Håkan Hallbäck är lärare på Polisutbildningen vid Växjö universitet och undervisar bland annat i immaterialrätt. Han är jurist och har tidigare arbetat som advokat och polis. Håkan undervisar även på polisens vidareutbildning när det gäller underrättelseinhämtning och spaning på Internet.

Växjö universitet
ISSN: 1654-6776

HÅKAN HALLBÄCK

DIGITALA BROTT OCH STRAFFPROCESSUELLA ÅTGÄRDER I DIGITAL MILJÖ

Växjö universitet
Polisutbildningen

VÄXJÖ UNIVERSITY STUDIES IN POLICING
NR 001-2009

HÅKAN HALLBÄCK

Digitala brott och straffprocessuella åtgärder i digital miljö

Digitala brott och straffprocessuella åtgärder i digital miljö.

Håkan Hallbäck

Inledning

I takt med att digitaliseringen sedan 1980-talet förändrat samhället har även kriminella tillgodogjort sig och funnit sig tillrätta med den nya tekniken. Denna skrift är ett försök att i korthet beskriva och klargöra några av de straffrättsliga och straffprocessrättsliga aspekterna av den digitala tekniken.

I första delen av skriften genomgås några vanliga brott som kan begås i anslutning till digital teknik. Efter detta analyseras den digitala tekniken ur straffprocessrättsliga synvinkel. Den processuella genomgången påbörjas med en undersökning av hur det befintliga regelverket fungerar i digital miljö för spaning och annan förutredning (utanför ramarna för förundersökning enligt rättegångsbalken). Därefter granskas den digitala tekniken i förhållande till reglerna om förundersökning och straffprocessen enligt rättegångsbalken.

Inledningsvis kan fastslås att det till stor del saknas lagstiftning för hantering av spaning- och förundersökningsåtgärder i digital miljö samt synes lagstiftaren inte ha hängt med i teknikutvecklingen. Vi har till exempel ett välfungerande regelverk såvitt avser beslag av telegram (27 kap 1 § 2 st m fl rättegångsbalken), men vi har inte något regelverk som talar om när och hur man ska ta omhand informationen som är lagrad på en hårddisk, mobiltelefon, usb-minne eller annat digitalt media. Det är även tunnsått med rättsfall och andra auktoritativa avgöranden. En del förslag till lösning av de frågeställningarna som finns runt hur den digitala tekniken skall behandlas straff- och straffprocessrättsligt blir därmed mer eller mindre kvalificerade gissningar av hur problematiken skall behandlas.

Innehållsförteckning

Digitala brott

> *4 kap 9 c § Brottsbalk (Dataintrång)*
> *Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för* ***dataintrång*** *till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.*

Brottet återfanns ursprungligen i datalagen från 1973. När denna lag ersattes av nuvarande personuppgiftslagen överfördes straffstadgandet till 4:9 c brottsbalken. Senaste lagändringen skedde efter prop 2006/07:66, då stadgandet ändrades i enligthet med EUs rambeslut om angrepp mot informationssystem[1].

Genom brottet dataintrång har man straffbelagt i princip alla olovliga intrång i datoriserad miljö. För straffbarhet räcker det att gärningsmannen berett sig tillgång, d v s öppnat för att kunna ta del av uppgifter som finns i datamediet. Gärningsmannen behöver dock inte ha hämtat ut informationen. Det har i lagtexten inte heller ställts något krav på att uppgiften måste ha omgärdats med särskilt skydd eller att gärningsmannen kringgått en säkerhetsåtgärd, utan det torde räcka att det av omständigheterna framgår att uppgiften inte är avsedd för gärningsmannens ”ögon”. Förenklat innebär detta att uppgifter som envar förvarar i sin egen pc skyddas av stadgandet. Likaledes ger stadgandet skydd för uppgifter som blir åtkomliga endast efter att man angivet lösenord eller kod. Däremot uppgifter som läggs ut på Internet med avsikt att vara publika är det straffritt att ta del av.

För straffbarhet krävs att intrånget eller angreppet sker olovligen, d v s utan samtycke. Det är ett uppsåtligt brott och intrång som sker av misstag eller oaktsamhet är följaktligen inte straffbara. Såsom

[1] Rådets rambeslut 1005/222/RIF (bilaga 1, prop 2006/07:66)

alltid i straffrätten ligger bevisbördan för att angreppet skett olovligen och uppsåtligen på åklagaren. Enkelt uttryckt innebär detta exempelvis att om en misstänkt påstår att han av misstag skickat ett datavirus eller av misstag gjort intrång så har åklagaren bevisbördan för att styrka att det inte skett av misstag, utan det är en uppsåtligt företagen handling.

En intrikat fråga blir om någon i och för sig lägger ut uppgifter via Internet så att de är tillgängliga för envar, men tydligt på sidan anger att det rör sig om ”hemligt” material och att envar inte äger rätt att ta del av uppgifterna. Om någon, oaktat ”förbudet”, ändå tar del av de påstått hemliga uppgifterna så skulle detta objektivt kunna utgöra ett dataintrång. Om gärningsmannen subjektivt vidgår att han uppfattade förbudet att ta del av uppgifterna så medför det i så fall att brottet formellt är fullbordat. I utredningen Elektronisk dokumenthantering framförs att ett förbudsmeddelande med innehåll att polis eller åklagare inte äger ta del av innehållet inte medför att myndigheten gör sig skyldiga till dataintrång eftersom användaren uppenbarligen inte kan förfoga över olovlighetsrekvisitet i dataintrångsbestämmelsen[2]. Av utredningen framgår inte på vilket sätt det är uppenbart att ett dylikt förbud saknar verkan. Sannolikt har utredningen tänkt sig att om någon lägger ut information publikt så saknar den här typen av förbudsmeddelanden verkan; ett förbud av arten att utlagt material inte får tas del av exempelvis vänsterhänta saknar rättsverkan och kan inte konstituera ett brott.

Verkan av förbudsmeddelande på hemsida

Som ovan nämnts ställs i lagrummet inte något krav på uppgiften skall vara ”inlåst”, skyddad genom kod eller liknande, utan för straffbarhet räcker det att gärningsmannen olovligen bereder sig tillgång till uppgiften. En parallell kan dras till det närliggande hemfridsbrottet, 4:6 1 st BrB, där det inte uppställs något krav på att gärningsmannen ska forcera lås eller liknande, utan det blir ett hemfridsbrott redan när gärningsmannen går in genom en olåst ytterdörr till någons bostad. Om gärningsmannen inte förstod att det var en bostad han olovligen inträngde i kan han inte dömas för det uppsåtliga hemfridsbrottet (möjligen föreligger istället ett olaga intrång). De båda brotten hemfridsbrott och varianten med olovligt beredande av tillgång till uppgift i dataintrångsbrottet uppvisar många likheter samt har en liknande systematik.

[2] SOU 1996:40 s 210

Jag håller med SOU 1996:40 om att ett förbigående av ett allmänt hållet förbudsmeddelande av typen ”no pigs and cops” inte får någon rättsverkan i förhållande till dataintrångsbrottet. Om jag däremot stöter på ett förbudsmeddelande som anger att hemsidan tillhör familjen Svensson och endast får besökas av de som tillhör denna familj så är jag definitivt inte säker på att det är lika uppenbart att förbudsmeddelandet skulle sakna rättsverkan. Rimligen måste familjen ifråga få lov att bestämma vilka som ska få tillgång till informationen och ett förbud bör i sådant fall ha samma rättsverkan som en olåst ytterdörr i förhållande till hemfridsbrottet samt medföra att de som bryter mot förbudet kan dömas för dataintrång[3]. Det finns följaktligen en stor gråzon mellan de straffbara fallen av dataintrång och de fall där förbudsmeddelanden eller inträdeskraven är av sådan allmänt hållen art att de saknar rättsverkan.

Falsk identitet

Hur ska man behandla de fall då någon under föregivande att han har annan identitet än den uppgivna och med den falska identiteten lyckas ta sig in i en sluten digital miljö. Om någon ljuger om sin identitet och lyckas ta sig in i på annans sida för transaktioner vid en bank så är det ett klockrent fall av dataintrång. Men hur hanterar man fallet att en polis vid underrättelseinhämtning lyckas ta sig in i ett slutet forum under föregivande av att polismannen är ”GertSonny23somgillarheroin” och polismannen definitivt skulle nekats inträde av forumet om man känt till hans korrekta identitet? Ett dylikt förfarande påminner, ytligt sett, om en hemlig teleavlyssning. Enligt SOU 1996:40 om elektronisk dokumenthantering kan det inte komma ifråga att man inom den öppna polisverksamhet skulle kunna agera med felaktig identitet och, enligt det synsätt som det ges uttryck för i denna utredning, skulle ett sådant polisiärt agerande kunna betraktas som ett dataintrång/tjänstefel[4]. I propositionen som föregick lagstiftningen om kvalificerad skyddsidentitet[5] anlägger man dock ett helt annorlunda synsätt och man godtar i användandet av en felaktig identitet vid spaning/underrättelseinhämtning (se vidare nedan under rubriken kvalificerad skyddsidentitet). Min egen uppfattning är att de synsätt som kom tillkänna i SOU 1996:40 sannolikhet hade bärighet på rättsläget vid denna tidpunkt, men polisarbetet har utvecklats och vi är idag troligen mogna för att i högre utsträckning acceptera användandet av okonventionella metoder, så länge dessa inte kränker den personliga integriteten.

---

[3] J f r Stefan Kronqvist, Brott och Digitala bevis, s 117 – 118, redovisning av fall Intentia ./. Reuters

[4] J f r SOU 1996:40 s 210

[5] Prop 2005/06:149

Dataintrångsbrottet gäller såväl data som är fixerad på hårddisken, som data i arbetsminne eller som är under befordran[6]. Avsikten med lagrummet är att det ska vara teknikneutralt, d v s det skall träffa alla former av automatiserad uppgiftsbehandling oaktat i vilken teknikmiljö den befinner sig.

Stadgandet straffbelägger vidare den som olovligen ändrar, utplånar eller blockerar uppgift avsedd för automatisk behandling eller i register för in en sådan uppgift. Dessa fall tar i första hand sikte på olika former av s k datavirus och liknande, där virusskaparen skickar ut ett virus som på något sätt förändrar databaserad information hos mottagaren.

