JURIDISKA FAKULTETEN
vid Lunds universitet

Carl Skårman

Husrannsakan & beslag
-säkring av digitala bevis

Examensarbete
20 poäng

Handledare
Per Ole Träskman

Ämnesområde
Processrätt

VT 2007

Innehåll

Summary

When investigating crime, police and other investigating officials have the ability to perform searches of premises and seize certain objects. These are important measures to enable the police to gather information and evidence for crime investigations. The purpose of this thesis is to give an overlooking view of the legislation regulating search and seizure to see if the rules are well suited for measures in purpose of gathering digital evidence. Society today is in many ways dependant of Information Technology (IT). The vast spread of computers and the impact of Internet has created new channels for large quantities of information to spread between a large number of people. All this without the obstacles of national boundaries or geographical distances. Information technology is no longer considered as a new form of technology. However it still evolves and undergoes constant changes. In a world where technology seems to reach new landmarks every day, law has a tendency to fall behind of the developing changes. In order to achieve a legislation that doesn't become inadequate as the technology is evolving, legal rules must give a certain expression of neutrality towards the technology they are intended to govern. However, translating technical circumstances and definitions into legal rules has shown to be much difficult task.

The vast spread of computers within today's society has not only contributed to new crimes, usually called cybercrimes such as computer infringement in the Swedish criminal code chapter 4 paragraph 9, but has also led to traditional crimes performed in new ways where computers and other technical devices are used when crimes are committed. The last being some form of computer related crime where the use of computers and technical devices may be of major importance for completing the crimes or in some cases it might only play a minor role. In Sweden this type of crime has increased with 55 % since the year of 1995. As many traditional crimes nowadays are committed in untraditional environments, the crime investigating governments are forced to adapt their measures for fighting and investigating crime.

When investigating severe crimes the police often perform a search in order to seize computers or other electronically devices with digital technology. Computers and such technical devices can hold and produce vast quantities of digital information which can be of importance for a crime investigation. In the same way as computer technology has created new forms of crime, it has also contributed new forms of evidence, namely digital evidence. Digital evidence are any evidence that could be produced or held by some sort of electronically device. Hence, digital evidence often result in more detailed and thorough investigations than investigations that only consists of traditional evidence.

The Swedish legislation of search and seizure was passed in the early 20th century, why the legal rules hardly was intended to be applied in the purpose of gathering digital evidence. Because of this, crime investigations in purpose of gathering digital evidence has been a widely debated subject over the past decades. Even if there has been some proposals, it has not led to any changes of the legislation governing search and seizures. Many of the problems that has been discussed therefore remain unsolved.

When performing a search or a seizure it is of elementary importance that the measures are being carried out with support of the regulating legislation. Having a legislation which isn't in conformity with the technology of today results in measures being carried out with out any legislation, supporting the taken measures. When measures are carried out in digital environments it is also hard to predict the impacts of measure. The digital evidence can not be seen when stored on a hard drive why one might have to seize the device or perform searches that might take a long time. This may lead to damages and infringements that aren't proportional to the effect of the measure taken.

In means of a suspicion of a committed crime being committed, it doesn't take much for the investigating official to be able to perform a search and seizure. Hence, the measures can be widely applied. Also there are no specific rules governing how a search is to be performed. The wide spread of computers has resulted in information more often is stored digitally. This could be any kind of information but in many cases the information can consist of details which are threatening a person's integrity. As an example the digital evidence can be sent or received emails or certain information which is protected by secrecy.

To ensure that the executive authorities are considering this integrity when measures are carried out in digital environments, I believe it being of great importance for the governing principles of legality, means, need and proportionality to be considered not only when deciding upon and carrying out searches of the premises where the digital device is situated. In my opinion the considerations also need to be taken into account when performing the search of the device itself. This means that digital devices would get the status of a closed safekeeping ("slutet förvaringsställe 28 kap. 1 § RB). If a warrant is needed to perform a search of a digital device the mentioned principals would more likely be taken into account.

The problems that occur with search and seizures in digital environments leads up to question whether these measures are inadequate for these purposes. Threats of a more organised and severe criminality are already circumstances which gives reasons for more effective ways of fighting crime. Perhaps technology might be another circumstance which leads to new measures for investigating and fighting crime. Already there has been a suggestion to allow the executing authorities to perform secret readings of peoples computers. Although the suggestion was overthrown it is likely that such measures are to be considered again.

Sammanfattning

I det brottsutredande arbetet att inhämta information och säkra bevisning utgör straffprocessuella tvångsmedel viktiga inslag. Av de tvångsmedel som används i bevissäkrande syfte är förmodligen husrannsakan och beslag de vanligaste förekommande. Det övergripande syftet med uppsatsen är att ge en redogörelse över tillämpningen av åtgärder i form av beslag och husrannsakan för att samla in bevis för, och utröna omständigheter kring, brottsutredningar i digital miljö. Samhället är idag till stora delar helt beroende av Informationstekniken (IT). Dagens datortäthet och kanske framförallt Internet har bidragit till att och öppnat nya vägar för att sprida stora mängder information till ett stort antal personer utan eventuella hinder i form av geografiska avstånd eller nationella gränser. I dagsläget benämns IT knappast längre som den nya tekniken men trots detta är den alltid förnyande och ständigt under utveckling. I en värld där tekniken ständigt vinner nya landmärken kan juridiken få det svårt att följa utvecklingen. För att få en lagstiftning som inte riskerar att bli inaktuell i takt med att tekniken utvecklas och som till fullo reglerar IT-området, måste bestämmelserna präglas av en viss neutralitet gentemot den teknik som de avser reglera. Det har dock visat sig svårt att överföra tekniska omständigheter och begrepp till juridiska bestämmelser.

Datoriseringen i samhället har inte enbart skapat nya brott, som exempelvis kriminaliseringen av datorintrång i BrB 4 kap 9 c §, utan även medfört att traditionella brott idag utförs i nya former där man i större eller mindre utsträckning använder sig av datorer eller andra tekniska hjälpmedel för att genomföra brottet. Man kan tala om en IT-relaterad brottslighet i dess bredaste definition där brottsligheten sker i en datormiljö eller med hjälp av datorteknik. Sedan år 1995 har denna typ av brott ökat med 55 %.[1] Eftersom flera traditionella brott numera utförs till stor del i en otraditionell miljö har de brottsutredande myndigheterna varit nödgade att anpassa sina metoder för att bekämpa och utreda brottslighet.

Vid utredningar av grov brottslighet har det blivit vanligt att polisen vid en husrannsakan tar datorer i beslag för att söka efter bevisning som kan styrka misstanken om brott. Datorer och andra informationsbärare kan producera och innehålla mängder av digital information som kan vara relevant för en förundersökning. Bortser man från att informationstekniken har bidragit till en mer avancerad form av brottslighet, har den även skapat helt nya former av bevisning. Denna bevisning kan samlas under benämningen digitala bevis och kan utgöras av alla sorters bevis som kan tänkas lagras på eller produceras utav någon sorts elektronisk utrustning. Tillgången till digital bevisning kan ofta resultera i att man får ett större underlag för förundersökningen i jämförelse med de utredningar där man endast har tillgång till traditionell bevisning.

[1] BRÅ-Rapport 2000:2, IT-relaterad brottslighet s. 7.

När reglerna om husrannsakan och beslag infördes var avsikten dock inte att dessa tvångsmedel skulle komma att tillämpas i syfte att säkra digitala bevis. Detta har lett till att det under de senaste åren presenterats många förslag på lagändringar i flera olika utredningar som behandlat brottsbekämpning och brottsutredningar i digitala miljöer. Förslagen har dock inte föranlett några lagstiftningsåtgärder varför många frågor fortfarande står olösta. En grundläggande förutsättning för att vidta åtgärder i form av straffprocessuella tvångsmedel är att dessa åtgärder har stöd i lag. Med en lagstiftning som knappast kan anses vara anpassad till dagens teknik måste det ifrågasättas huruvida lagstiftningen ger uttryck för och berättigar åtgärder som vidtas i digitala miljöer. Ett annat problem med åtgärder i digitala miljöer är att det är svårt att på förhand kunna förutse omfattningen av åtgärderna. De digitala bevisen är inte direkt synliga då de ligger lagrade på någon form av elektronisk utrustning och för att säkra bevisningen kan det krävas omfattande beslag eller undersökningar. Detta kan leda till skador som kan vara oproportionella i förhållande till den nytta som åtgärderna medför.

För att de brottsutredande myndigheterna skall få vidta en husrannsakan krävs inte mer än att det förekommer anledning om att ett brott har förövats som kan leda till ett fängelsestraff. För att ett föremål skall få tas i beslag krävs det endast att det föreligger en misstanke om brott. Dessa tvångsmedel har alltså ett tämligen omfattande tillämpningsområde. Till detta tillkommer att det inte finns några särskilda bestämmelser över tillvägagångssättet för genomförandet av en husrannsakan. Den utbredda datoriseringen medför att information i allt större utsträckning lagras i digital form. Denna information kan utgöras av allsköns slag men är inte helt sällan information av integritetskänslig natur. Det kan exempelvis röra sig om korrespondens i form av e-post eller handlingar som omfattas av sekretesskydd.

För att tillse att åtgärder som vidtas i digitala miljöer inte skall komma att få en orimlig skadeverkan, både vad gäller rena förmögenhetsskador som skador vilka kan hänföras till kränkningar av den personliga integriteten, är det av stor vikt att de grundläggande principerna om legalitet, ändamål, behov och proportionalitet kan iakttagas vid beslutsfattandet och verkställigheten av åtgärder i digitala miljöer. Ett sätt att tillse detta är enligt min mening att jämställa digital utrustning med sådana *slutna förvaringsställen* som kräver ett särskilt beslut om husrannsakan för att få undersökas.

De betänkligheter som uppstår med anledning av teknikens utveckling leder även till frågan huruvida dagens regler om straffprocessuella tvångsmedel är tillräckliga när det handlar om att vidta åtgärder i digitala miljöer. En utvidgning av användningen utav tvångsmedel har redan genomförts i syfte att få en effektivare bekämpning av en brottslighet som framställs som allt grövre och mer organiserad. Att det i framtiden införs nya tvångsmedel som är ämnade för att säkra just digitala bevis är kanske därför inte helt otänkbart. Ett förslag om införandet av ett tvångsmedel som skulle medföra

att de brottsutredande myndigheterna skulle kunna bereda sig tillträde till datorer i hemlighet har redan varit uppe för behandling. Även om förslaget blev hårt kritiserat är det inte otänkbart att utvecklingen leder till att liknande förslag tas upp igen. I så fall är det enligt min mening av särskild vikt att hålla i åtanke de integritets aspekter som följer med digitala miljöer.

Förkortningar

BrB	Brottsbalken
BRÅ	Brottsförebyggande rådet
EKMR	Europeiska konventionen om de mänskliga rättigheterna och grundläggande friheterna
FuK	Förundersökningskungörelsen
IT	Informationsteknologi
LEK	Lagen (2003:396) om elektronisk kommunikation
RB	Rättegångsbalken
RF	Regeringsformen

1 Inledning

1.1 Syfte

Det övergripande syftet med uppsatsen är att ge en redogörelse över tillämpningen av åtgärder i form av beslag och husrannsakan för att samla in bevis för, och utröna omständigheter kring, brottsutredningar i digital miljö. Reglerna om husrannsakan och beslag stiftades i början av 1900-talet och var då knappast ämnade att tillämpas på dagens tekniska förutsättningar. Med ledning av det övergripande syftet kan följande frågeställningar aktualiseras.
Är dagens lagregler om husrannsakan och beslag väl anpassade till den digitala tekniken? Kan man alltså finna stöd i lagtexten för de åtgärder som praktiskt genomförs för att säkra bevis i digital miljö. Detta kräver en översyn kring reglerna om husrannsakan och beslag där åtgärderna som vidtas i digitala miljöer måste ses i ljuset av de allmänna principer och rättighetsskydd som utgör grundläggande förutsättningar för användningen av tvångsmedel.

I takt med att tekniken utvecklas blir det allt vanligare att tekniska hjälpmedel används i samband med utförandet av brott och brottslig verksamhet. Med anledning av detta är det även av intresse att fråga sig huruvida möjligheterna till säkring av digitala bevis genom husrannsakan och beslag är tillräckliga som medel. Krävs det en utvidgad tvångsmedelsanvändning eller andra åtgärder för att få en brottsutredande verksamhet som är mer anpassad till dagens teknik? I denna del blir det alltså närmast en diskussion i ett *de lege ferenda* perspektiv. För Sveriges del kan man se den närmaste framtiden utgöras av införlivandet av den konvention[2] som Europarådet antagit gällande IT-relaterad brottslighet och EU:s direktiv[3] om skyldighet för operatörer att lagra trafikuppgifter. Dessa två rättsakter kommer troligtvis att medföra stora förändringar när det handlar om de brottsutredande myndigheternas möjligheter till att säkra digital bevisning. Ser man till framtiden i ett längre perspektiv kan man tänka sig en teknikutveckling med en allt större datortäthet där man inte längre har flera olika medier för olika funktioner utan istället ett integrerat informationsmedium som kan utföra flera funktioner. Som exempel kan nämnas Internettelefonin som idag är relativt väletablerad. Det nyligen presenterade förslaget om ett nytt hemligt tvångsmedel i form av hemlig dataavläsning skulle kunna få en central betydelse i en sådan framtid.

För att besvara dessa frågeställningar måste hänsyn tas till samtliga delar av tillämpning, alltså tillståndsgivningen och verkställigheten av beslutet om

[2] Convention on Cybercrime, ETS no. 185.
[3] EU direktiv 2006/24/EG.

tvångsmedel samt hanteringen av den information som framkommit genom åtgärden.

1.2 Avgränsningar

Den senaste tiden har det presenterats flertalet utredningar som har haft någon anknytning till brottsbekämpning i IT-miljö. Regleringen av straffprocessuella tvångsmedel är också ett aktuellt ämne som varit föremål för vida diskussioner. Detta gäller kanske framförallt diskussionen kring en utvidgad tvångsmedelsanvändning där bekämpningen av en alltmer organiserad och gränsöverskridande brottslighet ställs mot intressena av att ha ett samhälle som präglas av öppenhet och grundläggande friheter.

Med detta i åtanke och med anledning av det begränsade utrymmet som uppgiften erbjuder har det känts särskilt viktigt begränsa omfattningen av vissa av uppsatsens beskrivande delar. Arbetet har därför avgränsats genom att endast ta sikte på de straffprocessuella tvångsmedlen husrannsakan och beslag och betydelsen som de har när det kommer till säkring av bevis i digital miljö. Den presentation som sker utav andra åtgärder än husrannsakan och beslag, som kan bli aktuella för bevissäkring i digital miljö, är främst avsedd för att huruvida ingripanden genom husrannsakan och beslag kan anses utgöra en tillräcklig reglering för behovet av ingripanden i digital miljö. Huvuddelen av arbetet är således koncentrerat kring reglerna om husrannsakan och beslag varför andra åtgärder endast fått en begränsad omfattning.

Med anledning av att arbetets natur har det även varit nödvändigt att avgränsa omfattningen av de rent tekniska aspekterna i arbetet. Dessa avgränsningar och mer om de tekniska förutsättningarna för arbetet redovisas i kapitel två.

1.3 Metod

Det skall nämnas att detta är en juridisk uppsats och att den inte gör anspråk på att vara ett tvärvetenskapligt arbete. Trots detta har jag med anledning av min begränsade kunskap inom det tekniska området varit tvungen att använda vissa källor som inte är juridiska. Det har främst varit påkallat när det kommer till innebörden av vissa tekniska begrepp och omständigheter. När delar av arbetet har krävt viss datateknisk kunskap utöver min grundläggande användarnivå har jag valt att använda mig av de möjligheter till informationsinsamling som tekniken erbjuder. Som informationskälla är Internet ett överlägset verktyg varför jag valt att utnyttja möjligheterna som erbjuds för att komma åt information. Såsom alltid, när det kommer till att anpassa lagstiftning till modern teknik, måste man beblanda sig med tekniska begrepp som kan vara i behov av ytterligare förklaring för läsarens

intresse. Således har jag till stora delar använt mig av Internet som källa för förklaringar av tekniska aspekter och begrepp.[4]

I övrigt har genomförandet av arbetet skett med en traditionell juridisk metod. Det innebär att svaren på de valda frågeställningarna har sökts i såväl lagtext som förarbeten, praxis och doktrin. En stor del av materialet till arbetet utgörs av de utredningar och lagförslag som behandlar anpassningen till IT-utvecklingen. Trots det stora antalet utredningar är det få lagförslag som har resulterat i lagstiftning varför jag främst har valt att koncentrera framställningen kring de senaste förarbetena och utredningarna. Från det offentliga materialet har jag även haft stor användning av de yttranden och beslut från Justitiekanslern och Justitieombudsmännen som har behandlat området.

När det gäller regleringen kring straffprocessuella tvångsmedel har Gunilla Lindbergs bok, ”Straffprocessuella tvångsmedel – när och hur får de användas”, varit av stor betydelse för arbetet. Även Stefan Kronqvist framställning, ”Brott och digitala bevis – En handledning”, har varit av stor nytta när det kommer till samverkan mellan juridiken och tekniken.

1.4 Disposition

Som alltid när man saknar kunskap inom ett område är det viktigt att klargöra vissa grundläggande begrepp för att få en klar bild av sammanhanget. När man befattar sig med de utredningar som presenteras på området för informationsteknik (IT) är det dock lätt hänt att man går vilse i en djungel av olika tekniska termer och begrepp. Samtidigt påpekas vikten av att skapa en teknikneutral lagstiftning för att anpassa reglerna till tekniken. För att inte skapa oklarheter kring de tekniska områdena och begreppen i detta arbete inleds uppsatsen med ett kapitel som behandlar just de tekniska förutsättningarna och innebörden av vissa tekniska begrepp. Här ges bl.a. en närmare förklaring över innebörden av digitala bevis. I kapitel tre följer därefter en översikt över de allmänna reglerna och principerna gällande straffprocessuella tvångsmedel. I kapitel fyra och fem ges en redogörelse för reglerna om beslag och husrannsakan. Här behandlas även de särskilda frågor som uppstår när åtgärder i form av dessa tvångsmedel genomförs i digital miljö. Kapitel sex berör uppgifter om elektronisk kommunikation och den övergripande lagstiftningen på området. I kapitel sju diskuteras vissa lagförslag som presenterats under den senaste tiden och som skulle innebära en utvidgad tvångsmedelsanvändning. Avslutningsvis analyserar jag i kapitel åtta vad som framkommit i mitt arbete.

[4] Här kan nämnas de möjligheter som Internet erbjuder i form av gratis uppslagsverk som exempelvis tillhandahålls genom Wikipedia http://sv.wikipedia.org/wiki/Portal:Huvudsida

1.5 Vissa begrepp

Som ett samlingsbegrepp för de myndigheter som beslutar och verkställer åtgärder i form av husrannsakan och beslag, dvs. polis och åklagare, har jag valt begreppet brottsutredande myndigheter. Annars är begreppet brottsbekämpande myndigheter en vanligt förekommande benämning men jag har valt att inte använda mig av denna då husrannsakan och beslag endast används i syfte att utreda brott och inte för att upptäcka brott.

Genomgående i denna uppsats används orden digital miljö. Med detta åsyftas miljöer som har något slags inslag av digital teknik. I vissa fall kanske åtgärden helt och hållet genomförs i digital miljö medan det i andra fall endast är ett litet inslag av digital teknik. En annan vanlig förekommande term i detta arbete är informationsteknologi (IT). Här avses begreppets vidaste definition vilket innebär att det omfattar såväl datateknik som telekommunikation och till och med hemelektronik. Även om datortekniken står i fokus för detta arbete finns anledning att inte avgränsa begreppet IT till att endast avse datorteknik. Datortekniken har öppnat upp vägar för integrering mellan olika typer av teknisk utrustning. En dator kan kommunicera med andra kommunikationsverktyg såsom fast telefoni och mobiltelefoni. Kommunikationen kan även ske på flera olika sätt, exempelvis röstsamtal, snabbmeddelande (sms), bild- och filöverföring eller e-post. Dessutom blir det allt vanligare att övrig teknisk utrustning innehåller datorteknik. Som exempel kan dagens mobiltelefoner erbjuda flera kommunikationsmöjligheter som tidigare varit förbehållna datorerna. I en verklighet där varje form av teknisk utrustning skall vara kompatibelt att kommunicera via Internet blir samtidigt verktygen för kommunikation allt fler. Att jag i detta arbete valt att ha datorn som utgångspunkt kommer sig därför främst av att jag önskat förenkla framställningen varför jag kanske endast använder mig av ordet dator eller i vissa fall datorutrustning.

2 Digitala bevis

2.1 Vad är digitala bevis?

Vi använder oss dagligen utav teknisk utrustning så som exempelvis datorer och mobiltelefoner. Denna användning resulterar i att en otrolig mängd digital information skapas. Under år 2006 producerades det i världen så mycket som 161 miljarder gigabyte digital information. Denna siffra kan tyckas svåröverskådlig men som en liknelse skulle man få ett dussintals travar av böcker som sträcker sig mellan jorden och solen om hela informationsmängden istället skulle befästas på papper.[5] Den stora mängd digitala informationen som produceras har även lett till att det börjar bli ont om kapacitet för att lagra all information. Anledningen till att det rör sig om så stora siffror kommer sig av naturen hos den digitala tekniken. När begreppet digital används i samband med information handlar det om information som uttrycks i form av siffror. Information som behandlas i datorer utgörs av siffror från det binära talsystemet. Det binära talsystemet är en representation för tal som har talbasen två vilket innebär att man endast använder sig av två siffror för att presentera information, ettor och nollor. Ettorna och nollorna ges olika värden beroende av deras position i det binära talet. Med hjälp av datorprogram kan information i form av ettorna och nollorna bearbetas och presenteras i olika utföranden och format, exempelvis ljud, bild, video eller textmassa. Uppbyggnaden med ettor och nollor medför vissa karaktäristiska särdrag som gör digital information särskilt användbar. Digital information kan nämligen framställas i exakta kopior och kan överföras utan att informationen påverkas. Detta till skillnad från analog information, exempelvis en fotokopia, där resultatet alltid påverkas vid varje överföring eller kopiering. Samtidigt gör uppbyggnaden av ettorna och nollorna det möjligt att utan större problem ändra eller radera den digitala informationen.

Således är det av mindre relevans att tala i termer om original och kopia när det handlar om digital information. Enkelheten att producera exakta kopior är dock en bidragande anledning till den stora mängd digital information som produceras världen om idag. En del av materialet utgörs endast av flyktiga kopior som aldrig sänds vidare eller lagras. Den totala mängden digitala information som produceras beräknas nämligen framställas i tre separata kopior.[6] Fenomenet kan delvis förklaras med detta arbete som utgångspunkt. Förutom att kopior framställs genom inmatning av manuella kommandon i datorn, skapar datorn även kopior av informationen per automatik. Läses detta arbete i annan form än i pappersutgåva utgör exempelvis den information som presenteras på datorns bildskärm en kopia

[5] NyTeknik publicerad 2007-03-06 16:19 http://www.nyteknik.se/art/49413 hämtad 2007-05-19
[6] NyTeknik publicerad 2007-03-06 16:19 http://www.nyteknik.se/art/49413 hämtad 2007-05-19

av en datafil som finns lagrad, antingen på hårddisken i läsarens egen dator eller på en dator någon helt annanstans om informationen har överförs via ett nätverk. Förutom denna framställda skärmbildskopia skapar datorn även som oftast en tillfällig säkerhetskopia av den aktuella fil som behandlas på datorskärmen. Skulle man dessutom välja att skriva ut filen skapas det även ny utskriftsfil. Således finns den aktuella filen sparad i tre olika exemplar på tre olika ställen i datorns hårddisk.

