag i vissa situationer, exempelvis beslag gällande bokföringshandlingar, behövde tillgång till det beslagtagna föremålet. Om brottsbekämpande myndigheter endast är ute efter innehållet i det beslagtagna föremålet räcker det att de har en kopia av detta föremål. Till följd av den tekniska utvecklingen ökade behovet av kopiering och därmed frågan om huruvida kopieringsförfarandet bör tillåtas eller inte.[107] Forskningen om kopiering är generell men har i praktisken främst diskuterats och tillämpats på beslag av datorer. Denna forskning borde kunna tillämpas på beslag av mobil-telefoner. I det följande redogörs för kopiering och dess problematik vid beslag av mobiltelefoner.

5.1.1.1 Nuvarande rättsläge

Sverige har implementerat Europarådets konvention om IT-relaterad brottslighet. I konventionen stadgas att brottsbekämpande myndigheter ska ha rätt att upprätta och behålla kopior av databehandlingsbara uppgifter som säkras genom husrannsakan, beslag eller annat liknande förhållande.[108] Därmed har Sverige en skyldighet att tillåta kopiering av elektronisk information vid beslag av mobiltelefoner. Trots detta finns ingen lagregel

[104] SOU 2011:45 s. 24, 296
[105] Tibbling, 2014-04-28.
[106] Beslag: en handbok, 2013 s. 32.
[107] Lindberg, 2012 s. 442.
[108] Artikel 19 p. 3 Europarådets konvention om IT-relaterad brottslighet.

som uttryckligen stadgar att det är tillåtet att kopiera beslagtagen egendom.[109]

HD har uttalat att förfarandet med kopiering inte är förenligt med rätten till domstolsprövning. För att den drabbade ska få tillbaka det beslagtagna föremålet måste beslagsbeslutet upphävas. Därmed ersätts beslaget av kopior vilket gör att den drabbade i framtiden inte kan få en rättslig prövning av beslaget. Kopiorna som ersätter beslaget anses inte heller vara beslagtagen egendom.[110] Den drabbade riskerar således att få ett sämre rättsligt skydd om informationen på beslagsföremålet kopieras och beslagsbeslutet upphävs.[111]

JO och JK har i flera ärenden behandlat frågan om kopiering rörande beslag av datorer som innehåller elektronisk information. Båda önskar att reglerna på området klargörs.[112] Enligt JK sker ett stort integritetsintrång när elektroniska enheter, exempelvis datorer, beslagtas. Vid den här sortens beslag ska brottsbekämpande myndigheter överväga om syftet med beslaget kan nås genom en mindre ingripande åtgärd, så som kopiering.[113] Även JO anser att det är mer ingripande att beslagta hela enheter än att kopiera handlingar och elektronisk information.[114] Lindberg och Hjertstedt anser dock att kopiering generellt sett inte ska ersätta beslag eftersom den drabbades rättssäkerhet åsidosätts vid ett sådant förfarande. Om brottsbekämpande myndigheter ska kopiera egendom ska den vid kopieringstillfället vara beslagtagen.[115]

Enligt Åklagarmyndighetens och Ekobrottmyndigheten riktlinjer ska beslag i allmänhet inte ersättas med kopior av det beslagtagna. Detta beror på att rättssäkerhetsgarantierna vid beslag sätts ur spel. Om innehållet i det beslagtagna föremålet ska kopieras krävs som huvudregel att den enskilde individen önskar detta och att det är rimligt med hänsyn till proportionalitetsprincipen. Kopior får dock upprättas om syftet är att ha dem som arbetsmaterial. Vid beslag av mobiltelefoner görs alltid en kopia av innehållet. Därmed kan mobiltelefonen återlämnas så länge omständigheterna i det enskilda fallet talar för detta och det inte rör sig om grov brottslighet. Fördelen med att låta beslaget bestå är att brottsbekämpande myndigheter kan möta invändningar angående bevisningen och undersöka mobiltelefonen på nytt.[116]

Lindberg anser att de argument som motiverar kopiering är att beslag kan hävas snabbare vilket minskar integritetsintrång och det faktum att brottsbekämpande myndigheters arbete med det beslagtagna materialet förenklas eftersom originalhandlingar varken slits eller förstörs. Dessutom går det i

[109] Ds 2006:5 s. 305, 307.
[110] NJA 1988 s. 471.
[111] Ds 2006:5 s. 307.
[112] Se t.ex. JO 2007/08 s. 160, JK dnr 3954-99-40, JK dnr 2806-00-21.
[113] JK dnr 3954-99-40, JK dnr 2806-00-21.
[114] 2007/2008:JO1 s. 166.
[115] Hjertstedt, 2011 s. 259, Lindberg, 2012 s. 390.
[116] Beslag: en handbok, 2013 s. 37-38.

efterhand att klarlägga vad beslaget har omfattat.[117] Ytterligare en fördel med kopieringsförfarandet är att elektronisk information som kopieras inte kan förändras. Med kopiering kan brottsbekämpande myndigheter bevara informationen som den var vid en viss tidpunkt.[118]

De argument som talar mot kopiering är att det inte finns några begränsningar om hur kopiorna ska brukas och hur de ska hanteras när beslaget hävts. Därmed är det inte kopieringen i sig som är problematisk.[119] Det är exempelvis svårt att rättsligt pröva beslaget när kopiering brukas. Inte heller kan beslagslagstiftningen tillämpas på kopierat material och det finns risk för att information som fås vid beslaget sprids mer än nödvändigt om kopior upprättas. Eftersom kopior av beslagtaget material finns efter att beslaget hävts får inte heller detta avsedd effekt.[120]

5.1.1.2 Lagstiftningsåtgärder

Förfarandet kring kopiering av beslagtagen egendom har diskuterats i flera statliga utredningar. Utredningarna har främst berört det rättsliga skyddet för den enskilde individen och en eventuell lagreglering avseende förfarandet med kopiering.[121] Enligt Tvångsmedelskommittén får den drabbade ett sämre integritetsskydd om det beslagtagna materialet kopieras istället för om materialet enbart beslagtas. För att skydda den drabbade ska denne rättsligt kunna pröva beslagsbeslutet trots att beslaget hävts. En prövning ska tillåtas om uppgifter som härstammar från beslaget påträffas hos den myndighet som gjort beslaget eller om denna myndighet överlämnat uppgifterna till en annan myndighet.[122]

Polisrättsutredningen menar att kopieringsförfarandet inte är förenligt med rätten att begära domstolsprövning av beslag. Syftet med den rättsliga prövningen är att återföra beslagsföremålet till den som drabbats av beslaget. Om föremålet redan återställts är prövningen verkningslös då domstolen inte har rätt att förhindra brottsbekämpande myndigheter från att använda uppgifterna som påträffats i samband med beslaget. Detta följder av principen om fri bevisföring.[123]

I promemorian om *Brott och brottsutredning i IT-miljö* konstateras att det inte behöver införas några regler om kopiering. Det räcker med att det i Europarådets konvention om IT-relaterad brottslighet framgår att kopiering är tillåtet. Kopieringsförfarandet behöver inte begränsas på grund av att det inte går att begära domstolsprövning när information kopieras. Det som motiverar kopieringsförfarandet är att det är viktigt att frysa situationen vid

[117] Lindberg, 2012 s. 443.
[118] Ds 2005:6 s. 314.
[119] Ds 2005:6 s. 314.
[120] Lindberg, 2012 s. 443.
[121] Se t.ex. SOU 1984:54, SOU 1995:47, Ds 2005:6, SOU 2011:45.
[122] SOU 1984:54 s, 209.
[123] SOU 1995:47 s. 197-198.

beslag av elektronisk information. Detta görs för att det inte ska gå att förändra informationen som fås vid beslagstillfället. Det påpekas också att kopieringsförfarandet bör ses över i ett vidare perspektiv.[124]

Enligt Förundersökningsutredningen ger kopieringsförfarandet många fördelar ur effektivitets-, utrednings- och rättssäkerhetshänseende. Att inte tillåta kopiering av databehandlingsbara uppgifter strider mot Sveriges åtagande i Europarådets konvention om IT-relaterad brottslighet. Däremot är det inte rättssäkert att brottsbekämpande arbetsmetoder i tvångsmedelssammanhang är oreglerade. Legalitetsprincipen talar också för en lagreglering av kopieringsförfarandet. Således ska det i lag framgå att brottsbekämpande myndigheter får kopiera egendom vid beslag. Eftersom kopiering är en del av verkställigheten vid ett beslag ska det användas när brottsbekämpande myndigheter bedömer att kopiering kan innebära en fördel för brottsutredningen eller den enskilde. Hade det krävts samtycke av den enskilde skulle tillämpningsområdet för kopieringsförfarandet bli för snävt. Regleringen som utredningen förespråkar överensstämmer med den praxis som finns på området. En rättslig prövning av beslaget efter att beslagtagen egendom kopierats ska inte införas då det inte är förenligt med principen om fri bevisföring. Domstolen kan nämligen inte förhindra brottsbekämpande myndigheter från att använda bevisning som samlats in på ett felaktigt sätt.[125]

Enligt utredningen om it-brottskonventionen uppfyller svensk rätt artikel 19 p. 3 i Europeiska konventionen om IT-relaterad brottslighet. Detta beror på att det inte finns några egentliga invändningar mot förfarandet och att förfarandet är vanlig förekommande. Själva kopieringsförfarandet behöver inte kodifieras för att överensstämma med de svenska åtagandena.[126]

Hjertstedt menar att kopiering inte ska tillåtas eftersom den enskildes rättssäkerhetsgarantier åsidosätts. Om kopiering ska tillåtas i svensk rätt ska brottsbekämpande myndigheter behålla originalen och återlämna kopior. På så sätt kvarstår den enskildes rättssäkerhetsgaranti och denne kan överklaga beslagsbeslutet.[127]

5.1.2 Information i mobiltelefoner

All information i mobiltelefoner kan vara relevant i brottsutredningar. Viss information får betydelse i sin direkta form, exempelvis SMS och MMS, medan annan information, så som telefonens ID-nummer och operatörsuppgifterna, behövs för det fortsatta utredningsarbetet. Med hjälp av telefonens ID-nummer kan brottsbekämpade myndigheter begära ut telefonlistor som visar in- och utgående samtal, omkopplade samtal,

[124] Ds 2005:6 s. 305, 314-315.
[125] SOU 2011:45 s. 333-337, 339-341.
[126] SOU 2013:39 s. 153, 156.
[127] Hjertstedt, 2011 s. 249.

samtalslängd och om samtal besvarades. Operatörsuppgifter kan nyttjas för att ta reda på vem som är abonnent.[128]

Vid en beslagsundersökning är det tillåtet att läsa av samtalsloggar och textmeddelanden som finns lagrade i mobiltelefoner eller på SIM-kort. Detta beror på att telefonsvarare som beslagtas får undersökas på likartad information, exempelvis inspelade telefonmeddelanden. Brottsbekämpande myndigheter får även tillgång till kontaktuppgifter i telefonböcker eftersom handskrivna telefonböcker får undersökas. Däremot är det inte tillåtet att direkt ta del av meddelanden och uppgifter om telefonsamtal som inkommer efter beslagstillfället.[129] (Hur meddelanden och uppgifter som inkommer efter beslagstillfället ska hanteras redogörs för mer ingående i avsnitt 5.2.) Inte heller får brottsbekämpande myndigheter ringa upp teleoperatören för att avlyssna röstbrevlådor. Röstbrevlådor, liksom e-postbrevlådor finns nämligen inte lagrade på telefonen.[130]

E-postbrevlådor kan lagras på servrar i Sverige eller utomlands. Det är sällan mobiltelefoner innehåller information som lagras på en server utomlands men det är desto vanligare att sådan information lagras på datorer. När mobiltelefoner har information som lagras på en server rör det sig oftast om e-postbrevlådor. Problematiken med att information lagras på servrar är att det ofta är svårt att fastslå var någonstans servern finns.[131]

Lagras e-postbrevlådor på servrar utomlands krävs tillstånd från en domstol eller en myndighet i det landet för att brottsbekämpande myndigheter ska få tillgång till informationen i e-postbrevlådan.[132] Det anses inte vara tillåtet att tömma en server som finns utomlands med hjälp av ett verktyg som finns tillgängligt i Sverige. Således måste brottsbekämpande myndigheter begära internationell rättslig hjälp som grundas på konventioner eller avtal för att få ta del av innehållet i brevlådan.[133]

I Sverige kan e-postbrevlådor antingen lagras privat eller hos en teleoperatör eller en leverantör av allmänt tillgängliga elektroniska kommunikations-tjänster eller allmänna kommunikationsnät.[134] Finns brevlådorna lagrade hos någon av dessa aktörer stadgar LEK att de ska lagra trafikuppgifter så som SMS och e-post i minst sex månader.[135] Av de lagrade uppgifterna ska det framgå vem användaren kommunicerat med, hur kommunikationen skett, varifrån kommunikationen skett och längden på kommunikationen. Därmed kan brottsbekämpande myndigheter ta reda på om användaren upprepat kommunicerat med en viss person. Innehållet i kommunikationen får dock inte avläsas.[136] Den information som lagras får i vissa fall användas i