Lagkonkurrens

I de fall att dataintrånget är ett förled till ett bedrägeri uppstår s k lagkonkurrens, d v s förfarandet träffas av flera olika straffstadganden. En regel vid lagkonkurrens är att man dömer för det allvarligaste brottet. För det fall att ett eller flera brott utgör ett förled till annat brott eller en del av en övergripande brottsplan, döms för det avsedda fullbordade brottet[7]. Vid exempelvis försök till bedrägeri genom dataintrång torde gärningsmannen dömas för bedrägeriförsöket emedan dataintrånget utgjort en del av detta brott och vid straffmätningen får intrånget beaktas som en försvårande omständighet (se vidare nedan under bedrägeriavsnittet). Det finns dock i rättspraxis fall där man dömer för båda brotten[8]. I förundersökning eller förutredning är det dock mindre viktigt hur en domstol i framtiden kommer att bedöma brotten/brottet, utan det väsentliga i detta skede är att utreda och belysa samtliga rekvisit i samtliga tänkbara brott.

I litteraturen runt databrottslighet återfinns resonemang om att skadegörelsebrottet[9] skulle kunna användas för att beivra virusangrepp, och andra digitala angrepp, som digitalt skadar programvara och lagrad information. Min uppfattning är att sådana förfarande träffas av brottet dataintrång och att skadegörelsebrottet är mindre lämpligt. Avsikten med skadegörelsebrottet är att beivra fysiskt skadegörande handlingar. Visserligen avsätter ett datavirus förändringar i elektronstrukturen i en hårddisk, men det väsentliga är att

---

[6] prop 2006/07:66, s 23 (nederst) - 24

[7] Exempelvis NJA 1967 s. 93, RH 1992:81

[8] Exempelvis NJA 1972 s. 643

[9] Bl a Stefan Kronqvist, Brott och digitala bevis, andra upplagan sid 173, prop 2006/07:66, s 18, 26, 28 - 30

den lagrade informationen skadas och information/data är typiska immateriella objekt. Skadegörelsebrottet fungerar därmed väl i förhållande till fysisk skadegörelse mot en dator; klippa av sladden, klottra på skärmen, slå sönder hårddisken och liknande. Däremot torde legalitetsprincipen[10] hindra att man analogt tillämpar skadegörelsebrottet på handlingar som innebär en, i huvudsak immateriell, skada på en samling av information. Dataintrångsbrottet är specialskrivet för just olika angrepp i digital miljö och man behöver följaktligen inte laborera med konstruerade resonemang runt skadegörelsebrottet.

Opinionsyttringar

Det händer att det vid opinionsyttringar, genom att många skickar samma meddelande till befattningshavare, uppstår störningar och hinder för mottagarens dataanvändning. Dylika uppmaningar att skicka mail till utpekad politiker i aktuell fråga återfinns exempelvis ofta i våra stora i kvällstidningarna. Ett fall av dataintrångsbrottet är att gärningsmannen ”olovligen blockerar” datauppgift. Om exempelvis en kvällstidning skulle uppmana sina läsare att mejla en lokalpolitiker i Knäckebrödhults kommun i viss fråga och en halv miljon av läsarna tar uppmaningen på allvar, så förorsakar detta sannolikt en överbelastning och blockering av kommunens server. Objektivt har ansvarig utgivaren för kvällstidningen i sådant fall anstiftat blockeringen och subjektivt måste han haft insikt i att servern skulle bli blockerad om uppmaningen följdes av tidningsläsarna. Enligt förarbetet till dataintrångsbrottet omfattas dylika förfarande inte av straffstadgandet[11]. Det finns dock inte något direkt och uttalat undantag i stadgandet och förarbetena är något grumliga på den här punkten. Man skulle kunna resonera i termer av att dataintrångsbrottet endast straffbelägger olovliga blockeringar, medan åsikts- och opinionsyttringar alltid är tillåtna och lovliga samt att dessa åtnjuter ett grundlagsskydd. Detta är dock en förklaring som inte har uttalat stöd i lagrummet, men väl synes tolkningen stå i överensstämmelse med art 10 i europakonventionen och den praxis som utvecklats till detta lagrum.

Enligt 4 kap 10 § brottsbalken är förberedelse och försök till dataintrång straffbart, utom i fall då det fullbordade dataintrångsbrottet skulle ansetts vara ringa.

---

[10] 1:1 BrB m fl

[11] prop 2006/07:66, s 46

I de fall syftet med en blockering av datatrafiken är att *allvarligt* hindra eller störa rättsskipning eller förvaltning skulle förfarandet även kunna träffas av sabotagestadgandet, 13:4 BrB. Sabotagebrottet tar i första hand sikte på fysisk skador, men genom lokutionen[12] ”annan åtgärd” har man låtit brottet omfatta även andra åtgärder än rent fysiskt skadegörande handlingar. Likaledes bestraffas som sabotage att någon genom skadegörelse eller annan åtgärd *allvarligt* stör eller hindrar användande av telegraf, telefon eller dylikt allmänt hjälpmedel. Förfarandet skall allvarligt hindra eller störa, d v s det krävs att åtgärden får omfattande verkningar och att dessa inte är enbart hastigt övergående. Sabotaget är ett uppsåtligt brott, vilket medför att gärningsmannens uppsåt skall täcka omfattningen av skadan. Om gärningsmannen av misstag eller oaktsamhet orsakar en allvarlig och långvarig störning i teletrafiken så kan förfarandet inte straffas som sabotage. Straffet för sabotage av normalgraden är fängelse i högst fyra år.

Sabotagebrott som begås med *syfte* att injaga fruktan hos en befolkningsgrupp eller för att otillbörligt tvinga offentligt organ att vidta eller avstå från åtgärd kan straffas som terroristbrott enligt lag (2003:148) om straff för terroristbrott. Straffskalan för terroristbrott av normalgraden är fängelse viss tid, lägst fyra år och högst tio år, eller på livstid.

> *9 kap 1 § Brottsbalk (Bedrägeri)*
> *Den som medelst vilseledande förmår någon till handling eller underlåtenhet, som innebär vinning för gärningsmannen och skada för den vilseledde eller någon i vars ställe denne är, dömes för* ***bedrägeri*** *till fängelse i högst två år.*
>
> ***För bedrägeri döms också den som genom att lämna oriktig eller ofullständig uppgift, genom att ändra i program eller upptagning eller på annat sätt olovligen påverkar resultatet av en automatisk informationsbehandling eller någon annan liknande automatisk process, så att det innebär vinning för gärningsmannen och skada för någon annan.***

Bedrägeribrottet är i sin huvudform avsett för bedrägerier från person och riktade mot annan person, men genom stadgandet i 2 st har man även fört in olika manipulationer i datoriserad miljö under bedrägeristadgandet. Förutsättning för straffbarhet är att förfarandet innebär vinning för gärningsmannen och skada för annan.

---

[12] Utryck eller avgränsat begrepp bildat av flera ord

Bedrägeri, som med hänsyn till skadans omfattning och övriga omständigheter, är att anse som ringa bedöms som det ringa brottet bedrägligt beteende, 9:2 BrB. Brottet finns även i en grov variant – grovt bedrägeri, 9:3 BrB. Vid bedömning av om brottet skall anses grovt skall särskilt beaktas om

1. gärningsmannen missbrukat allmänt förtroende,
2. begagnat falsk handling,
3. använt vilseledande bokföring,
4. om gärningen eljest varit av farlig art,
5. avsett betydande värde eller
6. inneburit synnerligen kännbar skada

Om något/några av de angivna momenten finns för handen kan bedrägeriet kvalificeras till ett grovt dylikt. De kvalificerande faktorerna får inte enbart betydelse för bedömning av om brottet skall anses som grovt bedrägeri, utan man kan ta ledning av exemplifieringen även vid avgörande om exempelvis ett, med hänsyn till värdet, ringa brott skall kvalificeras till brott av normalgraden[13]. De exemplifierade omständigheterna kan även få betydelse för bedömning av brott av normalgraden och därvid höja straffvärdet.

I punkt 2 ovan anges som kvalificerande faktor att man vid brottet begagnat falsk handling. Fråga är om uppgifter i digital miljö kan utgöra handling i straffrättslig bemärkelse. Såvitt jag kan avgöra finns inte något prejudicerande avgörande som direkt avgör frågan. En viss ledning kan erhållas från Svea hovrätts dom av den 31 maj 2002 i B5358-01 gällande, bland annat, frågan om urkundsförfalskning för Jesús Alcalá. I målet åtalades Alcalá, bland annat, för urkundsförfalskning innebärande att han i sin dator själv förfärdigat ett utlåtande från professor Suzanne Wennberg.

I sin dom konstaterar hovrätten.

> *Upptagningar för automatisk databehandling (ADB) i faller i många fall under begreppet urkund. Urkundsbegreppet har således genom rättspraxis kommit att följa med den tekniska utveckling som har skett. Det är dock viktigt att man ställer lika höga krav på sådana upptagningar som på pappersdokument för att tillerkänna dem urkundskvalitet. Konsekvensen av detta blir att ett dokument som endast upprättats genom*

[13] Jämförelse kan göras med exempelvis NJA 1995 s. 561, där tillgrepp ur handväska, oaktat det låga värdet, bedömts som stöld av normalgraden.

ett ordbehandlingsprogram närmast blir att jämställa med en avskrift av en urkund. Eftersom avskrifter inte uppfyller kravet på originalkaraktär bör sådana handlingar, oavsett om de skrivs ut eller lagras elektroniskt, inte tillerkännas urkundskvalitet.

I 14 kap 1 § 2 st Brottsbalken ges en exemplifiering av olika urkunder och det gemensamma för dessa är att de är traditionella skriftliga handlingar som fungerar som bevis för visst förhållande. Svea hovrätt har i Alcalá-domen angivit att det finns möjlighet att en digital handling skulle kunna ha urkundskvalitet, bara den håller tillräckligt hög kvalitet gällande tillförlitlighet m m. Man konstaterar därvid att ett vanligt ordbehandlingsprogram inte uppfyller kriterierna för urkund.