Förutom att digital information utan större besvär kan kopieras i exakta kopior är det även tämligen enkelt radera information som lagrats digitalt. Detta kan givetvis skapa bekymmer ur bevissäkringssynpunkt genom att viktig information kan komma att förstöras innan de brottsutredande myndigheterna hinner ingripa för att säkra informationen. Även om en lagrad fil i en dator kan raderas med ett enkelt musklick innebär det dock inte att informationen har utplånats helt och hållet. En datafil utgörs av samlad information som organiserats efter ett bestämt mönster, baserat utifrån det datorprogram som lagrat filen. En datafil som skapats med hjälp av ordbehandlingsprogrammet Microsoft Word lagras exempelvis i filformatet doc. Förutom den information som en datafil innehåller, finns det även tillägg till datafilerna som kallas för metainformation. Metainformation är uppgifter som visar exempelvis datum och tid för när en fil skapades, när den sparades sist och när den senast blev läst.[7] Sådana uppgifter kan vara av stor betydelse i en brottsutredningen för att ytterligare klarlägga omständigheter kring de digitala bevis som förekommer i utredningen. När man tar bort en fil från datorn markeras det lagringsutrymme som tidigare disponerats av filen och dess metainformation som ledigt utrymme. Då det inte sker någon egentlig överskrivning av informationen förrän ny information har lagrats på utrymmet som markerats som ledigt kan informationen från den borttagna filen i många fall rekonstrueras med hjälp av speciella verktyg. Däremot är det i vissa fall omöjligt att återskapa den metainformation som hänger samman med datafilen.[8] Om det inte är möjligt att se när filen skapades eller när den öppnades sist torde värdet av de säkrade digital bevisen kunna ifrågasättas. Att ifrågasätta digitala bevis ur bevisvärderingssynpunkt är dock något som ligger utanför syftet med denna uppsats varför jag inte kommer att behandla problemet närmare.

Digital bevisning kan tänkas delas in i sådan digital information som är skapad av användaren utav den tekniska utrustningen och sådan digital information som skapas automatiskt utav den tekniska utrustningen. Sådan digital information som skapas utav användaren själv, genom verkställningen av manuella kommandon i den tekniska utrustningen, kan både bestå utav information som i sig utgör brott, t.ex. bilder med barnpornografiskt innehåll, och även information som kan styrka en brottsmisstanke, t.ex. innehåll i skickade e-post meddelanden. Som följd av att datorn har fått en alltmer utpräglad roll som verktyg för kommunikation

[7] Willassen, Svein, Lov & Data nr 78 s. 35.
[8] Ibid.

och med anledning av att datortekniken numera ingår i andra kommunikationsverktyg skapas det även automatiskt en hel del digitala uppgifter som kan vara till nytta, främst för att stärka misstanken om brott. Vid en normal användning av t.ex. en persondator lämnas flera digitala spår som vanligtvis registreras helt utan användarens vetskap. Dessa kan vara av särskild vikt när det kommer till att utröna omständigheter kring ett brott eller för att ge stöd åt ett påvisat orsakssamband. De digitala spåren kan exempelvis utgöras av uppgifter om skickad och mottagen e-post, spår efter kopierade eller raderade filer, uppgifter om användningen av Internet, uppgifter om utförda utskrifter, tidsuppgifter om användningen av datorn och loggade uppgifter som visar vad, hur, när och av vem som utfört vissa åtgärder i ett datorsystem.

2.2 Digitala bevis och gällande rätt

I rättegångsbalken finns inga regler att finna som ger någon definition över, eller särskilt reglerar, bevis i digital form. Troligtvis skulle en sådan definition även vara överflödig då det i svensk rätt inte görs någon större åtskillnad mellan olika slags bevisning. Detta gäller i alla fall så länge man håller sig till den prövning av bevis som sker inför rätten. Begreppet bevis kan å sin sida innefatta en mängd olika element. Detta framgår av RB 35 kap 1 § där det anges att rätten skall pröva allt som förekommit i målet och därefter avgöra vad som är bevisat. Härmed fastslås även principen om fri bevisprövning, vilket innefattar såväl fri bevisföring som fri bevisvärdering. Enligt svensk rätt är alltså i princip alla bevis tillåtna.[9] Visserligen finns det i rättegångsbalken särskilda bestämmelser för bevis som presenteras på olika sätt. I 36 kap finns bestämmelser om vittne, i 37 kap regleras förhör med part och med målsägande som inte för talan, 38 kap handlar om skriftliga bevis och i 39 kap anges vad som gäller för bevisning som presenteras med hjälp av syn. Även om digitala bevis inte skiljer sig från övrig bevisning när det kommer till själva bevisprövningen så medför de karaktäristiska dragen hos bevis i digital form vissa betänkligheter när det kommer till att samla in, eller säkra bevisningen. Som framgår av detta arbete författades inte lagstiftningen om husrannsakan och beslag i syfte att åtkomma bevis i digital miljö.

Även om säkring av digitala bevis inte är något vidare omtalat ämne inom doktrinen har en definition av begreppet växt fram. Den digitala tekniken härrör från elektronik och information i digital form kan således inte enbart presenteras med hjälp utav datateknisk utrustning, dvs. datorer och annan teknisk utrustning som innehåller datateknik, utan även med hjälp av elektronisk utrustning. I vissa framställningar används därför begreppet elektroniska bevis medan andra använder sig av begreppet digital. Den normala uppfattningen är att digitala eller elektroniska bevis kan utgöras av all slags information som härrör från digitala tekniska miljöer, eller

[9] Vissa begränsningar uppställs dock, jmf 35 kap 14 § och 36 kap 3 § RB.

bearbetas och presenteras med hjälp av elektronisk utrustning.[10] Denna definition ger således ett väldigt omfattande tillämpningsområde vilket är viktigt att bära med sig genom denna uppsats. Även om det mestadels är datorer som åsyftas i denna uppsats när det hänvisas till den tekniska utrustningen kan tillvägagångssättet alltså som oftast även tillämpas på andra sorters teknisk utrustning.

[10] Kronqvist, Stefan, Brott och digitala bevis s. 15 (hädanefter Kronqvist).

3 Straffprocessuella tvångsmedel

3.1 Allmänt om straffprocessuella tvångsmedel

I polisens arbete att bekämpa och utreda brott ingår en hel del olika åtgärder för att samla in information och uppgifter. Informationen och uppgifterna skall ge stöd åt den förundersökning som bedrivs för att utreda det misstänkta brottet. Som ett särskilt led i detta arbete kan de brottsutredande myndigheterna tillgripa åtgärder i form av straffprocessuella tvångsmedel i syfte att säkra bevis under en förundersökning. Den huvudsakliga regleringen av straffprocessuella tvångsmedlen finns i rättegångsbalken (RB) men dessa bestämmelser kompletteras eller ersätts i vissa fall utav särskilda regler i vissa straffrättsliga författningar. Någon definition på vad som utgör ett tvångsmedel finns inte i RB.

Begreppet tvångsmedel får anses innebära sådana direkta ingripanden mot en person eller egendom som är ett led i myndighetsutövning och som dessutom utgör någon form av intrång i en persons rättssfär.[11] Det är dock inget krav på att ingripandet utförs med tvång gentemot den som drabbas av åtgärden. Vissa tvångsmedel, av särskild natur, utförs nämligen i hemlighet, utan att den som drabbas av åtgärden är medveten om ingripandet värför det inte kan sägas föreligga något inslag av tvång i själva ingripandet.[12] För att betraktas som tvångsmedel bör åtgärderna syfta till att åstadkomma ett konkret, och inte endast rättsligt, resultat. Dessutom måste åtgärden medföra synbara eller kännbara verkningar för den som berörs av åtgärden.[13] Avgränsningen av begreppet tvångsmedel får därmed närmast ske mot den delen av den brottsutredande verksamheten som endast består i ett informationssamlande som inte har inslag av synbara eller kännbara verkningar för en enskild. Denna gränsdragning är inte alltid så tydlig som kan önskas. Genom reglerna om husrannsakan och beslag har det skapats ett regelverk över befogenheterna för de brottsutredande myndigheterna att tvångsvis kunna säkra bevis. Däremot finns det inga bestämmelser som reglerar polisens rätt att samla information i allmänhet vilket kan leda till oklarheter huruvida man i vissa situationer är tvungen att tillämpa tvångsmedel eller inte.

Att ett tvångsmedel är av straffprocessuell karaktär följer av att åtgärden vidtas som ett led i ett straffrättsligt förfarande. Åtgärder som husrannsakan och beslag syftar exempelvis till samla in bevis till underlag för en förundersökning. De straffprocessuella tvångsmedlen kan därefter

[11] SOU 1995:47 s. 137.
[12] Lindberg, Gunnel – Straffprocessuella tvångsmedel; När och hur får de användas, Stockholm: Thomson Fakta, 2005 (hädanefter Lindberg).
[13] SOU 1995:47 s 178.

kategoriseras i olika grupperingar. Den vanligaste förekommande indelningen sker i tvångsmedel som riktar sig mot person (personella tvångsmedel) och tvångsmedel som riktar sig mot egendom (reella tvångsmedel). Ett annat exempel är att det sker en indelning där vissa tvångsmedel ses som momentala, vilket innebär att de avslutas inom en kortare tidsrymd i jämförelse med perdurerande tvångsmedel som kännetecknas av att åtgärden är mer bestående. I regel upphör de momentala tvångsmedlen automatiskt medan de perdurerande kräver ett särskilt beslut för upphörande.[14]

Användningen av tvångsmedel präglas alltid av en avvägning mellan den effektivitet som åtgärderna medför i brottsutredande syfte och den skada som följer av intrånget som åtgärderna innebär. I RB är de straffprocessuella tvångsmedlen indelade med utgångspunkt efter att de avser intrång i olika skyddade intressen. För att motverka kränkningar av dessa intressen krävs det en balans mellan en uttömmande och exemplifierande reglering för att motverka analogitolkningar av reglerna om de skulle bli föråldrade eller om reglerna inte täcker alla tänkbara situationer som tvångsmedlet kan komma att användas för. Eftersom dagens teknik ställer nya krav på de brottsutredande myndigheternas rutiner för att säkra bevis kan man i högsta grad ifrågasätta hur väl anpassat dagens regelverk egentligen är. Reglerna om husrannsakan och beslag var vid sin tillkomst knappast avsedda att tillämpas i situationer där man befattar sig med information i digital form. En användning av tvångsmedel i situationer som de inte är avsedda för kan vara beklagligt ur rättssäkerhetssynpunkt. Regler som inte ger tydliga och detaljerade beskrivningar utav de föreskrivna tvångsmedlen försvårar en tillämpning och kontroll av att åtgärderna företas i enlighet med de principer som hela systemet med tvångsmedel vilar på (se nedan). Det är dock närmast en omöjlighet att tillskapa ett tvångsmedelssystem där man enbart behöver ta hänsyn till fakta för att avgöra om förutsättningarna för användningen av ett tvångsmedel är uppfyllda. För att få en hel bild av verkan av ett tvångsmedel måste det även finnas ett visst utrymme för subjektiva bedömningar eftersom varje enskilt fall är unikt.[15]

3.2 Effektivitet och integritet

Användningen av straffprocessuella tvångsmedel präglas utav avvägningen mellan den effektivitet som kan uppnås genom åtgärden när det handlar om att utreda brott och den kränkning av den personliga integriteten som åtgärden kan medföra. Att straffprocessuella tvångsmedel överhuvudtaget tillåts följer av att det anses godtagbart att inskränkningar sker i enskildas integritet eftersom dessa är en följd av behovet att effektivt kunna bekämpa och utreda brottslighet. Denna dragkamp mellan å ena sidan allmänhetens, eller statens, intressen och å andra sidan den enskildes intressen kan följas långt tillbaka i tiden. Straffprocessuella tvångsmedel utgör otvivelaktigt

[14] Lindberg s. 6.
[15] SOU 1995:47 s. 153 f.

effektiva rättsmedel i de brottsutredande myndigheternas arbete. Utan åtgärder i form av husrannsakan och beslag hade polisen exempelvis haft mycket svårt att säkra bevis och information som kan utgöra stöd i en förundersökning. Att en åtgärd är effektiv när det kommer till att utreda brott behöver dock inte innebära att den är nödvändig.

För att få en tydligare bild utav avvägningen mellan dessa två intressen skall den närmare innebörden av begreppet integritet belysas något. Att ge en exakt definition över begreppet integritet är i det närmaste omöjligt. Även om man skulle kunna finna någon entydig definition skulle det vara till föga hjälp i praktiken eftersom det inte skulle leda till någon klarhet i vad som skall skyddas eftersom man måste ta hänsyn till de legitima motstridiga intressena som föreligger i varje situation.[16] Skall man något sånär ge en förklaring över begreppet får det anses ha ett samband med mänsklig värdighet och en rätt för enskilda att få sin personliga sfär respekterad. Således handlar personlig integritet i mycket om att få leva sitt eget liv med en minimal inblandning från myndigheter, allmänheten eller andra individer. Inom den juridiska doktrinen har begreppet integritet förklarats närmare genom att beskriva vissa typiska handlingar som innebär inskränkningar i den personliga integriteten. Dessa utgörs av 1) ingrepp i den enskildes personliga sfär, oavsett om detta sker fysiskt eller i annan mening, 2) insamlande av uppgifter om en persons privata förhållanden och 3) offentliggörande eller annan användning av uppgifter om en persons privata förhållanden.[17] En annan förklarande indelning av begreppet integritet framställdes av Tvångsmedelskommittén i samband med utredningens översyn av tvångsmedelsregleringen vid förundersökningen i brottmål. Indelningen tog sikte på de olika intressen som kan anses skyddsvärda:

- den rumsliga integriteten (hemfriden)
- den materiella integriteten (egendomsskyddet)
- den kroppsliga integriteten (skydd för liv och hälsa, kroppsvisitation, m.m.)
- den personliga integriteten i fysisk mening (skydd för den personliga friheten och rörelsefriheten)
- den personliga integriteten i ideell mening (skydd för personligheten och för privatlivet)[18]

Utformningen av dagens teknik och den snabba utvecklingstakten som sker på området har lett till särskilda betänkligheter vad gäller diskussionen om personlig integritet. Dagens teknik erbjuder avancerade möjligheter till avlyssning och lagring av uppgifter. Integritetsskyddskommittén menade att det föreligger två utvecklingslinjer där den första direkt syftar till en ökad kontroll, spårbarhet och övervakning av individer, medan den andra utgörs av tekniker som egentligen är harmlösa men som kan användas för andra

[16] SOU 2007:22 del I s. 52.
[17] Strömholm, Integritetsskyddet, ett försök till internationell lägesbestämning, SvJT 1971 s. 698.
[18] SOU 1984:54 s. 42 f.

integritetskänsliga syften.[19] Den andra kategorin utgörs exempelvis av sådana digitala spår (se ovan avsnitt 2) som lagras vid ett normalt användande av den tekniska utrustningen.

3.3 Rättighetsskyddet

3.3.1 Grundlagen

Till de mänskliga fri- och rättigheterna, som föreskrivs genom grundlagen, straffrättslig lagstiftning och konventioner, hör ett skydd för den privata sfären. Detta skydd uppställs bland annat i 2 kap. Regeringsformen (RF), som föreskriver skydd för olika mänskliga fri- och rättigheter som den enskilde är tillförsäkrad gentemot det allmäna. Grundlagen möjliggör dock även att dessa fri- och rättigheter får inskränskas genom lag i de fall ändamålet med inskränkningen kan anses godtagbart i ett demokratiskt samhälle. För att de brottsutredande myndigheterna skall kunna fullgöra sitt uppdrag har man ansett att användningen av straffprocessuella tvångsmedel och dess brottsutredande ändamål är godtagbar med hänsyn till den kränkning av de mänskliga fri- och rättigheterna som följer av åtgärderna.

I 2 kap 1 § RF föreskrivs vissa fri- och rättigheter som den enskilde är tillförsäkrad gentemot det allmäna. Av relevans för de straffprocessuella tvångsmedlen framgår det närmare i 2 kap 6 § RF att enskilda är skyddade mot angrepp såsom kroppsvisitation, husrannsakan eller liknande angrepp samt mot undersökning av brev och mot avlyssningar. Här uppställs alltså ett skydd som omfattar flertalet av de åtgärder som följer vid tillämpningen av vissa tvångsmedel, innefattat husrannsakan och beslag. Som tidigare nämnts har man dock tillåtit användandet av tvångsmedel i syfte att de brottsutredande myndigheterna skall kunna genomföra utredning, lagföring och verkställighet av påföljd för brott. Användandet av tvångsmedel legaliseras genom att själva syftet med användningen anses godtagbart i ett demokratiskt samhälle vilket innebär att lagliga regler får begränsa skyddet som uppställs i delar av RF.[20]

3.3.2 Europakonventionen

Genom Europakonventionen, som gäller som svensk lag, tillförsäkras ett ytterligare skydd för de mänskliga rättigheterna och de grundläggande friheterna. För denna framställning är det främst konventionens artikel 6 och artikel 8 som är utav intresse.

Artikel 6 behandlar rätten till domstolsprövning och en rättssäker process. I denna rättighet ligger ett krav på en rättvis rättegång (”fair trial”). Bestämmelsen tar bl.a. sikte på parternas likställdhet i processen (”equality

[19] SOU 2007:22 del I s. 67.
[20] Se 2 kap 12 § RF.

of arms”). I brottsmål genomsyrar principen processen på så sätt att den tilltalade måste ha samma möjligheter som åklagaren att utföra sin talan för domstolen. Artikeln förhindrar dock inte att den tilltalade i somliga fall ges en starkare ställning än åklagaren i processen. Så är exempelvis fallet med den grundläggande föresatsen att ett domslut skall vara den tilltalade fördelaktigt om det uppstår tveksamheter i skuldfrågan (”in dubio pro reo”).[21] Användandet av straffprocessuella tvångsmedel torde i praktiken medföra att den misstänkte får ett sämre utgångsläge i processen jämfört med åklagaren. Här har alltså intresset av att effektivt kunna bekämpa, utreda och lagföra brott vägt över intresset av att ha en helt likställd process. Ett viktigt inslag i rätten till en rättvis rättegång utgör kravet på att parterna har tillgång till allt processmaterial och att parterna får möjlighet att bemöta de bevis som läggs fram emot honom.[22] Detta kan medföra komplikationer när det handlar om just digital bevisning då det kan ställa krav på särskild utrustning för att presentera materialet.[23]

Artikel 8 i Europakonventionen innehåller bestämmelser om rätten till respekt för privat- och familjeliv, hem och korrespondens. Artikeln syftar främst till att ge ett skydd mot åtgärder som innebär ingrepp i de föreskrivna rättigheterna. Dessutom medför artikeln åläggande för staten att vidta positiva åtgärder i syfte att skydda den privata sfären för enskilda. För att uppfylla detta åläggande kan staten genom att stifta lagar och förordningar tillse att det finns ett tillfredställande skydd för privatliv, familjeliv, hem och korrespondens.[24]

En hel del företeelser kan tänkas falla in under rätten till respekt för privatlivet. En något sånär definition av innebörden av rättigheten kan endast framställas genom rättspraxis. Förutom rätten till respekt för privatliv ger artikel 8 även ett skydd för familjelivet samt för hem och korrespondens. Vid ett ingripande som medför en kränkning av någons privatliv tenderar även andra skyddsvärda intressen att påverkas, som exempelvis rätten till korrespondens och till hemmet. Som exempel innebär en husrannsakan inte bara ett ingrepp i respekten för hemmet utan även ett ingrepp i respekten för privatlivet.[25]

Som tidigare nämnts kan uppgifter om kommunikation utgöra ett viktigt inslag i myndigheternas brottsutredande arbete. Med ”korrespondens”, avses i Europakonventionen inte endast befordran av brev och andra försändelser med post utan även kommunikationer via telefon eller telegraf samt överförande av meddelanden med hjälp av datorer, exempelvis e-post.[26] Eftersom begreppet korrespondens innefattar de flesta olika typer av

[21] Danelius, Hans, Mänskliga Rättigheter i europeisk praxis; En kommentar till Europakonventionen om de mänskliga rättigheterna s. 194 f (hädanefter Danelius).
[22] Ibid. s. 202.
[23] Kronqvist s. 88f.
[24] Danelius s. 261.
[25] Ibid. s. 260 f.
[26] Ibid. s. 270.

kommunikation och då artikel 8 inte uppställer några tekniska krav torde skyddet för korrespondens därför kunna tillämpas på all kommunikation som kan befordras med hjälp av en dator.

3.4 Allmäna principer

3.4.1 Legalitetsprincipen

Legalitetsprincipen gäller för användningen av samtliga tvångsmedel och innebär i stort att en myndighet inte får ingripa i enskilds rättssfär utan stöd i lag. Principen kan härledas från regelverket i 1 och 2 kap. RF och kommer till direkt uttryck i 1 kap. 1 § 3 st RF där det anges att den offentliga makten skall utövas under lagarna. Som tidigare nämnts medför ett utövande av tvångsmedel inskränkningar i den enskildes rättssfär. Legalitetsprincipen medför att utövandet av tvångsmedel måste regleras i lag som medger den inskränkning som följer utav åtgärden.

Reglerna om husrannsakan och beslag var vid sin tillkomst knappast ämnade för att tillämpas för annat ändamål än att eftersöka och beslagta fysiska föremål. En tillämpning av regelverket på digitalt lagrad information kan därför leda till rättsliga betänkligheter, inte minst med tanke på legalitetsprincipen. I avsaknad av lagregler på området har det i praxis utvecklats metoder för användningen av tvångsmedel i digital miljö (se nedan kapitel 4.6). I det omfattande arbetet inom IT-området som presenterades av datastraffrättsutredningen[27] under 1990-talet, konstaterades det att det krävdes ett övergripande synsätt för digitalt lagrad information, grundat på principerna för IT, men att en särreglering på IT-området borde undvikas i möjligaste mån eftersom det skulle medföra gränsdragningsfrågor.[28] Varken utredningens, eller senare utredningars, förslag har dock lett till några ändringar i form av en anpassning av regelverket om husrannsakan till digitala miljöer.