[128] Beslag: en handbok, 2013 s. 31.
[129] Lindberg, 2012 s. 429.
[130] Beslag: en handbok, 2013 s. 36.
[131] Tibbling, 2014-04-28.
[132] Beslag: en handbok, 2013 s. 36.
[133] Tibbling, 2014-04-28.
[134] SOU 2005:38 s. 120, 126.
[135] 6 kap 16a, 16d §§ LEK.
[136] Prop. 2010/11:46 s. 1.

brottsutredningar. Brottsbekämpande myndigheter kan inte inhämta uppgifterna med editionsföreläggande eller husrannsakan i förening med beslag.[137] Om detta vore tillåtet skulle LEK och reglerna om hemlig tvångsmedelsanvändning sakna betydelse.[138] Istället ska brottsbekämpande myndigheter ansöka om tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation för att få tillgång till informationen.[139] Hemlig avlyssning av elektronisk kommunikation innebär att brottsbekämpande myndigheter får ta del av innehållet i meddelandet antingen i realtid eller i förfluten tid.[140] Hemlig övervakning av elektronisk kommunikation innebär att brottsbekämpande myndigheter får ta del av uppgifter om meddelandet, bland annat när meddelandet skickats och om meddelandet kommit fram.[141]

Allt fler privata företag säljer servertjänster, så som lagringsutrymme på servrar. De här företagen omfattas inte av LEK. För att kunna ta del av informationen i dessa servrar behöver brottsbekämpande myndigheter göra en husrannsakan i företagens serverrum och därefter beslagta den relevanta servern. Företagens affärsidé är att lagra information åt kunder och därmed låta kunderna vara anonyma. Detta leder till att företagen inte vill lämna ut uppgifter om lösenord, åtkomstkoder eller vilken server som innehåller den relevanta informationen. Då företagen innehar flera servrar blir traditionella tvångsmedel ineffektiva. Det går inte ur resurssynpunkt att genomsöka alla servrar på plats vid en husrannsakan och troligtvis skulle proportionalitets-principen förhindra ett beslag av samtliga servrar. Uppgifter riskerar således att ändras eller förstöras innan de hinner bevissäkras. Ur ett brotts-bekämpande perspektiv vore det positivt att införa ett föreläggande där företag tvingas lämna ut viss information för att underlätta husrannsakan, beslag och i förlängningen även bevissäkring.[142]

Den 8 april 2014 underkände EU-domstolen Datalagringsdirektivet 2006/24/EG som till viss del implementerats i LEK. Även om trafik-uppgifter lagrades i syfte att hjälpa nationella myndigheter att värna om allmän säkerhet utgör direktivet ett synnerligt allvarligt intrång i rätten till privatliv. Ingreppet ansågs vara allvarligt då uppgifterna kunde ge exakta upplysningar om en persons vardagsliv, stadigvarande och tillfälliga vistelseorter, aktiviteter, sociala relationer och umgängeskretsar samt att lagringen också kunde ge den enskilde individen en känsla av att denne står under konstant bevakning. Dessutom fanns en risk för att uppgifterna kunde missbrukas då det inte fanns något effektivt skydd mot att uppgifterna användes för andra ändamål än att förebygga, avslöja eller väcka åtal för brott. Datalagringsdirektivet har inte i tillräcklig utsträckning beaktat proportionalitetsprincipen.[143] Polisen tror att det kommer att bli svårare att utreda brott i och med ogiltigförklarandet av direktivet. Detta beror på att

[137] SOU 2005:38 s. 120, 126.
[138] Prop 2002/03:74 s. 45.
[139] 6 kap. 22 §§ LEK.
[140] 27 kap. 18 § RB.
[141] 27 kap. 19 § RB.
[142] SOU 2013:39 s. 160-161.
[143] EU-domstolens mål C-293/12 och C594/12 Digital Rights Ireland Ltd mot Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl.

polisens tillgång till data och personuppgifter minskar. Direktivet har redan införlivats i svensk rätt och det är ännu oklart hur den svenska regleringen kommer att förändras till följd av domen.[144] Flera teleoperatörer har valt att sluta lagra trafikuppgifter trots att detta strider mot gällande svensk lagstiftning.[145] För svensk lagstiftning är det dock inte relevant om direktivet är giltigt eller inte utan det viktiga är att pröva om den svenska regleringen uppfyller de integritetsmässiga krav som uppställs på lagstiftningen.[146] En utredning som ska ske över den svenska lagstiftningen har tillsatts.[147]

5.2 Meddelanden inkomna efter beslagstillfället

Vid beslag av mobiltelefoner som innehåller elektronisk information görs en skillnad mellan meddelanden som finns lagrade i telefonen vid beslagstillfället och meddelanden som inkommer efter beslagstillfället. Meddelanden som redan finns lagrade i telefonen får avläsas vid en beslagsundersökning oavsett om mottagaren hunnit tillgodogöra sig meddelandet eller inte.[148] Däremot är det oklart hur meddelanden som inkommer efter beslagstillfället ska behandlas.

5.2.1 Nuvarande rättsläge

Rättsläget avseende brottsbekämpande myndigheters hantering av meddelanden som inkommer efter beslagstillfället är oklar. Det finns en osäkerhet kring vilka förfaranden som är tillåtna och vilka som inte är det.[149] Om brottsbekämpande myndigheter får undersöka meddelanden som inkommer efter beslagtillfället skulle skyddet för hemlig kommunikation avsevärt försvagas och den hemliga tvångsmedelsregleringen sättas ur spel. Detta beror på att brottsbekämpande myndigheter skulle få tillgång till information som inte är möjlig att inhämta med hemliga tvångsmedel. Enligt Lindberg kan det därmed inte anses tillåtet att använda beslag för att ta del av meddelanden som inkommer efter beslagstillfället.[150] Syftet med beslagslagstiftningen är att omhänderta den information som finns vid beslagstillfället, vilket gör att ett förfarande där brottsbekämpande myndigheter

[144] http://www.dagensjuridik.se/2014/04/chefen-rikskriminalen-till-angrepp-mot-eu-domstolens-beslut-om-datalagringsdirektivet.
[145] http://www.dagensjuridik.se/2014/04/mp-kraver-stopp-datalagring-efter-eu-domstolens-dom-men-regeringen-vill-vanta.
[146] Tibbling, 2014-04-28.
[147] http://www.dagensjuridik.se/2014/04/utredare-ska-analysera-svensk-ratt-utifran-eu-domstolens-upphavande-av-datalagringsdirektive.
[148] Beslag: en handbok, 2013 s. 31, 33.
[149] Beslag: en handbok, 2013 s. 34.
[150] Lindberg, 2012 s. 429-430.

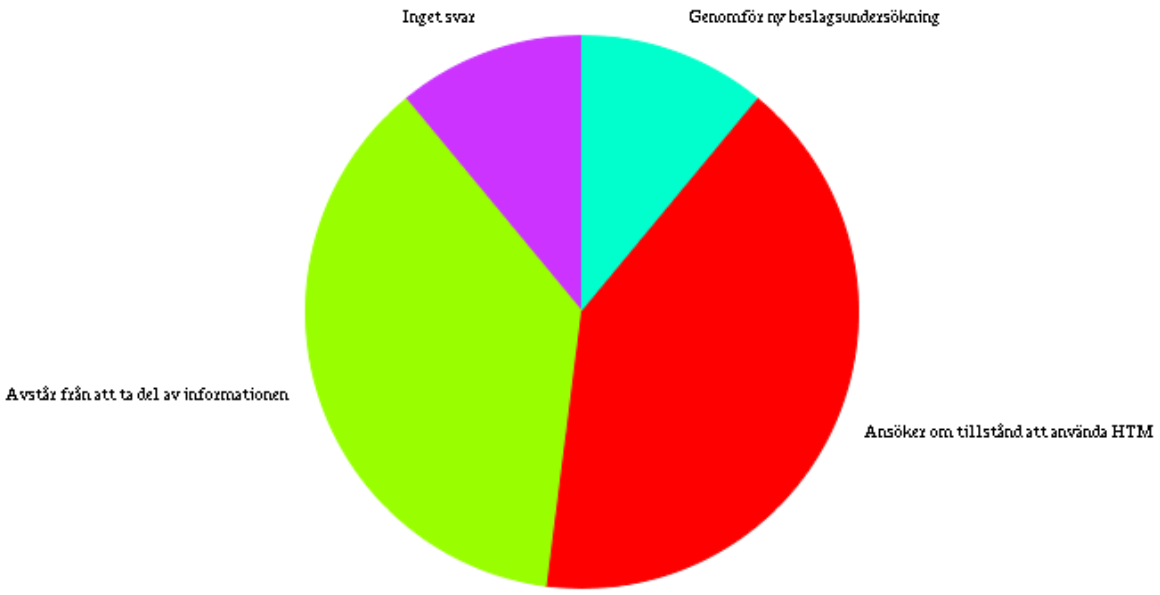
avläser meddelanden som inkommer efter beslagstillfället inte överensstämmer med regleringens ändamål.[151] Brottsbekämpande myndigheter kan inte heller tillämpa LEK på meddelanden som inkommer efter beslagslagstiftningen, då lagen inte tillåter att innehållet i ett telemeddelande utlämnas. Utgångspunkten för att läsa inkomna meddelanden efter beslagstillfället borde således vara hemlig avlyssning av elektronisk kommunikation. Att använda hemlig avlyssning av elektronisk kommunikation på meddelanden som inkommer efter beslagstillfället rekommenderas i Åklagarmyndighetens och Ekobrottmyndighetens riktlinjer. Hemlig avlyssning av elektronisk kommunikation kan därmed anses komplettera beslagslagstiftningen.[152]

De villkor som uppställs för hemlig avlyssning av elektronisk kommunikation är att någon ska vara skäligen misstänkt, att åtgärden är av synnerlig vikt för utredningen och att det finns en teleadress som kan knytas till den som är skäligen misstänkt.[153] Med teleadresser avses telefonnummer, telefonens operatörsuppgifter, telefonens ID-nummer och e-postadresser.[154] Hemlig avlyssning av elektronisk kommunikation får tillämpas på pågående kommunikation.[155] Tillstånd till hemlig avlyssning av elektronisk kommunikation kan således avse realtid eller förfluten tid. Båda tillstånden kan i olika situationer nyttjas för att avläsa meddelanden som inkommer efter beslagstidspunkten. Finns ett tillstånd till hemlig avlyssning för den beslagtagna telefonen och detta tillstånd avser realtid borde ett sådant tillstånd tillåta att brottsbekämpande myndigheter tar del av meddelanden som inkommer efter beslagstillfället. Om brottsbekämpande myndigheter däremot inte har något tillstånd till hemlig avlyssning för beslagsföremålet och det inkommit ett meddelande efter beslagstillfället kan de i efterhand ansöka om tillstånd till avlyssning i förfluten tid. På så sätt kan brottsbekämpande myndigheter tillgodogöra sig det nya meddelandet.[156]

Säkerhets- och Integritetsskyddsnämnden har gjort en undersökning om hur åklagare hanterar elektroniska meddelanden som inkommer efter beslagstillfället. Enligt Säkerhets- och Integritetsskyddnämnden ger undersökningen en tydlig bild av åklagarnas hantering av situationen då undersökningen besvarades av 124 åklagare vid 34 åklagarkammare och då endast ett fåtal åklagare använder hemliga tvångsmedel regelbundet. Resultatet, se diagram 3, visar att åklagarna antingen genomförde en ny beslagsundersökning, avstod från att ta del av informationen eller ansökte om hemliga tvångsmedel. Åklagarna menade dock att omständigheterna i det enskilda fallet hade en stor inverkan på hur situationen hanterades.[157]

[151] Hjertstedt, 2011 s. 246.
[152] Beslag: en handbok, 2013 s. 34.
[153] 27 kap. 20 § RB.
[154] Beslag: en handbok, 2013 s. 34-35.
[155] Lindberg, 2012 s. 428.
[156] Beslag: en handbok, 2013 s. 35.
[157] Rapport 2011-06-09 s. 8-9, 13.

Diagram 3: Hantering av meddelanden som inkommer efter beslagstillfället



Källa: Säkerhets- och Integritetsskyddsnämnden, Rapport 2011-06-09.

