

Regeringskansliet
Justitiedepartementet
Åklagarenheten
103 33 Stockholm

**Tillgång till elektronisk kommunikation i brottsutredningar m.m.
Delbetänkande (SOU 2005:38)**

Datainspektionen har utifrån sitt verksamhetsområde följande synpunkter på förslagen i betänkandet.

Under de senaste åren har olika utredningar lagt fram en rad förslag som syftar till att underlätta brottsbekämpningen. Det gäller såväl förstärkta tvångsmedel som utökade möjligheter till insamling och registrering av personuppgifter. Från senare tid kan exempelvis nämnas förslaget om vidgad tvångsmedelsanvändning i IT-miljö (se Ds 2005:6 Brott och brottsutredning i IT-miljö), förslaget om utvidgad tvångsmedelsanvändning för att förebygga eller förhindra allvarlig brottslighet (se Ds 2005:21) och förslagen om hemlig rumsavlyssning (Promemoria från justitiedepartementet). Till detta kommer redan antagna förslag såsom det om utökad användning av DNA-teknik inom brottsbekämpningen jämte olika internationella förslag om åtgärder för att underlätta för de brottsbekämpande myndigheterna såsom förslag om obligatorisk skyldighet för operatörer m.fl. att bevara uppgifter som avser enskilda personers telefon- och datakommunikation (uppgifter från elektronisk kommunikation). De brottsbekämpande myndigheterna måste naturligtvis ges effektiva medel för att kunna utreda brott. Samtidigt måste enskildas rätt till respekt för sitt privatliv upprätthållas. Eftersom varje tvångsmedel och övervakning av enskilda personer innefattar ett integritetsintrång måste nödvändigheten av dessa metoder alltid vägas mot integritetsskyddsintresset. Vid dessa bedömningar måste hänsyn tas till regeringsformens och

Europakonventionens krav. Enskildas rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens är en grundläggande rättighet i ett demokratiskt samhälle. Varje inskränkning i denna rättighet måste bygga på ett angeläget samhälleligt behov av inskränkningen och den måste stå i rimlig proportion till det syfte som ska tillgodoses genom ingreppet. Vidare måste undantagen vara utformade med sådan precision att inskränkningen av rättigheten är förutsebar i rimlig utsträckning. Vid bedömningen om det föreligger ett behov av ett nytt tvångsmedel spelar frågan om effektiviteten och det praktiska värdet av det en stor roll. Datainspektionen saknar förutsättningar att närmare bedöma behovet av de av utredningen föreslagna nya tvångsmedlen. Datainspektionen kan dock konstatera att det nu, som anges ovan, finns ett antal olika förslag till åtgärder som är avsedda att underlätta för de brottsbekämpande myndigheterna i kampen mot den allt mer avancerade brottsligheten. Det är enligt Datainspektionens mening nödvändigt för lagstiftaren att vid sin prövning göra en sammantagen bedömning som tar hänsyn till de samlade effekterna av de förslag som man avser att genomföra.

Datainspektionen anser också att en analys behövs av konsekvenserna när det gäller den vidare hanteringen av den mängd uppgifter om enskilda människor som samlas in. En ny polisdatalagstiftning är i detta sammanhang angelägen.

Datainspektionen lämnar i det följande närmare synpunkter på några av förslagen i betänkandet.

4 En samlad reglering i rättegångsbalken

Utredningen föreslår (s. 198) att det i lagtexten inte ska finnas någon motsvarighet till det krav som finns idag på att ett beslut om hemlig teleavlyssning eller hemlig teleövervakning ska ange vilken teleadress tillståndet gäller. Det innebär att det inte längre ska vara ett krav att ett specificerat tekniskt hjälpmedel anges i domstolens beslut.