Handlingsbegreppet

Det får poängteras att brottet urkundsförfalskning inte har anpassats till digitala handlingar. Lagstiftaren hade enkelt genom ett smärre tillägg kunnat förtydliga lagrummet genom att ange att detta gäller även urkunder skapade genom automatisk informationsbehandling eller liknande lokution, men detta har man inte gjort. Av legalitetsskäl kan det därför bli svårt att generellt påstå att urkundsförfalskningsbrottet även omfattar digitala handlingar. Ett trivialt exempel: två avtalsparter förfärdigar och ömsesidigt accepterar ett avtal i digital miljö. Om avtalet skulle tillkommit på traditionellt sätt i pappersform skulle det tveklöst fått urkundsstatus och tjänat som bevis över avtalsinnehållet, men om det endast finns ett ”lättflyktig” digital upplaga av avtalet så får det ett lägre bevisvärde samt är det svårt att hävda att handlingen utgör en urkund. Ett annat exempel. Bussbiljetter och andra bevismärken har hittills funnits i den varaktiga pappersformen och en kontrollant har genom att känna på papperskvaliteten, skärskåda texten m m kunnat avgöra om det var en riktig biljett eller ej. Bussbiljetten har därmed uppfyllt kriterierna för urkund, men hur ska man hantera manipulation och förfalskning av de biljetter som enbart finns i digital form. Jag har svårt att se att dessa digitala bussbiljetter uppfyller samma krav på varaktighet, tillförlitlighet och kontrollbarhet som gäller för sådana i pappersform.

Enligt lag (2000:832) om kvalificerade elektroniska signaturer finns möjlighet att skapa en elektronisk signatur, som är en särskilt kvalificerad legitimation i digital miljö. De som äger rätt att utfärda elektroniska signaturer skall bland annat enligt 3 § tillse att signaturen är tillfredsställande skyddad mot förfalskning. En elektronisk signatur har sådan kvalitet att den ligger nära det man traditionellt

avsett med begreppet urkund. Möjligen kan en förfalskning av en elektronisk signatur anses som urkundsförfalskning.

Straffstadganden i ny digitalt anpassad lag

Under de senaste åren har delar av allmänhetens ingivande av handlingar m m till myndigheter digitaliserats. Det gemensamma för dessa nya lagar är att man i varje fall infört separata straffbestämmelser gällande ingivande av falska uppgifter. I lag (2004:115) om självbetjäningstjänster via Internet inom socialförsäkringens administration har införts möjlighet att utföra vissa ärenden i förhållande till socialförsäkringssfären och i de fall en dylik uppgift avges på heder och samvete har införts en separat straffbestämmelse[14]. Det är även öppnats möjlighet att ge in handlingar digitalt i inskrivningsärende och på samma sätt har det i en separat straffbestämmelse gjorts straffbart att i digital form lämna oriktiga intyganden om det medför fara i bevishänseende[15]. Likaledes har det för aktiebolag, ekonomiska föreningar m fl företagsformer blivit möjligt att ge in en mängd uppgifter i elektronisk form till Bolagsverket. Ingivande av oriktiga uppgifter medför straffansvar enligt separata straffbestämmelser i respektive lag[16]. Det får noteras att man i propositionen till lagändringarna för ekonomiska föreningar och vissa andra företag (bl a aktiebolag)17 konstateras följande.

> *Rättsläget beträffande förfalsknings- och sanningsbrott som sker genom användning av elektroniska handlingar anses emellertid oklart. Det har i olika sammanhang ifrågasatts bl.a. i vilken utsträckning en elektronisk handling kan ha urkundsstatus eller om uppgifter i en sådan handling kan anses vara lämnade i skriftlig form i den mening som brottsbalken avser. Det går därför inte att säkert säga att en manipulation avseende t.ex. en inskannad handling eller en osann uppgift på heder och samvete som har lämnats elektroniskt omfattas av brottsbalkens regler.*

---

[14] 5 § lag (2004:115) om självbetjäningstjänster via Internet inom socialförsäkringens administration
[15] 19 kap 11 a § Jordabalk
[16] Exempelvis 30 kap 2 § Aktiebolagslagen
[17] Regeringens proposition 2007/08:45 Elektronisk ingivning för ekonomiska föreningar och vissa andra företag, m.m s 58

Mot bakgrund av de ovan anförda särbestämmelserna som har införts i samband med olika lagverk som reglerar olika former av digitala handlingar tillsammans med det faktum att urkundsförfalskningsbrottet är utformat med tanke på handlingar i pappersform har jag sammantaget svårt att se att urkundsbegreppet, utan någon lagändring och endast i undantagsfall, omfattar digitala handlingar.

Handlingsbegreppet i bedrägeribrottet

Då det gäller att avgöra om en digital uppgift kan utgöra handling och ligga till grund som kvalificerande faktor vid bedömning av grovt bedrägeri kan konstateras att det rimligen inte kan ställas lika höga kvalitetskrav på en skapelse för att den ska uppfylla kriterierna för handling som man ställer på en urkund. Handling är ett vidare och mer ospecificerat begrepp än urkund. Det är generellt fler alster som kan betraktas som handlingar än som uppfyller kriterierna för urkund samt är det av detta skäl enklare att inordna digitala handlingar under handlingsbegreppet i exempelvis det grova bedrägeriet.

Dock får det beaktas, liksom i fallet beträffande urkundsförfalskningen, att stadgandet ursprungligen skrevs med åsyftande av skriftliga handlingar och inte har anpassats till den digitala miljön. Vid en restriktiv tolkning av stadgandet skulle man mycket väl kunna komma till slutsatsen att med handling endast avses fysisk handling i pappersform eller liknande, medan digitala uppgifter inte kan inordnas i detta handlingsbegrepp.

Sammantaget är det min uppfattning att en digital uppgift kan omfattas av det ospecificerade begreppet handling i det grova bedrägeriet. Som exempel över sådana digitala handlingar som jag anser skulle kunna ligga till grund för ett grovt bedrägeri är de fall då bedragaren skickar ut förfalskade uppmaningar från banker och andra kreditinstitut samt vilseleder bankkunder att lämna ifrån sig kontonummer, inloggningsuppgifter m m. Om den utsända handlingen är försedd med bankens varumärke och firma samt är välliknande i förhållande till utseendet på dylika utskick, så är förfarandet lika straffvärt som andra förfarande där man använder sig av falska handlingar.

I vart fall är det inget som hindrar att man, i exemplet med bankhandlingar ovan, i förundersökningen rubricerar förfarandet som grovt bedrägeri. Det får noteras att straffsatsen för grovt bedrägeri är fängelse sex månader till sex år. Den s k proportionalitetsprincipen går som en röd tråd genom hela förundersökningsförfarandet

och vid beslut om tvångsåtgärder i förundersökning skall det alltid göras en avvägning så att skälen för tvångsåtgärden uppväger det intrång eller men i övrigt som tvångsåtgärden innebär[18]. Vid denna avvägning av tvångsåtgärden i förhållande till ”intrång och men” för den misstänkte är brottets svårighetsgrad en viktig faktor; ju grövre brott som skall utredas ju lättare är det att motivera ianspråktagandet av tvångsåtgärder.

Brott mot upphovsrättslagen

Det är inget ovanligt att kriminella skyddar den grova kriminaliteten från insyn, men de är mer vårdslösa då de utför mindre allvarliga brott. Det får anmärkas att det aldrig gick att beslå Al Capone med annan kriminalitet än skattebrott och för detta tilltag dömdes han till fängelse 11 år. På liknande sätt är det, vid utredning av ekonomisk brottslighet, ofta är svårt att belägga exempelvis oredlighet mot borgenär, men väl kan man styrka ett bokföringsbrott. I det dagliga polisarbetet jagar man tjuvar och knarklangare, men denna kriminalitet kan vara svårbevisad. Däremot och som en sidoeffekt av spaningen döms dessa småtjuvar och langare ofta för grov olovlig körning samt annan liknande kriminalitet.

Den numerärt största brottskategorin på Internet idag är brott mot upphovsrättslagen bestående av olaglig kopiering av musik- och filmverk (fildelning). Vid spaning på Internet efter narkotikaaffärer och liknande grövre kriminalitet är det gissningsvis svårt att komma åt den grövre kriminaliteten på grund av att gärningsmännen skyddat denna från insyn, men däremot kan det vara betydligt enklare att belägga den fildelning som samma gärningsmän ägnar sig åt.

Sverige har genom EU-medlemskapet och genom internationella överenskommelser förbundits att ha viss lagstiftning till skydd för upphovsrätten på det immaterialrättsliga området[19]. Vidare har Sverige, genom europakonventionens tilläggsprotokoll av den 20 mars 1952, förbundit sig att tillse att varje fysisk eller juridisk peron skall ha rätt till respekt för sin egendom och inte får berövas sin egendom, annat än i fall som står i överensstämmelse med lag och folkrätten. I europakonventionens huvudprotokoll, artikel 13, har

[18] Exempelvis 24:1 3 st, 25:1 sista st, 26:1 sista st RB m fl

[19] Se bl a Europaparlamentets och rådets direktiv 2001/29/EG om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället, fördrag antaget av FN:s organ för immaterialrätt, World Intellectual Property Organisation (WIPO) i december 1996, Europaparlamentets och rådets direktiv 2004/48/EG

Sverige även förbundit sig att tillse att envar har rätt till effektiva rättsmedel om någon eller några av fri- och rättigheterna enligt konventionen kränks. Det får noteras att Sverige den 15 maj 2008 dömdes av EG-domstolen för att man inte antaget upphovsrättslig lag med innehåll enligt direktiv 2004/48/EG[20]. Det finns därför skäl att Sverige tar immaterialrätten på allvar och tillse att man både har fungerande lagstiftning samt effektiva rättsmedel för efterlevnad av lagen.

Det har i Sverige under senare år förts en het debatt om nedladdning och upphovsrätt till musik- och filmverk samt har det därvid framförts att Sverige borde tillåta upphovsrättsbrott och inte beivra dessa. Sanningen är den att Sverige är uppbundet av internationella överenskommelser m m och det är inte praktiskt möjligt att Sverige ensidigt skulle genomföra något dylikt. Sverige är följaktligen skyldig att ha ett fungerande skydd för bland annat upphovsrätten och även tillhandahålla effektiva rättsmedel så att denna kan upprätthållas.

De immaterialrättsliga brotten är till sin karaktär att jämställa med stöldbrotten i 8 kap brottsbalken. Skillnaden är den att i 8 kap brottsbalken beivras olika olovliga tillgrepp av fysisk egendom eller pengar, medan de immaterialrättsliga brotten berör fall då någon olovliga tar immateriell egendom. Det har stundtals i debatten framförts att polis och åklagare inte borde syssla med immaterialrättsliga brott, eftersom dessa riktas mot ekonomiskt starka aktörer (filmbolag, musikförlag m m). Frånsett att Sverige, som ovan anförts, inte kan ensidigt inta en sådan ståndpunkt så skulle synsättet även medföra att polis och åklagare skulle befrias från hantering av exempelvis bankrån, eftersom även dessa brott riktas mot ekonomiskt mycket starka aktörer.