Av de svarande angav lite fler än en tredjedel att de ansöker om tillstånd att använda hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på meddelandena som inkommer efter beslagstillfället. Detta berodde på att de följde Åklagarmyndighetens och Ekobrottsmyndigheten riktlinjer. Ytterligare en anledning till agerandet var att åklagarna ansåg att meddelandet var ”under befordran” vilket innebar att hemlig avlyssning och övervakning av elektronisk kommunikation var de enda möjligheterna att ta del av meddelandet.[158]

Ungefär lika många som ansökte om hemlig tvångsmedelsanvändning valde att inte ta del av informationen i det inkomna meddelandet. Åklagarna hade flera olika motiv till detta. En del ansåg att det inte gick att ansöka om tillstånd för hemliga tvångsmedel då telefonen eller teleadressen inte kunde kopplas till den misstänkte. Andra ville inte avläsa meddelandet då de ansåg att meddelandet fortfarande var under befordran. En tredje grupp påtalade att informationen saknade betydelse eller att de inte tagit del av informationen på grund av försiktighetsskäl.[159]

En mindre grupp av åklagarna uppgav att de hade rätt att genomföra en ny beslagsundersökning där de kunde ta del av det inkomna meddelandet. Detta eftersom telefonen var beslagtagen och att det därmed var tillåtet att undersöka telefonen i enlighet med det ursprungliga beslagsbeslutet. Andra

[158] Rapport 2011-06-09 s. 9-10.
[159] Rapport 2011-06-09 s. 10.

menade att beslaget kunde hävas trots att egendomen fortfarande var i deras besittning. Därefter kunde ett nytt beslagsbeslut och en ny beslagsundersökning genomföras. På så sätt kunde åklagarna få tillgång till det nya meddelandet.[160]

5.2.2 Lagstiftningsåtgärder

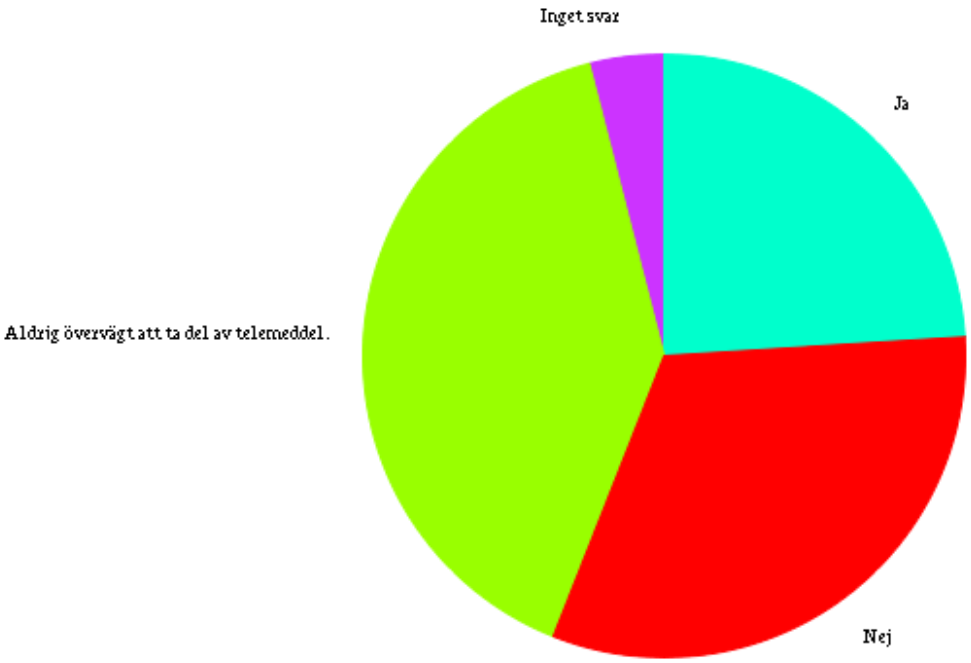
Säkerhets- och Integritetsskyddsnämndens menar att deras undersökning visar att åklagares hantering av meddelanden som inkommer efter beslagstillfället varierar. Även åklagare som tillhör samma åklagarkammare hanterar situationen olika. Alla åklagare följer därmed inte Åklagarmyndighetens och Ekobrottmyndighetens riktlinjer. Rättsläget är således oklart och rättstillämpningen är inte enhetlig. Säkerhets- och Integritetsskyddsnämnden anser att en lagreglering behövs.[161]

Nästan en tiondel av åklagarna som deltog i undersökningen påtalade att det vore bra om lagstiftaren klargjorde hur situationen ska hanteras.[162] I intervjun med Tibbling konstaterar han att rättsläget inte alls är oklart eftersom det inom åklagarväsendet finns tydlig information om hur situationen ska hanteras. Dock tror han att många i praktiken är osäkra på hur de skulle använda reglerna.[163]

I undersökningen framkommer det även att åklagarna anser sig ha behov av att tillgodogöra sig elektroniska meddelanden som inkommer efter en första beslagsundersökning. Enligt åklagarna har behovet ökat i takt med den tekniska utvecklingen inom mobiltelefoni. I Säkerhets- och Integritetsskyddsnämndens undersökning ställdes frågan om de som tagit del av meddelanden som inkommit efter beslagstillfället haft nytta av meddelandena.[164]

[160] Rapport 2011-06-09 s. 9.
[161] Rapport 2011-06-09 s. 13-14.
[162] Rapport 2011-06-09 s. 9.
[163] Tibbling, 2014-04-28.
[164] Rapport 2011-06-09 s. 10, 14.

Diagram 4: Praktisk betydelse av meddelanden som inkommit efter beslagstidpunkten



Källa: Säkerhets- och Integritetsskyddsnämnden, Rapport 2011-06-09.

Nästan en fjärdedel uppgav att fått nytta av det inkomna meddelandet. Den information som erhållits hade hjälpt till att identifiera medgärningsmän och andra misstänkta. Dessutom hade informationen haft betydelse för förundersökningar och som bevisning. Av de som tagit del av nya meddelanden ansåg en tredjedel att informationen inte haft någon praktisk betydelse. Många av åklagarna hade aldrig övervägt att läsa meddelanden som inkommer efter beslagstillfället. Hälften av dessa åklagare ansåg att det trots allt fanns ett behov av att inhämta den sortens meddelanden.[165]

Mot det brottsutredande behovet av att få tillgång till uppgifter står den enskildes integritet. Vid beslag av mobiltelefoner och hemlig tvångsmedelsanvändning tar brottsbekämpande myndigheter del av enskildas korrespondens. Den information som brottsbekämpande myndigheter tillgodogör sig berör den misstänkte, dennes brottslighet och dennes personliga sfär men även de personer som den misstänkte kommunicerar med utsätts för integritetsintrång. Därmed uppstår risk för allvarliga integritetsintrång. Integritetsaspekterna för mobiltelefoner är annorlunda än för fasta telefoner. Fasta telefoner används oftast av fler personer än mobiltelefoner vilket gör att ett ingrepp i en fast telefon oftast leder till större integritetsintrång än ett ingrepp i en mobiltelefon. Ju fler personer som övervakas desto större anses intrånget vara.[166]

[165] Rapport 2011-06-09 s. 11.
[166] Rapport 2011-06-09 s. 13-14.

5.3 Beslagslagstiftningens integritetsskydd

Beslagslagstiftningen innehåller uttryckligen ett utvidgat integritetsskydd för såväl skriftliga handlingar som enskilda handlingar. Detta skydd återfinns i 27 kap. 2 § och 12 § RB. Syftet med reglerna är att skydda den enskildes korrespondens och förtroliga information.[167] Eftersom den tekniska utvecklingen har förändrat människors sätt att kommunicera uppstår frågan om meddelanden som lagras elektroniskt på en mobiltelefon inbegrips i beslagslagstiftningens integritetsskydd trots att detta uttryckligen gäller skriftliga handlingar och enskilda handlingar.

5.3.1 Beslagsförbudet

Beslagsförbudet regleras i 27 kap. 2 § RB och innebär att vissa skriftliga handlingar inte får beslagtas. Dessa handlingar innehåller information om sådant som en person enligt 36 kap. 5 § RB inte får vittna om. Inte heller får skriftliga meddelanden mellan den misstänkte och en närstående till denne beslagtas om det begångna brottet har ett lindrigare straff än två års fängelse.[168] I båda fallen får handlingarna beslagtas om de påträffas hos tredje man. Regeln syftar således till att skydda förtrolig information mellan vissa personkategorier.[169] Det är oklart om meddelanden som lagras elektroniskt på en mobiltelefon omfattas av beslagsförbudet. Forskningen på området har främst avsett datorer men borde kunna tillämpas på mobiltelefoner eftersom argumenten är inriktad på generella aspekter avseende elektronisk information.

5.3.1.1 Nuvarande rättsläge

Beslagsförbudet gäller enligt ordalydelsen skriftliga handlingar. I RB saknas en definition av begreppet skriftlig handling trots att begreppet från början avsåg skrift på papper. Till skillnad från när bestämmelsen trädde ikraft förmedlas idag stora mängder information elektroniskt. Enligt bestämmelsens ordalydelse är det oklart om denna information omfattas av beslagsförbudet.[170] Om beslagsförbudet inte är tillämpligt på beslag av mobiltelefoner innehållande elektronisk information är brottsbekämpande myndigheter beroende av vilket kommunikationssätt användare väljer. I promemorian om *Brott och brottsutredning i IT-miljö* påtalas att det är

[167] Bring, Diesen, 2009 s. 398-399, 459.
[168] 27 kap. 2 § RB.
[169] Bring, Diesen, 2009 s. 398-399.
[170] Lindberg, 2012 s. 402-403.

orimligt att samma sorts information har olika rättsliga skydd enbart på grund av valet av kommunikationsmedel.[171]

HD har inte behandlat frågan om beslagsförbudets tillämplighet på elektronisk information. Däremot har HD konstaterat att editionsreglerna i 38 kap. RB är tillämpliga på information som lagras elektroniskt.[172] Editionsplikten i 38 kap. 2 § RB innebär att den som besitter en skriftlig handling ska lämna den till brottsbekämpande myndigheter om handlingen antas ha betydelse som bevisning. Likt beslagsförbudet gäller editionsskyldigheten språkligt sett enbart skriftliga handlingar.[173]

Beslagsförbudets tillämplighet på elektronisk information vid beslag av datorer har flera gånger berörts av JK och JO. Båda aktörerna önskar att rättsläget ska tydliggöras.[174] JK har uttalat att regeln om beslagsförbud borde skydda all information som kan beslagtas. Regeln ska således inte vara beroende av vilket föremål som informationen lagras på eftersom syftet med beslagsförbudet är att skydda förtrolig information. Beslagsförbudet får däremot inte förhindra att ett föremål, så som en dator, med en stor mängd information inte kan beslagtas enbart på grund av risken att en liten del av informationen faller inom beslagsförbudets tillämpningsområde. JK anser sitt resonemang baserat på en analogisk tolkning av 27 kap. 2 § RB.[175]

Även JO anser att föremålet som informationen lagras på inte är relevant för bedömningen om beslagsförbudets tillämplighet eller inte. Detta beror på att samma sorts fakta blir tillgänglig för brottsbekämpande myndigheter oavsett vilket föremål som beslagtas. Då beslagsförbudet ska skydda förtroligheten mellan vissa personkategorier är behovet av att skydda information lika stort oavsett hur den lagras. Det är således orimligt att skyddet för elektroniskt lagrad information är sämre än skyddet för skriftlig information. Om skriftliga meddelanden mellan närstående inte ska få åberopas som bevisning i en brottsutredning, ska inte heller liknande meddelanden i elektronisk form få åberopas. Starka skäl talar således för att elektronisk och skriftlig information ska behandlas på samma sätt.[176]

Vidare har JO i ett ärende gällande mobiltelefoner uttalat att all sorts information som finns lagrad på mobiltelefoner kan skyddas genom beslagsförbudet. Därmed kan beslagsförbudet tillämpas på annat än innehållet i meddelanden till exempel information om när ett meddelande skickats. Likt JK anser JO att en elektronisk enhet får beslagtas trots att det är troligt att en del av informationen på föremålet inte får beslagtas.[177]

Beslagsförbudet infördes när det knappt fanns andra informationsbärare än papper. Elektronisk information, som i pappersform omfattas av beslags-

[171] Ds 2005:6 s. 279-280.
[172] NJA 1998 s. 829.
[173] SOU 2011:45 s. 292.
[174] Se t.ex. JK dnr 6372-07-31, JO 2009/10 s. 84-85, JO 2011/12 s. 146-147.
[175] JK dnr 6372-07-31.
[176] 2009/10:JO1 s. 84-85.
[177] 2011/12:JO1 s. 146-147.

förbudet i 27 kap. 2 § RB, ska enligt riksåklagaren inte avläsas eller åberopas som bevisning i brottmål eftersom det ur ett etiskt perspektiv inte är rimligt att behandla elektronisk och skriftlig information olika.[178] Riksåklagarens uttalande har fastställts i Åklagarmyndighetens och Ekobrottmyndighetens riktlinjer. Där framhålls det också att SMS och intalade meddelanden ska likställas med skriftliga handlingar och att undersökningar av mobiltelefoner och röstbrevlådor ska ske med försiktighet. Påträffas meddelanden som inte får beslagtas enligt beslagsförbudet ska denna information inte återges i förundersökningsprotokollet. Istället ska det noteras att meddelanden mellan närstående eller annan information som omfattas av beslagsförbudet funnits i mobiltelefonen men att informationen inte tagits in i protokollet.[179]

Enligt Lindberg är det huvudsakliga argument för beslagsförbudets tillämplighet på elektroniska handlingar att intresset av att skydda förtrolig information är lika starkt oavsett hur informationen har lagrats. Det är dock oklart om detta ställningstagande stöds i lagens utformning.[180] Handlingsbegreppets språkliga lydelse borde kunna inbegripa upptagningar av skrift men inte framställningar av bilder eller upptagningar som endast kan avlyssnas eller läsas med tekniska hjälpmedel. Eftersom det inte framgår vilka föremål som beslagsförbudet kan tillämpas på är rättsläget oklart. Att bestämmelsen förbjuder beslag av skriftliga handlingar men inte andra föremål verkar, enligt Hjertstedt, obefogat.[181]

5.3.1.2 Lagstiftningsåtgärder

Beslagsförbudets tillämplighet på elektronisk information har behandlats i flera statliga utredningar eftersom svårigheter vid beslag av datorer har påträffats. Utredningarna har främst inriktats på om beslagsförbudet är tillämpligt på elektronisk information och om det behöver vidtas åtgärder för att förtydliga detta. Inga förslag har lett till lagstiftningsåtgärder.[182] I utredningen om anonymitetsskydd vid beslag och husrannsakan konstateras att ur ett anonymitetsperspektiv ska det rättsliga skydd som gäller skriftliga handlingar även gälla elektroniska upptagningar med ett liknande innehåll. För att det rättsliga skyddet ska bli likvärdigt föreslås att handlingsbegreppet i RB ska utökas. Handlingsbegreppet i 2 kap. 3 § TF ska vara förebild för det nya begreppet i RB eftersom det inkluderar framställningar i skrift och bild samt upptagningar som avlyssnas eller läses med tekniska hjälpmedel.[183]

[178] ÅM-A 2006/1152.
[179] Beslag: en handbok, 2013 s. 35-36.
[180] Lindberg, 2012 s. 403.
[181] Hjertstedt, 2011 s. 214-215.
[182] Se t.ex. SOU 1976:36, SOU 1992:110, SOU 1995:47, SOU 1996:40, Ds 2005:6, SOU 2011:45.
[183] SOU 1976:36 s. 57-58, 85.