3.4.2 Ändamålsprincipen

Ändamålsprincipen innebär att tvångsmedel endast får användas för de, i lagstiftningen, angivna ändamålen. I 2 kap. 12 § RF kommer principen till uttryck, där det anges att begränsningar i det rättighetsskydd som framställs genom RF endast får ske för sådana ändamål som är godtagbara i ett demokratiskt samhälle. Dessutom anges det att sådana begränsningar aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett begränsningen. Ändamålsprincipen kräver alltså att lagstiftningen kring varje tvångsmedel anger det eller de ändamål som tvångsmedlet får användas för. Som exempel får husrannsakan enligt huvudregeln användas för att eftersöka föremål som är underkastat beslag eller för att utröna

[27] SOU 1992:110.
28 Ibid. s. 343.

omständighet som kan vara av betydelse för utredningen av brottet. Det anses att nuvarande lagstiftning ger klara uttryck för att tvångsmedlen inte får användas för något annat ändamål än det beslutats för, varför det inte har ansetts behövligt med en uttrycklig lagfäst ändamålsprincip.[29]

Ändamålsprincipen kan anses vara överordnad behovs- och proportionalitetsprincipen, då prövningar som finner att ändamålet inte ligger inom tvångsmedlets tillämpningsområde medför att tvångsmedlet inte får användas. Först när ändamålet ansetts ligga inom tillämpningsområdet kan det prövas huruvida tvångsmedlet faktiskt behövs eller är proportionerligt med anledning av skadan som följer av åtgärden.[30] Förutom att principen iakttas vid ett beslut om att visst tvångsmedel skall vidtagas, skall principen även tillämpas vid verkställigheten av ett tvångsmedel på så sätt att man tillser att tvångsmedlet inte används för annat ändamål än det beslutats om. Det kan därför vara nödvändigt att förena ett beslut om tvångsmedel med villkor om hur beslutet skall verkställas.[31]

För åtgärder som vidtas i digitala miljöer får syftet främst anses vara att eftersöka och eventuellt beslagta utrustning som kan äga betydelse för utredningen eller i syfte att få uppgifter och information som kan utröna omständigheter kring ett brott. Som medel för informationssamling torde det, vid en husrannsakan eller genomsökningen av beslagtagen datorutrustning, vara specifika uppgifter, eller åtminstone uppgifter av visst slag, som eftersöks. Med anledning av de lagringsmöjligheter som erbjuds genom den digitala tekniken kan det inte vara oväntat att en eftersökning i datorer även kan resultera i att uppgifter, som ligger utanför ändamålet med åtgärden, skall komma att behandlas. Uppgifter som omfattar annat än syftet med åtgärden kallas överskottsinformation. I vissa fall kan en genomsökning resultera i uppgifter som rör nya brott vilka inte ligger till för de vidtagna åtgärderna. Överskottsinformation kan även utgöras av uppgifter av ren privat karaktär som överhuvudtaget inte är av intresse för i en utredning om brott. Användningen av överskottsinformation har främst diskuterats när det handlar om tvångsåtgärder i form av hemlig teleavlyssning. Av ovan nämnda skäl torde en sådan diskussion även kunna bli aktuell när man vidtar tvångsåtgärder i form av husrannsakan och beslag i digitala miljöer. Nyligen lagstiftades det, genom införandet av 23 a § i 27 kap RB, om användningen av överskottsinformation vid användningen hemlig teleavlyssning och hemlig teleövervakning. Av paragrafen framgår det att framkomna uppgifter om annat brott än det som legat till grund för beslutet om åtgärderna får användas för att utreda brottet om det för brottet är föreskrivet fängelse i ett år eller däröver, eller om det annars föreligger särskilda skäl. Har det förekommit uppgifter om ett förestående brott får dessa uppgifter användas för att förhindra brott. Hur rättsläget är med överskottsinformation som erhålles efter en husrannsakan eller beslag är kanske mer oklart. Visserligen är det föresatsen i svensk rätt att polisen fritt

[29] Prop. 1988/89:124 s. 27.
[30] Lindberg s. 20.
[31] Ibid. s. 22.

får använda sig av den information som man kommit över, oavsett på vilket sätt detta skett. Skulle man vid en husrannsakan komma över föremål eller information som tyder på annan brottslighet än den som åtgärden beslutats för, får husrannsakan även utökas till att även omfatta den nya brottsmisstanken.[32] Då överskottsinformationen kanske inte påträffas förrän efter det att åtgärden avslutats skulle det närmast handla om efterkonstruktioner. Att användningen av överskottsinformation till viss del gjorts laglig vid användningen av hemlig teleavlyssning och hemlig teleövervakning torde nog ändå tala för att sådan information som framkommer efter husrannsakan och beslag i digitala miljöer fritt kan användas. Av större intresse, främst ur integritetssynpunkt, är då kanske den överskottsinformation som utgörs av rent privata uppgifter som kan förekomma vid ingripanden genom husrannsakan och beslag i digitala miljöer.

3.4.3 Behovsprincipen

Behovsprincipen innebär att ett tvångsmedel endast får användas om det finns ett verkligt behov för tvångsmedlet samtidigt som det förväntade resultatet inte kan uppnås med mindre ingripande medel. Behovsprincipen innehåller alltså en viss proportionalitetsbedömning och kan sägas överlappa proportionalitetsprincipen till viss del. En annan viktig funktion av behovsprincipen är att användningen av ett tvångsmedel skall upphöra så snart syftet med det har uppnåtts eller om det på grund av andra skäl inte finns behov av det. Vid en husrannsakan kan det med tanke på behovsprincipen övervägas om innehavaren av ett visst eftersökt föremål kan väntas att frivilligt överlämna föremålet till polis eller åklagare.[33]

Som framgår av kapitel 5.6 finns det flera olika tillvägagångssätt för att säkra digital bevisning genom husrannsakan och beslag. Beroende på omständigheterna i den miljö som åtgärden skall utföras i kan det bli aktuellt med olika slags ingripanden. Med anledning av detta och kanske framförallt med tanke på de alternativ till husrannsakan och beslag som presenteras i kapitel 6 kan det tänkas att behovsprincipen är av särskild vikt när det handlar om säkring av digitala bevis.

3.4.4 Proportionalitetsprincipen

Proportionalitetsprincipen genomsyrar användningen av tvångsmedel på så sätt att arten och omfattningen av ingripandet måste stå i rimlig proportion till det resultat man önskar uppnå med åtgärden. Skälen för ingripandet måste således uppväga den skada och men som följer av användningen av tvångsmedel. Föreligger anledning att ett ingripande kan antas medföra större skada än vad som är rimligt kan en bedömning utifrån proportionalitetsprincipen leda till att man antingen väljer annat medel för

[32] Fitger, m.fl. Rättegångsbalken I, andra häftet s. 28:22 b (hädanefter Fitger).
[33] Lindberg s. 23.

ingripandet eller till att man helt avstår från ett ingripande.[34] För åtgärder enligt 27 kap. och 28 kap. RB finns numera, i respektive kapitel, lagregler som ger uttryck för proportionalitetsprincipen. Avvägning mellan skälen för åtgärden och skadan som följer därav skall inte endast påkallas när ett beslut fattas om ingripanden genom tvångsmedel utan måste även iakttagas vid själva verkställigheten av beslutet.

3.5 Samtycke

Som nämnts innebär tvångsåtgärder någon slags form av intrång i en persons rättssfär. För att åtgärden skall ses som ett tvångsmedel krävs det att den sker med direkt tvång eller åtminstone att den utförs i syfte att utgöra myndighetsutövning. Med ledning av detta kan det ifrågasättas om ett samtycke till sådana ingripanden medför att åtgärden inte skall betraktas som ett tvångsmedel då den inte kan anses utförd i strid mot den enskildes vilja. Åtgärder i form av husrannsakan och beslag utgör straffbara gärningar om de vidtas utan stöd i lag. Frågan är om ett samtycke kan befria från ansvar för sådana olagliga gärningar. På så sätt skulle en polisman kunna bereda sig tillträde till utrymmen och ta föremål i förvar utan att straffas för olaga intrång eller egenmäktigt förfarande. Skulle detta innebära att ett samtycke i så fall befriar från kravet att tvångsåtgärder endast får vidtas om de har uttryckligt stöd i lag? Även om en polisman inte skulle kunna hållas ansvarig för sådana åtgärder får det emellertid inte anses att åtgärden vidtagits inom polismannens befogenhet.[35] För husrannsakan finns en särskild bestämmelse i 28 kap. 1 § RB som reglerar samtycke. Här anges det att samtycke aldrig får åberopas som skäl för en husrannsakan hos en misstänkt, förutom i de fall när den misstänkte själv begärt att åtgärden skall vidtas. Eftersom ett samtycke till husrannsakan inte skall tillmätas någon betydelse kan inte heller en polisman enbart med stöd av samtycket få vidta sådana ingripanden. Det kan även ifrågasättas vad samtycket egentligen skulle ha för praktisk betydelse eftersom åtgärden ändå kan genomföras under alla förhållanden.[36] Någon bestämmelse om samtycke till att föremål tas i beslag finns inte i 27 kap. RB. Att ett sådant samtycke skulle föreligga kan dock medföra att själva behovet av att tillämpa beslagsinstitutet kan ifrågasättas.

3.6 Internationellt samarbete

Den svenska domsrätten omfattar, enligt 2 kap 2 § BrB, inte endast brott som begåtts inom det svenska riket, utan även brott som begåtts utomlands av svenska medborgare eller personer med hemvist i Sverige. Detta förutsätter dock att det föreligger dubbel straffbarhet. Förutom att de svenska brottsutredande myndigheterna kan vara nödgade att utreda brott

[34] Ibid. s. 25.
[35] SOU 1995:47 s. 145.
[36] Ibid.

som begåtts utomlands med anledning av att det föreligger svensk domsrätt, kan det även föreligga andra omständigheter som medför att myndigheterna är i behov av att inhämta uppgifter från andra länder. Förhållandet kan givetvis även vara det omvända, att det finns utländska myndigheter som har intresse av att söka stöd till en utredning om brott inom gränserna för det svenska riket. Att bedriva brottsutredningar inom andra staters territorium skulle dock kränka statens suveränitet varför det inte är möjligt för de brottsutredande myndigheterna att bedriva myndighetsutövning inom en annan stats territorium. Skulle de svenska brottsutredande myndigheterna vara i behov av att genomföra exempelvis en husrannsakan utomlands finns dock en möjlighet till detta genom att de söker internationell rättslig hjälp. Lagen (2000:562) om internationell rättslig hjälp i brottmål reglerar såväl rättslig hjälp i Sverige som rättslig hjälp för svenska myndigheter utomlands. Utvecklingen på området har gått mycket snabbt under den senaste tiden, framförallt inom den Europeiska Unionen, varför lagen har varit föremål för flera ändringar. Lagens tillämpningsområde innebär att samtliga åtgärder och tvångsmedel som kan förekomma i en svensk förundersökning får vidtas på ansökan av en främmande stat.[37] Den enda begränsningen som uppställs är att det i vissa fall förutsätts ett krav på dubbel straffbarhet. För åtgärder i form av husrannsakan och beslag är det dock inte en förutsättning att gärningen är straffbar i Sverige om ansökan om rättslig hjälp kommer från ett land inom EU eller från Island eller Norge, så länge det kan utdömas fängelse för gärningen i den ansökande staten.[38] Inte heller finns det några hinder mot att rättslig hjälp lämnas genom andra åtgärder om det kan ske utan att man behöver tillta tvångsmedel eller tvångsåtgärder.[39] Lagen reglerar främst ett internationellt samarbete mellan åklagare och domstolar men kan även komma att omfatta situationer där bindande internationella överenskommelser medger att utländsk polis- eller tullmyndighet kan söka rättslig hjälp om t.ex. en husrannsakan. Ansökan ses då som om den utfärdats av en utländsk åklagare eller domstol och förfarandet har ansetts nödvändigt eftersom flertalet länder inte har organiserat sin brottsutredande verksamhet på samma sätt som i Sverige.[40] Förutsättningarna för att vägra rättslig hjälp regleras i lagens 2 kap. 14 § och omfattar fall där förfarandet skulle kränka Sveriges suveränitet, medföra fara för riket eller strida mot allmänna svenska rättsprinciper eller andra väsentliga intressen. En begäran om rättslig hjälp får även avslås om gärningen har karaktär av ett politiskt brott, förutsatt att ansökan inte kommer från ett land inom EU eller från Island eller Norge, eller om gärningen utgör ett militärt brott och inte omfattas av annat brott enligt svensk lag som inte utgör militärt brott. En ansökan får dessutom avslås om det i Sverige har fattats beslut eller dom om åtalsunderlåtelse beträffande gärningen eller om omständigheterna i övrigt är sådana att ansökan inte bör bifallas. Förfarandet med framställningar till och från Sverige om internationell rättslig hjälp granskas och

[37] Se 1 kap. 2 § Lagen (2000:562) om internationell rättslig hjälp i brottmål.
[38] Se 4 kap. 20 § Lagen (2000:562) om internationell rättslig hjälp i brottmål.
[39] Se 1 kap. 2 § Lagen (2000:562) om internationell rättslig hjälp i brottmål.
[40] Ds 2005:6 s. 141.

vidarebefordras av Centralmyndigheten för internationellt samarbete inom Justitiedepartementet.

4 Beslag

4.1 Allmänt om tvångsmedlet

Bestämmelserna om beslag återfinns i 27 kap. RB. Själva syftet med tvångsmedlet är att ge de brottsutredande myndigheterna möjlighet att tillfälligt beröva någon besittning över ett föremål. Ägaren eller innehavaren av ett föremål förlorar därmed rätten att fritt kunna disponera föremålet. Eftersom ett beslag endast föreligger under en tillfällig period berövas dock aldrig ägaren eller innehavaren helt från rätten till föremålet. Ett beslag av föremål ses således som en inskränkning i rätten till egendom. Denna rätt har inte fått något grundlagsskydd i svensk rätt utan upprätthålls genom straffrättsliga bestämmelserna. Däremot har rätten till egendom fått ett uttryckligt skydd i Europakonventionen.[41]

I 27 kap 1 § RB anges tre olika omständigheter som kan aktualisera ett beslag av föremål. Enligt lagrummet får ett föremål tas i beslag om det skäligen kan antas ha betydelse för utredningen av brott, eller vara någon avhänt genom brott, eller vara förverkat på grund av brott. I många situationen kan det föreligga flera grunder för ett beslag. Som exempel kan nämnas att bilder med barnpornografiskt innehåll skall företas som bevisning om brott och samtidigt begäras förverkade. För sådana beslag som sker i utredningssyfte gäller inga särskilda förutsättningar eller krav avseende föremålen för beslag. Dessa kan således vara av vilket slag som helst. Det är inte heller nödvändigt att föremålet skall komma att åberopas som bevisning inför rätten, eftersom föremålet även kan äga betydelse för utredningen om brott genom att utröna vissa oklara omständigheter.[42]

4.2 Misstankegraden

För att ett föremål skall få tas i beslag krävs det, enligt 27 kap 1 § RB, att det föreligger en misstanke om brott. Det behöver dock inte finnas någon misstanke mot en viss person. Så länge som föremålet uppfyller något av de krav som uppställs i 1 § kan det alltså tas i beslag, oavsett om det innehavs av den som är misstänkt för ett brott eller av någon annan icke misstänkt person. Således saknar det alltså betydelse vem som äger föremålet eller vem som har det i sin besittning. Förutom det särskilda stadgandet i 27 kap 3 § RB om beslag av postförsändelser m.m. där det krävs att det för brottet är föreskrivet fängelse i ett år eller däröver, uppställs det i övrigt inte några krav på att brottet skall vara av en viss svårhetsgrad. Reglerna om beslag kan därmed tillämpas på samtliga typer av brott.

[41] Artikel 1 i tilläggsprotokoll den 20 mars 1952 till Europakonventionen.
[42] NJA II 1933 s. 97.

Den närmare innebörden av att föremålet ”skäligen kan antagas” antingen ha betydelse för utredningen, vara berövat någon genom brott eller vara förverkat på grund av brott, anses kunna likställas med kravet på skälig misstanke. Polisrättsutredningen menade att kravet på skälig anledning ansågs utgöra en lämplig avvägning mellan effektivitets- och integritetsintressena och att det närmare förutsätter att det finns konkreta omständigheter av viss styrka som tyder på att föremålet har betydelse för utredningen.[43] På samma sätt som man i 28 kap RB infört en bestämmelse som ger uttryck för proportionalitetsprincipen anges det i 27 kap 1 § 3 st att åtgärder enligt 27 kap. endast får beslutas om skälen för åtgärden uppväger det intrång och men som åtgärden kan medföra.

Då det inte finns några regler om samtycke till beslag torde det sakna betydelse om innehavaren frivilligt kan tänka sig att lämna ifrån sig ett föremål. Denna föresats framgår även av förarbetena där skäl anges för att beslagsinstitutet skall kunna tillämpas oavsett om innehavaren lämnar sitt samtycke till att han berövas besittningen över föremålet.[44] Skulle ett samtycke om beslag föreligga kan man ju däremot ifrågasätta själva behovet av att ta föremålet i beslag. Kan det bli aktuellt med ett förverkande av föremålet borde föremålet dock alltid tas i beslag. Så får även anses vara fallet om föremålet har betydelse som bevisning. Den enskilde får då möjlighet till rättsprövning av beslaget samtidigt som brottsutredande myndigheten har full kontroll över bevismaterial.[45]

4.3 Omfattningen av åtgärderna

Av 27 kap 1 § RB framgår det att beslag endast kan tillämpas på lösa saker. Som tidigare nämnts ger alltså beslagsrätten i sig inte någon befogenhet för brottsutredande myndigheter att söka efter föremål. För att eftersöka föremål är myndigheterna förpassade till att vidta åtgärder som husrannsakan eller kroppsvisitation. Det innebär att ett beslut om husrannsakan inte kan innefatta ett beslut om att visst föremål skall tas i beslag. Givetvis kan beslutet om husrannsakan innehålla instruktioner över vilka föremål som skall eftersökas men beslutet om att ta föremålen i beslag måste fattas av personal vid platsen för husrannsakan.[46] Sagda grundar sig i att beslagsrätten endast avser föremål som är tillgängligt för beslag.[47] På vilket sätt som föremålet har gjorts tillgängligt har däremot ingen betydelse för frågan huruvida föremålet kan tas i beslag. Det innebär att, trots det faktum att en tjänsteman överskridit sin befogenhet eller handlat lagstridigt för att få tillgång till föremålet så föreligger det inte några hinder mot att föremålet tas i beslag.[48]

[43] SOU 1995:47 s. 357 f.
[44] NJA II 1933 s. 97.
[45] SOU 1995:47 s. 356.
[46] Fitger s. 27:5.
[47] NJA II 1933 s. 97.
[48] Lindberg s. 379.

I 27 kap. 1 § RB andra stycket anges att vad som gäller för föremål även skall gälla för skriftliga handlingar i den mån annat inte föreskrivs. Bestämmelsen klargör att skriftliga handlingar, likt andra föremål, får tas i beslag även i fall då det inte är själva handlingen som är av intresse utan dess innehåll.[49]

Ett beslag av viss utrustning för lagring av digital information torde i de flesta fallen syfta till att säkra digitalt lagrade uppgifter som äger betydelse för en brottsutredning. Digitala bevis kan även bli föremål för förverkande om de utgörs av material med brottsligt innehåll. Förverkande av digitala bevis försvåras dock på grund av de karaktäristiska dragen hos digitalt material som innebär att kopior kan framställas i oändligt antal. Det är inte heller uteslutet att beslag av datorer syftar till att säkra digitala bevis som avhänts någon genom brott.[50]

Polisrättsutredningens har lagt fram ett lagförslag om en total omarbetning av reglerna om beslag i 27 kap RB. Bland annat föreslogs det att begreppet föremål skulle bytas ut mot egendom. Det har uttalats att begreppet föremål inte omfattar lösa saker som t.ex. bilar, båtar eller större transportfordon.[51] Genom att ändra lydelsen till egendom istället för föremål skulle således bestämmelserna om beslag omfatta all lös egendom, inklusive handlingar. Dessutom skulle det enligt förslaget framgå av lagtexten att beslagtagen egendom får undersökas. Är egendomen sådan att den kan undersökas med stöd av reglerna i 28 kap RB skulle det dock även fortsättningsvis krävas ett beslut om husrannsakan för att få undersöka egendomen.[52]

Det har även föreslagits att särskilda regler om de brottsutredande myndigheternas befogenheter att inhämta information i allmänhet skulle införas. Sådana regler skulle även omfatta förbud mot att inhämta viss integritetskänslig information oavsett om det rör sig om en skriftlig handling eller t.ex. datalagrad information.[53] Några konkreta förslag på en sådan reglering presenterades dock aldrig. En annan möjlighet presenterades av Datastraffrättsutredningen som menade att det kunde vara tänkvärt att beslagsreglerna ändras till att även omfatta inhämtande av information och inte bara omhändertagande av föremål.[54] Polisrättsutredningen, menade å sin sida att det skulle kunna leda till att reglerna om beslag och husrannsakan överförs till ett område som de inte är avsedda för och att inhämtandet av information inte bör betraktas som något egentligt tvångsmedel.[55] Istället eftersöktes en reglering som inte bara reglerar polisens befogenheter för att bereda sig tillträde till upptagningar i datorer,

[49] NJA II 1943 s. 359.
[50] Se 41 § Varumärkeslagen, 59 § Upphovsrättslagen, 59 § Patentlagen, 37 § Mönsterskyddslagen, 20 § Firmalagen, 13 § Kretsmönsterlagen och 9 kap. 8 § Växtförädlarrättslagen.
[51] Prop. 1993/94:24 s. 24.
[52] SOU 1995:47 s. 489.
[53] Ibid. s. 177.
[54] SOU 1992:110 s. 353.
[55] SOU 1995:47 s. 187.

utan även föreskriver på vilket sätt åtgärden får ske, vilket skulle underlätta den praktiska tillämpningen av bestämmelserna samtidigt som integritetsskyddet förstärktes.[56] Frågan är vilken verkan sådana regler skulle få då man i svensk rätt utgår från principen att all information som inhämtas av polisen får användas fritt.

4.3.1 Beslagsförbudet i RB 27:2

Bestämmelsen i 27 kap. 2 § RB ger ett särskilt skydd för vissa uppgifter som anses vara särskilt integritetskänsliga. Här föreskrivs ett förbud mot att lägga beslag å skriftlig handling med innehåll av särskild karaktär. Förbudet gäller handlingar vars innehåll kan antagas vara sådant, att befattningshavare eller annan som avses i 36 kap 5 § RB inte får höras som vittne därom. I lagrummet ges hänvisningar till vissa bestämmelser i Sekretesslagen gällande bl.a. skydd för rikets säkerhet. I 36 kap 5 § 2 st. RB nämns även vissa yrkeskategorier, exempelvis läkare, advokater och psykologer, för vilka särskild tystnadsplikt för anförtrodda uppgifter gäller. Förbudet gäller endast om handlingen innehas av den som har tystnadsplikt eller av den till förmån för vilken tystnadsplikten gäller. Förbud gäller även mot att, hos den misstänkte eller honom närstående, lägga beslag på skriftliga meddelanden mellan den misstänkte och närstående eller mellan närstående inbördes. Sistnämnda förbud gäller dock inte om det rör sig om brott för vilket inte är stadgat mindre än fängelse i två år.

Eftersom det inte finns någon definition av begreppet skriftlig handling i RB kan det diskuteras vilken omfattning begreppet bör ges och då särskilt huruvida även handlingar i form av datoriserat material, som inte har fixerats fysiskt, kan tas i beslag. En handling utgör ett generellt samlingsbegrepp för informationsinsamling eller i vissa fall informationsbärare. I vissa fall avses specifika former av informationsbärare eller representation av information. Som exempel kan handlingen vara av en viss typ eller ha ett särskilt rättsligt eller formellt innehåll.[57] Begreppet handling kan alltså ha olika innebörd beroende på i vilket sammanhang som begreppet förekommer i. En central definition av begreppet handling kan dock hämtas från 2 kap. 3 § Tryckfrihetsförordningen (TF). Enligt lagrummet avses då inte endast framställningar i skrift eller bild utan även upptagningar som endast kan läsas, avlyssnas eller på annat sätt uppfattas, med hjälp av tekniska hjälpmedel. Svårigheterna med att tolka begreppet handling när det gäller digital information har behandlats i flera förarbeten och utredningar.[58] Normalt sett anses begreppet numera även innefatta sådana handlingar som bygger på elektroniska rutiner. Skulle det i särskilda fall anses att digital information inte kan innefattas i begreppet handling torde det, om det inte framgår av sammanhanget, krävas ett förtydligande i lagstiftningen att den endast tar sikte på fysiska handlingar.[59]

[56] Ibid. s. 181 ff.
[57] Ds 2003:29 s. 95 f.
[58] Se Prop. 1998/99:11 s. 54 f, SOU 1996:40 s 59 f, SOU 1997:39 s. 493 f.
[59] Ds 2003:29 s. 95.