En stor del av brotten mot upphovsrättslagen begås i digital miljö och jag har därför valt att i korthet genomgå denna.

> *Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk*
>
> *1 kap. 1 § Upphovsrättslagen*
> *Den som skapat ett litterärt eller konstnärligt verk har upphovsrätt till verket oavsett om det är*
> 1. *skönlitterär eller beskrivande framställning i skrift eller tal,*

[20] Mål C-341/07

2. *datorprogram,*
3. *musikaliskt eller sceniskt verk,*
4. *filmverk,*
5. *fotografiskt verk eller något annat alster av bildkonst,*
6. *alster av byggnadskonst eller brukskonst, eller*
7. *verk som har kommit till uttryck på något annat sätt.*

Till litterära verk hänförs kartor, samt även andra i teckning eller grafik eller i plastisk form utförda verk av beskrivande art.
Vad som i denna lag sägs om datorprogram skall i tillämpliga delar gälla även förberedande designmaterial för datorprogram.

Lagen är avsedd att ge skydd åt olika konstnärliga skapelser och man ger upphovsmannen en ensamrätt att själv exploatera dessa. I lagens 1 § fastslås att upphovsmannen erhåller upphovsrätt till sina litterära eller konstnärliga verk oavsett i vilken form de är skapade. Lagen omfattar konstnärliga verk och därmed avses skapelse som har sådan grad av självständighet och individuell särprägel i förhållande till andra konstnärliga verk att det uppnått s k verkshöjd. Det ställs inte några krav på att det ska vara ”god konst” eller att denna ska ha hög konstnärlig kvalitet, utan även hötorgskonst och dåliga konstnärliga alster uppnår verkshöjd och erhåller skydd genom upphovsrättslagen. Kraven på självständighet och individuell särprägel är ganska låga. Även verk som är enkla till sin karaktär och sitt utförande uppnår verkshöjd. Lite förenklat kan sägas att det inte krävs många nedslag på pianotangenterna förrän verket erhållit verkshöjd.

1 kap. 2 § Upphovsrättslagen
Upphovsrätt innefattar, med de inskränkningar som föreskrivs i det följande, uteslutande rätt att förfoga över verket genom att framställa exemplar av det och genom att göra det tillgängligt för allmänheten, i ursprungligt eller ändrat skick, i översättning eller bearbetning, i annan litteratur- eller konstart eller i annan teknik.
Framställning av exemplar innefattar varje direkt eller indirekt samt tillfällig eller permanent framställning av exemplar av verket, oavsett i vilken form eller med vilken metod den sker och oavsett om den sker helt eller delvis.

Verket görs tillgängligt för allmänheten i följande fall:

1. *När verket överförs till allmänheten. Detta sker när verket på trådbunden eller trådlös väg görs tillgäng-*

ligt för allmänheten från en annan plats än den där allmänheten kan ta del av verket. Överföring till allmänheten innefattar överföring som sker på ett sådant sätt att enskilda kan få tillgång till verket från en plats och vid en tidpunkt som de själva väljer.

2. *När verket framförs offentligt. Offentligt framförande innefattar endast sådana fall då verket görs tillgängligt för allmänheten med eller utan användning av ett tekniskt hjälpmedel på samma plats som den där allmänheten kan ta del av verket.*
3. *När exemplar av verket visas offentligt. Offentlig visning innefattar endast sådana fall då ett exemplar av ett verk görs tillgängligt för allmänheten utan användning av ett tekniskt hjälpmedel på samma plats som den där allmänheten kan ta del av exemplaret. Om ett tekniskt hjälpmedel används är det i stället ett offentligt framförande.*
4. *När exemplar av verket bjuds ut till försäljning, uthyrning eller utlåning eller annars sprids till allmänheten.*

Med överföring till allmänheten och offentligt framförande jämställs överföringar och framföranden som i förvärvsverksamhet anordnas till eller inför en större sluten krets.

Upphovsrätten innebär att det endast är upphovsmannen (eller hans rättighetshavare) som äger rätt att exploatera verket, göra det tillgängligt för allmänheten och i övrigt förfoga över verket.

2 kap. 12 § Upphovsrättslagen
Var och en får för privat bruk framställa ett eller några få exemplar av offentliggjorda verk. Såvitt gäller litterära verk i skriftlig form får exemplarframställningen dock endast avse begränsade delar av verk eller sådana verk av begränsat omfång. Exemplaren får inte användas för andra ändamål än privat bruk

Första stycket ger inte rätt att

1. *uppföra byggnadsverk,*
2. *framställa exemplar av datorprogram, eller*
3. *framställa exemplar i digital form av sammanställningar i digital form.*

Första stycket ger inte heller rätt att för privat bruk låta en utomstående

1. *framställa exemplar av musikaliska verk eller filmverk,*
2. *framställa bruksföremål eller skulpturer, eller*
3. *genom konstnärligt förfarande efterbilda andra konstverk.*

Denna paragraf ger inte rätt att framställa exemplar av ett verk när det exemplar som är den egentliga förlagan framställts eller gjorts tillgängligt för allmänheten i strid med 2 §.

Det finns en viss rätt att för privat bruk framställa kopior av offentliggjorda verk. Dock undantas film- och musikverk, vilka man inte får låta någon utomstående kopiera. Man har även undantaget kopieringsrätten om förlagan har gjorts tillgänglig i strid med 1 kap 2 § upphovsrättslagen.

7 kap. 53 § Upphovsrättslagen
Den som beträffande ett litterärt eller konstnärligt verk vidtar åtgärder, som innebär intrång i den till verket enligt 1 och 2 kap. knutna upphovsrätten eller som strider mot föreskrift enligt 41 § andra stycket eller mot 50 §, döms, om det sker uppsåtligen eller av grov oaktsamhet, till böter eller fängelse i högst två år.
Den som för sitt enskilda bruk kopierar ett datorprogram som är utgivet eller av vilket exemplar har överlåtits med upphovsmannens samtycke, skall inte dömas till ansvar, om förlagan för kopieringen inte används i näringsverksamhet eller offentlig verksamhet och han eller hon inte utnyttjar framställda exemplar av datorprogrammet för annat ändamål än sitt enskilda bruk. Den som för sitt enskilda bruk framställer exemplar i digital form av en offentliggjord sammanställning i digital form skall under de förutsättningar som nyss nämnts inte dömas till ansvar.
Vad som sägs i första stycket gäller också, om någon till Sverige för spridning till allmänheten för in exemplar av verk, där exemplaret framställts utomlands under sådana omständigheter att en sådan framställning här skulle ha varit straffbar enligt vad som sägs i det stycket.
Den som har överträtt ett vitesförbud enligt 53 b § får inte dömas till ansvar för intrång som omfattas av förbudet.
För försök eller förberedelse till brott som avses i första och tredje styckena döms till ansvar enligt 23 kap brottsbalken.

Den som uppsåtligen eller av grov oaktsamhet begår intrång i upphovsrätten döms till böter eller fängelse i högst två år. Brottet är straffbart på förberedelse- och försöksstadierna.

Fildelning

Det finns sparsamt med rättsfall beträffande s k fildelning. Ett av de få fall som kommit upp i domstol de senaste åren är domen i mål B 1066-06 vid Linköpings tingsrätt. I målet dömdes en fildelare till villkorlig dom och 40 dagsböter vid brott mot upphovsrättslagen bestående i att han på nätet tillgängliggjort 30 filmverk och 4.592 musikverk/ljudfiler. Därutöver förverkades två hårddiskar, vilka var tagna i beslag. Jag har inte heller lyckats finna någon vägledning i doktrin såvitt avser straffvärdet av olika upphovsrättsliga brott; den senaste verket på området Martin Borgekes ”Att bestämma påföljd för brott”, utgiven 2008, upptar inte särskilt frågan om straffvärdet av olika immaterialrättsliga brott. Med ledning av straffsatsen i lagstadgandet (böter eller fängelse högst 2 år) och målet vid Linköpings tingsrätt kan man dock dra slutsatsen att en fildelning av icke ringa omfattning normalt har ett straffvärde som överstiger ett rent bötesstraff.

Min uppfattning är att man bör beakta att värdet/den ekonomiska skadan av en fildelning är relativt högt redan vid måttliga ”fildelningar”. Som ett tankeexperiment kan man åskådliggöra värdet av skadan i Linköpingsfallet genom att beräkna att ett ordinärt film- eller musikverk (dvd eller cd-skiva) i handeln kostar i genomsnitt 100 kr. Varje musik-cd innehåller uppskattningsvis 12 musikstycken. Det Linköpingsfildelaren tillhandahållit är följaktligen cirka 412 dvd och cd-skivor till ett sammanlagt inköpspris i butik om 41.200 kr. Om Linköpingsfildelaren låtit en annan person olagligt kopiera verken har han följaktligen orsakat skada till ett belopp om 41.200 kr. Det är dock ovanligt att delade filer endast olagligen kopieras av så få som en person, utan en fildelning medför ofta att de tillgängliggjorda filerna kopieras av ibland tiotusentals andra personer. Värdet av ”den tillgripna” immateriella egendomen kan därmed bli astronomisk. Dessa värden kan sättas i relation till snatterigränsen som vid senaste prövningen hamnade på 800 kr[21]. En vanlig invändning är att gärningsmannen ju aldrig skulle ha köpt verken om han fått betala fullpris och att man därför ska räkna värdet efter någon annan och lägre tariff. En sådan invändning godtas inte såvitt gäller förmögenhetsbrotten enligt brottsbalken och det

[21] NJA 2003 s 495

finns inte skäl att acceptera en mildare syn på upphovsrättsbrotten[22]. Om man sätter värdet av Linköpingsfallet i relation till de fall då man dömer stöldbrott med endast ett hänsynstagande till värdet, så hade straffvärdet av Linköpingsfallet måhända bedömts som grov stöld. I Linköpingsfallet saknas dock uppgift om hur många som laddat ned filer, utan man dömde endast på det olovliga tillgängliggörandet.