Datastraffrättsutredningen hävdar att beslagslagstiftningen gäller skriftliga handlingar och inget annat. Alla regler i 27 kap. RB är då inte tillämpliga på elektronisk information. Reglerna i RB ska anpassas till IT-miljön genom att begreppet ”skriftliga handlingar” likställs med elektronisk information. Ett nytt övergripande handlingsbegrepp som avser både traditionella handlingar och data borde införas. Om delen skriftlig i begreppet ”skriftlig handling” tas bort omfattar beslagsregleringen även data. Representationen av informationen anses då vara beslagsföremålet. Vidare menar Datastraffrättsutredningen att handlingsbegreppet i TF inte är ett gångbart begrepp. Detta beror på att elektroniska upptagningar är något immateriellt som inte kan beslagtas.[184]

Även Polisrättsutredningen menar att beslagsförbudet inte kan tillämpas på datalagrad information. Integritetskänsliga uppgifter som lagras elektroniskt får därmed ett sämre integritetsskydd än uppgifter som är skriftliga. Myndigheter får således större tillgång till individers privata förhållanden. Detta beror på att den nuvarande lagstiftningen inte är anpassad till IT-miljön. Elektroniskt lagrad information kan inte anses vara mindre skyddsvärd än skriftlig information vilket gör att beslagslagstiftningen måste förändras. Polisrättsutredningen avfärdar Datastraffrättsutredningens förslag. Det Datastraffrättsutredningen kallar representation av information kan nämligen inte beslagtas eftersom det inte kan besittas. Dessutom skulle förslaget innebära att användningsområdet för beslag skulle utvidgas. Beslag tillämpas för att omhänderta egendom men Datastraffrättsutredningen förslår då också att beslag skulle kunna nyttjas för att inhämta information. Förslaget innebär att beslag skulle brukas för ett annat syfte än vad som avsågs vid tvångsmedlets införande. Polisrättsutredningen påpekar även att insamling av information inte ska regleras genom tvångsmedel. För att underlätta polisens insamling av information borde det istället införas likartade regler för hur elektronisk och skriftlig information får inhämtas. På så sätt skulle integritetsskyddet för elektronisk information stärkas. Utredningen föreslår även att begreppet ”föremål” i 27 kap. RB skulle ersättas med egendom. Beslagsförbudet kan då omfatta skriftliga handlingar men även annan egendom som innehåller skyddsvärda uppgifter.[185]

IT-utredningen besvarar frågan om beslagsförbudet är tillämpligt på elektronisk information på ett annat sätt än de andra utredningarna. I utredningen konstateras att bestämmelserna i 27 kap. RB är tillämpliga på datalagrad information. Då beslagsreglerna är tillämpliga vid förundersökningar rörande elektroniska förmedlingstjänster ska reglerna även vara tillämpliga på beslag av elektroniskt lagrad information.[186]

I promemorian *Brott och brottsutredning i IT-miljö* anses beslagsförbudet inte tillämpligt på elektroniskt lagrad information. Beslagsförbudets ordalydelse avser nämligen endast traditionella handlingar och inte elektroniskt lagrad information. Begreppen förekommer i ett sammanhang

[184] SOU 1992:110 s. 347-348, 371, 459, 606.
[185] SOU 1995:47 s. 177, 184-188, 193, 490.
[186] SOU 1996:40 s. 209.

som tyder på att elektroniska handlingar inte kan inbegripas i 27 kap. 2 § RB. Återigen påpekas att skyddet för elektronisk information är sämre än skyddet för skriftlig information och att detta inte har varit lagstiftarens avsikt utan har uppstått till följd av den tekniska utvecklingen. Beslagsförbudet borde omfatta elektroniskt information då detta är det vanligaste sättet att kommunicera och lagra information på. Det ska således framgå av lagtexten att elektroniska upptagningar kan tas i beslag och att dessa omfattas av beslagsförbudet.[187]

Förundersökningsutredningen anser att beslagsförbudet inte ska göras direkt tillämpligt på elektroniska handlingar och uppgifter. Anledningen är att elektronisk information lagras på informationsbärare, så som datorer, och dessa digitala informationsbärare kan beslagtas vilket gör att elektronisk information blir tillgänglig för brottsbekämpande myndigheter. Ett uttryckligt förbud mot att beslagta vissa elektroniska handlingar skulle leda till att myndigheter inför ett beslag måste försäkra sig om att den digitala informationsbäraren inte innehåller några uppgifter som skyddas av beslagsförbudet. Att undersöka den stora datamängd som finns i en digital informationsbärare skulle vara krävande ur resurshänseende. Det är dessutom vanligare att digitala informationsbärare innehåller integritetskänslig information än att de inte gör det. Om det finns misstanke om att integritetskänslig information finns i informationsbäraren kan den inte beslagtas vilket leder till att ingen annan information kan säkras genom beslag. En sådan reglering skulle omöjliggöra beslag av digitala informationsbärare eftersom ett sådant beslag alltid innebär beslag av informationsbärarens innehåll.[188]

I Förundersökningsutredningen konstateras också att det som är problematiskt med beslag av elektronisk information är att brottsbekämpande myndigheter får del av integritetskänslig information. Integritetsskyddet för elektronisk information bör stärkas. Detta ska inte ske genom ett beslagsförbud som förhindrar beslag av digitala informationsbärare innehållande integritetskänslig elektronisk information. Författningsregler om hur undersökningen av digitala informationsbärare ska gå till borde istället utformas. En sådan reglering kan ta utgångspunkt i Åklagarmyndighetens riktlinjer som innebär att integritetskänsliga dokument ska släckas ner och inte användas som bevisning. Eftersom det inte behöver göras någon omfattande undersökning av ett dokument för att inse att det är integritetskänsligt överensstämmer en sådan reglering med att skriftliga handlingar får okulärbesiktas innan det avgörs om handlingarna omfattas av 27 kap. 2 § RB. Förfarandet vid beslagsundersökningen skulle bli mer rättssäkert om regler avseende undersökningsförfarandet införs. Reglerna borde bli tillämpliga då det finns omständigheter som i det enskilda fallet talar för att det finns skyddsvärda uppgifter i den digitala informationsbäraren. Ett annat

[187] Ds 2005:6 s. 303-304.
[188] SOU 2011:45 s. 353-354.

sätt att skydda den personliga integriteten är att låta den utsatte närvara vid beslagsundersökningen.[189]

Yttrandefrihetskommittén menar att reglerna om beslag och därmed 27 kap. 2 § RB ska omfatta elektroniska upptagningar för att säkerställa grundlagarnas anonymitetsskydd. Skyddet för elektroniska upptagningar och skriftliga handlingar ska vara lika eftersom det är obefogat att skyddet är olika enbart på grund av teknisk utveckling. Yttrandefrihetskommittén påpekar att de flesta utredningar belyser frågan om beslagsförbudets tillämplighet på elektronisk information utifrån ett brottsbekämpande perspektiv. Fråga ska även belysas utifrån ett tryck- och yttrandefrihetsrättsligt perspektiv. Enligt kommittén ska riksåklagarens riktlinjer för genomsökning av datorer lagstadgas för att öka skyddet för elektroniska uppgifter och handlingar. Påträffas information som skulle omfattas av beslagsförbudet om den var skriftlig ska den släckas ner eller förstöras och får inte åberopas som bevisning.[190]

5.3.2 Granskning av information

Enligt 27 kap. 12 § RB får enbart vissa specifika personkategorier granska handlingar vid beslagsundersökningen. De som får granska handlingar är domstolen, undersökningsledaren, åklagaren, eller någon sakkunnig som anlitats för utredningen av brottet.[191] Syftet med regeln är att skydda den enskildes integritet genom att förhindra att vem som helst kan tillgodogöra sig innehållet i handlingen.[192] Eftersom denna regel uttryckligen anger att den tillämpas på ”enskilda handlingar” är det oklart huruvida regeln är tillämplig på beslag av mobiltelefoner innehållande elektronisk information.

5.3.2.1 Nuvarande rättsläge

Vid undersökningen av mobiltelefoner får brottsbekämpande myndigheter ta del av stora mängder information. För att sortera ut information som är relevant för brottsutredningen töms mobiltelefonen på information och därefter granskas materialet av en utredare. Utredaren är oftast en polis som är insatt i ärendet. Det material som har betydelse för brottsutredningen tillförs sedan förundersökningsprotokollet.[193]

Enligt Lindberg finns inga krav på att vissa specifika personkategorier ska granska beslagtagna digitala informationsbärare. Detta leder till att en dagbok enbart får undersökas av vissa personer medan liknande information som lagras elektroniskt får undersökas av vem som helst. Därmed har

[189] SOU 2011:45 s. 355-356, 359-360.
[190] SOU 2012:55 del 1 s. 414-415, del 2 s. 93-94, 103-104.
[191] 27 kap. 12 § RB.
[192] Bring, Diesen, 2009 s. 459.
[193] Tibbling, 2014-04-28.

elektronisk information så som e-postmeddelanden sämre rättsligt skydd än meddelanden som sänds i pappersform. Lindberg påpekar dock att om e-postmeddelanden skrivs ut borde 27 kap. 12 § RB tillämpas på utskriften.[194] En upptagning som gjorts vid en hemlig avlyssning eller övervakning av elektronisk kommunikation ska dock granskas enligt 27 kap. 12 § RB.[195]

Hjertstedt förordar en mer extensiv tolkning och menar att 27 kap. 12 § RB kan vara tillämpligt på elektroniska meddelanden. Om elektroniska handlingar omfattas av begreppet ”skriftliga handlingar” borde elektroniska handlingar även innefattas i handlingsbegreppet i 27 kap. 12 § RB. Lindbergs resonemang innebär att elektroniskt lagrad information skulle få ett avsevärt sämre integritetsskydd än skriftlig information.[196]

Europadomstolen har behandlat ett österrikiskt mål där både skriftlig och elektronisk information beslagtogs och granskades. Det fanns inga specifika lagregler om hur den elektroniska informationen skulle behandlas. Dock hävdar Europadomstolen att det skett ett intrång i den enskildes rätt till privatliv, enligt 8 artikel EKMR, och att den österrikiska tvångsmedels-regleringen i sin helhet ska tillämpas på den elektroniska informationen. Skyddet vid granskning av elektronisk information ska vara samma som skyddet vid granskning av skriftlig information.[197] Domen kan tolkas så att skyddet i tvångsmedelsregleringen ska var likadant för elektronisk och skriftlig information vilket leder till att 27 kap. 12 § RB ska tillämpas på elektronisk information.[198]

5.3.2.2 Lagstiftningsåtgärder

Ingen statligt utredning har direkt utrett om 27 kap. 12 § RB är tillämplig på elektronisk information. Däremot har frågan behandlats inom den juridiska doktrinen. Lindberg har konstaterat att det är oklart om 27 kap. 12 § RB är tillämpligt på beslag av elektroniskt lagrad information och att det ur ett integritetsperspektiv är problematiskt att skriftliga handlingar och elektronisk information har olikartade rättsliga skydd.[199] Även Hjertstedt har bedömt att rättsläget är oklart och att ett tydliggörande är önskvärt.[200]

[194] Lindberg, 2012 s. 428-429.
[195] 27 kap. 24 § RB.
[196] Hjertstedt, 2011 s. 246-247.
[197] Europadomstolens dom Wieser and Bicos Beteiligungen GmbH mot Österrike den 16 oktober 2007.
[198] Fitger m.fl. Rättegångsbalken (oktober 2013, Zeteo), kommentaren till 27 kap. 12§.
[199] Lindberg, 2012 s. 428-429.
[200] Hjertstedt, 2011 s. 247.

6 Analys

I det inledande avsnittet 6.1 redogörs i korthet för de villkor som gäller vid beslag av mobiltelefoner. Fyra lagtekniska och praktiska problemområden har identifierats i denna studie. Hur ska mobiltelefoner undersökas? Hur ska elektronisk information beslagtas? Hur ska föränderlig information hanteras? Är integritetsskyddet i beslagslagstiftningen tillämpligt på elektronisk information? Dessa problem behandlas var och en för sig i avsnitt 6.2 – 6.5. I samband med att problemen behandlas redovisas även huruvida det bör vidtas lagstiftningsåtgärder för att förändra eller klargöra rättsläget. Avslutningsvis, i avsnitt 6.6, tas ställning till om beslagslagstiftningen behöver anpassas till teknisk utveckling eller om den nuvarande lagstiftningen är tillräcklig.