Skulle information från en skriftlig handling inhämtas genom att en polis tar kopia av handlingen eller genom att digitalt lagrad information omhändertas genom att t.ex. en dator, innehållande handlingen, tas i beslag blir alltså reglerna inte tillämpliga. På detta sätt ger beslagsförbudet i 27 kap. 2 § ett otillräckligt skydd för digitala handlingar. Syftet med beslagsförbudet torde vara att bl.a. skydda medborgarna mot att myndigheterna får kännedom om deras mest privata förhållanden. Beslagsförbudet i 27 kap 2 § RB uppfyller däremot inte dessa krav i praktiken eftersom det inte finns något som hindrar att någon vid utredningen av ett brott nöjer sig med att läsa en handling för att få del av informationen. Digitalt lagrad information kan överföras till andra datamedier utan hinder av beslagsreglerna. Förbudet förhindrar inte heller att fotokopior görs av handlingen.[60]

För att anpassa bestämmelserna om förbud mot beslag av vissa handlingar så att de även omfattar digitala handlingar föreslog Datastraffrättsutredningen att kravet på att handlingar skall vara skriftliga skulle utmönstras. Då digitala handlingar kan förekoma i flera exemplar föreslogs det även att uttrycket ”handlingen innehaves” skulle ersättas med ”handlingen förvaras”, vilket skulle markera att det inte är avgörande var någonstans som handlingen finns lagrad.[61] Det ansågs även vara nödvändigt att införa en definition av handlingsbegreppet i RB som omfattar sådan data som endast kan läsas, avlyssnas eller på annat sätt uppfattas med hjälp av tekniska hjälpmedel.[62] Polisrättsutredning ansåg att betänkligheterna med ett minskat skydd för digitala handlingar vid en tillämpning av förbuden i 27 kap 2 § RB enklast kunde överkommas genom praktiska åtgärder där man överför det särskilt skyddade materialet till ett lagringsmedium och på så sätt avlägsnar det från beslagsföremålet.[63]

4.3.2 Beslagsförbudet i RB 27:3

I 27 kap 3 § ges ett särskild skydd mot beslag av försändelser som finns hos post- eller telebefordningsföretag. För att sådan försändelse skall få tas i beslag krävs det att brottet har föreskrivit fängelse i ett år eller däröver. Det krävs även att försändelsen skall kunna tas i beslag hos mottagaren vilket innebär att försändelser som innehåller uppgifter av sådant slag som anges i 27 kap 2 § faller utanför bestämmelsens tillämpningsområde. Bestämmelsen tar endast sikte på traditionella postförsändelser, t.ex. brev och paket, och är inte tillämplig när det handlar om elektronisk post. Med anledning av att en allt större del av den kommunikation som tidigare skedde genom postförsändelser, idag utgörs av elektronisk post har bestämmelsen i RB 27:3 förlorat lite av sin betydelse. Anledningen till att elektronisk post inte omfattas av bestämmelsen är att sådana meddelanden är telemeddelanden

[60] SOU 1995:47 s. 186.
[61] SOU 1992:110 s. 607.
[62] Ibid. s. 625.
[63] Ibid. s. 382.

enligt lagen (2003:389) om elektronisk kommunikation (LEK).[64] Således krävs det ett beslut om hemlig teleavlyssning för att polis eller åklagare skall få tillgång till ett elektronisk meddelande under befordran. Eftersom ett sådant beslut endast får avse brott som har inte har lindrigare straff än två års fängelse i straffskalan har meddelanden som överförs elektronisk fått ett betydligt starkare skydd än försändelser som befordras via traditionella post- och telebefordningsföretag. Detta särskilda skydd för elektroniska meddelanden kan dock inge vissa betänkligheter. I Ds 2005:6 illustrerades problemet med ett exempel där bilder med barnpornografiskt innehåll skickas som en bilaga till elektroniskt post, varå hela innehållet av meddelandet utgör ett telemeddelande. Det innebär att de brottsutredande myndigheterna är oförhindrade att få tillgång till innehållet i meddelandet, när det är under befordran, eftersom straffskalan för barnpornografibrott inte når upp till kraven för ett beslut om hemlig teleavlyssning.[65] Hade de barnpornografiska bilderna istället skickats med traditionell post hade försändelsen däremot kunnat kvarhållas och tas i beslag. Visserligen kan man med stöd av reglerna om hemlig teleövervakning[66] få tillgång till uppgifter om att kommunikation av en viss omfattning har skett mellan datorer vid en viss tidpunkt. Fortfarande är man dock förhindrad att få tillgång till själva innehållet av uppgifterna varför man inte kan säkerställa att meddelandet har innehållit något olagligt material. Således har information av samma slag olika skydd beroende av vilket kommunikationssätt som används för att överföra informationen.

4.3.3 Postkontroll

Enligt bestämmelsen i 27 kap. 9 §, ges myndigheterna möjlighet att hålla kvar en försändelse som väntas komma in till ett befordningsföretag till dess att man tagit ställning i frågan huruvida försändelsen skall tas i beslag. Denna åtgärd kallas även postkontroll. Ett förordnande om att viss försändelse skall hållas kvar framställs av rätten på yrkande av undersökningsledare eller åklagare. Rättens beslut om att hålla kvar en försändelse skapar således endast möjlighet för att ta försändelser under befordran i beslag. Ett beslut om att därefter ta försändelsen i beslag fattas av åklagaren. En förutsättning för att hålla kvar försändelsen är självfallet att försändelsen även kan tas i beslag. Således måste bestämmelserna i 27 kap. 1-3 §§ vara uppfyllda vilket bl.a. innebär att det för brottet måste vara föreskrivet fängelse i minst ett år. Förordnandet skall gälla för viss tid, dock högst i en månad från den dag som förordnandet delgavs befordningsföretaget. Med befordningsföretag avses företag som på affärsmässiga grunder huvudsakligen förmedlar information som andra lämnar för distribution.[67] Det förordnande som tillställs befordningsföretaget skall innehålla en underrättelse om att meddelanden om åtgärden får lämnas till mottagaren, avsändaren eller någon annan utan

[64] se 6 kap. 1 § LEK.
[65] Ds 2005:6, s. 278 f.
[66] Bestämmelserna utvidgades nyligen till att även omfatta barnpornografibrott.
[67] Prop. 1992/93:200 s. 161 f.

tillstånd från undersökningsledaren eller åklagaren. Då dagens kommunikation i allt större utsträckning sker via elektronisk post har de brottsutredande myndigheternas möjligheter till postkontroll minskat.

4.4 Beslut om beslag

Eftersom ett beslag oftast avser ett föremål som påträffas i samband med att man utför en husrannsakan, eller annan tvångsåtgärd, anges det som huvudregel, i 28 kap. 4 § 1 st, att samma person som utför denna åtgärd även får ta ett påträffat föremål i beslag. Skulle ett föremål påträffas i annat fall framgår det av andra stycket samma lagrum att föremålet får tas i beslag efter beslut av undersökningsledaren eller åklagaren. Skulle det dock vara fara i dröjsmål får denna beslutsrätt även utvidgas till att även omfatta polisman om det inte rör sig om beslag av sådan försändelse som avses i 27 kap 3 § RB. I de fall som ett föremål har tagits i beslag av annan än förundersökningsledaren eller åklagaren och utan att någon av dessa har beslutat om beslaget, skall en anmälan om beslaget snarast tillställas dessa, som har att pröva beslaget.[68]

I 27 kap 5 § RB ges en möjlighet för rätten att förordna om beslag. Sådant beslut får ske om föremålet företes vid rätten eller om föremålet annars finns tillgängligt för beslag. Skulle det således kräva en husrannsakan för att eftersöka föremålet skall alltså rätten istället förordna om en sådan åtgärd istället för ett beslut om beslag.[69] Som tidigare nämnts är det en förutsättning att föremålet som tas i beslag finns tillgängligt. Detta innebär alltså att det inte går att fatta beslut om att ett visst föremål skall tas i beslag, t.ex. en dator, innan föremålet påträffats efter genomförd husrannsakan. Däremot kan det i beslutet om husrannsakan anges att t.ex. datorer skall eftersökas. Huruvida datorn därefter skall tas beslag blir närmast en praktisk fråga som behandlas närmare i följande kapitel.

4.5 Rättssäkerhetsgarantier

4.5.1 Rättens prövning av beslag

Enligt 27 kap 8 § RB skall det under tiden som ett beslag består ske fortlöpande prövningar över huruvida utredningen fortfarande kräver att egendomen skall vara underkastat beslag. När åklagaren väcker åtal tar denne ställning till vilken bevisning som åberopas och dessutom eventuella yrkanden om förverkande eller återlämnande av viss egendom. Beslag som inte omfattas av sådana yrkanden skall därför hävas i samband med att åtal väcks. Vad gäller bevisbeslag finns det dock ett visst utrymme för att låta beslaget bestå trots att den beslagtagna egendomen inte åberopats som bevisning i målet. Eftersom bevisläget kan komma att ändras under

[68] Se RB 27 kap 4 § 3 st.
[69] Fitger s. 27:18.

processens gång har det ansetts nödvändigt att tillförsäkra åklagaren denna möjlighet att kunna undersöka och åberopa sådant beslag som från början inte tagits upp som bevisning. När dom väl fallit i målet måste dock beslag hävas över sådant som rätten inte prövat.[70]
Denna fortlöpande prövning av beslagets bestånd kräver alltså inte åtgärder från den som berörs av beslaget utan skall ske ex officio. I 27 kap 6 § RB ges dock en möjlighet för den som drabbats av beslaget att få en domstolsprövning av beslutet. En domstolsprövning förutsätter att beslaget verkställts utan rättens förordnande. Att någon drabbats av beslaget behöver inte innebära att egendomen tagits från just den personen. Möjligheten till rättslig prövning anses i allmänhet tillfalla den som påstår att det, genom beslaget, skett en inskränkning i dennes äganderätt till egendomen.[71]

Rättens prövning av beslutet avser endast ett eventuellt återställande av besittningen av föremålet som tagits i beslag varför en prövning aldrig kan komma i fråga om beslaget hävts. Ett inte ovanligt tillvägagångssätt när föremål tas i beslag är att polisen framställer en kopia av föremålet varefter beslaget hävs och egendomen återlämnas till den som drabbats av beslaget. Ett sådant förfarande kan även, av olika skäl, ligga i den enskildes intresse då det resulterar i denne kan återfå egendomen så snart som möjligt.[72] Nackdelen är dock att kontrollsystemet i 27 kap RB, med möjligheten till rättslig prövning av beslutet sätts ur spel. I rättsfallet NJA 1977 s 573 fann därför Högsta domstolen (HD) inte anledning att pröva ett yrkande om hävande av ett beslag som bestod av fotokopior av skriftliga handlingar. Genom att framställa kopior av det beslagtagna föremålet och därefter häva beslaget finns alltså risken att brottsutredande myndigheterna kan kringgå de rättsgarantier som framställs genom möjligheten till domstolsprövning. HD har uttalat att ett sådant förfarande, om det inte kan grundas på önskemål eller ett medgivande från den som drabbats av beslaget, inte kan anses väl förenligt med grunderna för bestämmelsen om rätten att begära domstolsprövning av beslag.[73] Rättsfallet kommenterades av Polisrättsutredningen som menade att ett förfarande med kopior av det beslagtagna föremålet måste ses i belysning av själva syftet med regeln om domstolsprövning av ett beslut av beslag. Eftersom en sådan prövning endast tar sikte på ett eventuellt återställande av besittningen av föremålet och är oberoende av huruvida kopior framställts av föremålet eller ej. Även om rättsordningen skulle erbjuda en domstolsprövning efter det att ett beslag hävts skulle det inte kunna resultera i något förbud för polisen att använda den information som kopian ger då polisen fritt får använda information som man inhämtat. Dock ansågs det, med hänsyn till behovsprincipen, att kopior inte borde framställas i större omfattning än vad som är nödvändigt för brottsutredningen.[74]

[70] Lindberg s. 408.
[71] Fitger s. 27:20.
[72] SOU 1995:47 s. 197
[73] Se NJA 1988 s. 471.
[74] SOU 1995:47 s. 197 ff.

4.5.2 Dokumentation över beslag

Skulle rätten besluta eller fastställa åtgärder genom tvångsmedel föreligger en dokumentationsskyldighet som framgår av reglerna i 30 kap. RB. För husrannsakan och beslag finns särskilda regler om protokollföring i 27 och 28 kap. RB. Dessa bestämmelser är således inte avsedda att tillämpas av domstolen i de fall rätten beslutar om en husrannsakan eller ett beslag. Den reglering som sker i 27 och 28 kap. om dokumentering av är dock inte i närheten så ingående som bestämmelserna i 30 kap. RB. Enligt Lindberg beror detta på att RB förts och främst skrevs för domstolen varför sådana tvångsmedel som nästan uteslutande beslutas av polismän eller åklagare kom att få en mindre omfattning.[75] Dokumentation av husrannsakan och beslag regleras även i 27 § Polislagen men dessa bestämmelser hänvisar till RB:s regler om protokoll varför de får anses vara av mindre betydelse. Uppgifter om tvångsmedel och beslut därom skall även ingå i förundersökningsprotokollet.[76] Av en generell föreskrift över dokumenteringen av straffprocessuella tvångsmedel från Riksåklagaren framgår det att dokumentationen bl.a. skall klargöra vem som fattat beslutet om tvångsmedel och vilken tidpunkt detta skedde. Av föreskrifterna framgår det inte något krav på att omständigheterna som har legat till grund för beslutet skall framgå i dokumenteringen.[77]
Att föra dokumentation över tvångsmedel fyller flera olika syften. Ur rättssäkerhetssynpunkt är det viktigt att tvångsmedel dokumenteras eftersom de innebär ingrepp i den personliga integritetssfären. Framgår det vad som förekommit vid verkställigheten av ett tvångsmedel kan man således kontrollera att åtgärden vidtagits inom ramarna för förundersökningen. Att ett tvångsmedel har dokumenterats är ofta även en förutsättning för att en fråga angående tvångsmedlet skall komma under prövning, exempelvis rättens prövning av beslag i 27 kap. 6 § RB.

Tas något i beslag föreligger det en skyldighet, enligt 27 kap. 13 § RB, att föra protokoll över åtgärden. Av protokollet skall ändamålet med beslaget framgå och dessutom vad som förekommit vid verkställigheten av åtgärden. Egendom som tagits i beslag skall beskrivas och det skall framgå från vem egendomen tagits i beslag och vilka som varit närvarande. Ett protokoll över beslag skall i princip upprättas omedelbart i samband med att egendomen tas i beslag.[78] Skulle förhållandena vara sådana att det, exempelvis vid omfattande beslag, skulle innebära ett alltför stort intrång mot den som beslaget berör om protokoll skall omedelbart upprättas på plats kan protokoll upprättas i efterhand.[79] Utgörs det beslagtagna av datorutrustning, t.ex. en persondator, externt datorminne eller cd-skivor, krävs det inte att man i protokollet anger eller beskriver samtliga de dokument som finns

[75] Lindberg s. 74.
[76] Se 20 § Förundersökningskungörelsen (FuK).
[77] RÅFS 2002:1 om dokumentation och underrättelser vid tvångsmedel.
[78] JO 2004/05 s. 70.
[79] JO 1975/76 s. 154, JK 1981 s. 38.

lagrade på utrustningen utan det är tillräckligt att utrustningen i sig beskrivs.[80]

4.6 Beslag av datorutrustning

Digitala bevis utgörs alltså av information av olika slag som på något sätt kan lagras i, eller förmedlas av, elektronisk utrustning. Ett lämpligt tillvägagångssätt för de brottsutredande myndigheterna att komma åt dessa bevis är således att, med stöd av reglerna i 27 kap. RB, beslagta den utrustning varå informationen är lagrad. Särskilt när det gäller grövre brottslighet har det blivit allt vanligare att datorer läggs i beslag. Efter att datorutrustningen tagits i beslag kan en närmare undersökning av utrustningen genomföras i polisens lokaler för att man skall finna de bevis som är av relevans för utredningen. För att överhuvudtaget komma åt den utrustning som skall tas i beslag krävs det vanligtvis en husrannsakan i den lokal eller det utrymme där utrustningen befinner sig.[81]

Att beslagta datorutrustning är oftast det enklaste sättet att genomföra en husrannsakan i digital miljö. Åtgärden kräver ingen särskild utrustning eller kompetens utav personalen på plats. Sedan datorutrustningen tagits i beslag kan undersökningen därefter ske i en kontrollerad miljö i myndighetens lokaler. Nackdelen med att beslagta utrustning ligger främst i den ökade risken för att utrustningen skall skadas när den flyttas till myndighetens lokaler och att information på så sätt skall gå förlorad.[82] För den enskilde innebär det givetvis även ett större ingrepp om denne förlorar besittningen över sin egendom. När det kan bli aktuellt med ett förverkande av ett föremål torde man dock vara tvungen att beslagta datorutrustningen för att inte lämna kvar något brottsligt material i den misstänkte personens besittning.

Vid beslag av datorteknisk utrustning löper man även en stor risk att andra personer, som inte omfattas av brottsmisstanken, skall komma att påverkas negativt av åtgärden. JK har i ett beslut yttrat att särskild försiktighet är påkallad vid beslag av datorutrustning och att man därför alltid borde överväga om man kan uppnå samma resultat som beslaget på annat sätt, utan att datorutrustning tas om hand. I situationer där ett beslag av datorer kan påverka centrala delar av t.ex. ett företags datornätverk får åtgärden anses vara av särskild ingripande natur, särskilt om beslaget omfattar utrustning som tillhör annan än den misstänkte.[83] Ett mer konkret vägledande kan hämtas från Justitieombudsmännens prövning av ett omfattande beslag av datorservrar i samband med en husrannsakan i

[80] Lindberg s. 412.
[81] Fitger s. 27:3.
[82] Angerfeldt, Bengt, Husrannsakan & Beslag i IT-miljö: en lathund s. 7 (hädanefter Angerfeldt).
[83] JK-Beslut 2001-01-22.

lokalerna för ett så kallat webhotell[84]. Husrannsakan syftade till att vinna utredning om brott mot upphovsrättslagen och resulterade i att över 180 datorservrar togs i beslag. Eftersom det inte direkt kunde avgöras vilket material som var av intresse för utredningen drabbades flera företag och privatpersoner, som hade delar av sin verksamhet lagrad på de beslagtagna servrarna, av men och skada trots att de inte omfattades av brottsmisstanken. Dagen efter tillslaget påbörjade polisen arbetet med att sålla bort de datorer som inte innehöll något material av betydelse för utredningen och efter en veckas tid hade beslagen hävts avseende dessa datorer. De förevarande beslagen var även föremål för rättslig prövning.[85] Även om JO inte fann skäl för att ifrågasätta proportionaliteten av åtgärden höjde man farhågor över att brottsutredningar i digitala miljöer kan komma att drabba privatpersoner och företag som inte omfattas av brottsmisstanke. Här ansågs det vara av särskild vikt att avsätta resurser för att minimera dessa skador, exempelvis genom att så fort som möjligt häva beslagen på datorer som inte är vikt för utredningen.[86]

Beslag av viss datorteknisk utrustning, varå information i digital form är lagrad, kräver oftast även ett stort utredningsarbete när det gäller att finna den önskvärda bevisningen. Då man kan lagra stora mängder information på utrustning som bygger på digital teknik kan det vara nödvändigt att begränsa beslaget endast till det som är absolut relevant för utredningen. Att initialt begränsa beslaget till sådan information kan däremot vara mycket svårt eftersom informationen inte är direkt synlig, då den exempelvis är lagrad på en hårddisk, cd-rom skiva eller ett externminne.[87]

4.7 Undersökning av beslagsföremål

Med stöd av reglerna om beslag får brottsutredande myndigheter, under en kortare eller längre tid, beröva någon besittningen över ett föremål. När exempelvis en dator tas i beslag i syfte att ge vinning för utredningen av brott är det oftast inte tillräckligt att den misstänkte inte längre har besittning över föremålet. För att kunna få fram de bevis som behövs för brottsutredning krävs det oftast en närmare undersökning av föremålet. Som exempel kan ett beslagtaget skjutvapen behöva undergå en närmare undersökning och provskjutning för att man skall kunna knyta vapnet till en viss gärningsman eller brottsplats. Det får därför anses ligga i syftet med beslag av föremål att de även skall kunna undersökas. Detta är även den rådande allmänna uppfattningen vilken kan tänkas få stöd i lag av stadgandet i 27 kap. 12 § RB. Lagrummet anger att post-

[84] Ett webhotell erbjuder lagringsutrymme för användare som vill publicera material på Internet men inte har tillgång till en egen datorserver. Lagringen kan erbjudas gratis eller mot en kostnad.
[85] Rättens beslut i beslagsfrågorna ingår i den föreliggande brottsutredningen. Eftersom utredningen pågår i skrivande stund har det inte varit möjligt att få tillgång till rättens beslut i beslagsfrågan.
[86] JO-Beslut 2007-04-02.
[87] Kronqvist s. 80.

telegramförsändelse, handelsbok eller annan enskild handling som tas i beslag inte närmare får undersökas av annan än rätten, undersökningsledaren eller åklagaren. Härifrån skulle man således indirekt kunna utläsa en rätt att föremål som tas i beslag får undersökas med förbehåll för ovan nämnda undantag.[88] Då bestämmelsen endast tar sikte på undersökning av enskilda handlingar kan dock sådana tolkningar ifrågasättas. Lagrummet påvisar även en ytterligare skillnad mellan skyddet för digital information och information i traditionell form. Som handelsböcker räknas normalt uppgifter i form av bokföring. Sådant material utgörs idag i allt större utsträckning av digital information och utgör självfallet centrala bevis vid utredning av ekonomisk brottslighet. Eftersom bokföring som utgörs av digitalt lagrad information troligtvis inte kan hänföras under begreppet handelsböcker omfattas dessa uppgifter inte av det särskilda skyddet i 27 kap. 12 § RB.[89] En motsvarande bestämmelse för husrannsakan återfinns i 28 kap. 8 §.

Det torde följa av syftet med beslagsreglerna att dessa endast ger polisen en befogenhet att beröva någon besittningen av ett föremål under en viss tid och att de således inte skapar någon direkt rätt för polisen att också undersöka föremålet. I de fall en undersökning av ett föremål inte kan ske med stöd av reglerna om husrannsakan kan det ifrågasättas huruvida det föreligger ett uttryckligt lagstöd för att beslagtagna föremål skall få undersökas. Med anledning av detta har det från polisens håll ansetts önskvärt att, i 27 kap RB, införa en bestämmelse som ger ett positivt stöd för brottsutredande myndigheter att undersöka egendom som tas i beslag.[90] För att motverka att man genom ett beslag skulle kunna kringgå bestämmelserna om husrannsakan skulle det dock vara nödvändigt att en sådan bestämmelse utformas så att den inte kan tillämpas på föremål som får undersökas endast genom ett beslut om husrannsakan.[91] Å andra sidan kan man ifrågasätta om det var tänkt att systemet med reglerna om beslag skulle utesluta någon befogenhet för polisen att också undersöka den beslagtagna egendomen. Ett sådant synsätt skulle kunna leda till att polisen i vissa fall skulle vara skyldig att ta hand om slutna föremål som inte fick undersökas.[92]

[88] Lindberg s. 402.
[89] SOU 1995:47, s 181 ff.
[90] SOU 1995:47 s. 217 ff.
[91] Ibid. s. 351 f.
[92] Fitger s. 27:16.