En ytterligare aspekt av upphovsrättsbrottet som man i vart fall kan reflektera över är att dessa brott riktar sig mot egendom som ofta är svår att freda mot intrång. Det är svårt att förhindra att någon olovligen exempelvis fildelar. En stöld kan kvalificeras till grov stöld om den avsett egendom som är särskilt svår att skydda mot obehöriga angrepp (8 kap 4 § 2 st BrB; ”gärningen eljest varit av särskilt farlig art”)[23]. Upphovsrättsbrottet är mycket likt stöldbrottet; i båda fallen rör det sig om olovliga taganden av egendom. För kongruensen inom det straffrättsliga området bör man av detta skäl inte ha en alltför mild syn på upphovsrättsbrotten.

I 7 kap 53 § 3 st upphovsrättslagen straffbeläggs även att någon för in/tillgängliggör exemplar av verk i Sverige om framställningen skett i strid med svensk lag och denna framställning skett utanför Sverige.

I 7 kap 53 a § upphovsrättslagen ges möjlighet att förverka egendom som varit föremål för brott, det ekonomiska utbytet av brott och hjälpmedel/brottsverktyg.

Enligt 7 kap 59 § upphovsrättslagen äger åklagaren väcka tala om målsägande anger brottet till åtal eller åtal är påkallat från allmän synpunkt. Angivelse kan enkelt och snabbt inhämtas via Medlemsföretag i IFPI Svenska Gruppen, Stockholm (musikverk) och Svenska Antipiratbyrån, Stockholm (filmverk)

Producenterna av film- och musikverk har, med skiftande framgång, försökt att med olika digitala spärrar förhindra olaglig kopiering av verken. Den senaste förändringen som gjorts i upphovsrättslagen innebär att man i 6 a kap 52 d – 52 e §§ upphovsrättslagen infört ett förbud mot att kringgå dylika kopieringsskydd samt även förbjudit tillverkning, marknadsföring, spridning m m av anordning och komponenter som avser att användas för att ta sig förbi sådana kopieringsskydd. Straffet för att tillverka, marknadsföra,

---

[22] J f r NJA 1990 s 355 där man fastslog att värdet vid häleri skulle fastställas utifrån det värde som gäller för det försäljningsled varifrån godset stals.

[23] Exempelvis NJA 1980 s 253

sprida m m sådana anordningar/komponenter är böter eller fängelse högst sex månader och straffet för att kringgå kopieringsskydd är böter, 7 kap 57 b § upphovsrättslagen.

Slutsatser upphovsrättsintrång

Upphovsrättsbrott är relativt enkla att belägga. Nedladdningar och tillgängliggörandet av de skyddade film- och musikverken är ju direkt observerbara på nätet och bevisningen finns omedelbart tillgänglig.

Vid samtal med Henrik Pontén, jurist vid Svenska Antipiratbyrån, framkommer att det sannolikt är få polisiära ingripanden som får sådan omedelbar och mätbar effekt på brottsligheten som just ingripanden mot fildelningsbrott. Ett ingripande mot fildelare uppmärksammas, vilket medför en omgående minskning av denna brottstyp. Det blir följaktligen ett stort utbyte, i form av minskad kriminalitet, av en relativt ringa polisiär insats.

Sammanfattningsvis kan konstateras att upphovsrättsbrotten i de flesta fall är relativt enkla att hantera; om någon privatperson i Sverige via nätet tillgängliggör ordinära filmer och musik så är det i de flesta fallen uppenbart att vederbörande saknar rätt till detta samt att han bryter mot upphovsrättslagen. Brottet är lätt att styrka – bevisningen finns tillgänglig på nätet – och en lagföring får en omedelbar allmän- och individualpreventiv effekt.

Olovligt brukande

> *10 kap. 7 § Brottsbalken*
> *Om någon olovligen brukar någon annans sak och därigenom vållar skada eller olägenhet, döms han för olovligt brukande till böter eller fängelse i högst ett år…..*
>
> *Är brott enligt första stycket grovt, döms till fängelse, lägst sex månader och högst fyra år.*

Den som olovligen brukar annans sak och med detta vållar skada eller olägenhet kan dömas för olovligt brukande. Det krävs inte att den olovligt brukade saken finns i gärningsmannens besittning, utan denne kan göra sig skyldig till brott även vid ett olovligt ”distansbrukande” av annans sak. Tidigare fanns ett krav på besittning i stadgandet, men detta borttogs under 1980-talet för att man skulle kunna använda brottet mot bland annat så kallade tidsstölder vid

olovligt brukande av större datoranläggningar[24]. Före lagändringen (samt förtydligandet av denna i förarbetena) frikände Svea hovrätt från olovligt brukande gällande en tidigare telefonabonnent som olovligen kopplat in sin telefon på nätet[25]. Målet hade sannolikt fått annan utgång om brottet begåtts efter lagändringen och bevisningen hade sett annorlunda ut i målet.

Med rekvisitet skada avses ekonomisk sådan. Däremot rekvisitet olägenhet tar sikte på obehag i annat än rent ekonomiska hänseende. I doktrin exemplifieras olägenhet[26] som att någon olovligen använder någon annans kläder, utan att det uppstår någon påvisbar ekonomisk skada. Redan det obehag som ägaren till klädesplagget upplever vid vetskap om att någon annan använt plagget uppfyller kravet på olägenhet enligt stadgandet.

Brottet är uppsåtligt och gärningsmannen skall ha uppsåt till det olovliga brukandet. Dock har man använt benämningen ”vållar” i förhållande till skadan eller olägenheten, vilket indikerar att det räcker att gärningsmannen är oaktsam i förhållande till skadan eller olägenheten. Om lagstiftaren avsett att även skade- och olägenhetsrekvisitet skulle omfattas av uppsåtet hade man använt begreppet ”orsakar” eller något liknande begrepp.

Från rättspraxis kan nämnas RH 2004:18 där en arbetstagare dömdes för olovligt brukande gällande hans arbetsdator, vilken han använt för att privat bruk kopiera ett kundregister. Hovrätten för västra Sverige fann i målet att den tilltalade olovligen brukat arbetsgivarens dator vilket inneburit olägenhet för arbetsgivaren.

Lagrummet kan exempelvis användas i de fall någon olovligen kopplar upp sig mot annans trådlösa router. Det olovliga nyttjandet riktas sig mot någon annans sak – routern – och även om man inte kan belägga ekonomisk skada genom snyltandet så innebär förfarandet i vart fall en olägenhet i form av minskad bandbredd för målsägande.

---

[24] NJA II 1986 s. 82 ff

[25] RH 1982:54

[26] Norstedt Juridik, kommentar t 10:7 BrB

Spaning, förutredning och annan underrättelse-inhämtning utanför förundersökning

Det saknas generellt lagstiftning för förutredning, spaning och underrättelseinhämtning som sker utanför ramen för förundersökning. Det finns följaktligen inte något regelverk för hur polis och åklagare allmänt sett får förfara under sådan utredning och det saknas även regler för vilka åtgärder som får vidtas, i vilka sammanhang den ena eller andra åtgärden kan anses befogad m fl frågeställningar. Det finns därför inte heller något samlat regelverk som reglerar underrättelseinhämtning som sker via Internet eller i annan digital miljö.

Det regelverk som finns är dels de allmänna reglerna som gäller för myndighetsutövning som följer av europakonventionen och regeringsformen samt i spridda myndighetsföreskrifter.

Generellt äger myndigheterna inte på något sätt göra intrång i den personliga integriteten utan att det föreligger uttryckligt lagstöd för åtgärden. D v s så snart man visiterar någon, i undersökningssyfte tar sig in i någons bostad eller annat utrymme, undersöker korrespondens eller annan kommunikation, frihetsberövar eller på annat sätt vidtar en åtgärd som kränker den personliga sfären så krävs det lagstöd för åtgärden. Avsaknaden av regelverk för området för underrättelseinhämtning medför generellt att polis och åklagare inte får vidta åtgärd som kan anses integritetskränkande under en underrättelseinhämtning utanför ramen för förundersökning. Rent teoretisk kan man invända att det faktisk är möjligt att ta i beslag, medtaga till förhör, gripa m m utan att det fattats beslut om förundersökning, d v s åtgärden sker utanför själva förundersökningsförfarandet. Dock har man i doktrin och praxis tolkat förundersökningsreglerna så att i sådana fall så igångsätts förundersökningen defacto

genom den företagna tvångsåtgärden[27]. Utöver de nämnda undantagen finns det dock inte något utrymme för att vidtaga tvångsåtgärder i en underrättelseinhämtning utanför förundersökning.

Kvalificerad skyddsidentitet

Enligt lag (2006:939) om kvalificerade skyddsidentiteter kan man tilldela polis eller anställd vid försvaret s k särskild skyddsidentitet som består av andra identitetsuppgifter än de egna verkliga. Särskild skyddsidentitet kan tilldelas någon när det behövs för att inte röja åtgärder inom verksamheten och det finns en påtaglig risk för att ett sådant röjande allvarligt skulle motverka verksamheten eller utsätta någon som berörs av denna för allvarlig fara. Kvalificerad skyddsidentitet skall förbehållas fall då det avser spaning/underrättelseinhämtning gällande grövre brottslighet, 2 § 1 st 1 p lag (2006:939) om kvalificerad skyddsidentitet.

I propositionen till nämnda lag[28] konstateras att polisen m fl myndigheters dolda uppträdande genom täckidentitet m m inte utgör något sådant ingrepp som avses i 2 kap 6 § regeringsformen och för detta krävs det inte något lagstöd.

Om polisen däremot under det förtäckta arbetet vidtar åtgärd som innebär en kränkning av fri- och rättigheterna i regeringsformen eller europakonventionen så krävs det grund för och beslut om någon form av tvångsmedel (j f r ovan beträffande resonemang runt dataintrång).

I propositionen till lag om kvalificerad skyddsidentitet accepteras användandet av dolda spaningsmetoder och där anges[29].