6.1 Beslag av mobiltelefoner

Vid beslag av mobiltelefoner uppstår integritetsintrång. Ingreppet utgör dels ett intrång i den enskildes rätt till egendom, dels ett intrång i den enskildes rätt till korrespondens. Egendomsintrånget sker till följd av att brottsbekämpande myndigheter omhändertar mobiltelefonen så att den enskilde inte kan förfoga över den. Rätten till korrespondens inskränks då brottsbekämpande myndigheter tar del av elektronisk information som finns i mobiltelefonen och som utgör kommunikation.

Beslag används i syfte att utreda brott och det är tillåtet att inskränka den enskildes rätt till egendom och korrespondens under vissa förutsättningar. En mobiltelefon får beslagtas enligt 27 kap. 1 § RB så länge den är tillgänglig samt så länge det finns ett samband mellan mobiltelefonen, brottet som utreds och en beslagsgrund. Vidare krävs att mobiltelefonen ”skäligen kan antas” ha betydelse för utredningen samtidigt som brottsbekämpande myndigheter inte kan uppnå resultatet på något annat mindre ingripande sätt. Dessutom ska skälen som talar för beslaget väga tyngre än skälen som talar mot beslaget. Beslagslagstiftningen uppställer tydliga villkor för beslag av mobiltelefoner.

6.2 Undersökning av mobiltelefoner

Dagens användning av smartphone har skapat en ny livsstil. En smartphone är bland annat lätt att bära med sig, enkel att koppla upp mot internet, ger åtkomst till sociala medier och har för många blivit en viktig del av vardagen. Många har ersatt traditionella kalendrar, adressböcker, fotoalbum och inköpslistor med olika funktioner som finns i smartphonen. Vid beslag

av smartphonen kan brottsbekämpande myndigheter således få tillgång till en stor mängd information som kan vara relevant vid brottsutredningar men som även kan vara integritetskänslig. Beslaget omfattar således även insamling av allmänna uppgifter om enskilda individers privata förhållanden.

Sammanställs allt material som finns i telefonen kan brottsbekämpande myndigheter kartlägga en stor del av den enskildes privatliv, allt från dagliga aktiviteter till internetvanor. Det abstrakta integritetsintrång som uppstår vid beslag av mobiltelefoner är således mycket stort. Det faktiska intrånget är sällan lika stort då brottsbekämpande myndigheter varken har tid eller resurser att genomsöka allt material. Det är dock viktigt att den enskildes integritet skyddas vid beslag av mobiltelefoner eftersom mobiltelefoner innehåller stora mängder integritetskänslig information och då den enskilde inte frivilligt delar med sig av privat information vid beslaget.

Mobiltelefoners innehåll genomsöks med hjälp av valda sökord och telefonnummer. Ju mer avancerade och ovanliga ord desto större är chansen att relevant information påträffas. Riktlinjer om hur sökorden bör väljas är nödvändiga utifrån dels resurssynpunkt då allt material inte kan genomsökas, dels ett integritetsperspektiv. Påträffas integritetskänsligt material som inte är relevant för utredningen borde detta material släckas ner eller förstöras. Den enskildes integritet kan även skyddas om den enskilde eller ett offentligt ombud närvarar vid undersökningen.

Kopieringsförfarandet är en viktig del vid undersökningar av mobiltelefoner. Brottsbekämpande myndigheter kan lättare arbeta med materialet om kopior upprättas samtidigt som det ur säkerhetssynpunkt är bättre att arbeta med kopior. Vid arbete med originalet finns alltid risk för att innehållet oavsiktligt förstörs eller förändras. Det finns även risk för att brottsbekämpande myndigheter oavsiktligen manipulerar innehållet genom att tillföra information eller använda information taget ur sitt sammanhang. För att förhindra detta kan det vara lämpligt att låta en offentlig försvarare vara delaktig vid beslaget och beslagsundersökningen. Ytterligare en rättssäkerhetsgaranti som kan förhindra manipulation är själva kopieringsförfarandet. Genom att jämföra kopior och original kan det klargöras vad beslaget omfattat. Dessutom kan den misstänktes försvarare genom att ta del av det beslagtagna materialet granska de brottsbekämpande myndigheternas beslagsundersökning, vilket också är en sorts rättsäkerhetsgaranti.

En fördel med kopiering är att beslag kan hävas snabbare och att den enskilde individen snabbare kan få tillbaka mobiltelefonen. Egendomsintrånget upphör men brottsbekämpande myndigheter har fortfarandet tillgång till den information som fanns på mobiltelefonen vid beslagstillfället. Således kvarstår integritetsintrång avseende den enskildes rätt till korrespondens och rätt till att inte behöva dela privat information med andra. Kopieringsförfarandet minskar alltså integritetsintrånget men det upphör inte helt.

Det kan konstateras att kopiering är tillåtet enligt svensk rätt. Detta på grund av Sveriges åtaganden i Europarådets konvention om IT-relaterad brotts-

lighet och det faktum att förfarandet i sig är allmänt accepterat. Det kan dock diskuteras huruvida lagstiftningsåtgärder behöver införas för att reglera kopieringsförfarandet. Det är positivt med en lagreglering eftersom kopiering är en vanlig arbetsmetod vid beslag av mobiltelefoner. Nackdelen med en lagreglering är att brottsbekämpningen riskerar att bli mer ineffektiv i och med ett ökat byråkratiskt förfarande. Lagregleras brottsbekämpande myndigheters vanliga arbetsmetoder minskar dock subjektiva bedömningar då förutsättningar för en mer enhetlig rättstillämpning uppställs, vilket gör att allmänhetens förtroende för brottsbekämpningen ökar. Även om endast praxis kodifieras är det således en fördel ur brottsbekämpande perspektiv, integritetshänseende och rättssäkerhetssynpunkt att införa lagregler avseende kopiering.

Det är också relevant att utreda vilket integritetsskydd som ska gälla vid kopiering av beslagtagna föremål. En rätt till domstolsprövning kan inte införas eftersom det inte överensstämmer med principen om fri bevisföring. Principen har stor betydelse inom svensk processrätt och ska inte åsidosättas. I den mån det går att återlämna kopior till den drabbade bör det göras eftersom den enskildes rätt till domstolsprövning då kvarstår.

Kopior upprättas i samband med beslag. Då det i beslagslagstiftningen uppställs ett integritetsskydd för beslagtagen egendom är det rimligt att detta skydd även ska omfatta kopiorna. Information som fås när föremål omhändertas borde hanteras på samma sätt oavsett om informationen har kopierats eller inte. En lagstiftningsåtgärd är således önskvärd ur ett integritetshänseende.

6.3 Elektronisk information

Elektronisk information kan lagras på olika elektroniska enheter och den tekniska utvecklingen har lett till att dessa enheter är uppbyggda på ett likartat sätt. Mobiltelefoner, datorer och surfplattor är bland annat utrustade med nätverksanslutningar och kan förmedla samma tjänster och funktioner. De innehåller även stora mängder elektronisk information som kontinuerligt förändras. Med hänsyn till dessa grundläggande likheter borde samma regler kunna tillämpas på samtliga elektroniska enheter. Då juridisk doktrin och de statliga utredningarna främst utrett och analyserat beslag av datorer borde denna forskning i stor utsträckning kunna appliceras på mobiltelefoner och andra digitala informationsbärare.

Beslag av mobiltelefoner är tillåtet men det är oklart huruvida elektronisk information kan beslagtas. Elektronisk information är i grunden elektroniska impulser där ström slås på och av så att olika kombinationer bildar information. Ström och därmed även elektronisk information är ett immateriellt föremål som inte kan beslagtas. Precis som elektronisk information är innehållet i en skriftlig handling något immateriellt. I utredningen om it-brottskonventionen hävdas att elektronisk information kan beslagtas

om den lagras på en elektronisk enhet, så som en mobiltelefon. Påståendet får anses motiverat eftersom det är allmänt accepterat att skriftliga handlingars innehåll kommer brottsbekämpande myndigheter tillhanda när den skriftliga handlingen beslagtas. Detta leder till att elektronisk information i sig inte kan beslagtas men att ett föremål som innehåller elektronisk information kan beslagtas och därigenom även den elektroniska informationen. Ett beslag av en mobiltelefon resulterar alltså i förlängningen i ett beslag av elektronisk information.

Vid beslagslagstiftningens införande var det inte meningen att elektronisk information skulle kunna beslagtas eftersom elektronisk information vid den tidpunkten inte hade något värde som bevisning. Behovet av beslag av elektronisk information har uppstått på grund av att information till följd av den tekniska utvecklingen fått värde som bevis. I och med detta kan det diskuteras huruvida beslagslagstiftningens tillämpningsområde har utvidgats. Det är allmänt accepterat att innehållet i skriftliga handlingar får beslagtas utan att detta uttryckligt angetts i lagen. Därmed borde även innehåll i andra föremål, så som en mobiltelefon, få beslagtas. Legalitetsprincipen stadgar att tvångsmedelsregleringen ska tolkas restriktivt. En utvidgande tolkning som innebär att innehåll i alla sorters föremål får beslagtas borde därmed inte vara tillåten. Med tanke på det ökade behovet av att beslagta elektronisk information, det faktum att den sortens beslag är vanliga och legalitetsprincipen borde lagstiftaren förtydliga att beslag av föremål innehållande elektronisk information är tillåtet.

Elektronisk information är en typ av indirekt kommunikation som avläses på mobiltelefoner och elektroniska enheter. Informationen behöver inte vara lagrad på den enhet som den kan avläsas på. Därmed uppstår frågan om det är nödvändigt att beslagta den enhet, telefonen, SIM-kortet eller servern, som faktiskt lagrar informationen eller om det är tillräckligt att beslagta en enhet där informationen kan avläsas. Ur integritetshänseende är det nödvändigt att beslagta den bärare som faktiskt lagrar informationen eftersom integritetsintrången annars riskerar att få oförutsedda konsekvenser. Om information som lagras på en server eller ett SIM-kort avläses med hjälp av en beslagtagen mobiltelefon utsätts inte bara den som drabbats av beslaget utan även den som denne kommunicerat med för ett integritetsintrång. Innehavaren av servern eller SIM-kortet utsätts också för integritetsintrång. Finns servern dessutom i ett annat land utsätts även detta land för integritetsintrång. Proportionalitetsprincipen skulle troligen förhindra beslag av mobiltelefoner innehållande elektronisk information om beslaget omfattar all information som kan avläsas på mobiltelefonen. Detta eftersom det ur integritetshänseende skulle vara svårt att bedöma vem som omfattas av beslaget och dess omfattning. Mot bakgrund av detta måste den elektroniska enhet som lagrar elektronisk information beslagtas för att informationen ska komma brottsbekämpande myndigheter tillhanda.

Att rätt elektroniska enhet måste beslagtas för att brottsbekämpande myndigheter ska få avläsa elektronisk information är negativt ur ett brottsbekämpande perspektiv. Villkor som innebär att beslaget ska omfatta den elektroniska enhet som lagrat den elektroniska informationen gör att

brottslingar kan placera information på flera SIM-kort, eller servrar runtom i världen i syfte att försvåra brottsutredningar. Det är mer eller mindre omöjligt att bevissäkra elektronisk information om brottslingar regelbundet flyttar runt informationen mellan olika servrar och olika länder. Brottsbekämpande myndigheter får svårt att ta reda på var servern finns och vilken elektronisk enhet som ska beslagtas för att komma åt informationen. Upptäcker de brottsbekämpande myndigheterna att exempelvis den relevanta server är placerad utomlands blir även förfarandet för att få tillgång till informationen extra byråkratiskt då brottsbekämpande myndigheter måste vända sig till det landets myndigheter och begära ut servern.

För att underlätta situationen kan det införas ett föreläggande om att företag som tillhandahåller servertjänster ska tvingas lämna information i syfte att underlätta brottsutredningen. Tvingas dessa företag lämna uppgifter om var servern är placerad blir det enklare att lokalisera servern och beslagta den. Föreläggandet är grundat på den Europeiska konventionen om IT-relaterad brottslighet. Det kan därför diskuteras om inte länderna inom EU skulle kunna samarbeta avseende denna typ av förlägganden eller om föreläggandet ska kunna användas inom EU på ett förenklat och standardiserat sätt. Ett standardiserat förfarande för hur svenska myndigheter ska beslagta de servrar som finns inom EU bör i så fall också utformas. Är ett föreläggande tillämpligt inom hela EU borde svenska brottsbekämpande myndigheter direkt kunna vända sig till ett företag i ett EU-land som tillhandahåller servertjänster och begära ut information om var servern som innehar relevant information är placerad. Ett sådant föreläggande skulle således underlätta för brottsbekämpande myndigheter att lokalisera servrar. Därefter kan beslag göras enligt sedvanliga regler.

