

Regeringskansliet  
Justitiedepartementet  
103 33 Stockholm

## **Ds 2005:6 Brott och brottsutredning i IT-miljö**

Datainspektionen har granskat förslagen i promemorian huvudsakligen utifrån sin uppgift att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter.

### **11.1.3 Olovlig avlyssning**

Datainspektionen har ingen erinran mot att olovlig avlyssning av datorer kriminaliseras. Tvärtom är det en åtgärd som är önskvärd om den kan förhindra att uppgifter om enskilda personer kommer i orätta händer. Det torde dock vara förenat med stora svårigheter att närmare precisera det kriminaliserade området. De bestämmelser som utredaren förslår (9 c och 9 d §§ BrB) kan med hänsyn till hur den tekniska verkligheten ser ut bli svåra att tillämpa. Den enskilde datoranvändaren kan få svårt att förutse vad som är brottsligt. Nedan följer några tekniska frågeställningar som behöver belysas och klargöras.

Vad avses med *avlyssning med tekniskt hjälpmedel*? Omfattar det viss programvara och i så fall är det användningen eller förekomsten av programvaran som är olaglig? När gör man sig skyldig till brott? När man söker efter öppna noder (ibland görs detta automatisk av datorn när den slås på), vilket ju innebär avlyssning av det frekvensband som nätverket använder sig av? När man ansluter sig till en s.k. hotspot? För att göra det måste man avlyssna etern efter signalerna från denna s.k. hotspot och då får man oundvikligen in även signaler från andra nätverk. Det finns då även risk för att man kan råka ansluta sig till "fel" nätverk.

*Förberedelse till olovlig avlyssning*? Bärbara datautrustningar som PDA och Laptop har inbyggda WLAN och kan visa automatiskt vilka nät som finns tillgängliga. De kan vara inställda på att ansluta till trådlösa nät automatiskt utan att användare upptäcker att man anslöts till någon annans accesspunkt t.e.x. grannens. Detta inträffar i det mobila samhället på grund av att man inte kan skilja på allmänna accesspunkter och ad-hoc uppsatta nät. Kan förekomsten av programvara i en dator räknas som förberedelse till brott? Mycket av den programvara som

används för avlyssning, övervakning och dataintrång används i legitima syften. Som IT-säkerhetskonsult kan man i sin vanliga bärbara dator ha program för penetrations- och säkerhetstestning av trådlösa nätverk och kan tänkas ofta använda sig av s.k. hotspots eller andra ”öppna noder” för att ansluta sig till Internet. I sådana fall utför man samma åtgärder för att få tillgång till nätresurser som den som har för avsikt att begå dataintrång eller olovlig avlyssning. Hur ska man i praktiken kunna skilja ut det kriminaliserade agerandet?

*Icke allmänt tillgängliga signaler?* Om man lovligt nyttjar ett nätverk kan man enkelt ta del av trafiken i det. Kan man då ”olovligen” avlyssna trafik i ett nät man lovligt använder? Är signalerna från en s.k. accesspunkt i ett trådlöst nät allmänt tillgängliga i den mening som avses i de föreslagna bestämmelserna? Är det fråga om icke allmänt tillgängliga signaler i ett trådlöst nätverk som det inte är lovligt att ansluta sig till, exempelvis i situationer när

- nätägaren stänger av ”broadcast SSID” (som nätet använder för att ge sig och sin identitet till känna)
- nätägaren krypterar nätkommunikationen
- nätägaren använder sig av särskilda säkerhetsprodukter för stark autentisering
- nätägaren på annat sätt styr tillgång till nätet exv. med hjälp av MAC-adresslistor?

Om man har s.k. bluetooth eller liknande funktion påslagen i sin mobiltelefon försöker den automatiskt ansluta till andra närliggande enheter (s.k. ad hoc nätverk). Det är ett ytterligare exempel på en situation som kan bli svår att bedöma.

I den föreslagna bestämmelsen 9 c § BrB har det nuvarande begreppet automatisk databehandling ersatts i första meningen med begreppet automatiserad databehandling och sista meningen med begreppet automatiserad informationsbehandling. Det bör klargöras om avsikten är att automatiserad informationsbehandling ska avse något annat än automatiserad databehandling. Vad är i så fall tänkt att det först nämnda begreppet ska ha för innebörd.

#### **11.4 Ett nytt tvångsmedel**

Utredarens förslag är att ett nytt tvångsmedel, frysning av elektronisk kommunikation, införs. Ändamålet med tvångsmedlet ska vara att på området för elektronisk kommunikation förhindra att bl.a. trafikuppgifter och andra uppgifter om kommunikationen går förlorade innan domstol har hunnit ta ställning till användningen av hemliga tvångsmedel.

Frysning är ett förslag till nytt tvångsmedel som förutsätter att det är fråga om förundersökning angående konkret brottslighet av viss svårighetsgrad. Enligt Datainspektionens mening är det en åtgärd som bättre bevakar rätten till privatlivets fred än det förslag till rambeslut inom EU som ålägger operatörer att lagra trafikdata om alla, oavsett misstanke om brott, under mycket lång tid för att kunna användas av de brottsbekämpande myndigheterna. Datainspektionen har mot den bakgrunden ingen erinran mot förslaget.

## **11.5 Förbud mot att rubba bevisning i elektronisk form**

Enligt förslaget ska åklagare få förbjuda den som innehar data i elektronisk form att förstöra, förändra eller på annat sätt göra dessa oåtkomliga om det finns risk att de annars går förlorade.

Eftersom de tekniska förutsättningarna för hantering av data i elektronisk form är komplicerade vill Datainspektionen peka på att en åklagares föreläggande kan behöva innehålla mycket tydliga instruktioner till den mot vilken förbudet riktas om hur denna ska förfara för att inte förstöra, förändra eller på annat sätt göra en viss närmare angiven information i elektronisk form oåtkomlig.

## **11.6.3 Ändrade regler om husrannsakan**

### **Husrannsakan via elektroniska kommunikationsnät (s. 299)**

Utredaren föreslår att de enda regler i 28 kap. 7 § RB som ska vara tillämpliga på husrannsakan via nät är bestämmelserna om rätt att anlita biträde av målsägande, sakkunnig eller annan, om målsäganden eller dennes ombuds rätt att närvara samt om underrättelse till den som har drabbats av åtgärden.

Husrannsakan via nät skapar, som utredaren själv anger, större risker för missbruk, eftersom den som drabbas av husrannsakan inte har samma möjligheter som annars att genom sin närvaro hindra övertramp. Det föreslagna nya tvångsmedlet ligger till sin natur nära tvångsmedel som verkställs i hemlighet. Av rättssäkerhetsskäl föreslår utredaren därför att endast domstol ska få besluta om husrannsakan via nät. Datainspektionen tillstyrker att domstol ska fatta beslut om sådan husrannsakan. Enligt Datainspektionens mening finns det en del ytterligare frågor som behöver belysas för att inspektionen ska kunna ta ställning till om det nya tvångsmedlet kan godtas ur rättssäkerhetssynpunkt. Hur kommer husrannsakan via nät att gå till tekniskt, hur åstadkommer man en säker identifiering av den dator eller datorsystem som ska undersökas, vilka risker finns det för förvanskning av informationen vid en sådan husrannsakan och hur ska dokumentation av de tekniska åtgärder som vidtas vid denna form av husrannsakan säkras är exempel på frågor som behöver närmare belysas.

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

Göran Gräslund

Hans-Olof Lindblom