5 Husrannsakan

5.1 Grundläggande förutsättningar

Genom en husrannsakan ges de brottsutredande myndigheterna möjligheten att genomsöka utrymmen man annars inte skulle få tillträde till. Normalt sett är enskilda, genom regler i exempelvis RF och Europakonventionen, skyddade mot åtgärder som innebär intrång i exempelvis den enskildes bostad eller arbetsplats. I RF 2 kap 6 § anges uttryckligen att varje medborgare, gentemot det allmänna, är skyddade mot husrannsakan och liknande intrång. Med husrannsakan avses i regeringsformen alla undersökningar som myndigheter företar sig i hus, rum eller slutet förvaringsställe, oavsett vad syftet med dem undersökningarna är.[93] Givet är dock att det måste röra sig om undersökningar som sker i ett brottsutredande syfte. Skulle polisen exempelvis tränga in i en bostad för att ingripa mot ett överhängande brott, t.ex. en misshandel, kan åtgärden därför inte betraktas som en husrannsakan.

Den huvudsakliga regleringen om husrannsakan återfinns i 28 kap RB. Bestämmelserna utgår från två typer av undersökningar. En reell husrannsakan syftar till att eftersöka föremål som är av intresse för brottsutredning medan en personell husrannsakan syftar till att eftersöka personer. Med anledning av syftet med detta arbete kommer således endast reglerna om reell husrannsakan att behandlas.

5.2 Ändamålen med åtgärderna

Syftet med en reell husrannsakan framgår av 28 kap. 1 § RB, där det anges att husrannsakan får företas i syfte att eftersöka föremål som är underkastat beslag, eller för att utröna omständighet som kan vara av betydelse för utredningen av ett brott. Att använda husrannsakan i syfte att upptäcka brott stämmer således inte överens med kravet på att det skall föreligga anledning att ett brott har förövats. Inte heller får syftet med husrannsakan vara att skaffa information om annat brott än det som husrannsakan utställts för.[94] Vidare får en husrannsakan inte vidtas i syfte att undersöka huruvida den som misstänks för ett brott kan tänkas ha gjort sig skyldig till brottslighet i en större omfattning än vad som kunde förutses genom de föreliggande omständigheterna.[95]

En husrannsakan skapar alltså möjligheter för brottsrutredande myndigheter att använda andra tvångsmedel t.ex. beslag eller förverkande. Däremot kan man inte säga att en reell husrannsakan direkt syftar till att finna föremål

[93] Prop. 1975/76:209 s. 147.
[94] JO 1988/89 s. 53.
[95] Fitger s. 28:5.

som omfattas av ett beslut om beslag. Istället förhåller sig husrannsakan och beslag till varandra på så sätt att husrannsakan används för att eftersöka föremål som kan komma att tas i beslag. Ett beslut om att ta föremål i beslag kan nämligen ske först när föremålet påträffas.[96] För att avgöra om en husrannsakan får företas måste man alltså först se till ändamålen med beslagsreglerna. Är det inte möjligt att ta föremålet i beslag, t.ex. på grund av att föremålet utgörs av sådant material som omfattas av beslagsförbuden i 27 kap. 2 och 3 §§ RB, får man således inte heller företa en husrannsakan i syfte att eftersöka föremålet.

Förutom att husrannsakan får företas i syfte att eftersöka föremål som skall tas i beslag, kan tvångsmedlet alltså även användas i syfte att utröna omständighet som är av betydelse för utredningen av brott. Genom bestämmelsen har husrannsakan fått ett mycket brett tillämpningsområde som tvångsmedel då det exempelvis kan användas i syfte att söka efter spår av ett brott eller i syfte att undersöka en misstänkt brottsplats.

När det rör sig om en husrannsakan i syfte att få tillgång till digitalt lagrad information kan det vara av intresse att utröna vad som är själva objektet för åtgärden. Objektet för husrannsakan kan antingen utgöras av själva databäraren (vanligtvis en dator), eller viss lagrad data på databäraren eller det mönster av ettor och nollor, utan anknytning till viss data, som representerar den lagrade informationen.[97] Vilket synsätt man väljer kan få betydelse, exempelvis för reglerna om beslagsförbud i 27 kap RB. Är själva databäraren och inte data objekt för åtgärden borde de särskilda reglerna om skriftlig handling inte bli tillämpliga. Detta trots att databäraren kan innehålla stora mängder integritetskänsligt material.[98] Polisrättsutredningen presenterade ett förslag som syftat till att få mer nyanserade bestämmelser om husrannsakan där man föreslog att sådana undersökningar skulle delas upp efter graden av det intrång som följer av åtgärderna. Istället för husrannsakan skulle åtgärderna, enligt lagförslaget, benämnas undersökningar, där åtgärder som företas i hus, rum eller slutna förvaringsställen hörde till den kategori som medförde ett större integritetsintrång än övriga undersökningar. Det klargjordes dock att undersökningar av slutna förvaringsställen inte nödvändigtvis behövde medföra ett större ingrepp än undersökningar av sådana förvaringsställen som hålls olåsta.[99]

5.3 Brottsmisstanken

Enligt 28 kap 1 § RB får en husrannsakan företagas om det förekommer anledning om att brott har förövats varå fängelse kan följa. Här kan det konstateras att beviskravet för brottsmisstanke är lägre ställt vid

[96] Se NJA II 1933 s. 97.
[97] SOU 1992:110 s. 344.
[98] Ibid. s. 350.
[99] SOU 1995:47 s. 513.

husrannsakan jämfört med de flesta andra tvångsmedel. Kravet överensstämmer dock med förutsättningarna för att få inleda förundersökning.[100] Gällande brottsmisstanken anledning om att brott har förövats, anges det i förarbetena att det inte behöver konstateras att ett brott har förövats utan det är tillräckligt att det förekommer en misstanke därom.[101] Ekelöf ger en närmare innebörd av beviskravet och menar på att man inte behöver ha någon kännedom om samtliga detaljer kring brottet, t.ex. var och när det förövades. Däremot vore det inte tillräckligt att det finns anledning att någon ägnar sig åt brottslig verksamhet då sådan verksamhet endast kan utövas men inte förövas.[102]

Husrannsakan får även i vissa fall ske hos annan än den som är misstänkt för brott. Enligt 28 kap 1 § andra stycket får husrannsakan hos annan än den misstänkte ske om, brottet förövats hos personen, den misstänkte gripits hos personen eller om det annars förekommer synnerlig anledning att det genom en husrannsakan skall anträffas föremål som är underkastat beslag eller om husrannsakan kan leda till någon annan vinning i utredningen om brottet. För att få genomföra en husrannsakan hos annan än den misstänkte förutsätter det alltså ett högre beviskrav än vad som gäller för en normal husrannsakan. Med synnerlig anledning att anta får anses innebära att man i stort sett skall vara säker på att åtgärden leder till det önskvärda resultatet. Detta kan uttala sig genom att det finns en faktisk omständighet som påvisar att man skall finna ett föremål eller få vinning i utredningen av brottet.[103]

5.4 Omfattningen av åtgärdena

Föreligger anledning att anta att ett brott har förövats får husrannsakan företas i hus, rum eller slutet förvaringsställe. Med hus avses inte endast bostadshus utan även byggnader såsom fabriker, magasin och uthusbyggnader. Rum innefattar även kontors- och lagerlokaler samt hytter och rum på fartyg. Som ett slutet förvaringsställe betraktas exempelvis en stängd bil eller ett kassafack i bank.[104] Polisrättsutredningen menade att en undersökning av ett föremål bör betraktas som ett tvångsmedel på samma sätt som en undersökning av rum eller liknande utrymmen betraktas som sådant. Detta skulle gälla oavsett om föremålet finns i någons besittning eller inte, eftersom undersökningen ändå får betraktas som ett intrång i ägarens rättssfär.[105]

Utan stöd i lag skulle undersökningar av låsta eller slutna utrymmen som kan betraktas som förvaringsutrymmen komma att utgöra brottsliga handlingar genom kriminaliseringen av olaga intrång i 4 kap 9 § BrB. Ett omdiskuterat ämne är huruvida förvaringsstället måste vara låst för att det

[100] Se 23 kap. 1 § RB.
[101] NJA II 1943 s. 369.
[102] Ekelöf, Ett problem med hemlig avlyssning , SvJT 1982 s. 658.
[103] SOU 1995:47 s. 239 f.
[104] NJA II 1943 s. 369.
[105] SOU 1995:47 s. 217 ff.

skall omfattas av bestämmelsen i 28 kap 1 § RB. Exempelvis har JO ansett att det inte skulle krävas ett beslut om husrannsakan för att undersöka en bil som är olåst och obevakad.[106] Med anledning av detta skulle man således kunna tänka sig att det krävs att föremål, där man kan förvara andra föremål, skall vara låsta för att en undersökning av föremålet skall omfattas av reglerna om husrannsakan.[107] En annan uppfattning är att det i många fall inte är någon skillnad mellan den integritetskränkning som föranleds av undersökningen av ett låst förvaringsutrymme eller ett utrymme som enbart är stängt, varför det inte skulle vara lämpligt att göra sådana gränsdragningar.[108]

Frågan om ett föremål skall vara låst, eller om det är tillräckligt att det är stängt, för att betraktas som ett slutet förvaringsutrymme kan få betydelse för undersökningar av datorer. Sett ur det intresse som skyddas av grundlagen kan informationsbehandlingen i en dator och ett traditionellt arkiv oftast framstå som lika skyddsvärda. Detta borde vara särskilt tänkbart med anledning av de möjligheter till lagringskapacitet som erbjuds genom den digitala tekniken samt att allt fler pappershandlingar, som omfattas av grundlagsskyddet, ersätts av elektroniska handlingar.[109] En annan fråga är huruvida informationen som finns lagrad i datorn måste vara låst genom tekniska lösningar som lösenord eller behörighetsbegränsningar för att förvaringen skall anses utgöra ett slutet förvaringsställe. Vid införandet av reglerna om ADB-revision i bevissäkringslagen (1975:1027) för skatte- och avgiftsprocessen, menade dock departementschefen att datorer inte kunde jämställas med sådant förvar eller utrymme för vilket en husrannsakan krävs för en undersökning. Enligt departementschefen omfattade en eftersökning endast själva uppletandet av vissa bevismedel, varför en bearbetning av information i den skattskyldiges egen dator skulle falla utanför tillämpningsområdet.[110] Ett sådant synsätt skulle alltså innebära att myndigheternas tillträde till ett datorutrymme inte skulle innebära ett ingrepp i den enskildes fri- och rättigheter enligt 2 kap 6 § RF. Det har dock uttryckts en viss restrektivitet när det kommer till att överföra traditionella rumsbegrepp till tekniska miljöer, vilket förmodligen även är en anledning till den sparsamma lagstiftningen på området. Sådan liknelser skulle kunna leda till att tvångsmedelsanvändningen blir helt beroende av olika tekniska förutsättningar istället för att vara beroende av de begränsningar som uppställs i lagstiftningen.[111]

För att få en lagstiftning som, åtminstone till viss del, reglerar eftersökandet av information i datorer lade Datastraffrättsutredningen fram ett förslag om införandet av en ny paragraf i 28 kap RB. Paragrafen angav att vad som

[106] JO 1974 s. 128.
[107] Fitger 28:6.
[108] Ekelöf, Rättegång III s. 74.
[109] SOU 1992:110 s. 351.
[110] Prop 1987/88:65 s. 62.
[111] Ds 2005:6 s. 281.

nämns i kapitlet om slutet förvaringsställe även skulle gälla förvar av data för automatisk databehandling.[112]

5.5 Beslut om husrannsakan

Ett beslut om en reell husrannsakan fattas antingen av åklagare, förundersökningledare eller av rätten.[113] Normalt sett borde åklagaren vara den som fattar beslut om husrannsakan.[114] Om en husrannsakan kan antas bli av stor omfattning eller medföra synnerlig olägenhet för den som drabbas av åtgärden, bör istället rätten fatta beslut om husrannsakan, om det inte föreligger fara i dröjsmål. Eftersom rättens beslutsbehörighet endast är fakultativ inkräktar den inte på något särskilt område för åklagarens behörighet att fatta beslut. Att en husrannsakan kan bli av stor omfattning borde i första hand ha sin utgångspunkt i den rent fysiska omfattningen av åtgärden.[115] Som exempel anges i förarbetena husrannsakan i större affärslokaler, kontor eller hotell vara åtgärder som till omfattningen kan medföra att rätten bör fatta beslut om husrannsakan.[116] Även om en husrannsakan kan anses särskilt omfattande på grund av att den företas i en stor lokal eller flera olika utrymmen är den tidsmässiga varaktigheten av ingripandet och omfattningen av resultatet av husrannsakan av mindre betydelse. Exempelvis ansåg JO att en husrannsakan som pågick under två dagar och resulterade i ett stort antal beslag, inte kunde anses vara en husrannsakan av stor omfattning. Däremot skulle sådana omständigheter kunna medföra synnerlig olägenhet för den som drabbas av åtgärden varför rätten bör fatta beslutet om husrannsakan.[117]

Någon ytterligare vägledning av vad som kan medföra synnerlig olägenhet för den som drabbas av en husrannsakan finns inte att hämta från förarbetena. Med beaktande av vad som får anses utgöra en husrannsakan av stor omfattning borde ingripanden som medför synnerlig olägenhet främst grunda sig på omfattningen av det integritetsintrång som följer av ingripandet. Denna föresats angavs av Polisrättsutredningen som ansåg att desto starkare integretetsintrång som följer av åtgärden, desto starkare skäl för att rätten skall besluta i frågan.[118] Förutom att en husrannsakan kan föranleda synnerlig olägenhet med anledning av varaktigheten och omfattningen av resultatet av åtgärden kan vissa lokaler och utrymmen vara av särskild integritetskänslig karaktär. Som exempel kan tas att det i lokaler av sådant slag bedrivs verksamhet som omfattas av tystnadsplikt eller är skyddade av andra skäl. Åtgärder som riktas mot t.ex. advokatkontor eller tidningsredaktioner torde därför vara förbehållna att beslutas av rätten.[119]

[112] SOU 1992:110 s. 23.
[113] Se 28 kap 4 § RB.
[114] Lindberg s. 533.
[115] JO 1992/93 s. 143.
[116] SOU 1938:44 s. 329.
[117] JO 1963 s. 103.
[118] SOU 1995:47 s. 305.
[119] Ibid. s. 304.

I 28 kap. 5 § anges det att beslut om husrannsakan även får fattas av polisman om det skulle föreligga fara i dröjsmål. Att det föreligger fara i dröjsmål borde i allmänhet innebära att åtgärden är så brådskande att man vid ett avvaktande med ingripandet skulle förlora ändamålet med åtgärden. För att avgöra om det föreligger fara i dröjsmål måste man se till omständigheterna i det enskilda fallet varför en allmän definition av begreppet är närmast omöjlig.[120]

Det finns inga formkrav på ett beslut om husrannsakan som kan vara såväl skriftligt som muntligt. Det krävs dock att beslutet dokumenteras på något sätt (se nedan 5.7.2). För att ett beslut skall kunna verkställas i enligt med gällande rätt krävs det att, det av dokumentationen, framgår vad som varit grunden för beslutet samt att omfattningen av den vidtagna åtgärden anges.[121] Av beslutet skall framgå vilka områden, t.ex. bostadsutrymmen, som åtgärden skall omfatta samt vilka eventuella föremål som skall eftersökas. Vidtas en husrannsakan i syfte att utröna omständigheter som har betydelse för utredningen om brott är det svårare att närmare precisera vad åtgärden skall omfatta. Normalt sett kompletteras därför beslutet med muntliga instruktioner, exempelvis över vilken bevisning som skall eftersökas.[122]

5.6 Verkställigheten av åtgärder i digital miljö

Det finns inga bestämmelser som närmare reglerar genomförandet av en husrannsakan. Genom nya arbetsrutiner har polisen utvecklat en praxis för att verkställa åtgärder i miljöer där det finns inslag av digital teknik. Oavsett om den digitala informationen är lagrad på en persondator, på en datorserver eller på annat datatekniskt hjälpmedel borde det krävas ett beslut om husrannsakan för att polisen skall få tillgång till den lokal eller utrymme där datorn befinner sig i. När väl polis fått tillgång till utrymmet finns flera olika tillvägagångssätt för att omhänderta den eftersökta informationen. En husrannsakan i digitala miljöer skiljer sig därför på flertalet sätt i jämförelse med en traditionell husrannsakan. Som nämnts ovan kan en husrannsakan genomföras varefter påträffade datorer eller bärare av digital information tas i beslag för att senare undersökas i myndighetens lokal. Ett andra alternativ är att istället genomföra en total kopiering av hårddisken i den påträffade datorn (spegling) på platsen för husrannsakan. Som ett sista alternativ kan man, på platsen för husrannsakan, välja att selektivt kopiera viss utvald information som finns lagrad på datorutrustning. Vilket alternativ man väljer beror mycket på det aktuella brottets beskaffenhet och på den miljö som åtgärden skall verkställas i.[123] Nedan följer en närmare genomgång av dessa olika metoder.

[120] Ibid. s. 165.
[121] Lindberg s. 535.
[122] Ibid. s. 536.
[123] Angerfeldt s. 7.

5.6.1 Total kopiering (”Spegling”)

En ”spegling” innebär att man framställer en exakt kopia av en dators hårddisk. Resultatet av en spegling är därför i princip detsamma som om man hade tagit datorutrustningen i beslag. Genom en spegling får man tillgång till samma information som när datorn tas i beslag och dessutom skapar speglingen samma förutsättningar för att, i efterhand, analysera informationen i en säker miljö. Metoden har en stor fördel i och med att man kan undvika beslag som skulle innebära sådan skada som inte står i proportion till själva brottet. Särskilt när åtgärder vidtas mot företag där man har ett stort beroende av IT-system eller där risken för att tredje man skall komma till skada torde en spegling vara att föredra framför ett beslag av datorutrustning.[124] Har polisen vid en husrannsakan valt att ta en dator i beslag kan en spegling genomföras i polisens lokaler för att möjliggöra ett hävande av beslaget och på så sätt minska det intrång som följer av att utrustning hålls i beslag under en längre tid.

I praktiken innebär en spegling att man framställer en logiskt identisk kopia av den ursprungliga hårddiskens innehåll. Vid en spegling kopieras alltså inte endast de filer som finns på hårddisken utan även hela filstrukturen inklusive dolda och raderade filer. Däremot finns det en risk att viss data går förlorad vid kopieringen. Detta är särskilt fallet med så kallad metadata[125], som utgörs av mer eller mindre ”osynlig data” vilken kan lagras i oåtkomliga sektorer av en dator. Det får dock anses vara en liten risk för att användare skall kunna gömma information i sådana oåtkomliga sektorer. Däremot kan metadata bidra med viktig information över hur datasystemet har använts varför man inom polisen fortlöpande arbetar med metoder för att även kunna komma åt sådan information.[126] Jämfört med beslag av föremål får en spegling även anses minska risken för att utsätta datorer och andra föremål för skada. En spegling kan dock vara mycket tidskrävande och ställer höga krav på särskild utrustning och utbildad personal för att bistå vid platsen för åtgärden.[127]

5.6.2 Selektiv kopiering

Kan man på förhand ha klart för sig vilken information som skall eftersökas, kan en total spegling anses överflödig. Den verkställande myndigheten kan därför välja att endast selektivt kopiera visst material från en dator. Åtgärder i form av beslag av datorer eller omfattande speglingar kan även anses för ingripande för att stå i proportion till brottet varför man istället väljer att sålla ut onödig information på plats och endast kopiera det som verkligen är nödvändigt för utredningen. Att selektivt kopiera information torde vara den

[124] Ibid. s. 7 f.
[125] Se ovan Kapitel 2.
[126] Kronqvist s. 81f.
[127] Angerfeldt s. 7 f.

smidigaste praktiska lösningen och dessutom den snabbaste. Skadan av sådana åtgärder får betraktas som relativt liten och samtidigt ställs inga särskilda krav på särskild teknisk utrustning eller särskilt utbildad personal. Från rättssäkerhetssynpunkt har metoden även den fördelen att den inte producerar någon överskottsinformation. Däremot kan sådan information givetvis komma att behandlas under sökningen efter det som skall kopieras. För att effektivt kunna utföra en selektiv kopiering krävs det dock att de som verkställer åtgärden har någon vetskap om den information som man söker efter. Vet man inte exakt vad det är för information man söker efter kan det underlättas genom att man i förväg upprättar listor med olika sökord för att underlätta sållandet av information. Vid en selektiv kopiering finns det även alltid en risk för att man vid sökningen skall missa bevisning som skulle vara till nytta för utredningen om brott.[128]

5.6.3 Undersökningen av föremål på plats för husrannsakan

Som framgår av RB 28 kap 1 § får föremål som betraktas som slutna förvaringsställen endast undersökas med ett beslut om husrannsakan. Detta torde innebära att föremål som inte faller under denna kategori får undersökas som ett led i den husrannsakan som företas i det rum där föremålen påträffas. En annan tankegång är att föremålet måste tas i beslag för att närmare få undersökas. Att applicera ett sådant synsätt på undersökning av datorer som påträffas vid husrannsakan är dock inte helt utan invändningar. Med anledning av den praxis som utvecklats på området, samt med tanke på bristen av lagstiftning över tillvägagångssättet vid en husrannsakan, får det anses klargjort att datorer inte utgör sådana föremål som skulle kräva ett särskilt beslut om husrannsakan för att få undersökas närmare. Självfallet krävs det i regel ett beslut om husrannsakan för att polis skall kunna få tillträde till den lokal där datorutrustningen finns, varför undersökningen av en påträffad dator borde utgöra en sekundär fråga.[129]

Datastraffrättsutredningen som föreslog att förvar av data skulle likställas med slutna förvaringsställen, vilket skulle möjliggöra eftersökande i påträffade datorer, ansåg att undersökningar av datorer på platsen för husrannsakan oftast kan motiveras utifrån den berördes intressen. Valmöjligheten står ju närmast i att vidta andra mer ingripande åtgärder istället varför en rättstillämpning som möjliggör för undersökningar i datorer på platsen för husrannsakan torde vara förenlig med såväl behovs- som proportionalitetsprincipen.[130]

Även om undersökningar av datorer kan syfta till att utröna omständigheter som är av betydelse för en brottsutredning finns det alltså inget uttryckligt lagstöd för att polisen skall få genomföra sådana undersökningar. Det har ansetts att polisen borde ha samma befogenheter när det kommer till att

[128] Ibid. s 8, s 10.
[129] Fitger s. 28:7.
[130] SOU 1992:110 s. 368.