Förläggandet skulle även kunna utformas så att företagen ska tillhandahålla informationen som finns på den efterfrågade servern. Om ett svenskt företag har servern på svensk mark är det möjligt att beslagta den i enlighet med den svenska beslagslagstiftningen. Om det svenska företaget istället har servern utomlands antingen hos en underleverantör eller i egen regi borde ett sådant föreläggande kunna innebära att den efterfrågade informationen som vid detta tillfälle finns lagrad på servern ska flyttas till en digital informationsbärare i Sverige och som svenska brottsbekämpande myndigheter sedan kan beslagta. Företaget, som tillhandahåller servertjänster, hålls ansvarig för de servrar eller informationsbärare de använder i sin verksamhet oavsett var de är placerade eller vem som äger dem. De ges också ett ansvar för att flytta aktuell information till en informationsbärare, som kan beslagtas, i det land där företaget är registrerat. Därmed skulle brottslingar få svårare att utnyttja teknik för att dölja brottslighet. Det faktum att Datalagringsdirektivet har ogiltigförklarats borde inte påverka ett sådant här förslag då företagen inte ska lagra någon kommunikation eller information under en viss tid. Föreläggandet avser endast den information som finns vid tidpunkten för föreläggandet. För ett föreläggande av detta slag borde det kunna införas ett förenklat förfarande inom hela EU och övriga länder som är benägna att anslutna sig till ett sådant förförande.

Båda förslagen är inriktade på att effektivisera brottsbekämpningen och förhindra att brottslingar kringgår svenska lagar genom olika tekniska lösningar. Ett föreläggande där företag endast informerar brottsbekämpande myndigheter om var servern är placerad är inte så integritetskränkande då brottsbekämpande myndigheter inte får del av den enskildes information utan endast får reda på var den enskildes privata information finns någonstans. Huruvida integritetsintrånget väger tyngre än det brotts-utredande intresset får sedan avgöras vid beslaget av servern. Ett föreläggande där företag tillhandahåller information är mer integritetskränkande. En fördel ur integritetsperspektiv är att inte hela servern behöver beslagtas vilket innebär att företaget endast tillhandahåller data som avser en person. Därmed uppstår inga abstrakta integritetsintrång för andra individer som har data lagrad på servrar som beslagtas. Däremot åläggs företag att göra integritetsintrång i en enskilds privata sfär. Eftersom företaget till stor del utför beslaget finns risk för kvalitetsbrister så som att all relevant information inte kommer brottsbekämpande myndigheter tillhanda eller att de får ta del av för mycket information. Förslaget är således intressant ur ett teoretiskt och brottsbekämpande perspektiv men behöver utredas och konkretiseras utifrån ett integritetsperspektiv och ett praktiskt perspektiv.

Ett effektivt bevissäkrande av information på servrar placerade runtom i världen skulle underlättas av att ovanstående förelägganden är tillämpliga i ett så stort antal länder som möjligt. Det kan dock vara svårt att få länder att komma överrens om hur ett föreläggande ska utformas och vad det ska innehålla. Det kommer trots allt att finnas en möjlighet att lagra information i de länder som skulle stå utanför ett samarbete. Därmed skulle förelägganden enligt förslagen ovan inte helt kunna förhindra ett kringgående av svenska rättsregler utan endast försvåra detta.

6.4 Föränderlig information

Innehållet i mobiltelefoner kan förändras, vilket aktualiserar frågan om huruvida meddelanden som inkommer efter beslagstillfället ska omfattas av beslaget eller inte. Beslagslagstiftningen reglerar inte denna situation och inte heller andra situationer där information förändras efter beslagstillfället. Detta eftersom lagstiftarens syfte med beslag är att ta del av information som finns på beslagsföremålet i det ögonblick beslaget sker. Teknik som möjliggör att elektronisk information förändras fanns nämligen inte när lagstiftningen infördes.

Att få ta del av meddelanden som inkommer efter beslagstillfället är positivt för brottsbekämpande myndigheter om ytterligare information som tillförs mobiltelefonen har betydelse för brottsutredningen. Men det kan även vara negativt om relevant information raderas. Enligt Tibbling vill åklagare som utgångspunkt inte att materialet förändras. Ur integritetshänseende kan det också vara problematiskt med föränderlig information. Integritetsintrånget ökar om brottsbekämpande myndigheter kan ta del av framtida information

och kommunikation. Det är även svårare att på förhand bedöma integritetsintrånget utifrån proportionalitets- och behovsprinciperna.

Med hänsyn till lagstiftarens syfte, som enligt legalitetsprincipen inte kan utvidgas utan lagstöd, borde inte meddelanden som inkommer efter beslagstillfället omfattas av beslaget. De negativa konsekvenserna ur integritetshänseende och ur ett brottsbekämpande perspektiv stödjer detta ställningstagande. Ställningstagandet överensstämmer med Åklagarmyndighetens och Ekobrottsmyndighetens riktlinjer. Att ta del av nya meddelanden genom att häva beslagsbeslutet och därefter ta ett nytt beslagsbeslut kan uppfattas som ett kringgående av ovanstående ställningstagande. Det faktum att det råder tveksamhet om kringgående eller ej borde vara tillräckligt för att förfarandet ur rättsäkerhets- och integritetsperspektiv inte ska vara tillåtet.

De meddelanden som inkommer efter beslagtillfället borde således inte kunna komma brottsbekämpande myndigheter tillhanda genom beslag. Dock borde det gå att ta del av meddelanden genom att kombinera beslaget med ett annat tvångsmedel. Eftersom meddelanden som inkommer efter beslagstillfället anses vara ”under befordran” är det endast genom hemlig avlyssning och övervakning av elektronisk kommunikation som brottsbekämpande myndigheter kan avläsa eller få uppgifter om meddelandet. Alltså borde meddelanden som inkommer efter beslagstillfället ses som pågående kommunikation.

Utifrån ett sådant ställningstagande kan det diskuteras om inte olästa meddelanden som finns på mobiltelefonen vid beslagstillfället ska ses som pågående kommunikation. Alla olästa meddelanden i mobiltelefonen får vid beslagstillfället läsas eftersom beslaget omfattar all information som finns i beslagsföremålet vid beslagstillfället. Den som äger mobiltelefonen kan dessutom haft möjlighet att läsa de meddelanden som finns i mobiltelefonen före beslagstillfället men har ingen möjlighet att läsa meddelanden som inkommer senare. Meddelanden så som e-post kan markeras som olästa efter att mottagaren har läst meddelandandet vilket gör att brottslingar skulle kunna fördröja brottsutredningar genom att markera relevant information som oläst. En reglering som kräver tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation för olästa meddelanden vid beslagstillfället skulle därmed kunna utnyttjas av brottslingar för att fördröja utredningsarbetet. Således är det ur ett brottsbekämpade perspektiv motiverat att meddelanden som finns vid beslagstillfället omfattas av beslaget medan meddelanden som inkommer efter beslagstillfället anses vara pågående kommunikation.

Kombineras tvångsmedlen beslag och hemlig avlyssning och övervakning av elektronisk kommunikation på ovanstående sätt får integritetsintrånget klart stå tillbaka för det brottsutredande intresset. Om brottsbekämpande myndigheter kombinerar tvångsmedlen kan de inte bara kartlägga var den enskilde individen varit och vad den enskilde individen gjort utan även var den enskilde individen ska vara och vad den enskilde individen ska göra. Det ska dock påpekas att en kombination av beslag och hemlig övervakning

av elektronisk kommunikation är mindre integritetskränkande än en kombination av beslag och hemlig avlyssning av elektronisk kommunikation. Det faktiska integritetsintrånget som kan uppstå vid en kombination av tvångsmedlen riskerar dock att bli stort vilket gör att det krävs en noggrann behovs- och proportionalitetsbedömning när tvångsmedlen ska kombineras. Nästan hälften av de åklagare som deltog i Säkerhets- och Integritetsskyddsnämndens undersökning uppgav att de aldrig tagit del av meddelanden som inkommer efter beslagstidpunkten. Av undersökningen framkom det inte varför de inte tagit del av meddelanden men agerandet kan tyda på att det redan görs en noggrann behovs- och proportionalitetsbedömning. Vid en kombination av tvångsmedlen borde det även ställas högre krav på att användandet av hemliga tvångsmedel ska tillföra något nytt eftersom brottsbekämpande myndigheter redan har tillgång till så stor del av en individs privata förhållanden genom beslaget av mobiltelefonen.

Det bör även utredas om det finns ett verkligt behov av att kombinera tvångsmedlen. Enligt åklagarna som deltog i Säkerhets- och Integritetsskyddsnämndens undersökning ansåg de flesta detta. Trots det uppgav mer än hälften av de som tagit del av nya meddelanden att de inte haft någon praktisk nytta av de inkomna meddelandena. Detta kan tolkas som att behovet av att ta del av meddelanden som inkommer till en mobiltelefon efter det första beslagstillfället inte är så stort. Huruvida det verkligen finns ett behov behöver utredas mer ingående. En sådan utredning bör studera hur ofta åklagare tagit del av inkomna meddelanden, i vilka typer av brottsutredningar detta skett och vid vilka brott meddelandena haft betydelse. Det är möjligt att en kombination av dessa tvångsmedel endast bör användas i utredningar rörande vissa speciella brott. En sådan reglering skulle beakta det brottsbekämpande behovet samtidigt som den enskildes integritetsskydd skulle stärkas eftersom åklagare då inte kan göra subjektiva bedömningar om när tvångsmedlen ska kombineras.

Det bör även utredas om lagstiftningsåtgärder behöver vidtas för att klargöra rättsläget för meddelanden som inkommer efter beslagstillfället. Säkerhets- och Integritetskyddsnämnden har i en undersökning konstaterat att rättstillämpningen inte är enhetlig. Detta är ett argument som talar för lagstiftningsåtgärder. Det kan dock vara så att rättstillämpningen är mer enhetlig än undersökningen visar. Säkerhets- och Integritetsskyddsnämnden konstaterar att undersökningen ger en rättvisande bild av rättsläget eftersom få åklagare nyttjar hemliga tvångsmedel. Detta kan ifrågasättas då det är möjligt att de åklagare som faktiskt använder hemliga tvångsmedel inte deltagit i studien och att resultatet på grund av detta är missvisande.

Undersökningen kan även påvisa att rättstillämpningen är enhetlig. Mer än två tredjedelar av deltagarna i undersökningen svarade att de antingen använder hemlig avlyssning och övervakning av elektronisk kommunikation eller inte alls tar del av informationen. Därmed visar undersökningen att de flesta tillämpar Åklagarmyndighetens riktlinjer eller anser att de inte haft möjlighet eller behov att göra det. Av de övriga deltagarna besvarade hälften inte frågan. Därmed var det endast en liten del av åklagarna som uppgav att

de gjorde en ny beslagsundersökning eller tog ett nytt beslagsbeslut för att därefter undersöka det inkomna meddelandet. Sett ur detta perspektiv kan rättstillämpningen vara mer enhetlig än vad Säkerhets- och Integritetsskyddsnämnden vill påvisa. Det faktum att endast en tiondel av åklagarna som deltog i undersökningen, cirka 12 av 124 åklagare, ansåg att rättsläget var oklart och Tibblings uttalade om att rättsläget är klart men att flera åklagare har svårt att praktiskt tillämpa reglerna kan anses stödja detta. Svårigheterna att tillämpa reglerna kan även vara en förklaring till varför så många som en tredjedel inte ansökt om hemliga tvångsmedel när ett meddelande inkommit efter beslagstillfället.

Säkerhets- och Integritetsskyddsnämndens undersökning, Tibblings uttalande och det faktum att det i Åklagarmyndighetens och Ekobrottsmyndighetens riktlinjer tydligt anges att hemlig avlyssning av elektronisk kommunikation ska användas på meddelanden som inkommer efter beslagstillfället tyder på att några omfattande lagstiftningsåtgärder inte behöver vidtas eftersom rättstillämpningen verkar vara relativt enhetlig. Lagstiftaren kan dock tydliggöra att meddelanden som inkommer efter beslagstillfället är pågående kommunikation. Ett sådant tydliggörande skulle leda till att det klart framgår att beslag ska tillämpas på den information som finns i mobiltelefonen vid beslagstillfället medan hemlig avlyssning och övervakning av elektronisk kommunikation ska tillämpas på meddelanden som inkommer efter beslagstillfället. Om det inte sker ett klargörande är det möjligt att det behövs en informationsinsats gentemot åklagare för att rättstillämpningen ska bli mer enhetlig.

6.5 Integritetsskydd

Då mobiltelefoner innehåller en stor mängd integritetskänslig information är det av vikt att beslagslagstiftningen tar hänsyn till detta. Det är dock oklart om beslagslagstiftningens integritetsskydd gäller vid beslag av mobiltelefoner innehållande elektronisk information. Beslagsförbudet som syftar till att skydda den enskildes förtroliga kommunikation gäller nämligen uttryckligen skriftliga handlingar. Om bestämmelsen tolkas bokstavligen skulle elektronisk information i mobiltelefoner inte omfattas av bestämmelsen. I så fall skulle skyddet för förtrolig kommunikation och de brottsbekämpande myndigheternas möjligheter att säkra bevisning i form av information bli beroende av vilket kommunikationssätt den enskilde använder. Ur ett integritetsperspektiv och ett brottsbekämpande perspektiv kan detta inte vara rimligt.

Tolkas regeln ändamålsenligt, det vill säga utifrån att all sorts förtrolig information ska skyddas, omfattar bestämmelsen elektronisk information. Skyddet för elektronisk information skulle då vara lika omfattande som skyddet för skriftlig information. Ur ett integritetsperspektiv är en ändamålsenlig tolkning att föredra framför en bokstavstolkning. Bevissäkrandet för skriftlig och elektronisk information blir också likställt vilket

är positivt ur ett brottsbekämpande perspektiv men det kan även konstateras att det blir svårare att bevissäkra elektronisk information. Flera rättsliga aktörer bland annat JO, JK och riksåklagaren förespråkar den ändamålsenliga tolkningen. Detta tyder på att brottsbekämpande myndigheter redan idag likställer elektronisk information med skriftlig. HD:s dom från 1998 avseende editionsreglerna kan även tyda på att HD anser att elektronisk information ska inkluderas i begreppet ”skriftlig handling”. Generellt sett brukar nämligen ett begrepp som förekommer på olika ställen i samma lag ges samma innebörd.