> *De grundläggande principer som gäller för användningen av bl.a. dolda spaningsmetoder är en konsekvens av vad som föreskrivs i polislagen och annan lag. Tre grundläggande principer brukar framhållas. Den första principen är att polisen aldrig själv får begå en kriminaliserad handling för att efterforska eller avslöja ett brott. En andra princip är att polisen aldrig får provocera eller i övrigt förmå någon att inleda en brottslig aktivitet. En tredje princip är att polisen aldrig av*

---

[27] Exempelvis Bring/Diesen, Förundersökning, s 216 - 217

[28] Prop. 2005/06:149 s 16

[29] Prop. 2005/06:149 s 18

spaningsskäl får låta bli att vidta föreskrivna åtgärder mot brott eller en för brott misstänkt person. Därtill gäller de ovan nämnda behovs- och proportionalitetsprinciperna; en åtgärd måste alltså även vara nödvändig i förhållande till sitt syfte och den får inte vidtas om de skador och olägenheter som den kan medföra står i missförhållande till syftet.

Avsikten med kvalificerad skyddsidentitet är inte att reglera användandet av dold identitet som arbetsmetod, utan lagens syfte är endast att skydda inblandade personer och den polisiära verksamheten. Kvalificerad skyddsidentitet är följaktligen inte ett tvångsmedel som i sig ger rätt att vidta integritetskränkande åtgärder.

En fråga är om det i sig kan anses vara en integritetskränkning att en tjänsteman under falskt namn/skyddsidentitet kommer i kontakt med människor, samlar information om dem och får dem att lämna ut information, som de kanske inte skulle givit ut till en myndighet. I propositionen till lag om kvalificerad skyddsidentitet anges att det ”endast är när en myndighet på ett mycket mera omfattande sätt följer och noterar de personliga aktiviteter som en person utför, för att på ett mera systematiskt sätt kartlägga personens liv, som skyddet för privatlivet blir mera allmänt kränkt”[30]. Användandet av skyddsidentitet utgör därför enligt propositionen i normalfallet inte någon sådan kränkning av privatlivet, vilken kräver lagstöd för att kunna genomföras.

I propositionen ger man vidare uttryck för att det är en allmän princip att myndigheterna får låta sina tjänstemän använda sig av skyddsidentiteter och att ett användande av dylika inte är vare sig kontroversiellt eller att det föreligger osäkerhet runt detta användande[31]. D v s det är ett tillåtet förfarande som inte är integritetskränkande och det behövs därmed inte heller någon särskild lagstiftning för att reglera användandet. Propositionen hänvisar till att användningen får ske inom de ramar som uttrycks i 8 § polislagen, d v s med iakttagande av proportion och behov.

Enligt propositionen till lag om kvalificerad skyddsidentitet synes det därmed inte finnas några hinder mot att t ex vid inhämtning av information via Internet låta tjänstemännen ”bygga” olika fiktiva identiteter och genom dessa fiktiva identiteter inhämta information. Kontakterna på Internet är, typiskt sett, ytligare och flyktigare än verkliga fysiska kontakter utanför den ”virtuella världen”. Den yt-

[30] Prop 2005/06:149 s 30
[31] Prop 2005/06:149 s 31

lighet som präglar internetkontakterna medför även att handlingsutrymmet för informationsinhämtningen blir större och att det är ett större spann innan man når upp till den nivå av sådan omfattande och systematiskt kartläggning av en person att skyddet för privatlivet blir mera allmänt kränkt. D v s den nivå då det krävs lagstöd för åtgärden.

Jag är personligen inte lika övertygad som propositionen till lag om kvalificerad skyddsidentitet om att ett nyttjande av en sådan fiktiv identitet inte skall betraktas som ett tvångsmedel. Användandet av en fiktiv identitet innebär att tjänstemannen i lönndom inhämtar information om bevakningsobjektet och på ett, måhända försåtligt sätt, vilseleder spaningsobjektet att avslöja information som denne inte skulle avslöjat för en myndighet. Ett nyttjande av en fiktiv identitet påminner i stora delar om en hemlig telefonavlyssning; spaningsobjektet tror sig prata för och med någon viss person, men är omedveten om att samtalet samtidigt ”avlyssnas”/dokumenteras av någon annan. Om förfarande är att anse som ett tvångsmedel eller att det på annat sätt anses integritetskränkande så skall det, enligt art 8 europakonventionen och 2:6 samt 2:12 regeringsformen, finnas lagstöd för åtgärden.

För Sveriges del går utvecklingen sannolikt åt en uppstramning av arbetsmetoderna och en anpassning till europakonventionen. I vart fall finns en tendens till att i svenska domstolar ta hänsyn och intryck av de tankegångar som ligger bakom europakonventionen om skydd för de grundläggande mänskliga fri- och rättigheterna. Jag har i denna del inte gjort någon efterforskning av hur europadomstolen tolkar användandet av fiktiv identitet i förhållande till regelverket om rätten till rättvis rättegång enligt art 6. Med hänsyn till de tankar och åsikter som högsta domstolen gav uttryck för i NJA 2007 s 1037 kan det dock inte uteslutas att man vid en rättslig prövning konstaterar att den tilltalade inte fått möjlighet till rättvis rättegång på den grunden att bevisningen avlockats den tilltalade av tjänsteman med skyddsidentitet samt att detta skett utan vederbörligt lagstöd för åtgärden.

Sammanfattningsvis är det min uppfattning att lagstiftaren alltför lättvindligt har avstått från att lagstifta om användandet av skyddsidentitet samt att man därmed skjuter över ansvaret till de polismän som hanterar ärendena. Polismännen kommer därmed, i brist på ordentligt regelverk, riskera att begå tjänstefel då de arbetar under skyddsidentitet samt kan avsaknaden av ordentligt lagstöd även medföra att eljest skyldiga kommer att frias av domstol. Givetvis måste svensk polis kunna arbeta under fiktiv identitet och det hade varit betydligt mer rakryggat av lagstiftaren om man försett denna polis med ordentliga arbetsverktyg.

Brottsprovokation/bevisprovokation

I denna del hänvisar jag helt till åklagarmyndighetens RättPM 2007:4, uppdaterad i mars 2008 efter NJA 2007 s 1037. De regler för provokation som uppställs i åklagarmyndighetens rättsutredning håller sådan hög juridisk kvalitet att den, i brist på lagstiftning eller annat regelverk, väl kan läggas till grund för den praktiska hanteringen.

Den enda notering jag vill göra är att det är viktigt att dokumentera och säkra bevisning om att det rör sig om en bevisprovokation, till styrkande av att den misstänkte inte blivit provocerad att begå brottet. D v s ett styrkande av att myndigheten inte brutit mot europakonventionens art 6 om rätten till rättvis rättegång. Denna bevisning torde generellt sett vara svårare att hämta in i digital miljö, än det eljest är att säkra bevisning i den ”verkliga” världen.

Tvångsåtgärder/ undersökning inom ramen för förundersökning

Straffprocessuella tvångsmedel

Det utmärkande draget för ett straffprocessuellt tvångsmedel är att det är frågan om[32].

1. andra åtgärder än straff eller sanktioner,
2. åtgärder med funktioner i straffprocessen eller
3. tvång mot person eller egendom

Till detta kan även tilläggas att åtgärder som innebär intrång i den personliga integriteten såsom hemlig teleavlyssning skall hänföras till kategorin straffprocessuella tvångsmedel. Tvång eller integritetskränkningar gällande att man bryter mot någon av fri- och rättigheterna i regeringsformen eller europakonventionen får endast genomföras med stöd av lag.

[32] Gösta Westerlund, Straffprocessuella tvångsmedel, s 21

Beslag

Beslag innebär att man tar omhand ett fysiskt föremål[33]. När det gäller skriftliga handlingar är det egentligen inte den fysiska handlingen man vill åt, utan istället vill man få del av innehållet/den information som nedtecknats på handlingen. För att undanröja osäkerhet i frågan om skriftliga handlingar skall kunna inordnas under begreppet ”föremål” i 27:1 RB så har man i 2 st i stadgandet infört ett förtydligande innebärande att skriftlig handling omfattas av beslagsbestämmelserna.

Det finns ett väl utvecklat regelverk för beslag och undersökning av brev, telegram, handelsbok m fl typiskt skriftliga handlingar. Frågan uppkommer därmed om ett inhämtande av information från exempelvis den misstänktes dator eller mobiltelefon kan inordnas under rättegångsbalkens regelverk för skriftliga handlingar eller om området är oreglerat.

Skriftlig handling från inte tas i beslag om det kan antagas att handlingen är ställd till eller härrör från befattningshavare enligt 36:5 RB (advokater, läkare m fl) som inte får höras som vittne, 27:2 RB. I samma stadgande finns likaledes ett beslagsförbud för handlingar i förhållande till närstående, enligt 36:3 RB, om det inte för brottet är föreskrivet fängelse i två år eller däröver.

I 27:3 RB föreskrivs att brev, telegram och andra försändelser får tas i beslag vid post- eller telebefordringsföretag om det för brottet är föreskrivet fängelse ett år eller däröver.

Enligt 27:12 får postförsändelse, handelsbok m fl enskilda handlingar endast undersökas av rätten, undersökningsledaren eller åklagaren och dessa äger rätt att ta hjälp av sakkunnig vid denna undersökning. Om beslaget görs av annan än den som äger rätt att undersöka handlingen så skall denne försegla handlingen.

Om det vid husrannsakan anträffas ”post- eller telegrafförsändelse, handelsbok eller annan enskild handling”[34] så skall denne tas omhand i den ordning som anges i 27:12 RB

Sammantaget kan konstateras att det finns ett strikt och noggrant regelverk gällande skriftliga handlingar och telegram. Telegram är, för övrigt, numera en mycket ovanlig företeelse; senast jag själv

[33] 27:1 RB
[34] 28:8 RB

stötte på ett telegrambud var i en av Sveriges television repriserad pilsnerfilm från 1940-talet.

Såvitt jag kan avgöra är regleringen runt skriftliga handlingar i stort oförändrad sedan antagandet av rättegångsbalken 1942, d v s när texten skrevs fanns inte annat än skriftliga handlingar i pappersform (och telegram). Redan det faktum att lagstiftaren rimligen inte kunde ha en tanke på digitala handlingar vid tillkomsten av rättegångsbalken och avsaknaden av straffprocessuellt regelverk runt dessa talar enligt ändamålsprincipen[35], 2:12 RF, mot att man låter utvidga regelverket runt skriftliga handlingar till att omfatta även digitala sådana.