Enligt Datainspektionens mening är det nödvändigt att en bestämmelse om vad som får avlyssnas eller övervakas är så konkret utformad att domstolen kan ta ställning till lagligheten och åläggs att i beslutet ange den konkreta åtgärd som

avses. Datainspektionen är inte övertygad om att förslaget om att slopa kravet på att ange en specificerad teleadress innebär att man fortsättningsvis kommer att nå upp till de krav på sådan precision beträffande förutsebarhet som krävs för lagligheten av inskränkningar av rättigheter som avser enskildas skydd för privat- och familjeliv och sin korrespondens. Utan tillräcklig precisering kan förslaget i dessa delar komma att anses som oförenligt med Europakonventionens artikel 8.

4.5 Identifiering av tekniskt hjälpmedel

Utredningen föreslår att övervakning enligt 27 kap. 19 § RB i fortsättningen även ska innebära att uppgifter i hemlighet få hämtas in för identifiering av tekniska hjälpmedel.

Som Datainspektionen uppfattar förslaget ska de brottsutredande myndigheternas nuvarande möjligheter till teleövervakning utvidgas till att avse en möjlighet att söka av och ringa in vilka tekniska hjälpmedel som finns inom ett geografiskt område. Den beskrivning som ges av innebörden av metoden (s. 212) ”att med hjälp av en speciell typ av tekniskt hjälpmedel, som används i vissa närliggande länder, identifiera andra tekniska hjälpmedel, dvs. de teleadresser som är aktuella och används av en viss person” ger enligt Datainspektionens mening inte tillräckligt underlag för att bedöma om metodens risker kan accepteras från integritetsskydds- och rättsäkerhetssynpunkt.

7 Bevarandeskyldigheten

När det gäller bevarandeskyldigheten för operatörerna lägger utredningen inte fram något förslag utan beskriver det behov som de brottsutredande myndigheterna har av att få tillgång till trafikuppgifter i förundersökningar. Vidare beskrivs de ”operativa” problem som de nuvarande reglerna enligt utredningens bedömning skapar.

Datainspektionen konstaterar att frågan om bevarande av trafikdata är föremål för gemensamma överväganden inom EU. När det gäller synpunkter på dessa förslag inom EU vill Datainspektionen hänvisa till bilagda yttranden från den s.k. artikel 29-gruppen (se bilaga 1 och 2).

9.4 Hemlig dataavläsning – ett nytt tvångsmedel

Ett nytt tvångsmedel föreslås som innebär att information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål. Det ska således bli möjligt att undersöka allt informationsinnehåll i enskildas datorer genom att i hemlighet skicka en mjukvara till en dator eller att genom ett fysiskt ingrepp placera en hård- eller mjukvara i en dator, t.ex. vid ett hemligt intrång i en persons bostad eller på dennes arbetsplats. I vissa fall ska åtgärderna inte ens kräva att någon är skäligen misstänkt för brott.

Som anges ovan saknar Datainspektionen förutsättningar att närmare bedöma behovet av att införa detta nya tvångsmedel. När det gäller avvägningen mot integritetsskyddsintresset inger förslaget betänkligheter. Tillämpningsområdet är visserligen klart avgränsat till allvarigare brottslighet med hög straffskala men även dataintrång som har en låg straffskala finns med i tillämpningsområdet. Vidare lämnar den s.k. straffvärdeventilen i förslaget öppet för en tillämpning som gör att åtgärden kan komma att användas vid brottslighet där straffvärdet senare visar sig vara betydligt mindre än vad som först antagits. Än mer betänkligt är att hemlig dataavläsning också ska få äga rum när det inte finns någon som är skäligen misstänkt för brottet. Detta sammantaget med att avläsningen ska få avse ett informationssystem vilket utgör ett icke närmare definierat begrepp gör att Datainspektionen ifrågasätter om förslaget når upp till de krav på sådan precision beträffande förutsebarhet som krävs för lagligheten av inskränkningar av rättigheter som avser enskildas skydd för privat- och familjeliv, sitt hem och sin korrespondens.