Legalitetsprincipen borde förorda en bokstavstolkning då principen stadgar att tvångsmedelslagstiftningen ska tolkas restriktivt. Med tanke på att beslagsförbudet ska skydda den enskilda individen och dess integritet skulle dock legalitetsprincipens krav på en bokstavstolkning minska den enskildes integritetsskydd. Syftet med legalitetsprincipen är att förhindra ökade ingrepp i enskilda individers rättsliga sfärer. Om principen förhindrar ett utökat integritetsskydd motverkar den sitt eget syfte. Således bör även legalitetsprincipen tala för en ändamålsenlig tolkning av beslagsförbudet.

Då elektronisk information ska skyddas i samma utsträckning som skriftlig information uppstår frågan om det behöver förtydligas att beslagsförbudet gäller elektronisk information och i sådana fall hur förtydligandet ska utformas. Utifrån det oklara rättsläge som presenterats står det klart att ett klargörande behövs. Detta överensstämmer med idén om att brottsbekämpande myndigheters vanliga arbetsmetoder ska lagregleras om de orsakar integritetsintrång. En lagreglering skulle även öka allmänhetens förtroende för de brottsbekämpande myndigheterna. Troligtvis skulle det heller inte bli någon större förändring i den brottsutredande verksamheten då det verkar som elektronisk information redan likställs med skriftlig. Mot bakgrund av detta borde beslagslagstiftningen tydligt ange att integritetsskyddet i 27 kap. 2 § RB avser såväl skriftlig information som elektronisk information.

Svårigheten med att införa ett förtydligande om att beslagsförbudet ska omfatta elektronisk information avser förtydligandets utformning. Utredningen om anonymitetsskydd vid beslag och husrannsakan, Datastraffrättsutredningen, promemorian om *Brott och brottsutredning i IT-miljö* föreslår tre olika men snarlika lösningar: att handlingsbegreppet i beslagslagstiftningen ska utformas efter handlingsbegreppet i TF, att begreppet elektroniska upptagningar tillförs lagtexten eller att delen skriftlig i begreppet ”skriftlig handling” tas bort. Alla tre förslagen innebär att immateriella föremål beslagtas vilket inte är möjligt då ett sådant föremål inte är fysiskt. Används handlingsbegreppet i TF skulle beslagsföremålet vara framställningen av skriften och bilden eller en elektronisk upptagning som kan avlyssnas och avläsas med tekniska hjälpmedel. Själva framställningen eller upptagningen består av elektroniska impulser vilket innebär att denna ström är immateriell och inte möjlig att beslagta. Handlingsbegreppet i TF kan därmed inte tillämpas i beslagslagstiftningen. Ett tillägg av begreppet elektroniska upptagningar kan av samma anledning inte heller användas. Om delen skriftlig i begreppet ”skriftlig handling” tas bort hävdas det att representationen av informationen beslagtas. Därmed är

det presentationen som sker på datorn, mobiltelefonen eller surfplattan som beslagtas. Presentationen består precis som framställningar och upptagningar av en ström av elektroniska impulser som inte kan beslagtas. Om lagtexten skulle utformas enligt ovanstående förslag hade det varit tillåtet att beslagta varje elektronisk enhet där den sökta informationen kan avläsas. Detta är inte tillåtet ur ett integritetsperspektiv då integritetsintrången skulle bli oförutsebara, se avsnitt 6.3.

Istället för att förändra beslagslagstiftningen föreslog Polisrättsutredningen att en ny reglering avseende insamling av bevis skulle införas. Reglerna skulle innehålla ett integritetsskydd som förhindrade att viss sorts bevis skulle kunna samlas in. Integritetsskyddet för elektronisk och skriftlig information skulle därmed bli detsamma. Förslaget är intressant men torde inte vara praktiskt genomförbart. Principen om fri bevisföring skulle göra en reglering om insamling av bevis verkningslös då brottsbekämpande myndigheter får åberopa bevisning som insamlats på ett lagstridigt sätt. Om regleringen ska få avsedd effekt skulle stora revideringar av det svenska brottmålsförfarandet krävas och med hänsyn till detta är förslaget inte praktiskt genomförbart.

I Polisrättsutredningen föreslås också att begreppet egendom skulle ersätta begreppet ”skriftlig handling”. Förundersökningsutredningen föreslog en liknande åtgärd då de ville införa specifika regler för hur digitala informationsbärare ska undersökas. Båda förslagen innebär att den informationsbärare, mobiltelefonen, som lagrar den elektroniska informationen är beslagsföremålet. Det är även detta föremål som beslagsförbudet skulle kunna tillämpas på. Med en sådan reglering uppstår inte oförutsedda integritetsintrång. Att beslagsförbudet ska avse hela mobiltelefonen är dock en för långtgående åtgärd ur ett brottsbekämpande perspektiv. Eftersom digitala informationsbärare så som mobiltelefoner näst intill alltid innehåller integritetskänsliga uppgifter skulle beslag av mobiltelefoner omöjliggöras till följd av att beslagsförbudet gäller hela mobiltelefonen. För att brottsbekämpande myndigheter ska kunna utreda brott måste mobiltelefoner kunna beslagtas vilket Förundersökningsutredningen, JO och JK argumenterar för. Dock borde det tydliggöras att den information som finns lagrad i mobiltelefonen och som beslagsförbudet skulle vara tillämplig på om informationen varit skriftlig varken får läsas eller åberopas som bevisning. På så sätt skulle beslagsförbudet gällande skriftliga handlingar och föremål som innehåller elektronisk information vara likvärdigt.

Det är även oklart om 27 kap. 12 § RB är tillämpligt vid beslag av mobiltelefoner innehållande elektronisk information. Även här borde resonemanget angående bokstavstolkning, ändamålstolkning och legalitetsprincipen vara tillämpligt. Då ändamålet är att skydda den enskildes korrespondens och minska integritetsintrånget talar detta för att elektronisk information ska inbegripas i 27 kap. 12 § RB. Enligt ovanstående resonemang borde också legalitetsprincipen stödja detta. Då bestämmelsen i 27 kap. 12 § RB gäller ”enskilda handlingar” och inte ”skriftliga handlingar” är det även möjligt att en bokstavstolkning motiverar att elektronisk information kan inkluderas i bestämmelsen. Begreppet ”enskilda

handlingar” är nämligen i sin ordalydelse mer vidsträckt än begreppet ”skriftlig handling”. Dessutom har Europadomstolen i ett österrikiskt mål uttalat att vid granskning av elektronisk och skriftlig information ska samma integritetsskydd gälla. Vidare är det värt att notera att 27 kap. 12 § RB är tillämplig på upptagningar som görs vid hemlig avlyssning av elektronisk kommunikation. Detta kan tala för att bestämmelsen antingen inkluderar elektronisk information i begreppet ”enskild handling” eller att bestämmelsen borde tolkas analogt på elektronisk information. Det kan dock också tyda på att om det inte finns någon regel som uttryckligen anger att bestämmelsen ska gälla elektronisk information så är det inte möjligt att inkludera elektronisk information i bestämmelsen. Mot bakgrund av detta resonemang talar starka skäl för att elektronisk information ska inkluderas i 27 kap. 12 § RB men med tanke på att rättsläget är oklart vore ett förtydligande önskvärt. Klargörandet borde utformas så att det framgår att 27 kap. 12 § RB gäller alla handlingar och föremål som innehåller integritetskänsliga uppgifter.

6.6 Behov av en ny beslagslagstiftning?

Syftet med beslagslagstiftningen är att säkra bevisning så att brott kan utredas. Beslagslagstiftningen är tillämplig på lös egendom i fysisk form och därmed kan immateriella föremål så som elektronisk information inte beslagtas. Det finns dock behov av att beslagta elektronisk information eftersom denna information har stor betydelse som bevis i brottmål. För att beslagta elektronisk information krävs att den är lagrad på en digital informationsbärare. Eftersom digitala informationsbärare är föremål kan de beslagtas enligt den nuvarande beslagslagstiftningen. Detta och det faktum att digitala informationsbärare i grunden är likartade gör en teknikbaserad lagstiftning omotiverad. Specifika regler för varje kommunikationssätt respektive kommunikationsmedel är därmed inte nödvändigt och inte heller önskvärt då en sådan reglering riskerar att vara ohållbar över tid. Således är dagens teknikneutrala beslagslagstiftning att föredra framför en teknikbaserad.

Den nuvarande beslagslagstiftningen är dock problematisk på fyra områden då lagen inte är anpassad till den tekniska utvecklingen. Hur ska mobiltelefoner undersökas? Hur kan elektronisk information beslagtas? Hur ska föränderlig information hanteras? Är integritetsskyddet i beslagslagstiftningen tillämpligt på elektronisk information?

Beslagslagstiftningen är omodern och behöver förändras. En förändring är önskvärd utifrån både ett integritets- och brottsutredande perspektiv. Tydliggörs lagstiftningen skapas förutsättningar för en mer enhetlig rättstillämpning samtidigt som allmänheten får större förtroende för de brottsbekämpande myndigheterna. Det är även rimligt att skyddet för information är samma oavsett om informationen är skriftlig eller elektronisk och oavsett om informationen återges i en originalhandling eller i en kopia.

Flertalet statliga utredningar har utrett delar av ovanstående problematik och påpekat att lagstiftningsåtgärder är önskvärda. Även Säkerhets- och Integritetsskyddsnämnden, JO, JK och åklagarväsendet önskar att beslagslagstiftningen förtydligas och att lagstiftningsåtgärder vidtas. Ett reformbehov är påtagligt och därmed räcker det inte att lagstiftaren enbart utreder och diskuterar problematiken. Lagstiftaren behöver klargöra hur problematiken gällande beslag av föremål, så som mobiltelefoner, innehållande elektronisk information ska hanteras och införa flertalet lagstiftningsåtgärder på området.

De förändringar som enligt denna studie förespråkas är:

- att beslagslagstiftningen uttryckligen anger att kopieringsförfarandet är tillåtet,
- att lagstiftaren tydliggör att i den mån det är möjligt ska kopior istället för original återlämnas till den drabbade så att den enskildes rätt till domstolsprövning gällande beslaget kvarstår,
- att beslagslagstiftningen stadgar att det integritetsskydd som finns i 27 kap. 2 § RB och 27 kap. 12 § RB ska vara tillämpligt på de kopior som upprättas vid beslagsundersökningen,
- att lagstiftaren förtydligar att beslag av digitala informationsbärare i förlängningen innebär att elektronisk information beslagtas,
- att lagstiftaren konstaterar att inkommande meddelanden efter beslagstillfället är pågående kommunikation,
- att beslagslagstiftningen uttryckligen anger att beslagsförbudet inte är tillämpligt på digitala informationsbärare,
- att lagstiftaren ska tydliggöra att elektronisk information varken får läsas eller åberopas som bevisning om motsvarande skriftlig information inte får beslagtas enligt beslagförbudet i 27 kap. 2 § RB samt
- att beslagslagstiftningen uttryckligen anger att digitala informationsbärare som innehåller integritetskänslig information ska granskas enligt 27 kap. 12 § RB.

Bilaga A: Intervju med Jan Tibbling

Telefonintervju, 2014-04-28, med Jan Tibbling, Kammarrättsåklagare Ekobrottsmyndigheten i Stockholm, om beslag av mobiltelefoner och elektronisk information.

1. Hur går en beslagsundersökning av en mobiltelefon till praktiskt?

Svar: Först tar åklagaren ett beslagsbeslut. Det krävs inget ytterligare beslut om husrannsakan för att undersöka en mobiltelefon eller en dator. Mobiltelefonen undersöks genom tömning. Förfarandet påminner om speglingsförfarandet som görs när datorer undersöks. Innehållet i mobiltelefonen kopieras så att det inte kan förändras. Grundprincipen för tömning är således detsamma som för spegling. Enda skillnaden är att tömningsverktygen är annorlunda.

2. Kan undersökningar rikta sig mot endast en viss selektiv del av innehållet i en mobiltelefon? Om detta är möjligt, hur går en sådan undersökning till?

■ Ja ☐ Nej

Svar: Teoretiskt ja. Oftast görs det inte någon selektiv undersökning. En selektiv undersökning kan ske om informationen som eftersöks finns i raderade filer. Stora datamängder undersöks vilket gör att undersöknings-arbetet sker med hjälp av sökord. Sökorden kan bestå av telefonnummer, ord eller bilder. Sökningen sker med successiv relevans och den kan även ske i olika sekvenser.

3. Hur behandlas undersökt information som inte är relevant för utredningen?

■ Förstörs ☐ Sparas

■ Annat

Svar: Information som inte verkar vara relevant kan få betydelse senare i utredningen. Därför kopieras innehållet i mobiltelefonen så att mobil-telefonen kan återlämnas. Med hjälp av kopian kan utredaren vid behov eftersöka mer information med hjälp av sökord. Förr eller senare förstörs informationen, vanligtvis efter avslutad utredning.

