

DIGITAL BESLAG OCH SPANING UNDERCOVER. REFLEKTIONER RUNT TVÅ POLISIÄRA ARBETSMETODER

AV UNIVERSITETSADJUNKT HÅKAN HALLBÄCK

*This article deals with two aspects of Swedish criminal procedure: police investigations in digital environments and the possibilities that police have to work undercover. In both cases, the Swedish rules and regulations are set in relation to the European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention). Concerning digital investigations, the Swedish police execute examinations of computers and other digital media belonging to suspects on a daily basis. Both the European Convention and the Swedish constitution state that everyone has the right to privacy concerning their correspondence and that public authorities can transgress this right only via specific legal exceptions. The Swedish code of judicial procedure provides strictly regulated possibilities for the police to investigate the contents of different kinds of written material. There is, however, no law supporting investigations in a digital environment, which means that the police violate the European Convention and Swedish constitution each time they carry out an investigation of digital media. In Sweden, the law about qualified protection of identity provides the legal basis for undercover investigations, which are primarily used to combat organized crime. This law contains no concrete stipulations as to how an undercover search should be carried out. This kind of search can give a considerably more thorough mapping of the life of a search object than e.g. wire-tapping. Yet one can wonder whether the gathering of information by undercover means should require legal stipulations similar to those the police are forced to abide by when conducting other types of criminal investigations.**

Inom ramen för förundersökning enligt rättegångsbalken genomför polis och åklagare dagligen undersökning av digitalt material, såsom mobiltelefoner, datorer, usb-minne, minneskort och andra media som kan bära information. Om man frågar polis och åklagare om den rättsliga grunden för tvångsmedlet erhålles därvid hänvisning till en mängd skiftande rättsgrunder för tvångsåtgärden; allt från rättegångsbalkens beslagsregler till att en undersökning av digitalt material utgör en husrannsakan. Avsikten med denna utredning är att klargöra om det behövs lagstöd för myndighets undersökning av digitala media och, i så fall, om det verkligen finns något sådant lagstöd.

* Title in English: *Digital and Undercover Investigations: Reflections on Two Methods of Police Work.*
Original in Swedish.

Sist i utredningen klargörs lagen om kvalificerad skyddsidentitet (fiktiv identitet för poliser som arbetar "undercover").

Tvångsåtgärder/undersökning inom ramen för förundersökning

Det utmärkande draget för ett straffprocessuellt tvångsmedel är att det är frågan om¹.

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.

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

Beslag

Beslag innebär att man tar omhand ett fysiskt föremål². När det gäller skriftliga handlingar är det egentligen inte den fysiska handlingen man vill åt, utan istället vill man få del 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.

För skriftlig handling gäller att den inte får 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 beslagförbud för handlingar i förhållande till närstående 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 förseglja handlingen.

Om det vid husrannsakan anträffas "post- eller telegrafafförsändelse, handelsbok eller annan enskild handling"³ 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 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 inget 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 ändamålsprincipen⁴, 2:12 RF, mot att man låter utvidga regelverket runt skriftliga handlingar till att omfatta även digitala sådana.

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 telededdelanden, se vidare nedan beträffande hemlig teleavlyssning m m.

Utifrån nämnda lag (1994:466) om särskilda tvångsåtgärder i beskattningsförfarandet och regelverket runt hemlig teleavlyssning m m kan man e contrario 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 material⁵. Det har förekommit förslag till ändringar i den befintliga lagstiftningen⁶, men dessa har ännu inte föranlett någon lagändring och jag väljer därför att här inte beröra dessa.

I Fitger, "Särtryck ur rättegångsbalken"⁷, anges att en undersökning av innehåll 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*⁸. 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 husrannsakanbeslut för att sprätta ett kuvert för att komma åt brevet, men väl krävs ett beslagsbeslut för att kunna ta del av handlingen. Husrannsakan är ju endast ett medel för att med tvång ta sig in i rum, hus eller slutet förvaringsställe, däremot kan jag inte med stöd av husrannsakanreglerna ta omhand egendom eller vidta någon annan integritetskränkande åtgärd. Jag kommer i den fortsatta framställningen att bortse från Fitgers "husrannsakanstolkning"⁹.