Tvångsåtgärder inom skatteområdet

På skatterättens område har man i 3 § Lag (1994:466) om särskilda tvångsåtgärder i beskattningsförfarandet särskilt angivet att med handling avses även upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. Denna lag behandlar tvångsåtgärder vid skattemyndighets revision och därmed berör regelverket, liksom straffprocessrätten, statliga ingripanden/tvång i utredande syfte mot medborgarna. Det faktum att man i en legaldefinition tydligt angivit att det inte enbart är skriftliga handlingar som skall inbegripas i begreppet handlingar tyder på att det i frågor om processuellt tvång inte är självklart att handlingsbegreppet även omfattar digitala handlingar. Det kan vidare konstateras att vi har ett mycket strikt regelverk såvitt gäller att hämta ut information från teleoperatörer och liknande beträffande innehållet i telemeddelanden (se vidare nedan beträffande hemlig teleavlyssning m m). Även detta talar för att iaktta en viss restriktivitet då det gäller att analogt låta regelverket beträffande beslag av skriftliga handlingar även omfatta förtroliga meddelanden i digital form.

Utifrån nämnda lag (1994:466) om särskilda tvångsåtgärder i beskattningsförfarandet och regelverket runt hemlig teleavlyssning m m kan man e contrario[36] konstatera att rättegångsbalken saknar regelverk för undersökning av digitala media och i digital miljö. Även justitieombudsmannen har i sin granskning kommit till slutsatsen att det saknas regelverk för beslag m m av digitalt material[37]. Det har förekommit förslag till ändringar i den befintliga lagstift-

[35] Exempelvis Bring/Diesen, Förundersökning, sid 260
[36] Motsatsvis
[37] JO ämbetsberättelse 2007/08 s 168: synpunkter m anl av ingripande mot Pirate Bay

ningen[38], men dessa har ännu inte föranlett någon lagändring och jag väljer därför att här inte beröra dessa.

Datorundersökning som husrannsakan?

I Fitger, ”Särtryck ur rättegångsbalken”[39], anges att en undersökning av innehållet i en dator skulle vara en husrannsakan och om man beslutat om husrannsakan i rum eller hus så äger man rätt att utifrån detta beslut undersöka datorer som befinner sig där. Det finns inte något stöd för denna tolkning i utlåtande av JO i samband med Pirate Bay[40]. Min egen uppfattning är att husrannsakan mycket väl kan användas för att leta efter narkotika eller andra föremål som någon gömt i ett datorchassi, men så snart jag vill åt informationen handlar det om en beslagsliknande åtgärd. Det krävs ju inte något husrannsakansbeslut för att sprätta ett kuvert för att komma åt brevet, men väl krävs ett beslagsbeslut för att kunna ta del av handlingen. Husrannsakan är endast ett medel för att med tvång ta sig in i rum, hus eller slutet förvaringsställe, däremot kan jag inte med stöd av husrannsakansreglerna ta omhand egendom eller vidta någon annan integritetskränkande åtgärd. Vidare får påpekas att i 27:12 RB anges tydligt hur man ska förfara beträffande beslag av handelsbok. Om det varit lagstiftarens mening att låta åtkomsten av information i en bok omfattas av husrannsakansreglerna så hade man givetvis återfunnit regelverket runt handelsbok i husrannsakanskapitlet i rättegångsbalken. Jag kommer i den fortsatta framställningen att bortse från Fitgers ”husrannsakanstolkning”[41].

I artikel 8 Europakonventionen anges att envar har rätt till respekt för sitt privatliv, korrespondens m m samt att denna rätt endast får inskränkas av offentlig myndighet med stöd av lag samt att skälen i övrigt skall överensstämma med som kan anses godtagbart i ett demokratiskt samhälle. I 2 kap 6 § regeringsformen anges likaledes att varje medborgare är skyddad mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Inskränkning av skyddet för korrespondens kan endast göras genom lag, 2:12 RF. Den rimliga tolkningen av artikel 8 Europakonventionen och regeringsformen är att beslagsliknande åtgärder, som exempelvis spegling av hårddisk eller mobiltömning, är ett sådant

---

[38] Exempelvis SOU 2005:38

[39] Fitger, ”Särtryck ur rättegångsbalken”, kommentar t 28:1, s 28:7

[40] JO ämbetsberättelse 2007/08 s 168: synpunkter m anl av ingripande mot Pirate Bay

[41] ”Husrannsakanssynsättet” gällande undersökning av dator delas inte heller av Bring/Diesen, Förundersökning, s 378

intrång i privatliv och korrespondens som kräver lagstöd för att få genomföras.

Slutsats om tvångsmedel i digital miljö

Sammantaget kan konstateras att det saknas lagstöd för tvångsåtgärder gällande digital information och att polis samt åklagare borde ha lagstöd när man genomför beslags- och husrannsakansliknande åtgärder mot digital information. Likaledes kan enkelt konstateras att det saknas lagstöd för att vidta ”husrannsakan” via nätet, hemlig dataavläsning och andra liknande ingripanden. D v s egentligen saknas lagstöd för bevissäkring i digital miljö hos den misstänkte eller annan i de fall åtgärden på något sätt är integritetskränkande och den enda digitala bevisning som kan inhämtas är följaktligen öppen information som är tillgänglig för envar.

Det är otillfredsställande att det inte finns någon lagreglerad rätt till beslagsliknande åtgärder i digital miljö. Det är inte heller någon bra lösning att enskilda polismän skall behöva balansera på gränsen till tjänstefel[42] när de vidtar åtgärder mot digitalt media; åtgärder som om de riktat sig mot skriftligt material enkelt hade hanterats inom ramen för ett beslag. Lagstiftaren hade enkelt kunnat förtydliga 27 kap rättegångsbalken genom att utöka regelverket beträffande skriftliga handlingar till att även omfatta digitala sådana, men nu har man valt att inte göra detta. Genom Sveriges anslutning till Europakonventionen, 2:6 och 2:12 RF, 8 § 2 st polislagen m fl stadganden så finns det inte utrymme för polis och åklagare att vidta tvångsåtgärder utan uttryckligt lagstöd. Lagstiftaren har därmed åtagit sig att tillse att polis och åklagare, genom lag, har tillgång till fungerande arbetsverktyg. Det kan påpekas att man i Danmark kommit längre beträffande lagstiftningen för utredning av brott i digital miljö och man tillåter där s k hemlig dataavläsning via nätet[43]. Det strider inte heller mot europakonventionen att tillåta beslag- och husrannsakansliknande åtgärder mot digitalt media. Jag kan bara spekulera i varför man i Sverige inte har tagit i frågan om hur man straffprocessuellt skall hantera digitala meddelanden. Fenomenet digitala meddelanden har ju trots allt varit en allmänt spridd företeelse i omkring 20 år. Måhända beror det på en okunnighet och rädsla för den digitala tekniken i kombination med det svenska kynnet att det är bättre att inte göra någonting alls än att riskera att göra fel.

---

[42] 8 § 2 st polislagen
[43] SOU 2005:38 s 50

Min uppfattning är att man, i avvaktan på ordentligt lagstöd, vid mobiltömning/datorspegling samt liknande ”analogt” tillämpar beslagsreglerna i 27 kap rättegångsbalken gällande skriftliga handlingar. Det är visserligen regelvidrigt att tillåta en analog användning av ett straffprocessuellt tvångsmedel, men med en sådan ordning så upprätthåller man i vart fall en grundläggande rättssäkerhet. Skriftliga meddelanden och digitala sådana är väsentligen lika. Det huvudsakliga är ofta inte själva handlingen som sådan, utan det som är av intresse är innehållet. Med dagens kopieringsteknik så är det lika enkelt att kopiera en skriftlig handling och vidarebefordra kopian till den som åtgärden riktar sig mot som det är att kopiera/spegla digital information samt låta kopian eller originalet återgå till den misstänkte. Vi har av hänsyn till den personliga integriteten valt att ställa höga krav på hanteringen av skriftliga beslag och det synes rimligt att samma krav ställs på handhavande av tvångsåtgärder som syftar till att få del av information i digital form. Ett omhändertagande av digitalt material i samma ordning som gäller för skriftliga handlingar innebär bland annat att man är observant och inte tar del av meddelanden samt liknande från advokater och andra som inte skall avge vittnesmål enligt 36 kap 3 och 5 §§ rättegångsbalken, undersökning sker i enlighet med 27 kap 12 § RB m fl regler, j f r även nedan om 27:22 RB beträffande handläggning av hemlig teleavlyssning m m.

Kort om 27:3 RB

I 27:3 RB kan försändelse tas i beslag vid post- eller telebefordringsföretag om det för brottet är föreskrivet fängelse i ett år eller däröver samt försändelsen skulle ha kunnat tas i beslag hos mottagaren. Denna bestämmelse är i första hand utformad med tanke på sedvanlig postbefordran då försändelsen under en period befinner sig i postens besittning. Stadgandet ger möjlighet att göra beslag vid telebefordringsföretag när försändelsen befinner sig där. Såvitt gäller digitala meddelanden får bestämmelsen en liten praktisk nytta och den kan endast användas vid exempelvis webmail (Hotmail) samt liknande där meddelande rent faktiskt finns hos telebefordringsföretaget och jag hämtar hem meddelandet genom att kontakta tjänsten. Vid övriga vanliga mejltjänster, SMS och liknande så befinner sig meddelandet vid telebefordringsföretaget endast en mycket kort tidsperiod (i normalfallet endast under en del av en sekund) innan det befordras till mottagaren. Det får noteras att stadgandet endast ger rätt till beslag vid post- eller telebefordringsföretag. Det är inte ovanligt att ett mail, innan det når den slutliga mottagaren, läggs på en mailserver vid ett företag eller annan institu-

tion. 27:3 RB ger därvid inte någon rätt till beslag vid andra institutioner än just post- och telebefordringsföretag.

27:3 RB tar dock endast sikte på enstaka och utpekad försändelse som är under befordran. Om man i övrigt vill få del av telebefordrad korrespondens får detta ske inom ramen för hemlig teleavlyssning.

I 27:9 RB finns en möjlighet att förordna om att befordringsföretag skall kvarhålla försändelse till dess frågan om beslag kunnat avgöras. Kvarhållandet tar sikte på situationen att försändelsen skall kunna tas i beslag enligt 27:3 RB. Förordnandet meddelas av rätten, efter yrkande av åklagare eller undersökningsledaren, och gäller för högst en månad i sänder. Stadgandet kan formellt användas för digitala meddelanden, men liksom övriga stadganden i rättegångsbalken så är det inte skrivet för digital information[44] och man kan av legalitetsskäl ifrågasätta om det är förnuftigt att använda stadganden utöver dess ursprungliga ändamål[45].