4. Vem får granska innehållet i den elektroniska informationen vid beslag av mobiltelefoner?

☐ Rätten	☐ Åklagaren
☐ Undersökningsledaren	☐ Sakkunnig
■ Polisman	☐ Annan

Svar: Åklagaren tar beslagsbeslutet och en forensiker (polisman) utför tömningen av mobiltelefonen. Därefter undersöker en utredare som är insatt i ärendet materialet. Utredaren är oftast polis. Det relevanta materialet återges i förundersökningsprotokollet och övrigt material hamnar i slasken[201]. Materialet presenteras i en forensisk rapport som åklagaren föredrar muntligt inför rätten. Ingen granskar telefonen som sådan.

5. Elektroniska kommunikationssätt blir alltmer integrerade med varandra. Behandlas beslag av mobiltelefoner, datorer, surfplattor likadant om syftet med beslaget är att komma åt elektronisk information? Om beslagen behandlas olika, vilka är då skillnaderna?

■ Ja	☐ Nej

Svar: Det är ingen större skillnad. Den största skillnaden är att olika tekniska verktyg används. Det beror bland annat på om en android eller en iphone undersöks.

6. Vid ett beslag av mobiltelefoner finns det riktlinjer angående hur information som finns lagrad på SIM-kort och på själva telefonen ska hanteras. Information kan även finnas lagrad på servrar. Om servern finns i Sverige blir exempelvis LEK tillämplig. Det finns dock inga lagregler som blir tillämpliga om informationen finns lagrad på en server utomlands. Finns det några riktlinjer för åklagare och poliser om hur en mobiltelefon som innehåller elektronisk information som finns lagrad på en server utomlands ska behandlas? Om det finns riktlinjer, vad innebär dessa?

■ Ja	☐ Nej

Svar: Ja. Lagstiftningen i det land där servern finns ska tillämpas. Domstolen i det landet bedömer om materialet kan lämnas ut till de svenska myndigheterna. Om en server finns utomlands begärs rättslig hjälp via konventioner eller avtal. Det är inte tillåtet att tömma en server som finns utomlands med hjälp av en kod eller ett verktyg som finns tillgängligt i Sverige. Detta anses dock tillåtet i Belgien.

[201] Ett samlingsnamn på stället där utredningsmaterial som inte tagits med i förundersökningsprotokollet hamnar.

Mellan Sverige och USA finns ett avtal som innebär att svenska myndigheter kan vända sig direkt till amerikanska server providers för att få tillgång till information. Oftast brukar dock de amerikanska server providers vilja att svenska myndigheter har ett amerikanskt domstolsbeslut innan de lämnar ut information.

7. Hur skulle du behandla en mobiltelefon som innehåller elektronisk information som finns lagrad på en server utomlands?

Svar: Söka internationell rättshjälp.

8. Har du någon gång beslagtagit en mobiltelefon som haft elektronisk information lagrad på en server utomlands?

☐ Ja, hela tiden ☐ Ja, händer ganska ofta

■ Ja, någon enstaka gång ☐ Nej, aldrig

Svar: Det händer sällan. När det händer är det oftast e-postbrevlådan som lagrats utomlands. Det är vanligare att information i datorer är lagrade på servrar utomlands.

9. Är det tillåtet att låta en beslagtagen mobiltelefon stå påslagen för att åklagare/polis ska kunna läsa av senare inkomna meddelanden? Motivera ditt svar.

☐ Ja ■ Nej

Svar: Nej det är inte tillåtet. De meddelanden som inkommer efter beslagsundersökningen är att anses som under befordran. För att ta del av meddelandet kan hemlig avlyssning av elektronisk kommunikation användas. Helst ska telefonen stängas av eller försättas i flygplansläge. Detta beror på att innehållet i mobiltelefonen kan förändras. Information kan exempelvis fjärraderas.

10. Säkerhets- och Integritetsskyddsnämnden har gjort en undersökning bland åklagare (Rapport 2011-09-06) om hur textmeddelanden som inkom efter första beslagsundersökningen behandlades. Känner du till denna undersökning?

☐ Ja ■ Nej

Svar: Nej, inte denna undersökning.

11. Säkerhets- och Integritetsskyddsnämnden ansåg att åklagarnas hantering av inkomna textmeddelanden efter första beslagsundersökningen varierade kraftigt. Har det skett några förändringar för att göra rättstillämpningen mer enhetlig? Om det skett förändringar, vad innebär dessa förändringar?

☐ Ja ☐ Nej

Svar: Rättsläget är inte oklart eftersom det finns information om hur situationen ska hanteras inom åklagarväsendet. I praktiken är dock många osäkra på hur de ska använda reglerna som förespråkas av åklagarväsendet.

12. Övriga kommentarer.

Svar: Det som är problematiskt med att information lagras på servrar är att det oftast är oklart var någonstans servern finns.

I Europarådes konvention om IT-relaterad brottslighet finns regler om att brottsutredande myndigheter kan ta del av information om den misstänkte eller den som innehar informationen samtycker till detta. Då närvarar de vid en undersökning och så frågar utredarna om de får kolla på vissa dokument. Detta kan vara problematiskt om den som närvarar känner sig pressad att låta utredarna studera dokumenten. Det är en helt annan sak om de som närvarar vill att utredarna ska kolla på vissa dokument för att visar att de är oskyldiga. I USA finns även samtyckesblanketter som de som drabbas för beslaget skriver under. Det finns inte i Sverige.

EU-domstolens ogiltigförklarande av Datalagringsdirektivet är katastrofalt. Detta gör det mycket svårare att ta del av information vilket leder till att det blir svårare att utreda brott. Bland annat blir det svårare att ta fast pedofiler. Tidigare har privata leverantörer sparat uppgifter i två år för att de ska kunna fakturera kunderna. I och med direktivet minskade de flesta leverantörer lagringen av trafikuppgifter till sex månader. Många verkar tro att trafikuppgifterna lagras på en server hos svenska myndigheter vilket inte stämmer. Uppgifterna lagras hos privata företag och myndigheter kan endast ta del av uppgifterna om de har betydelse för en viss utredning av att visst allvarligt brott. En diskussion som helt gått förbi i Sverige är att det inte är relevant huruvida direktivet är giltigt eller inte, utan det viktiga är att pröva om den svenska lagen är giltig eller inte.

Käll- och litteraturförteckning

Offentligt tryck

Proposition

Prop. 2002/03:74	Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering
Prop. 2002/03:110	Lag om elektronisk kommunikation m.m.
Prop. 2010/11:46	Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG

Statens offentliga utredningar

SOU 1970:47	Skydd mot avlyssning
SOU 1976:36	Anonymitet och tvångsmedel
SOU 1984:54	Tvångsmedel, anonymitet och integritet
SOU 1992:110	Information och den nya InformationsTeknologin
SOU 1995:47	Tvångsmedel enligt 27 och 28 kap. RB samt polislagen
SOU 1996:40	Elektronisk dokumenthantering
SOU 2001:28	Yttrandefrihetsgrundlagen och Internet
SOU 2002:18	Personlig integritet i arbetslivet
SOU 2005:38	Tillgång till elektronisk kommunikation i brottsutredningar m.m.
SOU 2007:22	Skyddet för den personliga integriteten
SOU 2008:3	Skyddet för den personliga integriteten
SOU 2011:45	Förundersökning – objektivitet, beslag, dokumentation m.m.
SOU 2012:44	Hemliga tvångsmedel mot allvarliga brott
SOU 2012:55	En översyn av tryck – och yttrandefriheten
SOU 2013:39	Europarådets konvention om it-relaterad brottslighet

Departementsserien

Ds 1994:51	Skyddet för enskilda personers privatliv
Ds 2005:6	Brott och brottsutredning i IT-miljö

JK-beslut

Dnr 3954-99-40	Skadeståndsanspråk med hänvisning till ifrågasatt husrannsakan samt beslag av datorutrustning
Dnr 2806-00-21	Klagomål mot en åklagare med anledning av att denne beslagtagit och kopierat ett videoband tillhörande ett TV-bolag
Dnr 6372-07-31	Beslag av en dator hos en person med anknytning till ett medieföretag

JO ämbetsberättelser

2007/08 s. 160	Initiativärende beträffande den s.k. razzian mot Internetsajten The Pirate Bay
2009/10 s. 80	Den s.k. beslagsförbudsregelns tillämplighet beträffande elektroniska handlingar
2011/12 s. 141	Kritik mot att ett beslag ägt rum hos en advokat samt uttalanden om ett beslut att inleda förundersökning för skyddande av brottsling

Övrigt

Beslag: En handbok, 2013	Åklagarmyndigheten och Ekobrottsmyndigheten
Rapport 2011-06-09	Säkerhets- och Integritetsskyddsnämnden
ÅM-A 2006/1152	Tillsynsärende – Riksåklagaren

Artiklar

Abrahamsson, Olle; ”Integritetsskydd med eller utan förnuft”, *Svensk Juristtidning*, 2009 s. 421-434.

Axberger, Hans-Gunnar; ”Integritetsskydd i perspektiv”, *Svensk Juristtidning*, 2009 s. 468-482.

Eriksson, Anders; ”Några ord om reformbehovet i den lagstiftning som rör tvångsmedel m.m.”, *Svensk Juristtidning*, 2007 s. 130-135.

Lindberg, Gunnel; ”Straffprocessuella tvångsmedel – några utvecklingslinjer”, *Svensk Juristtidning*, 2007 s. 50-58.

Ramberg, Anne; ”Tvångsmedel, rättssäkerhet, integritet – går det att förena?”, *Svensk Juristtidning*, 2007 s. 154-170.

Strömholm, Stig; ”Integritetsskyddet”, *Svensk Juristtidning*, 1971 s. 695-736.

Svensk Juristtidning; 2007 s. 1-180.

Träskman, Per Ole; ”Brottsligheten och dess bekämpande – en reflektion om hot och hotbilder”, *Svensk Juristtidning*, 2007 s. 101-121.

Litteratur

Bring, Thomas, Diesen, Christian; *Förundersökning*, uppl 4, 2009, Norstedts Juridik AB, Stockholm.

Bryman, Alan; *Samhällsvetenskapliga metoder*, uppl 2, 2011, Liber AB, Malmö.

Danelius, Hans; *Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*, uppl 4, 2012, Norstedts Juridik AB, Stockholm.

Fitger, Peter, Sörbom, Monika, Eriksson, Tobias, Hall, Per, Palmkvist, Ragnar & Renfors Cecilia, Rättegångsbalken (oktober 2013, Zeteo), kommentaren till 27 kap. 12§.

Hjertstedt, Mattias; *Tillgången till handlingar för brottsutredare: en rättsvetenskaplig studie av beslag med husrannsakan, myndigheters utlämnandeskyldighet samt editions- och exhibitionsplikt*, 2011, Iustus Förlag AB, Uppsala. Skrifter från juridiska institutionen vid Umeå universitet, Nr 25.

Kronqvist, Stefan; *Brott och digitala bevis: en handledning*, uppl 3, 2013, Norstedts Juridik AB, Stockholm.

Lehrberg, Bert; *Praktisk juridisk metod*, uppl 6, 2010, Institutet för Bank- och Affärsjuridik AB, Uppsala.

Lindberg, Gunnel; *Straffprocessuella tvångsmedel: när och hur får de användas?*, uppl 3, 2012, Karnov Group Sweden AB, Stockholm.

Sandgren Claes; *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*, uppl 2, Nordstedts Juridik AB, Stockholm, 2007.

Internetkällor

Dagens Juridik. Hämtad den 2014-04-16. http://www.dagensjuridik.se/2014/04/chefen-rikskriminalen-till-angrepp-mot-eu-domstolens-beslut-om-datalagringsdirektivet.

Dagens Juridik. Hämtad 2014-04-24. http://www.dagensjuridik.se/2014/04/mp-kraver-stopp-datalagring-efter-eu-domstolens-dom-men-regeringen-vill-vanta.

Dagens Juridik. Hämtad 2014-05-03. http://www.dagensjuridik.se/2014/04/utredare-ska-analysera-svensk-ratt-utifran-eu-domstolens-upphavande-av-datalagringsdirektive.

Nationalencyklopedin. Sökord – Integritet. Hämtad 2014-03-03. http://www.ne.se.ludwig.lub.lu.se/sok?q=integritet

Nationalencyklopedin. Sökord – Mobiltelefon. Hämtad 2014-04-03. http://www.ne.se/enkel/mobiltelefon

Nationalencyklopedin. Sökord – Smartmobil. Hämtad 2014-04-03. http://www.ne.se/lang/smartmobil.

Stiftelsen för Internetinfrastruktur. *Svenskarna och internet 2013*. Hämtad 2014-04-03. http://www.soi2013.se/.

Otryckt källa

Tibbling, Jan, Kammarrättsåklagare Ekobrottsmyndigheten Stockholm, telefonintervju, 2014-04-28.

Rättsfallsförteckning

EU – domstolen

EU-domstolens dom den 8 april 2014 i de förenade målen C-293/12 och C594/12 Digital Rights Ireland Ltd mot Minister for Communications, Marine and Natural Resources m.fl. och Kärntner Landesregierung m.fl. (Ännu inte publicerad i REU.)

Europadomstolen

Wieser och Bicos Beteiligungen GmbH mot Österrike den 16 oktober 2007, appl. 74336/01.

Högsta domstolen

NJA 1988 s. 471
NJA 1998 s. 829