genomsöka en påträffad dator som de har för att undersöka och ta del av exempelvis handlingar som påträffas vid en husrannsakan.[131] Sådana påpekanden kan ge upphov till frågor kring själva gränsdragningen mellan husrannsakan och beslag, vilken kan vara svårare att nyansera när man befinner sig i digitala miljöer. Skulle en handling tas i beslag rör det sig utan tvekan om en form av tvångsingripande. Skulle en polisman istället välja att ta del av handlingens innehåll genom att läsa handlingen kan förfarandet däremot inte anses utgöra något tvångsmedelsförfarande. Detta gäller oavsett om det skulle krävas att polisen utför en husrannsakan för att få tag på handlingen. Normalt sett anses en husrannsakan som syftar till att eftersöka ett föremål avslutad i det skede som föremålet påträffas.[132] Tar man del av handlingens innehåll på platsen för husrannsakan kan det dock anses utgöra en fortsättning av husrannsakan just av den anledningen att man alltjämt befinner sig i lokalen för den vidtagna husrannsakan. Ett motsvarande tankesätt torde kunna appliceras när polisen väljer att undersöka en dator som påträffats efter husrannsakan.[133] Datastraffrättsutredningen ansåg det dock vara mindre lämpligt att låta platsen för åtgärden vara avgörande vid bedömningen av om en åtgärd skall ses som husrannsakan eller beslag. Istället skulle ändamålet med åtgärderna vara avgörande på så sätt att åtgärder som syftar till att söka efter objekt underkastas reglerna om husrannsakan och att reglerna om beslag tillämpas för åtgärder som syftar till att säkerställa och närmare undersöka data.[134] En undersökning av datorer skiljer sig dock på många sätt från en undersökning av andra föremål. Datorteknisk utrustning kan innehålla en väldigt stor mängd information och delar av denna kan vara av särskild känslig natur vilket kan leda till att det blir svårt att på förhand inse omfattningen av det integritetsintrång som följer av undersökningen. Dessutom kan en undersökning leda till upptagningarna i datorn skadas. Med anledning av detta har det föreslagits att man skall införa särskilda regler om polisens befogenheter att inhämta information som lagrats i datorsystem.[135]

5.7 Rättssäkerhetsgarantier

5.7.1 Närvaro vid husrannsakan

För att tillförsäkra att genomförandet av en husrannsakan sker med iakttagande av proportionalitet och i linje med ändamålet för åtgärden, föranstaltas det i 28 kap. 7 § RB att ett av förrättningsmannen anmodat vittne skall närvara vid husrannsakan. Skyldigheten att ha ett vittne närvarande sträcker sig dock endast till att avse fall där ett sådant anmodande är möjligt. Detta innebär att det inte föreligger hinder mot att genomföra en husrannsakan utan ett närvarande vittne om

[131] SOU 1995:47 s. 184.
[132] Ibid. s. 178.
[133] Ibid.
[134] SOU 1992:110 s. 369.
[135] SOU 1995:47 s. 178.

förrättningsmannen gjort vad som skäligen kan ankomma honom för att skaffa sådant vittne.[136] Av lagrummet framgår även att förrättningsmannen har möjligheten att ta med en sakkunnig eller annat biträde att bistå vid genomförandet av förrättningen. Angående utredningen av ett skattebrott påpekade JO att en sakkunnig kunde bistå förrättningen genom att påvisa vilka handlingar som var av intresse för utredningen vilket innebar att efterkommande beslag inte behövde omfatta onödiga handlingar.[137]

Av andra stycket i 28 kap. 7 §, framgår det att den hos vilken husrannsakan företas skall ha möjlighet att övervaka genomförandet av åtgärden. Här erbjuds även en möjlighet, för den som husrannsakan företas mot, att tillkalla ett vittne om så kan ske utan att undersökningen fördröjs. Har varken den som husrannsakan företas mot, dennes vittne eller dennes husfolk närvarit vid genomförandet av undersökningen skall den som husrannsakan företas mot, så snart som möjligt, underrättas om de vidtagna åtgärderna. När i sådana fall husrannsakan vidtas utan att den som berörs av åtgärden, eller dennes företrädare, är närvarande har det ansetts särskilt betydelsefullt att ett ojävigt vittne finns på plats under undersökningen.[138]

5.7.2 Dokumentering vid husrannsakan

En närmare översikt över de grundläggande förutsättningarna och syftena med dokumentation av tvångsmedel finns i avsnitt 4.5.2. Till skillnad från ett protokoll över ett beslag kommer protokollet över en husrannsakan inte att omfatta själva beslutet om husrannsakan eftersom dessa upprättas vid skilda tillfällen. Förutom innehållet i beslutet skall det även framgå vem som fattat beslutet och tidpunkten för detta. Ett beslut om husrannsakan upprättas givetvis före det att åtgärden vidtagits. När en husrannsakan avslutas skall protokoll föras enligt 28 kap. 9 § RB. Av protokollet skall framgå ändamålet med undersökningen, samt vad som förekommit under husrannsakan. Gällande ändamålet med åtgärden har det ansetts tillräckligt att det anges att ändamålet t.ex. varit att söka efter föremål som skall tas i beslag. Det är vanligt att grunderna för husrannsakan anges genom att man kryssar på förhand angivna grunder för en husrannsakan på en, till delvis ifylld, blankett för upprättande av protokoll över husrannsakan. Detta kan leda till att skälen som anges i protokollet inte överensstämmer med de skäl för beslut om husrannsakan som angivits i beslutet.[139] Den som drabbas av husrannsakan har möjligheten att få kännedom om omständigheterna kring undersökningen och även uppgift om det brott som misttanken avser. Eftersom en husrannsakan inte får användas som medel för att efterspana brott har JO uttryckt det vara av särskild vikt att det eller de brott som misstanken avser fullständigt anges i protokollet. Skulle det vid undersökningen påträffas föremål som grundar misstanke om annat brott och husrannsakan utvidgas till att omfatta även det nyupptäckta brottet

[136] Fitger s. 28:21.
[137] JO 1978/79 s. 280.
[138] JO 1974 s. 87.
[139] Lindberg s. 552.

måste detta framgå tydligt av protokollet.[140] Att protokollet skall innehålla uppgifter vad som förekommit vid förrättningen innebär att protokoll måste föras även om åtgärden inte resulterat i att något har påträffats.[141] Till skillnad från protokoll över beslag finns det inget formellt krav på att ett protokoll över husrannsakan skall upprättas omedelbart. Det är tillräckligt om protokollet utgörs av anteckningar som sedan tillförs förundersökningen.[142]

5.8 Husrannsakan i IT-miljö

Då en husrannsakan oftast sker i syfte att eftersöka visst föremål som skall tas i beslag är de lagtekniska komplikationerna för sådana åtgärder som företas i digitala miljöer i stort sett kopplade till de ovan nämnda behoven för anpassning av beslagsreglerna. Då IT skapar nya möjligheter till eftersökande av information har det istället diskuterats hur reglerna om husrannsakan kan anpassas till att eftersöka information i digitala miljöer. Förutom att jämställa upptagningar i datorer med slutna förvaringsställen framställde Datastraffrättsutredningen även ett förslag om husrannsakan via telenät. En sådan bestämmelse ansågs dock kräva tydliga begränsningar eftersom de naturliga gränser som uppställs genom indelningar i hus, rum och förvar inte existerar i en digital omgivning. Husrannsakan via telenät var främst avsedd att vidtas i en dator som påträffas på platsen för en husrannsakan och inte över distans.[143] Sådana ingrepp skulle alltså främst påverka det praktiska utförandet av undersökningen av den påträffade datorn. Enligt förslaget skulle det dock ges en möjlighet att, över distans, genomföra en husrannsakan via telenät mot sådana elektroniska anslagstavlor som är ägnade att användas vid brott eller vilkas spridande utgör brott. För att få använda husrannsakan via telenät i annat syfte skulle det enligt förslaget därför krävas att det föreligger särskilda skäl.[144] Införandet av regler som de föreslagna om husrannsakan via telenät torde kunna klargöra de oklarheter som råder för polisens befogenheter att samla in bevis från Internet. Eftersom Internet är allmänt tillgängligt finns det inga hinder för brottsutredande myndigheter att söka information som finns tillgänglig på Internet. Däremot är rättsläget oklart huruvida en polisman, genom att använda sig av falska användaruppgifter, får bereda sig tillträde till sådana sidor på Internet som normalt sett inte är tillgängliga för allmänheten.[145] När det kommer till informationsinsamling via Internet skapas även oklarheter utav det otydliga regelverk som reglerar Internet och som i mycket beror på Internets gränsöverskridande karaktär.

Möjligheterna att genomföra en husrannsakan enbart med tekniska hjälpmedel utan någon hänsyn till var den dator som skall undersökas

[140] JO 1956 s. 95.
[141] JO 1991/92 s. 108.
[142] Lindberg s. 551.
[143] SOU 1992:110 s. 363 f.
[144] Ibid. s. 23.
[145] Kronqvist s. 71.

befinner sig, har även behandlas i promemorian Ds 2005:6. I utredningen påpekades det att reglerna om husrannsakan, genom 28 kap 2 a § om husrannsakan i transportmedel och 3 § om husrannsakan på allmänt tillgängliga platser, redan har anpassats till särskilda miljöer och att en särreglering för husrannsakan i IT-miljöer därför inte borde vara något okonventionellt. En husrannsakan som genomförs via distans kan dock medföra komplikationer om fallet skulle vara att den utrustning som skall undersökas befinner sig utomlands. Då skulle det krävas att de brottsutredande myndigheterna begär internationell rättslig hjälp för att få fram informationen eftersom svensk myndighetsutövning inte får bedrivas på annan stats territorium. Den föreslagna regeln om husrannsakan utformades i stort efter den grundläggande bestämmelsen om husrannsakan i 28 kap 1 § RB. Lydelsen av förslaget skilde sig dock på så sätt att den inte gav någon rumslig begränsning för de vidtagna åtgärderna. Givetvis skulle tillämpning begränsas att endast avse datorer eller datorsystem som befinner sig i Sverige, med anledning av de ovan nämnda territoriella begränsningarna för användning av straffprocessuella tvångsmedel. Utformningen av lagförslaget skilde sig även på så sätt att syftet med åtgärden angavs vara att söka efter data i elektronisk form.[146] Skulle syftet med en åtgärd i IT-miljö vara något annat än att söka efter elektronisk data tillämpas således regeln i 28 kap 1 § RB. I övrigt stämde förutsättningarna för en husrannsakan i IT-miljö i stort sett överens med reglerna för åtgärder i traditionella miljöer. Den tekniska avgränsningen av bestämmelsen gjordes så vid som möjligt genom att regeln omfattar såväl datorer, datorsystem och delar därav, som annan liknande teknisk utrustning.[147]

[146] Ds. 2005:6 s. 367.
[147] Ibid.

6 Uppgifter om elektronisk kommunikation

Som tidigare nämnts utgör insamlingen av information otvivelaktigt ett viktigt inslag i polisens arbete för att utreda och bekämpa brottslighet. Det har även konstaterats att inhämtande av information, i sig, inte kan anses utgöra ett tvångsmedelsförfarande.[148] Polisrättsutredningen ansåg i sitt betänkande att den tekniska utvecklingen lett till att reglerna om beslag och husrannsakan, samt hemlig teleavlyssning och teleövervakning, framstår som otillräckliga när det gäller polisens möjligheter att inhämta information. Detta gällde särskilt när det rör sig om datalagrad information. Som exempel nämndes att det skydd, som framställs i 2 kap. 6 § RF, mot undersökning av brev eller annan förtrolig försändelse inte omfattar förtroliga uppgifter som lagras i en dator. Visserligen ger straffbarheten av dataintrång ett visst skydd för otillbörliga åtgärder av datalagrat material men detta skydd upprätthålls oavsett om åtgärden medför ett otillbörligt integritetsintrång eller ej. Med anledning härav ansågs det vara av vikt att man skapade enhetliga regler för polisens arbete att inhämta information, oavsett vilket tekniskt hjälpmedel som används för överföring av informationen.[149] Som framgår av kapitel två efterlämnas det alltså flertalet digitala spår vid en normal användning av en dator. Dessa uppgifter kan givetvis få relevans som underlag och stöd i en förundersökning om brott. De digitala spåren lämnas exempelvis när en dator används för att kommunicera, antingen med en annan dator eller med annan kommunikationsutrustning som exempelvis en mobiltelefon. Förutom att själva innehållet av kommunikationen kan vara av intresse för en brottsutredning, kan även uppgifter såsom när, var, under vilken tid och mellan vilka som kommunikationen i fråga fördes, vara av stor betydelse för att kunna utröna omständigheter kring brottet.

6.1 Lagen om elektronisk kommunikation (LEK)

I svensk rätt regleras behandlingen av uppgifter om elektronisk kommunikation genom lagen (2003:396) om elektronisk kommunikation (LEK). Lagen skall tillförsäkra att enskilda och myndigheter får tillgång till säkra och effektiva elektroniska kommunikationer. Uppgifter om elektroniska meddelanden samlas under begreppet trafikuppgifter, som utgörs av uppgifter som behandlas i syfte att befordra ett elektroniskt meddelande via ett kommunikationsnät, eller för att fakturera ett sådant meddelande.[150]

[148] SOU 1995:47 s. 178.
[149] Ibid. s. 181 f.
[150] Se 6 kap. 1 § LEK.

Tillämpningsområdet för LEK omfattar inte själva innehållet av ett elektroniskt meddelande som överförs via ett elektronisk kommunikationsnät eller kommunikationstjänst. Lagen riktar sig istället mot regleringen kring driften av själva elektroniska kommunikationsnäten och kommunikationstjänsterna.[151] För att myndigheterna skall kunna få ta del av innehållet av en kommunikation som sker från en dator via så kallad IP-telefoni krävs det ett beslut om hemlig teleavlyssning.[152] På samma sätt skulle det krävas ett beslut om hemlig teleövervakning för att ta del av ett meddelande som kommuniceras från en dator, exempelvis e-post.[153] Till skillnad från reglerna om husrannsakan och beslag är reglerna för hemlig teleavlyssning och hemlig teleövervakning redan teknikneutrala. Dessa två hemliga tvångsmedel är exklusivt förbehållna när det kommer till att få fram information om elektroniska meddelanden. Detta följer av den allmäna principen om *lex specialis* (dvs att lagar som reglerar speciella förhållanden har företräde framför lagar med allmänt hållna regler) och medför således att myndigheterna inte får använda sig av åtgärder som husrannsakan och beslag för att få fram sådana uppgifter hos en teleoperatör.[154] Då det får anses föreligga en rätt för polisen att undersöka en påträffad dator vid en husrannsakan, eller en dator som tagits i beslag, finns det dock inget hinder mot att polisen tar del av sådana meddelanden som finns lagrade i datorn då dessa inte är under befordran.

Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har emellertid en skyldighet att i vissa fall lämna ut uppgifter om elektroniska meddelanden till de brottsutredande myndigheterna. Skyldigheten att lämna ut sådana uppgifter regleras i 6 kap. 22 § LEK. I vissa fall kan det vara tillräckligt för de brottsutredande myndigheterna att de får vetskap om uppgifter kring ett abonnemang hos en teleoperatör som kan kopplas till vissa aktiviteter som kunnat spåras från en viss IP-adress. För att få ut uppgifter om abonnemang, vid en misstanke om brott, krävs det inte mer än att fängelse är föreskrivet för brottet och att det vid en bedömning kan antas att gärningen kommer att föranleda annan påföljd än böter.[155] För att det skall föreligga en skyldighet för utlämnande av andra uppgifter om ett elektroniskt meddelande, exempelvis tidpunkter och andra angivelser för kommunikationen, krävs det dock att det inte är föreskrivet lindrigare straff än två års fängelse för brottet.[156]

Syftet med lagen om elektronisk kommunikation är främst att tillförsäkra säker och effektiv elektronisk kommunikation. Med säker elektronisk kommunikation avses inte enbart krav på viss driftsäkerhet[157] för den som tillhandahåller elektroniska kommunikationstjänster, utan även ett krav på

[151] Se 1 kap. 4 § LEK.
[152] Se 27 kap. 18 § RB.
[153] Se 27 kap. 19 § RB.
[154] SOU 1998:46 s. 371 ff, JO 1997/98 s.47 ff.
[155] Se 6 kap. 22 § 1 st 2 p LEK.
[156] Se 6 kap. 22 § 1 st 3 p LEK.
[157] Se 5 kap. 7 § LEK.

att iaktta det integritetsskydd som förklaras närmare i 6 kap. LEK.[158] Av 6 kap. 5 § LEK framgår det att trafikuppgifter som lagras eller behandlas på annat sätt, skall utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande. Trafikuppgifter som behövs för fakturering får dock enligt 6 kap. 6 § sparas så länge de behövs för faktureringsperioden.

6.2 EU direktiv 2006/24/EG

Genom Europaparlamentets och rådets direktiv 2002/58/EG skall gemenskapens bestämmelser harmoniseras kring rätten till integritet, i synnerhet när det gäller behandling av personuppgifter vid elektronisk kommunikation. Direktivet skall även säkerställa fri rörlighet för sådana uppgifter, utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen. Direktivet bygger i stora delar på de principer som fastslagits genom dir. 97/66/EG om skydd av personuppgifter och integritet och syftar i mycket att ersätta detta direktiv med regler som ger ett skydd för alla användare av allmänt tillgängliga elektroniska kommunikationstjänster, oavsett vilken teknik som används.[159]

Direktivet, som till delar bygger på grundläggande fri- och rättigheter, medför i sin nuvarande form inga större betänkligheter för den svenska lagstiftningen på området. Kraven på säkerhet och integritet som framställs i direktivet är tillförsäkrade genom bestämmelserna i LEK. I Mars 2006 presenterade dock Europaparlamentet och rådet ett nytt direktiv[160] om ändringar till direktiv 2002/58/EG. Detta direktiv skall, i sin helhet, vara implementerat i svensk rätt senast år 2009, vilket kommer att medföra ändringar i den svenska lagstiftningen om elektronisk kommunikation. Syftet med direktivet är att få en harmoniserad lagstiftning kring skyldigheten för leverantörer av allmänna elektroniska kommunikationstjänster eller kommunikationsnät att lagra vissa trafikuppgifter för att hålla uppgifterna tillgängliga för de nationella myndigheterna i deras arbete att förebygga, utreda, avslöja och åtala allvarliga brott som terrorism och organiserad brottslighet.[161] En sådan skyldighet för leverantörer att lagra uppgifter är alltså direkt motsägande bestämmelsen i 6 kap. 5 § LEK, där det framgår att uppgifter skall raderas och avidentifieras när de inte längre behövs. Viktigt att poängtera är dock att direktivet, likt bestämmelserna i LEK, endast tar sikte på uppgifter om meddelandet och inte tillämpas på själva innehållet av meddelandet.

De uppgifter som skall omfattas av lagringsskyldigheten utgörs, enligt Artikel 5, av uppgifter som är nödvändiga för att spåra och identifiera, en kommunikationskälla, slutmålet av en kommunikation, datum, tidpunkt och

[158] Prop. 2002/03:110 s. 354.
[159] Se förordet till Dir. 2002/58/EG.
[160] Direktiv 2006/24/EG
[161] Se Artikel 1 direktiv 2006/24/EG.

varaktighet för en kommunikation samt uppgifter som är nödvändiga för att identifiera, typen av kommunikation, den utrustning som har använts eller tros ha använts för kommunikationen eller för att identifiera var någonstans viss mobil kommunikationsutrustning är belägen. Dessa uppgifter kan härröra från kommunikation med hjälp av såväl fast telefoni och mobiltelefoni som Internet. Lagringstiden för dessa uppgifter skall uppgå till minst sex månader och högst två år från det datum då kommunikationen ägde rum. Enligt Artikel 9 skall varje medlemsstat instifta en tillsynsmyndighet som övervakar bestämmelserna om lagring av uppgifter.

7 En utvidgad tvångsmedelsanvändning

Som en huvudpunkt i datastraffrättsutredningens direktiv framgick det att myndigheternas tillgång till information inte kan få vara beroende av det sätt på vilken information finns lagrad.[162] Idag anses utredningens förslag till stora delar vara obsolet. Det vore väl märkligt om läget skulle vara annorlunda då informationstekniken har utvecklats i en rasande fart under de senaste 15 åren. Faktum är dock att flera av de problem som utredningen påpekade, främst vad gäller att likställa datalagrat material med fysiskt material, fortfarande är olösta och uppe för diskussion.

Med anledning av de olika betänkligheter som uppstår vid tvångsåtgärder i digital miljö kan man fråga sig om det är tillräckligt att få ett regelsystem som är anpassat till tekniken eller om det skulle krävas mer omfattande åtgärder i form av införandet av nya tvångsmedel. De frågor som rör husrannsakan och beslag i digital miljö har redan diskuterats under en lång period utan att resultera i några lagändringar som syftar till att ge ett regelsystem som är väl anpassat till dagens teknik. Å andra sidan har det under denna tid utvecklats en praxis för verkställighet av husrannsakan och beslag i digitala miljöer där man inom de brottsutredande myndigheterna har väl anpassade metoder för bevissäkring i sådana miljöer. Trots detta har det under de senaste åren ifrågasatts huruvida dessa metoder kan anses tillräckliga och huruvida teknikens utveckling inte borde leda till ett behov av nya tvångsmedel.

När man talar om en utvidgad användning av tvångsmedel kan det vara av intresse att närmare se varför denna utvidgning sker. En förklaring är att det sker en ”normalisering av det exceptionella”. Genom att vissa särskilda hotbilder presenteras, exempelvis en alltmer utbredd terrorism, framställs motiv för införandet av nya metoder för brottsbekämpning. Efter det att de nya metoderna införts tenderar dessa dock att tillämpas även på lindrigare brottslighet. Att fallet skulle vara omvänt och att tvångsmedel tas ur bruk för att hotbilden inte är lika omfattande längre är dock mycket sällsynt.[163]

7.1 Hemlig dataavläsning

I betänkandet SOU 2005:38 presenterades ett förslag om att införa ett nytt tvångsmedel som benämndes hemlig dataavläsning. Genom ett beslut om hemlig dataavläsning skulle brottsutredande myndigheter kunna få tillgång till informationen som finns lagrad i datorer och dessutom skulle man även, i realtid, kunna få vetskap om de aktiviteter som utförs av datoranvändaren.

[162] SOU 1992:110 s. 333.
[163] Flyghed, Janne – Brottsbekämpning mellan effektivitet och Integritet s. 21 f.

Enligt förslaget definieras hemlig dataavläsning som att information i hemlighet avläses från ett informationssystem med hjälp av program eller annat tekniskt hjälpmedel. Någon närmare definition på begreppet informationssystem ansågs inte nödvändig eftersom begreppet redan används i många författningar och även i andra sammanhang utan någon vedertagen definition.[164] Vanligtvis ges begreppet en bred definition, som exempel kan nämnas den tolkning som ges i EU:s rambeslut om angrepp mot informationssystem där det anges att ett informationssystem utgörs av en apparat eller grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av datorbehandlingsbara uppgifter, samt datorbehandlingsbara uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av dessa för att de skall kunna drivas, användas, skyddas och underhållas.[165]

Tvångsmedlet skulle fungera på så sätt att informationen i ett datorsystem avläses genom att myndigheten i hemlighet skickar en viss mjukvara som, tack vare sin utformade programkod, kan ge myndigheten uppgifter om vilken information som finns i datorn och hur datorn används. Genom utformningen av programkoden för mjukvaran skulle man på så sätt kunna begränsa och precisera vad för slags information som sänds från datorn till myndigheten. När man med hjälp av hemlig dataavläsning upptäckt den information man letat efter skulle myndigheten ha flera alternativa möjligheter till att få tag på informationen. Informationen skulle t.ex. kunna sändas via Internet, radio eller till och med lagras i den genomsökta datorn för att sedan erhållas genom en framtida husrannsakan och beslag. Som ett alternativ skulle hemlig dataavläsning även kunna genomföras genom att hård- eller mjukvara, med programkod av samma funktion som ovan, installeras i en dator genom ett fysiskt ingrepp. För att genomföra en sådan installation skulle man alltså i hemlighet bereda sig tillgång till t.ex. en bostad eller arbetsplats där informationssystemet som är föremål för åtgärden befinner sig.[166]

Lagförslaget välkomnades av säkerhetspolisen, rikspolisstyrelsen och ekobrottsmyndigheten men möttes av hård kritik av övriga instanser som yttrade sig över förslaget. Även om någon lagstiftning om ett sådant nytt tvångsmedel troligtvis inte är aktuellt i dagsläget kommer delar av förslaget att presenteras här då det innehåller intressanta aspekter om bevissäkring i digital miljö. På grund av att förslaget inte har lagts under beredning har jag dock valt att inte i detalj redogöra för den föreslagna regleringen av hemlig dataavläsning.