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 husrannsakanliknande 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 på Internet 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 tjänstefel¹⁰ 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 nätet¹¹. Det strider inte heller mot europakonventionen att tillåta beslag- och husrannsakanliknande 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.

Min uppfattning och vilken också vidarebefordras till polisstudenterna är att man, om man trots avsaknaden av lagstöd, väljer att genomföra mobiltömningar, datorspeglning 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.

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

I 27:9 RB finns en möjlighet att förordna om att befordringsföretag skall kvarhålla försändelse till dess frågan om beslag kunnat avgöras. Förordnandet meddelas av rätten, efter yrkande av åklagare eller undersökningsledaren, och gäller för högst en månad i sänder. Stadgandet kan användas för digitala meddelanden, men liksom övriga stadganden i rättegångsbalken så är det inte skrivet för digital information¹² och man kan av legalitetsskäl ifrågasätta om det är förnuftigt att använda stadganden utöver dess ursprungliga ändamål¹³.

Sammanfattningsvis kan konstateras att det krävs lagstöd för att tvångsåtgärder innebärande att man säkrar digital information och att sådant lagstöd saknas. Det vore önskvärt att dylikt lagstöd snarast infördes och enklast görs detta genom en utvidgning av 27:1 2 st RB på sätt att begreppet handling även kommer att omfatta digitala sådana.

Kvalificerad skyddsidentitet och användandet av fiktiv identitet vid brottsspaning

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 lag¹⁴ 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 datainträng).

I propositionen till lag om kvalificerad skyddsidentitet accepteras användandet av dolda spaningsmetoder och där anges¹⁵.

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 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 någon 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"¹⁶. 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 användande¹⁷. 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 informationsinhämtning 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 ytlighet som präglar internetkontakterna medför även att handlingsutrymmet för informationsinhämtningen blir större och att det är ett större utrymme 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 löndom 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 i denna del 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 rakryggt av lagstiftaren om man försett denna polis med ordentliga arbetsverktyg.

Litteratur

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

Gösta Westerlund, *Straffprocessuella tvångsmedel*, tredje upplagan, 2007, Bruuns Bokförlag

Peter Fitger, Särtryck ur *Rättegångsbalken*, 1999, Norstedts Juridik JO ämbetsberättelse 2007/08 s 168: synpunkter m anl av ingripande mot Pirate Bay
SOU 2005:38

Prop 2005/06:149

Noter:

- 1 Gösta Westerlund, Straffprocessuella tvångsmedel, s 21
- 2 27:1 RB
- 3 28:8 RB
- 4 Exempelvis Bring/Diesen, Förundersökning, sid 260
- 5 JO ämbetsberättelse 2007/08 s 168: synpunkter m anl av ingripande mot Pirate Bay
- 6 Exempelvis SOU 2005:38
- 7 Fitger, "Särtryck ur rättegångsbalken", kommentar t 28:1, s 28:7
- 8 JO ämbetsberättelse 2007/08 s 168: synpunkter m anl av ingripande mot Pirate Bay
- 9 "Husrannsakaranssynsättet" gällande undersökning av dator delas inte heller av Bring/Diesen, Förundersökning, s 378
- 10 8 § 2 st polislagen
- 11 SOU 2005:38 s 50
- 12 Fitger 2:12 RF särtryck ur rättegångsbalken, kommentar t 27:9 RB
- 13 2:12 RF
- 14 Prop. 2005/06:149 s 16
- 15 Prop. 2005/06:149 s 18
- 16 Prop 2005/06:149 s 30
- 17 Prop 2005/06:149 s 31

Adresse:

Polisutbildningen

Växjö universitet

SE - 351 95 Växjö

E-mail: hakan.hallback@vxu.se