Hemlig teleavlyssning och hemlig teleövervakning

Tvångsmedlen hemlig teleavlyssning och hemlig teleövervakning är, till skillnad från vad som gäller för ”digitala beslag” enligt ovan, anpassade till den digitala tekniken. Tvångsmedlen tar sikte på att, under förundersökning, säkra bevisning i digital form när det förmedlas eller har förmedlats via elektroniskt kommunikationsnät. Den vanligaste är att sådan information inhämtas efter beslut genom att myndigheten tar kontakt med berört teleföretag och utfår informationen. Dock är tvångsmedlet inte begränsat till inhämtning via kommunikationsföretag, utan tvångsmedlet skall användas även i till exempel de fall man hämtar information genom att ringa upp en röstbrevlåda eller på liknande sätt kommer åt information som är lagrad vid kommunikationsföretag[46].

Hemlig teleavlyssning enligt 27:18 RB innebär att telemeddelanden, som befordras eller har befordrats till eller från ett telefonnummer, en kod eller annan teleadress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet. Tvångsmedlet får användas vid förundersökning beträffande brott för vilket inte är föreskrivet lindrigare straff än

[44] Fitger 2:12 RF särtryck ur rättegångsbalken, kommentar t 27:9 RB
[45] 2:12 RF
[46] Fitger 2:12 RF särtryck ur rättegångsbalken, kommentar t 27:19 RB, 27:34

fängelse i två år samt försök, förberedelse eller stämpling till sådant brott. Vidare kan tvångsmedlet även användas då det avser brott som med hänsyn till omständigheterna kan antas ha ett straffvärde överstigande fängelse i två år. Vid bedömning av brottets straffvärde enligt stadgandets 2 st 3 p får hänsyn tas till 29 kap BrB och den praxis som finns beträffande det aktuella brottet. Man får därvid vara restriktiv, i den misstänktes favör, då det gäller att bedöma straffvärdet[47]. Vid hemlig teleavlyssning äger man rätt att inhämta inte bara de meddelanden som är under befordran, utan stadgandet ger även rätt att inhämta sådana meddelanden som har befordrats.

Hemlig teleövervakning enligt 27:19 RB innebär att uppgifter i hemlighet hämtas in om telemeddelanden som befordras eller har befordrats från viss teleadress och det finns även möjlighet att hindra meddelanden att nå den angivna adressen. Stadgandet tar inte sikte på innehållet i meddelandena, utan de uppgifter som kan erhållas via tvångsmedlet är uppgifter om avsändare/uppringare, samtalslängd, samtals- eller avsändandetidpunkt m fl uppgifter hänförliga till tele- eller datatrafiken. Hemlig teleövervakning får användas vid förundersökning angående brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader samt dataintrång, barnpornografibrott, narkotikabrott av normalgraden och narkotikasmuggling av normalgraden jämte försök, förberedelse eller stämpling till samtliga angivna brott.

Hemlig teleavlyssning eller övervakning kan endast ske då någon är skäligen misstänkt för brottet och det ska vara av synnerlig vikt för utredningen, 27:20 RB. Vidare får åtgärden, enligt samma paragraf, endast avse teleadress som används, har använts eller kommer att användas av den misstänkte samt kan åtgärden även rikta sig mot annan teleadress om det finns synnerlig anledning anta att den misstänkte kommer att kontakta denna adress.

Beslut om hemlig teleavlyssning och övervakning fattas av rätten och beslutet får inte gälla för längre tid än en månad, 27:21 RB. Avlyssning får inte göras beträffande meddelanden eller samtal mellan den misstänkte och hans försvarare samt skall avlyssningen avbrytas om det framkommer att så sker samt skall sådan avlyssning omedelbart förstöras, 27:22 RB.

Avlyssningen skall upphöra om det inte längre finns skäl för åtgärden, 27:23 RB.

---

[47] Fitger 2:12 RF särtryck ur rättegångsbalken, kommentar t 27:18 RB, 27:35

Överskottsinformation får användas för att inleda förundersökning eller motsvarande utredning om det finns fängelse i ett år eller däröver i straffskalan för brottet och det kan antas att brottet inte kommer att föranleda endast böter eller om det finns särskilda skäl. Vidare får överskottsinformation användas för att förhindra förestående brott, 27:23 a RB.

Lag om elektronisk kommunikation

Lagen om elektronisk kommunikation (LEK) innehåller bestämmelser om elektroniska kommunikationsnät och handlingsnormer för de företag som tillhandahåller dessa tjänster. Lagen kan, förenklat uttryckt, anges vara manualen för telebolag och andra företag som agerar inom kommunikationssektorn.

De som tillhandahåller kommunikationsnät och –tjänster skall anordna verksamheten på sådant sätt att man kan bedriva hemlig teleavlyssning och hemlig teleövervakning[48].

I lagen åläggs de som tillhandahåller elektroniska kommunikationsnät och –tjänster tystnadsplikt samt skall de anordna verksamheten på sådant sätt att inte någon utomstående olovligen kan ta del av de skyddade uppgifterna[49]. Sekretesslagens bestämmelser gäller enbart för myndigheter. (Telebolag och liknande är enskilda företag samt för att ålägga dessa sekretess krävs separata tystnadspliktsregler enligt LEK.)

Tystnadsplikten kan brytas i förhållande till polis eller åklagare vid brottsutredning gällande[50]

1. abonnemangsuppgifter om det för brottet är föreskrivet fängelse och brottet, enligt polisens eller åklagarens bedömning, kan föranleda annan påföljd än böter.

2. andra uppgifter om ett särskilt elektroniskt meddelande än innehållet i detta om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år (vid försök, förberedelse eller stämpling till grova brott sänks straffminimum under denna nivå, 23:1 – 2 BrB).

---

[48] 6:19 LEK
[49] 6:3 LEK
[50] 6 kap 19 och 22 §§ LEK

Lagen ger följaktligen endast möjlighet att få ut abonnemangsuppgifter samt trafikuppgifter och liknande information gällande ett specificerat enskilt meddelande. Däremot kan man aldrig med stöd av LEK utfå uppgift om innehållet i meddelande eller uppgift om trafikinformation över en tidsperiod, utan för att utfå dessa uppgifter krävs beslut om hemlig teleavlyssning alternativt hemlig teleövervakning.

Praxis beträffande förverkande av digital utrustning

Den hittillsvarande och av mig kända praktiska tillämpningen av förverkandereglerna då det gäller att ta datorutrusning är att man ofta förverkat en stor del av datoranläggningen. Det finns dock en praxis[51], NJA 1996 s 74, innebärande att det är lätt att montera bort hårddisk och liknande, samt att förverkanden ska begränsas till att avse just hårddisk och liknande informationsbärande media.

[51] NJA 1996 s 74

Slutord

Ett av särdragen med den digitala tekniken är att information kan förvaras och flyttas utan att avsätta några direkta fysiska avtryck. Detta skiljer sig från äldre teknik där informationen varit knuten till en informationsbärare av traditionellt slag (från stentavlor till papper) och där en transport eller kopiering av informationen alltid krävt en fysiskt påtaglig insats. En stor del av vår lagstiftning inom områdena straff- och processrätt är tillkommen och formad i en tid långt innan den digitala tekniken överhuvudtaget existerade. Behovet av att anpassa lagstiftningen till den digitala tekniken har uppmärksammats i flera utredningar, bland annat Ds 2005:6 Brott och brottsutredning i IT-miljö, men dessa utredningar har hittills inte lett till några nämnvärda lagändringar. Framförallt har man ännu inte reglerat kärnfrågan, det vill säga hur man straffprocessrättsligt skall behandla digital information. Därutöver pågår ständig och snabb teknikutveckling, vilket medför att om regelverket har dålig anpassning idag så kan man räkna med att anpassning blir ännu sämre i förhållande till framtida kommunikationsteknik.

Däremot synes ny lagstiftning, som exempelvis lag (1994:466) om särskilda tvångsåtgärder i beskattningsförfarandet, vara formulerad och anpassad till den digitala tekniken.

Jag har undvikit att spekulera i orsaken till oviljan att anpassa äldre lagstiftning, utan jag stannar vid konstaterandet att den nuvarande tillämpningen när det äldre regelverket avsett för pappershandlingar används för digitala handlingar medför en tillämpning som strider mot regeringsformen och Europakonventionen. I förarbeten m m framförs ofta att avsikten är att göra lagstiftningen teknikneutral och att lagverket ifråga skall kunna fungera oavsett den tekniska kontexten. Under de senaste 100 åren har det dock tagits många tekniksprång vilka varit svåra att förutse. Lärdomen av denna utveckling är att vi inte heller för framtiden kan förutse den tekniska utvecklingen, utan vi blir tvungna att lära oss leva med den och måhända försöka att snabbare än hittills vara villiga att förändra den befintliga lagstiftningen allt efter förändringarna i våra kommunikationsmönster.

REFERENSER

Prop 2005/06:149
Prop 2006/07:66
Prop 2007/08:45

Europaparlamentet och rådets direktiv 2001/29/EG om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället
Europaparlamentet och rådets direktiv 2004/48/EG

EG dom i mål C-341/07

SOU 1996:40
SOU 2005:38

NJA 1967 s 93
NJA 1972 s 643
NJA 1980 s 253
NJA 2003 s 495
NJA 1995 s 561
NJA 1996 s 74
NJA 1990 s 355

NJA II 1986 s 82 ff

RH 1982:54
RH 1992:81
RH 2004:18

JO ämbetsberättelse 2007/08 s 168

Svea hovrätt, dom i mål B 5358-01, allm åkl ./. Jesus Alcalá
Linköpings tingsrätt, dom i mål B 1066-06

Martin Borgeke, *Att bestämma påföljd för brott*, 2008, Norstedts Juridik

Thomas Bring/Christian Diesen, *Förundersökning*, tredje upplagan, 2007, Norstedts Juridik

Peter Fitger, *Särtryck ur Rättegångsbalken*, 1999, Norstedts Juridik

Stefan Kronqvist, *Brott och digitala bevis*, andra uppl, 2007, Norstedts Juridik

Gösta Westerlund, *Straffprocessuella tvångsmede*l, tredje upplagan, 2007, Bruuns Bokförlag

Åklagarmyndighetens RättsPM 2997:4 (uppdaterad mars 2008), *Provokativa åtgärder*

Norstedts Juridik, kommentar t 10:7 BrB