[164] SOU 2005:38 s. 419.
[165] Europeiska Kommissionens rambeslut (EGT C 203 E, 27.8.2002) art 1 a.
[166] SOU 2005:38 s. 361.

7.1.1 Behovet av ett nytt tvångsmedel

Behovet av det nya tvångsmedlet ansågs främst ligga i hoten från den alltmer organiserade brottsligheten och den ökade terrorismen i omvärlden. Andra skäl utgjordes av möjligheterna som informationsteknikens skapar för skyddad (anonymitet) och säker (kryptering) informationsanvändning vilket leder till svårigheter i myndigheternas brottsutredande arbete.[167] Enligt utredningen har antalet brottsutredningar med påträffat krypterat material varit ett ökande problem. Att information är krypterad innebär att informationen har gjorts oläslig och att den endast kan läsas av den som innehar en krypteringsalgoritm med dithörande krypteringsnycklar. För att minska risken att information skall kunnas göras läslig kan flertalet nycklar krävas till en och samma algoritm. Någon statistik över utredningar där det påträffats krypterad information presenterades emellertid inte i betänkandet. Istället gav man några exempel från några utredningar där påträffad information varit krypterad. Av framställningen framgick inte vilken betydelse som den krypterade informationen hade för utredningen om brottet i fråga. Detta ledde till att flera remissinstanser ifrågasatte det verkliga behovet av ett tvångsmedel som hemlig dataavläsning.[168]

Här skall nämnas att ett tvångsmedel med motsvarande syfte som hemlig dataavläsning sedan några år tillbaka finns i Danmark. I den danska lagen har man valt att rada upp de brott för vilka dataavläsning kan äga rum. Det rör sig främst om allvarligare brott som kan ha samband med eller utgöra led av terrorhandlingar.[169] Det svenska lagförslaget har således en vidare utformning än vad de danska reglerna om hemlig dataavläsning har. Av utredningens arbete framgår det dock att tvångsmedlet främst har sitt behov vid planerad och organiserad brottslighet där det skulle finnas särskild kompetens på teknikområdet som används exempelvis för att uppträda i anonymitet, undangömma information och undgå upptäckt.[170]

7.1.2 Proportionalitetsavvägningen

Förutsättningarna för hemlig dataavläsning överensstämmer i mycket med regleringen av hemlig teleavlyssning[171] och hemlig kameraövervakning[172]. Således skulle det krävas ett straffminimum på två års fängelse för att man skulle få tillämpa hemlig dataavläsning som tvångsmedel. Hemlig dataavläsning skulle även få tillämpas när det föreligger misstanke om brotten dataintrång, barnpornografibrott och hets mot folkgrupp, om gärningen inte bedöms vara av ringa art. Gällande tillämpningen innehöll lagförslaget även en straffvärdeventil, enligt vilken hemlig dataavläsning även får tillämpas under förundersökning av brott där det kan antas att

[167] Ibid. s. 356 ff.
[168] JK-beslut 2005-12-08, JO-beslut 2005-12-13.
[169] Se Retsplejeloven § 791b.
[170] SOU 2005:38 s. 362.
[171] Se RB 27 kap. 18 §.
[172] Se 2 § lagen om hemlig kameraövervakning.

brottets straffvärde överstiger två år. Utredningen ansåg att de uttalanden som gjordes vid införandet av motsvarande straffvärdeventilen för hemlig teleavlyssning och hemlig kameraövervakning även skulle bli tillämpliga för hemlig dataavläsning. Här angavs bl.a. att rättens bedömning av straffvärdeventilen i princip motsvarar den bedömning som görs när rätten prövar om de omständigheter som åberopas av åklagare är tillräckliga för att ett brott skall falla in under viss brottsrubricering. Bedömningen skall i första hand utgå från omständigheterna kring gärningen men också omständigheterna kring gärningsmannens person om de är relevanta för gärningen även om det tidiga stadiet i brottsutredningen begränsar möjligheten till detta.[173]

Enligt utredningen skulle omfattningen av det integritetsintrång som följer av användning av hemlig dataavläsning vara svårt att uppskatta generellt. Man menade dock att intrånget i vart fall inte skulle komma att bli större än vid utövandet av hemlig teleavlyssning eller hemlig kameraövervakning som ansågs innefatta en mer total kontroll av, och insyn i, en persons förevaranden än vad hemlig dataavläsning skulle innebära. Risken att även andra, för utredningen ovidkommande personer, skulle drabbas av ett integritetsintrång ansågs mindre vid dataavläsning än vid andra nämnda hemliga tvångsmedel.[174]

Justitieombudsmännen (JO) menade tvärtom i sitt yttrande att hemlig dataavläsning skulle medföra mera långtgående integritetsintrång än exempelvis hemlig teleavlyssning. Vid en jämförelse menade man att den enskilde vid ett telefonsamtal har valt att delge en viss person vissa åsikter, medan den enskilde i sin datorn, av olika skäl, velat hålla viss information för sig själv. Särskilt ansågs intrånget öka i de fall som polisen bereder sig tillgång till enskilds bostad eller arbetsplats för att kunna installera teknisk utrustning för avläsning i dennes dator. Den enskilde drabbas ju då inte endast av avläsningen utan även utav intrånget i bostaden eller arbetsplatsen. Risken för att tredje man skulle komma till skada ökade även eftersom hemlig dataavläsning skulle kunna avse datorer som används av flera personer, exempelvis på arbetsplatser.[175]

Även Justitiekanslern (JK) menade att förslaget gav upphov till betänkligheter vad gäller integritetsfrågorna. I sitt yttrande påpekades förhållandet att hemlig dataavläsning eventuellt kunde aktualisera andra tvångsmedel som hemlig kameraövervakning eller rumsavlyssning, exempelvis i de fall en kamera eller mikrofon är ansluten till den avlästa datorn.[176] Datainspektionen påpekade i sin tur att möjligheten att avläsa all lagrad information i ett informationssystem samt den informationsbehandling som pågår under avläsningen och inte enbart

[173] Prop. 2002/03:74 s. 34.
[174] SOU 2005:38 s. 368.
[175] JO-beslut 2005-12-13.
[176] JK-beslut 2005-12-08.

meddelanden som är under befordran borde medföra att hemlig dataavläsning utgör ett större integritetsintrång än andra tvångsmedel.[177]

Förutom att hemlig dataavläsning, när åtgärden är av synnerlig vikt för utredningen och att skälen för åtgärden överväger det intrång och den skada som åtgärden medför, får riktas mot den som är skäligen misstänkt för brott skulle det även få tillämpas i syfte att fastställa vem som är skäligen misstänkt. Detta skulle dock förutsätta att det finns särskild anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av det informationssystem som skall avläsas. Skälen för en sådan reglering ansågs främst ligga i de svårigheter som följer utav möjligheterna till anonymitet vid användandet av informationsteknik. Även om polisen lyckas knyta en IP-adress till ett visst abonnemang är det inte alltid säkert att det är personen som står för abonnemanget som även har befunnit sig vid datorn vid tidpunkten för de relevanta händelserna. Avläsningar i sådant syfte begränsades dock till att endast avse det informationssystem som används eller har använts vid brottet.[178]

Att det måste finnas särskild anledning att anta att den misstänkte har använt sig eller kommer att använda sig av det informationssystem som skall avläsas innebar enligt utredningen att det måste finnas en faktisk omständighet som talar för att så är fallet. Endast ett antagande om att så är fallet skulle således inte vara tillräckligt.[179] Skulle avläsningen avse ett informationssystem som befinner sig hos någon annan än den som är skäligen misstänkt får avläsningen endast äga rum om det finns synnerlig anledning att anta att den misstänkte har använt sig av eller kommer att använda sig av informationssystemet. Detta högre krav på samband ansågs innebära att det i det närmaste är klart att kopplingen finns.[180]

Ett beslut om hemlig dataavläsning skall prövas av tingsrätten på ansökan av åklagaren. Beslutet skall innehålla uppgift om det eller de informationssystem som skall avläsas. Förslagsvis uppgav utredningen att detta kunde anges i form av viss statisk IP-adress eller exempelvis ”de persondatorer NN utnyttjar i hemmet”. Om den brottsbekämpande myndigheten skall få tillträde till plats för att installera tekniska hjälpmedel skall detta anges i beslutet. Ett beslut om hemlig dataavläsning är begränsat i tiden till en månad från dagen för beslutet. Föreligger förutsättningar får förlängning av beslutet dock meddelas. I övrigt får rätten även fritt föreskriva villkor för att motverka att integritetsintrånget blir alltför omfattande.[181]

7.2 Europarådets konvention om IT-relaterad

[177] Datainspektionens yttrande 2005-12-02.
[178] SOU 2005:38, s 384.
[179] Ibid. s 424.
[180] Ibid.
[181] Ibid. s 431.

brottslighet

I syfte att nå en större enhetlighet och ett ökat internationellt samarbete, för bekämpning av IT-relaterad brottslighet, upprättades Europarådets konvention om IT-relaterad brottslighet[182]. Sverige har undertecknat konventionen men har ännu inte ratificerat den fullt ut. Konventionen består dels av bestämmelser vilka syftar till att harmonisera den nationella lagstiftningen kring kriminaliseringen av vissa IT-relaterade brott som upptas i konventionen. Dessutom innehåller konventionen bestämmelser som syftar till att få medlemsstaterna att vidta åtgärder i form av processrättslig lagstiftning som skall underlätta utredning och lagföring av IT-relaterad brottslighet. Konventionen innehåller även bestämmelser som skall medföra ett ökat internationellt samarbete avseende den IT-relaterade brottsligheten.

Här skall kort nämnas några av de artiklar från konventionen som kan få betydelse, dels för reglerna om husrannsakan och beslag och dels för säkring av digitala bevis[183] i allmänhet. I konventionens Art. 16 och 17 föreskrivs det att åtgärder skall vidtas för att myndigheter, skyndsamt, skall kunna säkra fakta eller information som lämpar sig för behandling i ett datorsystem. Närmare innebär detta att myndigheter genom ett föreläggande skall kunna ålägga en enskild att bevara digitala uppgifter orubbade under högst 90 dagar även om ett föreläggande om att bevara vissa uppgifter får förnyas. Systemet med sådana förelägganden är främst avsett att användas då det kan befaras att uppgifterna skall försvinna eller förändras. Föreläggandet skall även innefatta ett åläggande för enskild som förelagts bevara viss uppgift att även hålla hemligt om att sådan åtgärd vidtagits.

Enligt konventionens Art. 18 skall det tillses att de behöriga nationella myndigheterna kan förelägga personer inom det nationella territoriet att lämna ut vissa särskilt angivna uppgifter, som vederbörande har i sin besittning eller under sin kontroll. Myndigheterna skall även ges möjlighet att förelägga en tjänsteleverantör, som bedriver verksamhet inom det nationella området, att lämna ut abonnentuppgifter som leverantören har i sin besittning eller under sin kontroll.

Art. 19 tar sikte på säkring av digitala uppgifter genom husrannsakan och beslag. Här föreskrivs det att varje att myndigheterna genom husrannsakan eller liknande åtgärd skall kunna bereda sig åtkomst till ett datorsystem eller en del av sådant system och de uppgifter som lagras däri. Åtkomst skall även kunna beredas till ett medium för lagring av uppgifter. Myndigheterna skall även ha möjlighet att beslagta, eller på annat sätt säkra, digitala uppgifter som man åtkommit genom en husrannsakan. Säkringen av de digitala uppgifterna innefattar inte enbart att myndigheterna skall kunna

[182] Convention on Cybercrime (CETS no:185).
[183] I konventionstexten används termen datorbehandlingsbara uppgifter som samlingsbegrepp för de uppgifter som avses i de olika bestämmelserna. För att anknyta till detta arbetet har jag valt att hålla mig till begrepp som digitala uppgifter.

framställa och behålla kopior av de åtkomna uppgifterna, utan de skall även ges möjlighet till att avlägsna sådana uppgifter från ett datorsystem eller göra dessa oåtkomliga.
Sistnämnda innefattar således att det skall finnas möjlighet till förverkande av åtkomna digitala uppgifter.

Artikel 20 behandlar insamling av digitala uppgifter i realtid. Här föreskrivs att behörig myndighet skall bemyndigas att med tekniska hjälpmedel kunna insamla eller ta upp trafikuppgifter i realtid som överförs med hjälp av ett datorsystem. Häri ligger att myndigheten även skall kunna ålägga tjänsteleverantörer att antingen insamla sådana uppgifter eller att samarbeta och bistå myndigheterna med insamling eller upptagning.

Med anledning av Sveriges eventuella tillträde till konventionen har justitiedepartementet i en promemoria[184] utrett frågan hur de svenska lagreglerna förhåller sig till konventionens bestämmelser. Utredningen påpekar att Sverige tillhör de länder som tidigt införde en reglering på det IT-rättsliga området och att kriminaliseringen av data- och datarelaterade brott ligger på en hög nivå. De straffrättsliga bestämmelserna som tas upp i konventionen omfattas redan i svensk rätt varför en anpassning till konventionen är genomförbart utan större ändringar på straffrättens område. Utredningen ansåg dock att konventionens krav på processrättsliga regler gällande utredning och lagföring av IT-relaterade brott skulle komma att medföra mer omfattande ändringar inom det processrättsliga området. Även om det tidigare gjorts utredningar kring reglerna om tvångsmedel och dess anpassning till ny teknik har några ändringar på området inte företagits med undantag för regleringen av hemliga tvångsmedel. Ett tillträde till konventionen skulle därför medföra en översyn kring reglerna om bevissäkring genom tvångsmedel.[185] Behovet av anpassning ansågs främst grunda sig i att beslagsinstitutet utgår från fysiska föremål varför det inte är tillämpligt på immateriella objekt.[186] För att kunna beslagta digital information torde det alltså förutsättas att informationen antingen har omvandlats till en utskrift eller att den har lagrats på något fysiskt medium, exempelvis en datorhårddisk. Vidare diskuterades huruvida själva omvandlandet av informationen skall ses som ett led i husrannsakans syfte att göra informationen tillgänglig eller om omvandlingen skall utgöra ett led i beslagsförfarandet. Här ansågs det förra alternativet vara lämpligast eftersom kravet för husrannsakan är högre ställt än vid beslag vilket skulle ge ett högre skydd för den enskilde och vara mer fördelaktigt ur rättsäkerhetssynpunkt. En sådan tillämpning skulle även stämma bäst överens med det grundläggande kravet om att beslagsföremålet skall vara tillgängligt.[187]

[184] Ds 2005:6.
[185] Ibid. s. 91.
[186] Ibid. s. 126 f.
[187] Ibid. s. 283.

7.2.1 Frysning av elektronisk kommunikation

För att de svenska processrättsliga reglerna ska överensstämma med de krav som uppställs i Europarådets konvention om IT-relaterad brottslighet presenterades ett förslag om nytt tvångsmedel i Ds 2005:6. Det nya tvångsmedlet benämndes frysning av elektronisk kommunikation och syftade till att förhindra att trafikuppgifter och andra uppgifter för elektronisk kommunikation går förlorade innan en domstol har hunnit fatta beslut om hemliga tvångsmedel. Själva frysningen av uppgifterna skulle innebära att en operatör, efter särskilt beslut, skall bevara vissa uppgifter om elektronisk kommunikation i väntan på ett beslut från rätten om hemlig teleavlyssning eller hemlig teleövervakning. Uppgifterna får lämnas ut först när ett domstolsbeslut om tvångsmedel har tagits.[188]

Behovet av ett tvångsmedel som frysning av elektronisk kommunikation, ansågs, enligt utredningen, ligga i de åtaganden som uppställs i Europarådets konvention på att myndigheter, i realtid, skall kunna samla in trafikuppgifter från särskilt angiven elektronisk kommunikation samt möjliggöra en snabb säkring och röjning för behöriga myndigheter av sådana uppgifter.[189] Trafikuppgifter som finns hos en operatör omfattas normalt av sekretess. Dessutom krävs det, enligt 6 kap. 5 § LEK, att trafikuppgifter som lagras eller behandlas på annat sätt hos en operatör utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande. Utredningen såg det därför nödvändigt att de brottsbekämpande myndigheterna genom ett snabbt ingripande skall kunna förhindra sådana trafikuppgifter från att försvinna innan myndigheter hunnit ta del av dem. Åtgärder enligt förslaget skulle tillgodose kraven på att snabbt kunna säkra uppgifter som uppställs i Europarådets konvention och samtidigt kunna uppväga kravet på integritetsskydd som uppställs i dir 2002/58/EG. Samtidigt menade man att det föreslagna tvångsmedlet skulle ligga inom utrymmet för inskränkningar om bl.a. trafikuppgifter och sekretess som föreskrivs i Art. 15.1 i EU-direktivet.

7.2.2 Förbud mot att rubba bevisning i elektronisk form

I samband med den utredning som genomfördes med anledning av Sveriges eventuella tillträde till Europarådets konvention om IT-relaterad brottslighet framställdes ett förslag om införandet av en ny bestämmelse i 27 kap. RB, som skulle förbjuda den som innehar bevis i elektronisk form att förstöra, förändra eller på något annat sätt göra bevisningen oåtkomlig.[190] Bestämmelsen skulle inte utgöra ett tvångsmedel utan vara utformat som ett föreläggande i syfte att snabbt kunna säkra digitala uppgifter i fall då det kan befaras att bevisen undanröjs, innan de brottsutredande myndigheterna hunnit vidta tvångsåtgärder för att säkra bevisen. Behovet av ett

[188] Ds 2005:6 s. 249 f.
[189] Se Artiklarna 16, 17, 20, 21 Europarådets konvention samt Ds 2005:6 s. 250.
[190] Ds 2005:6 s. 265 f.

föreläggande likt det föreslagna ansågs främst grunda sig i avsaknaden av regler som ger enskilda skyldigheten att bidra med bevis. Givetvis kan rätten inhämta bevis genom ett föreläggande om edition men ett sådant föreläggande kan först framställas när det finns någon som är skäligen misstänkt.[191] Föreläggandet om förbud att rubba bevisning får inte riktas mot den som är misstänkt. Förbudet skall avse ett bevarande av bevisningen under högst 90 dagar och åklagaren skall ges möjlighet att förbjuda den som har fått ett sådant föreläggande att yppa sig angående föreläggandet.[192]

7.2.3 Kvarhållande av elektronisk post

Eftersom elektronisk post utgör telemeddelanden är åtgärder som rör meddelandena förbehållna reglerna om hemlig teleövervakning och hemlig teleavlyssning. Detta medför att de brottsutredande myndigheternas möjlighet att få till postkontroll är begränsade då merparten av dagens kommunikation sker via elektronisk post istället för traditionell post. Rådande lagstiftning utgör således ett betydligt starkare skydd för elektronisk post än vad som kan anses motiverat med hänsyn till meddelandets karaktär.[193] För att anpassa reglerna om postkontroll till dagens teknik har det föreslagits att det införs en bestämmelse som gör det möjligt att hålla kvar elektronisk post. Bestämmelsen om kvarhållande av elektronisk post skulle utformas efter bestämmelsen om traditionell postkontroll. Eftersom elektronisk post kan förmedlas såväl som en webbaserad tjänst som en inkluderad tjänst i ett Internetabonnemang blir bestämmelsens tillämpningsområde en viktig fråga. I praktiken skulle åtgärden genomföras på så sätt att en kopia av ett meddelande som kommer in till en adress hålls kvar tills det att det fattas ett beslut om att meddelandet skall tas i beslag.[194] Förslaget förutsätter således att beslagsinstitutet kan tillämpas på såväl immateriella objekt som på kopior. En annan fråga är hur tillämpningen av tvångsmedlet skall avgränsas mot reglerna om hemlig teleövervakning och hemlig teleavlyssning. Som tidigare nämnts utgör elektronisk post ett telemeddelande varför det kan tänkas att tillämpningsområdet för kvarhållande av elektronisk post skulle komma att överlappa områdena för hemlig teleövervakning och teleavlyssning. Utredningen hävdade dock att detta inte skulle vara fallet eftersom ändamålen med åtgärderna skiljer sig åt.[195]

7.3 Internet

Med Internet har såväl enskilda som myndigheter fått en källa, av mycket stora mått, för insamling av information. Eftersom Internet är allmänt tillgängligt finns det inga hinder för brottsutredande myndigheter att söka

[191] Se NJA 2003 s. 107.
[192] Ds 2005:6 s. 265 f.
[193] Ibid. s. 285.
[194] Ds 2005:6 s. 289.
[195] Ibid. s. 290.

information som finns tillgänglig på Internet. Med detta i åtanke kan man kanske tänka sig att ett inhämtande av information från Internet skulle vara en mycket enklare uppgift för de brottsutredande myndigheterna än exempelvis deras arbete att inhämta information från en beslagtagen dator. Mycket på grund av Internets uppbyggnad kan det dock på många sätt vara mer problematiskt att inhämta information från Internet. För det första rör det sig nästan alltid om enorma mängder information vilket gör det svårare att sålla ut och hitta viss eftersökt information. Dessutom medför anonymiteten på Internet att det kan finnas tekniska svårigheter med att inhämta informationen. Som ett sista hinder ligger det otydliga regelverk som reglerar Internet och som i mycket beror på Internets gränsöverskridande karaktär.[196]

Kronqvist delar in bevis som inhämtas från Internet i två olika huvudtyper. Dels kan det röra sig om *identifieringsbevisning*, som utgörs av uppgifter om identiteten hos en för brott utnyttjad dator eller identiteten för en brottsmisstänkt person.[197] Det handlar alltså främst om uppgifter som framkommer efter polisiärt spårningsarbete. Identifiering av en dator sker genom datorns såkallade IP-adress. IP-adresserna utgör grunden till all kommunikation som utförs på Internet. Kort utgörs en IP-adress av ett tolv siffror långt nummer som är indelat i fyra olika segment med tre siffror i varje segment. För att underlätta användningen av Internet har IP-adresserna i vissa fall översatts till text i form av adresser websidor och e-post. Antingen kan man tilldelas en fast IP-adress, vilket oftast sker om man är ansluten till Internet via en fast uppkoppling (bredband), eller så tilldelas IP-adresser dynamiskt, vilket är fallet då man kopplar upp sig till Internet via modem. Den fasta IP-adressen innebär att meddelanden som skickas från denna adress så gott som alltid har samma nummerserie medan de med dynamiska IP-nummer tilldelas ett nytt serienummer för varje gång man kopplar sig mot Internet. Dynamiska IP-nummer kan efter en uppkoppling återanvändas vid ett senare tillfälle. För att kunna identifiera en dator med hjälp av ett dynamiskt IP-nummer krävs alltså inte endast själva nummerserien utan även en tidsstämpel som visar på en aktivitet från en viss IP-adress vid en viss tidpunkt. Kammarrätten i Stockholm har nyligen beslutat[198] att en IP-adress är en personuppgift, varför inhämtandet av sådan uppgift omfattas av personuppgiftslagen. Målet har överklagats till Regeringsrätten.