När det gäller de rätts säkerhetsgarantier som ska kringgärda tvångsmedlet finns det dessutom en del ytterligare frågor som behöver belysas för att man ska kunna ta ställning till om det nya tvångsmedlet över huvud taget kan godtas. De tekniska förutsättningarna för hantering av data i elektronisk form är komplicerade. Hur ska exempelvis en säker identifiering av den dator eller datorsystem som ska undersökas på distans via nät eller trådlöst kunna åstadkommas, dvs. till undvikande av att man undersöker ett informationssystem som inte omfattas av ett beslut om hemlig dataavläsning? Vilka risker finns det för förvanskning av

informationen vid en sådan dataavläsning och hur ska dokumentation av de tekniska åtgärder som vidtas vid denna form av avläsning säkras. Detta är exempel på frågor som behöver belysas närmare.

Enligt Datainspektionens mening måste hemlig dataavläsning, typiskt sett, anses betydligt mer integritetskänslig än andra, befintliga tvångsmedel. En av anledningarna till detta är att avläsningen inte som vid exempelvis teleavlyssning är begränsad till att fånga upp meddelanden som är under befordran utan kan omfatta all information som finns lagrad i någons informationssystem jämte den informationsbehandling som pågår när dataavläsningen utförs (avläsning i realtid). Det kan således omfatta all slags information i digital form exempelvis ljud, bild och privat korrespondens. Regleringen av hur den information som inhämtas genom hemlig dataavläsning ska få hanteras är av avgörande betydelse för effekterna av förslaget i fråga om integritetsskydd.

Utredningen anser att det inte ska finnas någon regel som anger att upptagningar som saknar betydelse från brottsutredningssynpunkt ska förstöras omedelbart efter det att de har granskats (se avsnitt 9.4.12 Hantering av inhämtad information). Utredningen föreslår istället en reglering som anger att en upptagning som har gjorts vid hemlig dataavläsning ska granskas snarast möjligt. De delar av upptagningarna som är av betydelse från brottsutredningssynpunkt ska bevaras till dess att förundersökningen har lagts ned eller avslutats, eller om åtal har väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra förestående brott, ska de bevaras så länge det behövs för att förhindra brott. De ska därefter förstöras.

Enligt Datainspektionens mening riskerar en sådan reglering att medföra att en stor mängd uppgifter rutinmässigt bevaras under en längre tid. Med hänsyn till den föreslagna åtgärdens särskilt ingripande karaktär och de avsevärda integritetsrisker som får anses vara förknippade därmed anser Datainspektionen att detta är otillfredsställande. Inspektionen anser att uttryckliga regler bör införas om att uppgifter som inte är relevanta för att utreda brott ska förstöras omedelbart efter att

de har granskats, i likhet med vad som gäller för tvångsmedlet hemlig kameraövervakning och i likhet med Buggningsutredningens förslag.

Datainspektionen noterar att 9 § tredje stycket förslaget till lag om hemlig dataavläsning innehåller ett undantag från vad som föreskrivs om förstörande av upptagningar i ett andra stycket. Enligt undantagsregeln ska de brottsutredande myndigheterna få behandla uppgifterna från upptagningar i enlighet med vad som föreskrivs i lag. Det kan vara exempelvis polisdatalagen. Konsekvenserna härav är inte belysta. Förslaget till ny polisdatalag bereds sedan lång tid tillbaka i Regeringskansliet.

Enligt förslaget ska giltighetstiden för lagen om hemlig dataavläsning till en början begränsas till fem år. Inspektionen konstaterar att det i förslaget inte anges något om formerna för en framtida utvärdering av lagen och dess tillämpning. För det fall lagen genomförs vill Datainspektionen understryka vikten av att en sådan utvärdering görs på ett så brett och objektiva plan som möjligt där effekterna för enskildas integritetsskydd beaktas och analyseras noggrant.

På hittillsvarande underlag avstyrker inspektionen förslaget om hemlig dataavläsning.

Detta yttrande har beslutats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Leif Lindgren, avdelningsdirektören Elisabeth Wallin och datarådet Hans-Olof Lindblom, föredragande.

Göran Gräslund

Hans-Olof Lindblom

Bilaga 1: Article 29 Data Protection Working Party, Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications network with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. [Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)]

Bilaga 2: Article 29 Data Protection Working Party, Opinion 113/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM (2005)438 final of 21.09.2005)