Den andra typen av bevisning benämns *informationsbevisning.* Till denna kategori hör dels information som i sig utgör brott. Det kan t.ex. röra sig om bilder med barnpornografiskt innehåll eller meddelanden som utgör hets mot folkgrupp. Dessutom innefattas härunder sådan information av olika slag som kan styrka en brottsmisstanke.[199]

[196] Kronqvist s. 52.
[197] Ibid.
[198] Kammarrätten i Stockholm 2007-06-08, Mål nr: 285-07.
[199] Kronqvist s. 52.

8 Analys

De slutsatser och analyser som presenteras i detta avsnitt kommer inledningsvis att härledas från de allmänna principer och det rättighetsskydd som reglerar användningen av straffprocessuella tvångsmedel. Avslutningsvis förs diskussionen kring en eventuell utvidgning av tvångsmedelsanvändningen och då främst med anledning av teknikens utveckling i framtiden.

8.1 Är reglerna om husrannsakan och beslag väl anpassade till dagens teknik?

Att tvångsmedel endast får vidtas med stöd i lag och för de, i lagen angivna, ändamålen är en grundläggande föresats. Eftersom det inte finns någon närmare reglering över tillvägagångssättet vid en husrannsakan blir en diskussion utifrån legalitets- och ändamålsprincipen därför inte särskilt givande. Detta gäller särskilt åtgärder som vidtas i digitala miljöer då dessa i mycket skiljer sig från åtgärder som vidtas i traditionella miljöer. Som visats ovan kan dessa åtgärder innehålla fler moment än ett eftersökande och omhändertagande av föremål. Den breda tillämpning som husrannsakan fått genom stadgandet att åtgärden får vidtas i syfte att utröna omständighet som kan vara av betydelse för utredningen har, med hjälp av teknikens utveckling, i än mån gjorts ännu bredare. Åtgärder som leder till att datorer och annan tänkbar digital utrustning undersöks har inget uttryckligt lagstöd. Undersökningarna ses inte vara annorlunda än andra undersökningar av helt vardagliga föremål. Att det inte finns något ytterligare skydd för undersökningar av exempelvis datorer, likt det skydd som omfattar slutna förvaringsställen, menar jag kan medföra vissa betänkligheter vad gäller rättssäkerheten. Som framgått av detta arbete utgörs den etablerade praxis på området av väl utformade rutiner för åtgärder i form av husrannsakan och beslag i syfte att komma åt och säkra digitala bevis. Troligtvis finns det inte heller anledning att betvivla den specialkompetens och tillgång till särskild utrustning som finns inom exempelvis polisen när det handlar om arbete inom området för IT. Oavsett denna praxis finns det inga bakomliggande regler eller bestämmelser som kan utgöra en kontrollfunktion för att åtgärderna vidtas i enlighet med de etablerade riktlinjerna.

Ser man till ändamålsprincipen skapar inte heller denna några egentliga förutsättningar för att upprätthålla någon slags rättssäkerhet. Både husrannsakan och beslag får användas i syfte att utröna omständigheter som kan vara av betydelse för utredningen. Redan här har man ett otroligt brett tillämpningsområde som knappast behöver följas av någon vidare motivering från den som verkställer åtgärden. Om gränserna för en husrannsakan inte tydligt framgår av beslutet skulle det kunna leda till en ökad risk för att husrannsakan vidtas i syfte upptäcka brott. Lika lite som en husrannsakan får användas i syfte att upptäcka brott, får den vidtas för att få

vetskap om den som misstänks för ett brott kan klandras för brottslighet i större utsträckning än vad som kan förutses med anledning av de på förhand givna omständigheterna. Med tanke på de olika digitala spår, som efterlämnas vid användandet av digital utrustning, torde en husrannsakan i digital miljö troligtvis kunna utröna omständigheter i de flesta utredningar. Här ligger begränsningen närmast i den brottsmisstanken som krävs för att få vidta åtgärderna. Detta krav är dock förhållandevis lågt ställt. Eftersom det inte heller krävs någon närmare precisering i beslutet om husrannsakan över den bevisning som skall eftersökas är befogenheterna att vidta undersökningar av datorer och liknande utrustning i det närmaste obegränsade. Ser man det något bakvänt skulle alltså den omständigheten att det finns en dator eller annan digital utrustning i ett utrymme kunna vara tillräckligt för att motivera en husrannsakan av utrymmet och beslag av utrustningen. Den enda möjligheten att garantera att den verkställande myndigheten inte otillbörligt bereder sig tillträde till datorer m.m. skulle vara om man uppställer sådana begränsningar i beslutet om husrannsakan.

Däremot får behovs- och proportionalitetsprincipen betydande roller när det rör sig om åtgärder i digitala miljöer. Både för husrannsakan och beslag anger lagtexten att åtgärder endast får vidtas om skälen som talar för åtgärden uppväger det intrång eller men som åtgärden innebär. Beslag av datorer kan, som tidigare nämnts, medföra stora skador för den som berörs av beslaget. Detta får särskilt anses vara fallet om datorn ingår i en verksamhet eller rörelse. Att även tredje man kan komma att skadas i dessa fall borde också tala för att skälen för åtgärden måste vara särskilt starka. I dessa fall härrör skadan från ett intrång i den materiella integriteten som uppstår när någon berövas besittningen över ett föremål. På grund av intrånget kan rena och mätbara förmögenhetsskador uppstå. Visserligen medför ju åtgärden även ett ingrepp i den rumsliga integriteten i samband med att den som verkställer åtgärder bereder sig tillgång till utrymmet där den eftersökta egendomen befinner sig. Detta får dock anses vara en förutsättning för att beslaget överhuvudtaget skall kunna genomföras. Sammantaget borde åtgärderna dock medföra skador som kan förutsättas och något sånär beräknas innan det man utför ingreppet. I dessa fall borde proportionalitetsbedömningen således stämma väl överens med det verkliga resultatet. Huruvida det föreligger ett behov för och även huruvida det kan anses motiverat att ta egendom i beslag får givetvis avgöras utifrån varje enskilt fall. Skulle det anses att ett omhändertagande av digital utrustning skulle medföra alltför stor skada finns det som sagt andra tänkbara åtgärder för att säkra den information som finns lagrad på utrustningen, utan att man behöver rubba någons besittning över föremålet. Genom att vidta någon av dessa alternativa åtgärder har man åtminstone lyckats förhindra de mest uppenbara och förutsägbara skadorna som kan följa av åtgärderna.

Elektronisk utrustning som innehåller digital teknik, exempelvis digitala minnen, erbjuder enorma lagringsmöjligheter. Genom EKMR och grundlagen har enskilda tillförsäkrats en rätt till privatliv vilket bl.a. innefattar ett skydd för den privata sfären och för korrespondens. Med tanke de uppgifter som kan finnas lagrad i en dator är det inte helt orimligt att

denna information även har ett visst skyddsvärde. Ser man endast till information som är hänförlig till meddelanden om elektronisk kommunikation får dessa anses ha ett tämligen högt skyddsvärde. Beroende på om det är uppgifter som är hänförliga till meddelandet eller om det är innehållet i meddelandet i sig som är av intresse för de brottsutredande myndigheterna krävs det att det för det misstänkta brottet är föreskrivet antingen fängelse i minst 6 månader eller i minst 2 år. Eftersom dessa uppgifter lagras i den digitala utrustningen kan de dock säkras genom en husrannsakan där man antingen tar utrustningen i beslag eller undersöker den på platsen för husrannsakan. Ett problem med åtgärder i digitala miljöer är att den önskvärda informationen inte är direkt synlig då den finns lagrad på t.ex. en hårddisk eller externminne. Det får därför anses vara näst intill omöjligt att på förhand kunna förutse omfattningen av åtgärden och på något sätt kunna bedöma det men eller skada som kan följa av åtgärden. Givetvis skulle man även kunna vända på resonemanget. Med anledning av värdet av den bevisning som kan väntas uppnås kan man tänka sig att skälen för åtgärden som oftast skulle överväga det intrång som åtgärden innebär. För att resonemanget skall hålla borde det dock förutsätta att det finns omständigheter som talar för att man skall uppnå önskvärda skälen. En oklar bild över dessa skäl torde aldrig kunna överväga en oklar bild över de men och den skada som åtgärden kan medföra.

Bristen på en anpassad lagstiftning ställer höga krav på att de beslutsfattande och verkställande myndigheterna vidtar åtgärder i linje med de reglerande principerna på området. De utredningar som presenterats på området har kommit fram till att den befintliga lagstiftningen inte ger ett fullgott skydd när det handlar om digital information. En lösning till problemen har sökts genom förslag till ändringar i vissa lagrum, främst i 27 och 28 kap. RB. Exempelvis har de flesta utredningar ansett att reglerna om förbud mot beslag av vissa handlingar inte ger det skydd som reglerna var avsedda att utge. Att man kan framställa kopior av sådana handlingar och på så sätt undkomma reglerna om beslagsförbud är dock inget som endast är förbehållet den digitala tekniken varför lösningen på problemet troligtvis ses bäst i ett annat sammanhang.

De karaktäristiska dragen hos den digitala informationen kan alltså enligt min mening skapa särskilda betänkligheter när det kommer till avvägningen mellan effektivitet och integritet. Särskilt borde detta gälla vad man kan kalla den personliga integriteten i ideell mening. En allt större användning av datorer av enskilda har lett till att den privata sfären har utvidgats och kommit att koncentrerats till digitala miljöer. Detta gäller inte enbart den skyddsvärda information som enskilda skapar på egen hand, t.ex. i form av elektronisk post eller digitala handlingar, utan även den stora mängd uppgifter och spår som skapas per automatik vid användandet av den digitala utrustningen. Tillgången till dessa uppgifter innebär att man i stort sett kan kartlägga större delen av enskildas privatliv. Dessa särskilda betänkligheter kan knappast framhävas genom utformningen av lagregler utan får istället tillgodoses vid den bedömning som sker utifrån de allmänna principerna i varje enskilt fall. För att tillse att bedömningen sker utifrån de

allmänna reglerande principerna måste således den digitala informationen komma i centrum. Det integritetsintrång som följer av en tvångsåtgärd är givetvis exceptionellt för varje enskild situation. I vissa fall kan en tvångsåtgärd dock ges en särskild verkan genom att man föreskriver att vissa förutsättningar skall gälla. Som exempel kan nämnas att ett frihetsberövande i häkte kan förenas med föreskrift om att åklagaren får ålägga den häktade med restriktioner av olika slag. På samma sett kan en husrannsakan skapa olika effekter beroende på omfattningen av eftersökningen.

Som påvisats ovan saknas det ett särskilt skydd för undersökningar av digital utrustning. Att särskilda föreskrifter skulle gälla för undersökning av sådan utrustning skulle kunna medföra att de oförutsägbara skador och men, som kan följa av åtgärden, beaktas i högre mån vid beslutsfattandet och verkställigheten av åtgärden. Det enklaste sättet att lösa detta vore förmodligen att införa ett skydd för undersökning av datorer och liknande utrustning motsvarande det skydd som finns för slutna förvaringsutrymmen. Detta skulle leda till att man får ett beslutsfattande och verkställande för åtgärder i digitala miljöer där man i bedömningarna, utifrån de övergripande principerna och rättighetsakterna, tar större hänsyn till den särskilda naturen hos den digitala informationen. Ett föremål betraktas som ett slutet förvaringsställe främst med anledning av att en undersökning av föremålet anses vara av särskilt ingripande natur. Detta kan styrkas av den debatt som förts över huruvida föremålet måste vara låst eller inte för att betraktas som ett sådant föremål. Ser man till syftet med bestämmelsen torde även andra föremål, som inte nödvändigtvis måste vara låsta, kunna betraktas som slutna förvaringsställen. Med anledning av möjligheterna till kommunikation, lagring av information och de digitala spår som datorer skapar torde det även stå klart att undersökningar av dessa är av en mer ingripande natur än vad gäller undersökningar av övriga vardagliga föremål. Att närmare bestämma vilka föremål som, sett till deras tekniska natur, kan betraktas som slutna förvaringsställen skulle dock kunna bli en utmaning. Teknikens framfart och den utveckling som leder till att allt fler elektroniska föremål innehåller digital teknik borde tala för en bred tillämpning. Tänkvärt vore kanske till och med att samtliga föremål som kan lagra digital information skulle ges ett motsvarande skydd likt det som gäller för slutna förvaringsutrymmen.

8.2 Ställer tekniken krav på andra åtgärder i nya former?

Behovs- och proportionalitetsprincipen ger även upphov till frågan om man kan uppnå samma resultat som vid tvångsåtgärder i form av husrannsakan och beslag med hjälp av andra mindre kännbara åtgärder. Genom det EU-direktiv som skall tillförsäkra att uppgifter om kommunikation lagras av operatörer skapas förutsättningar för att de brottsutredande myndigheterna kommer att ha större tillgång till sådana uppgifter. Är det främst uppgifter

om telemeddelanden som är ändamålet med åtgärderna torde de brottsutredande myndigheterna således alltid söka uppgifterna hos befordningsföretaget i första hand. Önskvärt vore kanske till och med att lagstiftningen om tillgång till uppgifter om elektronisk kommunikation även borde ses som *lex specialis* i förhållande till reglerna om husrannsakan och beslag. Eftersom uppgifter om telemeddelanden ofta har till syfte att utröna omständigheter som är av betydelse för utredningen av brott har man även fått en naturlig avgränsning av det breda tillämpningsområdet för husrannsakan och beslag. Dessutom innebär det att man fått ett reglerat område inom polisens arbete för att samla in bevis och information.

Behovet av att snabbt kunna säkra uppgifter om elektronisk kommunikation, utan att behöva vidta åtgärder i form av tvångsmedel, framgår även av de lagförslag som presenterades med anledning av Europarådets konvention om IT-relaterad brottslighet. Dessa åtgärder får samtliga anses vara tämligen begränsade när det kommer till omfattningen av det integritetsintrång som kan följa av åtgärderna. Samtidigt borde effekten av dessa åtgärder kunna bedömas med viss säkerhet varför jag kan ge medhåll till ett införande av motsvarande åtgärder. Däremot borde behovet av åtgärder av dessa slag komma att få en minskad betydelse med anledning av införlivandet av EU.s direktiv om lagring av uppgifter. Den oro som föranlett förslagen och som skapats över att brottsutredande myndigheter inte i tid skall kunna säkra digitala uppgifter borde i mycket kunna utraderas om det införs en skyldighet för befordringsföretag att lagra uppgifterna under viss tid. Förslaget om en postkontroll, omfattande elektronisk post, kan visserligen anses behövligt men i förslagets utformning kan gränsdragningen mot övriga tvångsmedel vara svår att urskilja. Dessutom föresätter förslaget att beslagsinstitutet kan tillämpas på immateriella objekt vilket förmodligen skulle kräva en hel del omarbetning av reglerna i 27 kap. RB.

Istället för att förespråka ändringar i den nuvarande lagstiftningen om husrannsakan och beslag, har den senaste tidens debatt främst handlat om att införa nya metoder och tillvägagångssätt för att säkra digital bevisning. Förslagen rör såväl införandet av nya tvångsmedel som andra icke tvångsbetonade metoder för att inhämta digital bevisning. Denna debatt har grundar sig främst i det utmålade hotet från en ökad IT-relaterad brottslighet, främst inom den organiserade och gränsöverskridande kriminaliteten. Det är föga tänkbart att den tekniska utvecklingen skall avstanna i framtiden. Troligare är istället en högre datortäthet och en större användarkunskap, även inom kriminella kretsar. Ser man till framtiden skall man dock erinra sig om att den teknik som redan finns tillgänglig idag ännu inte utnyttjas fullt ut. Lagringskapaciteten ökar ständigt liksom möjligheterna för kommunikation genom utbredningen av trådlösa nätverk. Samtidigt integreras olika tillämpningar av teknik genom standardiserade överförings- och lagringsmöjligheter. Internet utgör redan idag en enorm källa för spridning av information. Med tillgång till Internet kan man exempelvis, utan några större krav på datorkunskap, kryptera innehållet i ett meddelande eller upprätta en tillfällig e-post adress som upphör att existera efter endast en kort stund, i syfte att motverka obehöriga att få kännedom

om eller spåra den information som man skapat. För att kunna bedöma behovet av tvångsåtgärder i sådana miljöer skall det dock inte enbart ses till själva tekniken. Vad som är av störst intresse är istället den användning och tillämpning av tekniken som sker i vardagen.

Det mest omfattande förslaget för en utvidgad tvångsmedelsanvändning utgörs av införandet av tvångsmedlet hemlig dataavläsning. Med ett tvångsmedel som hemlig dataavläsning kan även andra hemliga tvångsmedel aktualiseras. Detta gör det självklart svårare att förutse omfattningen av det intrång som enskild kan komma att drabbas av vid användandet av tvångsmedlet. Önskvärt vore om man på förhand kunde se omfattningen av intrånget av åtgärden. En enkel lösning på detta torde vara att hålla isär vissa grundläggande begrepp avseende kommunikation och inte fokusera på vad för teknisk kommunikationstjänst som används. Om två eller flera personer utbyter ett kommunicerat röstsamtal torde det spela mindre roll vilken slags kommunikationstjänst som de använder sig av för att avgöra hur samtalet skall avlyssnas eller hur man skall kunna lokalisera den geografiska plats som samtalet överförs från. Att använda ett tvångsmedel som syftar till att avlyssna ett röstsamtal mellan flera personer borde alltid kräva ett föreliggande beslut om hemlig teleavlyssning. Att tränga sig in någons bostad eller arbetsplats borde alltid kräva ett beslut om husrannsakan.

Förslaget till hemlig dataavläsning medför ett väldigt stort intrång i den privata sfären eftersom det är möjligt att komma åt samtlig information som finns i en dator och dessutom få reda på vilka aktiviteter som utförs av användaren. Detta gäller oavsett om det rör sig om lagrad information eller sådan som behandlas i realtid. På så sätt liknar sig förslaget mycket vid någon slags buggning där man på ett enkelt sätt kan kartlägga en individs privatliv. Att utredningen inte beaktat de integritetsintrång som kan följa utav ett beslut om hemlig dataavläsning framgår tydligt när man ser till förslagets tillämpningsområde. Endast när det handlar om särskilt allvarlig brottslighet kan det tänkas att en åtgärd av sådant slag skulle kunna överväga den skada som ingripandet medför. När tvångsmedlet infördes i Danmark gjorde man detta tydligt genom att man i lagstiftningen uppräknade de brott för vilken åtgärden får vidtas. Detta borde vara en förutsättning för att man överhuvudtaget skall kunna behålla någon slags rättssäkerhet. Enligt min mening gavs det svenska förslaget en alldeles för vid tillämpning. En begränsning till att tvångsmedlet endast skulle få användas i ett visst antal uppräknade fall, likt man gjort i dansk lag, borde ge tydligare signaler för att den befarade skadan som kan uppstå vid verkställigheten av tvångsmedel varit nödvändig med hänsyn till det förväntade resultatet.

Hemlig dataavläsning skulle inte bara underlätta för polisen, i dess brottsutredande arbete, på så sätt att man skulle kunna verkställa flera tvångsmedel med endast ett beslut utan även genom att polisen kan säkra informationen från distans utan att den eller de personer som utsätts för tvångsmedlet är medvetna om detta. Det kräver inga stora personalinsatser

för att genomföra ett tillslag mot en misstänkts bostad för att åtkomma datorer eller för att bedriva omfattande eftersökningar i allmänna serverutrymmen. Som JO har påpekat får tvångsmedel dock inte användas endast i syfte att underlätta för brottsutredningar. Även om ett tvångsmedel som hemlig dataavläsning kräver ett tämligen högt föreskrivet fängelsestraff för det brott som ska utredas befarar jag att det skulle komma att användas även i fall där mindre ingripande åtgärder hade kunnat ge samma resultat just av den anledning att det är en relativt enkel åtgärd att utföra. Hemlig dataavläsning är ju till sitt ändamål kanske trots allt mer lämpat för åtgärder i digitala miljöer än vad en husrannsakan är.

Litteraturförteckning

Litteratur

Angerfeldt, Bengt – Husrannsakan & Beslag i IT-miljö; en lathund, utbildningskompendium, 2003.

Danelius, Hans – Mänskliga Rättigheter i europeisk praxis; En kommentar till Europakonventionen om de mänskliga rättigheterna, Stockholm: Norsteds Juridik, 2007, tredje upplagan.

Ekelöf, Per Olof, Bylund, Torleif, Boman, Robert – Rättegång III, Stockholm: Norsteds Juridik, 1994, sjätte upplagan.

Ekelöf, Per Olof – Ett problem med hemlig avlyssning, SvJT 1982 s. 654-663.

Fitger, Peter, Eklycke, Lars,Eksborg, Ann-Louise, Gullnäs, Ingvar – Rättegångsbalken I; En kommentar, 2:a häftet, Norsteds Juridik.

Flyghed, Janne – Brottsbekämpning mellan effektivitet och Integritet, Lund: Studentlitteratur, 2000.

Kronkvist, Stefan – Brott och digitala bevis; En handledning, Stockholm: Norsteds Juridik, 2003.

Lindberg, Gunnel – Straffprocessuella tvångsmedel; När och hur får de användas, Stockholm: Thomson Fakta, 2005.

Strömholm, Stig – Integritetsskyddet, ett försök till internationell lägesbestämning, SvJT 1971 s. 695-736.

Willassen, Svein – Slettede data som bevis, Lov & Data nr 78, juni 2004.

Offentligt tryck

BRÅ-Rapport 2000:2 – IT-relaterad brottslighet

Datainspektionens yttrande 2005-12-02, Dnr. 1391-2005

Ds 2003:29 – Formel formkrav och elektronisk kommunikation

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

Europeiska Kommissionens rambeslut (EGT C 203 E, 27-08-2002)

JK 1981 s. 38.
JK – beslut 2001-01-22, Dnr. 3954-99-40
JK – beslut 2005-12-08, Dnr. 4667-05-80

JO 1956 s. 95
JO 1963 s. 103
JO 1974 s. 87
JO 1974 s. 128
JO 1975/76 s. 154
JO 1997/98 s. 47
JO 1978/79 s. 280
JO 1988/89 s. 53
JO 1991/92 s. 108
JO 1992/93 s. 143
JO 2004/05 s. 70
JO – beslut 2005-12-13, Dnr. 4009-2005
JO – beslut 2007-04-02, Dnr. 2762-2006

NJA II 1933

NJA II 1943

Prop. 1975/76:209 – om ändring i Regeringsformen

Prop. 1987/88:65 – om vissa ändringar i reglerna om tvångsmedel

Prop. 1988/89:124 – om vissa tvångsmedelsfrågor, taxeringsrevision, m.m.

Prop. 1993/94:24 – med förslag till ändrade regler om kroppsvisitation och kroppsbesiktning, m.m.

Prop. 1998/99:11 – Ny skyddsåtgärd vid immaterialrättsintrång

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

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

RÅFS 2002:1 – om dokumentation och underrättelser vid tvångsmedel

SOU 1938:44 – Processlagberedningens förslag till Rättegångsbalk

SOU 1984:54 – Tvångsmedel, anonymitet, 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 1997:39 – Integritet, Offentlighet, Informationsteknik

SOU 1998:46 – Om buggning och andra hemliga tvångsmedel

SOU 2005:38 – Tillgång till elektronisk kommunikation i brottsutredningar, mm.

SOU 2007:22 – Skyddet för den personliga integriteten

Internet

NyTeknik publicerad 2007-03-06 16:19 http://www.nyteknik.se/art/49413 hämtad 2007-05-19

Rättsfallsförteckning

Högsta domstolen

NJA 1977 s. 573

NJA 1988 s. 471

NJA 2003 s. 107

Kammarrätten

Kammarrätten i Stockholm 2007-06-08, Mål nr: 285-07.